Modern Grid Strategy team

Energy Central series on the Seven Principal Characteristics of the Modern Grid

[Article 6 of 7: ***Research on the Characteristics of a Smart Grid by the NETL Modern Grid Strategy team***

Operates Resiliently against Attack and Natural Disaster

Last month we presented the fifth principal characteristic of a Smart Grid, "Power Quality for the Digital Economy." This month we present the sixth characteristic, "Operates Resiliently against Attack and Natural Disaster."

This characteristic is aimed at improving the resiliency and robustness of the grid to make it less vulnerable to attack and natural disaster. Given the Smart Grid's dependency on digital technologies and advanced communication systems, a major effort is needed to address cyber security in addition to the more conventional physical security aspects. This characteristic along with the other six define a Smart Grid that will power the 21st Century economy. For a more detailed discussion on this characteristic, please refer to the Modern Grid website: http://www.netl.doe.gov/moderngrid/docs/Resists%20Attack_Final%20_v2_0.pdf

Summary

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 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've been lucky in the past, but the 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 both physical and cyber attack is growing and a widespread attack against the infrastructure is more likely today than ever before. There is evidence that Al Qaeda has been tracking debates in the United States related to the cyber vulnerability of control systems in the energy infrastructure[1]. 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, the designers of the Smart Grid should plan for a dedicated, well-planned, and simultaneous attack against several parts of the system.

Whether a physical or cyber attack, the Smart Grid must resist two different attack strategies:

- ***Attacks on the overall power system***, in which the infrastructure itself is the primary target either by direct attack or attack through other infrastructures.

- ***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.

For the Smart Grid to operate resiliently against attack and natural disaster, it must reduce the:

- ***Threat*** by drastically lowering the odds that any attack can succeed
- ***Vulnerability*** of the grid to attack by protecting key assets from physical and cyber attack.
- ***Consequences*** of a successful attack by focusing designs and resources on rapid recovery.

C*urrent State*

Today's grid lacks the robustness needed to withstand attacks by either saboteurs or Mother Nature. Several physical weaknesses are inherent with today's grid:

- The grid is aging, based largely on technology developed in the 1950s or earlier. This aging infrastructure is stressed by a lack of adequate investment to meet the growing demand for electric power.
- Demand is increasing putting additional stresses on the grid
- The centralized operating model of today's grid creates a number of assets that if targeted could result in significant system-wide consequences
- Key transmission lines are frequently congested
- Industry publications, maps, and other materials are available on the internet and provide information that could assist saboteurs plan attacks on the grid.

Ironically, recent advances in technology and changes in the electricity sector, such as deregulation and dependence on 20th century technologies, may be adding to the security problem. Examples include:

- Increased reliance on unprotected telecommunications networks and associated Supervisory Control and Data Acquisition (SCADA) systems
- The growth of independent power producers without the budget to address security
- Outsourcing of maintenance and security functions

Threats to the security of the grid's cyber backbone are increasing. 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. Application of existing security technologies, such as encryption and the widespread use of routine security procedures will 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 use even the current state of the art in cyber protection.

We are vulnerable and the target has great appeal.

Future State

Achievement of other Smart Grid Principal Characteristics will increase the physical robustness of the grid and therefore supports the achievement of this principal characteristic. For example:

- Moving to a more de-centralized operating model to reduce the number of "targets" that 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 giving 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 to enable 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
- Creating an image of robustness so great that potential attackers are deterred from attacking in the first place.

Planning for manmade threats should consider not only single, but also multiple points of failure. 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 exercises that will improve the security aspects of the Smart Grid, as well as its design and operation. Metrics are needed to gauge success and guide improvements.

The Smart Grid must address critical cyber security issues from the outset, making security a requirement for all the elements of the grid. Advanced cyber security protection systems will be integrated with standards to ensure that new Smart Grid technologies are "hack-proof" 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.

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

Modern Grid Key Technologies	Security Solutions
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 and Measurement	• Remote monitoring that detects challenges anywhere

	in the grid • Cyber protection of sensors and measuring devices
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 • Recommendations for addressing security threats provided to operators in real time • Advanced modeling and simulation capability with predictive capability
Advanced Components	• Tolerant and resilient grid devices • Rapid response to emergent threats • Fewer critical points of failure • Reduced consequences of failure • Distributed, autonomous resources
Decision Support	• Greatly enhanced situational awareness • 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

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.

Many utilities have taken some action on security, but the question remains: Are we gaining ground or losing ground on security? Although we can't provide a definitive answer, we can pinpoint some of the specific barriers that must be overcome to achieve the Smart Grid vision of a system that resists intentional attack. These barriers include:

- ***Incomplete understanding of threats, vulnerabilities and consequences***. Some utilities conduct vulnerability and risk assessments and a fraction of them apply the results to security upgrades. Industry as a whole lacks a standard approach to conducting these assessments, understanding consequences, and valuing security upgrades. Additionally, limited access to government-held threat information makes the case for security investments even more difficult to justify.
- ***Perception that security improvements are prohibitively expensive***. When examined independently, the costs and benefits of security investments can seem unjustifiable.
- ***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. The increasing use of open systems must be met with industry approved and adopted standards and protocols that consider system security.

- ***Increasing number of grid participants***. The growing number of entities participating in the electric system increases the complexity of physical and cyber security issues. Security measures must be built into the functions that support distributed generation owners, Independent Power Producers, and consumers active in demand response and automated metering programs.
- ***Difficulty in recovering costs***. Utilities must be armed with sufficient knowledge and justification to make the case for security investments. Applying a cost-benefit analysis to the Smart Grid system as a whole will reflect the true value of security and system investments that support it.

Benefits

A Smart Grid that is resilient to attack and natural disaster provides a number of benefits. These benefits include:

- Deterring an attack from occurring thereby reducing the number of 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 of grid repair and 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

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:

- Leverage methods developed by DOD, DOE, and DHS to increase survivability of systems.
- Create a government-industry team, including state regulators, specifically to address issues of unacceptable risk to the public from disruptions and return on investment for industries' investments in security.
- 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 on 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 for 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.
- Include security benefits in all Smart Grid business cases.

More Information Available

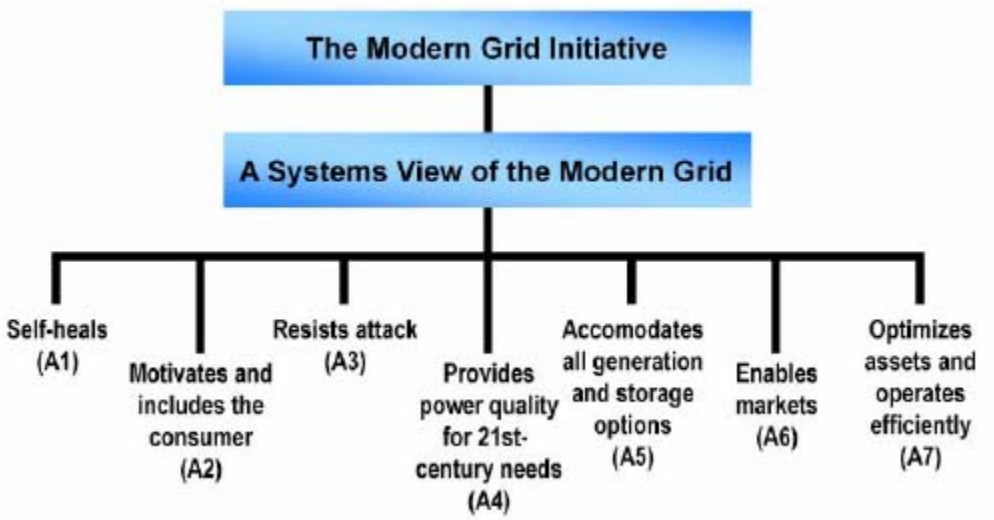

Figure 1: Principal Characteristics of a Modern Grid

Documents are available for free download from the Modern Grid website:

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

Email: moderngrid@netl.doe.gov

(304) 599-4273 x101

[1] Hamre, J. 2003. "Cyberwar! Interview with John Hamre." PBS Frontline, February 18.