Vulnerability Assessment for Cascading Failures in Electric Power Systems

Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failures
IEEE PES Computer and Analytical Methods Subcommittee

***Abstract*—Cascading failures present severe threats to power grid security, and thus vulnerability assessment of power grids is of significant importance. Focusing on analytic methods, this paper reviews the state of the art of vulnerability assessment methods in the context of cascading failures. These methods are based on steady-state power grid modeling or high-level probabilistic modeling. The impact of emerging technologies including phasor technology, high-performance computing techniques, and visualization techniques on the vulnerability assessment of cascading failures is then addressed, and future research directions are presented.**

***Index Terms*—Cascading Failure; Vulnerability Assessment; Probability Analysis; Electric Power Systems; Phasor Technology.**

I. Introduction

THE concept of a vulnerable system is defined in [1] as a system that operates with a "reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances". The term *vulnerability* in this paper is defined in the context of cascading events and therefore it is beyond the traditional concept of N-1 or N-2 system security criteria [2]. *Vulnerability* is a measure of the system's weakness with respect to a sequence of cascading events that may include line or generator outages, malfunctions or undesirable operations of protection relays, information or communication system failures, and human errors. The potential sources of system vulnerability are categorized in [3]. In this definition, it is noted that "it is rare that a major system failure is the result of one catastrophic disturbance". In other words, major blackouts often involve a sequence of cascading events. One event may create an operating condition that triggers another event. In an outage scenario, a line fault can cause rerouting of the power flow, leading to overloading of other lines. The overloaded lines may be tripped by impedance relays due to the low voltage and high current operating conditions. Line outages may also cause low voltage and high reactive power demand on nearby generators. The undesirable generator tripping events by over-excitation protection is also a typical cascading pattern. Some other typical patterns of cascading events include line tripping due to loss of synchronism, generator tripping due to abnormal voltage and frequency system condition, and under-frequency or under-voltage load shedding. Identifying these typical patterns of cascading events and studying how these patterns can be combined into sequences is an important research subject [4][5].

Vulnerability is an essential indication of a system prone to cascading failures. Many analytical methods have been proposed for vulnerability assessment. Traditionally, a power system can be modeled as a (quasi-) steady-state system or as a dynamic system. A wealth of literature can be found on vulnerability assessment based on these modeling perspectives. Some recent work also introduced vulnerability assessment which is not based on the traditional steady-state or dynamic models of a power system. Examples include hidden failures, wild life impact, weather impact and complex system effects. The research results in the literature show that the trend of vulnerability assessment of power systems is evaluated from individual events to multiple events, from local area to system wide analysis, and from simple analysis tools (e.g., transient analysis or reliability analysis only) to mixed analysis tools (considering dynamics, reliability, different operations, complex network theory, and their combinations), which is implied by the fact that cascading failures or blackouts are very complex events and a number of factors are involved.

The first paper [6] generated by this Task Force gives a comprehensive overview of the mechanism and properties in terms of cascading failures. This second paper reviews the state of the art of the above mentioned topics in the context of vulnerability assessment for cascading failures. At present, there is not a commonly accepted vulnerability index or assessment method for power systems. If a power system loses a significant portion of its ability to carry the power flows due to cascading line outages, it is considered a vulnerable configuration [7]. This paper reviews this topic based on different modeling approaches: steady-state modeling based analysis is presented in Section II; High-level probabilistic models of cascading in Section III; and role of emerging technologies, including phasor technology, high-

Authors: Ross Baldick, Badrul Chowdhury, Ian Dobson, Zhaoyang Dong, Bei Gou, David Hawkins, Zhenyu Huang (task lead), Manho Joung, Janghoon Kim, Daniel Kirschen, Stephen Lee, Fangxing Li, Juan Li, Zuyi Li, Chen-Ching Liu, Xiaochuan Luo, Lamine Mili, Stephen Miller, Marvin Nakayama, Milorad Papic, Robin Podmore, John Rossmaier, Kevin Schneider, Hongbin Sun, Kai Sun, David Wang, Zhigang Wu, Liangzhong Yao, Pei Zhang (task force chair), Wenjie Zhang, Xiaoping Zhang.

978-1-4244-3811-2/09/$25.00 ©2009 IEEE

performance computing techniques, and visualization techniques on the vulnerability assessment of cascading failures is then addressed in Section IV; Recommendations on industry practices and future research needs in Section V.

II. Vulnerability Assessment with Steady-State Modeling

For most of the time, a power system experiences only slow changes and migrates from one steady state to another. In the context of cascading failures, a scenario could be that power ramping-up of power plants leads to transmission line overloading which triggers impedance relays to trip off the line, and a sequence of cascading events is resulted in. In this case, a (quasi-) steady-state model of the power system is adequate for assessing the vulnerability and analyzing the cascading nature of the events. Based on steady-state modeling, vulnerability can be performed by power flow analysis such as N-x contingency analysis, graph analysis and probability analysis. Though presented separately in the next few sections, the methods may be used in a combined manner.

A. Power flow based analysis

1) N-x contingency analysis

"N-1" contingency analysis is an essential part of industry practices in anticipating potential failures in a power grid [8][9]. In the case of cascading failures, a series of power flows is computed with consideration of sequentially related events such as operations of protective relays and control systems. For example, if a problem occurs on a power grid, such as a transmission line going out of service due to contact with vegetation, there are various issues that may surface across the grid, including line overloading, voltage sag or collapse, and load losses. There may be generation re-dispatch or operator actions in response to those issues. Each switching event results in a power flow case. This approach and its various elaborations are the most systematically developed approach for modeling and simulating cascading failure. Operators refer to such initiating outages as "contingencies" and manage the system in a way that ensures *any single credible contingency will not propagate into a cascading blackout*, which approximately summarizes the N-1 contingency standard established by the North American Electric Reliability Corporation (NERC) [2]. In order to ensure that a single contingency does not result in cascading outages, grid operators continuously run contingency analysis to study all credible "what-if" cases and check for intolerable consequences.

Though it has been a common industry practice, analysis based on the N-1 criterion may not be adequate to assess the vulnerability of cascading failures as the assumption is that a cascading failure is caused by a single credible contingency, but multiple unrelated events may occur in a system and result in cascading failures. Therefore, N-2 and even higher order (N-x) contingency events need to be analyzed. One example is the separation of administrative boundaries – called Balancing Areas (or BAs) – which own, operate, and/or manage their own areas of the grid.

When performing contingency analysis, each BA looks no further than its own boundaries. For areas within the interconnection where several BAs reside next to each other, seams issues may come into play. If the BAs all evaluate their system to be "OK" with the contingencies within their own systems, they will not prepare for the simultaneous occurrence of multiple contingencies. Individually, model results from each BA may show that each contingency does not cause a problem. However, if these contingencies occur simultaneously, there will likely be a very large system-wide impact, but the urgency to restore the system is not fully recognized with today's N-1 or N-1-1 contingency analysis. Past power grid blackouts like the Northeast Blackout in 2003 [10] involve multiple contingencies prior to cascading. This clearly indicates the need for N-x contingency analysis, i.e. analysis of simultaneous occurrence of multiple contingencies. N-x contingency analysis can prepare grid operators with mitigation procedures so as to avoid cascading failures.

N-x contingency analysis is very challenging due to the combinatory number of contingencies and the extremely large amount of computational time. In the western North America power grid, there are approximately 20,000 elements that could fail. Checking each element takes about ½ CPU·second, therefore, the entire N-1 contingency case set would take about 10^4 CPU·seconds. In order to check all the combinations of x contingencies (x = 2,3,4,…), it would take approximately 10^{4x} CPU·seconds. In many cases, this is not feasible. Therefore, an important element of a practical solution is how to identify the credible N-x contingencies from a system-wide perspective [11] and apply high performance computing techniques and hardware to check a maximum number of contingencies within time constraints [12]. Many of existing contingency ranking methods can be applied. The performance of high-performance computing application to N-x contingency analysis heavily relies on computational load balancing. Ref. [12] points out static computational load balancing schemes do not make full use of computational resources due to uneven time required for different cases. A well-designed dynamic computational load balancing scheme considering the CPU speed, network bandwidth and data exchange latency is key to the performance.

2) Simulation models of cascading

TRELSS (Transmission Reliability Evaluation of Large-Scale Systems) [13][14] is an industrial tool used to identify cascading failure problems. TRELSS provides both ac and dc network models. The solution algorithms include fast power flow, unit margin, user participation factor and full or fixed-loss economic generation dispatch, a robust mixed-integer linear programming function for remedial actions, user specified remedial actions such as circuit switching, load transfer or load curtailment when contingencies or system problems occur, and both study and remedial action areas. TRELSS is designed to simulate enumerated contingencies with up to 4 generating units

and 22 circuits taken out, common mode, must-run, maintenance, and protection control group outages, and the impact of normal and adverse weather conditions. System failure criteria include circuit overloads, voltage violations, capacity deficiency, islanding, and area interchange failures. The load model allows three different load interruption classes at each bus, and up to ten load levels can be scaled automatically or specified as separate base cases by the user. TRELSS computes three types of reliability indices: 1) System problem indices include frequency, duration, number of inflicting contingencies, and maximum and average degree of violations of all failure criteria; 2) Load curtailment indices are frequency, duration, number of contingencies resulting in load loss**,** individual power and energy curtailment for buses, contingencies, failure criteria, average indices, and bulk power interruption indices; and 3) Customer indices include customer interruptions, unserved customer hours, system interruption frequency index, system and customer interruption duration index, and system service availability. Better modeling and sequencing of cascading steps have been identified for further development [15].

The Oak Ridge-PSERC-Alaska (OPA) model [16] for a fixed network represents transmission lines, loads and generators with the usual dc load flow approximation. Starting from a solved base case, blackouts are initiated by random line outages. Whenever a line is outaged, the generation and load are re-dispatched using standard linear programming methods. The cost function is weighted to ensure that load shedding is avoided where possible. If any lines were overloaded during the optimization, then these lines are outaged with a fixed probability. The process of re-dispatch and testing for outages is iterated until there are no more outages. The total load shed is, then, the power lost in the blackout. The OPA model neglects many of the cascading processes in blackouts and the timing of events, but it does represent in a simplified way a dynamical process of cascading overloads and outages that is consistent with some basic network and operational constraints. OPA can also represent complex dynamics as the network evolves. The model developed using the PSA suite at Los Alamos National Laboratory represents the timing of blackout events and operator actions [17].

The Manchester model is based on ac power plow that represents a range of cascading failure interactions, including cascading and sympathetic tripping of transmission lines, heuristic representation of generator instability, under-frequency load shedding, post-contingency re-dispatch of active and reactive resources, and emergency load shedding to prevent a complete system blackout caused by a voltage collapse [18]. The Manchester model is used by Rios et al. [19] to evaluate expected blackout cost using Monte Carlo simulation with a 53-bus system and by Kirschen et al. [20] to apply correlated sampling to develop a calibrated reference scale of system stress that relates system loading to blackout size on a 1000-bus large power system.

A new vulnerability index – called the overload risk index (ORI) – is being developed. The method utilizes a two-fold approach that incorporates both deterministic and stochastic calculations. Security analysis involving line outage distribution factors is used to quickly derive the operational state of a system in terms of power flows, while risk assessment is used to calculate the likelihood of such operational states coming into being. The ORI is a measure designed to reflect the likelihood and severity of line overloads in a power system given current system loading levels and component failure rates. Though the specifics concerning the depth of the ORI calculation are still being developed, a general framework and methodology is more defined. Based on the desire to quickly calculate a representative vulnerability index, network sensitivity factors are used to quickly estimate the power flows for a system over a large number of simulations. Line outage distribution factors (LODFs) are used to solve for up to N-3 events in the system, while forced outage rates are used to determine the frequency of these events. Monte Carlo methodology is then used to simulate the likelihood of failure states in the lines of a transmission system, including common structure and right-of-way connections. Failed lines are considered properly disconnected from the system, with all power flows readjusted through the use of the LODFs. Additional reliability calculations could also determine the proper operation of connected relays and breakers. The redistributed power flows are compared with line limitations, and additional outage conditions are determined, allowing for a propagation of line outages due to overloading. Additional contingency tests are performed as lines are removed due to redistribution and new overloading, until the cascade ends without additional overloads or an N-4 or higher event occurs. The index itself is calculated in relation to the amount of line overloads over the total number of simulations using a level of convergence. The significance of this index has yet to be defined in terms of dangerous levels of vulnerability.

3) Hidden failures

The hidden failure in power system refers to permanent defects that would cause a relay or a relay system to incorrectly and inappropriately react to disturbances [22]. The hidden failures in power system are usually triggered by other events, and not frequently occur, but they may have disastrous consequences [21]. Hidden failures of the protection system are modeled with probabilistic approaches as follows [22][23][24][25]:

$$P_{hf} = P_0 \exp(-Z/3Z_3)$$

where P_{hf} is the probability of hidden failure of a relay, Z is the impedance seen by this relay, and Z_3 is the zone 3 setting.

Fast simulation techniques and heuristic random search are applied to identify critical relays that contribute to many possible cascades. Maintaining these relays is a cost-effective mitigation of cascading failures. The availability of protection data to support simulation and the burden of processing it are issues.

4) Risk assessment of cascading failures

All the simulations require some variation in the cases simulated in order to avoid repeatedly simulating the same cascade. This is done by varying the initial conditions of the cascading event or by introducing randomness by Monte Carlo methods in the cascading mechanisms as the cascading proceeds or both.

Several questions can be addressed by these simulations. Some produce likely or high risk cascading sequences and others sample more broadly from all the cascading sequences to approximate the overall cascading risk. Controlling the high risk sequences is one possible tactic to mitigate cascading (e.g. [24][26][27]) and finding the overall cascading risk is basic to evaluating the benefits of mitigation efforts [28]. Some simulations can produce conventional customer availability indices.

All the simulations approximately represent only a selected subset of the possible cascading interactions. This is necessary and pragmatic at the current state of the art. Little is currently known about how much of a gap there is between the various simulations and reality. However, even with this gap, the simulation results can still be of good value in detecting vulnerabilities and guiding mitigation efforts.

III. High-level Probabilistic Models of Cascading

High-level probabilistic models refer to those describing the statistics of cascading failures but with no power flow or network modeling. These models capture some generic features of the cascading process but do not attempt to represent details of the cascading mechanisms. The CASCADE model [29] has an initial disturbance overloading the system, many identical components that fail when their load exceeds a threshold, and the additional loading of components by the failure of other components. The initial component loadings vary randomly between upper and lower bounds. The model parameters describe the size of the initial disturbance and the amount of additional loading when another component fails. Branching process models [30][31][32][33] can approximate the CASCADE model and are established models for cascading processes in many other fields. The failures occur randomly in a series of stages. The model parameters are the average number of initial failures and the average tendency for the failures to propagate. An accelerated propagation failure model for the number of transmission line failures is proposed in [11]. In this model, the conditional probability of a further failure increases geometrically as the cascading event proceeds up to a limited number of failures, such as seven failures. For more than seven failures the system is considered to be collapsed. The accelerated propagation and branching process models are both consistent with aggregated historical data for North American line outages [34], and a closer fit is possible with the accelerated propagation model.

Power grids are not the only types of systems that suffer from cascading failures. This phenomenon also occurs in fault-tolerant computing systems, which have extremely high dependability requirements. For example, banks use fault-tolerant computers to record financial transactions, and overnight-delivery companies employ such systems to track packages. Several software packages have been developed that allow the user to model cascading failures in these types of systems. For example, Galileo [35] incorporates (dynamic) fault trees, which can model propagating failures by using functional dependency gates. OpenSESAME [36] is another software package that quantitatively evaluates fault-tolerant high-availability systems. The input to this package is an enhanced version of a traditional reliability block diagram, thereby allowing inter-component dependencies like failure propagation, failures with a common cause, different redundancy types, and non-dedicated repair. The combinatorial growth in the number of ways cascading failures can occur make them very difficult to analyze, and [37] develop a continuous-time Markov chain model of a dependability system that explicitly tackles this problem. This paper also describes a software package that was developed to take as input a high-level view of the system as a collection of components, from which it calculates various dependability measures of the overall system.

These high-level probabilistic models offer some new possibilities for understanding and monitoring cascading failure. They provide analytic formulas for the total number of failures as functions of easily understood parameters quantifying the overall progression of the cascading failure. If these models become established, they could allow statistical estimation of the model parameters from short observed or simulated data sets and hence the estimation of the total number of failures from short data sets. This would enable the quantification of overall cascading risk from real data or simulations. That is, it could become possible to monitor cascading risk from real data and quantify the risk benefits of simulated improvements. Note that since the high-level probabilistic models do not model detailed cascading mechanisms, they cannot be used as detailed simulations to suggest weaknesses that should be fixed or to understand particular cascading sequences. The high-level probabilistic models are complementary to more detailed models.

A. Graph analysis of grid topology

A category of vulnerability assessment for cascading failures is the application of graph theory to study the power grid topology, largely ignoring the electrical quantities and power flow constraints. Several graph analysis techniques have been applied to power grid vulnerability assessment, including small-world networks, scale-free networks, and centrality [38]. The basis of graph analysis applications is the mapping of the power grid topology to a complex network by converting generators and substations to nodes and transmission lines and transformers to links with impedance being the path length. The resulting network is an undirected and sparsely connected graph with N nodes and K links.

1) Small-world network

The *small-world network* concept was introduced to study social networks [39][40]. It was discovered that power grids have the properties of a small-world network [41][42]: having relative big clustering coefficient and relative small characteristic length path (i.e. impedance in the case of power grids). Clustering efficient C and characteristic length path L are defined in the following equations:

$$C = \frac{1}{N}\sum_i \frac{\text{number of edges in } G_i}{k_i(k_i-1)/2}$$

where k_i is the number of neighboring nodes of node i and G_i is the sub-graph associated with node i.

$$L = \frac{1}{N(N-1)}\sum_{i\neq j} d_{ij}$$

where d_{ij} is the shortest path length between nodes i and j.

Figure 1 illustrates the concept of small-world networks. P is an index of randomness. Small-world properties exist when $0 < P < 1$. Small-world network theory reveals that a few remote connections greatly decrease the path length, i.e. the electrical distance. The loss of those remote connections will increase the characteristic path length, decrease the transfer capacity of power grid, cause partial power shortage and ultimately lead to cascading failures. As a result these remote connections have important influence on power system stability. If we can identify these remote connections, the vulnerable lines in the power grids can be identified [43].

A cascading failure model based on small-world networks was proposed in [44] and can be used to identify the vulnerable lines. The model assumes that a node will fail if a given fraction γ of its neighbors have failed. Starting with initial failures on a few isolated nodes, the process will become cascading when these initial failures lead to subsequent failures due to exceeding of the fraction γ. Those lines with the initial failures would be the remote connections and are the vulnerable lines according to the small-world network theory. A Monte-Carlo search can be conducted in combination with the small-world network cascading failure model to identify all the vulnerable lines.

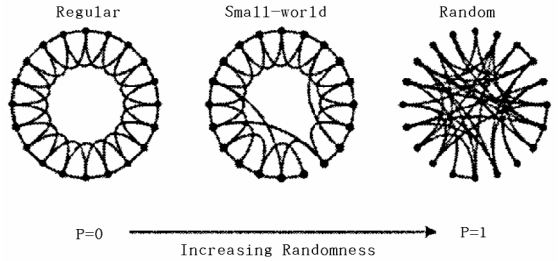

Figure 1 Small-world network

2) Scale-Free Networks

The *scale-free network* model was proposed by Barabasi and Albert in 1999. The formation of scale-free networks is described as a two-step process in [45] – *Growth* and *Preferential Attachment*. *Preferential Attachment* results in a vast number of links. The step of *Growth* starts with a small number n_0 of nodes and at every time step, adds a new node with m ($\leq n_0$) links to m different nodes already existing in the network. The step of *Preferential Attachment* determines which new node should be added at each time step using the probability of a new node connecting to an existing node i. The probability P_i is defined below:

$$P_i = \frac{k_i}{\sum_j k_j}$$

where k_i, the degree of node i, is the total number of its connections, and j is the rest of the nodes. Thus, the larger the degree, the "more important" the node is in a network [46]. After α time steps, this process results in a network with N (= $\alpha + n_0$) nodes and $m\alpha$ links.

Scale-free networks have important properties that the degree distribution follows the power-law distribution and a few nodes have a large number of links but most nodes have only a few links. Simultaneity scale-free networks have other properties, e.g., they are remarkably resistant to accidental attacks but extremely vulnerable to coordinated ones.

Ref. [47] applies the scale-free network theory to the power grid and derives a measure of "electrical centrality" for ac power networks. It was found that when measured electrically, power networks appear to have a scale-free network structure. Thus, unlike previous studies of the power grid topology, the scale-free network application reveals that power networks have a number of highly-connected "hub" buses. This result and the structure of power networks in general are likely to have important implications for the reliability and security of power networks. **Based on topological characteristics of scale-free networks and discrete particle swarm optimization, a skeleton-network reconfiguration strategy is proposed in [48].** It is expected that the theory of scale-free networks will play an important role in the study of power system blackouts and related problems.

3) Betweenness centrality

Betweenness centrality intends to assess the load on the nodes or links of a network with the assumption that communication between any two nodes is done along the shortest path. The betweenness centrality of a node i – $C_B(i)$ – and a link l – $C_B(l)$ are defined as follows [49][50][51]:

$$C_B(i) = \sum_{(j,k)} \frac{a_{jk}(i)}{a_{jk}}, \quad C_B(l) = \sum_{(j,k)} \frac{a_{jk}(l)}{a_{jk}}$$

where a_{jk} is the number of shortest paths between nodes j and k, $a_{jk}(i)$ is the number of shortest paths between j and k containing node i, and $a_{jk}(l)$ is the number of shortest paths between j and k containing link l. The a's are considered the load of a node or link.

If the betweenness centrality exceeds a pre-specified threshold, i.e. $C_B(l) > C_B^{\max}$ (or $C_B(i) > C_B^{\max}$), link l (or node i) is overloaded and removed from the graph. All betweenness centrality is updated. As the iteration process goes on, a cascading failure propagates. In this application, an underlying assumption is that the capacity for each link and each node is the same, which is not true for a power grid. To overcome this limitation, diversified capacity is introduced in

[52][53]. The capacity of node i is proportional to its initial load, i.e. $C(i) = (1 + \alpha)a_{i0}$, where α is a tolerance parameter that denotes the ability of a node's handling increasing load in order to resist disturbances. The betweenness approach is further improved by the introduction of an efficiency index [54][55]. The vulnerability assessment with the efficiency index suggests that the removal of 0.33% of the high-load transmission nodes results in an efficiency loss of 40% and the loss of one node with high load can decrease the efficiency by 25%.

IV. Role of Emerging Technologies

This section reviews the impact of some of the emerging technologies, including phasor technology, advanced visualization, high-performance computing (HPC), and data mining, on cascading failure analysis.

A. Phasor technologies

Phasor measurement units (PMUs) can provide operators with time-synchronized phasor data, which contain valuable dynamics information indicating system vulnerabilities and even precursor signals of potential system collapse. In order to help operators beware of serious system vulnerabilities and predict cascading failures, a scheme based on phase-space visualization and pattern recognition has been proposed to find "precursor signals", e.g. abnormal dynamics patterns, recorded by PMUs [56]. The scheme monitors real-time phase-space snapshots about critical system variables measured by PMUs and analyze their dynamic patterns using the knowledge obtained through offline learning. If PMUs are installed at multiple key locations in a transmission system, a real-time, approximate potential energy of the system can be calculated using synchronized phasor data. Visualizing the potential energy index in its phase space can clearly exhibit "precursor signals" indicating potential cascading failures before control actions are too late to help. In general, phasor measurement, given its high-speed and time-synchronization, provides a well-captured current condition of the power grid to cascading analysis tools as input. It also opens opportunities for new analysis algorithms and methods for cascading failures [57][58].

B. Advanced Visualization

An situational awareness tool presented in [59] is a wide-area visualization tool based on Google Earth® to enhance the situational awareness of power grids. It helps power system operators across different regions to understand the operational condition in its own region as well as neighboring regions to reduce the likelihood of large-scale blackouts. Customized libraries describe the electric transmission network in different regions as well as the status of each transmission line. The visualization capabilities include: line descriptions, line flows and status of outage lines; geo-spatio-temporal information and impacts – population, transportation, and infrastructure impacts; analysis and predictions results; and weather impacts and overlays.

Once fully implemented, this tool will have various features to support situational awareness including real-time status of transmission lines, predictive impact models & animated replay, and data analysis as well as visualizing analysis results from cascading analysis tools.

C. High-performance computing techniques and hardware

Given the large size of practical power systems and the large number of cases to be analyzed, cascading failure analysis is a computation- and data-intensive process. High-performance computing techniques (e.g. paralleling computing) and hardware (multi-processor computers) would be a must for cascading failure analysis. The computer industry is undergoing a significant change from the traditional single-processor computers to multi-core-based computing platforms [60]. Experimental 80-core processors were announced by Intel and 128-core by IBM. A key implication of this multi-core trend is that while the aggregate computational power of a microprocessor is increasing, only explicit parallel algorithms can take advantage of the increased number of cores and realize the computational power of modern and next generation microprocessors [61]. The trend is a result of thermal limitations with the current CMOS process technologies, which limits the speed of single processors [62]. Early application of high-performance computing to state estimation and contingency analysis have achieved promising results [63][64][65]. When applying HPC technologies, a key success factor is the match of computer architectures with problem characteristics. Shared memory computers with a multi-threading environment can efficiently execute applications with irregular memory references such as state estimation and dynamic simulation. Distributed memory architecture, like PC clusters well suits applications which can be divided into sub-tasks with minimum data communication requirements, like contingency analysis in power systems.

D. Data mining

Data mining has been identified as one of the emerging technologies to assess stability for cascading failures. It is the process to identify valid, previously unknown, potentially useful and understandable information from large databases, [66]. Vulnerability assessment for cascading failures is a very complex task which requires processing of huge amounts of data in order to obtain reliable results in very short time. For most realistic large scale power systems, the amount of corresponding system operational data has been increasing exponentially. The most important feature is their statistical robustness, i.e. if the system is assessed to have a security problem, then it will experience such problem with given probability of occurrence if no actions are taken. Data mining based real-time stability assessment approaches are able to provide statistically reliable results. Data mining has been successfully applied to a number of areas including monitoring and optimization of thermal power plants, fault diagnosis and condition monitoring of power system equipment such as transformers, obtaining customer load

profile in an electricity market [67], and wide variety of tasks for power system operations [68][69][70]. A number of data mining methods have been proposed, such as classification algorithms [71], decision tree algorithms [72], statistical methods [73], neural-network-based methods [74]. Their application to cascading failure analysis should be explored [75].

V. Concluding Remarks and Future Research Needs

Since power system cascading is diverse, complicated, and computationally intractable, there is no single model, tool or approach that can address all aspects of cascading or answer all the questions about managing the risk of cascading failures. However, we expect that useful approaches and answers can be developed for some specific questions. Each question will require different modeling, approximations, assumptions and data in order to make them tractable. We now list some specific questions that are or might be capable of solution to challenge the power system community and help organize the various ongoing efforts to develop methods and tools. We emphasize that the first six of the following questions each has several very different versions according to the operational or planning time scale considered:

- What is the overall risk of cascading failure (including rare events)?
- What are the cascading failure sequences of highest probability or highest risk?
- What are the next few possible or high risk or high impact cascading events?
- What is the vulnerability to cascading resulting from an attack of a limited size?
- Where is the "edge" for unacceptable risk of cascading failure?
- How do we quantify the benefits and costs of new devices, procedures, upgrades, or security criteria with respect to cascading failure risk?
- What happened in a particular cascading blackout? What is learned and what changes should be made?
- What are the monetary, human and reputational costs of a given cascading failure incurred by each of the various groups affected?
- How do we balance cascading risk against mitigation costs?

The methods presented in previous sections can partially answer some of the questions. Further research is needed to improve those methods so vulnerability assessment can be performed with confidence and the above questions can be fully answered.

In addition, future research needs in vulnerability assessment for cascading failures also include methods based on dynamic modeling and non-traditional modeling as stated below.

A. Vulnerability Assessment with Dynamic Modeling

With the evolution of cascading events, the angular instability, voltage and power oscillations, significant imbalances between reactive power reserves and the demand may occur, leading to uncontrolled system separation and voltage collapse. Voltage collapse was a key factor in the 1996 blackout and the 2003 blackout in North America. It is identified that distance relays plays a big role in various regional cascading outages. These distance relays should also need to be modeled properly in simulating the cascading events. In some systems, out of step relays would block zone 2 and zone 3 from tripping. However, simulations and real cascading outages show line tripping on Zone 1. Steady state analysis cannot provide the details of scenarios based on system representation and modeling. In order to study cascading failures due to the dynamics of a power system, comprehensive and detailed dynamic models are necessary. Generator and protection/control devices play a critical role in the dynamic behavior of a power system. Generator controllers including automatic voltage regulators, power system stabilizers, over-excitation limiters, and governors need to be modeled. Dynamic response of generator plays an important role in power system blackout events. The deployment of power system stabilizers is a critical component in the U.S. Western Interconnection to increase the stability of the system. Protective devices can contribute to the cascaded events. Typical generation protection devices are generator loss of field, loss of synchronism, over/under-voltage and under-frequency relays. Load characteristics should be included in the dynamic models. In addition, automatic under-frequency load shedding and under-voltage load shedding scheme may be triggered when the system voltage or frequency in some area drops to a pre-specified value for a period of time. They should be incorporated into dynamic simulations. It is highly desirable to develop simulation tools that incorporate these dynamic models that will enable realistic and detailed simulations and analysis of complex outage scenarios.

B. Vulnerability Assessment with Non-traditional Modeling

Traditional power system modeling is focused on network topology and/or physical equipment, e.g. transmission lines, transformers, and generators. However, cascading failures can be caused by some factors other than the topology or physical equipment characteristics. Examples include vegetation management, and weather impact. These factors are non-traditional in the sense that they are not normally considered as part of current operational planning and real-time analysis tools.

"Terrain, Training, Tools and Terrorists" are commonly referred to as "4T's". Since each of these factors can have a major impact on increasing the risk of cascading failures, a holistic approach will somehow quantify the impact of these factors. *Terrain* includes trees as a well as other local environmental conditions such as salt spray, birds. The 2003 Northeast Blackout Report [10] concluded vegetation management is one of the causes of the blackout. The impact of Terrain can be factored into vulnerability assessment by adjusting the probabilities of equipment outages. The lack of

training of power system operators for handling emergency situations has been well documented and has often been a cause for major disturbances. The evaluated performance levels of operators could be factored into the assessment of the likelihood of cascading outages, but how these operator performance levels can be quantitatively related to the probabilities of cascading outages is an open area for research. *Tools* include the hardware and software tools used for data acquisition, alarming, data communications, data visualization, data processing (state estimation) and data analysis (contingency analysis). In a number of major blackouts (northeast blackouts of 1965, 1977 and 2003), false or incomplete information given by the tools have been a factor. Quantifying the impact remains to be a question. *Terrorists* become more recognized issue after the 911 event. Not only the physical networks may be attacked, but also cyber security may be compromised. Cyber security has been a research topic for years [76]. They are yet to be incorporated into cascading failure analysis.

In the area of weather impact, of significant importance to power grids is temperature. It affects line sags, load demand, energy generation (e.g. solar). We can use temperature as a factor in a variety of weather conditions that can increase risk of major outages. The conditions include: 1) Very hot, calm and sunny days which decrease equipment thermal ratings and decrease wind generator output; 2) Low temperature and high humidity days that cause transmission line icing; 3) Days with thunderstorms and lightning strikes; and 4) Sun spots and increased levels of solar activity.

Analysis towards these factors is at a beginning stage. Significant work needs to be done to develop methods which can consider these factors in cascading failure analysis.

VI. References

[1] L. H. Fink, K. Carlsen, "Operating under stress and strain," IEEE Spectrum, pp. 48-53, March 1978.

[2] NERC standards, Transmission System Standards – Normal and Emergency Conditions, available at www.nerc.com.

[3] C. C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A. G. Phadke, "Conceptual Design of the Strategic Power Infrastructure Defense (SPID) System", *IEEE Control System Magazine*, Aug. 2000, pp.40-52.

[4] J. Li, K. Yamashita, C. C. Liu, P. Zhang and M. Hofmann, "Identification of Cascaded Generator Over-Excitation Tripping Events," 16th Power Systems Computation Conference 2008, Glasgow, Scotland.

[5] C. C. Liu, et al., Learning to Recognize the Vulnerable Patterns of Cascaded Events, EPRI Technical Report, 2007.

[6] IEEE PES CAMS Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failures, "Initial review of methods for cascading failure analysis in electric power transmission systems," IEEE Power and Energy Society General Meeting, Pittsburgh, PA, USA July 2008.

[7] C. C. Liu and F. F. Wu, "Analysis of Vulnerability of Power Network Configurations," Proc. IEEE Int. Symp. Circuits and Systems, 1985, pp. 1513-1515.

[8] Quirino Morante, Nadia Ranaldo, Alfredo Vaccaro, Member, IEEE, and Eugenio Zimeo, "Pervasive Grid for Large-Scale Power Systems Contingency Analysis," IEEE Transactions on Industrial Informatics, vol. 2, no. 3, August 2006

[9] Chen, R.H.; Jingde Gao; Malik, O.P.; Shi-Ying Wang; Nian-De Xiang; "Automatic contingency analysis and classification," The Fourth International Conference on Power System Control and Management, 16-18 April, 1996.

[10] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United State and Canada: Causes and Recommendations", April 2004. Available at https://reports.energy.gov/.

[11] Qiming Chen; McCalley, J.D.; Identifying high risk N-k contingencies for online security assessment, Power Systems, IEEE Transactions on, Volume 20, Issue 2, May 2005 Page(s):823 – 834.

[12] Zhenyu Huang, and Jarek Nieplocha, "Transforming Power Grid Operations via High-Performance Computing," in: Proceedings of PES-GM2008 – the IEEE Power and Energy Society General Meeting 2008, Pittsburgh, PA, USA, July 20-24, 2008.

[13] M. Kumbale, T. Rusodimos, F. Xia, and R. Adapa, TRELSS: A Computer Program for Transmission Reliability Evaluation of Large-Scale Systems, EPRI TR-I00566 3833-1, Vol. 2: User's Reference Manual, April 1997.

[14] Rodney C. Hardiman, Murali Kumbale, and Yuri V. Makarov, Multiscenario Cascading Failure Analysis Using TRELSS. CIGRE/IEEE PES International Symposium on Quality and Security of Electric Power Delivery Systems, 8-10 Oct. 2003.

[15] Rodney C. Hardiman, Murali Kumbale, and Yuri V. Makarov, "An Advanced Tool for Analyzing Multiple Cascading Failures," The 8th International Conference on Probabilistic Methods Applied to Power Systems, Iowa State University, Ames, Iowa, September 12-16, 2004.

[16] B.A. Carreras, V.E. Lynch, I. Dobson, D.E. Newman, Critical points and transitions in an electric power transmission model for cascading failure blackouts, Chaos, vol. 12, no. 4, December 2002, pp. 985-994.

[17] M. Anghel, K.A. Werley, A.E. Motter, Stochastic model for power grid dynamics, 40th Hawaii International Conference System Sciences, Hawaii, Jan 2007.

[18] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," Int. J. Electr. Power Energy Syst. 28, 627–633, 2006.

[19] M. A. Rios, D. S. Kirschen, D. Jawayeera, D. P. Nedic, and R. N. Allan, "Value of security: modeling time-dependent phenomena and weather conditions," IEEE Trans. Power Syst. 17, 543–548, 2002.

[20] D. S. Kirschen, D. Jawayeera, D. P. Nedic, and R. N. Allan, "A probabilistic indicator of system stress," IEEE Trans. Power Syst. 19, 1650–1657, 2004.

[21] A. G. Phadeke, J. S. Thorp, "Expose hidden failures to prevent cascading outages," IEEE Computer Application in Power, vol.9, pp. 20-23, 1996.

[22] S. Tamronglak, S.H. Horowitz, A.G. Phadke, J.S. Thorp, Anatomy Of Power System Blackouts: Preventive Relaying Strategies, IEEE Transactions on Power Delivery, Vol. 11, No. 2, April 1996

[23] K. Bae, J. S. Thorp, A stochastic study of hidden failures in power system protection, Decision Support Systems, vol. 24, no. 3/4, pp. 259-268, Jan. 1999.

[24] H. Wang, J. S. Thorp, Optimal locations for protection system enhancement: A simulation of cascading outages, IEEE Trans. Power Delivery, vol. 16, no. 4, October 2001, pp. 528-533.

[25] J. Chen, J.S. Thorp, I. Dobson, Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model, International Journal of Electrical Power and Energy Systems, vol. 27, no. 4, May 2005, pp. 318-326.

[26] L. Mili, Q. Qui, A.G. Phadke, "Risk assessment of catastrophic failures in electric power systems," International Journal of Critical Infrastructures, vol. 1, no. 1, pp.38-63, 2004.

[27] J.D. McCalley, S. Khaitan, Risk of cascading outages, Part A, PSerc publication 08-04, February 2008. available at http://www.pserc.org.

[28] I. Dobson, B.A. Carreras, V.E. Lynch, D.E. Newman, Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization, Chaos, vol. 17, no. 2, 026103, June 2007

[29] I. Dobson, B.A. Carreras, D.E. Newman, A loading-dependent model of probabilistic cascading failure, Probability in the Engineering and Informational Sciences, vol. 19, no. 1, January 2005.

[30] I. Dobson, B.A. Carreras, D.E. Newman, A branching process approximation to cascading load-dependent system failure. 37th Hawaii International Conference on System Sciences, Hawaii, January 2004.

[31] I. Dobson, B.A. Carreras, D.E. Newman, Branching process models for the exponentially increasing portions of cascading failure blackouts, 38th Hawaii International Conference on System Sciences, January 2005, Hawaii.

[32] I. Dobson, K.R. Wierzbicki, B.A. Carreras, V.E. Lynch, D.E. Newman, An estimator of propagation of cascading failure, 39th Hawaii International Conference on System Sciences, January 2006, Kauai, Hawaii.

[33] I. Dobson, K. R. Wierzbicki, J. Kim, H. Ren, Towards quantifying cascading blackout risk, Bulk Power System Dynamics and Control - VII, Charleston, South Carolina, USA, August 2007.

[34] R. Adler, S. Daniel, C. Heising, M. Lauby, R. Ludorf, T. White, An IEEE survey of US and Canadian overhead transmission outages at 230 kV and above, IEEE Trans. Power Delivery, vol. 9, no. 1, Jan 1994, pp. 21-39.

[35] K. J. Sullivan, J. B. Dugan and D. Coppit, The Galileo Fault Tree Analysis Tool, Proceedings of the 29th Annual International Symposium on Fault-Tolerant Computing, IEEE, 1999, 232-235.

[36] M. Walter, M. Siegleb and A. Bode, OpenSESAME --- the simple but extensive, structured availability modeling environment, Reliability Engineering & System Safety, Volume 93, Issue 6, June 2008, pp. 857-873.

[37] S.M. Iyer,M. Nakayama and A.V. Gerbessiotis, A Markovian Dependability Model With Cascading Failures, preprint, Dept. of Computer Science, New Jersey Institute of Technology, Newark, NJ 07102-1982, U.S.A. 2007.

[38] Ke Sun, Zhen-Xiang Han, Analysis and Comparison on Several Kinds of Models of Cascading Failure in Power System, 2005 IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific, Dalian, China

[39] P. S. Dodds, R. Muhamad, D. J. Watts, "An Experimental Study of Search in Global Social Networks", Science, vol. 301, pp. 827-829, 2003.

[40] D. J. Watts, S. H. Strogatz, "Collective Dynamics of 'Small-world' Networks," Nature, vol. 393, pp. 440-442, 1998.

[41] Lu Zongxiang, Meng Zhongwei, and Zhou Shuangxi, Cascading Failure Analysis of Bulk Power System Using Small-World Network Model, The 8th International Conference on Probabilistic Methods Applied to Power Systems, Iowa State University, Ames, Iowa, September 12-16,2004.

[42] G. Surdutovich, C. Cortez, R. Vitilina, J. R. Pinto da Silva, "Dynamics of 'Small World' Networks and Vulnerability of the Electric Power Grid," The VIII Symposium of Specialists in Electric Operational and Expansion Planning, 2002.

[43] Xiaogang Chen, Ke Sun, Yijia Cao, and Shaobu Wang , Identification of Vulnerable Lines in Power Grid Based on Complex Network Theory.

[44] D. J. Watts, "A simple model of global cascades on random networks," Proc. Natl. Acad Sci. vol. 99, pp. 5766-5771, 2002.

[45] X. Li, G. R. Chen, "Local-world Evolving Network Model", Vol. 328, Physical A, 2003, pp.274-286.

[46] Xiao Fan Wang; Guanrong Chen; "Complex networks: small-world, scale-free and beyond." IEEE Circuit and Systems Magazine, Vol. 3, No. 1, 2003 Page(s):6 - 20

[47] P. Hines, S. Blumsack, "A Centrality Measure for Electrical Networks." The Proceedings of 41sh Annual Hawaii International Conference on System Science, 7-10 Jan. 2008 Page(s):185 – 185.

[48] Y. Liu and X. Gu, "Skeleton-Network Reconfiguration Based on Topological Characteristics of Scale-Free Networks and Discrete Particle Swarm Optimization." IEEE Trans. on Power Systems, Vol. 22, No. 3, Aug. 2007, pp: 1267-1274.

[49] P. Holme, "Edge overload breakdown in evolving networks," Phys. Rev. E vol. 66, 036119 ,2002.

[50] P. Holme, B. J. Kim, "Vertex overload breakdown in evolving networks," Phys. Rev. E vol. 65, 066109, 2002.

[51] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, "Attack vulnerability of complex networks," Phys.Rev.E, vol. 65, 056109, 2002.

[52] Y. C. Lai, A. E. Motter, T. Nishikawa, "Attacks and Cascades in Complex Networks," Lect. Notes Phys, vol. 650, pp. 299-310, 2004.

[53] A. E. Motter, Y. C. Lai, "Cascade-based attacks on complex networks," Phys. Rev. E, vol.66, 065102, 2002.

[54] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," Phys. Rev. E, vol. 69, 045104, 2004.

[55] R. Kinney, P. Crucitti, R. Albert, V. Latora, "Modeling cascading failures in the North American power grid," [Online]. Available: http://www.springerlink.com/content/v163831253t3m122/

[56] K. Sun, S. Lee, "Power System Security Pattern Recognition Based on Phase Space Visualization", *IEEE Int. Conf. on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT 2008)*, Nanjing, April 6-9. 2008

[57] C. Taylor, D. Erickson, K. Martin, R. Wilson, and V. Venkatasubramanian, "WACS – Wide Area Stability and Voltage Control System: R&D and Online Demonstration," *Proceedings of the IEEE*, Vol. 93, No. 5, May 2005, pp. 892-906.

[58] Marek Zima, and Goran Andersson, Wide Area Monitoring and Control as a Tool for Mitigation of Cascading Failures, The 8th International Conference on Probabilistic Methods Applied to Power Systems, Iowa State University, Ames, Iowa, September 12-16, 2004.

[59] http://www.ornl.gov/sci/electricdelivery/visualization.html.

[60] Niagara: A Torrent of Threads, http://www.aceshardware.com/reads.jsp?id=65000292

[61] T. Ungerer, B. Robi, and A. Jurij, "A survey of processors with explicit multithreading," *ACM Comput. Surv.,* vol. 35, pp. 29-63, 2003.

[62] Moore, Gordon E. Cramming more components onto integrated circuits. Electronics Magazine. Electronics, Volume 38, Number 8, April 19, 1965.

[63] Zhenyu Huang, and Jarek Nieplocha, "Transforming Power Grid Operations via High-Performance Computing," in: Proceedings of the IEEE Power and Energy Society General Meeting 2008, Pittsburgh, PA, USA, July 20-24, 2008.

[64] J. Nieplocha, A. Marquez, V. Tipparaju, D. Chavarría-Miranda, R. Guttromson, Zhenyu Huang, "Towards Efficient Power System State Estimators on Shared Memory Computers," in: Proceedings of the IEEE Power Engineering Society General Meeting 2006, Montreal, Canada, June 18-22, 2006.

[65] Zhenyu Huang, Ross Guttromson, Jarek Nieplocha and Rob Pratt, "Transforming Power Grid Operations via High-Performance Computing," Scientific Computing, April 2007.

[66] C. Olaru and L. Wehenkel, "Data Mining", CAP Tutorial, July 1999, pp. 19 – 25.

[67] V. Figueiredo, F. Rodrigues, Z. Vale and J. B. Gouveia, "An electric energy consumer characterization framework based on data mining techniques", IEEE Trans. on Power Systems, Vol. 20, No. 2, May 2005, pp. 596 – 602.

[68] S. Madan, W.-K. Son and K.E. Bollinger, "Applications of Data Mining for Power Systems", Proc CCECE'97, pp 403 – 406.

[69] S.K. Tso, J.K. Lin, H.K. Ho, C.M. Mark, K.M. Yung and Y.K. Ho, "Data mining for detection of sensitive buses and influential buses in a power system subjected to disturbances", IEEE Trans. on Power System, Vol. 19, no. 1, Feburary 2004, pp. 563 – 568.

[70] J.A. Pecas Lopes, and M.H. Vasconcelos, "On-line dynamic security assessment based on Kernel Regression Trees", 2000 IEEE, pp. 1075 – 1080.

[71] Sebastiani, F. (2002) "Machine Learning in Automated Text Categorization", ACM Computing Surveys (CSUR), 34(1):1-47.

[72] Quinlan, T.R. (1996) "Improved use of continuous attributes in c4.5", Journal of Artificial Intelligence Research, 4:77-90.

[73] Lewis, D.D. (1998) "An Naïve (Bayes) at Forty: The Independence Assumption in Information Retrieval", Proc. ECML-98, 10th European Conference on Machine Learning, pp. 415, Chemnitz, DE, 1998. Springer Verlag, Heidelberg, DE.

[74] Rumelhart, D.E., G.E. Hinton, and R.J. Williams (1986) "Learning internal representations by error propagation", in D.E. Rumelhart and J.L. McClelland, edt., Parallel Distributed Processing, Cambridge, MA: MIT press.

[75] J.H. Zhao, Z.Y. Dong and P. Zhang, "Mining Complex Power Networks for Blackout Prevention", Proc of the Thirteenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Jose, CA, 12-15 Aug 2007.

[76] C. Ten, C. C. Liu, M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees." The Proceedings of PES General Meeting, 24-28 June 2007 Page(s):1 – 8.