Submitted for review,
IEEE Trans. Power
Systems, 28 Sept 2016

Cascading Blackouts: Stress, Vulnerability, and Criticality

Hyde M. Merrill, *Fellow, IEEE* and James W. Feltes, *Senior Member, IEEE*

***Abstract*-- The problem of cascading blackouts is defined in the context of a new perspective of the electric power system. A new failure network is defined, based on well-known line outage distribution factors. Following the practice of network (graph) theory, the structure and properties of this network are analyzed with metrics (statistics) that measure stress (susceptibility to cascading outages). The metrics can be applied in real-time operations or in planning to identify vulnerability to cascading and to take corrective actions. Two studies are presented, one on a very large North American system, the other on the smaller national system of Peru. New insights are presented and a new class of power system options is defined, to reduce susceptibility to cascading rather than to increase transfer capability.**

***Index Terms*-- blackouts, network theory (graphs), power system operation, power system planning, power system security.**

I. Introduction and Conclusions

THIS paper describes a transformative approach to measuring the susceptibility of electric power systems to cascading blackouts.

Since 1965, large interconnected systems have experienced a new class of disruptions – wide-area cascading blackouts. These blackouts can cause billions of dollars in damage. The root causes of cascading blackouts are not well understood, so in spite of great efforts they keep occurring.

We draw on two bodies of knowledge – electric power engineering and network (graph) theory – to develop and apply a new failure network based on line-outage distribution factors, for modelling and analyzing cascading blackouts. We study the properties of this network in a new context of the three elements of the power system and with new metrics (statistics) based on new use of well-known data and tools.

We conclude that our methods measure vulnerability and exposure to cascading and network stress for real time operations and for planning. Our models reveal important contributors to risk, some of them counter-intuitive. For example, large interconnections seem inherently more risky. Reinforcing a system to reduce congestion or facilitate long-range transfers can make it more brittle. Normal growth of demand, generation, and transmission can make a system more vulnerable. Heavy loading can increase susceptibility. Interestingly, these also reflect actual blackout experience.

We recommend developing new planning and operating options, designed to protect against blackouts rather than to increase transfer capability.

Paraphrasing a grander thinker than either of us in another context, "There is grandeur in this view . . . from so simple a beginning endless forms most beautiful and most [useful] have been, and [can be] evolved [1]."

II. Previous Work

Extensive work has been done on analyzing cascading blackouts, seeking ways to eliminate them or at least to reduce their frequency or extent and speed recovery. We will not pretend to be comprehensive, but will mention highlights.

Many blackouts have been subject to post-mortem analyses. The largest blackout as of this writing was described in an illuminating three-volume report [2]. This report also has useful descriptions of a number of earlier events.

The U.S.–Canadian power industry organized the NERC (North American Electric Reliability Corp., previously with other names but always the same acronym) after the 1965 blackout to improve reliability, notably by producing criteria and collecting data. Its transmission planning criteria have evolved, but have been reasonably stable for decades. Major changes in format and nomenclature were made recently. Preventing cascading blackouts always has been central [3].

A useful state model was developed for treating power system security and reliability [4].

State estimation was introduced to provide accurate inputs to real-time procedures for increasing reliability [5]. (Black-outs seem to imply that state estimation contributes more by making data reliably available than by improving accuracy.)

Much labor has been invested in a host of efforts to solve the blackout problem. Recently network theory has been applied to blackouts and other problems in power. We will review these efforts later, after establishing our context. But blackouts continue: the problem has not been solved.

III. Cascading Blackouts

A cascading blackout is an uncontrolled, unexpected chain of cause-and-effect events that interrupts bulk power service over a large area. Cascading blackouts are of concern because

- A blackout can cause billions of dollars of damage,
- It can take hours or days to restore the system, and
- Health, police, defense, etc., functions are degraded.

This work was supported in part by the Committee for the Economic Operation of the National Electrical System, Lima, Peru.

H. M. Merrill is with the Department of Electrical and Computer Engineering, University of Utah, Salt Lake City, UT 84112 USA (e-mail: hyde@merrillenergy.com).

J. W. Feltes is with Siemens - Power Technologies, Schenectady, NY 12301 USA (e-mail: james.feltes@siemens.com).

A. Typical Events

The 9 November 1965 Northeast blackout occurred when there were heavy flows from the Niagara Falls area to Toronto, Canada. A relay was set too low; the system operators didn't know it. As a result, a line opened needlessly. That caused one and then three others to overload and open. The Ontario and New York systems formed islands. Ontario had too little generation, New York too much. They could not absorb the sudden imbalances and blacked out [2, p. 104].

The US-Canada blackout of 14 August 2003 occurred with high flows in Ohio and nearby. Three 345-kV lines failed between 15:05 and 15:46 EDT. Though not overloaded, they sagged into trees that were taller than they should have been. The economic effect in the US was estimated at $4 to $10 billion. Canada's GNP was measurably affected [2].

August 2003 precursor events included serious procedural failures in two control centers and computer failures. Precursor outages weakened the system and increased stress. Notwithstanding these, the very thorough post-mortem concluded that at "15:05 EDT . . . the system was electrically secure . . . Determining that the system was in a reliable operational state at 15:05 . . . is extremely significant for determining the causes of the blackout [2, p. 23]."

But in just 41 minutes, at 15:46, "the blackout might have been averted [but] it may already have been too late . . . to make any difference [2, p. 45]." The final straw, loss of a fourth 345-kV line at 16:06, was a relay misinterpreting high current and low voltage as a short circuit, and tripping its line.

"[D]etermining that the system was in a reliable operational state at 15:05" is extremely significant *for showing that present methods of measuring susceptibility to cascading are inadequate*. The post-mortem seemed to recognize this, saying, "Although FirstEnergy's system was technically [i.e., by present definition] in secure electrical condition before 15:05 EDT, it was still highly vulnerable [2, p. 44]."

Cascading blackouts that might have happened but didn't also are instructive. For instance, on 11 April 1965, 37 "Palm Sunday" tornados in Ohio, Michigan, and Indiana destroyed 27 transmission lines and two substations of a single utility. Customers served from failed radial lines lost power but there was no cascading blackout [6]. It was Sunday of an off-peak month so the system was lightly loaded. (The system was not designed to survive 29 contingencies.)

The authors have studied many cascading blackouts and non-blackouts around the world. All share the characteristics illustrated above and described below.

B. Diagnosis of the Cascading Blackout Problem

The electric power system is a man-machine energy conversion system of three major elements:

- Current-generating and current-carrying hardware,
- Control and protective devices, and
- Practices and procedures.

Cascading blackouts always involve overloads or failures of current-carrying hardware. But these always are triggered by failures of one of the other two elements of the power system. These failures only cause blackouts if the system is stressed, usually by high inter-regional transfers. Cascading blackouts are phenomena of large interconnections.

These four sentences are easily dismissed as old news. But their significance is neither appreciated nor reflected in planning and operations.

For instance, the NERC transmission planning standards generally assume that control and protective devices and policies and procedures will work properly. Exceptions: stuck breaker and relay failures are listed, but as "Multiple Contingency" conditions (formerly Category C) that systems generally were not planned to withstand [3]. Most network upgrades and real-time operator studies have been for n-1 (formerly Category B) conditions.

A study by the NERC found that 73.5% of significant disturbances were aggravated by protection system "hidden failures" [1] [7], [8].

A half century ago a brilliant electrical engineer said, "Power systems have grown enormously and have become interconnected over vast regions. And we have had two severe blackouts and are undoubtedly headed for more." He also observed, "The more complex a society, the more chance there is that it will get fouled up [9]."

Illustrating his point, the large eastern and western North American interconnections have had cascading blackouts but the smaller Texas system has not. The latter is not synchronously connected to the others. A representative of the Texas system told the authors in 2008 that it had never had a cascading blackout. It had had voltage collapse, which can be a precursor to cascading, in the Bryan/College Station area in April 2003 and October 2006 [10]. The system was *in extremis* during the Christmas seasons of 1983 and 1989, and on April 17, 2006, and applied its Emergency Electric Curtailment Program, including controlled rotating load shedding, but again without cascading [11], [12].

Another brilliant power engineer who was usually right wrote an important 1978 paper on the future of the power system. He spent about 1/6th of his paper on blackouts and concluded, "[Cascading] blackouts will not exist in the year 2000. . . . There is a good chance that by the year 2000 the term [cascading blackout] will be considered to be a term out of the Dark Ages (sic) [13]."

The authors were active professionally in 1978. The feeling then seemed to be, "The utilities will figure this out and we

[1] Medicine provides a problem which is not totally unlike ours. A recent paper claims that medical error is the third leading cause of death in the US [27]. It notes that "medical error" is not a choice for "cause of death" on death certificates. One commenter said that the "data shows that the vast majority of errors are caused by failures in the system." Another observed that the death rate declined in California during a two-week stoppage when only emergency medical care was available. Yet another revealed that death is inevitable. (One trusts that cascading blackouts are not.) Medical errors are much more critical when the patient is very sick. One commenter dismissed all this as "junk science"; others also were skeptical. (Is it reasonable to expect the medical system to function perfectly? The power system?)

won't have any more of them." We clearly did not appreciate the complexity and significance of this problem.

IV. Networks

We cannot hope to forestall or even to test for all failures in control and protective devices, and in policies and procedures. The possibilities are astronomical; individual events are improbable; their effects on the system lack models. But we can do something about stress. The authors have developed new tools, including metrics of stress, or susceptibility to cascading. We have built on two very different theoretic bases to develop methods that planners and operators can use to spot stressed operating states and regions, and to plan and operate the system securely. (We do not expect that either the network theorists or the power engineers will be totally happy with what we have done. But we thank them for their tools.)

A. Network (Graph) Theory

Network theory responds to three observations.

- Large networks are pervasive.
- They are too big to view or study element by element.
- "Big is different." Large networks behave differently than small networks. "The problem with systems like the power grid is that they are built of many components whose individual behavior is . . . well understood . . . but whose collective behavior . . . can be sometimes orderly and sometimes chaotic, confusing, and even destructive [14, p. 23]."

Therefore, concludes network theory, we must study structural properties and metrics (statistics) of large networks. (Analogously, Hooke's law says useful things about a volume of gas without focusing on individual molecules.)

References [14] and [15] survey network theory and give many examples. Fig. 1 presents the basic nomenclature.

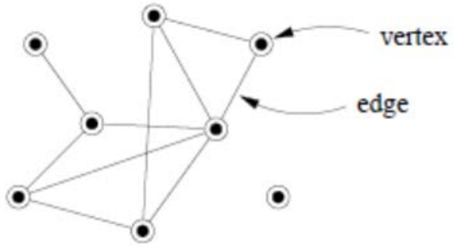


Fig. 1. Network nomenclature [15].

Network theory has been applied to a variety of problems in power, including attempting to determine contributions of each generator to each load [16] and generating random networks for studying widespread failures [17].

Applications to cascading blackouts we have found apparently always use models where buses are vertices and lines are edges [18], [19], [20], [21], [22]. They consider the probability of a random failure at one *bus* propagating to a neighboring *bus*. They are often based on abstract networks rather than real power systems. Some do not appear to use Ohm's and Kirchhoff's laws to model the mechanisms for percolation or propagation of failures.

Two papers present work complementary to ours [7], [8]. They identify and simulate problems which affect cascading: network loading, spinning reserve, controls, and "hidden failures." The latter are not manifested until the system is stressed by a contingency. As do others, they importantly assume that the probability of cascading due to hidden failures increases from Pr = 0 below a threshold loading (for instance, 100% of rating) to Pr = 1 above a second threshold (say, 140% of rating). (Cascading has occurred without overloading.)

A team from many entities analyzed n-k conditions on a 3-area part of the 50,000-bus and 65,000-branch Eastern Interconnection of North America. But analyzing all n-k conditions is impossible. A few (~ 31,000) n-2 outage combinations were tested from a user-supplied list of contingencies. Most n-2 events ended uneventfully after overloaded elements tripped. Some 38 led to voltage collapse or islanding, but none took more than three steps to do so [23].

What is wrong with the efforts described immediately above? Nothing, as far as they go. Importantly, they question the usual assumption that control and protective devices and manual system adjustments will work right, and the loading at which a line trips. The first paper prescribes better relaying, spinning reserve, and control. No surprise here, but perfection isn't possible. The third suggests planning or operating to n-k. But in real blackouts, n-0 or n-1 plus hidden failures is more common than n-k alone. All three use assumed probabilities of failures and cascading. But knowing true probabilities might not change their conclusions.

The leap that they don't quite make is to say: "When the system is stressed, it is more susceptible to cascading due to a variety of failures (most of which we can't model). Therefore, let's focus on modeling and managing stress."

B. Conventional Power Networks Based on Ybus

Traditional engineering studies (short circuit, power flow, stability and their derivatives) are performed frequently for system planning and operation. They model the current-generating and current-carrying hardware well in detail. But they don't seriously consider the second and third elements of the transmission system or its "sometimes chaotic" behavior. And we still have cascading blackouts (though no doubt less than we would have without conventional efforts).

Traditional power system models use a network represented by the n x n bus admittance matrix, Ybus, where n+1 is the number of buses. Each vertex in the network is a bus. The edges include lines and transformers. The Ybus network is good for studying how power flows through a system from bus to bus, and for analyzing weaknesses in a specific element. But for contagion to cascading, the issue is how failures can propagate from line to line through a system, and Ybus is not convenient for this.

C. Cascading Failure Network

We have combined elements of network theory and traditional power system analysis to develop and analyze a network that models how failures propagate through a system. The failure network is based on the matrix of the partial derivatives of flows in vertices (lines and transformers) with respect to outages in other vertices. The elements of this matrix are called line outage distribution factors (LODF or colloquially DFAX). They are calculated using conventional power flow software. Ours may be the first application that uses the DFAX to define a formal failure network.

Vertices in the DFAX network are transmission lines (and transformers), and the edges – the DFAX – represent how the effect of a failure of one vertex propagates to others. A DFAXij of 0.5 means that 50% of the pre-outage flow on vertex j is added to the pre-outage flow in vertex i, should vertex j go out of service. Post-outage flow on vertex i for the outage of vertex j is:

$$f_i \cong f_{i0} + DFAX_{ij} \times f_{j0}. \qquad (1)$$

The relationship is approximate because the power system is only approximately linear. Power system planners and operators use DFAX extensively in contingency analysis. In our experience, for real power analysis, which we believe to be the key issue, the nonlinearity is rarely troublesome. The failure network reflects Kirchhoff's laws and Ohm's law.

(It can be argued that nonlinear and dynamic issues, and voltage problems, which are not reflected in the linearized DFAX, are part of cascading. We of course agree that such effects occur, for example in the two famous blackouts we described above. But cascading begins with the linearizable real-power stresses that our network captures.)

The DFAX matrix is larger than Ybus, in concept m x m, with m the number of vertices, but it needs not be square, as discussed below. The failure network is bigger (more vertices and edges) than the power flow network.

The DFAX matrix is not symmetrical. It is a full matrix, whereas Ybus is symmetrical and for large systems extremely sparse. Nonetheless, for large systems most of the DFAX are very small. In a passive linear network, the value of each DFAX is between -1.0 and + 1.0.

The state of the power flow network is the voltage at each bus. The state of the failure network is described by metrics.

Network theory inspired using a failure network distinct from a power flow network. Network theory also supports analyzing a network with statistics. The metrics we describe below are variants of statistics used commonly in network analysis. Classic power engineering contributed the DFAX, the concepts of non-probabilistic contingency analysis, and the ability to compute pre- and post-contingency loading.

V. Exposure to Cascading

Large positive or negative values of DFAX make cascading more likely. Tighter coupling is more likely to make vertex i overload and go out of service if vertex j has an outage, all else being equal. With a DFAX of zero, the outage of vertex j by itself will not cause an overload or outage of vertex i.

Fig. 1 contrasts the distribution functions of the absolute values of DFAX for two very different systems. The first is a 1,706 vertex portion of the Eastern Interconnection of the US and Canada. Although only this subsystem of the Eastern Interconnection is outaged and monitored, the DFAX matrix reflects the changes in flows throughout the interconnection.

The second system, of 169 non-radial vertices, is one of several possible plans for the future national interconnected system of Peru, based on a 2012 planning study [24].

Each symbol in Fig. 2 represents the number of DFAX with values equal to or greater than the value shown on the x-axis.

The two systems could hardly be more different, yet the shapes of the distributions are similar. For each system, the density function (not shown) looks like a "power law" with "fat tails", where the probability of DFAX with large values is greater than for a normal distribution. Power law distributions are often found in networks [14].

There is much more exposure to cascading in the larger system, all else being equal. This is because the statistics differ in an important way. The modeled portion of the Eastern Interconnection, with ten times the vertices, has twenty times the number of DFAX with large values.

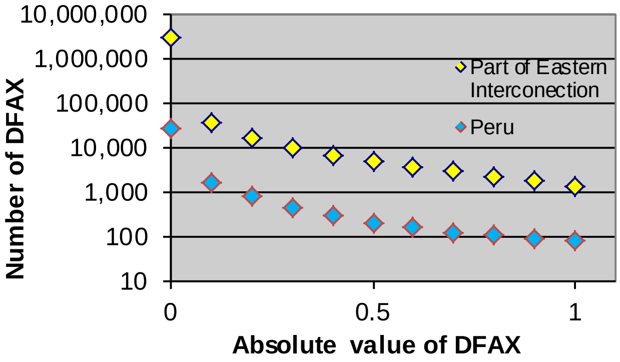


Fig. 2. DFAX distribution function for very large and small systems.

VI. Measures of Stress

History shows that cascading depends critically on how the system is loaded. Neither the DFAX matrix nor Ybus is a matrix of power flows. The stress metrics described next reflect the pre-contingency and post-contingency flows.

A. Vulnerability and Criticality

Vulnerability metrics show how the loading of a monitored vertex changes with contingencies elsewhere, given the pre-contingency loading on the vertices. This pre-contingency loading is determined by the demand and the dispatch of generation. For planning, these are hypothetical. For operations, the pre-contingency loading is from real-time metering, processed by the state estimator.

Criticality metrics show the effects of the outage of a particular vertex on the rest of the system, given the pre-contingency loading on the vertices[2].

Most vertices are power lines and transformers. But interfaces (paths) also are vertices, subject to overloading but

[2] Mnemonic: a vulnerable vertex is a victim; a critical vertex is a culprit.

usually not considered as contingencies. The rating of an interface is its transfer capability[3], which usually is less than the sum of the ratings of its constituent lines. The interface is made up of other vertices, as the constituent lines are also vertices and can be represented individually. Vertex ratings, especially for interfaces, may be different for flows in positive and negative directions.

Both vulnerability and criticality are expressed with two metrics, rank and degree.

B. Rank

For vulnerability, rank measures how severely the flow on a monitored vertex is affected by the worst outage of any other vertex. It is the highest absolute value (supremum) of the post-contingency flows on vertex i, for the outage of any other vertex j. It is expressed in per unit of the rating of vertex i:

$$Vrank_i = \sup\left(\frac{|flow_{i,j}|}{rating_i}\right). \qquad (2)$$

In this equation and in the ones that follow, *flow*$_{i,j}$ is the flow on vertex i after the outage of vertex j, calculated using (1).

For criticality, rank measures how severely the outage of a particular vertex j affects all of the other (unoutaged) vertices i. It is the supremum of the flows on any of the vertices i, following the outage of vertex j. It is expressed in per unit of the rating of each vertex i:

$$Crank_j = \sup\left(\frac{|flow_{i,j}|}{rating_i}\right). \qquad (3)$$

The difference between the two equations is whether the supremum is over all contingencies (2) or all observed vertices (3). This also applies to calculation of degree using (4) and (5). See Table I.

C. Degree

For vulnerability, the degree of vertex i is the number of single (n-1) outages of other vertices j that will cause the absolute value of the flow on vertex i to exceed an arbitrary threshold, expressed in per unit of the rating of vertex i:

$$Vdegree_i = count\_if\left(\frac{|flow_{i,j}|}{rating_i} > threshold_i\right). \quad (4)$$

For criticality, the degree of vertex j is the number of other vertices i whose flows will exceed their thresholds, expressed in per unit of the ratings of the vertices i, for an outage of vertex j:

$$Cdegree_j = count\_if\left(\frac{|flow_{i,j}|}{rating_i} > threshold_i\right). \quad (5)$$

The degree thresholds are chosen to make visible (by "zooming") the changes in degree when loading changes or when the network is upgraded. For instance, one might use 125% to focus on heavy overloads, or 75% to consider loading which is not technically a violation, but which may trigger hidden failures (see the Eastern Interconnection example below). The thresholds are not the familiar "bright line" of system planning, where a loading of 101% of rating requires a fix, whereas a loading of 99% does not. Threshold values used to study one system will not necessarily be appropriate for another system.

TABLE I
ILLUSTRATION OF VULNERABILITY AND CRITICALITY METRICS

		Criticality (outaged vertices "j")			
		Crank	2.43	0.87	0.87
		Cdegree*	2	1	1
Vrank	Vdegree*	vertex	1	2	3
0.49	0	1		0.49	0.49
2.43	2	2	-2.43		0.87
2.43	2	3	-2.43	0.87	
Vulnerability (monitored vertices "i")			Post-outage flows (per unit of monitored vertex ratings)		

* Threshold = 75% of monitored vertex ratings for this example.

D. Why these Metrics are Reasonable

A necessary condition for cascading to propagate from n-1 to n-3 and beyond is that cascading occurs from n-1 to n-2.

A sufficient condition for cascading to occur from n-1 to n-2 is that Vrank be high enough. Higher Vdegree and Cdegree mean greater exposure – more states with Vrank high enough.

A sufficient condition for failure of a particular element to cascade from n-1 to n-2 is that Crank be high enough.

What constitutes "high enough" is unknown (but see the Peru study below). Built-in conservativism should allow minor overloads. But hidden failures in control and protection systems (e.g., relaying) and practices and procedures (e.g. tree trimming, situation awareness) have caused cascading with Vrank less than 1. Hidden failures are more likely to be manifested as rank and degree increase, all else being equal.

With computation of rank suitably modified, these statements remain true for non-linear failure networks (e.g., due to remedial action schemes or active compensation).

VII. TWO STUDIES

A. Eastern Interconnection of the US and Canada

For a portion of the Eastern Interconnection, Fig. 3 is the distribution function of degree of vulnerability as power transferred from one sub-region to another changes, using a threshold of 75% of each observed vertex's rating.

When transfers increase from zero to 2000 MW, there is no change in the vulnerability degree. Between 2000 MW and 4000 MW the degree of vulnerability increases. Not just one vertex, but many become more vulnerable. Beyond 4000 MW, this metric does not change. When transfers reach 4000 MW, every vertex affected by transfers is highly loaded, n-1.

It is interesting but not surprising that many vertices became vulnerable at about the same level of transfers. In a well-

[3] Transfer capability is a complex concept. Loosely, it is the maximum power that can be transferred reliably from area A to area B, under defined conditions. An interface is all or part of the network connecting A and B.

designed system, one would expect vertices to reach their limits at about the same time. A vertex that reached its limit much sooner than others would have been adjusted over the years, so that it alone would not unduly limit the transfers.

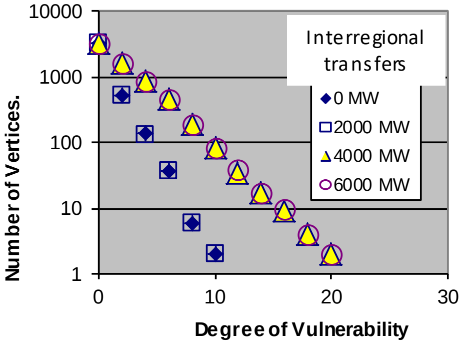


Fig. 3. Degree of vulnerability is affected by interregional transfers.

The tipping point at around 3,000 MW is consistent with the known transfer capability of that part of the system, based on conventional studies.

B. National System of Peru

An extensive study of the grid of Peru used twelve monthly pre-contingency dispatches, for peak, minimum, and shoulder loads. Three system expansion plans were evaluated for a 10-year horizon: light, medium, and heavy expansions.

Fig. 4 is the distribution function of rank of vulnerability for one month for a future with high load growth and a light transmission expansion plan – a highly stressed extreme case. As one might expect, the vulnerability is high, but substantially less during minimum load hours on weekends and in the middle of the night.

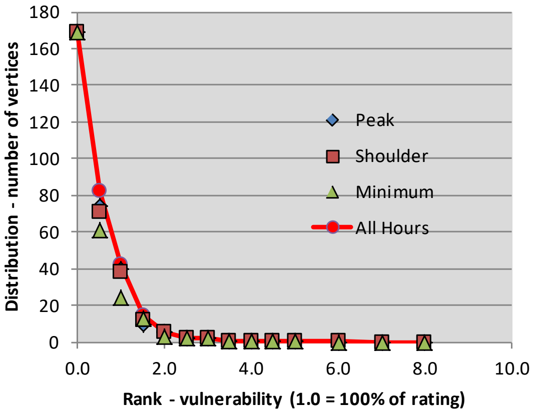


Fig. 4. Rank of vulnerability for peak, shoulder, and minimum loads.

It is interesting that the vulnerability is about the same during shoulder and peak load hours. As has been observed for US systems, the economic dispatch often loads the system with economy flows during shoulder (non-peak) hours.

Fig. 5 shows the criticality degree metrics for the same case. Again, criticality is generally high, but much lower during minimum load hours. There are about ten vertices whose outages would cause four or more other vertices to overload – but not necessarily the same ten for each load level.

The figure shows that three vertices, if outaged at peak load, would cause six other vertices to overload. Four would do so at shoulder load, and one at minimum load. No vertex has criticality degree greater than or equal to eight.

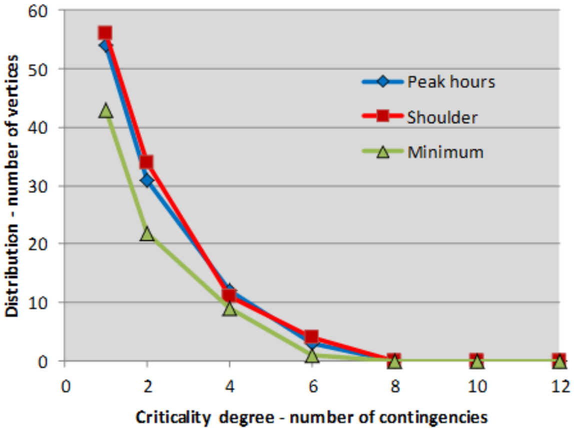


Fig. 5. Degree of criticality for peak, shoulder, and minimum loads.

It is interesting that though the degree of criticality is about the same for peak and shoulder hours, the vertices involved are not the same. The patterns of flows are different. Clearly one cannot study peak conditions alone.

Correlation analyses were performed. They showed that criticality and vulnerability, and rank and degree, are statistically relatively independent of each other. This means we cannot ignore any one of the four metrics – they each provide useful independent information.

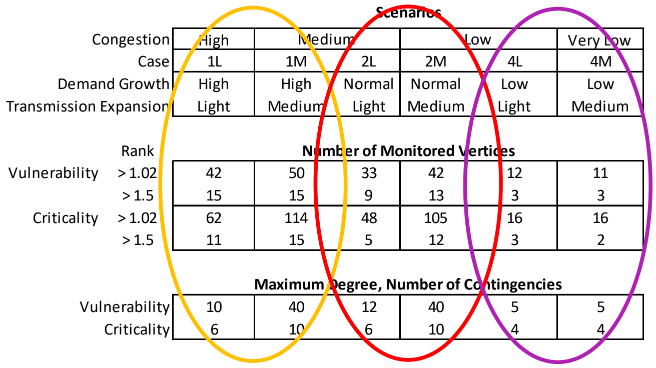
Before discussing Table I, we must digress briefly. Electric generators are dispatched or operated in real time so as to minimize the system-wide fuel cost. This is called “economic dispatch”. If the economic dispatch would cause one or more vertices to overload, the system is said to be “congested”. (Most power systems experience some level of congestion.) A constraint is applied and the generation is re-dispatched (at a higher fuel cost) to avoid overloading the vertices. System planners reinforce the network so as to keep congestion and re-dispatch at reasonably low levels in the future.

Table I compares several cases. Each of the three ovals in Table I covers a different load growth. Each oval covers two alternative expansion plans (“light” compared to “medium” expansions). Therefore each oval covers two different levels of congestion and stress. Six stress metrics are shown.

For the high and normal (expected) load growth futures (the first two ovals), the stronger network had less congestion but greater stress. Reinforcing the network, to reduce congestion, makes it more vulnerable to cascading.

Why is this so? We offer two explanations. First, after the system was reinforced to reduce congestion, the generation was re-dispatched. More power flowed across the system; n-1 loading was higher, and its stress increased. Second, reinforcements that allow more power to flow also make it easier for failures to cascade through the system.

TABLE I
LOAD GROWTH AND SYSTEM EXPANSION; CONGESTION AND STRESS



		Scenarios					
Congestion		High	Medium		Low		Very Low
Case		1L	1M	2L	2M	4L	4M
Demand Growth		High	High	Normal	Normal	Low	Low
Transmission Expansion		Light	Medium	Light	Medium	Light	Medium
	Rank	Number of Monitored Vertices					
Vulnerability	> 1.02	42	50	33	42	12	11
	> 1.5	15	15	9	13	3	3
Criticality	> 1.02	62	114	48	105	16	16
	> 1.5	11	15	5	12	3	2
		Maximum Degree, Number of Contingencies					
Vulnerability		10	40	12	40	5	5
Criticality		6	10	6	10	4	4

This did not occur for the third oval. The dispatches were about the same for the "light" and "medium" systems. There was little congestion for the former and little re-dispatch for the latter. The "medium" system may be over-designed for low load growth.

Another observation: the table shows that the vulnerability and criticality metrics increased as load, generation, and transmission increased, e.g. 2L versus 1M, and 4L versus 2M. Mere growth seems to make the system less robust, even when the transmission system is reinforced to keep up.

How should we define vulnerability and criticality – for n-1 flows greater than 75% of rating, or 100%, or 150%? Obviously, the higher the threshold is, the more likely cascading is to occur. But cascading can occur with n-1 flows considerably below ratings. And Table I shows that for understanding the cascading failures network, it doesn't matter which threshold we choose. The numbers are different but the conclusions are the same for 102% and 150% thresholds. (The results are blurred for thresholds below 102%, because a security constrained dispatch is not used, so that many lines are loaded to about their limits at n-0.)

VIII. ON-GOING AND FUTURE WORK

The methods described in this paper are in their infancy. We expect to grow this work further – it is worth doing.

A. WECC – University of Utah Study

A Western Electric Coordinating Council (WECC) – University of Utah research team is working on the theory and its application to a very large system. Issues being studied include:

- Comparison of metrics for WECC to those of other systems,
- Investigation of possible correlation among metrics for WECC,
- Variation of metrics seasonally and as demand changes, and
- Pre-blackout values of metrics.

B. Chains of Vulnerable and Critical Vertices

We will consider what can be learned by studying chains of critical and vulnerable vertices and computing metrics akin to the diameter of the network. Why, and how much, are large systems more vulnerable?

We have no reason to assume that measuring stress requires or will be improved by going beyond the n-1 effects modeled using the DFAX. But we plan to examine the need for re-computing the DFAX and metrics when real-time system configuration changes [25].

C. Design: Options for Decreasing Stress

We also will seek planning and operations options for increasing a system's resistance to cascading, especially when increasing transfer capability. We recall a 1973 paper which laid out the need and functional specifications for a then-nonexistent current-limiting device [26]. We seek cascade-limiting devices or techniques with the following properties.

- They should not reduce transfer capability in normal conditions.
- They should be inexpensive to acquire and use.
- They should reduce or at least not increase dependence on practices and procedures, or control and protection equipment, our Achilles heel.
- Therefore they likely should be in continuous operation so that any failures are not "hidden".

"Big is different" and hidden failures make this challenge daunting. For example, "Perhaps the most perturbing aspect of cascading failures . . . is that by installing protective relays . . . reducing, in effect, the possibility that individual elements of the system would suffer serious damage – the designers had inadvertently made the system as a whole more likely to suffer . . . global meltdown [14, pp. 23-24]."

IX. ACKNOWLEDGMENT

We acknowledge with gratitude the contributions to the work described in this paper of our distinguished colleagues Jefferson Chávez, Freddy Portal, Edward Angelino and Eduardo Antúnez de Mayolo, of the Committee for the Economic Operation of the National Interconnected Electrical System, (Comité de Operación Económica del Sistema Interconectado Nacional, or COES-SINAC), Lima, Peru. Their vision, ideas and hard work in the research described, and the far-thinking funding that was provided by COES-SINAC, quite literally made this paper possible. They and COES-SINAC may not necessarily agree with all of our conclusions, but this work could not have been done without them.

X. WORKS CITED

[1] C. Darwin, On the Origin of Species, 1872, p. 554.

[2] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada," April 2004.

[3] "Standard TPL-001-4 - Transmission system planning performance requirements", in "Reliability standards for the bulk electric systems of North America"," NERC, Atlanta, 17 August 2016.

[4] T. R. DyLiacco, "The adaptive reliability control system," *IEEE Trans. on Power Apparatus and Systems,* Vols. PAS-86, no. May 1967, pp. 517-531, 1967.

[5] F. C. Schweppe and E. Handschin, "Static state estimation in electric power systems," *IEEE Proceedings,* vol. 62, no. 7, pp. 972-982, 1974.

[6] "American Electric Power Company Annual Report," 1965.

[7] L. Mili, Q. Qiu and A. G. Phadke, "Risk assessment of catastrophic failures in electric power systems," *Int. J. Critical Infrastructures,* vol. 1, no. 1, pp. 38-63, 2004.

[8] J. Chen, J. D. Thorp and I. Dobson, "Cascadig dynamics and mitigation assessment in power system disturbances via a hidden failure model," *Int. J. of Electrical Power and Energy Syst.,* vol. 27, no. 4, pp. 318-326, 2005.

[9] V. Bush, Pieces of the Action, New York: Morrow, 1970.

[10] R. H. Drew, *personal communication,* Electric Reliability Council of Texas, Inc., Electric Reliability Council of Texas, Inc., 25 January 2008.

[11] ERCOT (Electric Reliability Council of Texas), "ERCOT Emergency Operation, December 21 - 23, 1989," ERCOT.

[12] ERCOT.com web site, "Event Summary -- Emergency Electric Curtailment Program - April 17, 2006," [Online]. Available: /ERCOT%20April%202006%20LoadShedReport--April%252017%25202006.pdf.

[13] F. C. Schweppe, "Power systems '2000': hierarchical control strategies," *IEEE Spectrum,* no. July, pp. 42-47, 1978.

[14] D. J. Watts, Six degrees: the science of a connected age, New York: W. W. Norton, 2003, pp. 104-107.

[15] M. E. J. Newman, "The structure and function of complex networks," *SIAM Rev.,* vol. 45, no. 2, pp. 167-256, 2003.

[16] S.-K. Chai and A. Sekar, "Graph theory application to deregulated power system," IEEE, 0-7803-6661 2001.

[17] Z. Wang, R. J. Thomas and A. Scaglione, "Generating random topology power grids," ECE Cornell University, Ithaca, NY.

[18] J.-C. Laprie, K. Kanoun and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *SAFECOMP 2007,* 2007.

[19] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature,* vol. 464, pp. 1025-1028, 2010.

[20] K. Sun, "Complex networks theory: a new method of research in power grid," in *IEEE/PES Trans. & Dist. Conf. & Exh.,* Dalian, China, 2005.

[21] I. Dobson, K. R. Wierzbicki, J. Kim and H. Ren, "Towards quantifying cascading blackout risk," in *iREP Symposium - Bulk Power System Dynamics and Control,* Charleston SC, USA, 2007.

[22] I. Dobson, "Where is the edge for cascading failure?: challenges and opportunities for quantifying blackout risk," in *IEEE PES Gen Mtg,* Tampa FL USA, 2007.

[23] N. Bhatt and 2. coauthors, "Assessing vulnerability to cascading outages," in *Proc. IEEE/PES Power Systems Conference and Exposition,* March 2009.

[24] COES SINAC, "Draft update of the 2013-2022 transmission plan (in Spanish)," Committee for the Economic Operation of the National Electric System, Lima Peru, 31 May 2012.

[25] T. Güler, G. Gross and M. Liu, "Generalized line outage distribution factors," *IEEE Trans. Power Syst,* vol. 22, no. 2, pp. 879-881, May 2007.

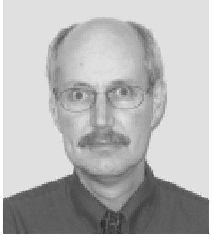
[26] C. A. Falcone, J. E. Beehler, W. E. Mekolites and J. Grzan, "Current limiting device - a utility's need," in *Paper C 73 470-2, IEEE PES Summer Mtg & EHV/UHV Conf,* Vancouver, G.C. Canada, 1973.

[27] M. A. Makary and M. Daniel, "Medical error - the third leading cause of death in the US," *BMJ 2016;353:i2139* , 3 May 2016.

XI. BIOGRAPHIES

Hyde M. Merrill (S'65, M'67, SM'81, F'93) received the BA degree in mathematics and MS degree in electrical engineering from the University of Utah and the PhD degree in electrical engineering from the Massachusetts Institute of Technology. He is a registered professional engineer in New York.

He has worked for the American Electric Power Service Corp, the MIT Energy Lab, Power Technologies, Inc., the Rensselaer Polytechnic Institute and Merrill Energy LLC. In 2015 he joined the University of Utah as adjunct professor. He teaches power systems and leads research on blackouts.



James W. Feltes (M'78, SM'94) received his BS degree with honors in electrical engineering from Iowa State University and his MS degree in electrical engineering from Union College.

He joined Power Technologies, Inc. (PTI), now part of Siemens Power Transmission and Distribution Inc., in 1979 and is currently a senior manager. At PTI, he has participated in many studies involving planning, analysis and design of transmission and distribution systems. He has also been involved in many projects involving development of models for studies of power system dynamics, testing to record equipment response, and model parameter derivation.

He is a registered professional engineer in the state of New York. He is a member of the IEEE Power Engineering Society and Industry Applications Society, and is active on several IEEE committees and task forces.