IBM end-to-end security for smart grids
Introduction

The electric grid has been providing reliable electric energy for decades. Comprised of generating, transmission, and distribution equipment along with its associated control systems and operating staff, the electric grid is vital to the world. And when it fails, civilization comes to a standstill.

The grid infrastructure has been subjected to minimal maintenance-mode investment for decades, and it needs to be overhauled. An aging workforce, rising energy costs, globalization, environmental issues, and terrorism or malicious abuse of these systems threaten the grid’s sustainability. Security concerns for these critical infrastructures in North America and Europe have recently been heightened.¹

Around the globe, the reliability of the grid is governed by various entities: government mandates and commissions, industry consortia, and regulatory bodies. In December 2008, the U.S. Department of Energy (DOE) published a report on the nation’s goal to transform its energy grid into a more intelligent, resilient, reliable, secure, self-balancing, and interactive network.² In March 2009, the U.S. Federal Energy Regulatory Commission (FERC) proposed a policy statement and action plan that provides guidance for the development of a smarter grid for the nation’s electric transmission system. This plan focuses on the development of key standards to achieve interoperability of smart grid devices and systems.³ An IBM white paper published five years ago concurs with these views of DOE and FERC to build smart grids.⁴

The Council of the European Union recently adopted a Council Directive for the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.⁵ While EU member states are responsible for policies regarding the security of energy facilities in...
their territories, the European Commission for Energy is responsible for developing pan-EU critical infrastructure protection policies and recommendations. In the UK, the Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides protective security advice to businesses and organizations across the national infrastructure.

This paper focuses on the security aspects of protecting the electric grid. It discusses the end-to-end security needs and solutions at various points in the smart grid chain. Security solutions related to the North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) requirements are used as examples of best-practice methods for securing the grid. In addition, this paper addresses security for remote device monitoring, Supervisory Control And Data Acquisition (SCADA) systems, and the Advanced Meter Infrastructure (AMI). The paper then explains how IBM software, hardware and services can help you meet these regulations and security requirements.

Why we need a smart grid

The concept of a smart grid is the application of a set of diverse digital technologies that enhance the value chain of the electric power industry. These digital technologies, comprised of new devices and applications, some of which are Internet Protocol (IP) enabled, will aid in the sharing of information and coordination of management of the generation, transmission, and distribution aspects of the infrastructure across distributed energy resources.

Grid modernization will overhaul the energy industry, creating better visualization and control for operators. The application of digital technologies can help reduce peak demand through dynamic optimization, reduce operations and maintenance costs, integrate renewable sources of energy, improve grid reliability, and make transmission and distribution more efficient. Such efficiencies can be established only with smart devices and applications that enable a finer level of visibility, control and automation.
On the residential front, consumers can be given more options to control home appliances and to derive on-demand information to better understand and manage their consumption.

We need a smart grid to manage not only energy flow but also information exchange and equipment operation. Regulations imposed by governments or industry consortiums oversee the development and enforcement of reliability standards and monitor the bulk-power systems. The stakeholders of the electrical grid include independent service operators (ISOs), remote transmission operators (RTOs), various utilities, and consumers.

**Security for the smart grid**

Security is a vital element of any technology related to sensitive assets, and new technological advancements force organizations to face new security concerns and risks. When devices like smart meters are made more secure, their business value increases because organizations can respond dynamically and with confidence to new market opportunities or changing conditions. This allows for improved efficiency, reduced costs, and improved continuity of services. Robust security for the grid can have a tremendous positive impact, as a lack of security directly threatens the safety of the public and all of those who are affected by grid failures.

As an example, there is a global effort to transform the electric grid to a digital infrastructure. A fundamental move like this is considered necessary in order to keep up with energy and utility operational demands while maintaining or improving the bottom line. A digital infrastructure can be more flexible and dynamic; however, such a network may expose the critical infrastructure to additional security concerns such as unapproved access and cyber attacks.
A lack of adequate security in the energy industry could pose threats of service disruption, which can impede safe and efficient functioning of the system. Added layers of security controls, policies, and procedures are necessary to help protect and manage the grid.

The best approach to securing smart grids is to identify and quantify the risks across the entire value chain, develop the appropriate policies and controls to manage these risks, deploy the policies and controls, and then perform systematic, periodic reviews, including vulnerability testing.

**How can IBM address smart grid security?**

IBM has been very successful in providing security consulting, design, build, and managed services solutions for critical infrastructure in a wide range of demanding industries, including defense, financial services, and energy and utilities. IBM security solutions are based on the IBM Security Framework (see Figure 1), which defines an end-to-end approach to developing, deploying and supporting security solutions across domains of people, networks, applications, data, and the physical plant.

*Figure 1: IBM takes a holistic approach to security through the IBM Security Framework.*
IBM has the technology and expertise to deploy end-to-end security solutions for smart grid implementations, and is committed to providing security solutions within the context of regulatory standards.

**Security for the utility business**

In-depth IT security design principles state that better security management is achieved when an entity is protected by not just one layer or one component, but by multiple, diverse mechanisms. These and many other IT security principles are addressed by global IT security standards ISO 27002:2005 and ISO 15408. They cover areas such as defense-in-depth principles, trusted and consistent identities, authentication and access control, information flow control, encryption of sensitive data at-rest and in-transit, audit and compliance, and resiliency. All energy and utility organizations should leverage these principles for their corporate business and IT infrastructures.

Business applications can pose a serious security threat when accessed by unauthorized users. Applications can produce unintended results with malformed input data. Thus, utility applications must be immune to issues such as suspicious demand-response bids from a home, a negative meter reading, or more subtle but seemingly valid scenarios. IBM can help utilities scan applications with security penetration testing for vulnerabilities before they are deployed and while they are in operation.

**Security for advanced metering data management systems**

IBM is working with utilities to implement smart meters as a core component of a new intelligent utility network infrastructure that uses digital technology. Many meter vendors have implemented their own protocols between the smart meter and the head-end collectors to comply with the security requirements...
While the jurisdiction between smart meters and the head-end collectors often lies with the meter vendor of choice, the utility meter network data is fed into different business processes and applications such as meter demand management, enterprise asset management, financial management, customer support, and outage management. IBM has been working with utility companies to rapidly adopt a service-oriented architecture (SOA) approach for such business processes and applications. Advanced meter management from IBM is a cornerstone of the IBM Intelligent Utility Network solution suite. Advanced meter management from IBM is a cornerstone of the IBM Intelligent Utility Network solution suite. Advanced meter management from IBM is a cornerstone of the IBM Intelligent Utility Network solution suite.

IBM has also developed the Solution Architecture for Energy (SAFE), a framework which enables integration across the enterprise with grid and distribution management, finance and administration, customer management, human resources, and procurement. As shown in Figure 2, the enterprise portion of SAFE is based on SOA, which enables the utility to build and extend new services to customers easily and cost-effectively through the efficient flow of information across the enterprise. This architecture is intended to provide business applications and services that can securely interoperate with business partners, suppliers, regulators, and utility customers while securely maintaining the confidentiality, integrity, and accountability of data exchanged, and that can also link to embedded and operational systems.
Security for SCADA systems

IBM recognizes that security for the smart grid goes beyond the business and IT domains. Conventional enterprise IT security measures must be adapted and extended into the industrial process control systems, which involve a myriad of proprietary interfaces, protocols, and heterogeneous devices spread over a large geographic and governance space. The challenge for smart grid security is that there are two distinct spaces that must be bridged securely.

The business enterprise operations of the energy utility often engage in data sharing that relies on the Internet as well as corporate intranets and extranets. Existing programmable logic controllers, remote terminal units (RTUs), and SCADA systems may have been designed with security based on physical isolation. Some utilities are using corporate intranets or even the Internet to access devices on the control systems in order to increase productivity and offer seamless connectivity. These approaches require thoughtful analysis because they may introduce new security vulnerabilities.
Industrial control systems security typically involves securing two different computing systems and networks. First, the operator consoles and applications that use commercial operating systems must be secured. These consoles are typically protected by enterprise role-based access control and governed by business-driven policy.

Second, the process equipment control systems that receive commands, measure data, and generate actions and events must be secured. These field devices were designed to reside in isolated process-control networks, with the assumption that only a few, trusted operators would have the ability to access them. IP-enabling this field equipment into intelligent electronic devices (IEDs) allows for seamless remote control but can make the control infrastructure more vulnerable. Proper network demarcation and protection of networks with appropriate security controls is essential for robust smart grid security (see Figure 3).
IBM participates in open security standards committees and embraces these standards to facilitate integration with industry-leading components, including integration with different end-point devices and with independent service vendors (ISVs) who are helping to create successful solutions. This is essential for SCADA security where there are several players that comprise the process control grid equipment.

Remote device monitoring is the key to enhancing the reliability of the grid. The substations along the electricity supply chain contain many RTUs or IEDs. However, the monitored data from these substations can only be relied upon if the integrity of the data is assured by the security of the substation equipment. Currently, there is a need to perform case-by-case technical assessments of vendor products, studying the interfaces they expose and the protocols they use so that their security can be assured within the greater cyber security context. Security for such devices is being standardized according to the IEC/TS 62351 and 62443 standards.

As more standardization occurs in smart grids, the process control networks can benefit from lessons learned from IT networks running business applications. This allows for some Internet technologies to be applied for remote device monitoring where applicable. Timing and deterministic properties have to be evaluated so security does not disrupt the prime mission of these systems. IBM’s IT security capabilities can be used for remote device monitoring, along with enterprise asset management software and grid operations.

**Supporting Critical Infrastructure Protection standards**

Most countries have developed mandatory reliability standards applicable to all energy-producing and transmitting utilities, like the NERC Critical Infrastructure Protection (CIP) standard in North America. One area of regulatory reliability specifically addresses protecting electric grid bulk-power cyber assets.
IBM can help utilities comply with critical infrastructure protection standards like the ones listed in NERC CIP-001 through CIP-009 by applying security offerings at consulting, design, development, build, and operational levels. Leveraging the IBM Security Framework infuses security into the lifecycle of energy management software and the networking of field control devices.

**Sabotage Reporting (CIP-001)** – NERC provides directives and procedures for detection, recognition and reporting of sabotage events. It specifies procedures for communications to appropriate parties and local authorities. It expects security monitoring tools to provide near real-time notifications for reporting. IBM solutions enable the utility to continuously monitor security violations during operations, as well as detect out-of-compliance conditions. These products can even help track user activity for privileged users, including physical location, deterring insider attacks.

**Critical Cyber Asset Identification (CIP-002)** – NERC has recognized the need for identification and documentation of critical cyber assets. Identifying these assets and their relationships helps lay the foundation for applying security principles within each asset’s function as well as communications between the asset and other assets in the grid value chain. IBM can assist in building an integrated asset management solution.

**Security Management Controls (CIP-003)** – This directive calls for responsible organizations to document and implement a cyber security policy to represent the company’s commitment to security and their ability to secure critical cyber assets. IBM can assist with a comprehensive cyber security solution with functions like policy management, authentication and authorization.
of grid systems commands, protection and inspection of all XML traffic across network boundaries, management of keys used in encryption of data stored on tapes and disk, enablement of change management processes for configuration changes to cyber assets, comparison of activity logs against security policies, and provision of centralized identity, access, attestation and audit services.

**Personnel & Training (CIP-004)** – With this directive, NERC defines the obligations of utility management to conduct thorough personnel risk assessments in accordance with federal, state, provincial, and local laws. All personnel having authorized cyber access or authorized unescorted physical access to critical cyber assets as well as field assets must get access on a “need-to-know” basis. IBM solutions can help oversee the entire process of managing personnel risk assessments, including enrollment, proofing, and background checks as part of the identity vetting process. IBM also provides tools for managing learning/training programs.

**Electronic Security Perimeter (CIP-005)** – According to NERC, the utility is responsible for ensuring that every critical cyber asset resides within an electronic security perimeter. This perimeter needs to be identified and all access points to it need to be identified, documented, and controlled. IBM solutions for intrusion and anomaly detection can not only protect IT networks from worms, malware and viruses, but also monitor traffic between intelligent field devices for signs of suspicious activity.

**Physical Security of Critical Cyber Assets (CIP-006)** – This directive defines the physical security of a critical cyber asset as being comprised of five distinct elements: deterrence, detection, assessment, communications, and
response. IBM’s command and control center solution provides advanced physical security integration, enabling organizations to control, monitor and maintain disparate security systems and assets through a single interface.

**Systems Security Management (CIP-007)** – This item in the standard directs security management and testing procedures, patch management, account management, and vulnerability analysis. Organizations need to ensure that new cyber assets and significant changes to existing cyber assets within the electronic security perimeter do not adversely affect existing cyber security controls.

IBM provides a comprehensive management suite that provides uniform patch management for heterogeneous platforms, change and configuration management, intrusion detection and analysis, authoring and enforcement of strict identity provisioning policies, vulnerability testing for applications, consolidated logging, event correlation, dashboards for visualization, and escalation mechanisms.

**Incident Reporting and Response Planning (CIP-008)** – This directive calls for the IT and process-control operations to develop and maintain a cyber security incident response plan, documenting procedures to classify and escalate events and report security incidents to authorities. IBM’s service, incident, and problem management capabilities help manage processes for security incidents with a well-documented, repeatable workflow.

**Recovery Plans for Critical Cyber Assets (CIP-009)** – Standard CIP-009 ensures that recovery plans are put in place for critical cyber assets and that these plans follow established business continuity and disaster...
recovery techniques and practices. IBM’s asset management solutions enable services delivery and support processes for the most dynamic IT infrastructures, ensuring business resilience and promoting faster recovery during failures.

Conclusion
IBM’s holistic approach to grid security is about not only the comprehensive set of capabilities listed above, but the ability to build on our common security framework, integrating and optimizing the built-in security features of IBM hardware, software and service offerings while providing a platform for other ISV security products as well (see Figure 4).

Figure 4: The IBM Security Framework integrates IBM hardware, software, and services while providing a platform for other ISV security products.
IBM provides a comprehensive set of products and consulting, design, deployment, and managed service offerings to help comply with NERC-CIP security requirements and other industry regulations. IBM also has the expertise to implement the 21 steps recommended by the DOE for SCADA security. IBM has a proven track record in securing our nation’s most critical infrastructures including military, banking, stock markets, and utilities. IBM is unique in its ability to provide an unparalleled breadth and depth of technology, services, and scalability for proven, quantifiable results.

For more information
To learn more about how IBM solutions can help your organization meet security regulations and requirements, contact your IBM representative or IBM Business Partner, or visit: [ibm.com/security](http://ibm.com/security) and [ibm.com/energy](http://ibm.com/energy)
The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.


7 Centre for the Protection of National Infrastructure. www.cpni.gov.uk


