Smart Grid as a Dynamical System of Complex Networks: A Framework for Enhanced Security

S. Massoud Amin* and Anthony M. Giacomoni*

*Department of Electrical and Computer Engineering,
University of Minnesota, Minneapolis, MN 55455 USA
(e-mail: {amin, giaco013}@umn.edu)

Abstract: From a strategic R&D viewpoint, a major challenge is posed by the lack of a unified mathematical framework with robust tools for modeling, simulation, control, and optimization of time-critical operations in smart electric power grids (spanning from fuel sources to end-use) as complex multi-component and multi-scaled networks. During the past four decades, much effort has been committed to better understanding the dynamics of large-scale power systems in order to enhance security, quality, reliability, and availability (SQRA) of the overall system. Specific attributes of SQRA are needed for electricity to meet the needs of the evolving digital society. This paper aims directly at the issue of metrics to determine security performance. It defines a framework for developing needed indices and standards for benchmarking security, quality, reliability, and availability in the future.

Keywords: Complex Systems, Power Systems Control, Smart Power Applications, Smart Grid, Uncertain Dynamic Systems

1. INTRODUCTION

As the world grows more interconnected, we are becoming surrounded by complex networked systems. These systems consist of numerous components interlinked in complicated webs. Because of the number of components and their intricate interconnections, they are extremely difficult to design, analyze, control, and protect. Despite these challenges, understanding such systems is becoming critical. Many of our nation's critical infrastructures are complex networked systems, including:

- Electric power grids with overlays of sensor/ communications/control systems, and markets
- Oil and gas pipelines
- Telecommunications and satellite systems
- The Internet, computer networks, and the "cyber infrastructure"
- Transportation systems
- Banking and finance systems
- State and local water supply, emergency response, and other services.

Secure and reliable operation of complex infrastructure systems such as these is fundamental to our economy, security, and quality of life. Of particular importance is the uninterrupted availability of inexpensive, high-quality electrical power and reliable, high-performance communication networks.

As the power grids become heavily loaded with long distance transfers, the already complex system dynamics become even more important. Analysis and modeling of interdependent infrastructures (e.g. the electric power grid, together with protection systems, telecommunications, oil/gas pipelines, and energy markets) is especially pertinent. Regarding the latter, during the past four decades, much effort has been committed to better understanding the dynamics of large-scale power systems in order to enhance security, quality, reliability, and availability (SQRA) of the overall system.

Specific attributes of SQRA are needed for electricity to meet the needs of the evolving digital society. Reliability and uninterruptability are practical necessities in digital enterprises. The digital society is expected (and designed) to be continuously operational, without interruption or denial of service. The interface between digital systems, processes, and enterprises and electric power delivery must support this reliability, with innovations spanning from the generation sources to the microchip. Similarly, availability of power is also a necessity. While higher reliability is nearly always a key objective for electric power suppliers, availability is the parameter with which users of sensitive digital equipment and processes are most concerned.

Today's accepted industry practice for power system performance measurements is the starting point for introducing new and more integrated performance metrics. The challenge is to bridge between independent mathematical models and performance metrics that are used at different levels of the power system. In some cases, the models and these independent metrics may conflict with each other to the extent that improving performance in one area may detract from others. This independence stems from several distinct performance areas such as distribution customer availability or outage reporting, grid operating contingencies, monitoring of power quality variations, and measurements of transmission reliability. The way that each of these

This work was supported by the National Science Foundation under grant number 0831059.

performance elements had been applied in the past depended on its area of use in the power system. In addition, industry performance measurement practices and standards evolved via groups that represented their own interests in the areas of end use, distribution, transmission, and generation.

This paper aims directly at the issue of measures to determine security performance. It defines a framework for developing needed indices and standards for benchmarking SQRA in the future. Section 2 describes the development of metrics used to measure the performance of a power system, and Section 3 discusses issues related to interdependent sensing, communications, cyber, and digital infrastructures. Section 4 provides a description of considerations for modeling and designing metrics for complex interconnected systems, and Section 5 presents technologies and initiatives currently underway to develop measurements and metrics to further enhance the security of power systems. Finally, Section 6 states some conclusions.

2. SECURITY, QUALITY, RELIABILITY, AND AVAILABILITY

2.1 Development of Current Standards

Data on outage occurrences of transmission facilities has been collected for many years, beginning in the 1940s and 1950s. Initially, reporting was limited to the frequency of outage occurrences on transmission lines. In the 1960s, methods were first proposed for calculating the reliability of transmission and distribution "systems" (networks) in terms of the reliability of their individual "components." Reliability calculation methods were developed, which led to the need for more formal definitions of terms to foster uniformity and standardization of language among engineers engaged in such practices. The first power industry reliability standard was IEEE Std 346-1973.

In the 1980s, with the advent of more digital processes and systems, more emphasis was placed on reliability measures and reporting. There was a need to include definitions for a broader scope of outage events. One development during this period was the creation of "related outage occurrences" and the need for redundancy. Such developments lead to the creation of IEEE Std 859, which provided standard terms for reporting and analyzing outage occurrences and outage states of electrical transmission facilities. When completed in 1987, IEEE Std 859 replaced Std 346-1973. However, terms related to distribution system facilities and interruptions were eliminated from the scope of the new document. This opened the way for a separate effort to define reliability more in terms of the affect on distribution-connected end users rather than measures of component and unit reliability in the transmission system.

Work continued through the 1990s on a new industry standard for measuring the performance of the power system at the distribution level. It was introduced in 1998 as IEEE Std 1366, Trial Use Guide for Electric Power Reliability Indices. This guide references both the IEEE Std 859 terms for reporting transmission outages and IEEE Std 493, the Gold Book, a recommended practice for reliability in industrial and commercial facilities.

Thus, the practice of reporting reliability in the power industry today is to have different standards for different parts of the power system. IEEE 859-1987 (reaffirmed as a standard in 2002) is for transmission, IEEE 1366-2001 (approved as a guide in 2001) is for distribution, and IEEE 762-1987 (reaffirmed as a standard in 2002) is for generation units. In addition, IEEE 493-1997 is a recommended practice for industrial and commercial power systems.

2.2 SQRA as One Measure of System Performance

Despite these disparate standards, once all the switches are closed, it is one system, and many of its component parts interact and combine in determining overall reliability of power delivery. Understanding the key performance parameters for SQRA will help in the development of new metrics that better integrate all the related parts and add up to improved performance at the point of end use. This defines the challenge of SQRA – to unify these various measures and indices.

As a first response to recognize and understand current practices, a recommendation came out of an industry-wide strategic roundtable to document existing standards, attributes, and metrics of SQRA. A comprehensive Electric Power Research Institute (2005) report summarized advances and showed that significant progress has been made in defining the attributes, terminologies, and indices for quality, reliability, and availability. The main issue for these three elements in describing performance of the power system is inconsistencies among utilities, system operators, and various federal and international standards-making and -approving bodies.

Furthermore, the report showed that several metrics have already been developed for QRA. In contrast, for the area of security, very little has been standardized. Many general studies and reports have focused on cyber, information, and IT security, and these are beginning to specifically address power system controls such as supervisory control and data acquisition (SCADA) systems, energy-management systems (EMSs), and distributed control systems (DCSs). From these security issues, recommended practices are emerging. However, specific standards and indices for measuring security performance do not yet exist.

3. INTERDEPENDENT SENSING, COMMUNICATIONS, CYBER, AND DIGITAL INFRASTRUCTURES

From an infrastructure-interdependency perspective, power, telecommunications, banking and finance, transportation, and other infrastructures are becoming more and more congested and are increasingly vulnerable to failures cascading through and between them. A key concern is the avoidance of widespread network failure due to cascading and interactive effects. Nevertheless, interdependence is only one of several characteristics that challenge the control and reliable operation of these networks. Other factors that place increased stress on the power grid include dependencies on

adjacent power grids (increasing because of deregulation), telecommunications, markets, and computer networks.

In regards to telecommunications, electric power utilities typically own and operate at least parts of their own systems, which often consist of backbone fiber optic or microwave systems connecting major substations, with spurs to smaller sites. The energy industry has historically operated closed, tightly controlled networks. Deregulation and the resulting commercial influences have placed new information-sharing demands on the energy industry. Traditional external entities like suppliers, consumers, regulators, and even competitors now must have access to segments of the network. Therefore, the definition of the network must be expanded to include the external wide-area network connections for these external entities. This greatly increases the security risk to other functional segments of the internal network that must be protected from external connections. This is true whether a private network or the Internet is used to support the external wide-area network.

The security of cyber and communication networks is fundamental to the reliable operation of the grid. While deregulation of the energy industry continues to unfold, information security will become even more important. For energy-related industries, the need to balance the apparently mutually exclusive goals of operating system flexibility with the need for security will need to be addressed from a business perspective.

For example, key electric energy operational systems depend on real-time communication links (both internal and external to the enterprise). The functional diversity of the organizations that control them has resulted in a need for such systems to be designed with a focus on open systems that are user configurable to enable integration with other systems (both internal and external to the enterprise). In many cases, these systems can be reconfigured using telecommunication technologies. However, any telecommunication link that is even partially outside the control of the organization that owns and operates power plants, SCADA systems, or EMSs represents a potentially insecure pathway into the business operations of the company as well as a threat to the grid itself. The interdependency analyses done by most companies during Y2K preparations have identified these links and the system's vulnerability to their failures. Thus, they provide an excellent reference point for a cyber-vulnerability analysis.

A survey of electric utilities revealed real concerns about grid and communication security. Fig. 1 shows a ranking of perceived threats to utility control centers. The most likely threats reported were bypassing controls, integrity violations, and authorization violations, with four-in-ten rating each as either a 4 or 5 out of 5. The rankings were consistent for utilities of all sizes, while the level of concern about potential threats generally increased as the size of the utility (peak load) increased.

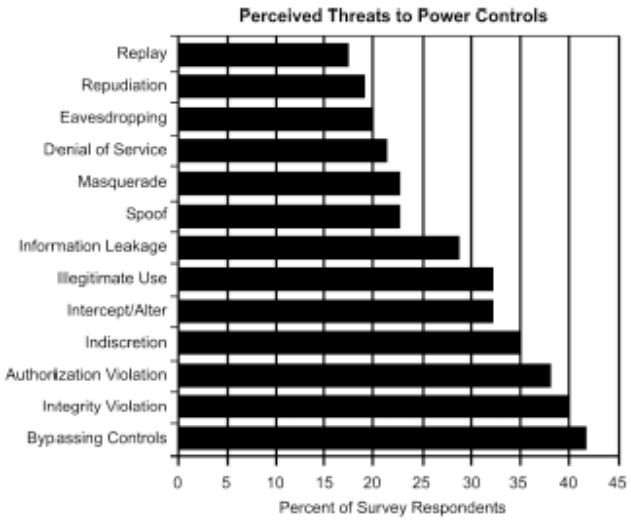

Fig. 1. Electric utility survey results of perceived threats to utility control centers (Electric Power Research Institute, 2000).

4. MODELING AND DESIGNING (S)QRA WITH HIGHLY INTERCONNECTED SYSTEMS

Accurately modeling highly redundant systems (such as an interconnected power system) is a complex process that is beyond the scope of this paper. However, a brief description illustrates the complexity. Most modeling approaches that reduce series and parallel combinations of elements with known failure rates assume that failures are independent. One commonly used example is a Markov process. However, most of the failures of highly redundant systems that occur in reality are common-mode failures (those where multiple components fail at the same time) or hidden failures (where a failure is not known until another component fails and causes an interruption to the end user). Dependencies of failures can occur for the following reasons:

- Facilities share common space (for example, utilities run two circuits on one structure)
- Separate supplies contain a common point upstream
- Failures bunch together during storms
- Maintenance considerations
- Hidden failures may be present.

Although each of these effects can be analytically modeled, much of the necessary input data is unavailable.

4.1 Current Practices for Security Assessment

Currently, notification processes and updates on various stages of electrical emergencies are in place at independent system operators (ISOs) and control centers. As an example, the California ISO's definitions for alerts are very pertinent. These include notification processes that span from multi-day ahead to within an hour – for example, for two-days-ahead forecast, day-ahead forecast, and within an hour. The stages of power system emergencies include:

- Stage 1 Emergency: Generating reserves are less than the required services (continuously recalculated, between 6 and 7%).

- Stage 2 Emergency: Generation reserves are less than 5% (which invokes a voluntary load-reduction program).
- Stage 3 Emergency: Generating reserves are less than the largest contingency (continuously recalculated, between 1.5 and 3%).

Colors can be associated with the three stages indicated above, such as yellow for Stage 1, orange for Stage 2, and red for Stage 3. These can also be made consistent with the North American Electric Reliability Corporation (NERC) and Department of Homeland Security (DHS) advisory systems.

As extensions, we can develop one or more metrics based on:

- Peak electricity demand forecast (demand exceeds previous levels)
- Inadequate generation availability to meet demand (by $x\%$) at any given hour, independent of the level of forecasted peak demand
- Loss of generation or transmission facilities, which triggers the item above
- Adverse weather at any given time or in a forecast (such as a hurricane or lightning storm)
- State/federal government terrorist alert levels.

Therefore, security metrics can be a multi-variable function of several variables: $Y = f(X_1, \dots, X_m) + V$. The variables X_i (for $i = 1, \dots, m$) can include reserve margins, voltage stability margins, frequency and its rate of change, area control error, $N - k$ contingency criteria, the status of protection devices, SCADA systems, EMSs, communication systems, and the status of fuel supply systems.

4.2 Need for the Identification of Disturbances

Reliable electric service is critically dependent on the whole grid's ability to respond to changing conditions instantaneously. Methods to identify changes in a network and their ranking will be critical for exercising the correct control effort. In particular, contingencies involving the loss of sources, sinks, and links need to be identified in real-time (or faster in a look-ahead) so that control actions can be taken in an effective manner.

The identification of disturbances in a network can be done in many ways. For example, in a power system, appropriate features of waveforms measured by dynamic recording devices can be used to extract some of the relevant information. In many networks, the main challenge is to identify a contingency consisting of a cascade of multiple events. Multiple-event contingencies are the ones that are most likely to lead to system-wide failures. The use of detection filters that are able to more clearly identify disturbances should be considered for this purpose.

4.3 Power System Reliability

Power system reliability can be classified into two components: adequacy and security (Billinton & Allan, 1984), (Billinton et al., 1991). Adequacy is the static evaluation of a system's ability to supply the load. Security refers to the system's capability to experience contingencies (outages), maintain service to all customers, and respect all equipment limits. Thus, security in this classical context refers to electrical system security, and does not include the impact of computer and communication systems. In general, adequacy is focused on planning, while security is focused on operations. Traditionally, these have been analyzed as separate issues, and it is quite possible to have a reliable but insecure system (say, in a system where critical contingencies are numerous but rarely occur) and vice versa.

A variety of reliability indices for distribution systems have been defined (IEEE Working Group on System Design, 1996). These indices can be divided into three categories: single-load-point indices, customer-orientated indices, and load-orientated indices. A survey by Warren (1991) indicates that the majority of the utilities use customer-based indices to evaluate their service reliability, with the most commonly used indices given as:

- System Average Interruption Frequency Index (SAIFI)
- System Average Interruption Duration Index (SAIDI)
- Customer Average Interruption Duration Index (CAIDI)
- Average Service Availability Index (ASAI)
- Momentary Average Interruption Frequency Index (MAIFI).

4.4 Power System Operating States

Several pertinent theories on power system operating conditions have been provided in the literature; these contributions not only provide mathematical foundations but also include some guidance on how to measure and adapt to disturbances. A power system can be characterized as having multiple states, or "modes," during which specific operational and control actions and reactions are taking place:

- *Normal mode*: Economic dispatch, load-frequency control, maintenance, forecasting, etc.
- *Disturbance mode*: Faults, instability, load shedding, etc.
- *Restorative mode*: Rescheduling, resynchronization, load restoration, etc.

Some authors include an alert mode before the disturbance actually affects the system. DyLiacco (1967) classifies power system operating states into normal, emergency, and restorative. This concept was extended by Chilar et al. (1969) by adding an alert state as shown in Fig. 2. Others add a system-failure mode before restoration is attempted (Fink & Carlsen, 1978). Fink and Carlsen further extended the classification by dividing the emergency state into two separate states, emergency and in extremis, based on system integrity and the balance between generation and load. Another contribution was provided by Zaborszky et al. (1979) who subdivided the emergency state into three crises (stability, viability, and integrity) to bring dynamics and time-frame characteristics into consideration.

Schulz and Price (1984) first addressed the issue of emergency identification by proposing emergency classification schemes with four dimensions: system integrity, branch loading, active power balance, and reactive

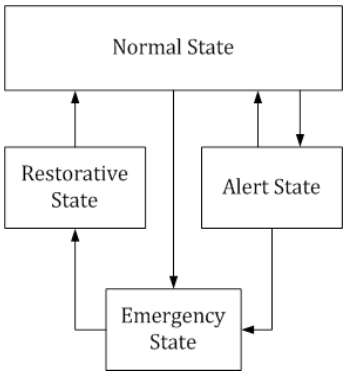

Fig. 2. Four states of a power system.

power balance. An emergency detector was proposed that sensed local variables (such as voltages, power, and frequency), processed the data, compared them to a priori analysis results, and initiated appropriate control actions if necessary.

Besides these many operational, spatial, and energy levels, power systems are also multi-scaled in the time domain, from nanoseconds to decades, as shown in Table 1. The relative time of action for different types of events, from normal to extreme, varies depending on the nature and speed of the disturbance, and the need for coordination. An example of the time frame for different types of events is shown in Fig. 3.

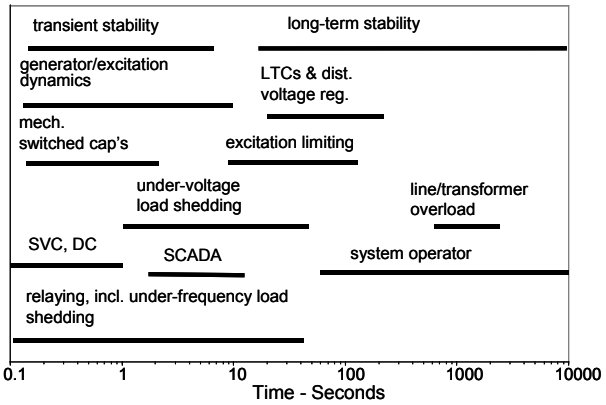

Fig. 3. System monitoring and operations along with their corresponding time frames.

Fig. 3 shows that for deployment of a well-coordinated overall defense plan, it is necessary to implement and coordinate various schemes and actions, spanning different time periods. Inadequacy of a well-coordinated overall defense plan makes it more difficult to prevent spreading of disturbances.

5. PATHWAYS FORWARD

The following examples highlight technologies and initiatives currently underway that can be used to further improve the measurements and metrics needed to enhance the security of our Nation's power systems.

5.1 Existing Capability: Complex Interactive Networks/ Systems Initiative

The goal of a completed joint Electric Power Research Institute (EPRI) and U.S. Department of Defense (DOD) program called the Complex Interactive Networks/Systems Initiative (CIN/SI) (Electric Power Research Institute, 2002) was to develop new tools and techniques that would enable large national infrastructures to self-heal in response to threats, material failures, and other destabilizers. Of particular interest was how to model enterprises at the appropriate level of complexity in critical infrastructure systems.

The CIN/SI research consortium developed a mathematical basis and practical tools for improving the security, performance, and robustness of critical energy, finance, communications, and transportation infrastructures. Among others, the technologies included intelligent adaptive islanding, a Strategic Power Infrastructure Defense (SPID) system, wide-area protection and control, neuro-fuzzy load forecasting and anticipatory dispatch, context-dependent network agents for real-time system monitoring and control, and computational mathematical foundations for complex networks.

For the power grid and other critical infrastructures, CIN/SI

Table 1. Time Hierarchy of Power Systems

Action/Operation	Time Frame
Wave effects (fast dynamics, lightning-caused overvoltages)	Microseconds to milliseconds
Switching overvoltages	Milliseconds
Fault protection	100 milliseconds or a few cycles
Electromagnetic effects in machine windings	Milliseconds to seconds
Stability	60 cycles or 1 second
Stability augmentation	Seconds
Electromechanical effects of oscillations in motors and generators	Milliseconds to minutes
Tie-line load-frequency control	1 to 10 seconds; ongoing
Economic load dispatch	10 seconds to 1 hour; ongoing
Thermodynamic changes from boiler-control action (slow dynamics)	Seconds to hours
System structure monitoring (what is energized and what is not)	Steady state; on-going
System state measurement and estimation	Steady state; on-going
System security monitoring	Steady state; on-going
Load management, load forecasting, generation scheduling	1 hour to 1 day or longer; ongoing
Maintenance scheduling	Months to 1 year; ongoing
Expansion planning	Years; ongoing
Power plant site selection, design, construction, environmental impact, etc.	2 years or longer

results laid the foundation for revolutionary self-stabilizing, self-optimizing, and self-healing capabilities. These capabilities will allow energy companies and other market actors to deliver energy and related products and services with unprecedented stability, reliability, efficiency, and power quality. In addition, more secure, reliable, and efficient operation of national infrastructures will enhance quality of life, economic productivity, and other essential parameters for modern society.

5.2 Emerging Effort: Fast Simulation and Modeling

Using fast simulation and modeling (FSM) techniques, pattern recognition and diagnostic models can determine the location and nature of suspicious events. In a project now underway, FSM will:

- Provide faster-than-real-time, look-ahead simulations and thus be able to avoid previously unforeseen disturbances
- Perform what-if analyses for large-region power systems from both operations and planning points of view
- Integrate market, policy, and risk analysis into system models and quantify their effects on system security and reliability.

5.3 Emerging Effort: Emergency Control and Restoration

Following a major terrorist attack or natural calamity, a system is needed that enables initial response to focus on creating self-sufficient "islands" in the power delivery system, which are able to make the best use of available network resources. Continuation of pioneering work completed as part of CIN/SI on an SPID system would enable analysis of information about the status of the power-delivery system and a secure communication system after a terrorist attack, as well as coordinate their use for adaptive islanding. Once a stable configuration of power-delivery system islands has been established, self-healing algorithms could then be used to gradually return the power delivery system to its normal state as more resources become available.

5.4 Emerging Effort: Smart Grid

The concept of smart grids, pertinent R&D programs aimed at developing self-healing grids, and the associated terminology, date back to 1990s. As noted above, of particular interest is the large-scale CIN/SI research program. Many define "Smart Grid" in terms of its functionalities and performance objectives (e.g., two-way communications, interconnectivity, renewable integration, demand response, efficiency, reliability, self-healing, etc.).

While there are many definitions, there is one vision of a highly instrumented overlaid system with advanced sensors and computing with the use of enabling platforms and technologies for secure sensing, communications, automation, and controls as keys to: 1) engage consumers, 2) enhance efficiency, 3) ensure reliability, and 4) enable integration of renewables and electric transportation. Recent policies in the U.S., China, India, EU, and other nations, combined with the potential for technological innovations and business opportunities, have attracted a high level of interest in smart grids. Smart grids are seen as a fundamentally transformative, global imperative for helping the planet deal with its energy and environmental challenges.

6. CONCLUSION

In this paper, a framework for developing needed indices and standards for benchmarking SQRA in the future is discussed, with an emphasis on the issue of measures to determine security performance. The immediate and critical goal is to avoid widespread network failure, but the longer-term vision is to enable adaptive and robust infrastructure. Installing modern communications and control equipment (elements of the smart grid) will help, but security must be designed into the system from the beginning, not pasted on as an afterthought.

REFERENCES

Billinton, R. and Allan, R.N. (1984). *Reliability Evaluation of Power Systems*. Plenum Press, New York.

Billinton, R., Allen, R.W., and Salvaderi, L., eds. (1991). *Applied Reliability Assessment in Electric Power Systems*. IEEE Press.

Chilar, T.C., Wear, J.H., Ewart, D.N., and Kirchmayer, L.K. (1969). Electric utility system security. In *Proc. of American Power Conference*.

DyLiacco, T.E. (1967). The adaptive reliability control system. *IEEE Trans. on Power Apparatus and Systems*, PAS-86 (5), pp.517-61.

Electric Power Research Institute (2000). *Communication Security Assessment for the United States Electric Utility Infrastructure*. EPRI, Palo Alto, CA.

Electric Power Research Institute (2002). *Complex Interactive Networks/Systems Initiative: Final Summary Report: Overview and Summary Report for Joint EPRI and U.S. Department of Defense University Research Initiative*. EPRI, Palo Alto, CA.

Electric Power Research Institute (2005). *Strategic Insights Into Security, Quality, Reliability and Availability Report*. EPRI, Palo Alto, CA.

Fink, L.H. and Carlsen, K. (1978). Operating under stress and strain. *IEEE Spectrum*, pp.48-53.

IEEE Working Group on System Design (1996). *Trial Use Guide for Electric Power Distribution Reliability Indices*. Draft #14.

Schulz, R.P. and Price, W.W. (1984). Potential applications of fast phasor measurements of utility systems. *IEEE Transactions on Power Apparatus and Systems*, PAS-103, pp.3471-79.

Warren, C.M. (1991). The effect of reducing momentary outages on distribution reliability indices. In *Proceedings of the 1991 IEEE T&D Conference*, pp.698-703.

Zaborszky, J., Whang, K.W., and Prasad, K.V. (1979). Monitoring, evaluation and control of power system emergencies. In *Proc. of the Systems Engineering for Power Conference*.