TESTIMONY OF

William H. Sanders

Donald Biggar Willett Professor of Engineering
Head, Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, IL

BEFORE THE

United States House of Representatives
Committee on Science, Space, & Technology

HEARING ON

Resiliency: The Electric Grid's Only Hope

October 3, 2017

Rayburn House Office Building
Washington, DC

(Portions of this testimony were taken verbatim from the National Academies of Sciences, Engineering, and Medicine report "Enhancing the Resilience of the Nation's Electricity System, ISBN 978-0-309-46307-2 | DOI 10.17226/24836, available at http://nap.edu/24836 and the associated "Report in Brief")

Introduction

Chairman Smith, Vice-Chairperson Lucas, Ranking Member Johnson, members of the committee: I am honored to appear before you today to discuss the resiliency of the United States power grid.

I am a Donald Biggar Willett Professor of Engineering and the Head of the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. I was the founding director of the Information Trust Institute at the University of Illinois, and served as director of the Coordinated Science Laboratory at Illinois. I am a professor in the Department of Electrical and Computer Engineering and in the Department of Computer Science. I am a fellow of the IEEE, the ACM, and the AAAS; a past chair of the IEEE Technical Committee on Fault-Tolerant Computing; and past vice-chair of the IFIP Working Group 10.4 on Dependable Computing.

I am an expert on secure and dependable computing with a focus on critical infrastructures. I have published more than 270 technical papers in those areas. I was the 2016 recipient of the IEEE Technical Field Award, Innovation in Societal Infrastructure, for "assessment-driven design of trustworthy cyber infrastructures for societal-scale systems." Since 2005, I have led or co-led major government-funded centers (TCIP, TCIPG, and CREDC) that work to make the grid secure and resilient. I was also a member of the committee that wrote the National Academies of Sciences, Engineering, and Medicine consensus report entitled "Enhancing the Resilience of the Nation's Electricity System" that is the subject of this hearing. In short, my experiences provide me with a unique perspective to offer the Committee insight and recommendations concerning the impairments to and approach for providing resiliency in the electric power grid.

In my remarks today, I will:

- Describe the concept of resiliency.
- Provide an overview of the report, why it is important, and the top recommendations from the report that should be implemented now and in the future.
- Describe the importance of resiliency on the cyber systems that control the grid and, because my personal expertise is cyber,

- Make specific recommendations to enhance the resiliency of the cyber portion of the power grid to cyberattacks and, in turn, the grid itself, while stressing that resiliency to other impairments is also very important.

Before doing so, I will provide a brief overview of the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project which I led, and the Cyber-Resilient Energy Delivery Consortium (CREDC), which I currently co-lead.

TCIP/TCIPG and CREDC

I served as the Director and Principal Investigator (PI) of the DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center and currently serve as the co-PI of the Cyber-Resilient Energy Delivery Consortium (CREDC), which conducts research at the forefront of national efforts to make the U.S. power grid resilient.

The Trustworthy Cyber Infrastructure for the Power Grid (TCIP (2005-2010) and TCIPG (2009-2015) projects, a partnership of four academic institutions, were conducted to meet the challenge of making the electricity grid resilient. The TCIP Project was funded primarily by the National Science Foundation, with additional support by the Department of Energy's Office of Electricity Delivery and Energy Reliability, and by the Department of Homeland Security's Science and Technology Directorate, HSARPA, Cyber Security Division. The TCIPG project was funded by the Department of Energy's Office of Electricity Delivery and Energy Reliability with partial support from the Department of Homeland Security's Science and Technology Directorate, HSARPA, Cyber Security Division.

In these projects, we collaborated with national laboratories and the utility sector to protect the U.S. power grid by significantly improving the way the power grid infrastructure is designed, making it more secure, resilient, and safe. In both technology and impact, TCIP/TCIPG was a successful partnership of government, academia, and industry, creating multiple startup companies and transitioning multiple technologies to industry. The projects also had a significant positive impact on workforce education, delivering successful short courses, producing graduates, and providing the knowledge necessary to do interdisciplinary work of this type at other universities.

CREDC (funded by the Department of Energy Office of Electricity Delivery and Energy Reliability with support from the Department of Homeland Security's Science and Technology

Directorate, HSARPA, Cyber Security Division) is a partnership of 10 academic institutions and 2 national labs that performs research and development in support of the Energy Sector Control Systems Working Group's Roadmap of resilient Energy Delivery Systems (EDS) that focuses on the cybersecurity of EDS. In doing so, CREDC addresses the cybersecurity of power grids, as well as oil and gas refinery and pipeline operations. To do this, CREDC develops projects with significant and measurable sector impact, involving industry partners (asset owners, equipment vendors, and technology providers) early and often, with activities that range from helping to identify critical sector needs, to performing pilot deployment and technology adoption.

Resiliency

The subject of this hearing is "resiliency," which is a fundamental and different concept from other "-abilities," such as, for example, reliability or cybersecurity. The Random House Dictionary of the English Language defines resiliency as "the power or ability to return to the original form, position, etc. after being bent, compressed, or stretched . . . [the] ability to recover from illness, depression, adversity, or the like . . . [to] spring back, rebound." In the context of electric power, resiliency is not just about being able to lessen the likelihood that outages will occur, but also about managing and coping with outage events when they do occur. The goal is to lessen outage impacts, regrouping quickly and efficiently once an event ends, and in the process learning to better deal with other events in the future.

Flynn (2008) has outlined a four-stage framing of the concept of resilience: (1) preparing to make the system as robust as possible in the face of possible future stresses or attacks; (2) relying on resources to manage and ameliorate the consequences of an event once it has occurred; (3) recovering as quickly as possible once the event is over; and (4) remaining alert to insights and lessons that can be drawn (through all stages of the process) so that if and when another event occurs, a better job can be done on all stages. Our committee used that framing to organize our report.

A key insight about the concept of resiliency is that it attempts, to the greatest extent possible, to avoid the large-scale event (in this case a long-term blackout), but understands and admits that it may not be totally possible to avoid it, and thus works to respond as quickly as possible to the event once it occurs, preserving "critical" individual and societal services during

the period of degraded operation and, over time, strives for full recovery and enhanced robustness to further impairments that could result in additional large scale events.

Because the power system is hierarchical, these same concepts apply at several different levels of the system, including across the high-voltage grid, the regional grid (some of which are operated by regional transmission organizations), local transmission and distribution systems (typically the domain of utilities), and the end-use level (on both the utility and customer side of the meter) and across the cyber and physical portions of the power grid. It is also clear that the resiliency of the power grid is critically dependent other interconnected infrastructures (e.g, oil and gas).

National Academy Report Overview

In its 2014 appropriations for the Department of Energy, Congress requested that the National Academies of Sciences, Engineering, and Medicine organize a study to identify technologies, policies, and organizational strategies to increase the resilience and reliability of the U.S. electricity system. The study focused largely on reducing the nation's vulnerability to large-area long-duration outages — those that span several service areas or even states and last three days or longer. It found that much can be done to make both large and small outages less likely, but they cannot be totally eliminated no matter how much money or effort is invested. To increase the resilience of the grid, our report argues that the nation must not only work to prevent and minimize the size of outages, but must also develop strategies to cope with outages when they happen, recover rapidly afterward, and incorporate lessons learned into future planning and response efforts. The report also recognizes that, at least over the next two decades, most customers will continue to depend on the functioning of the large-scale, interconnected, tightly organized, and hierarchically structured electric grid for resilient electric service. Recent and ongoing events, such as the hurricanes in the Southeast and wildfires in the West, make the consideration of grid resilience even more timely.

The Chair of the study was M. Granger Morgan, Carnegie Mellon University, and the committee members were Dionysios Aliprantis, Purdue University; Anjan Bose, Washington State University; Terry Boston, PJM Interconnection (retired); Allison Clements, GoodGrid LLC; Jeffery Dagle, Pacific Northwest National Laboratory; Paul De Martini, Newport Consulting Group; Jeanne Fox, Columbia University; Elsa M. Garmire, Dartmouth College

(retired); Ronald E. Keys, United States Air Force (retired General); Mark F. McGranaghan, Electric Power Research Institute; Craig Miller, National Rural Electric Cooperative Association; Thomas J. Overbye, Texas A&M University; William H. Sanders, University Illinois at Urbana Champaign; Richard E. Schuler, Cornell University; Susan F. Tierney, Analysis Group; David G. Victor, University of California San Diego.

The report notes that when major electricity outages do occur, economic costs can tally in the billions of dollars and lives can be lost. It argues that resilience is not just about lessening the likelihood that these outages will occur. It is also about limiting the scope and impact of outages when they do occur, restoring power rapidly afterwards, and learning from these experiences to better deal with events in the future.

Large outages have happened in the past as a result of hurricanes, ice storms, and a variety of other causes. Even larger outages, extending across many states for periods of many days, are possible in the future. Chapter 3 of the report discusses over a dozen events that could cause widespread outages of long duration.

The central chapters of the report (Chapters 4, 5, & 6) are organized around three critical elements of building a secure power system:

1. Taking step to be better prepared, long before an outage occurs.
2. Taking steps to minimize the individual and social cost of a large-scale long-term outage.
3. Putting the system back together after an event and learning from the process so we are able to do a better job of making the system more resilient in the future.

Report Recommendations

In addition to many specific recommendations directed to particular organizations, the report makes seven overarching recommendations (see the report for a precise statement of each recommendation, and the report's recommendation on what organizations should be responsible for implementation):

1. Conduct more emergency preparedness exercises that include multisector coordination.
2. Rapidly implement resiliency-enhancing technical capabilities and operational strategies that are available today, and speed the adoption of new capabilities and strategies as they become available.

3. Sustain and expand the areas of research, development, and demonstration that are now being undertaken by the Department of Energy's Office of Electricity Delivery and Energy Reliability and Office of Energy Efficiency and Renewable Energy, with respect to grid modernization and systems integration, with the explicit intention of improving the resiliency of the U.S. power grid.
4. Through public and private means, substantially increase the nation's investment in the physical resources needed to ensure that critical electric infrastructure is robust and that society is able to cope when the grid fails.
5. Carry out a program of research, development, and demonstration activities to develop and deploy capabilities for the a) continuous collection of diverse (cyber and physical) sensor data; b) fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical); c) visualization techniques needed to allow operators and engineers to maintain situation awareness; d) analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments; e) restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and f) creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.
6. Establish and support a "visioning" process with the objective of systematically imagining and assessing plausible large-area long-duration grid disruptions that could have major economic, social, and other adverse consequences.
7. Establish small System Resilience groups, informed by the work of the Department of Energy/Department of Homeland Security "visioning" process, to assess and, as needed, to mandate strategies designed to increase the resilience of the U.S. bulk electricity system.

The joint and collaborative involvement of government, industry, and academia in implementing these recommendations is key to their success.

Cyber Resiliency

A relatively new concern, and the subject of my core expertise, is the resiliency of the cyber portion of the grid, and how it affects overall grid resiliency. The electric power system has become increasingly reliant on its cyber infrastructure, including computers, communication networks, other control system electronics, smart meters, and other distribution-side cyber assets, in order to achieve its purpose of delivering electricity to the consumer. A compromise of the power grid control system or other portions of the grid's cyber infrastructure can have serious consequences ranging from a simple disruption of service with no damage to the physical components to permanent damage to hardware that can have long-lasting effects on the performance of the system. Any consideration of improved power grid resiliency requires a consideration of improving the resiliency of the grid's cyber infrastructure.

Over the last decade much attention has rightly been placed on grid cybersecurity, but much less has been placed on grid cyber resiliency. The sources of guidance on protection as a mechanism to achieve grid cyber security are numerous, and documented in the report. It is now, however, becoming apparent that protection alone is not sufficient, and can never be made perfect. Cybercriminals are difficult to apprehend, and there are nearly 81,000 vulnerabilities in the NIST National Vulnerability Database making it challenging to use safe code (NVD, 2016). An experiment conducted by the National Rural Electric Cooperative Association and N-Dimension in April 2014 determined that a typical small utility is probed or attacked every 3 seconds around the clock. Given the relentless attacks and the challenges of prevention, successful cyber penetrations are inevitable, and there is evidence of increases in the rate of penetration in the past year.

Fortunately, the successful attacks to date have largely been concentrated on utility business systems as opposed to monitoring and control systems (termed operational technology or OT systems), in part because there are fewer attack surfaces, fewer users with more limited privileges, greater use of encryption, and more use of analog technology. However, there is a substantial and growing risk of a successful breach of operational technology systems, and the potential impacts of such a breach could be significant. These risks are growing partially because, as the grid is modernized, there is greater reliance on grid components with significant cyber controls. Serious risks are posed by further integration of operational technology systems with utility business systems, despite the potential for significant value and increased efficiency.

Given that protection cannot be made perfect, and the risk is growing, cyber resiliency, in addition to more classical cyber protection approaches, is critically important. Cyber resiliency aims to protect using established cybersecurity techniques, but acknowledges that such protections can never be perfect, and requires monitoring, detection, and response to provide continuous delivery of electrical service. While some work done under the cybersecurity nomenclature can support cyber resiliency (e.g. intrusion detection and response), the majority of the work to date has been focused on preventing the occurrence of successful attacks, rather than detecting and responding to partially successful attacks that occur.

A cyber resiliency architecture should implement a strategy for mitigating cyberattacks and other impairments by monitoring the system and dynamically responding to perceived impairments to achieve resiliency goals. The resiliency goals for the cyber infrastructure require a clear understanding of the interaction between the cyber and physical portions of the power grid, and how impairments on either (cyber or physical) side could impact the other side. By their nature, such goals are inherently system-specific, but should balance the desire to minimize the amount of time a system is compromised and maximize the services provided by the system. Often, instead of taking the system offline once an attack is detected, a cyber resiliency architecture attempts to heal the system while providing critical cyber and physical services. Based on the resiliency goals, cyber resiliency architectures typically employ sensors to monitor the state of the system on all levels of abstraction and detect abnormal behaviors. The data from multiple levels are then fused to create higher-level views of the system. Those views aid in detecting attacks and other cyber and physical impairments, and in identifying failure to deliver critical services. A response engine, often with human input, recommends the best course of action. The goal, after perhaps multiple responses, is complete recovery, i.e., restoring the cyber system to a fully operational state.

Further work is critically needed to define cyber resiliency architectures that protect against, detect, respond, and recover from cyber attacks that occur.

Achieving Cyber Resiliency

In addition to overarching recommendation number 5, the report makes a specific recommendation regarding cyber resiliency. Specifically, it states that:

"The Department of Energy should embark upon a research, development and demonstration program that makes use of the diverse expertise of industry, academia, and national labs that results in a prototypical cyber-physical-social control system architecture for resilient electric power systems. The program would have the following components: 1) A diverse set of sensors (spanning the physical, cyber, and social domains), 2) a method to fuse this sensor data together to provide situational awareness of known high quality, and 3) an ability to generate real-time command and control recommendations for adaptations that should be taken to maintain the resiliency of an electric power system."

Physical Resilience is Equally Important

Because my personal expertise lies in the area of information, communication, and control technologies I have elaborated on cyber resilience. However, in closing I should stress that Chapter 3 of our report identifies and discusses over a dozen events such as hurricanes, earthquakes, tsunamis, ice storms, terrorist attacks, and large solar storms, that could cause wide *physical* damage to the power system that could result in large outages. Putting the system back together after one of these extreme events could require many days or even weeks.

Summary

The title of this hearing "Resiliency: The Electric Grid's Only Hope" is apt. Unlike some, I don't believe "the sky is falling" or that we are on the brink of a major disaster. However, the threat to grid resiliency is real, and the time to act is now, so we don't reach that brink. To summarize the points that I made in this testimony:

1) Grid resiliency is different than grid reliability, and requires a fundamentally new approach.
2) Grid resiliency attempts, to the greatest extent possible, to avoid long-term blackouts, but understands and admits that it may not be totally possible to avoid them, and thus works to respond as quickly as possible to the event once it occurs, preserving "critical" services during the period of degraded operation and, over time, strives for full recovery and enhanced robustness.
3) Efforts with appropriate funding must be put in place for:
    a) Emergency preparedness exercises that include multisector coordination,
    b) Implementing available technologies and best practices,

c) Supporting DOE research in grid resiliency,
d) Creating a stockpile of physical components that enhance resiliency,
e) Developing means for cyber resilience,
f) Continuous envisioning of possible impairments which could lead to large-scale grid failures, and
g) Ongoing efforts to assess and, as needed, to mandate strategies designed to increase the resilience of the electricity system.

4) The grid can only be resilient if its cyber infrastructure is resilient, so research and development are critically needed that provides assured mechanisms to ensure cyber resiliency.

Thank you for the opportunity to be here with you today. I would be happy to answer any questions that you have.

William H. Sanders Biography

William H. Sanders is a Donald Biggar Willett Professor of Engineering and the Head of the Department of Electrical and Computer Engineering (www.ece.illinois.edu) at the University of Illinois at Urbana-Champaign (illinois.edu). He is a professor in the Department of Electrical and Computer Engineering and in the Department of Computer Science. He is a fellow of the IEEE, the ACM, and the AAAS; a past chair of the IEEE Technical Committee on Fault-Tolerant Computing; and past vice-chair of the IFIP Working Group 10.4 on Dependable Computing. He was the founding director of the Information Trust Institute (www.iti.illinois.edu) at Illinois (2004-2011), and served as director of the Coordinated Science Laboratory (www.csl.illinois.edu) at Illinois from 2010 to 2014.

Dr. Sanders's research interests include secure and dependable computing and security and dependability metrics and evaluation, with a focus on critical infrastructures. He has published more than 270 technical papers in those areas. He served as the director and PI of the DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center (tcipg.org), which did research at the forefront of national efforts to make the U.S. power grid smart and resilient. He was the 2016 recipient of the IEEE Technical Field Award, Innovation in Societal Infrastructure, for "assessment-driven design of trustworthy cyber infrastructures for societal-scale systems."