Smart Grid: Reliability, Security, and Reslieincy

Paul Hines[1,2], Jason Veneman[3], Brian Tivnan[2,3]

[1]School of Engineering, The University of Vermont, Burlington, VT 05401, USA

[2]Vermont Complex Systems Center, The University of Vermont, Burlington, VT 05401, USA

[3]The MITRE Corporation, McLean, VA 22102, USA

January 28, 2014

Abstract

Smart grid technology has the potential to substantially improve electricity service by increasing reliability, reducing environmental impacts, and decreasing costs. However, smart grid deployment involves, by definition, an increased coupling between communication networks and electric power networks. Research on abstract networks indicates that increased coupling between networks can increase the risk of large failures. However, the existing research provides little understanding of how these general findings apply to the specific problems posed by the coupling of power grids to communication networks. Effectively understanding and mitigating new risks will require substantial improvements in our understanding of coupled networks. A first step in that direction is to clarify how risk is described in both systems, since similar terms are used to describe different concepts in these two increasingly coupled industries.

1 Introduction

The American Recovery and Reinvestment Act of 2009 dramatically accelerated the deployment of smart grid technology by initiating $4.5 billion in matching grants for smart grid technology, as well as tens of billions in parallel investments in communication and electricity infrastructure improvements. Despite warnings from some that smart grid communication security standards were not ready for large-scale deployment [7, 10, 8], smart grid investments proceeded. As a result, smart grid technologies, such as Advanced Metering Infrastructure (smart metering systems) and distribution system automation have been rapidly deployed. In part because of uncertainty about security in these systems, some smart grid capabilities have not yet been fully enabled or exploited. For smart grid to realize its potential, there is a need to understand how coupling between communication and power networks will affect the reliability, security, resiliency, and robustness of these networks.

However, these reliability concepts (reliability, security, vulnerability, etc.) differ from one another, and in some cases have different meanings in electricity industry

and IT industry contexts. Here we seek to define the terminology used in these two contexts, with the goal of setting the conceptual foundation for the science and engineering needed for progress in this domain.

2 The many smart grid networks

There are many definitions of smart grid [1, 12], but all acknowledge the significance of using information technology to improve electricity service. Thus, we define smart grid as the coupling of communications systems and power and energy technology to improve the reliability, environmental performance, and economic efficiency of electric power systems. Under all definitions, improved reliability is a key potential benefit of smart grid, particularly given increasing concerns about the risk from large natural disasters (e.g., superstorm Sandy and Irene) and the continued risk of terrorist attack. However, storms and attackers can also damage the information technology upon which smart grid depends. If smart grid is to realize its potential, it is critical that we understand how both natural failures and volitional attacks impact both systems.

However, smart grid couples together not a single unified power grid to a single information network, but rather different types of power networks to many distinct communication networks. Understanding the differences between these networks is key to progress in this field.

On the power grid side, continental-scale power grids are typically divided into interconnections, which are connected together only through direct current power lines. The result is that generators in different interconnections are not synchronized with one another; it is practically impossible for outages to spread across interconnection borders. The US power grid is divided into three interconnections: the Western, Eastern, and Texas Interconnections. Furthermore, the transmission networks, over which power is moved long distances, have a substantially different structure than the distribution networks, through which power moves from the bulk grid to individual customers. Transmission and distribution networks typically have separate control systems, with substantially more automation at the transmission level (though smart grid is rapidly adding automation at the distribution level).

The information networks that gather data from and control power grids are also diverse. Transmission networks have, for many years, been monitored and controlled by Supervisory Control And Data Acquisition (SCADA) networks. In a SCADA system, a remote terminal unit (RTU) collects data from devices in a substation, and delivers the data in packets, on command, to a central Energy Management System (EMS). SCADA systems typically move data over a combination of proprietary wireless (often microwave) and fiber optic channels. Some utilities are currently exploring the use of public information networks for SCADA, with Virtual Private Networking (VPN) tools to encrypt communications, though most rely on proprietary systems that have few, if any, connections to the utility's business networks, or the public Internet.

One of the most obvious outcomes of smart grid deployment is the smart meter and associated customer-utility communication systems, which are collectively known

as Advanced Metering Infrastructure (AMI). The two most common types of AMI communications networks are mesh wireless networks, in which meters connect to one another to build a network over which data can be moved to and from collectors, and Power Line Carrier (PLC) systems, in which data are embedded as pulses in the physical power lines. In both cases, data collectors are typically connected to the utility through proprietary fiber optic, or in some (particularly rural) cases, broadband wireless systems. AMI systems are used almost exclusively to move billing data and meter disconnect commands to and from meters. Since AMI and SCADA are typically designed to have a substantial barrier between them, AMI systems arguably present less risk to bulk power grid stability.

In some cases, utilities are building SCADA-like systems for their distribution networks. These communication networks are often more closely connected to AMI networks. Because these automation systems can control switches with substantial loads, increased coupling between AMI and SCADA is a more significant security concern.

On the customer side of the meter, many utilities are enabling wireless communication systems that allow for customer-owned devices to communicate with the smart meter. For commercial and industrial systems, these are typically known as Building Energy Management systems. Residential customer-side systems are known as Home Area Networks (HAN). Most HAN systems use either a form of Zigbee (IEEE Standard 802.15) or WiFi (IEEE Standard 802.11) communications systems. While the security risks from HAN systems are arguably limited, many have concerns about privacy issues that these relatively open networks introduce [11]. Because of the nature of customer-side applications, HANs are almost always connected to the public Internet in some way, introducing additional security and privacy challenges.

Finally, one of the most critical information network for electric power systems is that used by financial traders to buy and sell electricity-related contracts, as well as the networks used by generators to exchange bid and dispatch-related information with power market operators. In most cases, trading is performed over encrypted Internet-based channels. Because markets are critical for reliable and efficient power grid operations, these networks are increasingly important.

When we couple information networks to the power grid, we are really coupling many different communications networks to many different transmission and distribution networks. Understanding the full implications of this multi-faceted coupling is a significant research challenge.

3 Defining risk and reliability terminology

Risk, according to [2], is the exposure to the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility. In the context of risk analysis (e.g., [9]), risk is often more formally defined as:

$$\text{Risk} = \text{Exposure} \times \text{Vulnerability} \times \text{Cost} \tag{1}$$

Exposure is the extent to which a particular object or system is exposed to potential hazards. When expressed probabilistically, exposure is the probability that a particular object will be contacted by a hazard. Vulnerability, in this context, is the probability that an object fails, given that it is contacted by a hazard. Often exposure and vulnerability are combined into an overall probability that a particular component will fail. "Cost" refers to the total system cost that would result from the failure of a particular component. In the case of interconnected infrastructures, this cost needs to account for not only the immediate impact of the component failure (the cost of the transformer, for example), but also the costs incurred from potential cascading failures that might be triggered by a particular outage or set of outages.

It is common in risk analysis to use data on historical outages and simulations to assess the expected value of (1) over some range of potential set of failures. This expected value is often reported as a measure of system reliability.

3.1 Reliability

There are many terms used in reliability discussions, including security, resiliency, risk, robustness, and vulnerability. Reliability is often used to encompass all of these, representing an average or expected level of service provided by the system over a time period (often measured annually).

In the communications industry, reliability is typically measured as the fraction of time that a particular service (such as a web server) is available. Other reliability measures include the fraction of data packets that successfully reach their intended destination, or the latency associated with packet delivery.

In the electricity industry, reliability is often measured differently at the distribution (retail service) level and at the bulk transmission/generation (bulk) level. At the distribution level, two of the most common reliability metrics are the System Average Interruption Frequency Index (SAIFI) and the System Average Interruption Duration Index (SAIDI) [3]. SAIFI measures the average frequency of outages per customer and SAIDI measures the average duration of outages, over a one year period, per customer. At the bulk grid level, a common reliability metric is the expected amount of electric energy demand that goes unserved over a specified period (often referred to as the Loss of Load Expectation, LOLE).

There are a number of established methodologies and industry tools (e.g., GE MARS [4]) designed for reliability analysis for power systems. However, there is tremendous uncertainty about how to model the impact of smart grid in reliability analysis tools.

3.2 Security, Robustness and Vulnerability

The trouble with the conventional reliability metrics described above is that scalar values, such as LOLE can obscure the risk from high impact, low probability (HILP) events, such as a coordinated terrorist attack or an extreme weather event. While measuring risk from these events is difficult for statistical reasons, a variety of approaches exist to deal with HILP risk. When a system is relatively resistant to low

probability events, it is common to label the system as "secure," or more secure. Security is often associated with "robustness," in that a secure system is robust to (able to resist) attacks or random failure.

However, security has a very specific meaning in the electricity industry. A power system is said to be secure if no single component failure (also known as an outage or a contingency) will cause the system to violate its operating limits (typically voltage limits at nodes, and flow limits on transmission links). This is congruent with the general concept of security only if there is no chance of multiple components failing in close temporal proximity. However, when they do occur, storms and terrorist attacks typically result in several outages nearly simultaneously. As a result, declaring a power system secure does not mean that it is particularly resistant to high impact low probability events.

On the other hand, security in other domains often refers specifically to the ability to resist volitional attacks. A building is said to be secure when its doors are locked and its alarm system is running. A nation is secure when it has a strong military defense. In the communications industry, security often refers specifically to encryption: e.g., a secure wireless transmission. When used in smart grid contexts, security most frequently refers to cyber-security, or designing the smart grid communication systems such that they are resistant to attempted cyber-attacks.

3.3 Survivability and Resilience

There is increasing literature arguing that large interconnected systems, because of their inherent complexity, will sometimes fail despite best efforts to mitigate risks in those systems. Given the notion that some failures are inevitable (e.g., storms will always damage power lines, and hackers will always occasionally compromise some information systems) there is a need to ensure that the most important infrastructure services continue, even when components fail, and that after failures occur, infrastructures recover quickly from those failures.

The term survivability is often used to describe the idea of designing systems such that their most important functions can continue, even when the system as a whole is substantially degraded [14]. Measures that can increase survivability with respect to blackouts include adding battery backup to streetlights at critical intersections and ensuring that emergency service providers (police, fire, hospitals) have well-maintained backup power systems. In IT systems, survivability typically refers to the ability of the system to provide critical services, after some portion(s) of the network has been compromised.

Resilience, on the other hand, refers specifically to the ability of a system to recover from a failure after it has occurred. The importance of resilience became particularly clear in the wake of Superstorm Sandy (October 2012). Many critical services, such as the stock market, were disabled for days as a result of infrastructure damage in New York. There is broad agreement that a more resilient electricity infrastructure is desirable, however there is little agreement about exactly what actions need to be taken to make electricity more resilient.

In the context of power systems, resilience is closely related to restoration, which is

the process of restoring a power grid after a blackout. Restoration has been studied extensively in the literature (e.g. [5, 6]). One of the principal near-term benefits of smart grid is the ability to optimize the restoration process. For example, smart meters provide utilities with precise data regarding which locations do not have power, allowing them to more efficiently dispatch restoration crews. Also meters with remote disconnect switches should eventually enable utilities to switch off non-critical loads after a major outage, and use distributed generation (which may not be sufficient to supply the entire load) to quickly restore power to more critical ones [13].

Developing and evaluating new strategies for making electricity more resilient and more survivable are important areas for research and development going forward.

4 Moving forward

Given a common understanding of how reliability and security are understood in these two domains, much can be done to make the emerging Smart Grid more reliable and more secure.

Some problems can be solved in the near term. Developing standards that allow not-centrally controlled distributed generation to operate separately from the bulk grid (e.g., microgrids) after a storm or a terrorist attack could be hugely beneficial.

Other problems will take more research and development. More research is needed in order to, for example, understand where the largest risks are in coupled smart grid systems as well as finding the most effective strategies for mitigating those risks. Given that budgets are limited and that many different types of threats exist, the electricity industry needs better tools to be able to assess difficult tradeoffs, like choosing optimally among new investments in backup power systems (survivability), new technology for restoration (resilience) or more transmission lines (security). Better models are needed to make strategic choices among these options.

References

[1] The smart grid: An introduction: How a smarter grid works as an enabling engine for our economy, our environment and our future. Tech. report prepared by litos strategic consulting, US Dept. of Energy, 2009.

[2] *New Oxford American Dictionary*. Oxford University Press, USA, 2010.

[3] P1366/d8, mar 2012 - ieee draft guide for electric power distribution reliability indices. Online: http://ieeexplore.ieee.org/servlet/opac?punumber=6194243, March 2012.

[4] Mars: Ge concorda multiple area reliability simulator. Technical report, GE Energy Consulting, 2014.

[5] M Adibi, P Clelland, L Fink, H Happ, R Kafka, J Raine, D Scheurer, and F Trefny. Power system restoration-a task force report. *Power Systems, IEEE Transactions on*, 2(2):271–277, 1987.

[6] M.M. Adibi and L.H. Fink. Power system restoration planning. *IEEE Transactions on Power Systems*, 9(1):22–28, 1994.

[7] Seth Blumsack and Alisha Fernandez. Ready or not, here comes the smart grid! *Energy*, 37(1):61–68, 2012.

[8] Andy Bochman. Smart grid security blog. Online: http://smartgridsecurity.blogspot.com/, 2013.

[9] Louis Anthony Cox. Evaluating and improving risk formulas for allocating limited budgets to expensive risk-reduction opportunities. *Risk Analysis*, DOI: 10.1111/j.1539-6924.2011.01735.x, 2011.

[10] Linda R. Evers. Nist smart grid standards need work. *Smart Grid Legal News*, Feb. 1 2011.

[11] Patrick McDaniel and Stephen McLaughlin. Security and privacy challenges in the smart grid. *Security & Privacy, IEEE*, 7(3):75–77, 2009.

[12] M Granger Morgan, Jay Apt, Lester Lave, Marija D Ilic, Marvin A Sirbu, and Jon M Peha. The many meanings of "smart grid". Technical report, Carnegie Mellon University, 2009.

[13] Anu Narayanan and M Granger Morgan. Sustaining critical social services during extended regional power blackouts. *Risk Analysis*, 32(7):1183–1193, 2012.

[14] S.N. Talukdar, J. Apt, M. Ilic, L.B. Lave, and M.G. Morgan. Cascading failures: survival versus prevention. *The Electricity Journal*, 16(9):25–31, Nov. 2003.