

Initial review of methods for cascading failure analysis in electric power transmission systems

IEEE PES CAMS Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failures

Abstract—Large blackouts are typically caused by cascading failure propagating through a power system by means of a variety of processes. Because of the wide range of time scales, multiple interacting processes, and the huge number of possible interactions, the simulation and analysis of cascading blackouts is extremely complicated. This paper defines cascading failure for blackouts and gives an initial review of the current understanding, industrial tools, and the challenges and emerging methods of analysis and simulation.

I. INTRODUCTION AND DEFINITION OF CASCADING

Large blackouts generally involve complicated and cascading chains of events. The diverse phenomena involved in these cascades are explained in accounts of major blackouts such as [42], [48], [65], [87], [49], [84], [88]. Large blackouts, although infrequent, are costly to society with estimates of direct costs up to billions of dollars. There are also indirect costs such as possible social disruptions and the propagation of failures into other infrastructures such as communications, water supply, natural gas, and transportation. The vital importance of electric power to our society motivates continued attention to maintaining power system reliability and developing new methods to manage the risks of cascading blackouts.

We define cascading failure as a sequence of dependent failures of individual components that successively weakens the power system. This definition is consistent with the usage in [10]. It differs from [75], who limit their definition to failures that propagate between infrastructures.

In our definition we view the power system as including not only the many physical components but also the software, procedures, people, and organizations that design, operate, and regulate the power system. While the initial failure can usually be considered as being a random event, a causal link exists between the subsequent events. The nature of this link varies. In some cases it is “electrical” (e.g. when the loss of components causes other components to become overloaded). It can also be due to control or protection devices (both hardware and software) that react correctly or incorrectly to previous events. Finally, it can involve human operators that take inappropriate actions or fail to take action either due to lack of training, the unavailability of support tools, lack of situational awareness, or inappropriate procedures. These causal links are often “hidden” in the sense that they do not manifest themselves until some event exposes their existence. The best known example is hidden failures in protection relays that disconnect components unnecessarily when there is a fault.

Authors are Ross Baldick, Badrul Chowdhury, Ian Dobson (task lead), Zhaoyang Dong, Bei Gou, David Hawkins, Henry Huang, Manho Joung, Daniel Kirschen, Fangxing Li, Juan Li, Zuyi Li, Chen-Ching Liu, Lamine Mili, Stephen Miller, Robin Podmore, Kevin Schneider, Kai Sun, David Wang, Zhigang Wu, Pei Zhang (task force chair), Wenjie Zhang, Xiaoping Zhang.

II. CHALLENGES OF CASCADING

Consider checking combinations of failures in a power system model with n components. For practical models for large blackouts, n is in the thousands or tens of thousands. Checking for single failures requires only n cases to be checked, but checking for combinations of k successive failures requires n^k cases to be checked, which rapidly becomes infeasible even with the fastest computers for modest values of k . But large blackouts can involve cascades of tens to hundreds of events. It is clear that exhaustively checking all possible combinations of cascading failures that could lead to blackouts in practical power system models is computationally infeasible.

Because considerable effort is devoted to mitigating the likely and foreseen causes of failure, there is a tendency for blackouts to involve rare, unexpected or unforeseen events or combinations of events. There are a huge number of such events. Although each particular blackout can be explained (with effort) as a causal chain of events after it occurs, it is not feasible to identify all possible causes before the blackout.

Although there is a tendency to think that all blackouts happen during peak load days, the reality is that many blackouts occur during “shoulder” periods (spring and fall). During these periods, the grid operators typically have many facilities that are out of service for maintenance, repair, new construction or replacement. While the outage of each facility looks acceptable, the combination of these outages changes the power flows and dynamic characteristics of the system. The result may be a much higher probability of a cascading outage due to the unexpected forced outage of other pieces of equipment or operating mistakes.

Cascading phenomena are complicated because of the diversity of failures and the many different mechanisms by which failures can interact. There are varying modeling requirements and timescales (milliseconds for electromechanical effects and tens of minutes for voltage support and thermal heating). Combinations of several of types of failures and interactions can typically occur in large blackouts, including cascading overloads, failures of protection equipment, transient instability, forced or unforced initiating outages, reactive power problems and voltage collapse, software, communication, and operational errors, mismatch between planning studies and operational environment, rare and unusual failures or combinations of failures, operating mistakes and lack of situational awareness. Most work in power system security analysis has so far focused on only one of these aspects of cascading failures. While this approach has made possible impressive advances in understanding of each aspect, it does not provide a framework for understanding the overall phenomenon.

Since an exhaustive computation of all possible combina-

tions of failures is infeasible, and making a very detailed model of all possible failures and their interactions is beyond the state-of-the-art, compromises are needed in modeling and analyzing cascading failure, such as

- Analyze the detailed failures and interactions in a single blackout after it occurs.
- Analyze a selection of most probable or high risk failures.
- Statistically model the overall progression of cascading failures, while neglecting details of the interactions.
- Analyze a simplified power system model to explain the bulk properties of cascading failures, rather than modeling all of the equipment in detail.
- Analyze one or only a few of the cascading mechanisms.
- Analyze only an initial part of the sequence of failures; for example, up to a point of “no return.”
- Use real time information about the current power system configuration and the progress of the cascade (if slow enough) to help limit the possibilities to be considered.

III. INDUSTRY PRACTICE

In North America, the North American Electric Reliability Corporation (NERC) and its predecessor organizations have had standards that address cascading outages since the late 1960s. Until 2005, these standards were voluntary and relied on peer pressure and consensus for implementation. Driven by the 2003 blackout, the Energy Policy Act of 2005 created the basis for mandatory standards, enforcement and penalties. In the USA, the Electricity Reliability Organization is NERC and the main NERC standards addressing cascading failures are EOP-003-1, TOP-004-1, TPL-002-0, TPL-003-0, and TPL-004-0 [67].

The stated purpose of Transmission Operations TOP-004-1 is: “To ensure that the transmission system is operated so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single Contingency and specified multiple Contingencies.” and requires that: “Each Transmission Operator shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.” and that: “Each Transmission Operator shall, when practical, operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by Regional Reliability Organization policy.”

Emergency Preparedness and Operations EOP-003-1 requires that: “After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.” The purpose for EOP-003-1 is to ensure that “a Balancing Authority and Transmission Operator operating with insufficient generation or transmission capacity” has “the capability and authority to shed load rather than risk an uncontrolled failure of the Interconnection.”

Whether explicitly stated or not, for decades the heart of transmission planning in North America has revolved around what is now Table I in Transmission Planning TPL-001-0,

TPL-002-0, TPL-003-0, and TPL-004-0 [67]. Table I defines the system conditions Category A (normal system operations with no contingencies), Category B (event resulting in the loss of a single element or N-1), Category C (event(s) resulting in the loss of two or more (multiple) elements or N-2), and Category D (extreme event resulting in two or more (multiple) elements removed or cascading out of service). For Categories A, B, and C, cascading outages are not permitted. Table I is required reading for academics!

Category A analysis is straightforward: if any elements exceed their applicable rating, then transmission planners will add new transmission facilities, or write and implement procedures to avoid the condition. In the operating time frame, the transmission system will be reconfigured or re-dispatched to eliminate any violations. Category B analysis follows a path similar to Category A except that loss of each facility must be considered. Credible single contingencies are usually selected using engineering judgment, but modern computing capability allows analysis of all failures of single elements or at least a wide selection of them.

Category C analysis is complicated by the number of events that must be considered. Typically this list is reduced to a manageable number of events using engineering judgment. Contingencies that do not cause applicable rating violations are dismissed. However, those that do cause rating violations are not violations of Category C unless they cause unplanned or uncontrolled loss of demand or curtailment of firm transactions or cascading. Distinguishing which contingencies might cascade or result in unplanned or uncontrolled loss of demand is left to the analyst. For a broad study of the system, a typical simple criterion for cascading or unplanned or uncontrolled loss of demand is that overloads exceed 130%.

We note that the advent of defined penalties has resulted in weakening the standards. The operating standard focuses only on the most severe single contingency. The Category D standard used to include a prohibition against cascading but has been reduced to requiring that these events be evaluated for risks and consequences.

The following functions have become more or less standard tools to analyze the various phenomena that can endanger the security of the system and lead to cascading outages. These phenomena have different timescales and generally require different tradeoffs of modeling detail and simulation time. Operators use these tools in real-time or in operational planning to study the consequences of a fault or failure and how these consequences could be mitigated. To simplify the problem, each phenomenon is usually studied separately and interactions between phenomena are often ignored.

Static Security Assessment (SA) - SA programs typically screen a potentially large list of contingencies using fast approximate power flow methods and then solve the most harmful contingencies using a full power flow solution. These programs analyze a single post contingency snapshot.

Transient Security Assessment (TSA) - TSA programs use a combination of direct analysis methods, often based on energy functions for screening, and non-linear time domain simulation to analyze the capacity of the system to withstand various

faults. These programs include transient rotor oscillations and predict whether or not cascading outages will occur due to pole slipping and relay actions caused by power swings. They analyze post contingency conditions with time steps of around 0.01 seconds for up to 10 seconds.

Voltage Security Assessment (VSA) - VSA programs solve the steady state power flow equations, often using continuation methods, to determine P-V and P-Q curves and voltage collapse margins. The VSA programs may analyze a single snapshot of post disturbance conditions and the second-by-second long term response of AGC systems, tap changers and over excitation run back systems.

Small Signal Analysis (SSA) - SSA programs use a linearized system model and eigenvalue calculations to analyze the small signal stability of power systems and predict vulnerability to poorly damped or growing inter-area and inter-machine oscillations.

ATC Analysis - The ATC analysis programs take all of the constraints that are developed by the SA, TSA, VSA and SSA programs and compute the Available Transfer Capacity between specified Points of Receipt and Points of Delivery.

Cascading failure - The commercial TRELSS program [86], [37] has a mode in which it analyzes cascades of outages, protection and operator actions.

Static Security Assessment programs have been routinely used by Reliability Coordinators and large Transmission Operators since the 1980s. Programs for on-line DSA, VSA and SSA are maturing [23], [24] and have been widely deployed just recently. Most of these tools evaluate the consequences for a given contingency considering one of the phenomena. It is much harder to model and analyze successive combinations of the phenomena. In addition, commercial stability analysis programs usually focus on the electrical phenomena and often do not model protection, despite the routine involvement of protection in blackouts. In essence, the assumption is made that only "electrical" problems matter and that the protection, control, and human supervision systems always operate as expected. The more open environment which allows for new entrants and specialist companies bodes well for more rapid development and deployment of novel products [73].

Although power system operating conditions change over time due to load variations, switching actions, etc., the present protective systems are designed and installed based on off-line studies and do not adapt to these changes. Adaptive relaying is a possibility. Can modern relays be blocked during a vulnerable operating condition to avoid degradation of the overall system reliability? [70] shows that the relays can be blocked in real time from a technology point of view, but that it is not fully understood under what scenarios they should be blocked.

It is important to note that the power industry responds to each blackout with lessons learned. Thus each blackout results in an investigation and actions to prevent similar blackouts in the future. This process is one of the ways that power systems are upgraded to maintain reliability.

IV. METHODS OF ANALYSIS

Probabilistic and deterministic approaches. After the fact and with considerable effort, a blackout can be analyzed as sequence of largely deterministic and causal events. For example, for well-studied power systems, simulations can be tuned to reproduce the features of the blackout. However, it is another matter entirely to be able to predict or simulate the events of a blackout before it happens. It is thus often necessary to use probabilistic models. One reason is the huge number of rare, unusual or unforeseeable events that could cause cascading. Moreover, some phenomena are so complicated that it is infeasible to make a detailed deterministic model, obtain the data, and simulate the models quickly enough. For example, Thorp and coworkers [6], [89], [19] model hidden relay failures probabilistically. Other examples of complicated events that are hard to model deterministically are the location and timing of an initial fault, human and software errors, and transient stability. Many phenomena in cascading failure are events that propagate when some threshold is exceeded. Because the state of the power system is always imperfectly known, it may sometimes be useful to model exceeding the threshold as a probabilistic event [97]. Mili et al. [61], [26] propose short-circuit analyses together with reactive reserve calculations to identify the vulnerability regions of a system and thereby significantly decrease the number of cases to be investigated. Another useful initial simplification is to neglect the modeling of the time between cascading events.

From security to resilience. Mili and Dooley distinguish the concept of security from the concept of resiliency [60]. The power system is evolving from a deterministic concept of N-1 security against a credible set of contingencies towards the concept of resiliency to events of substantial risk, including those with low probability but high consequence. Some utilities include a selection of N-2 events and common mode events in their security analyses. Significant reduction in the cases to be considered can be achieved by assessing the impact of multiple faults in real-time and quickly computing remedial actions [20]. Reconfiguration can be viewed as a preventive or remedial action against cascading events. In anticipation of a vulnerable operating condition, such as a potential sabotage, or during a cascade, the power grid might be islanded to limit the spread of problems [53]. The vision of a self-healing power grid has attracted some power engineering researchers [56]. A self-healing grid would determine by itself the actions to take to recover from a vulnerable operating condition. A good example of self-healing actions is adaptive load shedding [44].

Formulation of risk objectives. Suppressing all blackouts is not a realistic goal. The question is: How should the problem of managing blackout risk be formulated? Several authors define blackout risk as the probability times the consequences, where the consequences can be measured by blackout costs such as technical, business, and social costs [60]. Carreras et al [15], [32] formulate the blackout mitigation problem as jointly mitigating the risk of small, medium, and large blackouts. This allows any tradeoffs between small and large blackouts to be assessed. Mili and Dooley [60] present a partitioned multiobjective risk method aimed at finding tradeoffs between

N-1 security and survivability to catastrophic events, namely between various levels of resiliency ranging from low to high damage severity while minimizing the cost.

Network theory approaches. There is an extensive literature on cascading in abstract networks [68], [11], [81] that is motivated in part by the propagation of failures and congestion in the internet. The dynamics of cascading is related to statistical topological properties of the networks. Although the cascading has similar general features, such as criticality and power laws, the models usually differ from power system models. The models typically consider flows of discrete packets that are injected and removed from all nodes and follow least distance paths. The importance of links or nodes is measured by “betweenness”, which is proportional to the number of least distance paths through the link or node. Some researchers have studied the statistical properties of the power system network as an abstract graph, neglecting power flows. For example, Watts [92] has shown that the topology of a typical electric power network is a small-world network and studied the bimodal size distribution of cascades on this network. Work on cascading phase transitions and network vulnerability that accounts for forms of network loading includes [91], [62], [25]. Moreover, several researchers have made progress in moving the network theory towards the assumptions and models of power systems. Hines and Blumsack [40] account for the electrical distances in the network to suggest that power systems have a scale free structure and generalize the betweenness concept. Lesieutre [50] applies topological graph concepts in a way that is more consistent with power system generation and load patterns. Other interdisciplinary approaches may also be suitable for analyzing cascading failures in electric power systems, such as analyses of cascades of broken fibers in fiber bundle models of material strength [45], [31]. Roy et al. [77] propose the “influence model” that is a tree network that abstractly represent influences between idealized components (this network of influences is different than the power system physical network). Components can be failed or operational according to a Markov model that represents both internal component failure and repair processes and influences between components that cause failure propagation. Pepyne et al. [72] also use a Markov model for nodal components, but propagate failures along the transmission lines of a power systems network with a fixed probability.

High-level probabilistic models. High-level probabilistic models describe the cascading process but do not model any power systems physics. For example, they may neglect the times between failures, the power grid structure, and the diversity of power system components and interactions. They are useful for understanding cascading failure in more detailed models. The CASCADE model [31] has many identical components that fail when their load exceeds a threshold, an initial disturbance loading the system, and the additional loading of components by the failure of other components. The initial overall system stress is represented by upper and lower bounds on a range of random initial component loadings. The model parameters describe the initial disturbance and the amount of additional loading when another component fails. There is an analytic

formula for the probability distribution of the total number of components failed. Branching process models [28], [29], [30], [33] can approximate the CASCADE model and are established models for cascading processes in many other fields [38]. The failures occur randomly in a series of stages. The model parameters are the average number of initial failures and an average tendency for the failures to propagate. There are also elaborations that consider continuously varying quantities such as load shed [95] and the time-evolution of failures [29]. An accelerated propagation failure model for the number of transmission line failures is proposed in [20]. This model has a good fit to historical data for North American line outages [1].

Critical components and high risk multiple contingencies. Practical computation of high-risk N-k contingencies is developed in [20] using dynamic decision trees and fast simulation. Wang and Thorp [89] use fast simulation of hidden failures to identify critical relays that contribute to many possible cascades. Maintaining these relays is a cost-effective mitigation of cascading. Several methods for identification of critical multiple contingencies have been proposed to identify vulnerabilities to deliberate attack or worst case scenarios. Optimization is used to maximize the blackout due to contingencies caused by an attack with limited resources [78], [5], [34]. Simple heuristics for attacking power systems also yield near maximal blackouts [9]. Lesieutre et al. [50] finds critical lines and cutsets by graph theoretic methods and considering load-generation mismatch.

Recognizing patterns. In major blackouts, a line fault can cause other lines to be overloaded due to rerouting of the power flow. The overloaded lines may then be de-energized by impedance relays seeing low voltages and high currents, e.g. zone 3 tripping. The line outage may also cause low voltages and high reactive power demand on close-by generators, leading to generator tripping by the over-excitation protection. Further generators can experience high reactive power output and may also trip. These are examples of typical basic patterns of cascading events. Identifying these basic patterns and then studying how they combine into cascading sequences is a new research direction [51], [52].

Conventional reliability methods. There is an extensive literature and assessment tools on power system reliability [10], including component reliability and maintenance, generation adequacy and assessments of transmission system reliability, the effects of weather, and common cause failure. These methods are very useful, but they are based on underlying assumptions of independent events and do not apply to cascading failure because the successive weakening of the system as the cascade proceeds makes the cascading events dependent. There are some methods in the wider reliability literature for cascading in systems with a limited number of components. [55], [83], [80] represent cascading failure by increasing the failure rate of remaining components when a component fails. [36] addresses cascading in a network.

V. SIMULATION METHODS

Cascading failure simulation methods are evolving and the various simulations have different compromises of cascading

phenomena modeled, modeling detail and approximations, and simulation techniques. Modeling detail must be traded off with simulation time and the availability of data. The best choices for modeling and simulation remain an open question. Most of the simulations concentrate on cascading phenomena that can be captured by successive static models, such as cascading overloads, protection, and voltage collapse. In particular, most simulations represent static line overloads, at least at the level of DC load flow, and a selection of other aspects of cascading.

There are different and sometimes incompatible objectives for different cascading simulations. The objectives include computing likely or high risk cascading failure sequences, computing the overall risk of cascading failure, and computing operator actions to mitigate cascading failure in real time. These different objectives have different requirements for modeling, data, speed, sampling methods, and processing the results to get useful answers. Modeling and simulation issues addressed include:

Protection. Hidden failures are modeled in [85], [6], [19], [89], [61] and protection control groups are modeled in [86], [37], [20]. The availability of protection data to support simulation and the burden of processing it are issues.

Operator actions. Operator actions are modeled in [4], [86], [37], [76].

Random or deterministic. Many simulations use some random modeling, while others use a more deterministic framework. However, it should be noted that when computing the deterministic outcome of a chosen set of initial conditions, the set of initial conditions can also be viewed probabilistically as a sample from all possible initial conditions.

Voltage collapse. Some simulations use an AC load flow and can model voltage collapse. Mili [61] uses a continuation method while others use simpler approximations.

Modeling scope and detail. Simulations vary in scope and modeling detail, but some of the more comprehensive and detailed simulations use an AC load flow and approximately represent protection, operator actions and voltage collapse as in the Manchester model [46], [64] and TRELSS [86], [37].

Real time. One way to reduce the possibilities to be processed simulates the cascade using real-time data and responds while the slower cascade processes evolve. McCalley [58] approaches this with fast simulation and dynamic decision trees.

Simulation methods. Simulation time and effective sampling from a huge number of possibilities are key constraints. There has been progress with importance sampling [6], heuristic search [89], correlated sampling [46], and fast numerical methods for computing N-k contingencies [58].

Application in industry. The cascading mode of TRELSS [86], [37] is used by industry to identify cascading failure problems in large power systems.

Islanding. Islanding is part of many blackouts and is particularly addressed in studies to optimize islanding such as [96]. Many of the cascading failure simulations can accommodate islanding.

Time evolution of events. Anghel et al [4] model time evolution of random disturbances and restoration processes.

Dynamics. Although generator protection and controls and dynamic stability play important roles in blackout evolution, dynamic analysis is seldom applied for reasons of modeling difficulties and complexities. In the advanced stages of a blackout, uncontrollable system separation, angle instability and generation tripping can occur. It is often necessary to study transient scenarios in more detail with adequate representation of synchronous generators and other dynamic elements [87]. Transient stability is often a serious problem because only a few cascading line trips may cause system instability [57]. Some of the challenges of determining cascading failure due to dynamic transients in hybrid nonlinear differential equation power system models are tackled by DeMarco [27] using Lyapunov methods applied to a smoothed model and by Parrilo et al. [71] using model reduction.

High risk cascades. High risk cascades are computed by a variety of approaches in [89], [63], [74], [20], [34], [22].

Agents. Simulations can be structured with agents [39].

Self-organization. Simulations such as OPA consider an evolving grid that is continually upgrading as a complex system to satisfy an increasing load demand and reliability requirements [16], [59], [90], [32].

Comparing the results from cascading failure simulations with real data (particular cascading sequences and/or overall cascading statistics) is needed to show how well the simulations capture reality and to help establish modeling goals.

VI. PROPERTIES OF CASCADING

Power laws in blackout size distribution. How much rarer are large blackouts than small blackouts? One might expect a probability distribution of blackout size¹ to fall off exponentially as the size of the blackout increases. That is, doubling the blackout size squares its probability and so, after many squarings, the largest blackouts have vanishingly small probability. However, analyses of North American blackout statistics [66] show that the probability distribution of blackout size does not decrease exponentially, but rather has an approximate power law region with an exponent between -1 and -2 [13], [18], [2], [17], [94], [79]. The power law implies that blackouts of all sizes can occur. Similar power law dependences of blackout probability with blackout size are observed in Sweden [41], Norway [8], New Zealand [3], and China [93] and these data are compared in [32]. It is striking that such different power systems show roughly similar forms of blackout size distribution. The power law data from these countries suggests that large blackouts are much more likely than might be expected from the common probability distributions that have exponential tails. The power law region is always limited in extent by a finite cut off corresponding to the largest possible blackout. Several researchers have studied the overall statistics of line failures [1], [21], [33] and these statistics also show heavy tails in the distribution of the number of line failures. There is a need to publish and analyze more data so that methods of cascading failure can be developed and tested against real-world experience. The heavy tails in

¹Useful measures of blackout size include power shed, energy unserved, customers disconnected, duration, and number of lines tripped.

distributions of blackout size can be qualitatively attributed to the dependency of events in a cascading blackout. As the blackout progresses, the power system usually becomes more stressed, and it becomes more likely that further events will happen. This weakening of the power system as events occur makes it more likely that a smaller blackout will evolve into a larger blackout.

Criticality. Cascading blackouts become more likely as the power system becomes stressed. Most of the research to date has stressed power system models by increasing the overall loading. As the load increases, the average blackout size increases very slowly, until, at a loading called the critical loading, there is a sharp change and average blackout size starts increasing much more quickly. Moreover, at this critical loading, there is a power law in the probability distribution of blackout size. Evidence for a critical loading is emerging in abstract models of cascading failure [31], [64] as well as in power system models that represent some cascading failure mechanisms [14], [54], [19], [64]. The critical loading defines a reference point for increasing risk of cascading failure. There have been several approaches to assess the probability of cascading blackouts as load increases. Kirschen et al [46] uses correlated sampling and Monte Carlo simulation to develop a calibrated reference scale of system stress that relates system loading to blackout size. Dobson and coworkers [30], [95] suggest estimating the average propagation of failures and the size of the initial disturbance from simulated or real data and then using these estimated parameters in branching process models to predict the distribution of blackout size.

Self-organization. Over time, system stress or loading tends to increase due to load growth and tends to decrease due to the system upgrades and improvements that are the engineering responses to simulated or real blackouts. This is a complex systems view of the evolving power system. It has been suggested [17], [32], inspired by theories of self-organized critical systems in statistical physics [7], [43], that these opposing forces tend to slowly shape the power system towards criticality. This has been demonstrated with a simple model of these opposing forces shaping the evolution of a power system model of cascading line overloads at the level of DC load flow and LP dispatch [16]. Furthermore, based on the NERC data on North American blackouts, Carreras et al [17] concluded that the dynamics of blackouts have some features of self-organized critical systems.

Highly optimized tolerance. Carlson and Doyle [12] have proposed Highly Optimized Tolerance (HOT) as a way of understanding engineered complex systems and applied it to forest fires, internet, and other applications. Because electric power systems are also partially optimized by design, HOT deserves to be investigated. HOT is a constrained optimization problem that minimizes the expected cost of cascading events subject to a bound on the cost of the resources required to limit their propagation. In power systems, events could be the outage size, dollar losses and the number of customers being disconnected. The resources include protection systems and special control schemes. HOT requires an a priori knowledge of (i) the event probabilities, (ii) a functional relationship

between the size of the events and the resources, and (iii) the number of dimensions of the space over which the events propagate. A preliminary application of the HOT methodology to power systems is reported in [82] under the assumptions of independent events, a single resource, and a one dimensional space of propagation. Further research is needed to make HOT a valid method for power system applications.

Probability distribution of the time between blackouts. For the NERC blackout data, [17] and [18] observed that the distribution of times between blackouts has an exponential tail, while [94] observed that this tail is somewhat fatter than exponential. [79] fit the number of blackouts in a given period of time with a negative binomial distribution. The frequency of blackouts is related to the frequency of the events triggering the blackout; some of these propagate to cause a blackout. [41] analyzes Swedish blackout data and fits the blackout times by a Poisson process. Gou et al. [35] model the blackout triggers as occurring independently at constant rates so that the time between triggers has an exponential distribution. The probability of the trigger causing a further cascade can be determined by simulation considering factors such as generation-load imbalance, voltage instability, frequency instability, branch overloads, and hidden failures. It then follows that the time between blackouts is a mixture of gamma distributions.

VII. DISCUSSION AND CONCLUSION

The power industry has always worked hard to avoid cascading blackouts. The main current approaches are applying deterministic criteria such as the N-1 criterion that help to suppress cascades from starting and a range of industry practices devoted to analyzing and mitigating failures caused by a variety of processes, such as overloads and various types of instabilities, as well as efforts to improve the reliability of individual components. Indeed there are analysis and simulation tools that apply separately for each of these processes. After a large blackout occurs, considerable efforts are made to analyze the detail of that particular cascade and improve the power system to minimize the chance of a similar cascade happening. Moreover, many of the various established ways to increase power system reliability tend to also mitigate the risk of cascading failures.

However, large cascading blackouts, although rare due to industry efforts, are a challenge to analyze and simulate in a predictive way due to the huge number of possible rare interactions and the diversity and complexity of these interactions. Analyses of blackout records in a number of countries show that, although large blackouts are rarer than small blackouts, blackouts of all sizes can occur, and there is a substantial risk of large cascading blackouts. Therefore one cannot dismiss large cascading blackouts as so unlikely that they should be neglected. At the same time it should be recognized that the current methods for directly understanding and mitigating cascading failure are not well developed.

Some insights and methods for a statistical analysis of cascading failure are starting to emerge. Large blackouts typically involve many separate processes so that current tools

focussing on a single process do not capture all the interactions. But analyzing all the possible processes and interactions in complete detail is infeasible. (A likely adverse interaction contributing to cascading failure that becomes known can, and probably will be, mitigated; the issue is how to systematically compute the likely interactions and also cope with the huge number of unlikely interactions.) We need to develop and test methods of modeling and analysis, including probabilistic risk-based approaches, that usefully capture cascading failure with the right compromises in modeling detail. Indeed there has been progress in simulations that approximate the cascading processes for a sample of initial failures, with an emphasis on modeling cascading overloads and protection and simple models for a selection of other processes, such as voltage collapse. Methods to incorporate dynamic stability, operator actions, and complex systems effects remain a challenge.

Making suitable forms of detailed blackout data available for research and analysis is a key issue for progress in cascading failure. In particular, the lack of detailed standardized data on faults and failures affecting not only primary components but also secondary protection and control systems is a major hurdle in the development of security assessment methods that account for multiple failures. Key issues for understanding cascading failure are developing and testing high-level statistical models. Goals include estimating the overall power system reliability with respect to cascading failure using simulation results or real measurements without waiting a long time for many blackouts to happen. Key issues for simulating cascading failure are sampling the cases to be simulated, tradeoffs between modeling detail and simulation efficiency, fast simulation methods, availability of data to the industry and research community, which cascading processes need to be modelled and in what detail, and methods to analyze and understand the results.

REFERENCES

- [1] 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.
- [2] M. Amin, North America's electricity infrastructure: are we ready for more perfect storms?, *IEEE Security & Privacy*, pp.19-25, Sept/Oct 2003.
- [3] G. Ancell, C. Edwards, V. Krichtal, Is a large scale blackout of the New Zealand power system inevitable?, *Electricity Engineers Association 2005 Conference "Implementing New Zealand's Energy Options"*, Auckland, New Zealand, June 2005.
- [4] M. Anghel, K.A. Werley, A.E. Motter, Stochastic model for power grid dynamics, *40th Hawaii International Conference System Sciences*, Hawaii, Jan 2007.
- [5] J.M. Arroyo, F.D. Galiana, On the solution of the bilevel programming formulation of the terrorist threat problem, *IEEE Trans. Power Systems*, vol. 20, no. 2, May 2005, pp. 789-797.
- [6] 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.
- [7] P. Bak, *How nature works: the science of self-organized criticality*, Copernicus books, New York NY USA 1996.
- [8] J.Ø.H. Bakke, A. Hansen, and J. Kertész, Failures and avalanches in complex networks, *Europhysics Letters*, vol. 76, no. 4, pp. 717-723, 2006.
- [9] V.M. Bier, E.R. Gratz, N.J. Haphuriwat, W. Magua, K.R. Wierzbicki, Methodology for identifying near-optimal interdiction strategies for a power transmission system, *Reliability Engineering and System Safety*, vol. 92, no. 9, pp. 1155-1161, Sept. 2007.
- [10] R. Billinton, R.N. Allan, *Reliability evaluation of power systems* (2nd ed.), New York: Plenum Press, 1996
- [11] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D-U. Hwang, Complex networks: structure and dynamics, *Physics Reports*, vol.424, pp.175-308, 2006
- [12] J.M. Carlson, J. Doyle, Highly optimized tolerance: a mechanism for power laws in designed systems, *Physical Review E*, vol. 60, 1999, pp. 1412-1427.
- [13] B.A. Carreras, D. E. Newman, I. Dobson, A. B. Poole, Initial evidence for self-organized criticality in electric power blackouts, *33rd Hawaii International Conference on System Sciences*, Maui, Hawaii, Jan. 2000.
- [14] 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.
- [15] B.A. Carreras, V.E. Lynch, D.E. Newman, I. Dobson, Blackout mitigation assessment in power transmission systems, *36th Hawaii International Conference on System Sciences*, Hawaii, 2003.
- [16] B.A. Carreras, V.E. Lynch, I. Dobson, D.E. Newman, Complex dynamics of blackouts in power transmission systems, *Chaos*, vol. 14, no. 3, Sept 2004, pp. 643-652.
- [17] B.A. Carreras, D.E. Newman, I. Dobson, A.B. Poole, Evidence for self organized criticality in a time series of electric power system blackouts, *IEEE Trans. Circuits & Systems I*, vol. 51, no. 9, Sept 2004, pp. 1733-1740.
- [18] J. Chen, J.S. Thorp, M. Parashar, Analysis of electric power system disturbance data, *34th Hawaii International Conference on System Sciences*, Maui, Hawaii, Jan 2001.
- [19] 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.
- [20] Q. Chen, J.D. McCalley, Identifying high risk n-k contingencies for online security assessment, *IEEE Trans. Power Systems*, vol. 20, no. 2, May 2005, pp. 823-834.
- [21] Q. Chen, C. Jiang, W. Qiu, J.D. McCalley, Probability models for estimating the probabilities of cascading outages in high-voltage transmission network, *IEEE Trans. Power Systems*, vol. 21, no. 3, Aug 2006, pp.1423-1431.
- [22] B. H. Chowdhury, S. Baravc, Creating cascading failure scenarios in interconnected power systems, *IEEE Power Engineering Society General Meeting*, Montreal, Canada, June 2006.
- [23] Review of on-line power system security assessment tools and techniques; *CIGRE Working Group C4.6.01*, CIGRE, Paris, 2006-2007.
- [24] L. Wang, K. Morison, Implementation of online security assessment tools for reducing the risk of blackouts, *IEEE Power and Energy Magazine*, vol.4 no.5 Sept/Oct 2006.
- [25] P. Crucitti, V. Latora, M. Marchiori, Model for cascading failures in complex networks, *Physical Review E*, vol. 69, 045104(R), 2004.
- [26] J. De La Ree, Y. Liu, L. Mili, A. G. Phadke, L. Dasilva, Catastrophic failures in power systems: Causes, analyses, and countermeasures, *Proceedings IEEE*, vol. 93, no. 5, May 2005, pp. 956-964.
- [27] C.L. DeMarco, A phase transition model for cascading network failure, *IEEE Control Systems Magazine*, December 2001, pp. 40-51.
- [28] 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.
- [29] 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.
- [30] 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.
- [31] I. Dobson, B.A. Carreras, D.E. Newman, A loading-dependent model of probabilistic cascading failure, *Probability in the Engineering and Information Sciences*, vol. 19, no. 1, January 2005.
- [32] 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 (13 pages).
- [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] V. Donde, V. Lopez, B. Lesieutre, A. Pinar, C. Yang, J. Meza, Identification of severe multiple contingencies in electric power networks, *37th North American Power Symposium*, Ames, Iowa, 2005.
- [35] B. Gou, H. Zheng, W. Wu, X. Yu, Probability distribution of power system blackouts, *IEEE Power Engineering Society General Meeting*, Tampa FL 2007.
- [36] G.L. Greig, Second moment reliability analysis of redundant systems with dependent failures, *Reliability Engineering and System Safety*, vol. 41, 1993, pp. 57-70.
- [37] R.C. Hardiman, M.T. Kumbale, Y.V. Makarov, An advanced tool for analyzing multiple cascading failures, *Eighth International Conference on Probability Methods Applied to Power Systems*, Ames Iowa, September 2004.
- [38] T.E. Harris, *Theory of branching processes*, Dover NY 1989.

- [39] P. Hines, S. Talukdar, Controlling cascading failures with cooperative agents, *International Journal of Critical Infrastructures*, vol. 3, no. 1/2, 2007, pp. 192-220.
- [40] P. Hines, S. Blumsack, A centrality measure for electrical networks, 41st Hawaii International Conference on System Sciences, Hawaii, Jan. 2008.
- [41] Å.J. Holmgren, S. Molin, Using disturbance data to assess vulnerability of electric power delivery systems, *Journal of Infrastructure Systems*, Dec 2006, pp. 243-251.
- [42] IEEE PES PSDP Task Force on Blackout experience, mitigation, and role of new technologies, blackout experiences and lessons, Best practices for system dynamic performance, and the role of new technologies, IEEE Special Publication 07TP190, July 2007.
- [43] H.J. Jensen, *Self-organized criticality*, Cambridge University Press, 1998.
- [44] J. Jung, C. C. Liu, S. Tanimoto, V. Vittal, Adaptation in load shedding under vulnerable operating conditions, *IEEE Trans. Power Systems*, Nov. 2002, pp. 1199-1205.
- [45] D.-H. Kim, B. J. Kim, H. Jeong, Universality class of the fiber bundle model on complex networks, *Physical Review Letters*, vol. 94, 025501, 2005.
- [46] D.S. Kirschen, D. Jayaweera, D.P. Nedic, R.N. Allan, A probabilistic indicator of system stress, *IEEE Trans. Power Systems*, vol. 19, no. 3, 2004, pp. 1650-1657.
- [47] D. Kirschen, G. Strbac, Why investments do not prevent blackouts, *Electricity Journal*, March 2004, pp. 29-34.
- [48] U.G. Knight, *Power systems in emergencies: From contingency planning to crisis management*, New York: Wiley, 2001.
- [49] D.N. Kosterev, C.W. Taylor, W.A. Mittelstadt, Model validation for the August 10, 1996 WSCC system outage, *IEEE Trans. Power Systems*, vol. 13, no. 3, pp. 967-979, 1999.
- [50] B. C. Lesieutre, S. Roy, V. Donde, A. Pinar, Power system extreme event screening using graph partitioning, 38th North American Power Symposium, Southern Illinois University Carbondale IL USA, Sept 2006.
- [51] J. Li, Identification of cascaded generator over-excitation tripping events, M.S. Thesis, Iowa State University, 2007.
- [52] C. C. Liu, et al., Learning to recognize the vulnerable patterns of cascaded events, EPRI Technical Report, 2007.
- [53] H. Li, G. Rosenwald, J. Jung, C. C. Liu, Strategic power infrastructure defense, *Proceedings of the IEEE*, May 2005, pp. 918-933.
- [54] H. Liao, J. Apt, S. Talukdar, Phase transitions in the probability of cascading failures, *Electricity Transmission in Deregulated Markets*, conference at Carnegie Mellon University, Pittsburgh PA USA Dec 2004.
- [55] D.V. Lindley, N.D. Singpurwalla, On exchangeable, causal and cascading failures, *Statistical Science*, vol. 17, no. 2, pp. 209-219, 2002.
- [56] C. C. Liu, J. Jung, G. Heydt, V.Vittal, A. Phadke, The strategic power infrastructure defense (SPID) - A conceptual design, *IEEE Control System Magazine*, Aug. 2000, pp. 40-52.
- [57] H.T. Ma, B. H. Chowdhury, Dynamic simulations of cascading failures, North American Power Symposium, Southern Illinois University, Carbondale, IL, USA, 2006.
- [58] J.D. McCalley, S. Khaitan, Pserc report: Risk of cascading outages, Part A, to appear in 2008.
- [59] S. Mei, Yadana, X. Weng, A. Xue, Blackout model based on OPF and its self-organized criticality, *Proceedings of the 25th Chinese Control Conference*, Harbin, Heilongjiang, China, August 2006.
- [60] L. Mili, K. Dooley, Risk-based power system planning integrating social and economic direct and indirect costs, Chapter 2 in *Electric Power Networks Efficiency and Security (EPNES)-Volume 2: Risk-Based Power System Planning and Control*, Eds. J. Momoh, L. Mili, John Wiley 2008.
- [61] 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.
- [62] A.E. Motter, Y-C. Lai, Cascade-based attacks on complex networks, *Physical Review E*, 66(6): 065102, 2002.
- [63] D.P. Nedic, D.S. Kirschen, Discovering mechanisms of disturbance development, IREP Conference on Bulk Power System Dynamics and Control VI, Cortina D'Ampezzo, Italy, August 2004.
- [64] D.P. Nedic, I. Dobson, D.S. Kirschen, B.A. Carreras, V.E. Lynch, Criticality in a cascading failure blackout model, *International Journal of Electrical Power and Energy Systems*, vol. 28, 2006, pp. 627-633.
- [65] NERC (North American Electric Reliability Council), 1996 system disturbances, NERC, Princeton, New Jersey 08540 USA, 2002.
- [66] NERC (North American Electric Reliability Council) Disturbance Analysis Working Group (DAWG) Database, NERC, Princeton, New Jersey USA 08540. <http://www.nerc.com/~dawg/database.html>
- [67] NERC standards and Table I, Transmission System Standards - Normal and Emergency Conditions are available at www.nerc.com
- [68] M.E.J. Newman, The structure and function of complex networks, *SIAM Review*, vol. 45, no. 2, 2003, pp.167-256.
- [69] M. Ni, J.D. McCalley, V. Vittal, T. Tayyib, Online risk-based security assessment, *IEEE Trans. Power Systems*, vol. 18, no 1, 2003, pp. 258-265.
- [70] T. Nye, C. C. Liu, M. Hofmann, Adaptation of relay operations in real time, *Power System Computation Conference*, Liege, Belgium, Aug 2005.
- [71] P.A. Parrilo, S. Lall, F. Paganini, G.C. Verghese, B.C. Lesieutre, J.E. Marsden, Model reduction for analysis of cascading failures in power systems, *American Control Conference*, vol. 6, 1999, pp. 4208-4212.
- [72] D.L. Pepyne, C.G. Panayiotou, C.G. Cassandras, Y.-C. Ho, Vulnerability assessment and allocation of protection resources in power systems, *Proceedings American Control Conference*, vol. 6, 2001, pp. 4705-4710.
- [73] R. Podmore, Criteria for evaluating open energy management systems, *IEEE Trans. Power Systems*, vol. 8, no. 2, pp. 466-471, May 1993.
- [74] S. J. Ranade, R. Kolluru, J. Mitra, Identification of chains of events leading to catastrophic failures of power systems, *International Symposium on Circuits and Systems*, pp. 4187-4190, 2005.
- [75] S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, *IEEE Control Systems Magazine*, pp. 11-25, December 2001.
- [76] M.A. Rios, D.S. Kirschen, D. Jayaweera, D.P. Nedic, R.N. Allan, Value of security: modeling time-dependent phenomena and weather conditions. *IEEE Trans. Power Systems*, vol. 17, no. 3, pp. 543-8, 2002.
- [77] S. Roy, C. Asavathiratham, B. C. Lesieutre, G. C. Verghese, Network models: growth, dynamics, and failure, 34th Hawaii International Conference on System Sciences, Maui, Hawaii, Jan. 2001.
- [78] J. Salmeron, K. Wood, and R. Baldick, Analysis of electric grid security under terrorist threat, *IEEE Trans. Power Systems*, vol. 19, pp. 905912, 2004.
- [79] J.S. Simonoff, C.E. Restrepo, R. Zimmerman, Risk-management and risk-analysis-based decision tools for attacks on electric power, *Risk Analysis*, vol. 27, no. 3, 2007, pp. 547-570.
- [80] N.D. Singpurwalla, C. Kong, Specifying interdependence in networked systems, *IEEE Trans. Reliability*, 2004, vol. 53, no. 3, pp. 401-405.
- [81] S. H. Strogatz, Exploring complex networks, *Nature*, vol. 410, 8 March 2001, pp 268 - 276.
- [82] M.D. Stubna, J. Fowler, An application of the highly optimized tolerance model to electrical blackouts, *International Journal of Bifurcation and Chaos*, vol. 13, no. 1, 2003, pp. 237-242.
- [83] Y. Sun, L. Ma, J. Matthew, S. Zheng, An analytical model for interactive failures, *Reliability Engineering & System Safety*, vol. 91, 2006, pp. 495-503.
- [84] U.S.-Canada Power System Outage Task Force, Final Report on the August 14th blackout in the United States and Canada. United States Department of Energy and National Resources Canada, April 2004.
- [85] J.S. Thorp, A.G. Phadke, S.H. Horowitz, S. Tamronglak, Anatomy of power system disturbances: importance sampling, *International Journal of Electric Power and Energy Systems*, vol. 20, no 2, pp 147-152, 1998.
- [86] Transmission reliability evaluation for large-scale systems (TRELSS): version 6.0 User's manual, EPRI, Palo Alto, CA: 2000. 1001035
- [87] V. Venkatasubramanian, Y. Li, Analysis of 1996 Western American electric blackouts, *Bulk Power System Dynamics and Control - VI, Cortina d'Ampezzo, Italy*, Aug 2004.
- [88] Union for the Co-ordination of Transmission of Electricity (UCTE), Final report, system disturbance on 4 November 2006. www.ucte.org.
- [89] 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.
- [90] D. Watts, H. Ren, Cascading failures in electricity markets: What about the prices?, *Bulk Power System Dynamics and Control - VII, IREP Symposium, Charleston, SC USA*, August 2007.
- [91] D.J. Watts, A simple model of global cascades on random networks, *Proceedings National Academy Sciences USA*, vol.99, no.9, 2002, pp.5766-5771.
- [92] D. J. Watts, Small worlds: The dynamics of networks between order and randomness, Princeton University Press, Princeton, NJ, USA 2003
- [93] X. Weng, Y. Hong, A. Xue, S. Mei, Failure analysis on China power grid based on power law, *Journal of Control Theory and Applications*, vol. 4, no. 3, August 2006, pp. 235-238.
- [94] R. Weron, I. Simonsen, Blackouts, risk, and fat-tailed distributions, in *Practical Fruits of Econophysics*, ed. H. Takayasu, Springer-Tokyo, 2005.
- [95] K.R. Wierzbicki, I. Dobson, An approach to statistical estimation of cascading failure propagation in blackouts, CRIS, Third International Conference on Critical Infrastructures, Alexandria, Virginia, Sept 2006.
- [96] H. You, V. Vittal, Z. Yang, Self-healing in power systems: an approach using islanding and rate of frequency decline-based load shedding, *IEEE Trans. Power Systems*, vol. 18, no. 1, pp. 174-181, Feb 2003.
- [97] M. Zima, G. Andersson, On security criteria in power systems operation, *Power Engineering Society General Meeting*, vol. 3, San Francisco CA USA 2005, pp. 3089-3093.