Cyber Security Concerns

for Local Government Energy Assurance Planning

LEAP

Local Government Energy Assurance Planning

pti Public Technology Institute

U.S. DEPARTMENT OF ENERGY

Acknowledgement

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000116.

Disclaimer

U.S. Department of Energy

The U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) funded the production of this publication. The Infrastructure Security and Energy Restoration Division (ISER) of OE is the primary DOE office responsible for energy emergency planning and response. For more information, visit the OE website at: www.oe.energy.gov. This Guidance document was produced by DOE/OE/ISER under the leadership of Alice Lippert, Program Manager for DOE's State and Local Government Energy Assurance Program.

Public Technology Institute

This document was developed by Public Technology Institute (PTI). As the only national non-profit technology organization created by and for cities and counties, PTI works with a core network of leading local government officials—the PTI membership—to identify opportunities for technology research, share best practices, promote technology development initiatives and develop enhanced educational programming. Visit PTI at www.pti.org.

Local Government Energy Assurance Planning (LEAP)

To find out more about local government energy assurance efforts, we encourage readers to visit www.energyassurance.us. This site, maintained by PTI, is designed to support all local governments, large, medium and small, across the nation that want to learn more about creating energy assurance plans for their communities. Once created, these plans will help ensure that local governments can provide life-saving services during an energy emergency.

Editorial Team

This publication would not have been possible without the efforts of Charles Bicknell and Mark Lesiw of The Cadmus Group, Inc. This work was managed by Ronda Mosley, Assistant Executive Director for Research and Government Services, Public Technology Institute.

Cyber Security Concerns for Local Government Energy Assurance Planning

1 Overview and Background

The Nation's energy infrastructure contains numerous vulnerabilities that local governments need to address in their energy assurance plans (EAPs). Disruptions to energy supplies are commonly attributed to natural disasters such as storms, floods and fires, or to situations where the demand for energy exceeds the supply. Because cyber security concerns are usually handled by Internet-focused industries and information technology departments, local governments may not typically consider vulnerabilities of computers and computer systems to unauthorized use or attack. However, with the increased use of interconnected, Internet-based technology in the energy industry, and with recent attempts to harm energy sector control systems, cyber security is an increasing concern for energy assurance planners. To mitigate the risk of cyber attack, it is necessary to harden computer and information systems by making them less vulnerable to external influences.

In the following passage, the Public Technology Institute's (PTI) *Local Government Energy Assurance Guidelines, Version 2.0* explains cyber security as it pertains to energy assurance.[1]

> *Cyber security is the protection of all things pertaining to the Internet, from networks themselves to the information stored in computer databases and other applications, to devices that control equipment operations via network connections. Vulnerabilities are present in nearly every aspect of the networks used in modern community energy infrastructure. Effective local government EAPs will investigate and address these vulnerabilities.*
>
> *Variables that may influence the cyber security aspects of a local EAP include the relationship between an energy service provider and the local government, the presence of critical energy infrastructure in the community, the size of the community, and the amount of funds available to the local government to provide more secure information. The degree to which a large city needs to investigate and plan for cyber security threats is likely to be significantly different than what is needed or affordable for a small rural community. As systems become increasingly interconnected and interdependent, however, the level of security necessary for all communities is increasingly equalized.*

Local governments should work with their energy service providers to investigate and address:

- Direct cyber security threats to energy generation, routing/transmission, and distribution systems
- Direct threats to users
- Ancillary threats to related personal or proprietary information
- Communication threats

[1] Public Technology Institute (PTI). *Local Government Energy Assurance Guidelines, Version 2.0.* 2011. http://dl.dropbox.com/u/14265518/leap/PTI_Energy_Guidelines.correx.v2.pdf.

In many cases, utilities may have already developed cyber security protections and may not want to share specific information with the public or local government due to potential security or proprietary information concerns. Similarly, local governments may not want to include detailed information on specific vulnerabilities and cyber security procedures in the public version of their EAPs due to the sensitive nature of the information. This document discusses different cyber security concerns that local governments should understand, and may want to discuss with their energy service providers as part of developing an effective EAP.

1.1 Recent Headlines in Cyber Security

Over recent years, multiple cyber attacks on energy infrastructure worldwide have highlighted the need for increased cyber security. The Stuxnet virus, for example, raised global concern in July 2010. Stuxnet was a self-replicating computer program that spread through network connections – otherwise known as a worm – and it was the first worm discovered that specifically targeted industrial control systems and had the potential to cause malfunctions in nuclear facilities.[2] In 2009, U.S. intelligence agencies found software left by cyber spies that had penetrated the U.S. electrical grid.[3] Officials do not believe that the intruders sought to cause damage to the power grid, though similar attacks could have applications during warfare or large-scale conflict. Other recent cyber attacks include attempts (successful in one case) to hack into two American electrical utilities: a single Internet Protocol (IP) address originating from China attempted to log into a Texas power company 4,800 times,[4] and in May 2009, an unknown assailant hacked into Florida's Lake Worth Master Supervisory Control and Data Acquisition (SCADA) computer.[5]

The United States has not yet suffered any damage or disruption of service as a result of cyber attack. However, blackouts in 2005 and 2007 caused by successful attacks in Brazil[6] emphasize the vulnerability of energy systems to cyber warfare. A March 2010 article written by the Center for Strategic and International Studies (CSIS) reports on the extent to which the U.S. electricity grid is susceptible to cyber attack.[7] The article describes the Aurora tests, conducted at Idaho National Labs, in which researchers were able to remotely change the operating cycles of the generators, causing them to run out of control.

---

[2] Markoff, John. *Worm Can Deal Double Blow to Nuclear Program.* New York Times. November 19, 2010. http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html.
[3] Gorman, Siobhan. *Electricity Grid in U.S. Penetrated by Spies.* Wall Street Journal. April 8, 2009. http://online.wsj.com/article/SB123914805204099085.html.
[4] Arnold, Robert. *Cyber Attack Aimed at Texas Electricity Provider.* Wall Street Journal. April 3, 2010. http://www.click2houston.com/news/23046216/detail.html.
[5] Mulvay, Dave & Mattey, Rebecca. *Uncorrected Security Breach at LWU Threatens Florida Bulk Power.* Lake Worth Media. May 27, 2009. http://lakeworthmedia.com/modules.php?name=News&file=print&sid=503.
[6] CBS News *Cyber War: Sabotaging the System.* http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.
[7] Center for Strategic and International Studies. *The Electrical Grid as a Target for Cyber Attack.* March, 2010. http://csis.org/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf.

Over the next decade, the electric grid – already vastly interconnected – will be upgraded to allow for multi-directional electricity flow. Numerous technologies using sophisticated computer systems and the Internet will be deployed to improve the connectivity of electric transmission and distribution systems. These systems are likely to be implemented in dozens of jurisdictions across the United States, based largely on utility interest and the ability of consumers and their utilities to pay for the systems. This new and improved electric grid, known as the smart grid, will allow electronic devices to communicate information, such as the price of electricity and the status of power lines. However, increased connectivity may make electricity delivery systems more vulnerable to cyber attack because the smart grid integrates public networks with power control networks that are typically closed. As the smart grid expands, it is important that planners understand and address these security concerns. (For more information on the smart grid, see PTI's "Smart Grid 101 for Local Governments."[8])

1.2 Potential Impacts on All Stakeholders

Recognizing the potential impact of cyber attack is critical to the development of a local government EAP. Because much of the public's way of life depends on electricity, natural gas, and petroleum products, cyber attacks on energy delivery systems have the potential to cause large-scale disruptions throughout the United States. Addressing cyber security concerns in local government EAPs can help reduce the chances that an energy disruption will have a devastating effect on the jurisdiction. The potential impact on all levels of critical infrastructure should be evaluated, including energy generation/supply, transmission and distribution infrastructure, and other key facilities. Attacks have the potential to affect electric, gas and petroleum delivery systems, and disruptions to those systems will in turn impact water and wastewater systems, financial networks, communication networks, and many additional entities, such as State and Federal governments.

2 Areas of Vulnerability

The current electric grid has numerous cyber security vulnerabilities. In general, any networked device along the grid is potentially vulnerable to cyber attack. As the number of smart grid technologies deployed on the grid increases, so too will the number of points along the grid that are vulnerable to cyber security threats. This growth pattern creates a need for increasingly robust protection of these access points. Another important consideration is that increased centralization of energy controls brings with it an increased susceptibility to cyber attack. To a saboteur, for example, one large control center may be a more valued target than 10 different regional control centers.

2.1 Internet-Connected Energy Management Systems

Utilities employ relatively sophisticated systems to monitor and control various components of the electricity grid. Until the proliferation of the Internet, many of these systems were isolated from outside influences and from one another. For example, monitoring systems for generation facilities were not necessarily directly linked to those for transmission and distribution systems.

[8] PTI. *Smart Grid 101 for Local Governments*. http://dl.dropbox.com/u/14265518/leap/Smart_Grid_101-7-6-2011.pdf.

However, as the Internet has evolved and as the majority of computers have become connected to the Internet, these distinct networks have become intertwined and more susceptible to cyber security threats. Energy management systems that are connected to the Internet are subject to the most serious cyber security threats because they are capable of changing physical settings of critical grid components such as valves in piping systems, voltage levels along electric transmission and distribution systems, and the speed at which generator turbines spin.

2.1.1 Overlap

The North American Electric Reliability Corporation (NERC) recommends specific cyber security standards that call for firewalls and separate networks to protect energy management systems from interference that could come through the Internet. However, it is difficult to completely isolate these systems. Shared communications infrastructure connecting metering and control equipment to energy management systems creates an inevitable overlap with the Internet. These overlaps are vulnerable points of access for hackers, and may provide the opportunity to interfere with the energy grid. Any large-scale cyber attacks on the energy grid will likely involve the malfunction or disabling of energy management systems.

2.1.2 Network Access Points

Nearly any point on the electric grid that can be accessed through the Internet has the potential to be exploited by hackers, particularly as the grid becomes more interconnected. The existing electric grid is a relatively closed system. In other words, most of the control functions take place through networks that only utilities can access. Data communication generally occurs in one direction; devices on the grid can report their condition to a central point, typically the utility control center. Some utility operations can adjust the grid by sending remote messages to devices, but most adjustments are made physically. Deployment of smart grid technologies capable of two-way communication, however, creates additional points along the electric grid that can be accessed by unauthorized individuals. For instance, smart meters that are equipped with two-way communication technology capable of sending and receiving information may be installed on residential, commercial, and industrial buildings. As the number of smart meters increases, and as other smart grid technologies are deployed, hundreds of millions of network access points are created, and will need to be secured. The wide area networks created by smart meters and other smart grid technologies will need to be adequately protected to reduce their vulnerability to potential cyber attacks.

2.2 Human Factors

The people who maintain the grid may be the source of one of the greatest cyber security vulnerabilities. Many computer cyber attacks—not necessarily energy related—are introduced via a simple e-mail or an infected storage device (such as a USB thumb drive). The energy grid and its related control systems were not initially designed with security as a priority, and the employees who operate them have traditionally been trained to focus on the generation, transmission, distribution and delivery of energy, rather than system security. Consequently, a significant cyber security risk to the energy grid may come from inadvertent exposure by staff of the energy systems.

Malicious attacks by employees or former employees of many systems can also occur. Employee login information could also be targeted to gain control of energy management or other control systems. To decrease vulnerability to attacks by employees, local governments may want to ensure that utilities restrict access to energy grid computer systems. Employees should only have access to the systems required for their job functions. Information technology staff members or other staff should consider monitoring system usage by employees and outsiders to quickly detect unauthorized or suspicious activity.

3 Direct and Ancillary Threats

In addition to understanding areas of vulnerability for both the existing electric grid and the smart grid, it is useful to understand the different types of cyber security threats when developing an EAP. Cyber security threats can be categorized into two types: direct and ancillary. Both types take the form of external influences or attacks on the electric grid. Direct threats are those that compromise energy delivery in the short term – or immediately. For example, a hacker can send control signals to a generation facility, causing the turbines to catastrophically fail. Ancillary threats pose long-term risk to energy delivery. An example of an ancillary threat would be unauthorized access to personal information or competitive information about business energy usage, which could threaten energy delivery in the long term.

3.1 Direct Threats to Supply and Reliability

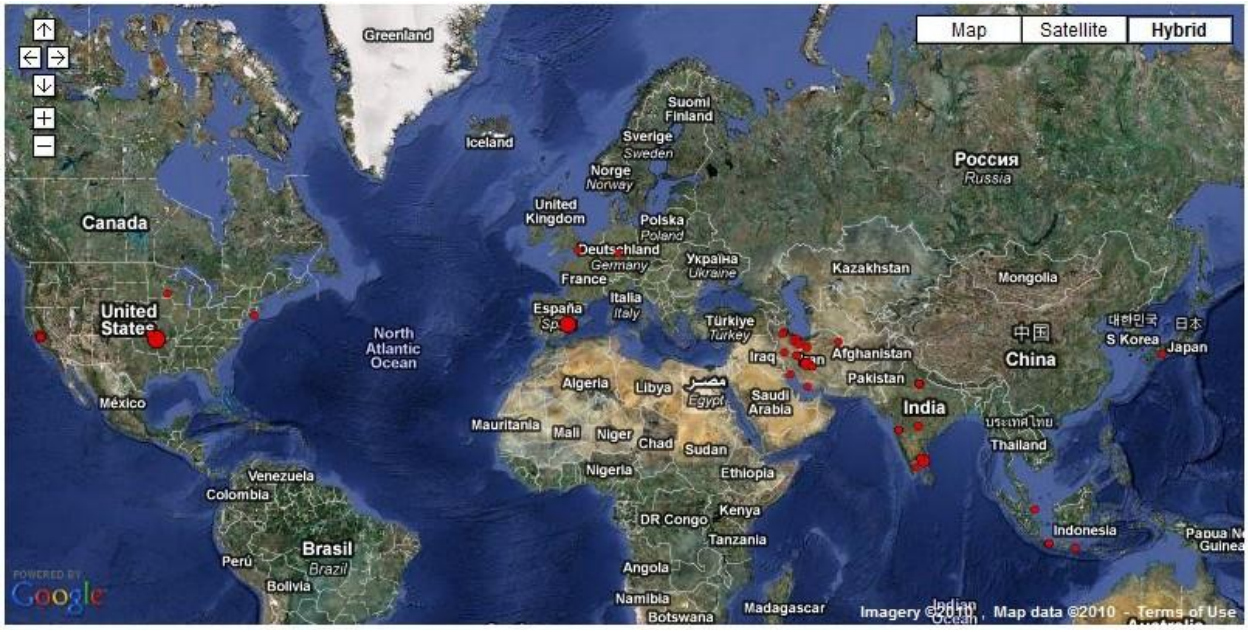
3.1.1 Generation

As noted earlier, the Stuxnet virus stands out as an example of what can happen to electric generation when cyber security is breached. Experts believe that the virus was transferred to an Iranian nuclear fuel processing facility from a portable storage device. As it did in Iran, the Stuxnet virus can disable uranium enriching centrifuges and steam turbines at nuclear power plants.[9] The Stuxnet virus also has the potential to affect programmable logic controller (PLC) systems made by Siemens.[10] The Siemens' PLCs run many different automated processes, including those found in electric power plants. The fact that the Stuxnet virus targets these controllers is further evidence that cyber attacks specifically designed to disrupt energy systems are being developed. Figure 1 below shows known outbreaks of the Stuxnet virus.

[9] Markoff, John. *Worm Can Deal Double Blow to Nuclear Program.* New York Times. November 19, 2010. http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html.

[10] Schneier, Bruce. *The Story Behind The Stuxnet Virus.* Forbes online. October 7, 2010. http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html.

Figure 1. Stuxnet Instances (September 2010)



Source: Schmugar, Craig. *Stuxnet Update.* September 24, 2010. http://blogs.mcafee.com/mcafee-labs/stuxnet-update.

3.1.2 Routing/Transmission and Distribution and Cascading Impacts

It bears repeating that the vast interconnectivity of the U.S. electric grid creates a vulnerability to cyber threat. This interconnectedness will only increase with the deployment of smart grid technologies that provide two-way communications on the needs, use, and flow of electricity. The smart grid will react quickly to energy demand, potentially prevent power outages, and recover from power outages or disruptions rapidly by routing power around damaged portions of the grid. However, existing vulnerabilities along transmission and distribution lines can become exacerbated as these new technologies add hackable points to the grid. Once a hacker gains access, power could be misrouted and false power problems could be reported, resulting in power outages, even if the system was, in fact, operating normally. If such an attack were not caught or prevented, an isolated incident could lead to a cascading power outage with wide-ranging impacts.

3.1.3 Metered Users

Outages can be also be triggered at customer facilities if remote management tools are exploited. This may be a concern to local communities that are deploying technologies such as smart meters. In March 2010, three anonymous utilities hired the security firm InGuardians Inc. to test smart meters, and found egregious flaws and vulnerabilities in the technology.[11] Some early smart meters may be vulnerable to computer viruses[12] that could make them unresponsive to utility commands. To address that risk, smart meter manufacturers are now incorporating additional cyber protection capabilities into their meters, including advanced encryption software

[11] Smart Meters – Smart Energy News. *Security Firm Reveals Smart Meter's Vulnerability.* March 31, 2010. http://www.smartmeters.com/the-news/893-security-firm-reveals-smart-meters-vulnerability.html.
[12] Fehrenbacher, Katie. *Smart Meter Worm Could Spread Like A Virus.* July 31, 2009. http://gigaom.com/cleantech/smart-meter-worm-could-spread-like-a-virus/.

to help prevent the possibility of a cyber attack. Because of the possibility of customer facility outages due to cyber security weakness, local governments should ensure that smart meters used by their local utilities have the most advanced cyber security controls.

3.2 Ancillary Threats

Ancillary threats may not have immediate impacts, and may not be directly relevant to a local EAP due to their limited impact on direct power delivery to customers. However, ancillary threats could include unauthorized access to personal or confidential information (such as billing and account information or meter data), and local governments may want to help address such concerns. Governments and utilities can work together to reduce the threat of private data theft from utility databases. Recently, many States have developed standards to protect customer information and to provide notification of an unauthorized data breach. When developing an EAP, local governments should confirm with their utilities that appropriate safeguards are in place to prevent such ancillary threats.

For more information about specific State standards, visit http://www.naruc.org.

4 Utility Safeguards and Cyber Security Measures

Because cyber security threats increase the potential for devastating impacts to energy infrastructure, the Federal Energy Regulatory Commission (FERC) has established critical infrastructure protection standards that are overseen by NERC. These standards will empower utilities to prevent and recover from cyber security attacks. The standards can be found on NERC's website,[13] and include provisions for:

- Identifying critical cyber assets (section 002)
- Developing security management controls (section 003)
- Implementing training (section 004)
- Identifying and implementing perimeter security (section 005)
- Implementing a physical security program for protecting critical cyber assets (section 006)
- Protecting assets and information within the perimeter (section 007)
- Conducting incident reporting and response planning (section 008)
- Crafting and implementing recovery plans (section 009)

Local governments may want to discuss the critical infrastructure protection standards with their utilities to understand the progress utilities are making in meeting these standards. This will help

[13] NERC website. http://www.nerc.com/page.php?cid=2%7C20.

ensure that utilities are taking proactive measures to protect cyber assets and the electric grid from cyber attack.

5 Cyber Threat Risk Reduction (Hardening) Steps for Local Governments and Utilities

Local governments should work with their local energy utilities and other stakeholders to understand and identify cyber security vulnerabilities and work to minimize threats. While local governments may not be directly responsible for cyber protection of energy infrastructure, they may want to discuss some of the solutions identified below with their utilities to ensure that plans are in place to respond to and mitigate cyber attacks.[14] Many of the strategies below can also be used by local governments to protect their own computer systems, especially those that may contain confidential information. Because education on cyber threats and the measures used to protect against them is often one of the first lines of defense, this activity is fundamental to the development of an EAP. Many of the protocols and techniques that are already in place in the information technology industry – some as simple as policies regarding password strength – will also be worth considering during EAP development. Once vulnerabilities are identified, prevention and mitigation activities can be undertaken. Such activities include:

- **Instituting access control policies**. Restrict access to key terminals, files, and networks, allowing only trained individuals who need to work with those resources.
- **Adopting security protocols**. Keep up to date on industry-standard software protection protocols, including the utilization of appropriate protective software, link scanning, maintaining sufficient firewalls, and regularly installing security patches and upgrades to protect against viruses, spyware, malware, phishing, spam, threats and error detection, and rootkits.
- **Monitoring and reporting threats**. Regularly monitor virus tracking and other threat assessment websites for updated information on threats and mitigation for those threats, and promptly report any threats encountered.
- **Monitoring systems**. Constantly monitor system usage and assess abnormal usage patterns to identify vulnerabilities and attacks before they occur.
- **Training**. Train individuals responsible for system reliability to recognize and respond to security threats.

[14] National Association of State Energy Officials. *Smart Grid & Cyber Security for Energy Assurance Planning Elements for Consideration in States' Energy Assurance Plans.* December 2010. http://www.naseo.org/energyassurance/Smart_Grid_and_Cyber_Security_for_Energy_Assurance-NASEO_December_2010.pdf.

- **Testing**. Test security protocols and procedures and ensure that the EAP includes regular cyber attack and response simulations; have tests and evaluations conducted by third parties to help identify potential vulnerabilities.

- **Verifying information**. Verify information before responding to a potential threat. Taking corrective action when there is no problem could result in unintended negative consequences.

- **Pre-planning and identifying threats**. Local governments may want to work with their utilities to develop a pre-plan to respond to a cyber security threat. The plan can include a process to identify cyber threats. In addition, local governments can prioritize event response for critical facilities based on whether the event was caused by cyber security vulnerability.

6 Case Studies

The following energy infrastructure case studies identify some of the threats associated with improper security protocols on networked systems.

6.1 Control System Cyber Security Case Study: Bellingham, Washington, June 1999

A gasoline pipeline rupture in Bellingham, Washington in June 1999 was caused by numerous factors including: damage to the pipeline during previous excavation work; failure of the pipeline company to detect and fix the damaged pipeline; a faulty pressure-release valve; a non-responsive SCADA system; failure of the company to follow standard policies and protocols; and failure to properly train employees. Functional energy management systems are critical for providing controllers with accurate information and the ability to take corrective actions. The Bellingham pipeline rupture shows how the failure of these systems can cause (or contribute to) significant damage, and that not all cyber security threats involve malicious intent.[15]

Smoke from the pipeline rupture.
Source: http://www.ens-newswire.com/ens/pics22/bellinghamsmoke.jpg.

A series of events caused the gasoline pipeline to rupture from over-pressurization. At 3 p.m. on June 10, 1999, gasoline delivery point information was changed in the SCADA system. At the same time, a system administrator created two new records in the historical database. Ten minutes later, error messages were generated by the SCADA computer relating to the historical database. The records were checked over by the system administrator, who then left the computer terminal for 15 minutes. The main SCADA system became non-responsive a few minutes later, was taken offline, and the backup SCADA system was brought online. A minute

[15] Abrams, Marshall and Joe Weiss. *Bellingham, Washington, Control System Cyber Security Case Study.* http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf.

after the backup system was in place, the pipeline ruptured. Once the new records were deleted, the backup SCADA system began to function properly, and pipeline flow resumed. Thirteen minutes later, after pipeline flow had resumed, the leak was detected by controllers. Because the controllers were unaware of the rupture during the time the SCADA system became non-responsive and the backup system was brought online, the controllers started pumps that eventually released approximately 250,000 gallons of gasoline. The gas soon caught on fire, killing three people and injuring eight, causing significant property damage, and leaving tremendous, lasting environmental impacts.

The National Transportation Safety Board (NTSB) was unable to determine if the unresponsive equipment was a result of malicious actions because the pipeline employees who were on duty at the time refused to be interviewed by the NTSB. The incident was further examined as part of a National Institute of Standards and Technology (NIST) project. The report noted that standard protocols and cyber security features were not in place at the time of this catastrophe; had such protocols been in place, the controllers would have been able to alert other controllers earlier of the malfunctioning SCADA system. Those interested in taking malicious action to cause similar impacts could potentially recreate events similar to this if they manipulated or impacted the normal communication of system data used to operate these systems.

6.2 Electric Power Systems Cyber Security Case Study: Power Substation, January 2006

The European Workshop on Industrial Computer Systems (EWIC) developed a framework for understanding the operation and networking of electric power systems. The framework describes the hazards associated with using networked computers to control electric power systems, and outlines ways to prevent those hazards from causing damage. The study also describes the vulnerability of electric substations from switching operations. The vulnerability could arise from either a failure of the software safety mechanisms intended to prevent catastrophic failures, or from a cyber attack. If the software does not open or close certain circuits in a proper sequence, electrical arcing could cause an explosion. Incorrect closing of some circuits could lead to a power disruption or full-scale blackout. Failures in both software protocols or failure to prevent a cyber attack increases the potential for catastrophic events to occur.[16]

7 Additional Resources

The following references provide more information about cyber security threats, as well as policies and procedures in place to address cyber security threats:

- Public Technology Institute's (PTI) *Local Government Energy Assurance Guidelines.* http://www.pti.org/docs-sust/LocalGovernmentEnergyAssuranceGuidelines.pdf.
- The National Association of State Energy Officials' (NASEO) *Smart Grid & Cyber Security for Energy Assurance: Planning Elements for Consideration in States' Energy Assurance Plans.*

[16] http://www.energycentral.com/download/products/EPSCyberSecurity.pdf.

http://www.naseo.org/energyassurance/Smart_Grid_and_Cyber_Security_for_Energy_Assurance-NASEO_December_2010.pdf.

- The National Institute of Standards and Technology's *Guidelines for Smart Grid Cyber Security*. http://www.nist.gov/smartgrid/.

- The Federal Energy Regulatory Commission's Smart Grid Policy. http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf.

- U.S. Department of Energy. http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

- U.S. Department of Homeland Security. http://www.dhs.gov/files/cybersecurity.shtm.

- U.S. Department of Defense. http://www.defense.gov/home/features/2010/0410_cybersec/.

8 Sources

Abrams, Marshall and Joe Weiss. *Bellingham, Washington, Control System Cyber Security Case Study*. Available at http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf.

Arnold, Robert. *Cyber Attack Aimed at Texas Electricity Provider*. Wall Street Journal. April 3, 2010. Available at http://www.click2houston.com/news/23046216/detail.html.

Center for Strategic and International Studies. *The Electrical Grid as a Target for Cyber Attack.* March, 2010. Available at http://csis.org/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf.

European Workshop on Industrial Computer Systems Technical Committee 7: Reliability, Safety, Security. *Subgroup Security Briefing Paper Electric Power Systems Cyber Security: Power Substation Case Study*. January 18, 2006. Available at http://www.energycentral.com/download/products/EPSCyberSecurity.pdf.

Federal Energy Regulatory Commission. 18 CFR Chapter I [Docket No. PL09-4-000]. *Smart Grid Policy*. July 16, 2009. Available at http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf.

Fehrenbacher, Katie. *Smart Meter Worm Could Spread Like A Virus.* July 31, 2009. Available at http://gigaom.com/cleantech/smart-meter-worm-could-spread-like-a-virus/.

Gorman, Siobhan. *Electricity Grid in U.S. Penetrated by Spies.* Wall Street Journal. April 8, 2009. Available at http://online.wsj.com/article/SB123914805204099085.html.

Markoff, John. *Worm Can Deal Double Blow to Nuclear Program.* New York Times. November 19, 2010. Available at http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html.

Mulvay, Dave & Mattey, Rebecca. *Uncorrected Security Breach at LWU Threatens Florida Bulk Power*. Lake Worth Media. May 27, 2009. Available at http://www.lakeworthmedia.com/modules.php?name=News&file=article&sid=503.

National Association of State Energy Officials. *Smart Grid & Cyber Security for Energy Assurance Planning Elements for Consideration in States' Energy Assurance Plans.* December 2010. Available at http://www.naseo.org/energyassurance/Smart_Grid_and_Cyber_Security_for_Energy_Assurance-NASEO_December_2010.pdf.

National Institute of Standards and Technology. Smart Grid website. Available at http://www.nist.gov/smartgrid/.

Public Technology Institute. *Local Government Energy Assurance Guidelines.* Available at http://www.pti.org/docs-sust/LocalGovernmentEnergyAssuranceGuidelines.pdf.

Public Technology Institute (PTI). *Local Government Energy Assurance Guidelines, Version 2.0.* 2011. Available at http://dl.dropbox.com/u/14265518/leap/PTI_Energy_Guidelines.correx.v2.pdf.

PTI. *Smart Grid 101 for Local Governments*. 2011. http://dl.dropbox.com/u/14265518/leap/Smart_Grid_101-7-6-2011.pdf.

Schneier, Bruce. *The Story Behind The Stuxnet Virus.* Forbes online. October 7, 2010. Available at http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html.

Smart Meters – Smart Energy News. *Security Firm Reveals Smart Meter's Vulnerability.* March 31, 2010. Available at http://www.smartmeters.com/the-news/893-security-firm-reveals-smart-meters-vulnerability.html.

Wei, Dong, Yan Lu, Paul Skare, Mohsen Jafari, Kenneth Rohde, and Michael Muller. *Power Infrastructure Security: Fundamental Insights of Potential Cyber Attacks and Their Impacts on the Power Grid.* Available at http://cimic.rutgers.edu/positionPapers/CPS_SCR_AC_1_IEEE.pdf.