INL/CON-16-39196
PREPRINT

Metrics required for Power System Resilient Operations and Protection

Resilience Week 2016

K. Eshghi, B. K. Johnson, C. G. Rieger

August 2016

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

Metrics required for Power System Resilient Operations and Protection

K. Eshghi, *Member, IEEE*, B.K. Johnson, *Senior Member, IEEE,* C.G. Rieger, *Senior Member, IEEE*

***Abstract*—Today's complex grid involves many interdependent systems. Various layers of hierarchical control and communication systems are coordinated, both spatially and temporally to achieve gird reliability. As new communication network based control system technologies are being deployed, the interconnected nature of these systems is becoming more complex. Deployment of smart grid concepts promises effective integration of renewable resources, especially if combined with energy storage. However, without a philosophical focus on resilience, a smart grid will potentially lead to higher magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially catastrophic event. Future system operations can be enhanced with a resilient philosophy through architecting the complexity with state awareness metrics that recognize changing system conditions and provide for an agile and adaptive response. The starting point for metrics lies in first understanding the attributes of performance that will be qualified. In this paper, we will overview those attributes and describe how they will be characterized by designing a distributed agent that can be applied to the power grid.**

***Index Terms*-- Communication System security, Information security, Power System Stability, Power transmission, Resilience.**

I. Introduction

Modern societies depend on the stable, efficient, and secure operation of critical infrastructure. Due to multiple redundancy bulk transmission system (BTS) equipment power outages due to transmission failures are much less frequent than those in distribution equipment, but transmission failures affect many more customers, and outage costs can be much higher. As a result less investment is made in protecting distribution systems from common outage mechanisms. This fact, combined with the high cost per mile or per piece of transmission equipment, has historically resulted in greater focus on transmission system reliability. Hurricane Sandy [1], the Havex malware [2], and the 2003 east coast blackout [3] and many other events on BTS have reminded us that natural and un-natural events can dramatically upset the complex systems that provide energy, transportation, water, medical care, emergency response, and security. Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience" [4] recognized the need to advance research and development for resilient critical infrastructures.

At the core of critical infrastructure operation are industrial control systems (ICS). Communication network capability has been added for central monitoring, and digital computers are used to ease implementation of feedback and relay controls in modern SCADA systems. Unfortunately, the use of distributed control network components has established a framework that introduces additional complex human cognitive and control system interdependencies and cybersecurity vulnerabilities, resulting in brittle systems with increased potential for cascading failures. Currently used control systems lack the inherent ability to analyze asymmetric, unexpected failures of the system controlled, and often require the operator/dispatcher to be the analyst and the root cause expert at a time of potentially high stress. Even with decision support tools, the human in the loop is required to mine a large volume of data. Ultimately, modern ICS are reliable but lack the resilient framework needed to achieve stable and secure operation in varied operating conditions, let alone the ability to recognize and optimize a response to a natural or manmade, malicious or benign, unexpected event. Therefore, there exists a gap in establishing resilient critical infrastructure systems.

A resilient control system design holistically considers the challenges in developing a control system that maintains state awareness and an accepted level of normalcy in response to disturbances, including threats of an unanticipated and malicious nature [5]. Therefore, resilient control is a design and operational methodology, which encompasses the whole of system performance, including cyber security, physical security, economic efficiency, dynamic performance, and process compliance, in large-scale, complex systems [6][6], [7].

In this paper we are evaluating metrics needed to develop "Region of Reliability" concepts for identifying unreliable operating states using decentralized agent throughout power system. The goal of Region of Reliability is to find the margin around the current operating point before any resiliency criteria are violated. This includes post contingency thermal, voltage stability constraints, cyber disturbances, and cognitive disturbances. For resilience agent to be affective needs to have to following characteristics as shown in Fig. 1.

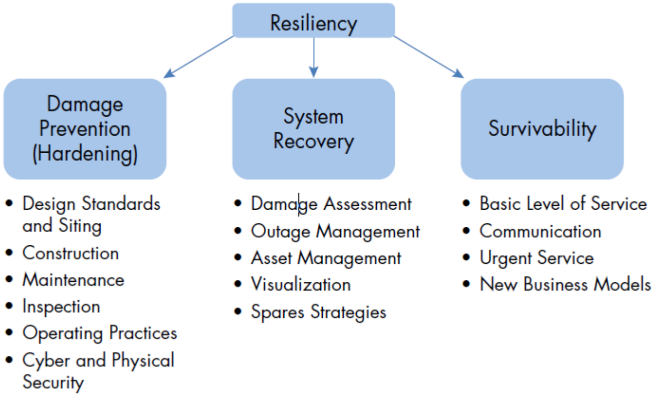

Fig.1 Resilience model

Electric grid modernization, through smart grid research and development, provides an opportunity to incorporate resilient control system architectures. Smart grids add many more capabilities to measure, control, and manage the generation, distribution and the consumption of electrical power in a manner that is intended to produce a more available, cleaner, stable and economical supply of electricity. The power of additional information is obvious (e.g. optimization of transmission assets, integration of greater renewable generation, and economic assessment and decision making put into the hands of consumers). However, the counterpoint is a more complex and computerized system that are operated with less margin to recover from threats and with more potential to be impacted through exploitation of cyber and physical vulnerabilities. In addition, the complexity of this environment also imposes additional human performance demands on the people monitoring and making operational decisions using a plethora of new, diverse types of data. Application of resilience seeks to optimize when possible, but to never sacrifice, operational minimums that risk large consequences through unintentional introduction of brittleness.

A unifying approach to produce metrics for such a diverse set of disturbances can be considered in looking at impact to the subsystems that make up critical infrastructure operation. With the implementation of an ICS, performance became dependent on both time (availability) and data integrity of the communications, sensing and control mechanisms. Time is important, both in terms of delay of mission and communications latency, and data, in terms of corruption or modification. In general, the idea is to base metrics on "what is expected" and not necessarily the actual initiator that caused the degradation.

To implement metrics we are going to suggest the development and deployment of agents, which offer a notional framework for distributed monitoring and analysis of precursors to disrupting events. Within these agents, we will be proactive in evaluating not only physical systems but also cyber systems and the hybrid interplay between the two. First we will overview the four separate attributes of such an agent including small signal stability, transient stability, communications latency, and degradation assessment. Then we will expand upon the fourth area and provide the experimental basis of this contribution as a work in progress. The theory and basis for the first three attributes are covered in another publication [9].

II. Performance Measures to Use in a Resilient Power System Agent

A. Power system small signal stability (Data Dependent)

As with any critical infrastructure system, ensuring the stability of a power system is a fundamental performance requirement [13], [14], [15] to characterize resilience. Traditional distributed control for most sectors predates digital control systems, and maintains global stability by maintaining local stability of individual control areas using local measurements. Within the power grid, stability is instead maintained through aggregating data for centralized control over larger geographic regions. While this mechanism remains the most practical, its flaw lies in the fact that maintaining global performance is not distributed and therefore localized feedback in response to disturbances is not achieved. To analyze global system performance at a planning stage, we traditionally apprehend power system reaction to small disturbances happening at specific locations and the systems capability to keep synchronism in the face of a set of feasible operating conditions using small signal stability analysis [16]. The ability to perform these studies is highly dependent on the a-priori knowledge on how the system is likely to respond of the person performing the studies.

B. Power system transient stability (Data Dependent)

Another global performance characteristic that is assessed in a planning stage is the transient stability margin. A power system is transiently stable if the power system maintains synchronism during the response to severe disturbances [17]. Performing real time simulation of large systems to determine the margin between stable response and unstable response for a given operating state may be untenable from a practical standpoint. This is due to limitations of computational power, and could be further limited by communication latencies. Mechanisms are needed to determine what the global optima are to measure and determine where a given operating condition is near a boundary of stability. In addition, global efficiency as well as stability is important to next generation resilient designs [7], [8]. A potential metric for this was developed in [9].

C. Power system communication latency (Time Dependence)

Consensus and feedback loop stability can be affected by latencies in the communication and in the computational processes of the control system architecture. Research into the effects and constraints on latencies has been performed to determine impact on control system stability [18], [18]. Several different approaches have been taken, including evaluating the impact on individual control algorithms and determining maximum acceptable latency. Other methodologies for developing metrics have characterized latency as part of the overall dynamics of a multi-agent hierarchy, representing communications links as transfer functions between individual agents that are stabilized by a given control algorithm [19].

D. Power system physical degradation (Data and Time)

Dependence upon sensor data for judgment dictates that a method to ensure that the impact of failed or inaccurate sensors needed to monitor health of the system is handled gracefully by identifying the degradation and changing sensor combinations used to achieve observability and controllability. In addition, the characterization of a physical attribute may include modeling coupled with sensor data, or strictly synthetic data from a mathematical observer. The sensory framework, therefore, must provide methods for interpreting information quality, in addition to sensor and control device redundancy and diversity to allow for reconfiguration based upon degradation or outright failure [10], [11], [12]. From a control theory perspective, similar considerations are necessary to enable maintaining critical control when failures are detected. This may include access to alternative paths and associated controls, but not necessarily the switching of components (parallel paths may be online at all times).

III. Resilience Agent for Real-Time Resilience Measurement

A. State estimator

The best way to develop a measure of resilience detects physical/cyber-attack on power system is by developing of detailed representation of station arrangements with the explicit modeling of circuit breakers and station layout, as shown in Fig.1, which has a series of advantages. There are a number of simple rules that have been used in practice for checking telemetry. For instance, if a bus injection is measured, or is treated as a zero injection pseudo-measurement, and all the incident power flows are measured as well, then the summation of the power flows can be checked against the injection value. This is a simple, effective application of the Kirchhoff's Current Law (KCL). If we take section of power system as the one represented in Fig. 2, the state estimator will develop all the network branches, would represent circuit breakers, and formulate a state estimation problem. In cases as when one of the power flows adjacent to a node are missing, it will calculate it automatically (if data available permits), and will supply the new information to the opposite side of the connection for KCL verification at that node. Still, the calculations are simple enough to be performed during the preprocessing of telemetry, or even at the remote units (other substations), if found it to be appropriate during operation and the resources are available.

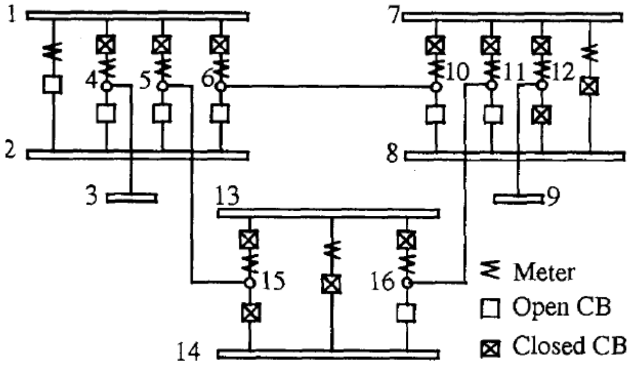

Fig.1 substation estate estimation

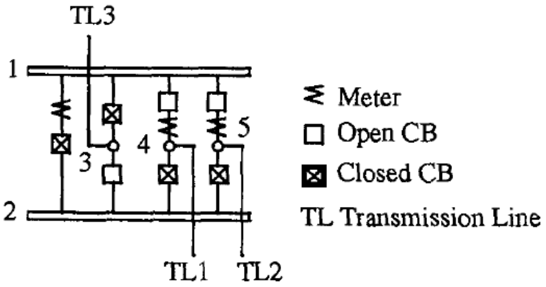

Fig.2 substation estate estimation

For state estimator to be able to calculate KCL and Kirchhoff's Voltage Law (KVL) equations on each substation bus and line, requires that state estimator routine to have a basic understanding or equipment impedance inside and outside of the substation and be able to use available/historical voltage transformer (VT) and current transformer (CT) values. These techniques will provide much better model but also would require a lot of computational power and data system management, complicating agent design.

After KCL and KVL calculation is done we can use state estimator to calculate unknowns and/or verify measurements in our system to do that first we need to define states for our power system. The system state is defined as the complex voltage magnitude and angle at each bus for each agent.

$$\widetilde{V_i} = V_i e^{j\delta_i} \qquad (1)$$

$$X = [\delta_1 \, \delta_2 \ldots \delta_n \;\; V_1 \, V_2 \ldots V_n]^T \qquad (2)$$

For each state we can observe the state by using measurement models at each bus as shown in (3).

$$z_i = h(x)_i + v_i \qquad (3)$$

Where *z* is calculated state h(x) is measurement model and *v* is noise. For above equations and using methods from well know published papers we can find the cost function using the following equation.

$$C(\hat{x}) = \sum_{i=1}^{m} \frac{(z_i - h_i(\hat{x}))^2}{R_i} \qquad (4)$$

The state estimator will work to minimize the cost function by

$$g(\hat{x}) = \frac{d}{d\hat{x}} C(\hat{x}) = -H^T(\hat{x}) R^{-1}\big(z - h(\hat{x})\big) = 0 \qquad (5)$$

Where

$$H(\hat{x}) = \left(\frac{d}{d\hat{x}} h(\hat{x})\right) \qquad (6)$$

After system estate estimation for local area is done each substation will send estimated changes to their local remote substation for a distributed power system model update.

B. Region of Stability

Subsequent to the completion of the state estimation process, the following constraints may be simultaneously monitored and enforced on the boundary:

- Steady-state stability
- Voltage constraint (voltage range and pre-to post contingency voltage drop.
- Thermal overloads.
- Small signal stability.
- Transient Stability

For example each agent can continuous monitor the system conditions in terms of its proximity to voltage collapse by running point to point the P-V and Q-V curve analysis on each local substation.

The next stage is this research is to implement these agents and test them…..

IV. Conclusion

The paper has laid out the requirements and operation of resilience metrics required for distributed agents, the attributes of which can be integrated to provide a localized means to recognize disturbances. The key attributes are localized small signal stability calculations, transient stability calculations, and addressing the impact of communication latency. To do this, each agent first needs to be able determine a local state estimation of power system using proposed techniques. Then each agent can share estimated qualities with neighboring agent for data validation and verification, producing a decentralized state estimate independent of the one computed at the system operating center. These attributes collectively evaluate the resilience threshold of a power system during abnormal events and measures the system performance against minimum performance expectations, providing an adaptive capacity that allows for proactive response. That is, measuring desired performance against necessary performance enables a proactive response. Having a metric independent of the system operating center, allows the decentralized control architecture to be able to respond to major disruptions to the system that include a loss of the SCADA system. The performance expectation will depend on system power system contingency status.

The distributed agent described here would improve state awareness of future grid operation with integration of more renewable and more volatile energy resources, through the ability of the distributed agent to quickly recognize disturbances before they propagate into cascading failures. Using distributed state estate estimation and above resilience metrics to find the most economical and maintaining resilience allows Transmission Operators and owners to plan transmission system maintenance outages and upgrades utilizing availability of more nontraditional generation. Also, having the set of accurate system models distributed in agents and high-performance controllers provides engineers with the ability to ensure reliability while quickly restoring customer access to transmission system due to any type of event.

V. References

[1] NERC *Hurricane Sandy Event Analysis Report*, October 2012.

[2] D. Walker, "'Havex' malware strikes industrial sector via watering hole attacks," *SC Magazine*, June 2014.

[3] G. S. Vassell, "Northeast blackout of 1965," IEEE Power Engineering Review, pp. 4–8, Jan. 1991.

[4] Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience" February 2013.

[5] C.G. Rieger, D. I. Gertman and M.A. McQueen, "Resilient Control Systems: Next Generation Design Research," *2nd Conference on Human System Interactions*, May 2009.

[6] C. G. Rieger, "Notional Examples and Benchmark Aspects of a Resilient Control System," *3rd International Symposium on Resilient Control Systems*, August 2010.

[7] Q. Zhu, C. Rieger and T. Basar, "A Hierarchical Security Architecture for Cyber-Physical Systems," 4th *International Symposium on Resilient Control Systems*, August 2011.

[8] C. G. Rieger, "Resilient Control Systems Practical Metrics Basis for Defining Mission Impact," 7th *International Symposium on Resilient Control Systems*, August 2014.

[9] K. Eshghi, B.K. Johnson and C. G. Rieger, "Power System Protection and Resilience Metrics," 8th *International Symposium on Resilient Control Systems*, August 2015.

[10] H.E. Garcia, W.-C. Lin, S.M. Meerkov, and M.T. Ravichandran, "Data Quality Assessment: Modeling and Application in Resilient Monitoring Systems," *Proceedings of the 5th International Symposium on Resilient Control Systems*, pp. 124--129, August 2012.

[11] H.E. Garcia, W.-C. Lin, and S.M. Meerkov, "A Resilient Condition Assessment Monitoring System," *Proceedings of the 5th International Symposium on Resilient Control Systems*, pp. 98--105, August 2012.

[12] H.I. Elsayed, B.K. Johnson, and L.L. Lai,, "Online Systems Potential Application in Intelligent Power Grid" *Power and Energy Society General Meeting*, 2012 IEEE.

[13] Y. J. Chan, *Margin of Maneuver Approach to Define Resilient Control Systems*, Ohio State University Master's Thesis, 2012.

[14] C. P. Steinmetz, "Power control and stability of electric generating stations," *AIEE Trans*., vol. XXXIX, Part II, pp. 1215–1287, July 1920.

[15] AIEE Subcommittee on Interconnections and Stability Factors, "First report of power system stability," *AIEE Trans*., pp. 51–80, 1926.

[16] P. Kundur, *Power System Stability and Control*, McGraw-Hill, 1994.

[17] C.G. Rieger and K. Villez, "Resilient Control System Execution Agent," *5th International Symposium on Resilient Control Systems*, pp. 143-148, August 2012.

[18] F. Wang and D. Liu, Networked Control Systems: Theory and Applications, Springer-Verlag, London, 2008.

[19] S. Hara, T. Hayakawa, and H. Sugata, "Stability Analysis of Linear Systems with Generalized Frequency Variables and Its Applications to Formation Control," 46th IEEE Conference on Decision and Control, pp. 1459-1466, December 2007.