NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Considerations from the Integration of Smart Grid

to ensure the reliability of the bulk power system

December 2010

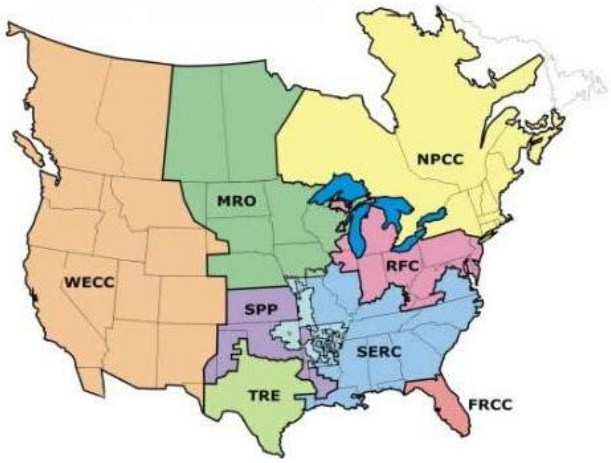
116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

(This page intentionally left blank)

NERC's Mission

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to evaluate reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; assesses adequacy annually via a ten-year forecast and winter and summer forecasts; monitors the bulk power system; and educates, trains, and certifies industry personnel. NERC is the electric reliability organization in North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.[1]

NERC assesses and reports on the reliability and adequacy of the North American bulk power system, which is divided into eight Regional Areas as shown on the map below (see Table A). The users, owners, and operators of the bulk power system within these areas account for virtually all the electricity supplied in the U.S., Canada, and a portion of Baja California Norte, México.



Note: *The highlighted area between SPP and SERC denotes overlapping Regional area boundaries: For example, some load-serving entities participate in one Region and their associated transmission owners and operators in another.*

Table A: NERC Regional Entities

FRCC Florida Reliability Coordinating Council	**SERC** SERC Reliability Corporation
MRO Midwest Reliability Organization	**SPP** Southwest Power Pool, Incorporated
NPCC Northeast Power Coordinating Council	**TRE** Texas Reliability Entity
RFC Reliability*First* Corporation	**WECC** Western Electricity Coordinating Council

[1] As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the BPS, and made compliance with those standards mandatory and enforceable. In Canada, NERC presently has memorandums of understanding in place with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, and Saskatchewan, and with the Canadian National Energy Board. NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. NERC has an agreement with Manitoba Hydro, making reliability standards mandatory for that entity, and Manitoba has recently adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the "electric reliability organization" under Alberta's Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and NPCC have been recognized as standards-setting bodies by the *Régie de l'énergie* of Québec, and Québec has the framework in place for reliability standards to become mandatory. Nova Scotia and British Columbia also have a framework in place for reliability standards to become mandatory and enforceable. NERC is working with the other governmental authorities in Canada to achieve equivalent recognition.

Table of Contents

NERC's Mission i

Executive Summary I

1. Introduction 1

Overview 1

The Grid Today 2

Defining and Envisioning the Smart Grid 3

Organization of this Report 5

2. Legislative and Regulatory Summary 6

Introduction 6

U.S. Legislative and Regulatory Summary 6

Canadian Legislative and Regulatory Summary 10

Chapter Findings 11

3. Characteristics and Technology Assessment 12

Introduction 12

Smart Grid Characteristics 12
Integration of Smart Grid Technology into the Bulk Power System 12
Reliability Considerations of Information Technology and Control System Integration 13

Technology Assessment 15

Smart Grid Technologies (Devices and Systems) on the Bulk Power System 15
Bulk Power System — Existing Devices 16
Bulk Power System — Developing Devices 25
Bulk Power System — Existing Systems 28
Bulk Power System — Developing Systems 31

Smart Grid Technologies on the Distribution System 32
Distribution System — Existing Devices 32
Distribution System — Existing Systems 34
Distribution System — Developing Devices 37
Distribution System — Developing Systems 39

Chapter Findings 42

4. Planning and Operations with Smart Grid 44

Introduction 44
Bulk Power System Reliability Risks 44
Planning for Smart Grid Uncertainty: Example from Southern California Edison 46
Planning and Operations Horizons 48

Long-Term Planning — Power System Considerations *49*
Advancing System Optimization and Efficiency 49
Effects of New Technology 49
Modeling and Simulation Requirements 50
New Reliability Tools 51
Developing Appropriate Performance Metrics 52
Distributed Resources, Microgrids, and Integrating Renewable Resources 53
Control System Architecture 54
Instrumentation, Control, and Protection Systems Impacts 55
Power Quality 58

Operations Planning *60*
Maintenance 60
System Efficiency 60

Same-day Operations *61*
Modes of Operation and System Modeling 61
Demand Response 61
Distributed Resources 63

Real-time Operations *63*
Failures 63
Operational Risks 63

Operations Assessment *65*
New System Performance Metrics Needs 65

Other Considerations *65*
Changing Organizational View 65
Life Expectancy Issues 66
Business Continuity 66
Evolutionary Implementation 66

R&D Requirements *66*

Chapter Findings *68*

5. Cyber Security for the Smart Grid 69

Introduction *69*

Loss of Control Center Systems *72*
Communications Systems 72
Command and Control Architecture 74
The Importance of Real-time Centralized Monitoring 74

Security Defense-in-Depth Model *78*

Risk Management *81*

Need for Robust and Adaptive Certification Process *82*

Coordination of Standards and Process Evolution *82*

Increasing Complexity of Asset Governance *84*

Balancing Internal and External Sources of System Risk *85*
The Use of Standardized Risk Identification for Smart Grid Integration 86
Unknown Risks in the Evolving Smart Grid 86

Other Considerations *89*
Physical Security of Assets Outside the Control Center 89
Continuity and Disaster Planning 91

R&D Requirements *92*
Cyber security 92
Cloud Computing 93
Computational Capabilities 94

Chapter Findings *95*

6.0 Conclusions and Recommendations 96

Appendix 1: Smart Grid and Reliability Standards 97

NERC Reliability Standards and Smart Grid *97*

Bulk Power System Reliability *97*

Smart Grid Options and NERC Standards *98*

Appendix 2: Follow-on Work Plan 104

Appendix 3: International Smart Grid Developments 106

Australia *106*

Germany *107*

South Korea *109*

Abbreviations 110

Glossary 114

Smart Grid Task Force Roster 118

NERC Staff Roster 127

Executive Summary

Governments, regulators, and industry organizations have proposed the "smart grid" to enhance consumer options, support climate change initiatives, and enhance the reliability of the North American bulk power system. The evolving integration of smart grid will require significant changes in bulk power system planning, design, and operations. This report defines smart grid, incorporating reliability of the bulk power system, and provides a preliminary assessment of successful smart grid integration.

The North American bulk power system is the largest interconnected electric system in the world. Its reliable operation depends on extensive application of real-time communications, monitoring, and control systems. As part of bulk power system's evolution, many "smart" technologies have been in operation for decades.

Recent federal, provincial, and state policy initiatives promote a vision of a smart grid that is more interactive and interoperable, efficient, reliable, and robust. At its foundation, smart grid characteristics include interoperable equipment enabled by advances in communications, intelligent systems, and information technology (IT) interfacing with existing and new control systems. Consistent, interoperable bulk system-wide communication protocols are meant to support a more dynamic system providing benefits to end-users, efficient use of transmission and improved overall system reliability with easy-to-deploy sensing and diagnostics. With advances in smart grid technology, unprecedented evolution to levels of system control and measurement are on the horizon. A number of ongoing efforts have proceeded over the past decade to promote and develop this smart grid infrastructure, each with its own focus and stakeholder engagement.

Today's bulk power system is planned and operated to provide an "adequate level of reliability." Smart grid can support and maintain an adequate level of reliability, even as the wider industry is challenged to meet broad policy and legislative directives that are affecting and changing the attributes of the U.S. bulk power system. The success of integrating smart grid concepts and technology will rely heavily on reliability of the existing bulk power system during its evolution. This report stands to shed light on various aspects of this fundamental concern.

The full impact of smart grid on the reliability of the bulk power system has yet to be seen. While the promise of smart grid is, in part, to enhance reliability, if it is poorly deployed the reliability of the bulk power system could suffer. Therefore, it is vitally important to ensure the evolution of smart grid does not increase the bulk power system's vulnerability, but rather supports industry's bulk power system reliability goals.

To investigate implications from smart grid devices systems to enable successful integration, the NERC Planning Committee formed the Smart Grid Task Force (SGTF). The SGTF charter is to *"identify and explain any issues and/or concerns of the smart grid with respect to bulk power system reliability"* and to *"assess smart grid reliability characteristics and how they may affect bulk power system planning, design and operational processes and the tools that may be needed to maintain reliability."*

The task force developed and agreed upon the following industry definition of the smart grid:

smart grid — The integration and application of real-time monitoring, advanced sensing, communications, analytics, and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure, reliable, and efficient electric power system, from generation source to end-user.

Based on this preliminary assessment, successful integration of smart grid can ensure reliability of the bulk power system. The following are key observations:

Government initiatives and regulations promoting smart grid development and integration must consider bulk power system reliability

The evolution of the smart grid is being accelerated by substantial legislative and regulatory initiatives throughout North America. Successful large-scale introduction of smart grid technologies will both deliver the potential benefits and maintain the reliability of the bulk power system. It will be important to consider how best to plan, design, and operate the system to successfully integrate smart grid devices/systems in all the various planning timeframes. To achieve this goal, sufficient time is required for industry to develop the experience with the smart grid and ensure the bulk power system is planned and designed to support reliable operation.

Integration of smart grid requires development of new tools and analysis techniques to support planning and operations

New tools and analysis techniques will be required to plan and operate the deployment of broad-scale smart control systems across the bulk power system. As the bulk power system is a large non-linear system using large amounts of inertia to create electricity, the ramifications and design of smart grid on control systems must be modeled, simulated, and designed to ensure that the expected performance improvements will be realized. Successful integration of smart grid devices and systems should address potential reliability considerations such as transient and long-term stability, small signal stability, voltage stability, intentional cyber attack or unintentional IT/communication errors, and component design issues such as short circuit considerations. In addition, operators of the smart grid will require improved models for identifying failure impacts based on a larger number of operating states and topologies.

Smart grid technologies will change the character of the distribution system, and they must be incorporated into bulk power system planning and operations

Integrating smart grid devices and systems on the distribution system can change its static and dynamic characteristics. Successful integration of smart grid systems/devices should consider and address bulk power system reliability considerations resulting from these changes. Further, bulk power system operators will need increased visibility and dispatchability as smart grid innovations change the character of distribution systems

Cyber security and control systems require enhancement to ensure reliability

The strength of the interoperability design of smart grids, unless carefully planned and operated, can provide a vehicle for intentional cyber attack or unintentional errors impacting bulk power system reliability through a variety of entrance and exit points. Many of the systems implemented using existing smart grid technologies are designed for control functionality and are not responsive to errors resulting from misuse, miscommunications, or information technology (IT) system failures. Security of these control systems can be intentionally defeated or unintentionally corrupted by the installation of software updates, etc. Improvements will be required to provide robust protection from IT and communication system vulnerabilities. "Defense-in-Depth" approaches, when coupled with risk assessment, can provide an overarching organizational approach to cyber security management. Use of risk assessment can help determine appropriate defensive measures.

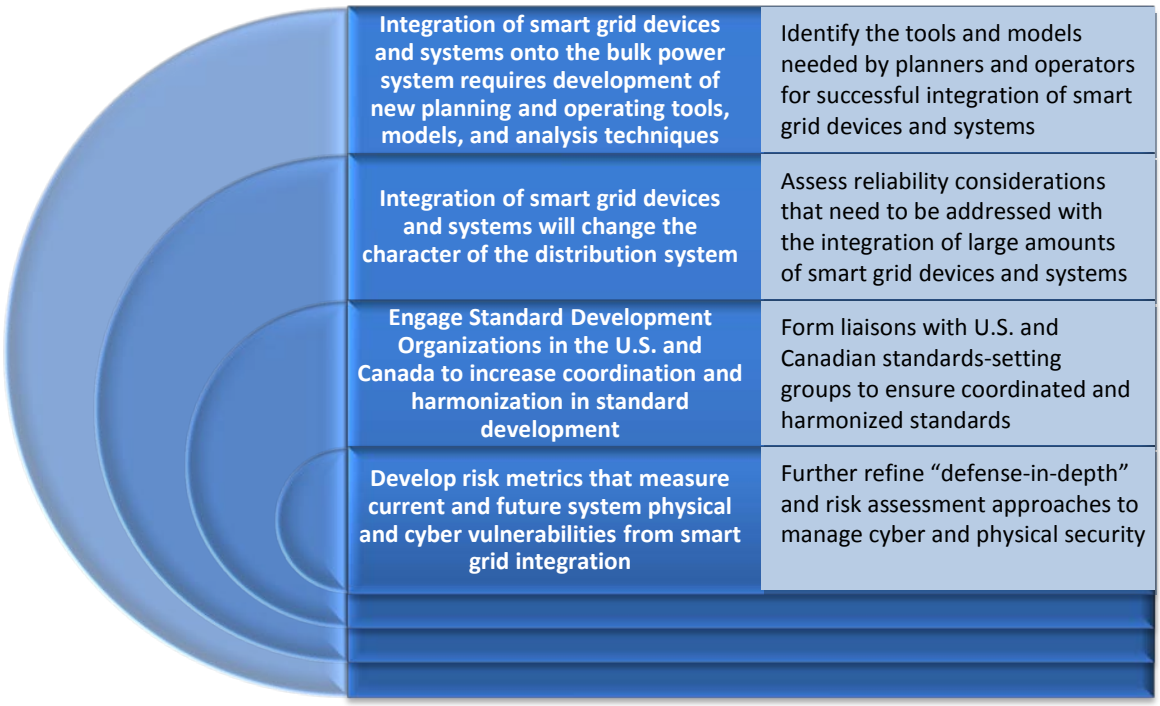
In addition, standard harmonization between North American Standard Development Organizations in Canada and the U.S. is important for the successful deployment of smart grid devices/systems, while addressing potential cyber vulnerabilities.

Research and development (R&D) has a vital role in successful smart grid integration

Given that the complex modeling, analysis, decision making, cyber/control system security challenges, and design of complex systems driven by highly variable inputs, close industry collaboration with government, R&D organizations, and universities is needed to develop future models, build simulators and create test systems to identify and resolve potential challenges. Therefore, R&D is an important ingredient in the evolution to the smart grid and is needed to harvest the benefits from integration of smart grid devices and systems while maintaining reliability of the bulk power system.

Recommendations

This preliminary assessment concludes that successful integration of smart grid devices and systems can improve bulk electric system reliability. Their integration may result in substantial changes to the bulk power system, along with the operators requiring more visibility and dispatchability of resources on the distribution systems. As it evolves, the bulk power system must remain reliability. To address these issues, the task force developed a work plan defining next steps for the successful integration of smart grid devices and systems:



In addition, NERC should:

1. Introduction

Overview

There is an unprecedented level of overlapping and coincident changes across the U.S. electrical power system, involving the integration of variable generation, increasing cyber security concerns, reactive power issues, and many other emerging issues.[2] It is an industry in transition. At the heart is the bulk power system, the core system that ties all of the actors and stakeholder parties together. Coordination among these parties at the bulk power system-level is essential to achieve renewable integration, smart grid implementation, enhanced end-user participation, and other objectives while ensuring the lights stay on. Despite emerging issues, credible contingencies, and the technological evolution of the entire system, the bulk power system must remain reliable. As such, the stakeholders who are directly responsible for the bulk power system have a responsibility to ensure reliability.[3] As part of its evolution, many "smart" technologies have been in operation for many decades.

Many smart technologies use localized control and interconnection, and coordination with other controls systems has been conventionally deployed with protocols that were proprietary. A basic tenet of the smart grid is to enable device interoperability and two-way flow of communications and energy enabled by advances in communications, intelligent systems, and information technologies. Recent federal, provincial, and state policy initiatives promote a vision of a smart grid that is "much more interactive and interoperable, reliable and robust."[4] While these words could be interpreted differently, this vision of the smart grid does address several objectives:

- reduce electric sector greenhouse gas emissions;
- enable consumers to better manage and control their energy use and costs;
- improve energy efficiency, demand response, and conservation measures;
- interconnect renewable energy resources;
- improve bulk power and distribution system reliability;
- manage energy security; and
- provide a platform for innovation and job creation.

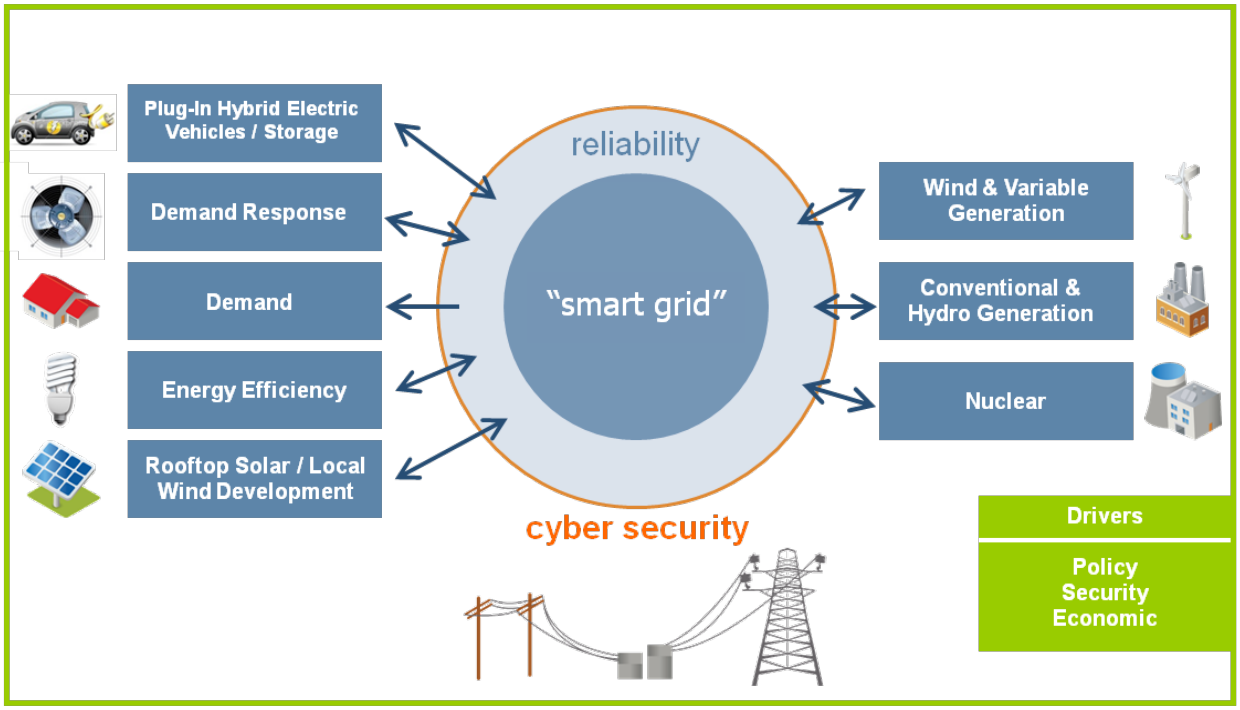
At its foundation, smart grid characteristics include interoperable equipment enabled by advances in communications, intelligent systems, and information technology (IT) interfacing with existing and new control systems. Consistent, interoperable bulk system-wide communication protocols are meant to support a more dynamic system providing benefits to end-users and overall system reliability with easy-to-deploy sensing and diagnostics. There have been

[2] For more information on these and other issues, review the Emerging and Standing Issues section of the *2009 Long-Term Reliability Assessment*: http://www.nerc.com/files/2009_LTRA.pdf
[3] See *Appendix 1: Smart Grid and Reliability Standards* for a definition of bulk power system reliability.
[4] IEEE Spectrum blog: http://spectrum.ieee.org/energywise/energy/the-smarter-grid/smart-grid-proof

a number of ongoing efforts over the past decade to develop this smart grid infrastructure, each with its own focus and stakeholder engagement.[5]

The term "smart grid" represents the force of new public policy ideas by promoting the expanded use of new technologies deploying advanced communications to improve the management, monitoring, and use of electricity. Many of these smart grid policies are targeted to enhance consumer services, with technology integration occurring on distribution systems of the electric power system, or even inside the customers' facilities. That said, smart grid devices and systems also integrate directly with the bulk power system having a bearing on its reliability (Figure 1).

Figure 1: Emergence of the 21st Century Grid



The Grid Today

Today's bulk power system is planned and operated to provide an "adequate level of reliability." Smart grid can support and maintain this adequate level of reliability, even as the wider industry is challenged to meet broad policy and legislative directives that are affecting and changing the attributes of the North American bulk power system.[6] The success of integrating smart grid concepts and technology will rely heavily on reliability of the bulk power system during its evolution.

[5] EPRI Report, "*Profiling and Mapping of Intelligent Grid R&D Programs,*" December 2006, Report 1014600

[6] See NERC's *Reliability Impacts of Climate Change Initiatives* at http://www.nerc.com/filez/riccitf.html and final report at http://www.nerc.com/files/RICCI_2010.pdf

To investigate implications from smart grid devices and systems to enable successful integration, the NERC Planning Committee formed the Smart Grid Task Force (SGTF).[7] The SGTF was charged to *"identify and explain any issues and/or concerns of the smart grid with respect to bulk power system reliability"* and to *"assess smart grid reliability characteristics and how they may affect bulk power system planning, design, and operational processes and the tools that may be needed to maintain reliability."*

Thus, the SGTF focused its investigation on the infrastructure associated with implementing smart grid and its successful integration on the bulk power system while addressing any impacts on reliability. This focus covers existing and new smart technologies, smart grid communication and control systems, smart grid options to meet NERC Reliability Standards (Appendix 1), and evolutions of legacy technologies. A work plan was developed (Appendix 2) defining additional activities to support successful integration of smart grid devices and systems. Finally, international activities on smart grid integration were evaluated (Appendix 3).

Defining and Envisioning the Smart Grid

The smart grid encompasses legacy and developing technologies. The development of an agreed-upon industry definition of the smart grid was an important step for this and future activities (see *Glossary* for a detailed explanation of the word choice for this definition).

smart grid — The integration and application of real-time monitoring, advanced sensing, communications, analytics, and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure, reliable, and efficient electric power system, from generation source to end-user.

Figure 2 illustrates the connectivity of many of these technologies with an overlay (colored clouds) of communications networks.[8] The status of smart grid integration may be summarized as follows:

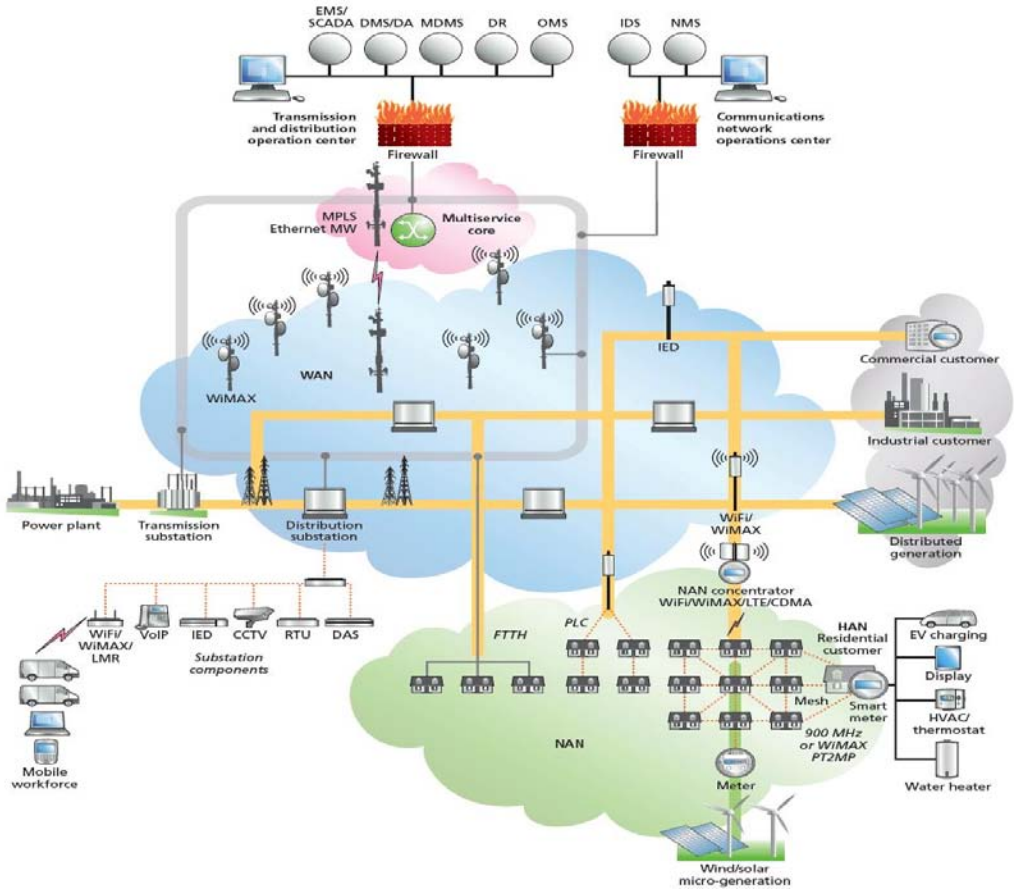
- There are no assumed immediate or dramatic changes in the way the bulk power system currently operates or is organized; integration will be an evolutionary process.
- Widespread smart grid implementation still lags the vision and policy debates, so the ultimate impact on the bulk power system is uncertain.
- The smart grid interoperability standards development currently coordinated by the National Institute of Standards and Technology (NIST) is a separate function and not directly related to the NERC bulk power system Reliability Standards[9] referenced in this report. NIST has identified standards for the smart grid and will be providing narrative summaries of the standards to support FERC and other regulators in their rulemakings. These summaries will address what is and is not covered in the particular standards,

[7] http://www.nerc.com/filez/sgtf.html
[8] Smart Choices for the Smart Grid by Alcatel-Lucent: http://www.alcatel-lucentbusinessportal.com/private/active_docs/1001_Smart%20Choices%20for%20the%20Smart%20Grid.pdf
[9] http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf

including equipment and systems, and how well cyber security is addressed, and will list FERC-approved reliability standards that may potentially be affected by the standards. These narratives will be posted in the near future on the Smart Grid Interoperability Panel (SGIP) Interoperability Knowledge Base (IKB) website.[10]

Smart grid technologies and systems are both bulk power system- and distribution-based. Their integration should also address the changes in the static and dynamic character of distribution systems.

Figure 2: The intersection of communications networks and electricity grids[11]



[10] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/InteroperabilityKnowledgeBase

[11] Source: Alcatel-Lucent, 2010: http://www.alcatel-lucentbusinessportal.com/private/active_docs/1001_Smart%20Choices%20for%20the%20Smart%20Grid.pdf

NERC develops, implements, and enforces mandatory Reliability Standards[12] for the bulk power system. NERC-enforced Reliability Standards are designed to ensure the reliability of the bulk power system and typically apply to facilities at the transmission and generation level. This includes the development of Reliability Standards designed to ensure the protection of cyber assets that are part of the bulk power system.

The advent of smart grid devices and systems can provide new options and additional ways to meet NERC's Reliability Standards. This can be done through the introduction of new and evolving concepts, devices, applications, data, and communications. As the smart grid crystallizes over time, industry may need to provide input into NERC's Reliability Standards process to either increase reliability requirements or enhance existing requirements. Appendix 1 provides insights on how smart grid devices and systems provide options to meet NERC Reliability Standards.

Organization of this Report

This report is organized into five additional chapters: Legislative and Regulatory Summary, Characteristics and Technology Assessment, Planning and Operations with Smart Grid, Cyber Security and Critical Infrastructure Protection, and Conclusions and Recommendations. Three Appendices are also included: comparison of smart grid options and NERC Reliability Standards, work plan definition, and international developments.

[12] http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf

2. Legislative and Regulatory Summary

Introduction

A key driver of smart grid development and integration has been recent federal, state, and provincial government action and incentives. This chapter provides a non-exhaustive review of these activities, through samples of North American legislation and regulations.

U.S. Legislative and Regulatory Summary

Federal and state policies have helped to shape the public's understanding of smart grid considerably in recent years. These policies continue to evolve, but are very informative in their current state. A few examples selected from the legislative and regulatory arenas are summarized and presented below to identify some specific tenets of smart grid as currently envisioned in public policy.

1. U.S. Congress
   Energy Independence and Security Act of 2007 (EISA)[13]
   The goal of EISA is for the United States to have greater energy independence and security; increase the production of clean renewable fuels; protect consumers; increase the efficiency of products, buildings, and vehicles; promote research on and deploy greenhouse gas capture and storage options; improve the energy performance of the federal government; and for other purposes. From the Act, the term "Smart Grid Functions" means any of the following (Section 1306(d)):

   i. 1306.(d).1 — The ability to develop, store, send, and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations, to or from or by means of the electric utility system, through one or a combination of devices and technologies.

   ii. 1306.(d).2 — The ability to develop, store, send, and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations to or from a computer or other control device.

   iii. 1306.(d).3 — The ability to measure or monitor electricity use as a function of time of day; power quality characteristics such as voltage level, current, cycles per second, or source or type of generation; and to store, synthesize, or report that information by digital means.

[13] http://energy.senate.gov/public/_files/getdoc1.pdf

iv. 1306.(d).4 — The ability to sense and localize disruptions or changes in power flows on the grid and communicate such information instantaneously and automatically for purposes of enabling automatic protective responses to sustain reliability and security of grid operations.

v. 1306.(d).5 — The ability to detect, prevent, communicate with regard to, respond to, or recover from system security threats, including cyber security threats and terrorism, using digital information, media, and devices.

vi. 1306.(d).6 — The ability of any appliance or machine to respond to such signals, measurements, or communications automatically or in a manner programmed by its owner or operator without independent human intervention.

vii. 1306.(d).7 — The ability to use digital information to operate functionalities on the electric utility grid that were previously electro-mechanical or manual.

viii. 1306.(d).8 — The ability to use digital controls to manage and modify electricity demand, enable congestion management, assist in voltage control, provide operating reserves, and provide frequency regulation.

2. U.S. Federal Energy Regulatory Commission (FERC)
Smart Grid Policy,[14] July 2009

This FERC Policy Statement provides guidance regarding the development of a smart grid for the nation's electric transmission system, focusing on the development of key standards to achieve interoperability and functionality of smart grid systems and devices. In this Policy Statement, the Commission provides additional guidance on standards to help to realize a smart grid. The Policy Statement identifies Crosscutting Issues and Priority Applications.

i. Cross-cutting Issues
   a. Cyber security
   b. Common semantic frameworks and software models needed to enable effective communication and coordination across inter-system interfaces

ii. Priority Applications
   a. Wide-area situational awareness
   b. Demand response
   c. Electric storage
   d. Electric transportation

[14] http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf

3. U.S. Department of Energy (DOE):

DOE *Smart Grid System Report – Characteristics of the Smart Grid*, July 2009[15]

Section 1302 of Title XIII of the EISA directs the Secretary of Energy to *"…report to Congress concerning the status of smart grid deployments nationwide and any regulatory or government barriers to continued deployment."* The *Smart Grid System Report* satisfies this directive and represents the first installment of this report to Congress, which is to be updated biennially. The report indicates that the state of smart grid deployment covers a broad array of electric system capabilities and services enabled through pervasive communications and information technology, with the objective to improve reliability, operating efficiency, resiliency to threats, and impact to the environment. By collecting information from a workshop, interviews, and research of existing smart grid literature and studies, the report presents a view of progress toward a smart grid across many fronts. While Section 1301 of the EISA legislation identifies characteristics of a smart grid (see above), the National Energy Technology Laboratory (NETL) Modern Grid Initiative[16] provides a list of smart-grid attributes in "*Characteristics of the Modern Grid*" from a Department of Energy-sponsored workshop on "Implementing the Smart Grid" and formulates the basis for the *Smart Grid System Report.* The characteristics[17] are:

a. enabling informed participation by customers;
b. accommodating all generation and storage options;
c. enabling new products, services, and markets;
d. providing the power quality for the range of needs;
e. optimizing asset utilization and operating efficiently; and
f. operating resiliently: disturbances, attacks, and natural disasters.

4. U.S. Federal Communications Commission (FCC):

National Broadband Plan (NBP)[18]

In early 2009, the U.S. Congress directed the FCC to develop a NBP to ensure every American has "access to broadband capability." Congress also required that this plan include a detailed strategy for achieving affordability and maximizing use of broadband to advance "consumer welfare, civic participation, public safety and homeland security, community development, health care delivery, energy independence and efficiency, education, employee training, private sector investment, entrepreneurial activity, job creation and economic growth, and other national purposes." The plan notes: "A

[15] http://www.oe.energy.gov/SGSRMain_090707_lowres.pdf The NETL Modern Grid Initiative provides a list of smart grid attributes in "Characteristics of the Modern Grid" (NETL 2008). These characteristics were used to help organize a Department of Energy-sponsored workshop on "Implementing the Smart Grid." The results of that workshop are used to organize the reporting of smart grid progress around six characteristics. The sixth characteristic is a merger of the Modern Grid Initiative's characteristics: a) self-heals and b) resists attack.

[16] http://www.netl.doe.gov/smartgrid/

[17] The sixth characteristic is a merger of the Modern Grid Initiative's characteristics: a) self-heals and b) resists attack. The same metrics substantially contribute to both of these concerns.

[18] http://www.broadband.gov/

broadband-enabled smart grid could increase energy independence and efficiency, but much of the data required to capture these benefits are inaccessible to consumers, businesses and entrepreneurs." A summary of some key elements of the NBP is provided below.

a. On March 16, 2010, the FCC released and sent to Congress its NBP. The NBP was developed at the direction of Congress pursuant to the American Recovery and Reinvestment Act of 2009 (ARRA). While not legally binding, the 360-page NBP contains a number of recommendations and goals for action by the FCC, the Congress, other federal agencies and the states designed to ensure that every American has access to broadband capability, as well as to, among other things, advance energy independence and security.

b. Although issues of serious consequence to electric utilities are discussed in almost every chapter of the NBP, Chapter 6, "Infrastructure," specifically addresses pole attachment pricing and procedures, while Chapter 12, "Energy and the Environment," specifically addresses a variety of smart grid issues. Of further note is the fact that, from page 1 of the NBP on, the FCC constantly cites the benefits derived from the 1930's electrification of America as the theoretical justification for many of its broadband deployment proposals.

c. Smart grid as "*The electric delivery network, from electrical generation to end-use customer, integrated with sensors, software, and two-way communication technologies to improve grid reliability, security, and efficiency.*"

5. Summary of U.S. State Legislation:

a. At least 10 U.S. states[19] have enacted laws that seek to advance smart grid development and that directly mention smart grid or component technologies such as advanced metering infrastructure (AMI).

b. Many of these provisions are in the context of measures encouraging or requiring reductions in energy demand. In addition, West Virginia has put in place—with federal, state, utility, and other private support—a statewide smart grid implementation plan.

c. Numerous other states have enacted laws addressing energy efficiency, conservation, and demand response and management, all of which serve as pieces of any comprehensive approach to achieving smart grid deployments.

d. However, states to date generally have shied away from sweeping legislative action on the smart grid, including measures addressing standards, as they await developments in federal policymaking. Lawmakers also are keeping a close eye on costs and potential bill impacts—and related consumer backlash—as their states continue to emerge from the effects of the recession.

e. Instead, state smart grid laws generally call on regulators and/or utilities to come up with smart grid strategy plans, study the cost-effectiveness of technology,

[19] Includes: California, Connecticut, Illinois, Maine, Maryland, Massachusetts, Ohio, Pennsylvania, Texas, and Vermont

and/or include consideration of smart grid measures in achieving required reductions in energy demand. A few have included more teeth, e.g., Maryland allows the state commission to mandate smart grid implementation, and Pennsylvania in 2008 specified all customers must have smart meters within 15 years.

f. California lawmakers now are debating a measure suggesting that meter data collected by a utility is the property of the customer, and requiring state regulators to ensure that each smart grid deployment plan include testing and technology standards and that metering technology work properly in a field test. The outlook for the bill is uncertain. Beyond specific smart metering and smart grid policy, passed legislation such as California's 33 percent renewable portfolio standard is driving utility action to improve the instrumentation, analysis, and control of the grid. Numerous states are also providing wind and solar tax credits, driving up the levels of non-hydro renewables from modest levels to levels where action by ISO and RTOs and utilities is mandatory simply to maintain the reliability of the grid.

Canadian Legislative and Regulatory Summary

The Canadian Constitution, Section 92A, gives provincial legislatures jurisdiction over the "*development, conservation and management of sites and facilities in the province for the generation and production of electrical energy.*"[20] This has empowered each province to develop an electricity system best suited to its natural resource base and population distribution. Alberta, for example, has a mandatory power pool for generators and open access for retailers, while British Columbia features wholesale and industrial open-access, but a single independent transmission entity. Ontario unbundled its electricity markets in 1998 and has had wholesale and retail open access since 2002, while Québec features open-access transmission and wholesale competition for any provincial load greater than 165 TWh. The generation mix used in each province is similarly diverse, with large-scale hydro, thermal, and nuclear generation featured prominently.

The Ontario Energy Board Act of 1998 identified the utilities commission's mandate[21] in traditional language:

Board objectives, electricity

- The Board, in carrying out its responsibilities under this or any other Act in relation to electricity, shall be guided by the following objectives:
  - "*To protect the interests of consumers with respect to prices and the adequacy, reliability and quality of electricity service*"; and
  - "*To promote economic efficiency and cost effectiveness in the generation, transmission, distribution, sale, and demand management of electricity and to facilitate the maintenance of a financially viable electricity industry.*"

[20] http://laws.justice.gc.ca/en/const/3.html#anchorbo-ga:s_91
[21] http://www.ene.gov.on.ca/publications/6874e.pdf

The Green Energy and Green Economy Act of 2009, however, amended this Act to include the following paragraphs:[22]

- *"To promote electricity conservation and demand management in a manner consistent with the policies of the Government of Ontario, including having regard to the consumer's economic circumstances.*
- *To facilitate the implementation of a smart grid in Ontario.*
- *To promote the use and generation of electricity from renewable energy sources in a manner consistent with the policies of the Government of Ontario, including the timely expansion or reinforcement of transmission systems and distribution systems to accommodate the connection of renewable energy generation facilities."*

This new mandate for smart grid and renewable energy integration is being implemented to differing degrees by industry and regulators across Canada. Policy makers, industry, and regulators expect that smart grid innovations can provide the tools needed to meet their mandate.

Chapter Findings

The evolution of the smart grid is being accelerated by substantial legislative and regulatory initiatives throughout North America. Successful large-scale introduction of smart grid technologies will both deliver the potential benefits and maintain the reliability of the bulk power system. It will be important to consider how best to plan, design, and operate the system to successfully integrate smart grid devices and systems in all the various planning timeframes. To achieve this goal, sufficient time is required for industry to develop experience with the smart grid and ensure the bulk power system is planned and designed to support reliable operation.

[22] http://www.oeb.gov.on.ca/OEB/_Documents/Audit/Smart_Meter_Audit_Review_Report.pdf

3. Characteristics and Technology Assessment

Introduction

This chapter develops a definition of smart grid and outlines the key functions of smart grid at the bulk power and the distribution systems. Relevant technologies are discussed and cyber security concerns introduced.

Smart Grid Characteristics

This section reviews the implications of smart grid integration, then identifies the bulk power system and distribution system "devices and systems," briefly explains what they are, describes why they are under the umbrella of smart grid, and identifies bulk power system reliability and cyber security concerns. Technologies are divided into bulk and distribution systems as well as into existing and developing categories to indicate the maturity and breadth of use.[23] As part of this effort, the status and international activities (Appendix 3) of smart grid devices and systems was reviewed. For use in this report, the components of the smart grid have been categorized as either devices or systems. Devices are specific, discrete pieces of equipment that, in total, make up the grid of the future. Systems are processes and ideas that enable the individual devices to work together.

Integration of Smart Grid Technology into the Bulk Power System

The smart grid integration enables the coordinated and system-wide ability to deploy automation through smart devices and systems on the bulk power system. Unlike today, where islands of automation are created without the ability to interoperate across their boundaries, smart grid provides the ability to create an overarching, coordinated, and hierarchical approach to automation, control, and effectiveness. The goal for these deployments is to better match energy supply with demand, improve asset management, and maintain bulk power system reliability.

The main challenge for the envisioned smart grid infrastructure is to integrate smart grid devices and systems while maintaining reliability. Careful study is required to ensure that these characteristic changes do not cause unintended consequences, such as introducing modes of instability and the need for additional coordination of controls. Current deployments of smart grid devices and systems serve as an important example of how new technologies are gradually diffused within the power industry. These have been localized in their implementation for some time at substations [in the form of SCADA, or supervisory control, intelligent electronic devices (IED), and data acquisition] and directly on the bulk transmission system. Some examples include phasor measurement units (PMUs), Dynamic Thermal Circuit Rating (DTCR), and Flexible AC Transmission Systems (FACTS).

[23] "Existing" indicates a mature technology with widespread use. "Developing" indicates the technology is of limited application, in demonstration, or unproven on the grid at this time.

- PMUs produce data useful to improve planning and operations for the purpose of disturbance monitoring, stability model validation, data retention, and disturbance analysis—enabling a more efficient transmission system use by dynamic rating and the advent of new special protection systems, significantly improving operating reliability.
- DTCRs are used to reliably increase the thermal loading capacity of individual transmission lines and substation equipment. Present limits are both static and often conservative, based on worst-case weather conditions. DTCR uses real-time information about weather, load, temperature, line tension, and/or line sag to estimate actual thermal limits, thus allowing higher thermal capacity of transmission lines and substation equipment.
- FACTS, coupled with storage devices, will increase the power transfer capability of individual transmission lines or a transmission corridor and improve overall system reliability by reacting almost instantaneously to disturbances, allowing lines to be loaded closer to their inherent thermal limits. Specifically, the deployment of Unified Power Flow Controllers (UPFC) and Convertible Static Compensators (CSC) will increase the ability to control both real and reactive power flows among transmission corridors and maintain the stability of transmission voltage.

Reliability Considerations of Information Technology and Control System Integration

The three fundamental components of the smart grid infrastructure, besides the availability of smart grid technologies, are 1) interoperability, 2) communications, and 3) Information Technology (IT) systems. These elements provide the basis for a smart grid giving the ability to integrate a variety of technologies and affording a seamless basis for automation.

For example, the U.S. National Institute of Standards and Testing (NIST) is currently developing interoperability standards for equipment, focused on defining consistent communication protocols enabling different types and groups of equipment to quickly and easily share information. Under the Energy Independence and Security Act of 2007 (EISA), NIST is assigned the "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems.…"[24] Also under EISA, the Federal Energy Regulatory Commission (FERC) is charged with instituting rulemaking proceedings and, once sufficient consensus is achieved, adopting the standards and protocols identified by NIST necessary to ensure smart grid functionality and interoperability in interstate transmission of electric power and in regional and wholesale electricity markets. In order to identify and remedy issues including gaps, overlaps, cyber security, etc. in standards, NIST has established a number of working groups and the Smart Grid Interoperability Panel (SGIP), a public-private partnership that provides a more permanent organizational structure to support the continuing evolution of the standards interoperability framework and support development of consensus on the standards. Since its establishment in November 2009, the SGIP membership has grown to exceed 600 organizations, divided among 22 stakeholder categories. The SGIP has launched 17 Priority Action Plan (PAP) working groups that coordinate with standards-setting issues to modify or develop standards that

[24] Energy Independence and Security Act of 2007 (Public Law No: 110–140) Title XIII, Sec. 1305

address issues identified in the NIST process.[25] These interoperability standards will enable the addition of different systems and devices in the future that are not available today, making it easy to add functionality and innovative electric products and services.

From a bulk system perspective, data and information are gathered from multiple locations: energy users, distribution systems, transmission, and generation. Every second, the bulk power system can adjust to accommodate dynamic changes in a user's behavior along with the status of countless numbers of system equipment. However, many of the systems integrated using existing smart grid devices and systems have been designed for control functionality and are not resilient to errors resulting from misuse, miscommunications, or IT system failures.[26] In fact, compared to modern IT and communication systems, these existing control systems have little built-in security and can be intentionally defeated or unintentionally corrupted, etc., which can lead to unexpected results and system failures. For example, through Microsoft Windows PCs attackers can upload encrypted code to the Programmable Logic Controllers (PLCs) that control the automation of smart grid devices and systems. An attacker could remotely control a number of functions, like download files, execute processes, and delete files. In addition, an attacker could interfere with critical operations of smart grid devices and systems, shutting down customer demand, tripping lines, defeating alarm signals for heavily loaded equipment, etc.

The integration of commercial IT systems and communications with existing control systems and PLCs can create reliability considerations. The ramifications and design of smart grid on control systems must be modeled, simulated, and designed to ensure that the expected performance improvements will be realized. Successful integration of smart grid devices and systems should address potential reliability considerations such as transient and long-term stability, small signal stability, voltage stability, intentional cyber attack or unintentional IT and communication errors, and component design issues such as short circuit considerations.

These challenges will require changes in the way the system is planned and operated. Without significant modifications, the bulk power system could be threatened with the integration of the smart grid devices and systems.

[25] See: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome#Priority_Action_Plans_PAPs

[26] U.S. DOE and DHS, *Roadmap to Secure Control Systems in the Energy Sector*, January 2006: www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf

Technology Assessment

Table 1: Smart Grid Technologies — Devices and Systems

Smart Grid Technologies (Devices and Systems) on the Bulk Power System

This section was developed to provide a non-exhaustive list of devices that may now or in the future affect bulk power system reliability. These devices and controllers are prioritized by impacts to bulk power system reliability.

Bulk Power System — Existing Devices

The existing devices below should be considered in bulk power system reliability assessment.

Disturbance Monitoring Equipment

Disturbance Monitoring Equipment (DME) refers to devices capable of monitoring and recording system data pertaining to a disturbance, including the following recorder categories:

- **Sequence of event recorders** accumulates data on equipment response to an event.
- **Fault recorders** document actual waveform data replicating the system primary voltages and currents, including intelligent electronic devices.
- **Dynamic disturbance** recorders portray incidents of power system behavior during dynamic events, such as small frequency (0.1–3.0 Hz) oscillations and abnormal frequency or voltage excursions.

The DME technology is mature, being in existence for over a decade. The data these devices gather can be used by industry to evaluate grid operations and planning. DME devices currently communicate system information for analysis of system disturbances, though they have not been deployed to control power flow. DME facilitates functions that are covered in the *Energy Independence and Security Act of 2007*, enabling the following:

- higher reliability;
- improved voltage and frequency stability and power quality;
- wide area situational awareness, system monitoring, maintenance planning and visualization tools; and
- real-time fault detection, isolation and recoverability.

To ensure reporting and response is accurate and timely, DME data should include accurate time synchronization, reliability, authenticity, and integrity of communicated data. Therefore, those devices with external communications should be protected against malicious or unintentional cyber intrusions, as disruption of communications can blind network operations. Unauthorized access to the communications network can target and disable or override control and protection functions as well as falsifying monitoring and metering information, affecting the operator's decision-making ability.

Phasor Devices

Phasor Measurement Units (PMU or synchrophasors) are devices that measure the phase and frequency for one or more phases of AC voltage and and or current. Phasor data are currently used for situational awareness and wide-area grid monitoring. The data are time-stamped using a global positioning system (GPS), enabling synchronization. The data are predominately used to visualize the phase-angle difference between two ends of transmission lines. To ensure reporting and response is accurate and timely, PMU data should include accurate time synchronization, reliability, authenticity, and integrity of communicated data. One use of PMU data is to identify the impact of variable generation, requiring data transmittal on a high-speed network reliably time-synched. Many PMUs use satellite clocks for time synchronization. Research projects are ongoing on the use of PMU data for determining real-time measures of system stability and may yield additional applications.[27]

PMUs can also provide measurement of other analog waveforms and digital signals, and may record data locally, having other optional functionalities such as:

- high-speed relaying,
- telemetering, and
- fault signal recording.

At present, approximately 161 PMU units are installed in North America. Synchrophasor data are used in a limited number of control centers, although most applications to present diagnostic or conclusive information to the operator are still in development. The North American Synchrophasor Initiative (NASPI)[28] predicts that in three to four years, synchrophasor data will be widely used for postmortem analysis, wide-area monitoring, power system restoration, and static-state estimation. In the next five to 10 years, these data have a potential for use in situational awareness alarming, disturbance prediction, day-ahead and hour-ahead planning, real-time automated grid controls, inter-area oscillation damping modulation controls, congestion management, unit dispatch, and various other emerging technologies for improving grid reliability. The PMU can also be used to identify the impact of changes in variable generation (wind and solar plants) power output over a short time period.

Synchrophasor data must provide time synchronization, reliability, authenticity, and integrity of communicated data to ensure reporting and response is accurate and timely. Malicious cyber security attacks on synchrophasors will affect response time and restoration activities. Disruption of communications can blind network operations. Unauthorized access to the communications network can target and disable or override control and protection functions. Monitoring and metering information can also be falsified, impacting operator decision-making. Synchrophasors that can affect the real-time operation of the bulk power system may require the appropriate application of NERC Critical Infrastructure Protection Reliability Standards.

[27] http://www.naspi.org/repository/projects.aspx
[28] http://www.naspi.org/resources/2009_march/phasortechnologyroadmap.pdf

Power Quality and Flow Control

A **Static VAr Compensator** (SVC) is defined in the Institute of Electrical and Electronics Engineering (IEEE) Standard 1031-2000 as "A shunt-connected static VAr generator or absorber whose output is adjusted to exchange capacitive or inductive current to maintain or control specific parameters of the electrical power system (typically bus voltage)." In practice, an SVC provides dynamic reactive power using thyristors to switch conventional passive components, such as reactors and capacitors, into the grid. An SVC can provide a smooth controllable range of reactive power (MVArs) in a shunt connection to the grid. SVC technology is a mature technology that has been in existence since the 1970s, with thousands of installations worldwide. SVCs have been used for transmission voltage support applications as well as industrial applications such as steel mills and other loads with heavy motor usage, and for maintaining power quality in grids supplying electrified rail traction. They require low maintenance and can be easily integrated into grids. Remote access to control and reference points are available through the current communication portals, such as SCADA systems.

SVCs can be considered smart grid technologies for many reasons. The nature of the power electronics allows the SVC to act extremely quickly to support the grid during contingencies and other system events. By doing so, this helps to alleviate voltage stability concerns, supports increased transfers on the existing power system without significant system upgrades, and facilitates incorporation of variable generation under stable conditions, a key feature in smart grids. SVCs can also be a tool to help mitigate the risk from Power Oscillation Damping (POD).[29] The dynamic nature of an SVC requires that performance studies be performed before installation to determine the optimal location and required size and rating and response characteristics. From an operational aspect, an SVC is a highly reliable system, with availability levels typically at 98 percent and above.

An SVC is a stand-alone system that can operate in an unmanned system without the need for any remote communication. Compliance with NERC Critical Infrastructure Protection (CIP) Reliability Standards and other applicable cyber security requirements are manageable should remote access be desirable.

A **Static Compensator** (STATCOM) is defined in IEEE Standard 1031-2000 as "A shunt-connected static VAr generator or absorber whose output is adjusted to exchange capacitive or inductive current to maintain or control specific parameters of the electrical power system (typically bus voltage)." In practice, a STATCOM provides dynamic reactive power support using turn-on/turn-off power electronics such as an insulated-gate bipolar transistor (IGBT) to modify waveforms of the grid. A STATCOM provides a smooth controllable range of reactive power (MVArs) in a shunt connection to the grid. STATCOM technology is a quickly maturing technology that has been around since the 1990s. STATCOMs have been used for transmission voltage support applications as well as in industrial applications such as steel mills and other loads with heavy motor usage, and for maintaining power quality in grids supplying electrified rail traction. Furthermore, the high dynamic response of STATCOM enables its use for active filtering.

[29] http://www.waset.org/journals/waset/v50/v50-184.pdf

The nature of power electronics enables the SVC to act quickly to support the grid during contingencies and other system events, and thus can be considered a smart grid device. Like SVCs, STATCOMs have extremely quick response times, quicker than those of virtually any other devices. This helps to alleviate voltage stability concerns and allows for increased transfer capacity of the existing power system without significant system upgrades. Remote access to control and reference points are available through the current communication portals such as SCADA systems. A STATCOM is a stand-alone system that can operate in an unstaffed system without the need for any remote communication, however, concerns for compliance with NERC CIP and other applicable cyber security requirements are manageable tasks in the integration of a SVC device, should remote access be desirable.

STATCOM with energy storage enables dynamic control of active as well as reactive power in a power system independently of each other and can provide load support, as well as ancillary services such as frequency regulating power. By control of reactive power, grid voltage and stability are controlled with high dynamic response. Equipping STATCOM with energy storage can be used to balance energy and can help improve stability and power quality in grids with increasingly strong penetration of variable energy resources such as wind and solar generation.

A **Thyristor-Controlled and Switched Series Capacitor** (TCSC or TSSC) is a fixed series capacitor bank equipped with a thyristor valve configured for control and switching of the series capacitor bank. A Series Capacitor (SC) is defined by IEEE Standard 824-2004 as "A three-phase assembly of capacitor units with the associated protective devices, discharge current limiting reactors, protection and control system, bypass switch, and insulated support structure that has the primary purpose of introducing capacitive reactance in series with an electric circuit."

A TCSC (or TSSC) bank provides a continuously variable (or switched) range of impedance in series with the transmission line. The variable impedance allows for a delicate control of power flow, which is helpful in certain network scenarios to avoid harmful resonance situations. This allows for the mitigation of phenomena such as Power Oscillation Damping (POD) and Sub Synchronous Resonance (SSR). This is especially important as the penetration of wind increases.

From a planning aspect, series capacitors are studied and sized in today's simulation programs with standard library models. TCSC's are more complex than series compensation (SC), requiring technical knowledge to design for POD and SSR mitigation. From an operation aspect, an SC is a highly reliable system that requires low maintenance and easy integration into current systems. SC banks have been installed since the 1950s and are a very mature technology. There are thousands of series capacitor installations worldwide. TCSC and TSSC installations are not as common, but are a technically mature technology with some five to 10 installations in operation in the world.

Remote access to control and reference points are available through current communication portals such as SCADA systems. An SC, TCSC and TSSC is a stand-alone system that can operate in an unmanned system without the need for any remote communication, however, concerns for compliance with NERC CIP and other applicable cyber security requirements are manageable tasks in the integration of an SVC device, should remote access be desirable.

Substation Automation

Intelligent Electronic Devices (IED) refers to a broad range of electronic microprocessor-based devices that reside within field substation automation systems and provide the direct interface to monitor and control substation equipment and sensors. The functions they perform include metering, monitoring, control, protection, and communications.

- Metering functions include sensing voltages, currents, frequency, reactive and active power, power factor, energy, harmonics, and transients.
- Monitoring functions include circuit-breaker condition monitoring, trip circuit supervision, switchgear gas density monitoring, sequence-of-event recording, auxiliary power, and relay and transformer temperatures.
- Control functions include both manual and automatic control of output devices including local and remote control of switches and control sequencing.
- Protection functions include trips and interlocks that prevent an impact on the bulk power system or damage to equipment and sensors in the event of a fault condition that results in exceeding operating limits.
- Communication functions include interoperating with other systems such as local RTUs (Remote Terminal Units), SCADA systems or MTUs (Master Terminal Units) and other IEDs through a broad range of communication technologies. Communications within a substation use high-speed physical networks while external communications include a variety of wired and wireless networks including switched telephone, leased line, power-line-carrier, radio, microwave, cellular, satellite, and wide-area networks using fiber optics. Communication protocols running over these networks include DNP3, IEC 60870 and IEC 61850 MMS.

IEDs can perform most, if not all, of the functions outlined in the *Energy Independence and Security Act of 2007* to be part of the smart grid. Of particular importance is the need for increased wide-area visibility, which has been defined by FERC as the top priority in the *FERC Policy Statement – Smart Grid Policy.* Achieving wide-area visibility will require the addition of new automated substations and the upgrading of existing substations with newer automation systems, which will significantly increase the number of IEDs in operation.

Future substations may contain a combination of IEDs with new functionality along with IEDs that provide existing functionality. The level of processing and communications capability within IEDs will increase significantly during the next several years. This will enable newer IEDs to perform advanced functions based on the results of both product research and development and academic research.

Most existing SCADA IED communication protocols were designed for internal high-speed substation communications and do not include indigenous security based on modern security technology. IEDs that communicate externally should use communication protocols based on open standards that incorporate modern security technology for access-control, authorization, authentication, confidentiality, integrity, availability, and non-repudiation. The growth of

SCADA communications networks and the reliance on wireless communication results in increased vulnerability. Malicious cyber security attacks on IEDs in transmission-level substations can have a detrimental impact on the bulk power system at a regional level. Attacks on distribution substations can have a large impact on cities and communities. Disruption of communications can blind network operations. Unauthorized access to the communications network can target and disable or override control and protection functions. Monitoring and metering information can be falsified, resulting in faulty decision-making.

Remote Terminal Units (RTUs) are microprocessor-based electronic devices that reside in a substation and provide data and control communications to the Master Terminal Unit (MTU) located at the central station or network operations center. RTUs transmit IED and directly connected field data to the MTU and alter the state of the IEDs and outputs based on control messages received from the MTU. An RTU can monitor and control both digital and analog data and can support a variety of standard serial and Ethernet protocols such as Modbus, IEC 60870, IEC 61850 MMS, and DNP3. In addition to their primary function as a network gateway, RTUs also provide local control functions with high availability.

These devices share many of the same smart grid characteristics as RTUs and IEDs. They will be used to augment RTUs and IEDs within substations. RTUs can perform most, if not all, of the functions outlined in the *Energy Independence and Security Act of 2007*. Of particular importance is the need for increased wide-area visibility, which has been identified by FERC as the top priority in the *FERC Policy Statement – Smart Grid Policy.* Achieving wide-area visibility in the bulk power system will require the addition of new automated substations and the upgrading of existing substations with newer automation systems, which will significantly increase the number of RTUs in operation. Future substations may contain RTUs with new advanced functionality along with RTUs that provide existing functionality. The level of processing and communications capability within RTUs will increase significantly during the next several years. This will enable newer RTUs to perform advanced functions based on the results of both product research and development and academic research.

Existing SCADA RTU communication protocols do not include indigenous security based on modern security technology. A variety of vendor-specific techniques have been used to add security to existing RTU communication protocols. RTU protocols used for external communications should be based on open standards that incorporate modern security technology for access-control, authorization, authentication, confidentiality, integrity, availability, and non-repudiation. Like IEDs, the growth of SCADA communications networks and the reliance on wireless communication results in increased vulnerability. Malicious cyber security attacks on IEDs in transmission-level substations can have a very detrimental impact on the bulk power system at a regional level. Attacks on distribution substations can have a large impact on cities and communities. Disruption of communications can blind network operations. Unauthorized access to the communications network can target and disable or override control and protection functions. Monitoring and metering information can be falsified, resulting in faulty decision-making.

In addition to RTUs and IEDs, other automation devices such as Programmable Logic Controllers and Programmable Automation Controllers (PAC) are being used to provide new and

advanced monitoring and control functions within substations. PLCs are real-time controllers that can be programmed to perform a variety of control functions using the IEC 61131 control language. PACs are compact controllers that combine the features and capabilities of a PC-based control system with that of a typical programmable logic controller (PLC). A PAC provides the reliability of a PLC with the task flexibility and computing power of a personal computer.

Transmission Equipment

Advanced transmission line sensors exist today that enable the safe capture of the underused design capability of the transmission line. Additionally, they protect the transmission line from overheating when real world cooling conditions, primarily the wind cooling effect, drop below the assumed cooling conditions used in calculating a static rating.

The sensing technology is not new. Tension sensors have been deployed on transmission lines since 1991; sag sensors have been deployed since 1999. Other devices to monitor conductor sag are emerging in the marketplace. They range from devices that use ultra-sound to measure conductor height above ground to devices that sense the electrical field surrounding an energized conductor to monitor the conductor's position in space.

The challenge faced in the use of these advanced sensors is in capturing the average conductor temperature of each line section comprising a complete transmission line. The average conductor temperature is a function of the ambient air temperature, solar radiation, and wind speed and direction. Ambient temperature and solar radiation are reasonably constant over time and distance. Wind, on the other hand, varies significantly over time and distance, and has a median spatial variability of approximately 200 meters. That means wind measured at one point on a transmission corridor has no statistical correlation to wind measured 200 meters away. Yet wind has significant influence in determining the transfer capacity (the rating) of an overhead transmission line. The solution to this challenge for calculating a rating for the transmission line lies in using the transmission line itself as part of the advanced sensors. As tension and sag are inversely and directly related, if one is measured, then the other can be determined. Therefore, combining either tension or sag-measuring devices with the transmission line's inherent resolution of weather variables provides the data required to deliver reliable dynamic line ratings to transmission system operators and planners.

The principle tension-monitoring sensor is installed in-line between the transmission structure and the insulator string to which a conductor is terminated. The location permits the unit to be operated at electrical ground potential while providing a direct reading of conductor tension. The principle sag sensor consists of a video camera installed at ground potential on the transmission structure and uses imaging technology to monitor the movement of a target installed on the conductor.

All of the sensors use radio, fiber optic, general packet radio service (GPRS), or other media to transmit their data to receiving units located inside secure perimeters. The data are subject to interception and manipulation. Encryption of data is the first line of defense. However, the strongest defense rests with the Dynamic Line Rating systems that use the raw data. Those systems must have the ability to identify sensors that have been breached and are delivering data that is out of bounds or inconsistent with data from other sensors. From a cyber security

standpoint, all of these sensors are located outside the protected perimeter of control centers and substations, and may be subjected to physical attack or direct manipulation of their data output. Those sensors located on the structure closer to energized conductors may benefit slightly from the deterrent value of high voltage. Sensors will be located along a transmission line with several miles separating one sensor from the next. The distance between sensors reduces the likelihood that all or several sensors will be simultaneously attacked.

Superconductors and advanced conductors currently play a niche role in bulk power system reliability. As improvements in these materials make them more attractive, they can be part of the smart grid of the future. The unique set of characteristics inherent to superconductor cables provides numerous opportunities to enhance the operation of both the transmission and distribution grids. Besides increased efficiency, the low impedance of AC superconductor cables allow for the addition of a controllable impedance to the cable via inductors or phase angle regulators, yielding effective and economical control of AC power flow similar to fully controllable DC circuits. Their higher power ratings allow for lower voltage levels to be used reducing costs and simplifying placement. They are thermally independent of the environment, and are both absent of, and immune to, electro-magnetic fields. Superconductor cables are identified as an Advanced Component in the National Energy Technology Laboratory's (NETL) Modern Grid Initiative. Further, they address two of the Modern Grid Initiative's six characteristics: 1) Optimizing Asset Utilization and Operating Efficiently, and 2) Operating Resiliently.

Taking advantage of the characteristics of superconductor materials allow superconductor cables to be manufactured with special fault current limiting characteristics, which reduce both fault current magnitudes and DC offsets. In the bulk power system, the cables can both strengthen the grid by increasing MVA transfer capacity, while reducing overall short circuit levels. In the distribution grid, this capability allows for tighter meshing of the network, improving asset use, reliability, and grid resiliency.

A status summary of superconductors follows:

- A number of superconductor-based devices are in various stages of development that offer the potential to increase grid efficiency and transmission capacity, and improve system resilience. These include cables (AC and DC), fault current limiters, and transformers.
- Superconductor cables are available today but require financial assistance for initial projects. Other devices require full-scale field demonstrations or even more basic R&D before deployment in the bulk power system.
- True commercialization of all these devices will require expanded activity by government, for example, the DOE's Office of Electricity Delivery and Energy Reliability's Superconductor program (which includes many of the national labs) as well as industry taking the initiative to integrate the devices, and to support manufacturing.
- Numerous manufacturers and national laboratories have been actively working on these devices and the basic underlying technologies with strong support by the U.S. Government—though this support seems to be winding down just as the technologies are

close to commercialization. Other international governments (most notably Korea, Japan, and China) are actively pursuing this technology in an effort to develop new smart grid and clean technology-based domestic industries.

Underground cables using high temperature superconductor (HTS) materials in lieu of copper or aluminum conductors offer very high power transmission capacities, very low impedance, low power losses, minimal right of way needs, and simplified siting requirements. AC superconductor cables have been successfully demonstrated and deployed in numerous locations throughout the world, and have been manufactured by, and are available from, a number of suppliers. DC superconductor cables are a straightforward adaptation of AC cable technology and promise to be the highest efficiency (lowest power loss) overhead or underground transmission method, as superconductors have zero resistance when carrying DC current. The first deployment of a DC superconductor cable (rated five GW) is planned for the *Tres Amigas* project in New Mexico. All superconductor cables require refrigeration to operate.

The concept of moving gigawatts of power underground for very long distances—previously impractical—is possible when DC power transmission is coupled with superconductor cables. Superconductor materials act as true, perfect conductors when moving DC electricity. Such cables will be capable of moving tens of thousands of MW of power for unlimited distances with no power losses other than a fixed amount consumed by their refrigeration system, producing a transmission system with one-half to one-fifth or less the losses of any other overhead or underground technology. Combining DC superconductor cables with modern multi-terminal, voltage-source converter-based HVDC technology will enable the construction of an underground DC supply grid to support and enhance the existing AC bulk power system.

Though in service today, superconductor cables are considered pre-commercial as their limited deployment to date has been insufficient to deliver acceptable cost reductions. As such, financial assistance may be required to accelerate acceptance for initial projects. While superconductor cables themselves are passive devices, equipment associated with their control may not be (e.g., High-Voltage Direct Current terminals, protective relays, etc), and the cyber security issues inherent to them will remain.

Advanced Conductors include those that are high temperature, low sag, overhead conductors, which are intended for use on existing or new overhead transmission lines. Their primary characteristic is the ability to operate at or above temperatures of 200° C, while maintaining similar sag characteristics of traditional conductors of the same size at lower temperatures. Therefore, they have higher current ratings (which produce heating) and provide modest increases in power handling capacity compared to traditional conductors. Depending on the resistivity of the conductor core, reduced power losses are also claimed. Because of their increased cost compared to conventional conductors, use of these high temperature, low sag, and increased capacity conductors is not widespread. At present, they are typically viewed as a special application product to minimize sag in long spans or to increase capacity on existing lines by replacing an existing conductor without replacing structures. There are currently three main commercial versions of these conductors: Aluminum Conductor Composite Reinforced (ACCR) conductor, Aluminum Conductor Composite Core (ACCC) conductor, and Aluminum Conductor Steel Supported (ACSS) conductor. There are no cyber security issues inherent with these conductors.

Bulk Power System — Developing Devices

The following developing smart grid devices may affect bulk power system reliability.

Energy Storage

Energy storage is an active part of the bulk grid, predominately in the form of 20,000 MW of pumped hydro storage that currently comprises two percent of U.S. generation nameplate capacity.[30] However, as the NERC 2009 *Long Term Reliability Assessment* identifies, energy storage is an emerging issue. This new focus on energy storage is driven by major advances in storage technology and the economics of using energy storage as a grid-connected asset. For example, in the U.S., the EISA specifically identifies energy storage as a characteristic of the smart grid[31] and, in the last two years, over 50 MW of advanced battery and flywheels have been approved for interconnection at four ISOs and RTOs now participating in these markets. One of the distinctive characteristics of the electric power sector is that the amount of electricity that can be generated is relatively fixed over short periods of time, although demand for electricity fluctuates throughout the day. Technologies to store electrical energy so it can be available to meet demand are a growing need of the electric grid. While the need has existed since the beginning of the electric grid, the recent and rapid integration of variable generation may intensify the need for storage systems.

Enhanced energy storage can provide multiple benefits to both the power industry and its customers. Among the benefits are improved: 1) power quality, 2) stability and reliability of transmission and distribution systems, 3) use of existing equipment, thereby deferring or eliminating costly upgrades, and 4) availability and increased market value of distributed generation sources. The predominant emerging technologies are batteries, flywheels, electrochemical capacitors, and compressed air energy storage (CAES).

- Grid-scale battery systems have been piloted and are now being installed as commercial systems in the grid. While lithium-ion battery systems are predominantly being deployed today, pilot programs and evaluation of lead-acid and flow batteries are underway.
  - With the federal government's call for one million electric vehicles by the year 2015, the implementation of smart charging software and systems may provide valuable storage of electricity through aggregation of electric vehicles.
  - Aggregated distribution storage, also called community energy storage, installed in residential areas provides:
    - improved service reliability and efficiency (close to customers);
    - voltage sag mitigation and emergency transformer load relief;
    - multi-MW, multi-hour storage when aggregated (leverage AMI); and

[30] http://www.eia.doe.gov/cneaf/electricity/epa/epat1p2.html
[31] Energy Independence and Security Act 2007, TITLE XIII Smart Grid

    - potentially low cost (synergy with PEVs).[32]
  - Research into liquid metal batteries is being funded by ARPA-E and holds promise for very large scale grid storage. Commercialization is not expected for five to ten years.
- Compressed air energy storage provides very large scale storage for long periods of time. While only two CAES facilities have been built, driven by government support, a re-emergence in construction of new CAES facilities during the period 2010–2014 may occur.

Ultra-capacitors hold less electricity than batteries but absorb and release it much more quickly, usually in a matter of seconds. The ability to absorb and release electricity quickly is crucial for time-sensitive electricity storage, including frequency regulation. As with any device, malicious cyber security attacks and accidental misconfigurations can have a detrimental impact on energy storage and the availability of that energy storage. Also, monitoring and metering information can be falsified, resulting in faulty decision-making.

For bulk energy storage systems, control has most typically emulated the control of generating resources, i.e., use of dispatch systems including Automatic Generator Control (AGC). The management of energy across hours through use of pumped storage and the more recent control of advanced fast-acting storage for provision of frequency regulation has both used AGC systems to control the bi-directional exchange of power and energy between the grid and connected storage systems. Relatively recent grid storage projects (for example, Golden Valley Electric, Anchorage, RMP, Castle Rock Utah, and ETT, Presidio, Texas battery systems) have leveraged advanced storage technology's higher device functionality, and inverter and PCS interfaces of newer advanced storage systems to access and use a wider range of grid-support functions. For example, they are used to provide voltage regulation support, transient mitigation support, event-triggered storage device output for system load relief, recurring and scheduled storage device dispatch for system load relief, and active islanding. These expanded and sometimes coincident services use both local and remote control of storage systems.

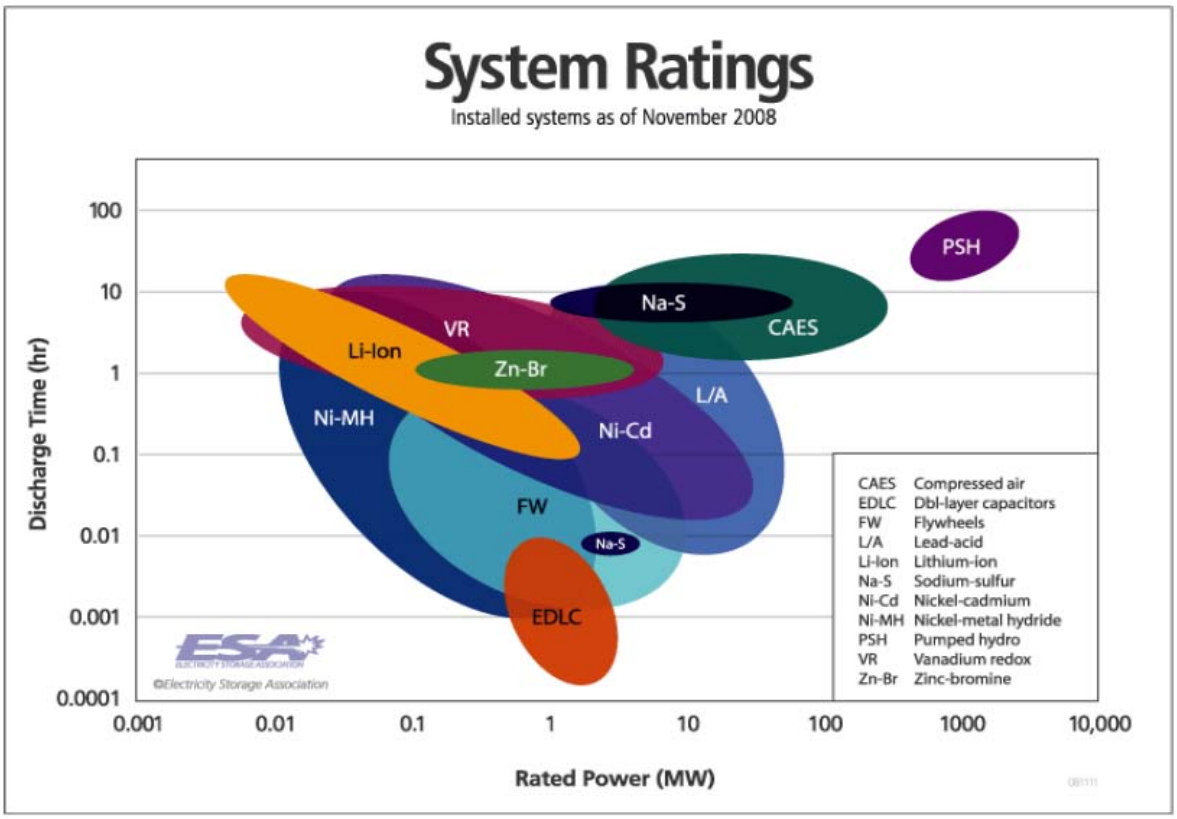
As the capabilities of advanced storage technologies are better understood and integrated within the context of transmission planning, controls will expand to include Phasor Measurement-based wide-area monitoring and management schemes, and relay-based special protection schemes. The types of expanded bulk storage applications that will be associated with these expanded controls will include blackstart and system restoration as well as active islanding at the circuit through local area and substation level. The vast majority of existing storage capacity in North America is in the form of pumped storage hydro. The next largest amount of grid-connected storage in the U.S. is in the form of Compressed Air Energy Storage (CAES). However, within the last five years, other relatively more advanced, and functionally robust, forms of grid-connected energy storage have started operating at MW scale in the U.S., including flywheels, advanced lead acid (PbA) batteries, flow batteries, Ni-cad batteries, Sodium Sulfur (NaS), Li-ion batteries, and thermal energy storage systems.

This summary level information is drawn in part from information posted by the Electricity Storage Association.[33] This is a recommended resource for additional information on both the

[32] This report addresses EVs and PEVs in the Electric Transportation Supply/Demand section of this report.

technologies and their applications across the electrical grid. A graphical illustration by the Electricity Storage Association[34] of the ratings (size and duration) of electricity storage deployed as of 2008 is shown below in Figure 3. There has been a rapid evolution within this grid asset group since 2008, as the data in Figure 3 shows. One example, since 2008, is that over 20 MW of Li-ion batteries systems have been interconnected to transmission systems for commercial operation within open markets.

Figure 3: Storage technology ratings, deployed systems as of 2008[35]



[33] http://www.electricitystorage.org
[34] http://www.electricitystorage.org/site/technologies/
[35] http://www.electricitystorage.org

Bulk Power System — Existing Systems

Existing systems on the bulk power system can have important reliability considerations.

Transmission Dynamic Line Rating (DLR) Systems

Most utilities rate the overhead transmission lines based on fixed weather assumptions, resulting in so-called static ratings. Static ratings tend to underuse the rating or the transfer capacity of the installed transmission lines while they fail to protect those same assets from overheating and over-sagging when the assumed weather conditions are not present. DLR systems allow the transmission operator to know the transfer capacity of the transmission line in real-time, taking into consideration actual weather conditions. DLR systems have been widely shown to increase the transfer capability of existing transmission lines by 10–30 percent without violating safety clearances and without exceeding the line's design criteria, including the conductor's design temperature. This technology has been deployed to remove system constraints, mitigate congestion, facilitate market deregulation, increase access to renewable energy resources, protect physical transmission assets from overheating, and increase system reliability. Some DLR systems help manage ice formation before it becomes irreversible or difficult to control.

Dynamic Line Rating systems have been deployed for many years and have a variety of characteristics and technologies. The least advanced systems consist of little more than sensors delivering data values; the host organization is expected to work out how to apply the value. The most advanced is a complete end-to-end solution embodying all the functions described in this report; the system installs on a 20-mile line in four to five days, including all line sensors and full integration with the EMS. The first end-to-end solution appeared on the market in the mid 1990s; the present state of the art has been available for five years. Some DLR systems have the advantage of being fully integrated with existing EMS and SCADA systems. In such cases, all pertinent functions are fully automatic; ratings are continuously displayed in a format familiar to system operators, and are also available to design engineers, planning engineers, state estimating programs, security analysis programs, etc. By definition, Dynamic Line Rating systems must reflect the impact of varying weather along a transmission line. As this is difficult, only a few dynamic rating methods are in widespread use.

Dynamic Line Rating systems are completely automatic and fully integrated into the EMS and SCADA system. On a typical transmission line, tension-monitoring equipment is installed at multiple structures. Solar powered transmitters send tension and other data back to a substation using spread spectrum radios. At the substation, a receiver translates the data into the EMS and SCADA protocol and sends the data directly to the EMS and SCADA master. An algorithm in the EMS and SCADA calculates the Dynamic Line Rating and displays the rating on the system operator's existing console. The ratings are also available to system planners, design engineers, security analysis programs, and state estimator programs.

From a cyber security standpoint, DLR systems must be viewed as an integrated entity. Field sensors are subject to physical attack and communications disruption and interception as delineated earlier in this report. As a result, raw data may be compromised before they arrive at the control center for processing into Dynamic Line Ratings for an entire transmission line. The processing software at the control center has the ability to identify data that are out of bounds or

inconsistent with data from other sensors. One of the strongest defenses to cyber attack rests in the way DLRs are determined. A DLR is independently established for each sensor along a transmission line. The lowest rating of all the sensors is then reported as the rating for the entire transmission line. If one or a few of the sensors are compromised and deliver data that produce an improperly high rating, it is simply ignored since it is not the lowest of the reported ratings. To produce a dangerously high rating for a transmission line would take a coordinated attack on every single sensor on the line along the entire length of the line. That attack would also have to find a way to simultaneously deliver to the EMS an erroneously high MVA reading on the transmission line. Under those circumstances, an erroneously high Dynamic Line Rating is possible. Since most transmission lines are dispatched to survive N-1 conditions, the attacker would have to simultaneously create an N-1 event that placed a high MVA load on the target transmission line. The MVA load would have to exceed the true (uncompromised) Dynamic Line Rating that would otherwise have been calculated for the line.

Special Protection Systems and Schemes

Special Protection Systems and Schemes (SPS), also called Remedial Action Schemes, refer to an automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and MVAr), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include 1) under-frequency or under-voltage load shedding; 2) fault conditions that must be isolated; or 3) out-of-step relaying [not designed as an integral part of a Special Protection Scheme (SPS)].

Although SPSs are not specific devices, with the continued development of microprocessor technologies, the smart grid will advance how these systems are deployed and monitored. The deployment of SPSs in the smart grid may introduce increased complexity and interdependency (interaction between SPSs) that requires incorporating a grid-wide view into the design in addition to input of local quantities. Unless carefully deployed, there can be risk to reliability resulting from inappropriate actions taken by SPS during system events causing unintended consequences. If SPSs are subject to malicious attacks, the result could be detrimental to the reliability of the bulk power system. Attacks on communication paths and data can blind network operations and reliability. Unauthorized access to communications and data can disable or override control and other protection functions. SPSs can control the flow of power on the bulk power system and require the appropriate application of the NERC *Critical Infrastructure Protection* Reliability Standards.

Advanced Relaying Systems

Advanced relaying systems provide for increased system visibility through integrated protection and monitoring systems. These systems use microprocessor technology, which provides far more benefits than traditional electro-mechanical protection. Ethernet and serial communications, which are included in many relays, also provide for synchronized phasor measurements, advanced fault location, determination of thermal line-loading limits, and information on system conditions. Microprocessor relays allow for increased line loading without loss of security, increasing line capacity by as much as 25 percent. Load-encroachment blocking, to meet NERC

guidelines, prevents unnecessary tripping during emergency conditions. Monitored communication ensures high-speed tripping for faults. Synchronized phasor measurements can alert system operators about loading problems or system oscillations that can lead to power loss. High-reliability components and self-test functions reduce maintenance costs and increase availability. Advanced monitoring informs operators of terminal and line status for improved situational awareness. Advanced relaying combined with the use of bulk power system operating parameters provides for the use of dynamic relay settings control. Some monitoring parameters that microprocessor relaying can use for number of dynamic operations are:

- breaker operating time, monitored both electrically and mechanically;
- battery voltage during tripping, recorded to avoid loss of operating capacity when needed;
- circuit breaker status, monitored to keep operators informed of excessive compressor running, breaker inactivity, total interruption duty, and pole discordance timing; and
- transmission conductor temperature, loading, and line sag.

Microprocessor relaying in transmission and distribution systems is a mature technology that continues to improve. Based on the functions outlined in the *Energy Independence and Security Act of 2007*, the particular smart grid enablers advanced relaying devices provide have:

- higher reliability;
- voltage and frequency stability and power quality;
- wide area situational awareness, system monitoring, maintenance planning, and visualization tools; and
- real-time fault detection, isolation, and recoverability.

Concerns caused from advanced relaying integration include the need to ensure time synchronization, reliability, authenticity, and integrity of communicated data to ensure reporting and response is accurate and timely. Malicious cyber security attacks on advanced relaying will affect response time and restoration activities. Disruption of communications can blind network operations. Unauthorized access to the communications network can target and disable or override control and protection functions. Monitoring and metering information can be falsified, resulting in faulty decision-making. Where advanced relaying can control the power flow of the bulk power system, it will require the appropriate application of NERC's Critical Infrastructure Protection Reliability Standards.

State Estimators

With the continued proliferation of microprocessor relay technology and the development of Phasor Measurement Units (PMUs), state estimation using real-time measured quantities will continue to develop and be incorporated by ISOs and RTOs and individual transmission operations and organizations. The forthcoming real-time state estimation technology will be used to evaluate, trend, and potentially control the operation (manual or otherwise) of the bulk power system.

State estimation facilitates functions are outlined in the *Energy Independence and Security Act of 2007*. The particular smart grid attributes that enhance bulk power system reliability through the use of Phasor Measurement Unit devices are:

- higher overall reliability;
- improved voltage and frequency stability and power quality;
- wide area situational awareness, system monitoring, maintenance planning, and visualization tools; and
- real-time bulk electric system degradation awareness and recoverability.

The real-time state estimation capabilities are not mature yet, but several DOE American Recovery and Reinvestment Act grants are evaluating this technology, developing interface software and the tools needed to operate the bulk power system more efficiently, economically, and with an even higher level of reliably. As real-time state estimation capabilities continue to mature, the applications developed that control physical transmission grid devices or affect the real-time operation of the bulk power system may require the appropriate application of the NERC Critical Infrastructure Protection Reliability Standards.

Bulk Power System — Developing Systems

New developing systems on the bulk power system can affect reliability

Wide Area Management Systems (WAMS)

WAMS, also known as Wide Area Time domain GPS Synchronized Sampling (WATSS), is defined as the "visual display of interconnection wide system conditions in near real-time at the reliability coordinator level and above."[36] WAMS offer bulk power system operators access to large volumes of high-quality information about the actual state of the electric system or wide area situational awareness (WASA). This should enable a visualization of the state of the grid and a more efficient use of assets, for example through a switch from static to dynamic line ratings.

WAMS, coupled with the knowledge of transmission line transfer capacity in real-time, taking into account actual weather conditions between substations and across regions, can enhance WASA as the thermal behavior of the line is complementary and synergistic to the PMU electrical outputs. These technologies will provide the infrastructure to perform grid control functions with precision and speed not possible with other technologies.[37] Possible control applications and functions are: 1) system protection (electrical and thermal), 2) state estimation, 3) visualization, situational awareness, alarming, 4) system stability, voltage, and frequency control, 6) post mortem analysis and play-back capability, 7) parameter estimation and model validation, 8) predictive analysis/look-ahead, 9) oscillation monitoring, 10) islanding monitoring, controlled islanding and restoration, 11) control of renewable resources, 12) system optimization, 13) load control, 14) dynamic line ratings and dynamic line thermal monitoring, and 15) voltage security monitoring.

[36] http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf
[37] http://cio.nist.gov/esd/emaildir/lists/t_and_d_interop/doc00049.doc

Smart Grid Technologies on the Distribution System

This section provides a thorough, but non-exhaustive, list of controllers and technologies that may now, or in the future, have material effect on bulk power system reliability. The effects of these devices, if installed in large numbers and controlled centrally, may need to be addressed by bulk power system planners in their evaluation of system protection and grid stability.

Distribution System — Existing Devices

The following existing distribution systems, in aggregate, should be considered as part of reliability assessment of smart grid integration.

Advanced Metering Infrastructure (AMI)

AMI uses an advanced electric meter that identifies consumption in more detail than a conventional meter and, optionally, communicates that information via some network for monitoring and billing purposes (telemetering), while providing customer information to distribution control applications. Advanced metering provides the ability for two-way communication from industry to end-users for programs such as Demand Response (load control), Remote Connect/Disconnect, Integrated voltage/VAr control, and potential use for automated responses of Distribution Automation devices for reconfiguration (self-healing).

An investment in smart grid AMI meters is a long-term commitment of 10 to 20 years. To "future-proof" this investment, several architectural features should be included. The first is the ability to upgrade the meter firmware or software settings "over the air" without having to visit the home or business. It is a given that networking technologies, Home Area networking protocols, and security techniques will evolve and change over time, not to mention the introduction of additional applications for the smart grid. In addition, the use of standards- based protocols and transports have the ability to "outlive" proprietary solutions, which requires AMI technologies to change. These devices should be considered long-term investments and designed with sufficient memory to support future features and functions.

With a large number of centrally controlled AMI meters, which typically have minimal physical security (other than the meter housing and tag lock), it is important to protect the communication channel and meter data from corruption and tampering. To do this, industry standards in encryption, certificate, and keys need to be employed to ensure that if the meter is tampered with, the impact will be minimal and localized to the individual meter. These protection and encryption schemes should be applied end-to-end from the meter to the back office systems to ensure no vulnerability in the entire communications path. AMI networks will carry more information and will require faster networks for near real-time information requests. Malicious cyber security attacks can preclude cities and communities from having reliable information. Disruption of communications can blind network operations from servicing AMI networks for outages. Unauthorized access to the communications network can target and disable or override control and protection functions. Monitoring and metering information can be falsified, resulting in unreliable information for decision-making.

Distributed Generation and Storage

Customer-distributed generation refers to electrical generators that are situated on-site behind the small industrial, commercial, or residential customer's revenue meter. These generators include an expanding variety of solar panels, small-scale wind turbines, fuel cells, and bio-fuel diesel generators. Residential solar panels and small-scale wind turbines are connected to the electrical system through inverters, which convert direct current (DC) to alternating current (AC) and tie into the distribution grid through the revenue meter. These generators typically output less than ten kW. Distributed energy storage acts both as load and distributed generation. Distributed energy storage may encompass more than the capacity of plug-in electric vehicles (PEVs), such as community battery banks. Depending on their application and amount, they can provide significant support for a system's capacity and energy requirements. Commercial and small-industrial distributed generators are similar to residential, but provide higher output power—in the range of 10 kW to 200 kW. Some of these produce AC power and must be synchronized to the grid. Systems that can feed energy into the grid are usually required to have anti-islanding protection that prevents feeding electricity back into the grid if a fault has occurred. Industrial customers may provide larger generation capacity. For example, at Manitoba Hydro, initial proposals are being considered for generation of up to ten MVA to be connected on the distribution system (12 or 25 kV) or high voltage distribution system (66 kV).

One of the key elements of smart grid is to enable customer participation and the ability to accommodate all generation and storage options. This is outlined in the DOE *Smart Grid System Report – Characteristics of the Smart Grid*, July 2009.[38] Small industrial, commercial, and residential customer generation may directly affect the distribution grid. As distributed generation expands and is aggregated, it may also affect the bulk power system. It is important to plan ahead for this scenario. Power flow into the distribution network will vary over time and needs to be monitored and factored into grid operations. It is recommended that an intelligent grid interface be defined for customer-sited equipment that exports power to the grid. This interface would provide industry with valuable information concerning the state of the generator in real-time along with the potential capability to island the generator under fault conditions. It is also recommended that this interface be integrated with (but separate from) customer demand response and pricing signals. It should also be extensible to enable customer participation in emerging retail markets.

New types of residential, commercial, and small industrial generators will be developed over the upcoming years, expanding the use of behind-the-meter distributed generation. If the time line for installation is accelerated, there may be impacts on the reliability of the bulk power system. Distributed generation and storage may have bulk power system impact when installed in large enough numbers and centrally controlled. Security considerations for the bulk power system will grow over time and will become important when significant customer generation capacity is being exported or aggregated. Maintaining cyber security at the substation level will be important. In addition, all communication interfaces between the residential, commercial, and industrial customers' energy export systems and the grid should take into account: access-control, authorization, authentication, confidentiality, integrity, availability, and non-repudiation.

[38] http://www.oe.energy.gov/SGSRMain_090707_lowres.pdf

Power Factor Correction Devices

Power factor correction devices are extensively used to minimize distribution system losses, to enhance system use, and to stabilize system voltage within acceptable range. Power factor correction devices are an integral part of a reliable and efficient distribution smart grid. As smart grid aims to provide enhanced electric system control and reliability, power factor correction devices garner a pivotal role in the electric distribution systems. As an example, a viable and practical redirection of power flow in response to localized disruption can only be facilitated by swift operation of coordinated power factor correction devices throughout the affected system.

Electronics-based power factor correction devices, based on high-power switching devices and equipped with digital controllers, should be able to communicate and respond at the distribution level to secure system operability, security, and reliability. The embedded intelligence in each device would communicate with decision-making centers to implement the decision and report on the status to these centers to provide real-time data for the decision-making process. There may be a bulk power system impact, but only in extreme conditions and only if power factor correction devices are widely installed over many distribution systems and centrally controlled.

Integrated Volt/VAr Control (IVVC)

IVVC is an optimization method to jointly achieve a near-unity power factor and meet voltage magnitude targets. As unity power factor and unity voltage are two competing criteria, IVVC method balances these two criteria and resolves any conflict between them. IVVC enables voltage and VAr management of distribution grid infrastructure and maximized field equipment use, and enables implementation of volt/VAr optimization and conservation voltage reduction. Conservation voltage reduction is a process by which an organization systematically reduces the voltages in its distribution network, resulting in a reduction of load on the network.

IVVC analyzes voltages from various regulators, load tap changing transformers, power factor correction devices, medium voltage sensors, customer meters, and supplementary monitoring points. IVVC can be integrated with SCADA, DMS, or OMS systems to maintain operational control, to monitor grid conditions in real-time in order to minimize the impact of VARs across the distribution system, and support reconfiguration of switches and energy rerouting strategy. There may be a bulk power system impact, but only in extreme conditions and only if IVVC devices are widely installed over many distribution systems and centrally controlled.

Distribution System — Existing Systems

The following existing systems on distribution can affect bulk power system reliability.

Demand-Side Management Programs

One of the key elements of smart grid is to enable customer participation.[39] Customer demand management programs are developed by utilities to enable customers to participate in grid load management strategies. Customers subscribe to these programs and are usually offered incentives to participate. They vary over a wide range from simple air conditioner cut-off during summertime peaks, to contracts that require energy curtailment when a signal is received, to dynamic pricing programs where a customer has the opportunity to respond to real-time energy pricing. These programs are typically designed to shed load and help balance the grid when there is insufficient generation capacity to service the load or to relieve stress on grid components. Dynamic pricing programs permit customers with automation systems to respond intelligently to price signals based upon their specific environment.

Customer demand management will directly affect the distribution grid. As demand management becomes aggregated, the net effect of load reduction or expansion may affect the bulk power system. It is important to plan ahead for this scenario. Demand management programs permit loads to vary over time, and must be monitored and factored into grid operations. It is recommended that an intelligent grid interface be defined for customer demand management. This interface would provide the industry/aggregator and customers with the information needed to reliably monitor and respond to grid demand response and pricing signals. It can also be extended to enable customer participation in emerging retail markets. An interface between the industry/aggregator and the bulk power system may be defined for delivering information related to the aggregated load under demand management. New types of demand management programs may be implemented over the upcoming years as new business models are developed. These may expand the use of demand management and accelerate the time line for when this capability has a direct impact on the bulk power system.

Security considerations for the bulk power system will grow over time and will become important when significant customer demand management capacity is being aggregated. It is important that communication interfaces between the residential, commercial, and industrial customers' energy management systems and the grid take into account access-control, authorization, authentication, confidentiality, integrity, availability, and non-repudiation. Therefore, there may be bulk power system impact with a large enough number of centrally controlled demand management systems.

Under-Frequency Load Shedding

Power system steady-state operation requires a balance between generation and load. A sudden loss of generation due to abnormal conditions, such as loss of generating units due to faults, disturbs this balance and the system frequency begins to deviate from nominal. System operation at low frequencies impairs the operation of power system components, especially turbines and, if not corrected, can lead to tripping of additional generators thereby further aggravating the situation.

To arrest frequency decline, the governors of the generators with spinning reserve act to attempt to make up for the lost generation. If the frequency decline is too fast (due to severe mismatch

[39] http://www.oe.energy.gov/SGSRMain_090707_lowres.pdf

between load and generation) and the governors cannot react fast enough or spinning reserve is not adequate, under-frequency relays are used for initiating automatic load shedding as a last-resort system preservation measure by implementing an Under-Frequency Load Shedding (UFLS) program. The under-frequency load-shedding scheme must be properly designed to:

- prevent excessive load shedding that may result in over-frequency conditions or unnecessary loss of service continuity and revenue;
- avoid insufficient load shedding, which in turn may lead to system blackout; and
- provide sufficient load shedding to maintain the frequency in an acceptable operating range.

A coordinated automatic under-frequency load-shedding program is required to maintain power system security during major system frequency declines. NERC has provided reliability standards, requirements, measures, and levels of compliance to ensure the proper implementation of UFLS programs. NERC Regional members have developed their own standards based on the Reliability Standards that also address their specific needs. Significant penetration of UFLS programs can affect the reliability of the bulk power system.

Under-Voltage Load Shedding

Under-Voltage Load Shedding (UVLS) is analogous to UFLS, which has become a common industry practice. UVLS schemes have been successfully applied in many power systems to protect systems from voltage collapse and/or prolonged low voltage operation. UVLS may be the most economical solution in preventing voltage collapse under low probability events and extreme contingencies leading to serious consequences such as widespread system collapse. UVLS schemes should be designed to distinguish between faults, transient voltage dips, and low voltage conditions leading to voltage collapse.

Voltage collapse or uncontrolled loss of load or cascading may occur due to lack of sufficient dynamic reactive power reserve, especially during contingencies. UVLS has been useful in slow-decaying voltage situations using typical relay time delay settings ranging from three to ten seconds. UVLS schemes are not usually helpful for mitigating transient instability conditions. Since the relay time delay setting is normally long (in order to avoid false tripping), the load tripping is usually not sufficiently fast to prevent a transient instability situation. Although application of UVLS in some power systems may be very helpful in preventing voltage collapse, it may not be effective in all systems. Where practical, using direct load shedding is superior and more reliable than automatic UVLS in systems with fast voltage decay (~one second). These systems (with fast voltage decay characteristics) may be at a risk of slower voltage decay under different conditions. Studies should be performed to determine which systems are the potential candidates for a UVLS scheme.

The complexity to arm UFLS and UVLS to shed the desired amount of load increases with the growing penetration of distributed generation, demand-side resources, and demand-side management. These technologies cause feeder loading to deviate significantly from a typical load duration curve reducing certainty as to the amount of (net) load available for load shedding at any given time. The smart grid could be used to enable intelligent, real-time arming of load to increase dependability of UFLS and UVLS programs. As with UFLS, significant penetration of UVLS programs can also affect the reliability of the bulk power system.

Distribution System — Developing Devices

New device integration on the distribution system can, in aggregate, affect bulk power system reliability.

Electric Transportation Supply/Demand

Electric transportation has the highest potential for direct distribution impact on the bulk power system, but significant distribution investments will need to be made prior to widespread adoption of this technology. Electric transportation is unique in that it can be designed, along with the distribution system, to provide supply or act as demand.

According to the Brookings Institution,[40] plug-in electric vehicle (PEV) introduction may take one of two scenarios:

1) Best-case scenario: smart grids ensure PEVs are powered by renewables that are generated during off-peak hours, or
2) Worst-case scenario: electricity providers and the government are not well equipped to deal with the rapid innovation and technology necessary for PEVs.

In the best-case scenario, no additional power plants would be needed and electric rates might increase by only one to two percent. Almost 73 percent of the existing U.S. vehicle fleet could be supported in this fashion, thus decreasing demand for oil in the U.S. by 50 percent and subsequently reducing greenhouse gas emissions. In the worst-case scenario where PEVs are charging on peak and vehicle-to-grid (V2G) systems are not properly functional, Load Serving Entities (LSE) will not be well prepared for high PEV penetrations. As a result, additional capacity may be required to support charging.

As a part of its energy-efficient federal vehicle fleet procurement,[41] the American Recovery and Reinvestment Act of 2009 (ARRA) sets aside $300 million and tax credits for capital and necessary expenditures for PEV purchases. Furthermore, the American Clean Energy and Security Act requires each organization to develop a plan "to support the use of plug-in electric drive vehicles." The Act further requires the Secretary of Energy to create a program that includes financial assistance for the integration of EVs in multiple regions.[42] A number of production PEV automobiles have already been introduced in North America. A recently released report suggests that PEVs will predominately grow in the coastal (West Coast and

[40] The Brookings Institution, "Plug-in Electric Vehicles 2008: What Role for Washington," June 2008, pg. 39
[41] Some of the material presented in this section was developed for the Reliability Impacts of Climate Change Initiatives Task Force report: http://www.nerc.com/filez/riccitf.html
[42] American Clean Energy and Security Act of 2009, pg. 99

Northeast) regions and large urban areas in North America, expecting almost one million vehicles in ten years.[43]

Advanced metering solutions, when implemented at scale, can increase the efficiency of battery recharging and discharging of electric-powered vehicles by signaling the most effective timing for either action. These metering applications, though, have not yet been widely deployed. Among other factors slowing PEV penetration are:

- distribution system infrastructure requirements;
- long cycle for the renewal of the automotive fleet—17 years;
- high cost of PEVs when compared with standard internal combustion cars;
- large deployment requirements of AMI to control charging times;
- significant cost and innovation requirements to improve electric batteries;
- uncertainty in preferred battery technology (e.g., lithium-ion versus nickel-metal hydride);
- modifications to home electrical systems; and
- development of requisite standards between automobile manufacturers and electrical building code authorities.

If the charge and discharge timing is controlled locally and without significant distribution infrastructure upgrades, electric transportation will have minimal bulk power system impact. If there is widespread adoption of this technology where major distribution upgrades are made and the supply and demand can be centrally controlled by bulk power system operators, then bulk power system planners must seriously consider the impact of electric transportation.

That said, PEVs could result in efficient use of generation capacity due to the vehicle-to-grid (V2G) system, as studied in detail by the Pacific Northwest National Laboratory (PNNL). In this system, PEVs act as energy storage in regions where renewable resources are available during off-peak hours. Electricity flows to the grid at peak usage time and the flow reverses back to the PEVs at nighttime, when more wind-generated energy is typically available. PNNL estimates this off-peak capacity could power more than 70 percent of the overall light-duty vehicle fleet in the U.S.[44] The total effect on reliability will be to stabilize power quality and the grid overall by balancing the voltage in the grid. However, V2G technology will not be commercially available to enable full integration into the grid for another 10 to 20 years.[45] In the near term, managed charging of PEVs, coordinated among megawatts of charging load, could help provide ancillary

[43] http://www.isorto.org/atf/cf/%7B5B4E85C6-7EAC-40A0-8DC3-003829518EBD%7D/IRC_Report_Assessment_of_Plug-in_Electric_Vehicle_Integration_with_ISO-RTO_Systems_03232010.pdf

[44] Pacific Northwest National Laboratory, "*Potential Impacts of High Penetration of Plug-in Hybrid Vehicles on the U.S. Power Grid*," June 2007

[45] Ibid. pg. 42

services or emergency reliability services.[46] Vehicle-to-grid electrical storage can provide multiple benefits, namely capacity, dynamic, and strategic benefits. The capacity benefit results from the ability to delay or circumvent supplementary central peaking capacity, transmission, or distribution. Operational reliability benefits could be realized by improving load following and spinning reserve and regulating frequency, voltage, and power factor. These characteristics can also support the system operator's ability to stabilize the variability of wind generation, increasing the dispatchability of renewable generation.

Some of the challenges to the reliability of the bulk power system from large-scale deployments of PEVs include significant changes to distribution system architectures to support two-way flows of energy (e.g., communications, protection systems, etc.). In aggregate, multiple injections from energy sources onto the bulk power system must be visible and dispatchable by the system operator to ensure reliability. Security considerations for electric transport loads will continue to grow over time and will become important when significant customer demand management capacity is being aggregated. It is important that communication interfaces between the residential, commercial, and industrial customers' energy management systems and the grid take into account access-control, privacy, authorization, authentication, confidentiality, integrity, availability, and non-repudiation.

Distribution System — Developing Systems

The following systems now under development can affect bulk power system reliability.

Home Area Network

The conventional definition of Home Area Network (HAN) states that it is comprised of linkages to the homeowner's various systems, computers, devices, and appliances. These can be telephones, VCRs, furnaces, air conditioning, video games, and home security systems. This network can then be used to help homeowners manage their equipment and energy costs more effectively. This type of HAN network or system is connected to the grid through an organization, or through and controlled by an intermediary such as a wireless connection. HANs are not new, though they are not yet in widespread use. New types of smart meters and smart transformers will be brought to market—and quickly. If utilities can secure the necessary wide-area situational awareness desired there might come a time when individual smart meters are redundant. Though several versions of upgraded smart meters are now in the market, manufacturers will look for strategies to keep these devices and their information flow at the homeowner level as e-billings can be affected. The deployed footprint of smart meters will make change-out expensive and problematic with so many units deployed today and millions more being installed monthly. These HAN systems units are here to stay for the foreseeable future.
The educational curve consumers are undergoing will eventually take shape in the form of serious customer demand management. The remote communications and control of the HAN devices are, by themselves, not a threat to the bulk power system. Security considerations for

[46] http://www.isorto.org/atf/cf/%7B5B4E85C6-7EAC-40A0-8DC3-003829518EBD%7D/IRC_Report_Assessment_of_Plug-in_Electric_Vehicle_Integration_with_ISO-RTO_Systems_03232010.pdf

HANs will continue to grow over time and will become important when customer implementations expand and the information demand increases. The threat to the bulk power system comes in the form of cyber attackers or system malfunctions enlisting many such devices for denial of service, shut down, or activation. Large scale swings in power shifts could impact substation operation and could cause instability on the bulk power system. HANs are an emerging technology and their impact on the reliability of the bulk power system would be aggregated activity, as observed on the bulk power system. HAN devices are the most vulnerable to cyber security concerns since they are outside the control of an organization. If one home or several homes connected to one transformer were to be compromised, this would not affect the bulk power system. But if the cyber attacker were able to manipulate thousands of homes together and turn off all their power at once using denial of service or other forms of malware, the reliability of the bulk power system would be affected. It is important that communication interfaces between the residential, commercial, and industrial customers' energy management systems and the grid take into account access-control, privacy, authorization, authentication, confidentiality, integrity, availability, and non-repudiation. Ensuring that robust meaningful cyber security is built into the Smart Meters used in Home Area Networks will be vital to avoiding serious threat to the bulk power system reliability. Equally, ensuring that Smart Transformers are eventually installed will provide utilities the home-by-home and neighborhood monitoring, measurement and, later, control of energy consumption at the local level with security that is more robust and with privacy built in.

Industrial Automation Systems

Industrial Automation Systems are systems installed in manufacturing facilities to control industrial manufacturing processes. These systems consist of Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs) along with a wide variety of instrumentation. They also include a variety of other systems such as supervisory control and information reporting systems. Industrial automation systems are widely used for managing and controlling the energy production and consumption within industrial processes. This includes controlling on-site cogeneration power plants and waste-heat turbines. One of the key elements of smart grid is to enable customer participation and accommodate all generation and storage options. This is outlined in the report entitled *DOE Smart Grid System Report – Characteristics of the Smart Grid*, July 2009. Although industrial automation systems are primarily isolated from the grid, these systems currently interact with the grid and enable large industrial facilities to act as both a source of generation capacity and load reduction. They differ from residential and commercial systems in that they are larger in size and fewer in number. This results in the scenario where a small number of industrial facilities can have a large impact on the bulk power system. This trend will increase in the years ahead.

Industrial generation directly affects the distribution grid. As industrial generation expands and aggregates into larger sources of energy, it may affect the bulk power system. It is important to plan for this scenario. New industrial automation systems may expand the participation of industrial customers in both reducing demand as well as exporting generation. This generation capability could have a direct impact on the bulk power system. Power flow into the distribution network will vary over time and needs to be monitored and factored into grid operations. It is recommended that an intelligent grid interface be defined for industrial customer-sited equipment that exports power to the grid. This interface would provide an organization or

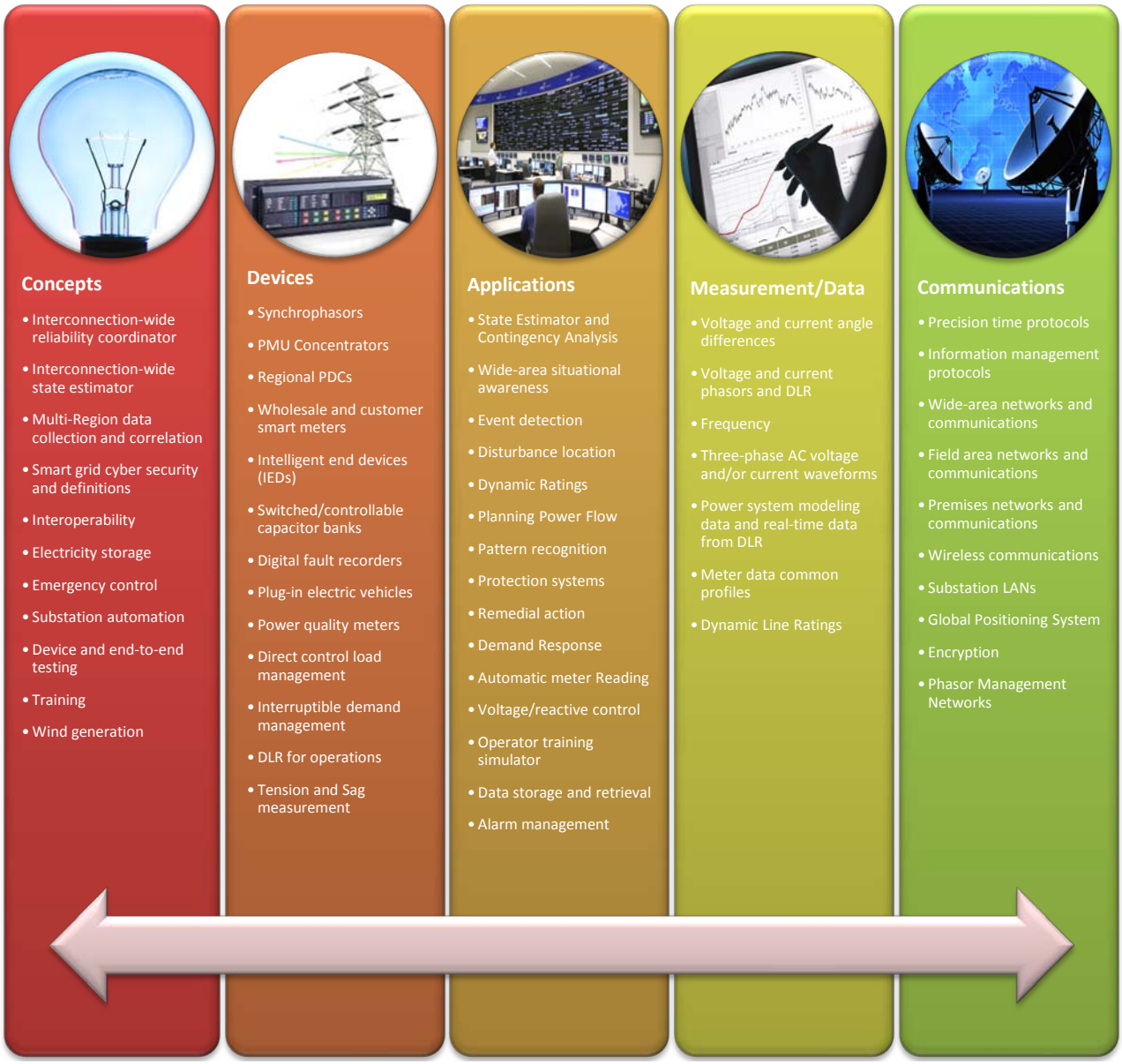
aggregator with valuable information concerning the state of the exported generation in real-time, along with the potential capability to island the generation under fault conditions.

A large enough number of centrally controlled industry control systems could affect the reliability of the bulk power system. Security considerations for the bulk power system are important today but will become critical as more and more industrial generation capacity is exported or aggregated. Maintaining cyber security at the substation level will be important. In addition, all communication interfaces between the industrial customer's energy management systems and the grid should take into account access-control, authorization, authentication, confidentiality, integrity, availability, and non-repudiation.

Chapter Findings

Table 2 below summarizes many of the technologies discussed in this chapter, identifying planning and operational considerations and potential impacts of smart grid technology integration on the bulk power system.

Table 2: Smart Grid High-Probability Impacts



Integrating smart grid devices and systems on the distribution system can change its static and dynamic characteristics. Successful integration of smart grid systems and devices should consider and address bulk power system reliability considerations resulting from these changes.

Further, bulk power system operators will need increased visibility and dispatchability as smart grid innovations change the character of distribution systems

The availability of reliable electric energy affects nearly every aspect of modern society. As reliance upon the system for delivering electric energy continues to grow, "smart grid" has begun to mean a modernized power system. These global and domestic challenges include climate change, increased energy independence and security, and providing reliable and sufficient electric energy. Driving this vision to reality will require increased investments in research and development to enable the systems and technologies for the future bulk power system.[47] If the vision of a more technologically advanced grid is to be realized, there must be a public and private investment in a robust and vibrant research, development, innovation, and commercialization infrastructure.

[47] "Electricity Technology Roadmap, 2003 Summary and Synthesis," EPRI, 2003

4. Planning and Operations with Smart Grid

Introduction

The projected advances in smart grid devices and systems potentially present new options to maintaining system reliability. However, the migration of control and data to the individual customer level could present new risks and opportunities to mitigate those risks. Historically, interconnected power systems have been controlled and monitored centrally through rigorous processes and measurements in order to maintain the highest levels of overall system reliability. The smart grid will rely on more distributed intelligence, not just geographically, but through multiple levels of the system. The increase in information and intelligence can provide a vehicle for enhancing bulk power system control while introducing new modes of operation.

That said, these implementations must be completed with a full understanding of their consequences to the reliability of the bulk power system. As smart grid devices and systems are deployed, reliability issues must be studied so that they are appropriately considered by the organizations installing them, as well as by the policymakers and regulators who are regulating and requiring their installations.

With advances in smart grid technology, unprecedented evolution to levels of system control and measurement may be available. Interactions among smart grid devices and systems are unknown, and careful planning of their integration can prevent any undesired interactions from causing reliability considerations.

Bulk Power System Reliability Risks

The impact of smart grid on the reliability of the bulk power system has yet to be experienced. Integration of smart grid devices and systems will change the way the bulk power system is planned and operated. The expansive and rapidly evolving nature of smart grid will require vigilance from all stakeholders to manage system reliability considerations, such as:

- cyber security;
- increased complexity;
- grid stability as the system characteristics and control systems are changed;
- close coordination of both intra- and inter-balancing areas to ensure close synchronization of control system development and deployment;
- operational security to ensure graceful degradation of the bulk power system to a reliable operating state if IT system vulnerabilities are detected and/or disabled;
- architecture that is neither small nor simple;
- not knowing if each component can fail safely and still allow availability;
- not knowing, much less understanding, existing and evolving risk vectors;

- not fully understanding the functionality of each component being used;
- inability to control the environment or physical access to components;
- inability to adequately monitor each component;
- single points of failure;
- diverse and discrete deployment; and
- new assumptions, processes, and ways of thinking for all parties.

Four fundamental components of the smart grid infrastructure, besides the availability of smart grid technologies, are interoperability, communications, intelligent systems, and information technology systems. Technology interoperability standards will enable the addition of different technologies than those available today, making it easy to add functionality and innovative electric products and services, though they represent a potential vulnerability. From a bulk system perspective, data and information are gathered from multiple locations from energy users, distribution systems, transmission, and generation. Every second, the bulk power system can adjust to accommodate dynamic changes in energy users' behavior and the status of countless pieces system equipment.

However, many of the control systems for smart grid technologies have been designed for local control and are not resilient to errors from miscommunications or IT errors. As mentioned before, successful integration of smart grid devices and systems should address potential reliability considerations from IT systems and communications with the existing control systems:

- First, control systems must be improved to provide robust protection from IT and communication vulnerabilities.
- Second, new tools and analysis techniques will be required to design and manage the deployment of broad-scale smart control systems across the bulk power system.

As it is a large non-linear system, the ramifications and design of smart grid on control systems must be modeled, simulated, and designed to ensure that the expected performance improvements will be realized. Successful integration must consider bulk power system reliability, such as transient and long-term stability, small signal stability, voltage stability, or component design issues such as short circuit considerations.

These challenges will require changes in the way the system is currently planned and operated. Assessing these impacts will require new planning and operations tools to manage the reliability of the bulk power system. The next section provides an example of scenario planning as a way to determine the penetration levels and requisite assessments.

Planning for Smart Grid Uncertainty: Example from Southern California Edison

Southern California Edison (SCE) has developed scenario planning as part of its strategy for ensuring success in achieving its smart grid vision.[48] SCE's scenario planning efforts have resulted in the development of four potential pathways for the pace of technology development and adoption of the smart grid. The scenarios were created following a careful analysis of the critical driving forces affecting the smart grid. After making some assumptions on the degree of impact (positive or negative) that these forces might have on the pace of technology development and adoption, the following driving forces were considered:

- economic growth;
- policy focus;
- technology innovation and adoption;
- energy markets;
- customer trends; and
- environmental developments.

The goal of scenario development is not to identify the most likely future, but to examine how external forces may shape smart grid deployment through 2020 and beyond. The characteristics of the resulting scenarios are used by SCE to prioritize and select smart grid technology projects. The smart grid future scenarios were developed by considering a spectrum of two of the most critical driving forces—Economic Growth and Policy Driven Innovation—placed along the horizontal and vertical axes in Figure 4.

These four scenarios are defined as follows:

- **Slow and Steady**: Policymakers continue to support industry investment in smart grid development and implementation. Progress toward energy and climate policy goals continues, but is slowed by economic forces.
- **Light Speed**: Policymakers issue mandates for industry investment in smart grid deployment and provide financial support for technology innovation. A "clean tech" investment boom spurs technology innovation and development.
- **Market Driven**: Policymakers shift emphasis toward market-driven outcomes for technology innovation and infrastructure investment. Strong economic growth and potential new market opportunities encourage new entrants into the energy market.
- **Keep the Lights On**: Continued economic stagnation squeezes consumers and industry, slowing venture and industry investment as well as decreasing innovation in smart grid technologies. Lower energy demand and regulatory focus on rate containment reduces funding available for additional smart grid investment.

[48] www.sce.com/smartgrid

Figure 4: Smart grid future scenarios (developed by Southern California Edison)

Across each of the four scenarios, SCE identified potential data points as "signposts" that would suggest the extent of progression into one or more different pathways over time, such as:

- the U.S. national unemployment rate (expressed as a percentage);
- average gasoline prices ($/gal);
- average natural gas prices (per million BTU);
- distributed resource cost effectiveness;
- consumer adoption rates for energy smart devices;
- consumer adoption of electric vehicles;
- customer response to dynamic pricing and usage information;
- U.S. economic GDP growth (as a percentage increase or decrease);
- annual clean technology venture capital investment; and
- industry and government investment in related technology R&D.

Regularly monitoring of these signposts can help determine whether there is movement in the direction of one or more of the developed scenarios, or if entirely new scenarios are emerging. This assessment provides input into the planning horizons and requisite analysis for successful integration of smart grid devices and systems.

Planning and Operations Horizons

This chapter assesses effects that smart grid devices and systems can have on the planning and operations horizons identified below:[49]

- **Long-term planning** — Planning horizon is for one year or longer. The concepts used in this time horizon will be altered as smart grid components and systems are integrated into the planning process. Integration of smart grid systems and devices will require maintenance and equipment replacement practices to account for new technologies and introduce new capital spending patterns, and will add new, non-traditional parties to operations.

- **Operations planning** — Operating and resource preparations used from day-ahead up to, and including, the upcoming seasonal plans. Integration of Smart grid systems and devices will both add and relieve stresses on the system that need to be monitored and accounted.

- **Same-day operations** — Routine actions and preparations required within the timeframe of a day, but not real-time. These operations will change as enhanced tools are incorporated into system operations.

- **Real-time operations** — Actions required within no more than one hour to preserve the reliability of the bulk power system. Real-time operations could change as new failure modes may be introduced and new ways of interacting with the grid on a collective basis (e.g., reacting to diverse and distributed actions occurring simultaneously).

- **Post-Operations Assessments** — Follow-up evaluations and reporting are used to assess experience from actual system operations. These assessments of the bulk power system will require change in conventional views of contingencies.

[49] http://www.nerc.com/files/Time_Horizons.pdf

Long-Term Planning — Power System Considerations

Advancing System Optimization and Efficiency

Current planning and operating practices result from over a century of experience and have worked well under the assumptions implied in their design. However, depending on the extent of deployment and smart grid devices and systems evolution, new approaches may be needed to support their integration, while maintaining bulk power system reliability. For example:

1. **Stochastic Optimization in Support of Enabling Reliable Integration of Variable Resources** — Probabilistic-based optimization methods and software focused on enhancing efficiency are needed to support integration of variable resources.[50] Current industry approaches consider deterministic uncertainty—for example the "N-1 criterion"—based on thermal generators and transmission system on-off characteristics. This may be unsuitable for variable energy resources, whose power output follows the pattern of their fuel availability. However, the conditional and sequential nature of availability of this generation is more certain as the timeframe is shorter. This will require a wider notion of risk to complement or advance industry's use of Loss-of-Load-Probability.
2. **Optimization of Inter-Control Area Resources** — Coordinated management of balancing areas could contribute significantly to increased, near-optimal use of resources at the regional (not necessarily NERC Region) and inter-regional levels, while preserving bulk power system reliability.
3. **Corrective Actions for Enhancing System Performance** — Relying on corrective actions instead of preventive control must consider impacts on the reliability of the bulk power system.
4. **Integrating Near-Real-Time Synchrophasor Measurements and Dynamic Line Ratings into Optimization Methods** — The information available from synchrophasors can be used in decision-making to reliably operate the system. Modeling and decision tools that use this technology and support implementation of key optimization results will need to be conceptualized, simulated, and ultimately deployed.

Effects of New Technology

Depending on regional availability, future electric energy systems may have large amounts of variable resources and demand response. Integration of these technologies will require careful planning and new tools to ensure the reliability of the bulk power system. For example, there are potential technical challenges that may occur at different time scales, ranging from split-second to more pronounced inter-area oscillations (0.1 to 1.0 hertz), as well as much slower frequency deviations caused by insufficient regulation in response to hard-to-predict power imbalances. It is likely that the effects of new technology on system stability will reduce their penetration, unless new methods and tools are developed such as next-generation frequency and voltage control methods.

[50] http://www.nerc.com/files/IVGTF_Report_041609.pdf

Synchrophasor measurements can provide early indications of reliability considerations to enable operator action in near real-time. More work is needed to formalize the placement and use of such measurements for predicting system behavior, such as dominant inter-area oscillations. Moreover, these new measurements and requisite communications should be considered for fast protection and control loops to manage bulk power system conditions in near real-time. Not only will synchrophasor measurements be used to analyze possible reliability concerns, the operator will need to be equipped with actionable advice to support reliability. The role of network phasor dynamics usually assumed to be instantaneous in today's power flow models used by the system operators will have to be assessed.

Finally, the potential for harmonic resonance in future electric power networks with large numbers of smart grid devices and systems will need study. This resonance results from the presence of harmonics somewhere else in an electric power network, which is amplified at the location where it is created. This resonance can cause equipment damage and system instability. Given the complexity of potential frequency, voltage regulation and harmonic instability problems, assessment of the modeling, analysis, and control and protection tools are essential for successful integration of smart grid devices and systems.

Modeling and Simulation Requirements

Systematic models need to be introduced to capture the effects of responsive demand and various distributed variable resources on system stability. The new models must account for predictions, effects of many actions by the small system users, as well as the effects of near real-time communications and control. Very complex distributed closed-loop systems, interacting internally within a control area and coordinated by the system operators, as well as the dynamics of WAMS-enabled monitoring and control across control areas, should be modeled. Given what is known at present, this is a major undertaking.

As real-time information, analysis, and control capabilities are integrated into the bulk power system, a widely shared view is that the system will become more and more automated and reconfigurable. This smart grid will also be inherently more complex incorporating distributed computing and communication functionalities. In this context, following are some challenges that could emerge:

1. Assessing the impact of smart grids resources on real-time operations using long-term, minute-to-minute load-flow patterns from historical operational data
2. Understanding and optimizing interactions between automated control and dispatcher actions
3. Investigating issues of distributed computing, data sharing, communication system capacity, and reliability
4. Assessing the benefits of more automation (i.e., "closing the loop")

Addressing these issues requires new simulation tools built on a power grid model that focuses on real-time control and related communication of information among entities that share the operation of the power grid. Existing software focuses on planning and market issues. Current

state-of-the-art studies rely on statistical methods and other *ad-hoc* tools to assess operational impacts of non-dispatchable resources. However, there are aspects of system operations that are difficult to model statistically or mathematically, such as resource limits, energy market dispatch ramping limits, regulating reserve dispatch ramping limits, etc.

Therefore, operational impact studies should combine a transmission grid representation with a distributed agent-based control architecture.[51] They should also involve a playback of historical state-estimator scenarios for several years to assess system control performance indicators (control performance standards such as CPS1 and CPS2), tie flows and operating transfer capability violations, and actual counts of generator or discrete shunt component start/stop activity to assist in evaluating appropriate mitigation solutions. The inclusion of new device technologies will require *both* new component and system models. The development of component models should be based upon their performance under rigorous testing and be measured with respect to physical impacts. High voltage transmission systems and their energy management systems (EMS) can potentially benefit from synchrophasors and high-resolution measurements. However, at the medium- to low-voltage distribution system levels, the installed and anticipated metering systems will not be synchronized and time-stamping quality will vary. Thus, to coordinate EMS and distribution management system (DMS) operations, models are needed to capture and predict behavior of power systems. This will require detailed component models of new and existing power hardware and control devices, and stochastic modeling coupled with deterministic system metrics.

For example, storage technologies may be an increasingly important application, including those explicitly meant for storage (e.g., batteries, compressed air, etc.) and those that indirectly serve this function (e.g., plug-in electric vehicles). Further, with the increased adoption of wide-area-based control and protection in the system, it is imperative to develop suitable publically available models for these control and protection schemes.

In developing the requisite models for planning and operations, sufficient flexibility will be required for user-specific options. Further, the models will require the ability to account for communication delays and provide features to represent the latency in time measurement and communicating wide-area signals to control and protection apparatus. With the inclusion of such devices, operation and planning criteria would also need to be revisited, as these devices could be critical in maintaining the reliability of the system, and the misoperation or failure of such devices could result in serious consequences.

New Reliability Tools

Current reliability engineering tools, although effective for today's electric power systems, cannot thoroughly capture the affect of integrating smart technologies. As the reliance on communication and control increases, systems can be operated closer to their physical limits to increase asset efficiency, although this potentially makes them vulnerable to system and device defects/attacks/failures. In conventional reliability analysis, it is usually assumed that component failures are unaffected by the evolution of system dynamics. This assumption needs to be

[51] http://www.osti.gov/bridge/product.biblio.jsp?osti_id=810936

revisited and appropriate modeling tools need to be developed to capture the effects of system dynamics on each individual component and, alternatively, how the stress of individual components affects system dynamics. Another example is the increased uncertainty in system behavior caused by any uncontrolled and unpredictable change on the demand or supply side of an electrical energy system, e.g., generation based on variable energy resources such as solar or wind. Although operational uncertainty is not at all new to electric power systems, its extension to a significant portion of the generation capacity caused by the increased penetration of renewable energy resources creates significant uncertainty.

The challenges ahead for developing systematic analytical tools that can properly model the impact of new technology integration include:

- coupling between cyber and physical components;
- coupling between system dynamics and component stress; and
- uncontrolled and unpredictable changes to demand and supply.

Developing Appropriate Performance Metrics

One of the key differentiating features of existing operating and planning T&D objectives, and the objectives of future smart grids, is to add new performance objectives driven by regulatory rules. For example, policies favoring efficiency over environmental impacts will require deployment of a qualitatively different smart grid than policies that favor environmental impacts over efficiency. Ensuring reliability and security may require different performance measures, depending on the regulatory rules concerning responsibilities for managing uncertain demand and supply.

The DOE 2009 report[52] presented 20 metrics in the areas of coordination, distributed resources, delivery infrastructure, and information networks to measure the progress of a modernizing grid characterized by the following:

1. enabling informed participation by customers;
2. accommodating all generation and storage options;
3. enabling new products, services, and markets;
4. providing the power quality for the range of needs;
5. optimizing asset use and operating efficiently; and
6. operating resiliently in the face of disturbances, attacks, and natural disasters.

The proposed metrics that support the bulk power system resilience (the sixth characteristic above) measure the degrees of implementation in real-time data sharing (moderately mature), grid-responsive load (nascent), delivery reliability (mature), advanced sensors (immature), and cyber security (moderately mature).

[52] Smart Grid System Report, U.S. Department of Energy, July 2009

The recent set of NERC metrics[53] are defined in relation to the Adequate Level of Reliability (ALR). All but one (planning reserve margin) are *post-facto* results based on undesired outcomes. It may also be desirable to establish metrics for quantifying the cyber security parameters for future systems as a way to manage risks.

Smart grid technologies can provide higher resolution data, both in time and location. This is critical to improve system performance as smart grid is integrated. Much can be done in terms of performance and risk management as more data become available. With this information, stochastic control and risk assessment can provide new insights into the risks to the reliability of the bulk power system.

Load Forecasting Under Greater Uncertainty

The net real power and power factor seen by the bulk power system at the interconnection with smart distribution systems may be different than past experience. The AMI-enabled responsive customers, load aggregators, and distributed generation will be equipped with sensing and automation that can create qualitatively different load characteristics. If such efforts result in larger-scale deployment of variable resources, these deployments must be coordinated. It is critical to understand the degree and types of complexities brought about through embedding of different technologies on today's grid, ensuring bulk power system operators do not lose system visibility and controllability.

Improved distribution system modeling will be needed to yield improved understanding of distribution level impacts on the bulk power system. As the penetration of distribution-connected distributed generation resources increase, there will be a greater need to transport these resources to various load locations in the system. In North America, most distribution systems at the secondary level are radial. To facilitate effective use of the distributed resources and enhance the redundancy of the system with increased penetration of such resources, one potential operation is to consider new architecture for networked distribution.

Assessments should include new sensitivity assessments. For example, supplementing (N-1) contingency analysis for bulk power systems with select load disturbances may also be needed. These load disturbances will not just represent a loss of one bus, but regional changes in distributed energy resources (e.g., aggregated based on weather forecasts, etc.). This category of disturbances and contingencies should also include both significant increases and decreases in load, along with associated dynamic stability and system regulation considerations.

Distributed Resources, Microgrids, and Integrating Renewable Resources

Large amounts of variable energy resources, such as wind power plants and photovoltaics in particular, are creating a need for new modeling, analyses, and simulation. A more detailed inclusion of PV and wind-based distributed generation is called for when completing system studies to examine their impact on system voltage performance for varying degrees of

[53] 2010 Annual Report on Bulk Power System Reliability Metrics, NERC, 2010: http://www.nerc.com/docs/pc/rmwg/RMWG_AnnualReport6.1.pdf

penetration at light loads. To integrate large amounts of variable generation, understanding, modeling, and controlling, voltage dynamics will become an important planning and operational challenge. Finally, as the role of power electronics used to switch control of unconventional distributed resources increases, there is a likewise concern for introduction of high levels of harmonics, which can damage equipment and disrupt load.

Understanding interconnection and reliability requirements is important to support variable resource integration. For example, with the injection of new power resources into the grid, the voltage angles will adjust to account for the new injection as a result of which synchronizing power coefficients and, therefore, the total inertia will reduce. With this understanding, a number of options to counter this reduction should be explored. One option—adding advanced power electronics—can be used to synthesize inertial and frequency response, supporting higher penetration levels of variable generation. This would have a direct impact on damping of critical modes of oscillation in the system and supporting the reliability of the bulk power system.

With increased penetration of distributed rooftop or PV-based solar generation, there could be significant impact on reactive control capability of the system, especially at light loads. Most rooftop or PV-based solar generation will have inverters that are not designed to provide reactive support. Detailed inclusion of PV-based distributed generation into system studies will enable an assessment of their impact on system voltage performance and exploration of options required to support integration and maintenance of bulk power system reliability.

A number of protection system design challenges are introduced with increased integration of renewable resources. For example:

- protection system design complexity associated with renewable resources may provide little or no short circuit contribution to the system;
- the time-voltage requirement for low voltage ride-through of wind generation creates issues with protection system clearing times; in particular, the potential need for redundant high-speed protection and challenges associated with meeting clearing time requirements for breaker failure protection. These concerns are further complicated by unavailability of adequate models, although the issue of sufficient models is not limited to protection system concerns; or
- integration of distributed and renewable resources, particularly when multi-terminal lines are used, creates the need for increased communication bandwidth for high-speed fault clearing. The need for faster fault clearing increases vulnerability of protection systems to operate for stable swings. High-speed protection systems must be capable of identifying fast swings that may be detected as faults.

Control System Architecture

The technology of emerging smart devices, which give bulk power system operators increased sensor and actuator fidelity, may be less rugged than traditional grid sensors and actuators. This is inherent in the technology transition. For example, there are fully functional analog voltage meters still in service that may have been installed prior to when the first transistor was invented. There is simply no real service life history for complex integrated circuits, which have only existed for the last four decades or so, when compared with the century of service for some of

the analog devices used to sense grid status. The rapid introduction and deployment of smart grid technologies means the complexity of grid control systems is also rapidly increasing. While having clear benefits in the areas of grid planning, reliability, and efficiency, these system changes also inherently increase system vulnerabilities.

A fundamental attribute of most existing control systems is that they generally use hierarchical architecture rather than distributed architecture. Aside from automatic, self-preservation actions, field devices have little if any decision-making ability when viewed from a substation perspective. Most substations today operate in a similar manner. They have some local decision-making capability based on their limited view of the grid, but for broader, coordinated actions they typically rely on higher-echelon systems, whether automated or manual, at a control room.

Reliable hierarchical control is yet another consideration. Much discussion on cyber security is focused on the legitimate risks of an outsider circumventing the security systems around a control room and initiating malicious actions in the bulk power system. There is also the persistent concern over whether disgruntled insiders may take similar actions. Similarly as important from a planning perspective, is consideration of accidental or inadvertent improper commands being sent to a substation or field devices. In reality, reducing the potential impact of these inadvertent actions has significant benefit when considering the potential for intentional and malicious actions by internal or external attackers. This is because the purpose of most external attacks is to circumvent security systems in order to have the same control over the bulk power system as the internal, approved system operators.

It is the combination of today's hierarchical control architecture, coupled with the high likelihood that there will be a loss of reliable hierarchical control, that drives the requirement for more distributed bulk power system control architecture. Going forward, bulk power system design may migrate to a more distributed sensor and control architecture.

Instrumentation, Control, and Protection Systems Impacts

Some key enablers of the smart grid in the protection area will be driven by two factors: synchrophasors and merging units (e.g., IEC61850 process bus). As synchrophasor technology becomes more prevalent, they are becoming more integrated into wide-area protection and control schemes to arm or disarm protection modes. Merging units could revolutionize protection within the substation. Initially, they will reduce the physical wiring and transform protection logic from hard-wired to software logic-based. Eventually, protection methods may be simplified by using digital schemes for adaptive relays.

That said, the introduction of more systems presents several reliability concerns that include the following:

- the potential for greater dependence on communications systems in protection and control system design requires higher reliability of communication systems;
- increased application of power electronic devices on the system will increase the need to assess the behavior of protective relays in the presence of harmonics and switching transients;

- increased use of software enlarges the vulnerability to errors in development, application, and installation;
- the use of protection devices with new settings and programming capability should be weighed against the added complexity of programming and the inherent increased likelihood of misoperations; and
- wide- and local-area islanding schemes, including portions of the system with high concentration of distributed generation, may require voltage and reactive power management within the island, including coordination of distributed generation and existing transmission and distribution controls.

i. Control Systems

Supervisory Control and Data Acquisition (SCADA) refers to the sensing, monitoring, and control systems for operating geographically-dispersed systems such as the power grid. In the case of the grid, much of this consists of providing measurements back to system control centers, and providing the ability to command critical breakers. Most of this is "open-loop" control. The application of closed-loop control is prevalent in the generating stations, with some advanced control applications such as model predictive control and sliding mode control, and including the generator controls, not only voltage (exciter) and frequency (speed) control, but also power system stabilizers (PSS). On the broader bulk power system, closed-loop control is, for the most part, limited to automatic generation control (AGC), based on system frequency and economic dispatch.

As faster and more accurate measurements, such as phasor measurement units (PMUs), become prevalent and grid operation becomes increasingly dynamic due to greater penetration of distributed and variable resources, potentially diminishing frequency response, longer distance bulk power transfers, and more complex and dynamic markets, there will be growing interest in closed-loop control. Closed-loop control also includes visualization and human interaction. In the smart grid, real-time information will multiply, while the grid itself continues to become only larger and more complex. How grid operators process and respond to this information will require a fresh look at engineering and human factors: visualization systems for presenting information, new ways to manage alarms and abnormal events, decision support systems for distilling information to actionable decisions, and training methods and systems.

As mentioned before, it is critically important that defense mechanisms are built into protection and control devices and systems to prevent both the deliberate or inadvertent modification of applications, settings, or data to cause harm or misoperation of the bulk power system.

ii. Protection and Fault Management Systems

Protection, as the name suggests, has long been primarily concerned with preventing damage to power system generation and delivery assets due to abnormal events causing electrical conditions outside the bounds within which the equipment is designed to perform.

Power system protection has primarily been accomplished in a localized fashion with electromechanical and digital relays. Special protection systems (SPSs) and remedial action schemes (RAS) are used and are customized to the particular application, to provide coordinated action over a larger area to detect particular combinations of circumstances thereby avoiding or lessening the severity of faults or equipment outages. Wide-area protection can locate and isolate faults in a system using information from multiple protection devices while keeping as much of the unfaulted portions of the system in service as possible. When a fault or major excursion occurs on the power system, mitigating action must occur very quickly—local protective devices typically act within a few cycles.

A smarter grid can increase the sophistication of protection schemes, particularly wide-area and special protection schemes that take advantage of multiple measurement and protection devices. Development of models and approaches for layered protection schemes is essential, so when more sophisticated schemes fail due, for example, to communications failure, local schemes still perform properly and bulk power system reliability is maintained. It is also possible for wide-area protection schemes to provide a backup, albeit slower, for failed local protection. However, increased use of software intensifies the vulnerability to errors in development, application, and installation.

It will be increasingly important to develop reliable simulation-based methods for testing smarter, more sophisticated, bulk power system protection schemes. Protection functions are currently implemented in relays, as distinct pieces of hardware, but with IEC 61850, they may become "functions" running on a suite of substation computers. Useful approaches may be adapted from established defense industry practices in verification, validation, and accreditation. Beyond just the protection of generation and delivery system assets, a smarter grid will require a new focus on fault limiting and fault management, including substantially reduced reaction times (e.g., on the order of 1/8 cycle) in interrupting or limiting fault energy, and sophisticated schemes for fault isolation and rerouting of energy to maintain power to the load.

Power system equipment must be sized to handle the maximum available fault current that may pass through it before devices such as breakers can interrupt the flow of energy. These very high current flows for very short duration can result in large damaging electromotive forces. Therefore, equipment must be designed structurally to handle these forces even though they are many times greater than what equipment and conductors would normally experience.

Solid-state and superconducting fault current limiting (FCL) devices, which can act much faster than the traditional widely deployed interrupting devices, offer a great deal of new flexibility in design of the power system. Though FCL devices are expensive and not widely used, they can substantially reduce the cost of downstream equipment and conductors, by reducing the necessary "withstand" current ratings. Use of FCLs has implications for the protective relays as well as possibly affecting the operation of protection devices. Therefore, the devices must be able to adapt their settings in the event of a fault current limiter action.

Fault management assumes faults will occur and, not only is it important to quickly isolate them or limit the resulting current flow, but also to maintain power to critical loads (survivability) by optimal rapid rerouting of energy without adverse affects to healthy parts of the system. Current protection practices require complete analysis of the expected system conditions or operating modes. Smart grid will introduce a large number of distributed devices that include sources of energy (PEV, EV, DG, PV, etc.) that are autonomously operating. It will become difficult to protect the equipment of such a system with traditional protection methods, requiring new approaches to support their integration.

Power Quality

Power quality is considered a measure of end-user quality that is indicative of upstream and downstream events and operations. Power quality monitoring, even when deployed at the customer interface, can provide intelligence and data on how the bulk power system is operating. It can give notice of grid disturbances and can be used to locate faults. To be most effective in analyzing grid disturbances, periodic data collection, aggregation, and analysis programs are needed to show the correlation amongst the various events. Power quality monitoring can quite easily identify faults on radial systems; however, the communications need to be periodic or on-demand to provide effective information. Since power quality monitoring is typically deployed at customer locations, one monitor alone is not sufficient to determine fault locations on the bulk power system. Power quality monitoring can also help identify equipment problems. After correlation of power quality disturbances to known events, the uncorrelated disturbances can be analyzed to determine if they are caused by equipment that is beginning to fail, which might otherwise go unnoticed.

Planners will need to be mindful of the potential for harmonic and flicker issues being created by the deployment of smart grid devices. Continued penetration of electronic devices will increase harmonic distortion. Frequent switching of loads in response to smart grid parameters may result in flicker. Flicker and harmonics would be expected to remain on the distribution system due to the robustness of the bulk power system and the transformation between the two systems, though a large aggregation of problems could result in power quality issues on the bulk power system as well. Smart grid devices are not expected to increase the number of faults on the system. Therefore, an increase in voltage sags is not expected.

In terms of “Power Quality” (PQ) impacts, generalizations are difficult because the majority of power quality concerns are either circuit specific, building specific, or load equipment specific. What this means in terms of how the smart grid may impact system-wide power quality is that we must consider only items that may impact either voltage magnitude, voltage waveform shape, or power frequency. Within this context, the smart grid has four basic considerations where a positive or a negative change might be expected in the future. These are the following:

New Load Proliferation Impact — More efficient transformers, advanced motor technologies, and assorted power electronic loads such as LED and electronic lighting, plug-in vehicles, and high-end PCs and gaming systems all have the potential to impact the power system negatively at certain harmonic frequencies. Aside from modeling and simulation for existing problem circuits, there has been no systematic effort to understand the impacts on a national basis. This potential proliferation concern should be monitored over time to watch for

trends such as increased voltage distortion (the smart grid-metering infrastructure will be able to produce that metric).

Reliability and other PQ metrics — The smart grid-metering infrastructure has the potential to more accurately characterize outage and voltage quality indices. Further, when circuit voltage and current measurements are integrated with other data systems such as weather information, circuit maps, and load flow data, the smart grid can enable trouble and repair crews to respond to system problems more quickly and more location specific.

Increased Localized Generation and Storage Impact — The smart grid will enable better communications and control for local generation and storage. Assuming the systems are properly characterized with modeling and simulation, and properly set up for quick dispatch and/or disconnect, the many benefits of localized distributed resources should be realized, while the potential adverse power quality implications that presently restrict large-scale penetration can be overcome.

Demand Response Impact — The ability to control loads on a large-scale basis requires smart grid communications infrastructure. The ability to take advantage of load control for power quality benefit will require versatility in terms of near real-time load responsiveness all the way out to day-ahead modeling—both of which the smart grid should enable. The overall suite of Demand Response opportunities, ranging from system-wide "conservation voltage reduction" to individual load control, is anticipated to improve overall power quality in terms of power system reliability and voltage waveform shape quality, but there likely will still be some negative impact on single customers or processes with extremely sensitive loads unless they have supplemental power conditioning.

Operations Planning

Operations planning will require much of the modeling considerations mentioned in the *Long-Term Planning* section to maintain reliability. The elements below are in addition to these requirements.

Maintenance

The ability to complete condition-based and preventative maintenance will be enhanced with the upgrade to smart grid. The communications infrastructure necessary to support the data transport of the smart grid devices and systems could provide a convenient opportunity to transmit asset condition- or health-related information to the enterprise for both operations and asset management functions. Through this near real-time information maintenance, the condition of an asset could be assessed to identify maintenance requirements.

System Efficiency

System efficiency is typically not viewed as a reliability issue on the bulk power system. Many view the smart grid concept as a way to increase system efficiency on the overall electric power system, but there are very few definitions as to what that typically means in relation to the many components of the smart grid. When applying the system efficiency concept under smart grid to the bulk power system, effective use of the bulk transmission system is one consideration.

The primary objective of Dynamic Line Rating systems is to enable the use of the additional transfer capability with deterministic safety. Alternatively, as described by CIGRE, "The main purpose of real-time line monitoring is to assist system operators in better use of the load current capacity of overhead lines, ensuring that the regulatory clearances above ground are always met." Many of the proponents of the smart grid would call for the accelerated and expanded use of Dynamic Line Rating systems to improve "system efficiency," which equates to a higher use of the transmission system for a greater percentage of time. Transmission lines are designed to operate up to a maximum permitted conductor temperature that will not harm the conductor and, more importantly, will not cause the conductor to sag below its designed clearance to ground as specified in the National Electrical Safety Code. Reliable Dynamic Line Rating systems ensure that the conductor operates at or under the specified temperature set point. Conductor temperature is the result of a thermodynamic balance between elements that add or remove heat from the conductor. Ambient air temperature, radiation from the sun, and energy losses generated by current flowing in the conductor add heat, while natural radiation (still air) and convective cooling (wind) can remove heat. Wind speed and direction affect line ratings much more than ambient temperature and solar radiation. Further, the random and potentially significant variability of the wind must be taken into consideration by the Dynamic Line Rating system technology for optimum and safe operation. That said, this high use will need to be balanced against the need to ensure that sufficient transmission capacity is available to meet unexpected contingency requirements.

Efficiency also means operating the grid safely at its optimum dispatch. Synchrophasors, which provide voltage and stability information, should be used in conjunction with Dynamic Line

Rating systems, to account for system conditions that affect reliability such as reactive power requirements, balancing, and regulation. The technology considers the highly variable local weather conditions, particularly wind, which affects the line transfer capacity substantially. Dynamic Line Rating systems, complemented with stability information from PMUs, help operate the transmission grid at optimum dispatch, while maintaining reliability.

Same-day Operations

Simplified modeling that supports energy management system models will be required to ensure the system is ready for the forecasted demand and resource levels. The elements below advance this further with additional considerations.

Modes of Operation and System Modeling

A substantial way the system could be impacted by smart grid technologies is in the way it is operated. Shorter timeframes, blurred boundaries between systems, and more reliance on actual data than estimates are key ways in which this may happen. As additional information is available from discrete devices down to and beyond the customer meter, this data can be aggregated to form better load models. These load models can be used to create more-accurate load forecasts. Coupled with advanced algorithms to manage and process large amounts of resulting data, more accurate load forecasts can be calculated to support operator's efforts to ensure reliability.

The distributed nature of demand-side resources requires consideration of the limitations imposed by, and the characteristics of, the distribution networks when using these resources for bulk power system operations. This may be accomplished in a number of ways:

1. Modeling of the distributed resources connected at specific grid locations, (e.g., distribution substations), whose capacity and operating parameters must be adjusted dynamically for each dispatch interval, based on underlying Demand Response programs, Distributed Energy Resource availabilities, and prevailing distribution system limitations such as distribution network congestion, phase balance, etc.
2. Modeling the distribution system is needed, by extending the bulk power network model to include equivalent three-phase models of the distribution grid.
3. The transmission network model should be enhanced with a more detailed model of the distribution grid.

Demand Response

Demand Response resources may provide energy, capacity, and ancillary services in support of bulk power system operations.

1. **Energy** — Energy scheduling and Demand Response resources can be modeled distributed resources depending on the distribution system model.
2. **Capacity** — In most regulatory jurisdictions, Demand Response resources qualify as resources satisfying the Balancing Authority's planning reserve requirements (Resource

Adequacy). Here, capacity will need to be modeled as a function of the available Demand Response resources for the peak hours of the operating day.

3. **Ancillary Services** — FERC Order 719[54] requires that all ISO/RTOs under FERC jurisdiction provide equal opportunity for the provision of ancillary services from Demand Response resources as that provided by conventional generation resources, subject to telemetry, dispatch capabilities, and other infrastructure requirements. Other Balancing Authorities may have their own specific requirements as imposed by local regulatory entities. In general, Demand Response qualifies for the provision of non-spinning (supplemental) reserves. Some jurisdictions allow provision of spinning reserve and/or regulation from Demand Response resources. To model Demand Response for the provision of various ancillary services a number of methods may be employed. The following are examples:

   a. *Grouping of Demand Response resources by their nature for the provision of each of the Ancillary Services.* These groupings may or may not be mutually exclusive, and the attributes of each group will need to be dynamically determined based on the availability and the characteristics of the Demand Response resources.

   b. *Modeling the Demand Response resources as Virtual Power Plants with attributes similar to those for conventional power plants.* Their parameters are a function of the underlying Demand Response resources characteristics, as well as the distribution grid limitations.

   In addition, telemetry and metering requirements for provision of ancillary services from Demand Response and demand-side resources need to be addressed. The cost and the effort to manage the volumes of data associated with telemetry from individual demand-side resources may be prohibitive. New approaches for the provision of telemetry from aggregated resources at a physical network location, such as a distribution substation, may have to be adopted.

Sensor Preparation

The proliferation of PMUs, smart meters, and other low cost sensors throughout the power system provide new opportunities for equipment condition monitoring and calculating the ratings of power system equipment dynamically, and more accurately. This is in contrast to the current methods for calculating the ratings off line using planning tools. For example, dynamically calculated ratings can be used in various applications such as Contingency Analysis, Security Constrained Economic Dispatch, and Interconnection-Wide Congestion Management tools.

[54] http://www.ferc.gov/whats-new/comm-meet/2008/101608/E-1.pdf

Distributed Resources

Distributed resources have the ability to supply isolated parts of the system during disturbances and to supplement generation requirements during large generator failures. At higher penetration levels, distributed resources can affect reliability, unless operators have visibility and the ability to send dispatch signals to them. Otherwise, balancing and regulation would be challenging, and overall bulk power system control, hampered.

Real-time Operations

Smart grid devices and systems increase the information available to operators, though they may also make operations more complex. The elements below identify some of the key reliability considerations.

Failures

Failures of devices and systems on the grid are normal occurrences; today the impacts of those failures are mitigated through sophisticated protection and control schemes, maintenance procedures, and backup devices. Currently, failure modes with significant impacts on the grid are primarily small in number and are carefully managed by system operators. Smart grid devices and systems in escalating numbers will bring new modes and consequences of failure.

As the operation of the system becomes more dependent on real-time always-on communication, the system will be more vulnerable to failures on those communication paths and to failures of the centralized control systems, which correlate and make recommendations on all the incoming data. As the grid relies on more time-dependent information, the ability to operate without that information decreases. These failure modes need to be understood as systems are being designed, so the system will remain reliable even with their failure. That is to say, redundancies and backups must be designed to ensure that the bulk power system will still transition into a reliable operating state.

Operational Risks

With the implementation of smart grid technologies, preventative maintenance and upgrades will be enhanced, but the physical risks are being expanded to include logical risk. This logical risk includes software and firmware, distributed deployments, and upgrades as well as remote-device reprogramming. The communications infrastructure to support data transport will be susceptible to single, multi-point, and multi-phase unplanned outages, operator error, and malicious attacks. The critical assets will create, store, and use more information.

As the need for the smart grid information increases, the difficulty to maintain the confidentiality, availability, and integrity of the information also increases. Processed information will need to have additional validation and more “depth in defense” to ensure the information is available real-time. The smart grid assets continue to be distributed throughout a vast network and the hardware of the remote smart devices will continue to have tamper risks. Along with tamper risks, things like unauthorized configuration updates and reprogramming

become more realistic. Configuration management will need to ensure the proper authentication and authorization is performed before devices are updated or tasked to complete requested commands. More depth in defense techniques will be required to ensure the protection of critical assets and the information that is created, stored, and used by those assets. Additional considerations include:

Real-Time Local and Remote control: Over the past decades, control of grid devices has transitioned from exclusively local control to a combination of remote control (often via protocols such as SCADA, MODBUS, or DNP3) with local override capabilities. Manual control of major grid components is vital to respond to certain emergency conditions or significant control system failures.

Real-Time distributed and hierarchical (supervisory) control: Over the past decades there has been a transition to a far more centralized, hierarchical model of automated control of grid devices. Devices such as circuit breakers and automatic reclosers are the obvious exceptions. The increased complexity of grid control systems, brought about by the increased use of intelligent electronic devices within the grid, can have a tendency to increase the vulnerability of the grid to control system failures. It is this consideration that drives the recommendation for bulk power system participants to implement what might be considered a hybrid of hierarchical (supervisory) and distributed control.

In this hybrid view, control center hierarchical systems are still critical to real-time operations, but a balance is needed. Considering the possibility of subsequent control room or communications failures requires a move to more distributed and automatic, if not autonomous, control system architecture. In this view, field devices will still inform the control room systems of various state changes, just as they do today. The difference is that distributed devices also need the ability to communicate directly with a subset of peer devices in order to take more complex and predictable actions if a control room system does not provide commands on how to respond to the state change. Taking such an approach has benefits to the bulk power system in that it helps manage the impact of cyber asset failure, regardless of whether that failure is inadvertent or malicious in origin. However, this approach can also challenge reliability if inappropriate action is automatically taken without operator intervention.

Therefore, operational risks are likely to increase as a result of smart grid implementation. These risks will go beyond just simple failure of smart grid devices and systems. As device implementation becomes widespread, simple malfunctions could result in major disruptions to the bulk power system. Since the smart grid relies on data, simply having disruptions in those data flows could impact operations significantly. Smart grid devices responding properly to bad data, such as an improper price signal, could result in disruptions. Erroneous data or even data noise could result in the wrong course of action being taken by a system operator. Common mode failures of smart grid devices whether they be hardware, software, or data related, could have a similar impact on the bulk power system. Another risk of smart grid devices lies in their reliance on firmware and software. Reprogramming of these devices would result in unintended and unplanned operations of these devices. These actions could result in disruptions and/or loss of equipment depending upon the smart grid device affected.

Early on in the smart grid implementation, these disruptions to the bulk power system would likely be the result of large blocks of distributed load being switched on or off in an unscheduled manner. Such distributed loads today are typically switched locally in response to local conditions (e.g., thermostatically controlled air conditioning). The smart grid will add and consolidate other switching factors and direct remote load switching for peak management. The addition of larger amounts of distributed generation controlled by the smart grid could also become a source of disruptions. Large swings in load and/or generation can cause frequency and voltage disruptions on the bulk power system. As the smart grid develops further, actual grid components such as transformers, conductors, etc, will become part of the smart grid. If these devices operate improperly or are forced offline, bulk power system reliability could be impacted.

Operations Assessment

New System Performance Metrics Needs

Today's system performance metrics are based on the current operating framework. With increased penetration of smart grid, these metrics will need to be reexamined to ensure viability with new threats and opportunities. As operators begin to rely on smart systems, they will need to include new threats in measurements of grid performance so that they can adequately be prepared for and prevent these threats from impacting the system.

As more dynamic and distributed forms of supply are brought into an increasingly dynamic topology of supply and demand, what passes for normal or steady-state operations will be replaced by an increasingly dynamic set of components, topologies, and conditions. In this model there will be increased challenges around consistently identifying the impacts of a variety of failures. In one potential topology, a distributed energy resource may have little or no impact on system reliability and integrity. In an alternate operating topology, it may be fundamental to maintaining system reliability. The nature of grid topology will change far more frequently with a smart grid, and the impacts of failure will change along with it. Operators of the smart grid will require better models for identifying failure impacts based on a higher number of operating states and topologies.

Other Considerations

Changing Organizational View

Smart grid will provide two-way visibility between the bulk power system operation, end-use devices, and customers. Today, bulk power system operations are substantially isolated from the distribution and customer sides of the business. With the smart grid, the separation between wholesale and retail, and transmission and distribution may be blurred. For example, bulk power system operations will need visibility into distribution operations when demand response, distributed generation, and distributed storage are offered as ancillary services.

Life Expectancy Issues

Within the smart grid, a number of new electronic devices and systems will not have the traditional 40-year or longer life. These devices include items such as microprocessor relays, communications devices, synchrophasors, merging units, software, and various sensors. Many of these devices will require periodic firmware upgrades, configuration files updates, and more. Communications networks are typically refreshed on a three- to seven-year interval. Microprocessor relays and their merging units have about a 15-year service life.

Business Continuity

Smart grid systems, as they are currently being designed and planned, may require sufficient levels of redundancy, similar to existing control systems. This redundancy can ensure that higher levels of dependence on smart grid systems will not cause reliability considerations if they fail

Personnel that are currently entrusted with maintaining system reliability are trained on overall reliability impacts and their role in maintaining that reliability. Curriculum for the personnel training must keep pace with the smart grid evolution to ensure reliable integration and operation.

Evolutionary Implementation

Smart grid implementation will be an evolving process. Design and operations will need to adapt to the changing conditions and customer needs over time. As the smart grid is expanded beyond the pilot stage, industry and vendors can leverage knowledge and tools to improve system reliability and information analysis. Due to the evolutionary nature, multiple projects at various stages could co-exist within an organization.

Careful balance must be taken into consideration while the transition from legacy (non-smart grid) systems, workforce, and processes are evolved into the smart grid. As the complexity of automated tools increases as seen by the system operator, the need for consistent visualization tools and human-factors engineering must be accounted for during design phases to reduce human errors.

R&D Requirements

R&D is an important ingredient in the evolution to the smart grid and is needed to obtain the potential benefits from integration of smart grid devices and systems while maintaining reliability of the bulk power system. Given that fundamentally new requirements will be imposed on existing T&D infrastructures, it is essential to consider the evolution of current operating and planning practices, which may enable as much sustainable energy use from the new resources as possible while ensuring that the electricity services remain reliable and secure. Introducing novel modeling, sensing, communications, and computing concepts to facilitate evolution of today's industry practices will require a major effort in the area of energy systems. The key challenge is how to integrate new resources into the existing bulk power system while maintaining reliability. The evolution of smart grid is a design problem of complex dynamic systems driven by

uncertainties not anticipated when today's T&D system was constructed or when industry practices were established.

Viewed from the reliability standpoint, it becomes critical to test the system with new devices, so that no hard-to-predict emerging technical problems occur in the actual operation. For example, it is essential to avoid situations in which relatively small changes cause undesired impacts on the reliability of the bulk power system. In order to avoid such problems it is critical to design new scheduling, regulation, and stabilization methods. For example, it is plausible that the effects of attempting to transfer large amounts of variable wind power across large electrical distances would be seen in amplified low frequency and voltage oscillations. Part of the currently envisaged solution, PMU-based fast and accurate measurements may become important to automation and closed-loop control. In addition, as the predictions about the availability of variable energy resources are made closer to near real-time, more dynamic dispatch of all available resources will become essential. The traditional time-scale separation of possible problems (non-existence of power flow solution—steady state stability, small signal stability, and transient stability) will no longer be possible, as the system is exposed to continuously varying deviations from schedules. New tools and models (planning and operations) will be needed to support reliable integration of smart grid devices and systems.

The aforementioned system may become a very complex-to-manage non-linear dynamic problem with cyber and control system security implications. In order to continue such an approach, a focused effort is needed toward the development of new models and simulations of system dynamics based on new models. The models should include sensing, communications, control, and decision-making, which are an integral part of this new cyber-physical energy system of the future.

Chapter Findings

The impact of smart grid on the reliability of the bulk power system has yet to be seen. For successful integration, it will be important that the various planning timeframes consider how best to plan, design, and operate the system in a way that mitigates or eliminates impact on reliability. Successful integration of smart grid devices and systems will need to address their potential interaction and synergies among various technologies that might be uncovered. New tools and analysis techniques will be required to plan and operate the deployment of broad-scale smart control systems across the bulk power system.

As the bulk power system is a large non-linear system using large amounts of inertia to create electricity, the ramifications and design of smart grid on control systems must be modeled, simulated, and designed to ensure that the expected performance improvements will be realized. Successful integration of smart grid devices and systems should address potential reliability considerations such as transient and long-term stability, small signal stability, voltage stability, intentional cyber attack or unintentional IT and communications errors, and component design issues such as short circuit considerations. In addition, operators of the smart grid will require improved models for identifying failure affects based on a higher number of operating states and topologies.

Integrating new smart grid devices and systems will rely heavily on advances in modeling and simulation. Real-time and dynamic performance become critically important as resources and loads on the grid become more dynamic and less deterministic. Understanding the behavior of individual component technologies must be in context with the dynamic behavior of the bulk power system. Integration of smart grid devices and systems, both hardware and software, may have varying affects on different parts of the system and on the performance of the bulk power system as a whole.

Systems engineering and R&D will be decisively important as the complexity and interdependency of the power system increases. Given that the complex modeling, analysis, decision making, cyber and control system security challenges, and design of complex systems driven by highly variable inputs, close industry collaboration with government, R&D organizations and universities is needed to develop the requisite models, build simulators, and create test systems to identify and resolve potential challenges. Therefore, R&D is an important ingredient in the evolution to the smart grid and is needed to harvest the benefits from integration of smart grid devices and systems while maintaining reliability of the bulk power system.

5. Cyber Security for the Smart Grid

Introduction

For decades, power system reliability has been viewed primarily as a matter of continuous power availability and the avoidance of uncontrolled cascading of the bulk power system.[55] This feat has been accomplished through an extensive and reliable transmission system delivering power generated in multiple locations to distributed load centers. This power supply is also continuously coordinated with system demand and uses robust delivery mechanisms with control centralized within an operating area. Information integrity and availability has been important for the success of this dynamic, real-time system to the extent it was required for system coordination and control. Smart grid technology provides opportunities to enhance the electric sector by significantly increasing information exchange, thus making data protection critical.

The breadth of the change from smart grid integration is highlighted by the objectives defined in the U.S. *Energy Information and Security Act of 2007* (EISA). This law identifies the following specific capabilities that would be enabled by a smart grid:

1. increased use of digital information and controls technology to improve reliability, security and efficiency of the electric grid;
2. dynamic optimization of grid operations and resources, with full cyber-security;
3. deployment and integration of distributed resources and generation, including renewable resources;
4. development and incorporation of demand-response, demand-side resources and energy-efficiency resources;
5. deployment of smart (real-time, automated, interactive) technologies that optimize the physical operation of appliances and consumer devices for metering, communications concerning grid operations and status, and distribution automation;
6. integration of smart appliances and consumer devices;
7. deployment and integration of advanced electricity storage and peak-shaving technologies including plug-in electric and hybrid electric vehicles, and thermal storage air conditioning
8. consumer access to timely information and control options;
9. development of standards for communication and interoperability of appliances and equipment connected to the electric grid including the infrastructure serving the grid; and
10. identification and reduction of unreasonable or unnecessary barriers to the adoption of smart grid technologies, practices, and services.

[55] NERC defines cascading as "*the uncontrolled loss of bulk electric system facilities triggered by an incident (or condition) at any location resulting in the interruption of electric service that cannot be restrained from spreading beyond a pre-determined area.*"

Integration of smart grid devices and systems will increase the sources of generation, flexibility and responsiveness of load, and distributed and diverse control systems. The timely and secure delivery of accurate and reliable information will become a more critical component of power system reliability due to these added and more complex variables. That said, the strength of the interoperability design of smart grids, unless carefully planned and operated, can provide a vehicle for intentional cyber attack or unintentional errors impacting bulk power system reliability through a variety of entrance and exit points.

These factors mandate the availability of reliable and secure information and highlight categories of vulnerabilities that can affect the bulk power system as follows:[56]

- Impacts on Timely Delivery: Denial of access to the information required to operate the grid is a significant concern, specifically the bulk power systems. The real-time nature of the data is vital to enable timely response. If information is delayed and cannot be responded to, many, if not all, of the consequences of outright denial are experienced. For information used to operate the grid, "timeliness" is often measured in milliseconds.
- Impacts on Information Accuracy and Reliability: Information must be obtained and delivered in a manner that assures that neither the data nor its attribution (source and time) has been tampered with, or that errors promulgated from information technology do not result in incorrect smart grid device and system actions.

There is a natural tendency when discussing cyber security to focus on deliberate external attacks on the information infrastructure. However, cyber security issues may also result from internal events, whether deliberate attempts to compromise a network, user error, software bugs, or equipment failures. In addition, the interconnected nature of the electric grid has already demonstrated that events in one area of the grid can have wide-reaching ramifications. Unlike many other industries, the bulk power industry does not have the option of responding to a "cyber-event" by simply shutting down communication and restarting (i.e., the classic "reboot" is not an option). The system must be able to continue to operate reliably even in the midst of a cyber-event, and ensure bulk power system reliability.

The priorities for the development of cyber security in the bulk power systems—especially with the smart grid deployments—need to focus on prevention, detection and response, and recovery. When aligning smart grid controls within bulk power to information security principles, we need to explore the security principles and risks as shown in Table 3. Overall, the key security issues range from physical to logical to administrative and, as such, encompass a broad range of areas needing focus to assure the smart grid is reliable and secure.

[56] While confidentiality and/or privacy are issues when dealing with information that can be traced to an individual, location, or market participant, as Reliability Standards do not address these areas, they lie outside the scope of this document.

Table 3: Information Security Principals

Security Core Principles[57]	Definition	Risk	Security Mechanism
Confidentiality	Ensuring that information is accessible only to those authorized to have access	Disclosure	Cryptography, PKI, access control, identity management, privilege management
Integrity	Ensuring the correctness, completeness, wholeness, soundness, and compliance with the intention of the creators of the data	Corruption	Backups, integrity checks, hashing, PKI
Availability	Ensuring the condition of being ready for use	Denial of service	Operating system security, application configurations, intrusion monitoring
Authenticity	Ensuring the origin of the information is a valid originator	Fraud, deceit	Verification and validation, reliability check
Usability and Interoperability	Ensuring the component can provide services to and accept services from other components to enable them to operate effectively together	Cannot function with other components	Key management, secure data transfers
Non-repudiation	Ensuring the inability to deny the integrity and authenticity of a document	Impersonation, false attribution, fraud, deceit	Digital signatures
Authorization	Ensuring the component has the right or permission to use a system resource and has been authorized	Theft of service	Identity and privilege management
Privacy	Ensuring the right of information to be free from intrusion	Public disclosure, misuse of personal information	Physical controls, firewalls, intrusion monitoring

Cyber security is a vital element of the reliability of the bulk power system, and part of NERC's Critical Infrastructure Protection (CIP) program and standards development activities. Further, through the Electricity Sub-sector Coordinating Council (ESCC), NERC is developing a *Critical Infrastructure Strategic Roadmap* to address a number of severe-impact scenarios, including a coordinated cyber attack.[58] Because of this examination, the remainder of this chapter is intended to serve as a summary of cyber security considerations and a guide to their implications for bulk

[57] Based on a table from Information Assurance Architecture by Keith Willett using information assurance mechanisms and information assurance core principles.

[58] Electricity Sub-sector Coordinating Council, "*Critical Infrastructure Strategic Roadmap,*" August 2010: http://www.nerc.com/docs/mrc/agenda_items/AgendaItem_6.b_Attach_1.pdf

transmission and generation. The detailed observations specific to the *Characteristics and Technology Assessment* and *Planning and Operations with Smart Grids* are contained in their respective chapters.

Loss of Control Center Systems

Before exploring reliability considerations from loss of control, a discussion of the distinction between "loss of control" and "loss of communications" is necessary. Loss-of-communications between control centers and substation or field devices is a fairly well understood failure mode and consideration is a requirement under NERC standard *EOP-008-0 – Plan for Loss of Control Center Functionality.* Already, most bulk power system operators have conducted vulnerability analysis and risk mitigation efforts. Strategies for risk mitigation include the implementation of redundant communications paths over separate physical paths, and using multiple media for primary and backup communications between critical devices. At a higher level, risk mitigation for loss of control center systems has also generally been well documented. Many control center environments use a series of primary and backup power systems, redundant communications modes, and computer hardware and software systems. Additionally, many bulk power system operators have entire standby control center facilities, which can be used when the primary control center is unavailable.

Still, loss of control remains a risk. Despite the above risk mitigation strategies, operators of the bulk power system must still consider other methods of maintaining grid operations. The loss of control of the physical and logical components constituting the smart grid can have a serious impact on the reliability of the bulk power system. Of course, the impacts can also be localized to one customer or broadened to encompass an entire balancing area—or even larger. Therefore, this discussion focuses on identifying those ways and means that loss of control of the bulk power system and smart grid components can occur, followed by a discussion of causes and their possible mitigation.

Before loss-of-control is reviewed, the key means of communication used to send command and control signals to the components on the grid to obtain information on the grid performance must be understood.

Communications Systems

There are several different communication systems used by industry to send command and control messages throughout their balancing area. These systems range from traditional methods (e.g., Plain Old Telephone Service—POTS) to the more advanced systems using satellites.

These communications systems can be categorized as "Wired" and "Wireless." A summary of the key systems of concern divided by category include the following:

Wired:

- **Telephone** — These systems are primarily used for voice transmission, but also can be used for data acquisition and command signals for selected devices.

- **Power-Line Carrier** — Protective relaying commands may be carried along the power-line on a carrier system as an alternative to telephone or microwave. Power-line carrier is used for protective relaying because of the high reliability of the transmission medium—the high-voltage transmission line conductors themselves.
- **Local Area Network/Wide Area Network (LAN/WAN)** — LAN/WAN is becoming a more prevalent way to communicate within a network of generators, substations, and switches due to the robust reliability of TCP/IP protocols. In addition, the added benefit of using fiber for LAN/WAN connectivity is that it increases network speed, adds immunity to radio-frequency and electromagnetic interference, and electromagnetic pulse, and it is much more difficult to "hack" a fiber line to intercept the data. In addition, fiber eliminates ground loops and, as such, can be used in substations where twisted-pair copper lines may not always be used or permitted.

Wireless:

- **Microwave (Radio)** — Used in addition to telephone trunk lines, microwave radio provides a means for alternative transmission of voice and data. However, with the trend toward increased high-speed data handling, digital microwave is a possible alternative to the older analog microwave systems.
- **Land Mobile Radio / Cellular Telephone / Satellite (Radio)** — The most common application of these radio systems is for dispatch service and emergency operations and command, and control of personnel resources. These systems are not used for protective relaying or direct component command and control due to their inherent latency. Due to the substantially reduced latency with cellular radio protocols such as EVDO and, ultimately, the LTE (Long-Term Evolution) of cellular, the LTE signals may be considered for command and control of the electric grid components.
- **Wireless Mesh (Radio)** — A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers, and gateways. The mesh clients are often laptops, cell phones, and other wireless devices, while the mesh routers forward traffic to and from the gateways, which may but do not need to connect to the internet. Currently, a form of wireless mesh is being considered for controlling multitudes of smart meters. However, as demonstrated at the BlackHat Convention in Las Vegas in 2009, a mesh network is susceptible to some forms of cyber attack.[59]
- **802.11x and WiMax (802.16)** — These are protocols that will allow an organization to establish a local- or wide-area or metropolitan wireless network for command and control and information signal management.

It is highly unlikely that an entire industry command and control and information infrastructure will be entirely "wired" or "wireless"; however, with the implementation of a wireless environment, the opportunity to disrupt the confidentiality, integrity, or availability of the signal is substantially increased.

[59] http://www.elp.com/index/display/article-display/2632770661/articles/utility-automation-engineering-td/volume-15/Issue-4/Features/In-Smart-Grid-Security-the-Details-Matter.html

Command and Control Architecture

Because of its geographic size and technical complexity, and its evolution over the past century, the electric grid currently has a very centralized command and control system architecture. This ensures the grid works reliably—especially during transients and unusual circumstances (e.g., loss of grid elements due to equipment failure, fires, etc.). Distributed grid devices typically are designed to react to system conditions rather than to proactively act. For instance, the circuit breaker may trip out of service due to grounding. Reclosers are often used to increase grid reliability by automatically attempting to restore service to a line that has suffered an intermittent fault. More complex functions, such as re-routing power around persistent problems and adjusting generation or loads in response to various events, is done either by complex automated systems or by individual control center operators. Properly designed smart grid technologies offer the opportunity to intelligently monitor and control the grid to a level of detail that is impossible to achieve manually. That said, centrally managed systems, which include human-in-the-loop interactions, are needed to improve the long-term reliability of the bulk power system.

With or without smart grid devices and systems, an implication of this hierarchical control architecture, however, is that loss of control system or control system communications can render a significant percentage of field equipment unavailable for remote command response, and leave this same equipment idle waiting for instructions from the control center. Inadequate monitoring, human and software errors, and incident response may result from failure of the control system or communications system. Consequently, reducing the real-time impact on bulk power system management caused by loss of control is an important consideration when integrating smart grid devices and systems.

The Importance of Real-time Centralized Monitoring

The electric grid, as well as smart grid design, requires constant analysis and monitoring to ensure that the system will sustain transients and contingencies. This requires real-time data such as the following:

- data measurement and system monitoring,
- transmission transfer capacity,
- control system state,
- control system action and efficiency,
- safety,
- system integrity,
- intra- and inter-substation autonomous response,
- command and control, and
- situational awareness.

Loss of control and communications

Seven characteristics of attack or failure on a control system have been identified by industry that may result in entire or partial loss of the communication's signal (availability), a breach of the signal's confidentiality and/or integrity, or some failure of the control system itself. Communications can take the form of radio frequency mesh, wireless, wire-line, fiber, microwave, satellite, etc. These characteristics (examples are provided in Table 4[60]) include:[61]

- **Logical** — Affects the storage, transmission, or processing of digital information, command and control signals, etc.
- **Physical** — Affects the existence and physical condition of tangible facilities, equipment, and components.
- **Administrative** — Affects the performance of people or processes by either the inclusion of or failure to provide thorough, vetted policies, standards, procedures, and/or guidelines.

Table 4: Threat agents

Attacker / Threat Agent	Motivation/Cause	Physical	Logical	Administrative
Computer Hackers	Fun, challenge, fame, boredom	X	X	
Organized Crime	Financial gain		X	
Environmental Extremist	Political gain, harm groups	X	X	
Terrorists	Cause fright, financial gain, economic damage	X	X	
Nation States / Foreign Governments	Strategic military and/or economic damage		X	
Insiders, Contractors	Revenge, labor relations issues, personal grievance	X	X	X
Errors and Omissions	No motivation—could be caused by negligence, inadequate or no training, poor policy enforcement	X	X	X
Natural Disasters	Includes earthquakes, weather, flooding, geomagnetic storms, solar flares, etc.	X		
Software Defects	Poor coding		X	
Carelessness	Similar to Errors and Omissions	X	X	X
Vulnerabilities of Assets—weaknesses that, if exploited, devalue the asset.	Poor manufacturing, aging, vulnerable materials, etc.	X	X	X
Unmanaged Vegetation Growth	Trees touch power lines resulting in grounding and line failure	X		

[60] "Securing Your SCADA Industrial Control Systems," V1.0, Technical Support Working Group, US Department of Homeland Security, Page 32

[61] *Bhaskar's Threat Matrix*: http://www4.ncsu.edu/~jjyuill/Professional/Research/Publications/bhaskars-threat-matrix.pdf

These threat types can further be sub-characterized as:

- **Deliberate** — An intentional act performed by an individual, or
- **Accidental** — An event or act that was an error or deviation from designed performance.

Finally, the threats can be:

- **Active** — The threat of a deliberate unauthorized change made to the state of a system.[62] Examples of security-relevant active threats are modification of messages, replay of messages, insertion of spurious messages, or masquerading as an authorized entity and denial of service.
- **Passive** — The threat of unauthorized disclosure of information made without changing the state of the system.

Causes of loss of control or loss of communications

Loss of control of the grid control systems or communications can occur due to a myriad of reasons as detailed above. Some different cyber attack techniques to consider include:

- **Brute Force methods** — Hacking systems for passwords;
- **Bypass methods** — Circumventing physical, logical, or administrative controls;
- **Destruction** — Physically damaging equipment or erasing data on a hard drive or other memory device;
- **Denial of Service methods** — Overloading a communication channel or processor to the point that it cannot perform its expected function;
- **Strategic Ping** — SCADA can be vulnerable to strategically timed ping;[63]
- **Malformed Packet** — Send a non-standard data packet to a control system, which causes it to abort, restart, or halt;
- **Hijack** — Taking possession of a grid control component or signal;
- **Malware** — Injecting a virus, worm, Trojan, or Root Kit, thus impacting the performance of the computer control system;
- **Spoofing** — Pretending to be another entity—physical or logical;
- **Tampering** — Modifying data or software to produce different than expected results; or

[62] https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/en/a/active_threat.htm

[63] A ping is normally 56 bytes in size (or 84 bytes when IP header is considered); historically, many computer systems could not handle a ping packet larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size could crash the target computer. However, though SCADA and other infrastructure is theoretically vulnerable to a direct PoD attack, many organizations have put in place countermeasures to manage this threat.

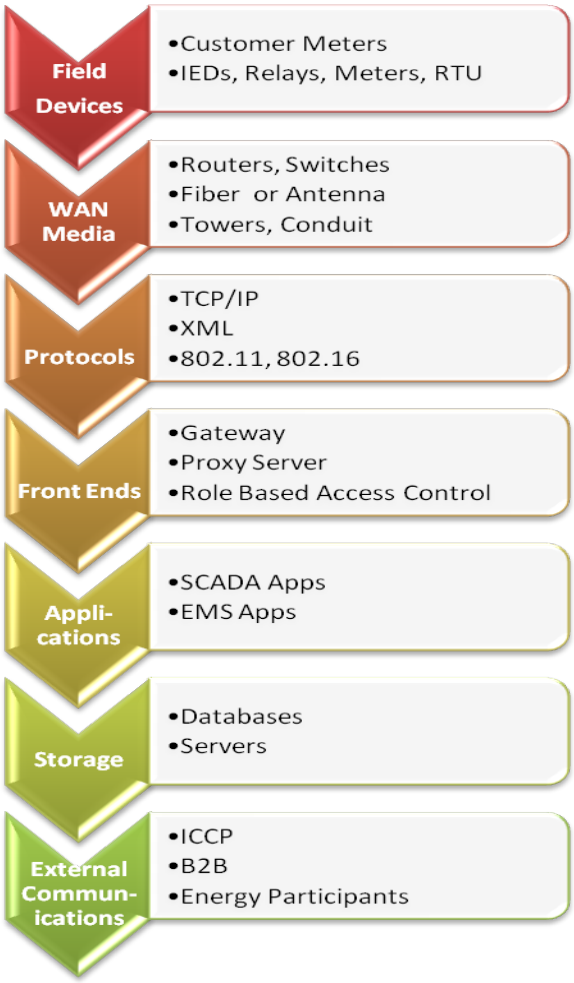
- **Intercepting, Man-In-The-Middle Attack** — Intercepting the signal or message in mid "flight" then modifying the message or command and sending it on to the controlled object.

Loss of communications can also occur due to non-malicious causes that result in damage to the physical lines or power outages to the system components, such as wind, ice, hurricanes, solar flares and electromagnetic pulse (EMP), communication infrastructure damage (e.g., damage by nearby construction projects), communication interference from vegetation growth, and human error.

Potential locations of loss of control or communications

Due to the large geographic footprint of the electric utilities and their associated control systems, the answers to "where" the failures can occur are substantial. For example, the loss of communications can occur anywhere along the control system components and the associated linkages. Figure 5 below shows the continuity of the network and where loss of control and loss of communications can occur.

Figure 5: Where loss of control and communication can occur



Consequences of loss of control or communications

Under most circumstances, and because of the robust design of the electric grid and the associated physics, the electric grid can withstand momentary failures in command and control systems. However, if these failures continue for a long period of time or if these failures occur in conjunction with another calamity such as a storm or fire, then the control system failures can result in cascading failures aggravated by the inability of grid control personnel to know what is happening because data are not available.

Some examples to consider in this arena include the following:

- **Loss of Control with Control System Communications** — Here, the result could be the inability to open/close circuit breakers, the inability to send load signals to generation, or the inability to communicate with adjacent organizations, Independent System Operators (ISOs), etc. Overall, the result could be a large-scale power outage over a large geographic area that is slow to recover.
- **Loss of Telemetry to Individual Devices** — This failure is not as severe as the above scenario. The inability to communicate with an individual device (e.g., meter, RTU) occurs relatively frequently within reliability coordinator or regional footprints. Also, this risk is mitigated due to the design of the electric systems with options for alternative or redundant controls and/or communications modes often available.
- **Loss of Inter/intra area communications** — Inter/intra area communications, for example using Inter-Control Center Communications Protocols[64] or ICCP, provides a data connection system between SCADA and EMS control centers, utilities, power pools, Regional control centers, and independent power producers. These inter/intra area communications are critical for real-time data exchange, especially as frequency, volume, and magnitude of energy transactions increases. As noted by the NERC's *ICCP Design Requirements for Optimal Availability and Performance*[65] document: "Without such data [a] exchange system, it will be impossible to ensure the necessary reliability of the national electrical grid."
- **Loss of Power to Customers** — The loss of communications and control to the grid—whether it is the major grid components or the smart grid devices—can result in unreliable operation or, in the worst case, a blackout.

Security Defense-in-Depth Model

Robust cyber security architecture involves the application of layered Defense-in-Depth[66] solutions to protect critical elements of the network environment. Figure 6 provides a high-level

[64] ICCP is also a recognized international standard (IEC TASE.2).
[65] www.nerc.com/docs/oc/dewg/isn/iccp_design_requirements.doc — 2003-07-29
[66] Defined in the NRC Glossary as: "*The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and*

defense-in-depth solution for a control center. In this model, the control center systems would be installed and operating within the innermost protective layer. This model provides a framework for recognizing defense-in-depth architecture. In addition to consideration of the general use of this model, the names of the various layers, and description of the systems implemented within each layer, may vary based on the needs of the organization. The definitions of the layers and systems given below are notional, to serve the purpose of the model. They are not prescriptive.

When taken together with the Risk Matrix and Risk Cube discussed in the following section, these models can be used to assess risk and determine which defensive measures are appropriate.

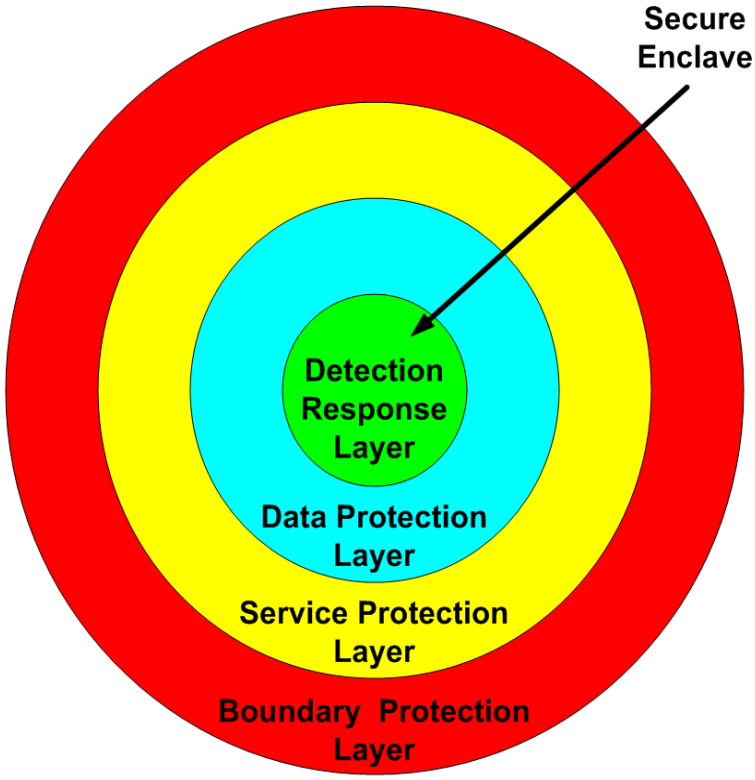


Figure 6: Cyber security defense-in-depth model

This model classifies control center cyber security controls and objectives within the following set of four layers:[67]

- ***Boundary protection layer:*** Contains controls for the cyber and physical perimeter. Perimeter security controls such as firewalls, intrusion prevention sensors, and honey

diverse key safety functions, and emergency response measures.": http://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth.html

[67] The layers described here, and the systems within the layers, are for reference only, and are not to be considered proscriptive.

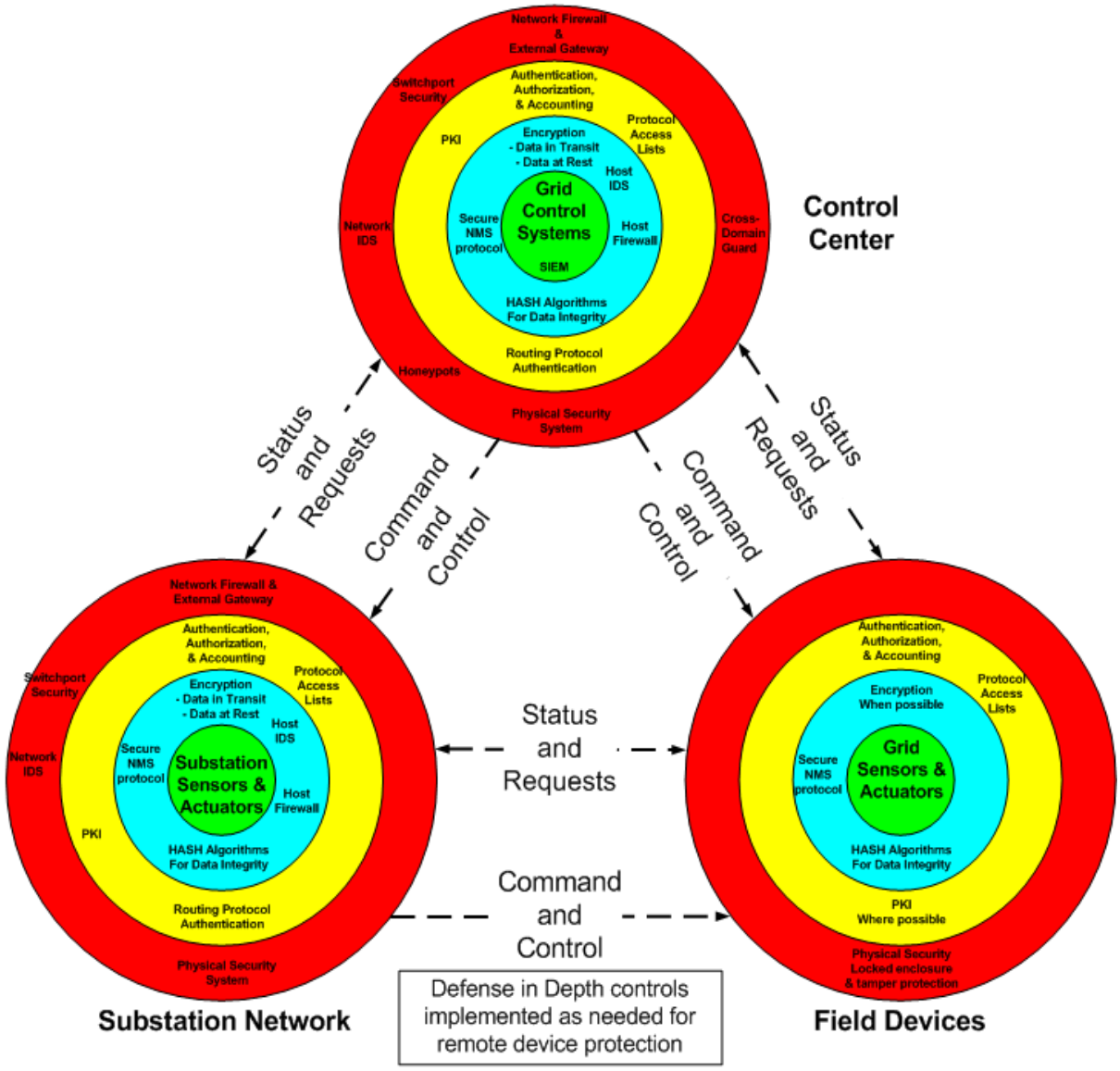
pots are categorized in this layer. Example controls include firewalls; physical security devices such as surveillance cameras, intrusion detection and prevention sensors, access security including wireless access point security and switch port security; and keycard access controls. Since the control center is normally a manned facility within a building, it is assumed the majority of physical security concerns for the control center will be addressed by general building physical security controls**.**

- ***Service protection layer:*** Contains controls for access to services and applications for users inside a high assurance smart grid cyber and physical perimeter. Example controls include public key infrastructure (PKI), key management, Role Based Access Control (RBAC), service control (e.g., authentication, authorization, and accounting), and protocol access lists.
- ***Data protection layer:*** Includes controls that protect data, control, and management traffic. In addition, it contains controls to protect data within the High Assurance Smart Grid perimeter. Example controls include file integrity checking, secure network management protocols such as Simple Network Management Protocol Version 3 (SNMPv3), encryption of data in transit and data at rest, host-based intrusion detection and security, authentication of routers for a given protocol (e.g., Message-Digest algorithm 5 authentication for Open Shortest Path First protocols), and operating system hardening procedures.
- ***Correlation/response layer:*** Contains controls to perform correlation of and response to security incidents. Example controls include a security information and event management system, event correlation, log scanning, and incident response by a human security analyst. The function of this layer is to take inputs from security devices such as Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS), sensors, and firewalls, along with log messages from network hosts, and security event monitoring and correlation. The primary element of this innermost layer is a security incident and event management (SIEM) system.

Certain cyber technologies may cut across multiple layers in the defense-in-depth model. One such technology uses distributed cyber agents, residing on many host control computers throughout the environment. These agents may perform a variety of functions locally, such as intrusion detection, log scanning, and event correlation.

To use the defense-in-depth model (with the risk model described later), each type of system is assessed independently. Control systems and control centers may have one set of defensive systems selected, while a substation or a field device may well have separate systems. Figure 7 shows such an example. While the layer identifiers are the same for all systems, the security controls for the control center, the substation, and the field devices are each selected separately. This example also shows a critical aspect of the recommended design: each system (or set of systems) attempts to protect itself from compromise originating from systems at the other end of its communications links. This concept is identifiable when comparing the security controls for field devices and security controls selected for the control center or substation.

Figure 7: Cyber security defense-in-depth example



Risk Management

Investment in wide-ranging smart grid marketplace transformation has been slow, due in part to poor business case support, and has primarily accelerated due to U.S. Department of Energy stimulus funds in 2010. As these new technologies become available, they tend to focus on functionality first and secure operations second, although this is slowly changing as the importance of security narrative becomes evident and as the National Institute of Standards and Technology (NIST) issues its Smart Grid Cyber security Guidelines in NISTIR 7628.[68] This

[68] See http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

three-volume report presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Since the smart grid is a collection of capabilities and attributes, each organization needs to view what it "means to them" to identify the relevant scope. Since security of the smart grid is effectively a risk management process, each organization needs to view what it means to them to effectively identify and manage the risk of their scope to their safety and operations. These variables drive independent responses to risk across different entities.

Need for Robust and Adaptive Certification Process

As the number of new intelligent devices connected to the bulk power system explodes, the complexity of the grid increases, and the number of new intelligent devices and systems integrated increases, they should be certified that the device and systems work in the manner they were intended. Adding new, as-yet undeveloped certification processes may impact testing costs and time to delivery of the smart grid devices and systems, but are vital to ensure reliable operation of the bulk power system. Therefore, a robust certification process is needed to ensure that new smart grid devices and systems added to a grid function in the manner they were intended.

It is not sufficient that smart grid devices and systems be certified. Rather, there must also be a robust change control process that will allow entities to document changes made to devices and systems after they are purchased and installed.

Coordination of Standards and Process Evolution

Much of the success of a seamless integration of the smart grid technologies with the bulk power system lies with the fact that the standards governing the interoperability of the smart grid must work on a harmonized platform. Some areas of importance are explained in this context.

Many cyber security standards and requirements already exist (e.g., NISTIR 7628[69]) that can stand independently, but when merged, may be in conflict with each other. One issue with the myriad of cyber security standards and requirements is they were developed within specific entities and Standard Development Organization (SDO) collaboration was not in place. This causes "compliance confusion" for the electric sector trying to implement the industry cyber security standards and requirements. Fortunately, NISTIR 7628 has collected recommendations that can be applied across all entities, such as vendors, and includes mapping and collaboration of cyber security requirements with the intent to ensure that they are not in conflict with each other.

However, there are issues requiring consideration and harmonization. For example, real-time synchrophasor measurements provide key information for system operators to determine the status of the power grid. Data sent by Phasor Measurement Units (PMU) are received and processed by Phasor Data Concentrators (PDCs). The current primary standard that governs the

[69] See http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

communication between PMU and PDC is IEEE C37.118. On the other hand, a key industry standard for wide-area communication between substation and field equipment is the International Electrotechnical Commission's (IEC) Standard number 61850.[70] There are significant differences and overlaps between the two standards. That said, it is possible to integrate the standards to establish a harmonized communication platform. Therefore, in this case, a new work item has been created by a joint team of IEEE and IEC participants to evaluate the harmonization of these standards. Further, on a broader scale, a NIST Priority Action Plan working group has been established to support coordination among the relevant standards development organizations (SDOs), including developments in North America.[71]

Another example that relates to time synchronization of all PMU data for phasor measurements is another factor for a robust smart grid in real-time. Guidelines for achieving an accurate synchronization can be found in IEEE 1588. However, a plan is required to implement the standard profile across the grid. IEEE is developing a IEEE Standard Profile for the Application of IEEE 1588 (Ver. 2) for Applications in Power (IEEE PC37.238), and there is an SGIP working group supporting this effort.[72]

A important example of why smart grid standards need to recognize the interoperability between equipments used in transmission and distribution, is the requirement of mapping of Distributed Network Protocol 3 (DNP3) with IEC 61850. DNP3 is the legacy communication protocol that is followed for large volume data exchanges between equipment. However, IEC 61850 is recognized to be a better standard suited for smart grid communications. To bridge the gap between the legacy DNP3 protocols and the newer IEC 61850, a mapping is required when exchanging certain data types. The goal is to ensure that data are seamlessly transported between devices regardless of their adopted communication standards. DNP3 has recently been adopted in IEEE Standard 1815. An IEEE standard and an SGIP PAP working group are currently supporting the mapping effort between IEC 61850 and the IEEE 1815/DNP3 standards.[73]

The role of internet technologies is an important part of smart grid applications. Development of guidelines for using suitable IP protocol for smart grid applications and identifying domain types is essential for the reliability of the bulk power system. The goal is to enhance the cyber security of the bulk power system with a defined suite of IP-based protocols for smart grid networks.

Wireless technologies are another area that require much consideration. Due to increased dependence on wireless communication between substation equipment, it is essential that the standards use a common set of terminologies and definitions. There are different types of wireless technologies that are available today from Zigbee Alliance, Utility Telecom Council (UTC), and WiFi Alliance to name a few. Each technology has its strengths, weaknesses, and capabilities depending on the specific smart grid application. They also have different security characteristics. The goal is to identify different technologies and their capabilities, and to

[70] See http://www.nist.gov/smartgrid/upload/13-Time_Synch_IEC_61850_and_C37118_Harmonize.pdf
[71] See http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP1361850C27118HarmSynch
[72] Ibid.
[73] See http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP12DNP361850

understand the security aspects of each so that they can be integrated within the requirements of bulk power system cyber standards to maintain the reliability of the bulk power system.
Harmonization of smart grid standards is an essential element that is to be implemented between various standard-making bodies and users in both the U.S. and Canada. In the U.S., NIST has undertaken priority action plans (PAP) to identify some of these issues. In Canada, the Canadian National Committee of the IEC in coordination with Standards Council of Canada created a task force to identify gaps between the IEC standards and standards developed by other vendors, and to work on those gaps.

Increasing Complexity of Asset Governance

Cyber security, physical security, compliance, business continuity planning, risk management, and incident response are among the many responsibilities of an enterprise's security program; however, they need to be treated as a coherent unit, with objectives, controls, and repeatable processes. With the addition of smart grid devices and systems, the importance of these activities multiplies.

A Governance, Risk, and Compliance (GRC) program to improve security, vital for successful integration of smart grid devices and systems, would address the following:

1. **Establish and Support Policies, Procedures, and Controls**: This area concentrates on creating and establishing policy, standards, procedures, and controls that are in alignment with business initiatives and risk analysis.
2. **Maintain Centralized Oversight**: Executive level oversight is needed for the program to work enterprise-wide and beyond the departmental silos.
3. **Maintain Decentralized Administration and Accountability**: The overall administration of this model has to be delegated to corresponding departments and individuals, so that any problem resolution or process improvement can be implemented at a much faster pace.
4. **Establish Communication Channels Across all Organization Levels**: This security model will allow departments to work together across the organization, from IT departments to the operations departments.
5. **Audit, Monitor, and Report**: This area will concentrate on monitoring all the processes that are implemented, thus increasing the ability of an organization to provide a more repeatable and sustainable process.
6. **Provide Uniform Support, Remediation, and Enforcement**: The overall GRC framework would give the organization a better way to run a complex security program that is repeatable and sustainable.
7. **Implement Continuous Process Improvement**: The GRC framework will ensure organizational agility to adapt to changed processes, threat environments, and technological advances.

The International Organization for Standardization (ISO) 27002, Section 0.7, entitled "Critical Success Factors," identified additional items elements of an effective GRC process:

- A high-level security policy should be created that specifies business and security challenges and objectives. This is different than the policies, procedures, and controls already referred to in the aforementioned material. For example, regarding budgets and staff, industry organizations appear to be "two companies in one" regarding security: operations and the rest of the company. Though the goals and controls differ, all corporate high-level concerns and goals should be clear in creating a corporate awareness of all security concerns. Examining high-level security policies would also support the development of industry-wide security metrics.
- Effective communication of information security as well as training and awareness programs for employees, vendors, stakeholders, and even consumers is important as part of smart grid integration. Aside from the regulatory requirements, proactive response could minimize customer resistance and improve education about the merits/demerits of smart grid technology integration.
- Management of the smart grid should not only maintain centralized oversight, but provide visible support, commitment, and funding for information security activities at all levels of management within all departments.
- The complex security programs should be repeatable, sustainable, and measureable. Implementation of a measurement system to evaluate performance outside of the checkbox compliance, including feedback suggestions for improvement, is critical for success of a program.

Balancing Internal and External Sources of System Risk

Despite the technical advances expected as the smart grid develops, the greatest potential risk factor remains the individual with access to high-level control system privileges. This individual may or may not have malicious intent and, due to the rapid evolution of mobile and decentralized control access, need not be physically located within the traditional control center. Thus, this risk can exist both internally and externally to the organization. As the boundaries between systems become more porous and the perimeters of systems less easily defined, the critical distinction between an insider and outsider will be based less on geographic location and more logically on access and level of privilege obtained (appropriately, inadvertently, or maliciously) within the control system. Thus, the greatest effort to protect control systems will need to be placed on protecting the system from those with insider access. The intent of an insider can be both malicious and accidental.

As control devices and the access to critical control systems migrate out of highly protected data control centers into the field, the boundary that defines where an insider can have access will change and potentially cease to exist as a relevant point of division. Thus, entities will need to ensure that there are more robust internal controls on insider behavior. This can include the traditional approaches to segmenting networks and duties, along with new and alternative approaches for managing these types of risks.

The Use of Standardized Risk Identification for Smart Grid Integration

A risk assessment method calls for the systematic analysis of threats and vulnerabilities, which provides the organization a way to both identify and prioritize technical and procedural controls needed for any system. Selection and practice of a risk method provides a way to reflect the needs of the organization—balancing specific system components, business goals and regulatory requirements. In addition, it is important to understand the enterprise's "risk appetite" to assess the resource level desired to respond to such threats and vulnerabilities. As such, risk assessment is a preferred method to the "checklist" model of applying controls and securing systems for the following reasons:

- Industries are the most important users of the risk assessment process since they are the implementers and most able to affect the impact of any smart grid investment. Risk assessment produces prioritization—imperative for investment as well as implementation.
- The vendors should consider that smart grid components will become part of a risk assessment and should create information that can assist in the assessment. For instance, well-documented implementation plans for devices that can create log-events should be developed to ensure the event data is stored and accessed by central control and provide a feature's control information that may differentiate products in a risk assessment.
- Regulators and auditors want to create rules that do not prescribe a "one size fits all" control, but rather apply the correct level of controls to the highest risk identified by the organization that can be objectively verified. When the auditors are aware of the risk assessment, they can assess the controls in place and adjust risk factors.

The selection and use of a risk assessment method is also a way for the organization to perform a self-assessment of its own risk profile. With the current approach to the development of smart grid technology, there is a high likelihood of failure and intentional or inadvertent breach to systems. Organizations that assess risk can build and deploy system components with security built into the design and implementation process. By addressing risk as a core process and determining residual risk, an organization may then be able to mitigate some reaction to incidents through the application of detective controls (like strong monitoring, log management, and change audit). While these are not often seen as preventive, the controls provide a way to determine what occurred, and devise new controls to close specific risk and threat vectors.

Unknown Risks in the Evolving Smart Grid

One way of evaluating risk is to evaluate a number of distinct attributes. These include the topology of the smart grid itself, vulnerabilities associated with the smart grid and how it is operated, vulnerabilities associated with the new technologies employed in the smart grid, and more esoteric, though none the less important, human threats, which could impact the integrity and, therefore, the reliability of smart grid deployments.

There are two basic formulas for addressing risk to an organization:

1. *Risk = Likelihood * Impact*
2. *Risk = Threats * Vulnerabilities * Impact*

In reality, these formulas are consistent; likelihood is just a factor of (Threats * Vulnerabilities). The first of these formulas is often used with a Risk Matrix to determine which risks are high, so the organization knows where to invest in order to reduce the overall risk. A Risk Matrix is often used to summarize the results of such an effort. The risk attributes are listed in Table 5.

Table 5: Example Risk Attributes for Risk Matrix

Likelihood – Threats	*Likelihood - Vulnerabilities*	*Impact Areas*
Naturally occurring events (regardless of how infrequent)	Communications	Generation sensors
Untrained and/or distracted personnel	The internet	Generation actuators
Insiders with malicious intent	Grid complexity	Transmission sensors
Cyber attack — lone actors (thrill seekers, script kiddies, etc.)	Grid control system complexity	Transmission actuators
Cyber attack — terrorism	New systems	Distribution sensors
Cyber attack — nation-states	New device	Distribution actuators
		Distributed generation
		Microgrids
		Communications networks
		Intelligent or autonomous systems

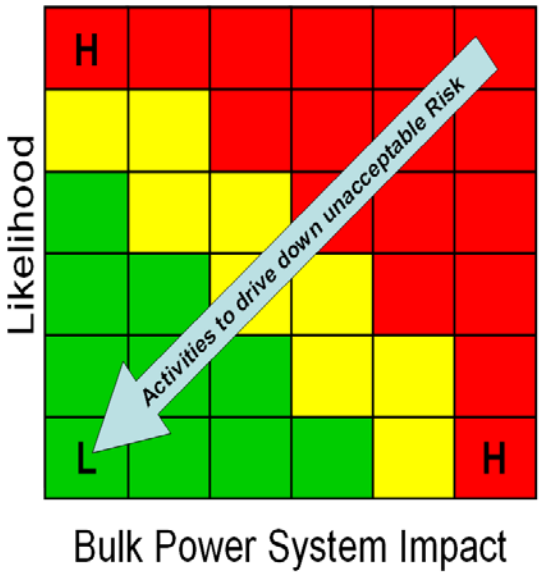
This list of risk attributes is not intended to be all-inclusive. The particular set of vulnerabilities and impacts will be unique to each participant. However, understanding these broad categories, and how they fit together into an overall Risk model, is necessary before organizations can assess their overall risk.

Industry practitioners may tend to rely upon proven models showing the "known unknowns" (i.e., functions, processes, existing devices, and systems) to scope future risks. This bias could limit an organization's ability to forecast future threats to that which are "known," including natural risks and threats. Since "we don't know what we don't know" about the future harms or risks from smart grid integration, new tools and methods are needed to monitor, in non-traditional places and through highly integrated approaches, those who wish to do harm to the bulk power system. Of note, the NIST Smart Grid Cyber Security Guidelines completed a substantial amount of work to help minimize the "we don't know what we don't know" element of the risk analysis for the smart grid deployments.

Using the two-dimensional risk matrix view (Figure 8), the likelihood and impact attributes can be categorized from lowest to highest. Areas where likelihood is high and impact is high are

typically the first chosen for remedial attention in order to bring them from the Red area down to the Yellow or Green areas, normally called a "Heat Chart."

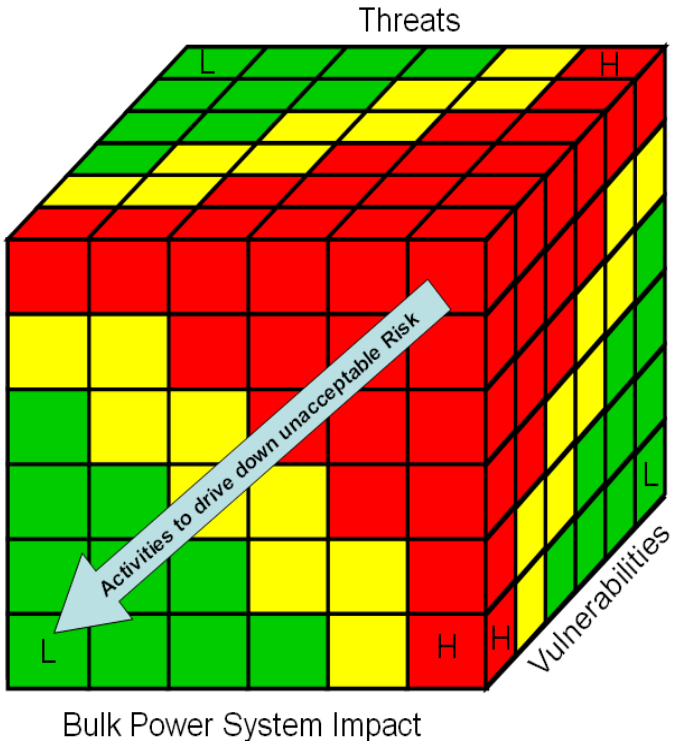
Figure 8: Risk matrix — a two-dimensional model for assessing risk



In reality, assessing risk requires use of the second formula, which addresses threats independently from vulnerabilities. This is because organizations typically have some control over vulnerabilities, but have little control over threats. The third factor in the three-dimensional view is the overall reliability of the bulk power system as affected by smart grid deployments. This three-dimensional Risk Cube provides a more complete model on how risk to the bulk power system should be assessed (Figure 9). In this case, threats and vulnerabilities are assessed independently. While more complex, the Risk Cube gives organizations a better way to determine where they should focus than can be achieved with the two-dimensional Risk Matrix. In the example below, one cube may give a combined rating of high risk, even though adjacent areas may be at moderate or low risk.

The layered protection methods selected from the defense-in-depth model described earlier, when applied to a control center, will be different from the protective methods selected for protecting distributed sensors and actuators. For example, while the full set of measures may be installed to protect control center systems, not all of these measures may be appropriate for application to distributed field devices. Namely, it is neither possible nor desirable for an organization to create an all-inclusive enclave of trust, which would encompass all control systems and distributed sensors.

Figure 9: Risk cube — a three-dimensional model for assessing risk



Both vulnerability and impact can be reduced when there is a healthy distrust between devices in the smart grid, rather than having a model with implicit trust in grid control devices currently in use. The risk assessment is completed separately for various control system and grid components. Protective measures from the defense-in-depth model above are selected based on the results of applying the Risk Matrix or the Risk Cube.

Other Considerations

Physical Security of Assets Outside the Control Center

Many times, the focus of cyber security is within the enterprise and control system data centers. These assets are normally contained within a six-walled, secured center that includes both physical and logical security. There are many existing standards and requirements for the physical security of enterprise and control system data centers, such as NERC's Critical Infrastructure Protection (CIP) standards CIP-002 to CIP-009.[74] What may be missing within the bulk power domain is a set of physical security requirements for assets that reside outside the enterprise and control system data centers. This can especially be true at the distribution level, where the jurisdiction of the NERC CIPs is not included While these assets reside outside locations that have standard physical security in many cases, a standard set of high level requirements needs to be developed for these assets that do not conflict with NERC's CIP

[74] http://www.nerc.com/page.php?cid=2|20

standards. Physical and environmental security encompasses protection of non-control center physical assets from damage, misuse, or theft. Physical security addresses the mechanisms used to create secure areas around hardware. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access control system equipment. Yet security requirements must balance the need to protect data from protection system IEDs with the ever-increasing need to access fault event and real-time data for analysis and restoration after a system disturbance.

Physically fortifying smart grid's critical infrastructure is a daunting challenge because assets tend to be spread out over vast distances (common issue amongst the current grid construction), yet protection can still exist. As far as physical security is concerned, four concepts can be deployed: 1) crime prevention through environmental design (CPTED), 2) mechanical and electronic access control, 3) intrusion detection, and 4) video monitoring. These basic concepts will add to a defense-in-depth posture and mitigate some (though not all) risks associated with physical attack.

Environmental security addresses the safety of assets due to damage from environmental concerns. Control system equipment can be very expensive and may ensure human safety; therefore, protection is important from fire, water, and other possible environmental threats. Environmental security should address or include the following:

1. A formal, documented field asset physical security policy that addresses:

a. the purpose of the field asset physical security program as it relates to protecting the organization's personnel and assets;

b. the scope of the field asset physical security program as it applies to all the organizational staff and third-party contractors; and

c. the roles, responsibilities, management commitment, and coordination among organizational entities of the field asset physical security program to ensure compliance with the organization's security policy and other regulatory commitments.

2. Formal, documented procedures to facilitate the implementation of the non-control center physical and environmental protection policy and associated physical and environmental protection controls

3. Development and maintenance of personnel lists with authorized access to facilities containing assets not within the control center, along with appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within an organization should review and approve the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

4. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the non-control center facility where assets reside (excluding those areas within the facility officially designated as publicly accessible)

5. Controls entry to field asset facilities containing control systems using physical access devices and guards

6. Monitors physical access to the field asset to detect and respond to physical security incidents. Also, access logs are reviewed on an organization-defined frequency.

7. The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and includes lighting for emergency exits and evacuation routes.
8. The organization implements and maintains fire suppression and detection devices and systems that can be activated in the event of a fire.
9. The organization regularly monitors the temperature and humidity within field asset facilities containing control system assets and ensures they are maintained within acceptable levels.
10. The organization protects the field asset from damage resulting from water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
11. The organization implements field asset location technologies to track and monitor the movements of personnel and vehicles within the organization's controlled areas to ensure they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.
12. The organization locates field assets to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
13. The organization protects field asset power equipment and power cabling from damage and destruction.
14. The organization employs hardware (cages, locks, cases, etc.) to detect and deter unauthorized physical access to non-control center devices.

Continuity and Disaster Planning

As the grid evolves and the integration of advanced control systems and information technology increases the automated nature of the grid, Contingency Planning and Disaster Recovery Planning (CP/DRP) will become more complex and more integral to maintaining stable overall grid operations. The availability of real-time event management capabilities associated with the evolution of communication and control systems will create greater reliability but require greater analytical resources to assess the nature of events (malicious, inadvertent, or acts of nature) within the grid. Unfortunately, this will also translate into increased costs associated with CP/DRP activities as they themselves become more dependent on increasingly complex technology to sustain a leaner but more stable grid operating posture. Finally, life cycle and legacy issues will affect operator's CP/DRP planning, as technology refreshers will become more frequent as new technology enters widespread use across the grid.

With the move toward a highly automated and self-healing grid, the complexity of recovery after a major grid-impacting event will increase substantially. The amount and types of physical equipment requiring replacement (and pre-positioning/stockpiling) will naturally increase. Additional security controls will need to be applied to CP/DRP activities and logistic acquisition. This is to ensure that the introduction of replacement equipment and potential temporary loss of access control integrity during grid reconstitution does not result in an increased likelihood of compromise to the communication and control systems.

A positive effect will be greater real-time compared to post-mortem analyses and event management as more data become available to control centers. However, this will complicate the analysis and decision cycle as data overload and conflicting data indicators become real possibilities. This could have the unintended effect of actually slowing down event response and even result in the possibility of causing the initiation of CP/DRP activities under false conditions in those cases where the grid continues to operate nominally. However, compromised data fed to the control center creates a conflicting picture of the grid's operating posture. Ensuring data integrity for CP/DRP triggering events will be critical.

Operating in an environment where equipment cycles are measured in decades has provided a benefit to CP/DRP planners in the industry. They could be fairly sure that replacement for a failed piece of equipment was in the operator's stockpiled reserve, even if the failed equipment was manufactured decades before. The smart grid communications and sensors expected to be integral to support the bulk power network will have life spans measured in years rather than decades. Thus, stockpile rotation will become critical.

In addition to the failure issue, the increased use of equipment with native software means that patching will become a significant issue as well. The replacement of a failed component that has resided in a depot site for several years will require a significant software security patch monitoring and enforcement regime to ensure "old" vulnerabilities are not reintroduced into the system every time a failed device is replaced.

R&D Requirements

Cyber security

The electric smart grid promises increased capacity, reliability, and efficiency through the marriage of communications and computing systems with the existing electricity network. This increased dependency on information technology creates additional vulnerabilities stemming from trusted and untrusted devices, cyber intrusion, and data/communications corruption potentially leading to devastating physical and logical effects. The scale and complexity of the smart grid, along with its increased connectivity and automation, make the task of cyber protection and security a cross-cutting challenge. One necessary R&D component is the development and enhancement of device integration standards along with best practices to promote cyber security. Such an approach should provide a convenient, yet rigorous framework for industry personnel to assess the reliability impacts of adding new devices to an existing smart grid infrastructure.

In the face of a successful attack, response and recovery approaches may require the isolation of core components necessary for bulk power system reliability from devices and systems that are prone to cyber attack. Thus, another significant R&D component is secure and reliable approaches to defining how to separate core reliability components of a smart grid from those elements that optimize performance.

Given the breadth of stakeholders, it is imperative that members from academia, industry, national labs, and government bodies collaboratively focus on cyber security for specific R&D

needs in support of designing a smart grid based upon a defense-in-depth architecture. Such a system is necessary for the future security and reliability of the smart grid. One of the primary applications for the integration of cyber security is the ability to form a predictive early warning system that can coordinate preventive and adaptive measures (on a real-time basis) that contain any attacks to the broader smart grid and quickly recover any impacted assets. This approach will aid in ensuring that even the most sophisticated cyber attacks have limited to no impact on the North American power grid.

Many of the existing security solutions that are available do not have true intelligence of the power system and control domain, and do not enable a predictive security framework. Security design and verification, and cross-domain real-time security event detection, analysis, and response tools are particularly needed. Additionally, a set of problems that could be addressed are those arising from malicious falsification of data—an integrity problem. In particular, malicious falsification of information must be distinguished from elements that may be attributable to "noise." On the design side, it is important to develop methods for defining and positioning sensors with predetermined redundancy to reliably differentiate among a variety of signals. Finally, new state estimation procedures should be designed to be robust against such attacks.

Cloud Computing

Cloud computing is the provision of one or more aspects of the computing environment (infrastructure, platform, application) through an array of resources generally[75] accessed over a large network, such as the internet. Advocates of cloud computing point to various advantages, such as the following:

- **Reliability/Resiliency/Agility/Scalability** — By locating and dynamically allocating resources "in the cloud" the loss of service in any one location does not halt operations, systems can be scaled as needed, and short-term needs can be responded to.
- **Cost Savings** — By paying for facilities and systems as they are used by multiple entities, the opportunity for cost savings by spreading costs over a larger array of applications and users and making fuller, more efficient use of resources.

Because the advantages of internet-based cloud computing involve shared quasi-public resources, security is inherently an issue. At this time, the security risks associated with cloud computing for grid operations and planning are not well identified or understood. Among the identified concerns are the following:

- **Accountability/Traceability** — Services may be provided by an affiliate, partner, or subsidiary of the contracted provider.
- **Data export regulations** — Unless the physical location of the equipment providing service is known, regulations regarding data export may be inadvertently violated.

[75] Some companies are suggesting the use of a "private cloud" in which the entire system remains controlled by the company desiring to use it. While this is contentious in the cloud-computing community, it does provide many of the reliability advantages of cloud computing with a more known set of security risks.

- **Routing** — Unless one can control the routing of data, the opportunity for interception or "man in the middle" attacks increases.
- **Control of Confidential or Sensitive Data** — Use of cloud-based storage and processing requires the loss of some levels of control over whom or what has access to the data. Encryption may partially address data transmission and storage, but data processing requires decrypted data, which in turn presents, among other issues, encryption key management issues.

The issue is well summarized by the following quotes:

> *One of the biggest security concerns about cloud computing is that when you move your information into the cloud, you lose control of it. The cloud gives you access to the data, but you have no way of ensuring no one else has access to the data. How can you protect yourself from a security breach somewhere else in the cloud?* – Mr. Eric Mandel[76]

> *[Cloud computing is] a difficult choice for any company considering the platform for protecting sensitive information [because of] the inability or unwillingness of cloud providers to give assurances of the controls surrounding computing resources….it would be difficult to impossible to achieve Payment Card Industry (PCI) compliance in a cloud provided by a service provider given the requirements for understanding precise system and network configurations and controlling access to the systems and the credit-card data.* – Mr. Dick Mackey[77]

At this time, reliance of grid operations on cloud computing resources appears inadvisable, but significant research in this area for the long-term implications of this computing technology is strongly recommended.

Computational Capabilities

Implementation of many advanced sensing, communication, and control solutions in smart grid deployments will require fundamentally more powerful computational capabilities. Today's EMS applications will have to be upgraded by new modeling and computing algorithms. Models depend on the type of measurements and control actions allowed. In addition, it is necessary to represent many previously unused technologies when simulating and analyzing performance of the smart grid. Research on converting data into information to be used and useful for operating and planning future systems is necessary to support operators who might face data saturation.

This is a significant R&D task and may be critical to the success of the smart grid in the long term. For successful and reliable smart grid implementation, it is essential to align the representation of the physical grid with its models, communication, and decision-making software.

---

[76] http://www.networkworld.com/news/2009/042709-burning-security-cloud-computing.html, quoting Eric Mandel, CEO of managed hosting services provider BlackMesh in Herndon, Va.

[77] *Ibid*, quoting Dick Mackey, analyst at consultancy System Experts.

Chapter Findings

Successful integration of smart grid devices and systems should include appropriate cyber and control system security. A cyber and physical secure smart grid will require advanced technological solutions. For example, cyber security requires focused efforts on forensic tools and network architectures to support graceful system degradation so operators would be able to maintain reliability with fewer controls.[78]

"Defense-in-depth" approaches, when coupled with risk assessment, can provide an overarching organizational approach to cyber security management. Robust cyber security involves the application of layered "defense-in-depth" solutions to protect critical elements of the network environment. The Risk Matrix and Risk Cube assess risk and determine which defensive measures are appropriate.

In addition, standard harmonization between North American Standard Development Organizations in Canada and the U.S. is important for the successful deployment of smart grid devices and systems, while addressing potential cyber vulnerabilities.

R&D is required to develop new tools and architectures that can support integration of smart grid devices and systems with advanced IT and communications technologies. It is imperative that members from academia, industry, national labs, and government bodies collaboratively focus on cyber security for specific R&D needs in support of designing a smart grid with a defense-in-depth architecture along with development of risk management models to manage cyber-security vulnerabilities.

[78] NERC's report entitled *High-Impact, Low Frequency Event Risk to the North American Bulk Power System* at http://www.nerc.com/files/HILF.pdf

6.0 Conclusions and Recommendations

The success of integrating smart grid concepts and technology will rely heavily on maintaining reliability of the bulk power system during its evolution. As part of this effort, an agreed-upon industry definition of the smart grid was developed:

> **smart grid** — *The integration and application of real-time monitoring, advanced sensing, communications, analytics, and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure, reliable, and efficient electric power system, from generation source to end-user.*

The expansive and rapidly evolving nature of smart grid will require vigilance from all stakeholders. Key conclusions from this assessment are:

- *Government initiatives and regulations promoting smart grid development and integration must consider bulk power system reliability*
- *Integration of smart grid requires development of new tools and analysis techniques to support planning and operations*
- Smart grid technologies will change the character of the distribution system, and they must be incorporated into bulk power system planning and operations
- *Cyber security and control systems require enhancement to ensure reliability*
- *Research and development (R&D) has a vital role in successful smart grid integration*

Recommendations

NERC should:

- Engage standard development organizations in the U.S. and Canada to increase coordination and harmonization in standard development;
- Monitor smart grid developments and remain engaged in its evolution (federal, state, and provincial efforts, ISO and RTO, IEEE and IEC, etc.);
- Support the development of tools, technology, and skill sets needed to address bulk power system reliability, including cyber and control systems, modeling, simulation, and operator tools and training; and
- Enhance NERC's Reliability Standards, if needed, as the character of the smart grid crystallizes over time.

A detailed work plan that outlines future Smart Grid Task Force activities is presented in Appendix 2.

Appendix 1: Smart Grid and Reliability Standards

NERC Reliability Standards and Smart Grid

This appendix provides NERC's definition of reliability and identifies how successful integration of the smart grid may provide new options to meet NERC's Reliability Standards.

Bulk Power System Reliability

The mission of NERC is to ensure the reliability of the bulk power system. To understand this mission in the context of smart grid, it is important to understand NERC's perspective on bulk power system reliability.

NERC's traditional definition[79] of "reliability" consists of two fundamental concepts: adequacy and operating reliability:

- **Adequacy** is the ability of the electric system to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.
- **Operating reliability** is the ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components.

This definition was further clarified to understand the characteristics leading to the "*Adequate Level of Reliability*":[80]

1. the system is controlled to stay within acceptable limits during normal conditions;
2. the system performs acceptably after credible contingencies;
3. the system limits the impact and scope of instability and cascading outages when they occur;
4. the system's facilities are protected from unacceptable damage by operating them within facility ratings;
5. the system's integrity can be restored promptly if it is lost; and
6. the system has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.

Throughout this report, successful integration of smart grid was evaluated against these reliability concepts.

[79] http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf
[80] http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf

The NERC Rules of Procedure states that systems "as identified by regional entities, electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher will be considered part of the bulk power system."[81] Similarly, Section 215, ELECTRIC RELIABILITY, of the U.S. Federal Power Act defines the bulk power system as:

> *''(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and*
>
> *''(B) electric energy from generation facilities needed to maintain transmission system reliability."*[82]

NERC's role as the Electric Reliability Organization (ERO) in the U.S. is to develop, implement, and enforce mandatory Reliability Standards for all users, owners, and operators of the bulk power system. In Canada, NERC presently has memorandums of understanding in place with five provincial authorities and the Canadian National Energy Board.

Smart Grid Options and NERC Standards

As the smart grid evolves, NERC Reliability Standards that do not already[83] address smart grid devices and systems may need enhancement.[84] A list of Reliability Standards categories[85] and the "Smart Grid Task Force Comments" in Table A-1 below indicate areas where smart grid options may provide additional ways to meet NERC Standards.

[81] http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20100121.pdf
[82] http://homeland.house.gov/SiteDocuments/20080521141621-50243.pdf
[83] The scope and requirements of many Reliability Standards are not prescriptive so changes may not be necessary, regardless of the development of smart grid.
[84] To learn more about the Reliability Standards development process, please review: Reliability Standards Development Procedure, Version 7, (FERC Approved: February 5, 2010): http://www.nerc.com/fileUploads/File/Standards/FERC_Approved_RSDP-V7_2010Feb5.pdf
[85] A complete set of Reliability Standards (approved 5/3/10) may be found at: http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf

Table A-1: NERC Reliability Standard and Smart Grid Options

NERC Reliability Standard Categories	Title	Smart Grid Task Force Comments
BAL	Resource and Demand Balancing	• PMU waveforms support and sub-second sampling may benefit reliability by supporting CPS1 and CPS2, and providing pre-disturbance data detection and remediation. • Better data from real-time monitoring tools could enable easier calculation of variable frequency bias. • Demand Response and energy storage could be used to improve frequency response. • Energy aggregators may become more popular with smart grid implementations. • Demand Response can provide regulating reserves.
CIP	Critical Infrastructure Protection	• Smart grid devices/systems will be tested to determine the category where they reside. • Advanced sensing devices may facilitate accurate and timely identification and reporting. • A number of Critical Cyber Assets may be expanded to include smart grid devices and related systems. • More frequent reviews (currently annually) may be necessary to determine if new smart grid devices coming online should be classified as Critical Cyber Assets. • Awareness and training programs may be expanded to convey important knowledge about smart grid devices classified as Critical Cyber Assets. • Expansion of Cyber Vulnerability Assessment to include new Electronic Security Perimeters created to handle smart grid devices classified as Critical Cyber Assets. • Creation of new and expanded Physical Security Perimeters and/or attendant physical access controls to encompass new Electronic Security Perimeters established • Additional checks, procedures, tests, and controls to ensure significant changes to smart grid devices classified as Critical Cyber Assets do not adversely affect existing cyber security controls may be necessary • A reevaluation of the definition of Cyber Security Incident to make sure it includes any peculiarities introduced by smart grid devices classified as Critical Cyber Assets • Expansion of the Cyber Security Incident Response Plan to encompass smart grid devices classified as Critical Cyber Assets may be necessary • More cyber incidents may be observed or recorded as a result of a large addition of smart grid devices classified as Critical Cyber Assets. • A review of recovery plans that include smart grid devices classified as Critical Cyber Assets may be necessary.

NERC Reliability Standard Categories	Title	Smart Grid Task Force Comments
COM	Communications	• Smart grid data may be included in the operating information exchanged between entities listed in the standard. • Entities may need to include plans for loss of telecommunications related to smart grid devices. • The smart grid may enable firm load customers to voluntarily respond to system conditions via demand response.
EOP	Emergency Preparedness and Operations	• Smart grid data and technologies can support plans to mitigate operating emergencies on the transmission system for insufficient generating capacity, load shedding, and system restoration. • Operation of selected smart grid devices may be added as part of Energy Emergency Alert Levels. • Voluntary DSM as a result of smart grid data signals should be considered when declaring Energy Emergency Alerts • As mentioned previously in this paper, smart grid applications are to be self-healing. • Some load shedding plans are affected by the resilient nature of the smart grid. • With smart grid devices, more potential triggers are available to start the recording of disturbance data. • Smart grid implementation will directly impact system restoration plans. • PMUs can be used by grid operators to select the best interconnection points when connecting islands during system restoration. • Wide area monitoring systems will help Reliability Coordinators better assess grid conditions and coordinate system restoration. • Smart grid energy generation and storage capabilities may be used in black start capabilities, especially when looking at the usefulness of resource aggregators. • Entities may need to include energy storage devices used during black start plans in their testing program.

NERC Reliability Standard Categories	Title	Smart Grid Task Force Comments
FAC	Facilities Design, Connections, and Maintenance	• Facility connection requirements for end-user and generation facilities may expand due to smart grid technologies. • Inclusion of selected smart grid devices as end-user devices may require entities seeking to use these devices to participate in Transmission and Resource planning activities • Smart grid devices may change facility ratings. • Entities must ensure that dynamic facility ratings are effectively communicated to all appropriate parties. • New and more robust applications using forensic smart grid device data may play an increasingly significant role in determining Operating Limits (OL) and for the Planning Horizon; therefore, this may need to be defined in the OL Method document (to include SOL and IROL). Possible applications include: 1. dynamic ratings 2. planning stability analysis (includes transient, voltage, and dynamic) 3. contingency analysis 4. planning power flow 5. remedial action 6. pattern recognition • New and more robust applications using smart grid data may play an increasingly significant role in determining transfer capability across multiple Regions • Assumptions and criteria used to calculate transfer capabilities in the planning horizon (beyond 13 months) depend on forecasts of generation and load. Potential benefits from changes in load response to system conditions need to be understood.
INT	Interchange Scheduling and Coordination	• Dynamic interchange scheduling practices may change due to smart grid implementation. • Data requirements from other functional entities including load-serving entities and generation owners and operators may change due to smart grid data availability.
IRO	Interconnection Reliability Operations and Coordination	• Forensic and real-time smart grid device data may provide better input to forecast IROL and SOL violations. Any additional benefits from smart grid applications may be accounted for in the day-ahead plans. They can provide input into new and improved applications to conduct more robust current-day reliability assessments. • Real-time smart grid device data may be beneficial as input to new and improved applications to provide more reliable alternatives to TLR (e.g., reconfiguration, redispatch, or load shedding) to mitigate potential IROL violations. • Forensic and real-time smart grid device data may be beneficial as input to new and improved applications to provide better next-day Operational Planning Analyses and current-day Real-Time Assessments. • Data requirements may change as a result of smart grid implementation.

NERC Reliability Standard Categories	Title	Smart Grid Task Force Comments
MOD	Modeling, Data, and Analysis	• Methods for calculating Total Transfer Capability (TTC) and Available Transfer Capability (ATC) may need to be expanded to accommodate study results produced by new and enhanced applications using additional data provided by the smart grid. • More data from smart grid devices may allow larger applications spanning multiple Regional areas to support more consistent and uniform ATC and TTC calculations over increasingly larger portions of the interconnection. • Transmission Reliability Margin (TRM) definition may need to be expanded to include electricity storage and demand response, thereby affecting requirements for TRM methodology and documentation. • Probabilistic analysis may be required to capture the full range of possibilities of depicting bulk power system conditions. • More accurate data from forensic and real-time devices should allow improved benchmarking of models after a disturbance. • The relationship of actual and forecast demands may change due to smart grid implementation. New data reporting requirements may be necessary. • Forensic and real-time data provided by smart grid devices may provide better information for past data and future forecasts. • Smart grid implementation may change how interruptible demands are managed.
NU	Nuclear	• Smart grid data availability may change how off-site power requirements are monitored and calculated.
PER	Personnel Performance, Training, and Qualification	• Data from forensic and real-time devices could be used to improve simulator-based training exercises.

NERC Reliability Standard Categories	Title	Smart Grid Task Force Comments
PRC	Protection and Control	• Data from PMUs could help operations personnel quickly review protection system operations and detect misoperations. • UFLS implementation may be improved by deploying smart grid devices through information or advanced controls, and could support adaptive UFLS schemes. • Smart grid devices may provide additional real-time and forensic data for analyzing UVLS performance during both operation and misoperation. This also applies to data before, during, and after an under-voltage event. • Advanced relaying with self-monitoring capabilities could allow for increased maintenance intervals. • New types of protection schemes may take advantage of PMU measurements that can signal when an instability condition is about to occur and automatically respond by opening breakers to minimize risk of the instability. • Real-time monitoring devices provide faster detection/analysis of SPS misoperations. • DME devices that are able to be time stamped across the entire Interconnection, may enable more accurate and robust disturbance monitoring over a wider area. • PMU phasor and phase difference measures are used as input to these relays to allow for dynamic calculation of theoretical power transfer capability.
TOP	Transmission Operations	• Operational planning study assumptions and criteria may change to anticipate voluntary DSM due to smart grid implementation. • Smart grid devices may provide additional real-time data to aid operators during normal operations to ensure that their system is within voltage, stability, and thermal limits. • Improved state estimation, contingency analysis, and offline study tools can help ensure the system is operated within established limits. • Real-time monitoring tools will help improve the accuracy and latency of data provided to Reliability Coordinators and neighboring entities. • Wide area monitoring systems should allow for better visualization of operating conditions and alarm prioritization. • Smart grid devices may provide real-time and forensic data and contribute to the inputs for determining the causes of SOL violations
TPL	Transmission Planning	• Smart grid devices may provide real-time and forensic data that may be fed into various system simulations. • Data from real-time and forensic devices could be used to improve dynamic load models used in stability simulations.
VAR	Voltage and Reactive	• Smart grid devices may support AVR systems and provide real-time information with regards to reactive resources. • Real-time monitoring tools could allow SVCs and STATCOMs to automatically be inserted to provide VAR support. • Smart grid devices may provide information and control functions for reactive power schedules.

Appendix 2: Follow-on Work Plan

Follow-on work for this task force will focus on those smart grid devices/systems that are most likely to have a material impact on planning and operations. While there may be some interest in investigating the broad range of various issues and technologies related to smart grid, a focused approach on specific technologies will have significant value for reliability of the bulk power system and future NERC programs and activities. These efforts address Item #K (Smart Grid Security) of the ESCC Critical Infrastructure Strategic Roadmap and the Technical Committee Critical Infrastructure Protection Coordinated Action Plan.[86]

1. Integration of smart grid devices and systems onto the bulk power system requires development of new planning and operating tools, models, and analysis techniques

Identify the tools and models needed by planners/operators for successful integration of smart grid devices and systems

SGTF – Planning/Operations Subgroup | Start Date: 1st Qtr. 2011 | End Date: 2nd Qtr 2012

Review modeling requirements for planning and operations to measure and understand system performance while accommodating smart grid integration as follows:

- identify bulk power system modeling requirements for bulk power level smart grid devices/systems, communications, IT, and control system interfaces;
- evaluate how to include cyber security and control system interfaces into planning/operation simulations to enhance control system security;
- assess the affect of bulk system smart grid devices/systems on system stability;
- Determine successful integration considerations to ensure reliability
- review the Modeling, Data, and Analysis (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements; and
- provide input into smart grid security and NERC's Standards processes as applicable.

2. Integration of smart grid devices/systems will change the character of the distribution system

Assess reliability considerations that need to be addressed with the integration of large amounts of smart grid devices and systems on the distribution system

SGTF – Planning/Operations Subgroup | Start Date: 1st Qtr. 2011 | End Date: 4th Qtr 2012

Review existing and new distribution smart grid devices and systems and assess if there are any potential failure modes that they need to address as part of their integration as follows:

- identify bulk power system modeling requirements for distribution-level smart grid devices/systems, communications, IT, and control system interfaces;

[86] See agenda item 2 of http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf and http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf

- evaluate how to include the affects of distribution-level cyber security and control system interfaces in the modeling/simulation of bulk power systems;
- assess the impact of distribution smart grid system devices/systems on system stability;
- Determine successful integration considerations to ensure reliability
- review the Modeling, Data and Analysis Standards (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements; and
- provide input into smart grid security and NERC's Standards processes as applicable.

3. Engage Standard Development Organizations in the U.S. and Canada to increase coordination and harmonization in standard development

Form liaisons with U.S. and Canadian standards-setting groups to ensure coordinated and harmonized standards to support reliability

SGTF – Cyber Security Start Date: 1st Qtr. 2011 End Date: 4th Qtr 2013

Create pathways for harmonization and coordination as follows:

- monitor smart grid developments and remain engaged in its evolution (federal/state/provincial efforts, ISO/RTO, IEEE/IEC, etc.);
- review existing and new standards developments;
- indentify those standards that are vital to bulk power system reliability, including cyber and control system security;
- work with Canadian and U.S. standards-setting organizations to ensure coordination and harmonization of vital standards; and
- report back on ongoing activities to the PC and CIPC.

4. Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration

Further refine defense-in-depth and risk assessment approaches to manage cyber and physical security with smart grid integration.

SGTF – Cyber Security Start Date: 1st Qtr. 2011 End Date: 4th Qtr. 2012

Refine and test defense-in-depth and risk assessment approaches as follows:

- further refine technical methods;
- identify characteristics that should be measured to provide a current reference and future system measurement;
- form metrics of performance and risk;
- pilot the approach for bulk power system application;
- further refine as required;
- develop a report outlining the methods and documenting the results; and
- report back on ongoing activities to the PC, OC, and CIPC.

Appendix 3: International Smart Grid Developments

Several countries outside North America have smart grid initiatives underway. This section provides a brief summary of some mature initiatives, which may provide insight.

Australia

The Australian Government has committed up to $AUS 100 million to develop the smart grid, Smart City (SGSC) demonstration project in partnership with the energy sector. The initiative will support the installation of Australia's first commercial-scale smart grid. Smart grids combine advanced communication, sensing, and metering infrastructure with existing energy networks. This enables a combination of applications that can deliver a more efficient, robust, and consumer-friendly electricity network. Smart grid infrastructure uses sensors, meters, digital devices, and analytic tools to automate, monitor, and control the two-way flow of energy from power plant to plug. The initiative is being delivered by the Department of the Environment, Water, Heritage and the Arts; in close consultation with the Department of the Prime Minister and Cabinet; the Department of Broadband, Communications and the Digital Economy; and the Department of Resources, Energy and Tourism.

Demonstrating best practice
This initiative demonstrates Australia's position at the forefront of global efforts to use energy more efficiently, ensure network reliability, and combat climate change. SGSC will deliver a fully integrated, commercial-scale smart grid and will inform the business case for broader industry investment in smart grids in Australia. SGSC will employ a mix of innovative technologies and demonstrate the potential of smart grids to monitor electricity supply, manage peak demand, and help customers make informed choices about their energy use. The project will provide a comprehensive dataset about the potential benefits of smart grid appliances, network improvements, and technological efficiencies whilst offering details on the effects of greater knowledge about energy consumption on consumer behavior. It is anticipated that interim data and results will be made available publicly over the course of the project to disseminate lessons to other electricity networks that are developing smart grids and to assist industry with the development of smart grid technologies. SGSC will also demonstrate the capacity of a smart grid to integrate electricity from renewable and distributed energy sources—such as wind and solar generation—more effectively into the existing electricity network. The data may also explore the capacity of smart grids to enable better integration of distributed generation, distributed storage, and plug-in electric vehicles, to allow better dispatch of energy to support the grid.

Project Design
The SGSC demonstration project will deploy a live, integrated, smart grid of commercial size and scope in a community within a single electricity distributor's network. The location of SGSC should provide a reasonable representation of the wider grid to produce credible results that can inform broader industry-led adoption of smart grids in Australia. For this reason, a model

demonstration area would include urban, suburban, and rural areas and contain diverse network, geographic, climate, and customer characteristics. A range of smart grid technologies and applications will be demonstrated. The SGSC project is expected to include demonstrations of customer applications; active voltage support and power factor correction; distributed storage; fault detection, isolation, and restoration; electric vehicle support; substation and feeder monitoring; and wide-area management and distributed generation. Submissions from industry consortia will be assessed by an independent panel and the successful consortium announced by government in mid 2010.

Germany

The "E-Energy: ICT-based Energy System of the Future" (E-Energy) program represents Germany's national smart grid program under the technology policy of the federal government. E-Energy includes six projects selected for funding (€140M), and their implementation paves the way towards an "Internet of Energy" that intelligently monitors, controls, and regulates the electricity system.[87] The program emphasizes efficiency and renewable integration, and each project was selected on meeting the following criteria:

1. creation of an E-Energy marketplace that facilitates electronic legal transactions and business dealings between all market participants;
2. digital interconnection and computerization of the technical systems and components, and the process control and maintenance activities based on these systems and components, such that the largely independent monitoring, analysis, control and regulation of the overall technical system are ensured; and
3. online linking of the electronic energy marketplace and overall technical system so that real-time digital interaction of business and technology operations is guaranteed.

The following E-Energy projects were selected:[88]

- **E-DeMa** — The "development and demonstration of decentralized integrated energy systems on the way towards the E-Energy marketplace of the future" project in the Rhein-Ruhr area. Highly heterogeneous density of supply is characteristic of the model region of the E-DeMa project, which comprises rural and urban areas with two different distribution networks in the Rhine-Ruhr area. This results in particular technical challenges, which are overcome by the creation of an intelligent ICT infrastructure. The research project builds on the existing distribution of digital smart meters to drive energy efficiency in integrated homes (new "ICT gateway"). The focus of the project includes the development of an intelligent power consumption control system and the real-time collection and provision of consumption data. Furthermore, the project also aims to optimize network operation management in decentralized distribution networks.
- **eTelligence** — Cutting-edge communication technology is the key, with a completely new marketplace for energy developing in and around Cuxhaven. Producers and

[87] http://www.e-energy.de/documents/bmwi_Leuchtturm_E-Energy_E_s4.pdf
[88] http://www.e-energy.de/en/32.php

consumers can not only use this marketplace to buy and sell electricity, but can also offer system services and idle power, and help reduce the load on the power grid. With minimum effort, even private households can put minute amounts of electricity on the market by using almost-fully-automated plug-and-play appliances that operate automatically in the market in line with the pre-programmed instructions of the appliance owners.

The E-Energy marketplace in Cuxhaven primarily takes advantage of the many refrigerated warehouses and the spa in the town. The water in the pool is heated if the electricity from the CHP power plants is needed. The refrigerated warehouses are cooled more than usual when electricity is cheap, with controls developed within the framework of E-Energy ensuring that the frozen fish does not spoil in the process.

- **MEREGIO** — The E-Energy MeRegio model house (in Baden) generates power on the roof or using a mini combined heat and power plant (CHP) in the basement. The household appliances are interlinked via communication technology, and connected to a smart system platform. The electric vehicle is parked in the garage: the vehicle battery is charged when the mini-CHP produces more electricity than the grid can take. If necessary, the electricity from the battery can also be fed into the grid. As a partner of the electricity provider, the consumer can view the processes in the system via an internet portal and play an active role in market activities.
- **Mannheim Model City** — The Model City of Mannheim project concentrates on an urban conurbation with a high penetration rate in which renewable and decentralized sources of energy are used. The trial uses new methods to improve energy efficiency, grid quality, and the integration of renewable and decentralized sources of energy into the urban distribution network. The focus is on developing a cross-sectoral approach (involving electricity, heating, gas, and water) to interconnect the consumption components with a broadband power line infrastructure. Proactive users in the energy market ("prosumers") can gear their power consumption and their power generation towards variable pricing structures. Furthermore, real-time information and energy management components also aim to help the customer contribute to even greater energy efficiency.
- **RegModHarz** — With E-Energy, the control centre at the renewable energy combined-cycle power plant in the Harz region receives real-time information on the energy situation in the region. With a complete overview of power generation, storage, and consumption, it is possible to make forecasts, and optimum use can be made of the renewable energy sources. The Harz model region boasts extensive sources of renewable energy, ranging from wind plants and solar power systems to hydroelectric power stations.
- **SmartW@TTS** — Greater efficiency and consumer benefit with the Internet of Energy and the "smart kilowatt-hour" model region of Aachen. SmartW@tts is developing new approaches for the energy market, portfolio management, the measurement and analysis of power consumption, and invoicing systems. SmartW@tts defines the Internet of Energy on three levels: at the system level, power generation, consumption and control systems communicate with one another. At the business level, the stakeholders plan,

control, monitor, and optimize the efficient use of plants and contract conditions depending on their particular market role. The information level is the centerpiece of E-Energy, linking the other two levels and allowing the stakeholders and systems in the "energy Web" to safely communicate with one another in real-time.

South Korea

South Korea's Ministry of Knowledge Economy announced a $24B program for smart grid technology in March 2010. The plan calls for all customers to be using smart-grid technology by 2030, with the goal of reducing power use by three percent and reducing greenhouse gas emissions by 150 million tons. This program is a continuation of South Korea's developments in smart grid that largely began in 2009 with the Smart Grid Tested on Jeju Island. The test bed serves to demonstrate advanced technologies and R&D results, develop business models, and serve as the foundation for the commercialization and industrial export of new technologies. The overall program is outlined in Figure A-1 below.[89]

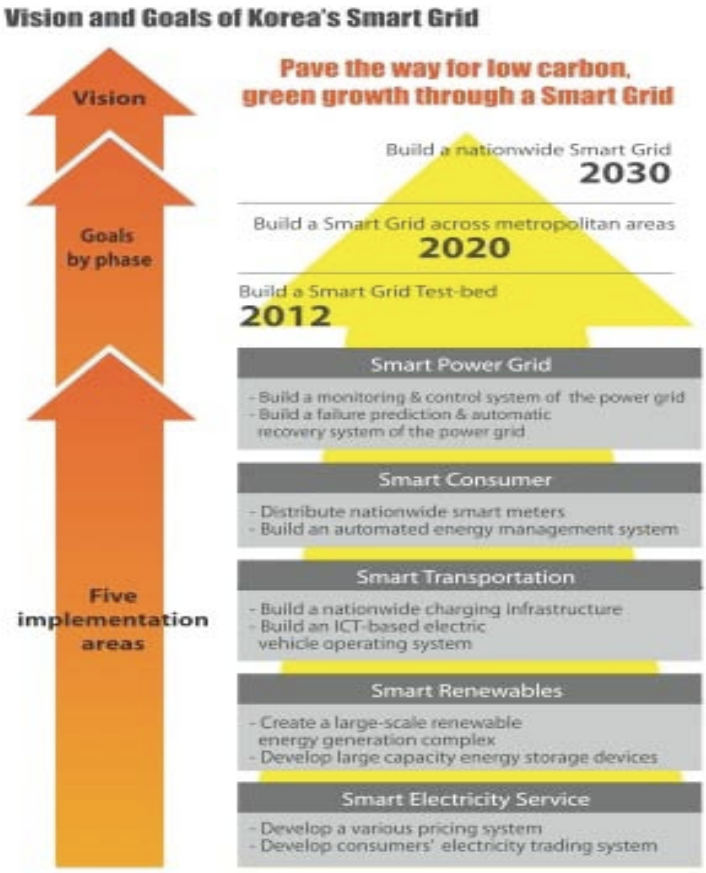


Figure A-1: Vision and Goals of South Korea's Smart Grid

[89] www.smartgrid.or.kr/eng, http://www.koreatimes.co.kr/www/news/biz/2010/04/123_57502.html

Abbreviations

A/C	Air Conditioning
AC	Alternating Current
ACCC	Aluminum Conductor Composite Core
ACCR	Aluminum Conductor Composite Reinforced (transmission cable)
ACSS	Aluminum Conductor Steel Supported (transmission cable)
AGC	Automatic Generator Control
ALR	Adequate Level of Reliability
AMI	Advanced Metering Infrastructure
ARRA	U.S. American Recovery and Reinvestment Act of 2009
ASIFI	Average System Interruption Frequency Index
ATC	Available Transfer Capability
AVR	Automatic Voltage Regulator
BAL	Resource and Demand Balancing (NERC Reliability Standards)
BES	Bulk Electric System
BEV	Battery Electric Vehicle
BPS	Bulk Power System
CAES	Compressed Air Energy Storage
CBM	Capacity Benefit Margin
CCA	Critical Cyber Assets
CHP	Combined Heat and Power
CIGRE	International Council on Large Electric Systems
CIP	Critical Infrastructure Protection (NERC Reliability Standards)
COM	Communications (NERC Reliability Standards)
COTS	Current Off-The-Shelf
CP/DRP	Contingency Planning and Disaster Recovery Planning
CPS1	NERC Control Performance Standard 1
CPS2	NERC Control Performance Standard 2
CSC	Convertible Static Compensator
dc	Direct Current
DCLM	Direct Control Load Management
DCS	Distributed Control Systems
DER	Distributed Energy Resources
DG	Distributed Generation
DLC	Direct Load Control
DLR	Dynamic Line Rating
DME	Disturbance Monitoring Equipment
DMS	Distribution Management System
DMZ	Network Demilitarized Zone
DNP3	Distributed Network Protocol
DOE	U.S. Department of Energy
DSM	Demand-Side Management
DVAr	dynamic VArs device
EE	Energy Efficiency
EEA	Energy Emergency Alert
EIA	U.S. Energy Information Administration (of DOE)
EISA	U.S. Energy Independence and Security Act of 2007

EMS	Emergency Management System
EOP	Emergency Preparedness and Operations (NERC Reliability Standards)
ERO	Electric Reliability Organization
ESP	Electronic Security Perimeter
EV	Electronic Vehicle
FAC	Facilities Design, Connections, and Maintenance (NERC Reliability Standards)
FACTS	Flexible Alternate Current Transmission System
FCC	U.S. Federal Communications Commission
FERC	U.S. Federal Energy Regulatory Commission
FCL	Fault Current Limiting
FIT	Feed-In Tariff
FPL	Federal Power Act
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRC	Governance, Risk, and Compliance
GWh	Gigawatt-Hour (one billion watts per hour)
HAN	Home Area Network
HVdc	High Voltage Direct Current
Hz	Hertz (one cycle per second)
ICCP	Inter-Control Center Communications
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IGBT	Insulated-Gate Bipolar Transistor
INT	Interchange Scheduling and Coordination (NERC Reliability Standards)
IPS	Intrusion Prevention System
IRO	Interconnection Reliability Operations and Coordination (NERC Reliability Standards)
IROL	Interconnection Reliability Operating Limits
ISN	Interregional Security Network
ISO	Independent System Operator
IT	Information Technology
IVVC	Integrated Volt/VAr Control
JIP	Just-in-place
JIT	Just-in-time
kV	Kilovolts (one thousand volts)
kW	Kilowatt (one thousand watts)
kWh	Kilowatt-Hour (one thousand watts per hour)
LAN	Local Area Network
LED	Light Emitting Diode
LOLP	Loss of Load Probability
LSE	Load Serving Entity
LTRA	Long-Term Reliability Assessment
MOD	Modeling, Data, and Analysis (NERC Reliability Standards)
m/s	meters per second
MTU	Master Terminal Units
MVA	Megavoltampere (one million voltamperes)
MVAr	Megavars
MW	Megawatt (one million watts)
MWh	Megawatt-Hour (one millions watts per hour)
NaS	Sodium Sulfur
NASPI	North American SynchroPhasor Initiative

NBP	National Broadband Plan
NIST	U.S. National Institute of Standards and Technology
NMS	Network Management Systems
NUC	Nuclear (NERC Reliability Standards)
OMS	Outage Management System
OSPF	Open Shortest Path First
PAC	Programmable Automation Controller
PAR	Phase Angle Regulators
PbA	Advanced Lead Acid
PC	NERC Planning Committee
PCI	Payment Card Industry
PDC	Phasor Data Collector
PER	Personnel Performance, Training, and Qualification (NERC Reliability Standards)
PEV	Plug-In Electric Vehicle
PJM	PJM Interconnection
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PMU	Phasor Measurement Units
POD	Power Oscillation Damping
POTS	Plain Old Telephone Service
PQ	Power Quality
PRC	Protection and Control (NERC Reliability Standards)
PSS	Power System Stabilizers
PV	Photovoltaic
R&D	Research and Development
RAS	Remedial Action Schemes
RTO	Regional Transmission Organization
RTU	Remote Terminal Units
SC	Series Capacitor
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Development Organization
SESG	Systems Engineering for Smart Grid
SGSC	Smart Grid, Smart City
SGTF	NERC's Smart Grid Task Force
SIEM	Security Incident and Even Management
SOL	System Operating Limits
SPS	Special Protection System/Schemes
SSR	Sub Synchronous Resonance
STATCOM	Static Synchronous Compensator
STE	Short-Term Emergency
SVC	Static VAr Compensator
T&D	Transmission and Distribution
TCP/IP	Transmission Control Protocol / Internet Protocol
TLR	Transmission Loading Relief
TOP	Transmission Operations (NERC Reliability Standards)
TPL	Transmission Planning (NERC Reliability Standards)
TRM	Transmission Reliability Margin
TSCS	Thyristor Switched Capacitor System
TSSC/TCSC	Thyristor Controlled/Switched Series Capacitor
TTC	Total Transfer Capability

TW	Terawatt (one million megawatts)
TWh	Terawatt-Hour (one million megawatts per hour)
UFLS	Under Frequency Load Shedding
UVLS	Under Voltage Load Shedding
VAr	Voltampere reactive
VAR	Voltage and Reactive (NERC Reliability Standards)
VFT	Variable Frequency Transformers
VPP	Virtual Power Plants
VV&A	Verification, Validation, and Accreditation
WAM	Wide Area Management System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WATSS	Wide Area Time domain GPS Synchronized Sampling System
WMN	Wireless Mesh Network
XML	Extensible Markup Language

Glossary

Adequate Level of Reliability — The intent of the set of NERC Reliability Standards is to deliver an Adequate Level of Reliability defined by the following bulk power system characteristics:

1. the system is controlled to stay within acceptable limits during normal conditions;
2. the system performs acceptably after credible contingencies;
3. the system limits the impact and scope of instability and cascading outages when they occur;
4. the system's facilities are protected from unacceptable damage by operating them within facility ratings;
5. the system's integrity can be restored promptly if it is lost; and
6. the system has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.[90]

Bulk Electric System — "As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition."[91]

Bulk Power System (BPS) — "Facilities and control systems necessary for operating an interconnected electric energy supply and transmission network (or any portion thereof), and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy."[92]

Cyber Assets — "Programmable electronic devices and communication networks including hardware, software, and data."[93]

Cyber Security Incident — "Any malicious act or suspicious event that:

- compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset; or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."[94]

---

[90] http://www.nerc.com/files/Adequate_Level_of_Reliability_Defintion_05052008.pdf
[91] Glossary of Terms Used in Reliability Standards, Updated April 20, 2009: http://www.nerc.com/docs/standards/rs/Glossary_2009April20.pdf
[92] Rules of Procedures of the North American Electric Reliability Corporation: http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20100903.pdf
[93] Ibid. 99

Energy Management System (EMS) — The suite of software and hardware that is used by electric grid operators to gather data about the electric system in real time. An EMS also includes tools that can be used by the operators to analyze data to assist in ensuring reliable delivery of energy to customers.

Phasor Measurement Unit — See ***Synchrophasor.***

Reliability — See ***Adequate Level of Reliability.***

Renewable Energy — The United States Department of Energy, Energy Efficiency and Renewable Energy glossary defines Renewable Energy as "energy derived from resources that are regenerative or for all practical purposes cannot be depleted. Types of renewable energy resources include moving water (hydro, tidal, and wave power), thermal gradients in ocean water, biomass, geothermal energy, solar energy, and wind energy. Municipal solid waste (MSW) is also considered to be a renewable energy resource."[95] The government of Canada has a similar definition.[96] Variable generation is a subset of Renewable Energy — See ***Variable Generation***.

Supervisory Control and Data Acquisition (SCADA) — "A system of remote control and telemetry used to monitor and control the transmission system."[97]

Synchrophasor — "Synchrophasors are precise measurements of the electricity grid, now available from grid monitoring devices called phasor measurement units (PMUs). PMUs measure voltage, current, and frequency at high speeds of 30 observations per second compared to conventional monitoring technologies (such as SCADA) that measure once every four seconds. Each phasor measurements is time-stamped according to the universal time standard, so measurements taken by PMUs in differing locations or with different owners can all be synchronized and time-aligned. This lets synchrophasor measurements be combined to provide a precise, comprehensive view of an entire interconnection. Monitoring and analysis of these measurements let observers identify changes in grid conditions, including the amount and nature of stress on the system, to better maintain and protect grid reliability."[98]

Smart grid — The integration and application of real-time monitoring, advanced sensing, communications, analytics, and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure, reliable, and efficient electric power system, from generation source to end-user. Where:

- *Real-time monitoring, advanced sensing* — The ability to more rapidly and accurately detect and measure the state of the electric system. This is critical to a more flexible, resilient, and dynamically responsive grid.

---

[94] Ibid. 99
[95] http://www1.eere.energy.gov/site_administration/ glossary.html#R
[96] http://www.cleanenergy.gc.ca/faq/ index_e.asp#whatiscleanenergy
[97] Glossary of Terms Used in Reliability Standards, Updated April 20, 2009: http://www.nerc.com/docs/standards/rs/Glossary_2009April20.pdf
[98] http://www.naspi.org/resources/2009_march/phasorfactsheet.pdf

- *Communications* — The transfer of information for the real-time operation, control, and maintenance of the electric system, primarily digital in the foreseeable future. Many aspects of a smart grid depend upon existing, expanded, or new communications technologies and infrastructure.
- *Analytics* — Tools and methods for sophisticated and accurate analysis of the electric power system to aid in operation, maintenance, planning, and decision-making. More extensive and accurate sensing and communication that accompany a smart grid also enable more powerful analytics.
- *Control* — Systems, technologies, and methods for operating the electric system in such a way as to achieve a desired state or response. Smart grid implies substantially greater application of automatic and advanced control capabilities.
- *Dynamic flow of both energy and information* — The flow of energy has always been dynamic. Under smart grid, the flow of information about that energy will be similarly dynamic. This expresses three important smart grid concepts: 1) energy and information are both essential components of the smart grid; 2) the smart grid flow of information and energy is not necessarily linear from power station to end-user and may be more complex than oft-cited examples of two-way flows of power—the information or energy may originate at multiple different points in the system and may flow to multiple different points in the system; and 3) the flows of information and energy are not necessarily prescript events—intelligence and advanced sensing, computing, and communications (described above) may enable adaptive routing of power or security measures to balance and safeguard the grid.
- *Existing and new* — There are legacy system in place that the smart grid will augment, then possibly replace over time. During the transition, the smart grid should cause no harm to the existing system.
- *Supply, delivery, and use* — Indicates the system's purpose is to augment the existing grid with new elements and practices (regardless of the intended ends: security, reliability, efficiency, system optimization, etc.). While some specific technologies and applications may not be "new" ideas per se, their widespread adoption or use in novel ways may be new to the system. Other developing technologies of smart grid will, in fact, be new to the grid. "Supply" and "Use" are broadly applicable terms.
- *Secure* — The uncompromised ability of the electric system to perform its intended purpose. Addresses both physical security and cyber security aspects. These are crosscutting issues for the grid.
- *Reliable* — Capable of delivering electric energy in the agreed upon or expected quantity, quality, and duration, at the agreed upon or expected place and time. Implies resource and transmission adequacy, operational reliability, power quality, and resiliency.
- *Efficient* — Performing in the best possible manner with the least waste.
- *Electric power system* — Characterizes one interconnected power generation and delivery system. Smart grid may enhance this system in terms of both efficiency and reliability, but does not fundamentally change its nature.

- *Generation source* — Broadly inclusive of all generation sources, regardless of energy source or power output.
- *End-user* — Broadly inclusive of all users from industrial plants to home owners.

State Estimator — A tool to provide estimates of the current and future states of the transmission system, including voltage magnitudes, angles, bus loads, and branch flows throughout the system. These data can be analyzed for bad data to help identify erroneous measurements, and can be used as historical data feeding into operations planning studies.

Transmission Line — "A system of structures, wires, insulators, and associated hardware that carries electric energy from one point to another in an electric power system. Lines are operated at relatively high voltages, varying from 69 kV up to 765 kV, and are capable of transmitting large quantities of electricity over long distances."[99]

Variable Generation — Variable generation technologies generally refer to generating technologies whose primary energy source varies over time and cannot reasonably be stored to address such variation.[100] Variable generation sources, which include wind, solar, ocean, and some hydro generation resources, are all renewable-based. Variable generation in this report refers only to wind and solar resources. There are two major attributes of a variable generator that distinguish it from conventional forms of generation and may impact the bulk power system planning and operations: variability and uncertainty.

- Variability: The output of variable generation changes according to the availability of the primary fuel (wind, sunlight, and moving water) resulting in fluctuations in the plant output on all time scales.
- Uncertainty: The magnitude and timing of variable generation output is less predictable than for conventional generation.

[99] Glossary of Terms Used in Reliability Standards, Updated April 20, 2009: http://www.nerc.com/docs/standards/rs/Glossary_2009April20.pdf
[100] http://www.nerc.com/files/IVGTF_Report_041609.pdf

Smart Grid Task Force Roster

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Chair	**Paul McCurley** Manager, Power Supply and Chief Engineer	National Rural Electric Cooperative Association Arlington, VA	703-907-5867 paul.mccurley@nreca.coop
Characteristics			
Vice-Chair	**Virginia Whitaker** Manager, Transmission Protection and Substations	E.ON U.S. LLC Lexington, KY	859-367-5753 virginia.whitaker@eon-us.com
Cyber security			
Vice-Chair	**Sandy Bacik** Principal Consultant	EnerNex Corp Knoxville, TN	865-696-4470 sandy.bacik@enernex.com
Vice-Chair	**Christopher Kotting** Administrator, Energy Assurance	Public Utilities Commission of Ohio Columbus, OH	614-466-0358 chris.kotting@puc.state.oh.us
Planning and Operations			
Vice-Chair	**Paul Myrda** Technical Executive	EPRI Orland Park, IL	708-479-5543 pmyrda@epri.com
Vice-Chair	**Trevor Siegfried** Senior Engineer	PPL Electric Utilities Corp. Allentown, PA	610-774-5718 tssiegfried@pplweb.com
Research and Development			
Vice-Chair	**Marija Ilic** Professor	Carnegie Mellon University Pittsburgh, PA	412-260-2471 milic@ece.cmu.edu
Task Force Participants			
Contributor	**Sandy Aivaliotis** Senior Vice President, Operations, Technology and Business Development	Nexans Ridgefield, CT	416-648-4382 sandy.aivaliotis@nexans.com
Contributor	**Farrokh Albuyeh** Vice President, Market Services and Consulting	Open Access Technology International, Inc. (OATI) Minneapolis, MN	763-201-2035 farrokh.albuyeh@oati.net
Contributor	**Sharla Artz** Director, Government Affairs	Schweitzer Engineering Laboratories, Inc. Alexandria, VA	703-647-6253 sharla_artz@selgs.com

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**JK August** Vice President, Operations	CORE Arvada, CO	303-425-7408 jkaugust@msn.com
Contributor	**David Batz** Manager, Cyber and Infrastructure Security	Edison Electric Institute Washington, DC	202-508-5064 dbatz@eei.org
Contributor	**Jonathan Booe** Staff Attorney	North American Energy Standards Board Houston, TX	713-356-0060 jbooe@naesb.org
Observer	**Scott Borre** Senior IT Analyst	US GAO Atlanta, GA	404-679-1894 borres@gao.gov
Contributor	**Joseph Bucciero** President and Executive Consultant	Bucciero Consulting, LLC Gilbertsville, PA	267-981-5445 joe.bucciero@gmail.com
Contributor	**Ken Caird** Senior Systems Engineer	GE Energy Atlanta, GA	678-844-6620 ken.caird@ge.com
Contributor	**James Calore** Manager, Interconnection Planning	Public Service Electric and Gas Co. Newark, NJ	973-430-6628 james.calore@pseg.com
Contributor	**Matthew Campagna** Director of Research	Howe Brand Communications Mississauga, ON Canada	905-507-4220 mcampagna@certicom.com
Contributor	**Rocky Campione** Director of Business Solutions	Planet Technologies Germantown, MD	301-721-0100 rocky@go-planet.com
Contributor	**Jay Cappy** Managing Principal, Global Services	Verizon Business Louisville, KY	502-395-2811 jay.j.cappy@verizonbusiness.com
Contributor	**Lawrence D. Carter** Electrical Engineer/Grid Expert	Bonneville Power Administration Portland, OR	360-931-2477 ldcarter@bpa.gov
Contributor	**Sunil Cherian** CEO	Spirae, Inc. Fort Collins, CO	970-372-3032 sunil@spirae.com
Contributor	**John L. Ciufo** Manager, P&C Strategies and Standards	Hydro One, Inc. Toronto, ON Canada	416-345-5258 john.ciufo@hydroOne.com

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**Tom Dagenais** Senior Transmission Planning Engineer	American Transmission Company, LLC Madison, WI	608-877-7161 tdagenais@atcllc.com
Contributor	**Dave Dalva** Smart Grid Security Lead	Cisco Systems, Inc. Potomac, MD	703-484-0129 ddalva@cisco.com
Contributor	**Ali Daneshpooy** Program Manger, Smart Utility	Powertech Labs, Inc. Surrey, BC Canada	604-590-6684 ali.danesh@powertechlabs.com
Observer	**Richard DeBlasio** National Renewable Energy Laboratory Program Manager	National Renewable Energy Laboratory Golden, CO	303-275-4333 dick.deblasio@nrel.gov
Contributor	**Rebecca Dietrich** Director	GridWise Alliance Washington, DC	202-530-9740 bdietrich@gridwise.org
Contributor	**Terry Dillon** System Ana/Intgrtr Ld	Arizona Public Service Co. Phoenix, AZ	602-371-5072 terry.dillon@aps.com
Observer	**Thomas Dion** Control Systems Security Program Manager	DHS National Cyber Security Division Washington, DC	703-235-5179 thomas.dion@ghs.gov
Contributor	**Alejandro Dominguez-Garcia** Assistant Professor, Department of Electrical and Computer Engineering	University of Illinois at Urbana-Champaign Urbana, IL	217-333-3953 aledan@illinois.edu
Contributor	**Christopher Eisenbrey** Director, Business Information	Edison Electric Institute Washington, DC	202-508-5574 ceisenbrey@eei.org
Observer	**Mark Fabro** President/Chief Security Scientist	Lofty Perch, Inc. Markham, ON Canada	647-226-4225 fabro@loftyperch.com
Contributor	**Norm Fraser** Chief Operating Officer	Hydro Ottawa Limited Ottawa, ON Canada	613-738-5478 normfraser@hydroottawa.com
Contributor	**Gerald John FitzPatrick** Leader, EEEL Smart Grid Project	National Institute of Standards and Technology 100 Bureau Drive, MS-8172 Gaithersburg, MD 20899-8172	301-975-8922 301-926-3972 Fx gerald.fizpatrick@nist.gov

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**Joel Garmon** Director of Information Security	Florida Power & Light Co. Miami, FL	305-552-3097 joel.garmon@fpl.com
Observer	**Paige Gilbreath** Senior Analyst	US Govt. Accountability Office Dallas, TX	214-777-5724 gilbreathp@gao.gov
Contributor	**Ed Goff** System Architect, IT&T Security	Progress Energy Raleigh, NC	919-812-2202 edwin.goff@pgnmail.com
Contributor	**Rich Gordus** Manager, Relay and Protection Engineering	ComEd Oakbrook Terrace, IL	630-437-2753 richard.gordus@comed.com
Contributor	**Amitabha Tab Gangopadhyay** Professional Engineer	National Energy Board 444 Seventh Avenue SW Calgary, AB T2P 0X8 Canada	403-299-3611 403-292-5503 Fx tgangopadhyay@neb-one.gc.ca
Contributor	**Neil Greenfield** Information Security Senior Specialist	American Electric Power Columbus, OH	614-716-3187 ngreenfield@aep.com
Contributor	**Vinit Gupta** Supervisor, EMS Applications	Entergy Services, Inc. Little Rock, AR	501-823-1630 vgupta@entergy.com
Observer	**Maria A. Hanley** Energy Analyst	Department of Energy (NETL) Pittsburgh, PA	412-386-5373 maria.hanley@netl.doe.gov
Contributor	**Rod C. Hardiman** Project Manager	Southern Company Transmission Company Birmingham, AL	205-257-7056 rchardim@southernco.com
Contributor	**Dave Hardin** Staff Engineer	Automation Federation Foxboro, MA	508-549-3362 david.hardin@ips.invensys.com
Contributor	**Ernie N Hayden** Professional Services Consultant	Verizon Business North Bend, WA	206-458-8761 ernest.hayden@verizonbusiness.com
Contributor	**Edward Hedges** Manager, SmartGrid Technology Planning	Kansas City Power & Light Co. Kansas City, MO	816-245-3861 ed.hedges@kcpl.com
Contributor	**Gavan Howe** President/CEO/ Owner	Howe Brand Communications Toronto, ON Canada	416-363-6591 gavan@ebranders.com
Contributor	**Lawrence Huang** Product Manager	Cisco Systems Milpitas, CA	408-525-5396 lahuang@sisco.com

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**Kenneth Huber** Senior Technology and Education Principal	PJM Interconnection, L.L.C. Norristown, PA	610-666-4215 huberk@pjm.com
Contributor	**Richard Kalisch** Senior Director Technology Initiatives	Midwest ISO, Inc. Carmel, IN	317-249-5265 rkalisch@midwestiso.org
Contributor	**Innocent Kamwa** Senior Scientist	Institut de Recherche d'Hydro Québec Varennes, QC Canada	450-652-8122 kamwa.innocent@ireq.ca
Contributor	**Jeffrey Katz** Chief Technology Officer, Energy and Utilities Industry	IBM Hartford, CT	877-540-6891 jskatz@us.ibm.com
Contributor	**Mladen Kezunovic** Professor	Texas A&M University College Station, TX	979-845-7509 kezunov@ece.tamu.edu
Contributor	**Brendan Kirby** Consultant	American Wind Energy Association Knoxville, TN	865-250-0753 kirbybj@ieee.org
Contributor	**Deepa Kundur** Associate Professor	Texas A&M University College Station, TX	979-862-8684 deepakundur@mac.com
Contributor	**Mike LaMarre** Division Manager of Infrastructure Management	Austin Energy Austin, TX	512-322-6883 Mike.Lamarre@austinenergy.com
Observer	**Annabelle Lee** Senior Cyber Security Strategist	NIST Gaithersburg, MD	301-975-8897 Annabelle.lee@nist.gov
Contributor	**John Lim, CISSP** Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York New York, NY	212-460-2712 limj@coned.com
Contributor	**Claudio Lima** Managing Director, Smart Grid	Sonoma Innovation San Jose, CA	470-390-7297 clima@sonomainnovation.com
Observer	**Jamie Link** Research Staff Member	Science & Institute Policy Institute Washington DC	202-419-5481 jlink@ida.org
Contributor	**Donald A. Lynd** Senior Engineer, HVD Planning	Consumers Energy Jackson, MI	517-788-1056 dalynd@cmsenergy.com

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**Madhav D. Manjrekar** Team Leader	Siemens Corporate Research Princeton, NJ	609-734-6566 madhav.manjrekar@siemens.com
Contributor	**Jack McCall** Director, Business Development Superconductors	American Superconductor AMSC) New Berlin, WI	262-901-6016 jmccall@amsc.com
Contributor	**James D. McCalley** Professor	Iowa State University Ames, IA	515-294-4844 jdm@iastate.edu
Contributor	**Devin McCarthy** Senior Advisor	Canadian Electricity Association Ottawa, ON Canada	613-688-2960 mccarthy@electricity.ca
Contributor	**Douglas McGinnis** IT Manager of Communications Infrastructure Strategy	Exelon Corporation Philadelphia, PA	717-413-3825 doug.mcginnis@exeloncorp.com
Contributor	**Rick Meeker** Program Development Manager, Industry Partnerships	Florida State University Tallahassee, FL	850-645-1711 meeker@caps.fsu.edu
Contributor	**Michael Mertz** Project Manager, Regulatory Compliance	Southern California Edison Co. Irwindale, CA	626-543-6104 Michael.Mertz@sce.com
Contributor	**Alessandro Meynardi** Managing Principal	Verizon Business Bala Cynwyd, PA	610-257-3170 Alessandro.m.meynardi@verizonbusiness.com
Contributor	**Nathan Mitchell, P.E.** Director of Electric Reliability Standards and Compliance	American Public Power Association Washington, DC	202-467-2925 nmitchell@appanet.org
Contributor	**Karen Miu** Associate Professor	Drexel University Philadelphia, PA	215-895-6207 karen@coe.drexel.edu
Contributor	**Paul Molitor** Senior Industry Director	NEMA Rosslyn, VA	703-841-3262 paul.molitor@nema.org
Contributor	**Austin Montgomery** Business Manager	Software Engineering Institute Arlington, VA	703-908-1110 amontgom@sei.cmu.edu
Contributor	**Nelson Muller** Executive Vice President	Open Access Technology International, Inc. (OATI) Minneapolis, MN	763-201-2000 nelson.muller@oati.net

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**Ian Mundell** Senior Business Analyst	PJM Interconnection, L.L.C. Norristown, PA	610-666-4617 mundei@pjm.com
Contributor	**Thomas Overman** Chief Architect, Boeing Energy Cyber Security	Boeing Defense, Space & Security Sunnyvale, CA	408-524-3721 thomas.overman@boeing.com
Contributor	**Avni Patel** Smart Grid Strategic Planning Manaer	Duke Energy Charlotte, NC	704-382-8264 avni-patel@duke-energy.com
Contributor	**Daniel E. Pfeiffer** Vice President of Regulatory Affairs	Itron, Inc. Liberty Lake, WA	509-891-3839 dan.pfeiffer@itron.com
Contributor	**Farrokh Rahimi** Vice President, Market Design & Consulting	Open Access Technology International, Inc. (OATI) Minneapolis, MN	763-201-2000 Farrokh, rahimi@oati.net
Contributor	**Bhasker Rao** CEO	Fortech Software Consulting Inc Tempe, AZ	480-730-0691 corpmail@fortechsw.com
Contributor	**James Resek** Executive Consultant	KEMA Consulting Chalfont, PA	215-674-2000 Jim.resek@kema.com
Observer	**Marie Rinkoski-Spangler** EIA-411 Survey Manager	U.S. Department of Energy Washington, DC	202-586-2446 marie.rinkoski-spangler@eia.doe.gov
Observer	**Sarah Ryker** Research Staff member	Science & Technology Policy Institute Washington, DC	202-419-3728 sryker@ida.org
Contributor	**Brett Sargent** Global Vice President of Sales	LumaSense Santa Clara, CA	404-512-6336 b.sargent@lumasenseinc.com
Contributor	**Venkat Shastri** President and CEO	PCN Technologies, Inc. San Diego, CA	858-434-0605 vekat@pcntechnology.com
Contributor	**Sean Sherman** Director of Security Solutions	PPC McLean, VA	360-609-9103 sean.sherman@ppc.com
Contributor	**Lindon Shiao** Chief Security Officer	GridSense West Sacramento, CA	916-372-4945 l.shiao@gridsense.com
Observer	**Nano Sierra** Group Manager	Federal Energy Regulatory Commission Washington, DC	202-502-8479 nano.sierra@ferc.gov

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**John P. Skliutas** Principal Engineer	GE Energy Schenectady, NY	518-385-0209 john.skliutas@ge.com
Contributor	**William Souza** Manager, Security Integration	PJM Interconnection Norristown, PA	610-666-2237 beknh03@gmail.com
Contributor	**Ron Stelmak** Vice President Sales and Marketing	The Valley Group (a Nexans Company)	203-431-0262 203-241-3513 Fx
Contributor	**Gary Stuebing** Strategic Planning Manager	Duke Energy Charlotte, NC	704-382-9787 gary.stuebing@duke-energy.com
Contributor	**Stephen Swan** Senior Manager, System Wide Operations	Midwest ISO, Inc. Carmel, IN	317-249-5075 sswan@midwestiso.org
Contributor	**Daniel Thanos** Chief Cyber Security Architect	GE Digital Energy Markham, ON Canada	905-201-2439 daniel.thanos@ge.com
Contributor	**Kevin Tomsovic** CTI Professor & Head	University of Tennessee Knoxville, TN	865-974-3461 tomsovic@tennessee.edu
Contributor	**Eli Turk** Vice President	Canadian Electricity Association Ottawa, ON Canada	613-230-9876 turk@electricity.ca
Contributor	**David Ulmer** Sr. Technology Architect	PJM Interconnection, L.L.C. Norristown, PA	610-666-2233 ulmerd@pjm.com
Contributor	**Pravin Varaiya** Professor	UC Berkeley Berkeley, CA	510-642-5270 varaiya@eecs.berkeley.edu
Contributor	**Charlie Vartanian** Director, Grid Integration	A123 Systems Huntington Beach, CA	626-818-5230 cvartanian@a123systems.com
Contributor	**Chris Villarreal** Regulatory Analyst	California Public Utilities Commission San Francisco, CA	415-703-1566 crv@cpuc.ca.gov
Contributor	**Vijay Vittal** Professor	Arizona State University Tempe, AZ	480-965-1879 vijay.vittal@asu.edu
Contributor	**Josh Wepman** AVP Smart Grid Security Practice Lead	SAIC Ann Arbor, MI	858-366-2175 wepmanj@saic.com

Position	Name / Title	Company City, State/Province	Phone/ E-mail
Contributor	**Ernest Wohnig** Senior Associate, Energy Security Sector	Booz Allen Hamilton, Inc. Mclean, VA	703-377-1249 wohnig_ernest@bah.com
Contributor	**Neng Eva Wu** Professor, Department of ECE	Binghamton University, SUNY Binghamton, NY	607-777-4464 evawu@binghamton.edu
Contributor	**Marzia Zafar** Program Manager	California Public Utilities Commission San Francisco, CA	415-703-1997 zaf@cpuc.ca.gov
Contributor	**Pamela Zdenek** Regulatory and Compliance Advisor	BP US Cogens Houston, TX	713-354-4830 pamela.zdenek@bp.com

NERC Staff Roster

North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721

Telephone: 609-452-8060
Fax: 609-452-9550

Reliability Assessment and Performance Analysis

Name	Title	E-mail
Mark G. Lauby*	Director, Reliability Assessment and Performance Analysis	mark.lauby@nerc.net
Aaron Bennett	Engineer, Reliability Assessments	No longer with NERC
John Moura	Technical Analyst, Reliability Assessments	john.moura@nerc.net
Eric Rollison	Engineer, Reliability Assessments	eric.rollison@nerc.net
Chrissy Vegso	Administrative Assistant	chrissy.vegso@nerc.net

Reliability Standards

Edward Dobrowolski	Standards Development Coordinator	ed.dobrowolski@nerc.net

Critical Infrastructure Protection

Scott Mix	CIP Technical Manager	scott.mix@nerc.net

*NERC Staff Coordinator for the Smart Grid Task Force.