Smart Grid Principal Characteristics

OPERATES RESILIENTLY AGAINST ATTACK AND NATURAL DISASTER

Developed for the U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
by the National Energy Technology Laboratory
September 2009

NETL

Office of Electricity
Delivery and Energy
Reliability

DISCLAIMER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The smart grid is defined by its seven principal characteristics. One of those characteristics is "Operates Resiliently Against Attack and Natural Disaster." How this characteristic might be attained is the subject of this paper.

The energy industry's assets and systems were not designed to handle extensive, well-organized acts of terrorism aimed at key elements.

The U.S. energy infrastructure is a huge network of electric generating facilities and transmission lines, natural gas pipelines, oil refineries and pipelines, coal mines, communications systems, and various other elements. Occasionally, these systems have been exposed to large-scale natural disasters such as hurricanes and earthquakes. Generally, industries have restored energy supplies relatively quickly. Sabotage of individual components has caused some problems, but the impacts have been managed. We have done well in the past, but our post-9/11 future will be more challenging.

Today's electric system was not designed to handle extensive, well-organized acts of terrorism aimed at strategic elements. The threat of attack is growing and a widespread attack against the infrastructure is more likely today than ever before. It is therefore critical that the smart grid address security from the outset, making it a requirement for all the elements of the grid and ensuring an integrated and balanced approach across the system.

Threats to the smart grid can be broken into two categories: physical attacks (explosives, projectiles, natural disaster) and cyber (computer-launched) attacks. Whatever the specific nature of the threat, designers of the smart grid should plan for a directed, well-planned, and simultaneous attack against several vital parts of the system.

For the smart grid to operate resiliently against attack and natural disaster, it must reduce the following:

- Threat by increasing grid robustness and projecting an image that deters those who would attack an easier target.
- Vulnerability of the grid to attack by protecting key assets from physical and cyber attack and by providing sufficient redundancy to tolerate the loss of multiple key assets.
- Consequences of a successful attack by focusing designs and resources on rapid recovery.

And the smart grid must resist two different attack strategies:

1. Attacks on the overall power system, in which the infrastructure itself is the primary target, either by direct attack or attack through other infrastructures.
2. Attacks through the power system, in which attackers target specific power system networks to take down other infrastructure systems, such as telecommunications, financial, or government.

The following topics are addressed in this paper:

- The current state and proposed future state of grid security.
- Requirements for implementation.
- Implementation barriers.
- Expected benefits.
- Recommendations for moving forward.

CURRENT AND FUTURE STATES

Before we discuss how the smart grid might improve resiliency against attack and natural disaster, we need to understand its current vulnerabilities and how to reduce them in the future. This section explores the current state and the desired future state of grid resiliency and security.

CURRENT STATE

"The vulnerability (of the power grid) is something that the Department of Homeland Security and the energy sector have known about for years." Homeland Security Secretary Janet Napolitano, April 2009

Threats to the security of the grid's cyber backbone are increasing. The application of existing security technologies, such as encryption and the widespread use of routine security procedures help, but more advanced techniques will be required to defeat today's sophisticated, modern terrorist. Many control devices in use on today's grid do not have the bandwidth and processing power to accommodate even the current state-of-the-art cyber protection. Future deployments of smart grid technologies will be easy targets for hackers if the needed cyber security techniques are not implemented at the foundational level.

Today's grid lacks the robustness needed to withstand attacks by saboteurs or acts of nature. Several weaknesses are inherent in today's grid:

- The grid is aging, based largely on technology developed many decades ago. This aging infrastructure is stressed by a lack of adequate investment to meet the growing demand for electric power.
- The centralized generation model of today's grid creates a number of vital assets that, if targeted, could result in significant system-wide consequences.
- Key transmission lines are frequently congested; their loss would ripple through the system.
- Industry publications, maps, and other materials are available on the Internet and provide information that could assist in planning attacks on the grid.
- Smart grid technologies are being deployed before security standards have been developed and endorsed.
- Grid operators place increased reliance on unprotected telecommunications networks and associated Supervisory Control and Data Acquisition (SCADA) systems.

Ironically, as older equipment is replaced with new smart grid technologies an interesting paradox could occur—while reliability increases from the installation of new equipment and systems, cyber vulnerability may also increase, especially where new devices are not properly protected. We are potentially more vulnerable, and the target has increasing appeal.

Today's grid lacks the information and control capabilities to rapidly recover from manmade or natural events. Most of today's distribution system is radial in design with one-way power flow capability. With limited ability to quickly identify, isolate, and correct a system problem, an attack or natural disaster can have a significant negative impact on large numbers of consumers.

FUTURE STATE

The smart grid will address critical security issues from the outset, making security a requirement for all its elements and adopting a systems view that enables an integrated and balanced approach.

Advanced cyber security protection systems will be integrated utilizing cyber security standards to ensure that new smart grid technologies are secure and that existing technologies such as SCADA, protective relaying, and communication systems are retrofitted with methods that provide the same level of advanced cyber security.

Other smart grid characteristics will increase the physical robustness of the grid and therefore support the achievement of this principal characteristic. For example—

- Moving to a more de-centralized operating model reduces the number of "targets" that could result in significant consequences.
- Increasing the situational awareness of both the transmission and distribution grid through the deployment of extensive monitoring and advanced decision support technologies gives system operators a better chance to detect potential security breaches.
- Increasing the intelligence and control granularity of the distribution and transmission system through "self-healing" technologies enables the grid to respond more effectively and efficiently to a security event.
- Deploying a smart grid communications platform having the reliability and bandwidth required to accommodate sophisticated encryption methods prevents hackers from corrupting the system.
- Creating a strong image of robustness would deter potential attackers.

Planning for manmade threats should consider not only single but multiple points of simultaneous attack. Federal, state, and local officials should work with individual utilities to address acceptable risk, possibly with support from DOE and Homeland Security officials. Additionally, government and industry should jointly conduct periodic exercises that will improve the security aspects of the smart grid. Metrics are needed to gauge success and guide improvements.

Grid security will be enhanced by the deployment of key smart grid technologies as shown in Table 1 below.

Modern Grid Key Technologies	Security Features
Integrated Communications	• Interoperability standards that include advanced cyber security protection • Transport vehicle that provides the needed operational and condition data to enable self healing • Redundant communication paths making interruption of data flows unlikely
Sensing & Measurement	• Remote monitoring that detects potential events anywhere in the grid • Sensors and measuring devices with embedded protection • Events detected in time to respond
Advanced Components (includes DER)	• Tolerant and resilient grid devices • Rapid response to emergent threats • Fewer critical points of failure • Reduced consequences of failure • Distributed, autonomous resources
Advanced Control Methods	• Islanding to isolate vulnerable areas in response to real or expected security events • Automated network "agents" for dynamic reconfiguration and demand management • Self-healing with preventive or corrective actions in real time
Improved Interfaces & Decision Support	• Greatly enhanced situational awareness • Recommendations for addressing security threats provided to operators in real time • Advanced real-time modeling and simulation tools with predictive capabilities • Improved operator training and guidance systems aimed at response to security events

Table 1: Key technologies of the smart grid contribute to solutions that resist attack.

REQUIREMENTS

With a broad understanding of the current and future state of the electrical power system, we can now discuss some of the requirements that need to be met to move forward. This section explores system requirements, as well as requirements for policy and regulation, and codes and standards.

SYSTEM REQUIREMENTS

A comprehensive risk-based approach to electric power security will assess the likelihood of threats, identify key vulnerabilities, and determine consequences of an attack. The designers of the smart grid can draw on extensive experience developed by the Department of Defense and the National Institute of Standards and Technology (NIST) in assessing threats and system vulnerabilities.

This approach applies risk management methods to prioritize the allocation of resources for security, including R&D. Particular goals of security programs would include:

- Identification of critical sites and systems.
- Protection of selected sites using surveillance and barriers against physical attack.
- Design and deployment of systems that can tolerate a disruption.
- Integration of distributed energy sources and using automated distribution to speed recovery from attack.
- Targeted and customized deployment of traditional security devices such as firewalls and intrusion detection systems within smart grid communication networks to detect and thwart attacks.

Resilience must be built in to each element of the system, and the overall system must be designed to deter, detect, respond, and recover from disruptions. The following features are required to support these objectives:

- Implement self-healing capabilities.
- Enable “islanding” (the autonomous operation of selected grid elements).
- Provide greater automation, wide area monitoring, and remote control of electric distribution systems.
- Acquire and position spares for key assets.
- Maintain equipment to a high level so it can better withstand disturbances.

- Employ distributed energy resources.
- Ensure that added equipment and control systems do not create additional opportunities for attack.
- Rapidly respond to impending disruptions with the aid of predictive models and decision support tools.

POLICY AND REGULATION REQUIREMENTS

An increased emphasis and priority on system security is imperative. The nuclear power industry provides some lessons learned that can be applied to the smart grid. In 1979, a number of new nuclear power plants were under construction. Although safe operation was very important to the industry, the accident at Three Mile Island nonetheless occurred on March 29 of that year, suggesting that the industry's focus on safety was not adequate. The accident was followed by a near complete cessation of the start of new nuclear plant construction in the United States. Since that accident, nuclear safety has been the top priority—even ahead of economics.

Today much is said about addressing the needed security features for the smart grid upfront, both physical and cyber related. We should not forget that focus and priority as we move forward with the smart grid. The consequences of a prolonged outage (e.g., months) from a highly targeted and coordinated attack are almost unimaginable.

Metrics to measure the results of security measures should be used to identify the most cost effective solutions. Utilities faced with investment costs to modernize the grid—even with possible government subsidies—will want a clear understanding of which security upgrades can be included in rate base. Coming up with the answers will require close coordination between federal and state regulatory authorities, DOE, and possibly homeland security officials.

CODES AND STANDARDS REQUIREMENTS

Grid owners and operators must take a systems view of security, applying industry best practices and standards.

NIST is leading the initiative for defining the standards needed for the smart grid. Standards that support interoperability are very important to ensure that all devices, applications, and systems are interoperable. Interoperability is a solution that makes the operation of smart grid components efficient but not necessarily secure. Development of standards that specifically address grid security should receive the highest priority.

BARRIERS

The physical and cyber security of the electric industry is a growing concern. Evolving national security threats, increasing interoperability in the grid, and expanded use of open systems in the grid's architecture all contribute to serious vulnerabilities.

Do we have adequate priority placed on ensuring the smart grid is secure? Although we cannot provide a definitive answer, we can pinpoint some of the specific barriers that must be addressed to achieve a secure smart grid. These barriers include:

- **Incomplete understanding of threats, vulnerabilities, and consequences.** Industry as a whole lacks a standard approach for conducting vulnerability and risk assessments, understanding consequences, and valuing security upgrades. Additionally, limited access to government-held threat information makes the case for security investments more difficult to justify.
- **Perception that security improvements are prohibitively expensive.** When examined independently, the costs and benefits of security investments can seem unjustifiable. But the cost of a significant grid security event can dwarf the costs of prevention.
- **Increasing use of open systems.** Open communication and operating systems are flexible, less costly, and improve system performance, but may not be as secure as proprietary systems.
- **Increasing number of grid participants.** The growing number of entities participating in the electric system increases the complexity of physical and cyber security issues.
- **Difficulty in recovering costs.** Given the lack of security metrics or indices, utilities currently lack the information needed to sufficiently quantify the potential impacts of security events or benefits of security investments.

BENEFITS

A smart grid that is resilient to attack and natural disaster provides a multitude of benefits. These benefits include:

Increasing the deterrence of an attack thereby reducing the number of potential events and the corresponding consequences.

Improving the operational readiness of our defense forces by ensuring security-of-supply for electric power.

Reducing the social and economic impacts of a security event or natural disaster, such as:

- Minimizing the costs associated with lost products and lost productivity.
- Minimizing the loss of life associated with a loss of power for extended periods of time.
- Reducing societal disruptions and mitigating psychological impact.
- Reducing the geographic extent of outages.
- Improving the recovery time from outages.

Solutions that enhance security are synergistic with improving grid reliability. For example—

- Integration of DER improves reliability and its decentralization decreases the vulnerability of the grid.
- Use of advanced modeling and simulation tools to monitor grid risks in real time can help prevent "normal" outages as well as spot vulnerabilities.
- Use of well-positioned spares to mitigate effects of equipment failure reduces recovery time no matter what the initiating event.
- Application of demand response (DR) increases system robustness and improves reliability.
- Greater use of distribution automation improves reliability and supports isolation of attacked grid components to the smallest possible area and impact.

RECOMMENDATIONS

To deploy a smart grid that resists attack, the coordinated efforts of planners, designers, developers, government, and industry are needed.

Planners of the smart grid should:

- Work with NIST to ensure that adequate priority is placed on the development of cyber security standards during its identification and development of smart grid standards.
- Leverage methods developed by DOD, DOE, and DHS to increase the survivability of systems.
- Create a government-industry team, including state regulators, to identify and address issues of unacceptable risk to the public.
- Establish a societal value for grid security. What is the value of preventing an attack?

Designers and developers of the smart grid should:

- Consider security as a system requirement that could affect virtually every element and sub-system of the smart grid.
- Ensure that additional equipment and control systems added to the grid do not increase its likelihood of disruption and do not create additional opportunities for malevolent actions against it.
- Apply the ongoing work by industry, government, and academia to reduce physical and cyber vulnerabilities.

Government and industry should:

- Evaluate and identify specific grid vulnerabilities and consequences to ensure the level of effort applied to their resolution is commensurate with their impact.
- Acquire and position spares to replace damaged key assets.
- Develop metrics to monitor the progress in implementing security enhancements.
- Ensure that the developers of the smart grid integrate security as an inherent characteristic—not as an optional feature.
- Ensure that the costs for appropriate security investments are approved for inclusion in rate base.
- Include security benefits in all smart grid business cases.
- Support the addition of traditional assets where appropriate, such as high voltage transmission lines that increase grid robustness.

SUMMARY

The threat of both physical and cyber attack is growing and a widespread attack against the infrastructure cannot be ruled out.

The 20th-century electrical power system is aging and its infrastructure was never designed to handle well-organized acts of terrorism.

In the 21st century, it is critical for the smart grid to address security from the outset, making it a requirement for all the elements of the grid and ensuring an integrated and balanced approach across the system. Lessons learned from the nuclear industry should be reviewed.

Whether the threat is physical or cyber, the smart grid must resist attacks that employ two different strategies:

1. Attacks on the power system, in which the infrastructure itself is the primary target.
2. Attacks through the power system, in which attackers exploit power system networks to affect other economic sectors such as telecommunications, financial, or government.

The complexity of the current electrical power system and the reliance on critical nodes to operate without interruption create vulnerabilities that can result in widespread disruptions. Beyond this, to resist organized attacks by a sophisticated adversary, the smart grid must consider the likelihood of targeted, multiple points of attack, not just single localized ones.

A systems approach to grid security would identify key vulnerabilities, assess the likelihood of threats that could exploit those vulnerabilities, and determine the probability and the possible consequences of a successful attack. Technologies and solutions to address security issues will complement communications, computing, decision support, self-healing, and equipment improvements needed for the smart grid.

Implementing cost-effective technologies to enhance the security of the grid will have positive impacts on reliability and resilience. The smart grid, if designed to deter, detect, respond, and recover from security and natural events, will also support the achievement of most other principal characteristics.

Metrics to measure security effectiveness are needed. Federal, state, and local policies and regulations need to be developed to allow utilities and others in the electricity industry to recoup reasonable costs for security upgrades that are part of the overall system design.

A great deal of work remains to develop and implement the security measures needed to enable the smart grid to operate resiliently against attack and natural disaster. If we place a high priority on achieving this principal characteristic, we will be successful.

The Modern Grid Strategy (MGS) is working with a wide range of stakeholders. The MGS will continue its outreach efforts to communicate and educate stakeholders on various smart grid concepts and to assist in better defining the smart grid value proposition.

For more information

This document is part of a collection of documents prepared by the Modern Grid Strategy team. Documents are available for free download from the Modern Grid website.

The Modern Grid Strategy

http://www.netl.doe.gov/moderngrid/

info@TheModernGrid.org

(304) 599-4273 x101

BIBLIOGRAPHY

1. Electricity Grid in US Penetrated by Spies, Wall Street Journal, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html.
2. The Security Vulnerabilities of Smart Grid, Journal of Energy Security, June 2009, http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345.