

Securing the Smart Grid

The smart grid promises a more efficient way of supplying and consuming energy. In essence, the smart grid is a data communications network integrated with the power grid and collects and analyzes data about power transmission, distribution, and consumption—all in near-real time. Based on this data, smart grid technology then provides predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power.

At the heart of the smart grid is integration of the data communications networks of the generation, transmission, distribution, and customer components of the electrical grid. Increased connectivity presents many benefits, including giving consumers greater ability to control their power consumption and their energy bills. The smart grid also gives distribution and transmission grid operators more visibility and control over power supply, source, quality, and costs.

Increased connectivity also presents challenges, especially in security. Because of the critical nature of the technology and the services it provides, the grid becomes a prime target for acts of terrorism and vandalism. Therefore, the transformation of traditional energy networks to smart grids requires an intrinsic security strategy to safeguard this critical infrastructure.

As a result, a security vision must include a sound design for proactive security as well as resilience in the event of a security breach. Furthermore, a cyber security plan is crucial to receiving Department of Energy grant funding for smart grid projects. The Energy Department's Office of Electric Delivery and Energy Reliability has made it clear that even grant awards that score 'A' grades on all aspects but cybersecurity may not be approved.¹

As the leader in secure data networking, Cisco has a unique perspective on how to prevent, detect, and mitigate threats to the energy grid. This paper describes Cisco's vision and activities to ensure a secure smart grid and a reliable, sustainable energy supply.

Unique Security Challenges

The smart grid is unique in several ways that present significant security challenges:

- **Scale:** The communications infrastructure necessary to support the global power grid has the potential to be larger than the Internet. As we've learned from the Internet experience, securing such a large network presents challenges such as segmentation, identity management for a large number of entities, the management of keys for data integrity and confidentiality, as well as integrating multiple wired and wireless communications mechanisms.
- **Legacy devices:** Unlike corporate IT systems that typically have a life span of three to five years, many devices in the smart grid have service lives measured in decades. Any attempt to design security for the smart grid must enable integration of legacy systems, many of which have only basic, if any, communications capabilities, and provide a long-term migration strategy to smarter devices.
- **Field locations:** The power grid contains millions of field devices, such as meters, transformers, and switches. While physical security of these field devices is an important design consideration, the fact that they are potentially vulnerable requires that network security design not rely on them for grid integrity.

¹ <http://www.washingtonpost.com/wp-dyn/content/article/2009/07/27/AR2009072702988.html>

- **A culture of “security through obscurity”:** Today’s grid security often assumes that if the location or access method of a vulnerable point isn’t widely known, it won’t be exploited. Some people believe that the smart grid data communications network will be secure if it is built with proprietary, non-routable protocols, which would make it more difficult to access than a standards-based network. In reality, vulnerabilities cannot remain hidden for any length of time. History has shown that public availability of security algorithms that are subject to peer review has increased the security of these systems. Some examples are the Advanced Encryption Standard (AES) cryptographic standard, Diffie-Hellman asymmetric encryption keys, and the Internet Engineering Task Force (IETF) IP Security (IPSec) security standard. Flaws are discovered and resolved more quickly than in proprietary systems.
- **Evolving standards and regulations:** In this early phase of smart grid implementation, vendors are implementing security controls using a variety of standard and proprietary mechanisms. This leads to poor interoperability and difficult management. Early efforts suffer from a lack of independent testing and from frequently insecure implementations. As the smart grid standards landscape matures, through efforts by the National Institute of Standards and Technology (NIST)² and others, we will see a gradual transition to a common set of security standards and testing.

Government and industry bodies are working to address smart grid security concerns by creating and updating security regulations and standards. The North American Electric Reliability Corporation (NERC) has published a set of regulations for critical infrastructure protection (CIP).³ However, these regulations are still maturing and subsequent revisions are already in process.

Other governing bodies are also participating in standards activities, although an agreed-upon set of standards is not yet final. Pursuant to the Energy Security and Independence Act of 2007 (P.L. 110–140), the U.S. Secretary of Energy has directed the NIST to publish and enforce a set of interoperability standards for emerging smart grids. NIST expects to release its draft interoperability report in September 2009.

Although smart grid security regulations and standards will continue to evolve as smart grid technology develops, utilities cannot afford to wait until standards are finalized to begin developing their smart grid implementation strategy and plan. But how should they proceed?

Smart Grid Security and the Internet Protocol

To achieve the level of interoperability and security needed for the smart grid, its secure data communications network architecture must be built using standard protocols. The standard protocol suite best suited for the smart grid is the Internet Protocol (IP).

IP made the Internet possible, but IP is not the Internet. The Internet is a public “network of networks” that use IP and the Internet architecture. It is not the only network that does so: Corporate networks are typically private networks that also use IP, but connect to the Internet only at controlled points and are often layered on top of it. Various militaries also run IP networks that do not connect to the Internet at all. The Internet will likely be used in the smart grid to provide customers with energy information on home, business, and portable devices and allow them to set configurable energy parameters, but Internet access to the smart grid will be limited to specific energy functions.

Cisco is active in guiding the energy industry toward open standards, and will consistently apply those standards in our solutions to improve manageability and security effectiveness. Nonetheless, as we plan for a long-term transition to a smarter grid, the integration of legacy devices will be a key design consideration. Devices that have serial interfaces can be adapted to integrate into a larger IP-based communications network with proper authorization and protocol management.

² National Institute of Standards and Technology. See <http://www.nist.gov/smartgrid>.

³ See <http://www.nerc.com/page.php?cid=2|20>.

Cisco's Smart Grid Security Vision

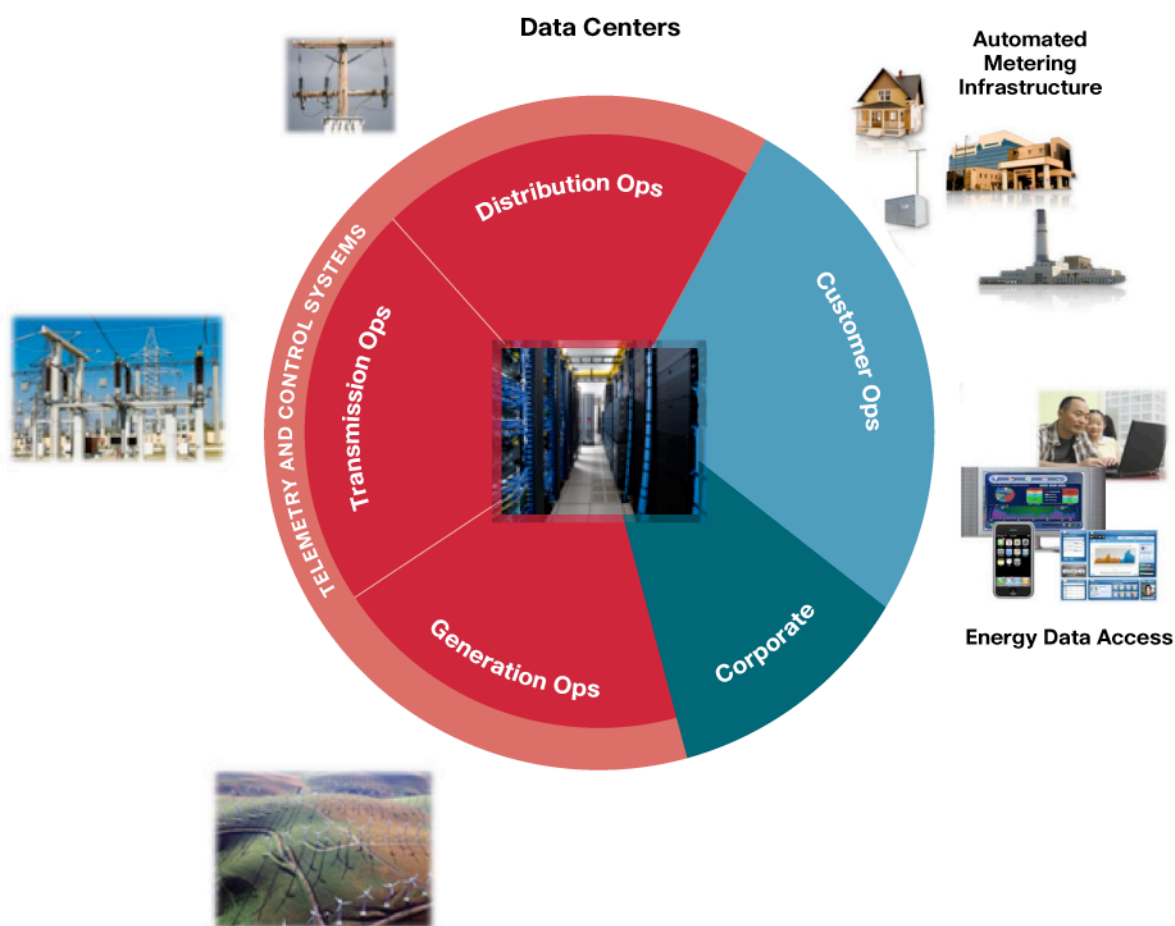
Cisco's vision for smart grid security is based on principles learned from years as the world leader in building secure data networks:

- Maximize visibility into the network environment, devices and events.
- Control network users, devices, and traffic.

These principles are detailed in Cisco's Secure Architecture for Enterprise (SAFE). Cisco applies these principles to the unique environment and demands of the smart grid to create a converged, modular security platform that provides fast response to threats and helps ensure regulatory security policy compliance while reducing operating and management expenses. The Cisco smart grid security vision takes a zone-based approach in which each security zone encompasses a discrete smart grid business function or operation. Cisco has defined three security zones to protect the major functions of the smart grid: customer operations; corporate; and telemetry and control systems (Figure 1).

These security zones follow established industry practices for delivering energy to customers, and protect assets for power generation, transmission, and distribution, as well as the "last mile" to energy consumers' premises. This zone-based model will support multiple utilities managing different parts of the grid, and provides a grid protection that is independent of topology or network transport.

Figure 1. Smart Grid Cyber Security Information Vision



Each security zone is comprised of the field devices, systems, and transmission media, as well as one or more data centers, which serve the specific operational functions of that smart grid security zone. This modular view accommodates architectures ranging from a model in which a single entity manages all grid functions to a model in which multiple entities manage different zones. Each entity defines the security policy that is active within each security zone, as well as the policy that defines the information sharing characteristics between security zones.

Each security zone implements a basic set of security features common among all the zones. These security features are central to the Cisco security solution portfolio and include:

- Identity management
- System integrity
- Secure access
- Threat protection

In addition, each security zone will implement security features specific to its business function and operations, as described below.

The Customer Operations Security Zone

The smart grid gives energy customers the tools to manage their energy consumption—and thus their energy bills—more precisely to meet their individual needs. Using smart grid technology such as Advanced Metering Infrastructure (AMI), real-time information about electricity price changes will be transmitted to smart meters, home energy controllers, or thermostats, which will then automatically adjust their own settings, and change settings on appliances—or even turn them off—according to guidelines set by the customer or “learned” by the home energy systems themselves.

The customer operations security zone contains the devices and processes that extend energy management to customers. This zone defines policies and procedures for customer energy management and demand response, load shedding, and automated meter reading. Among the systems and devices are smart meters, customer portals, and demand response systems that collect and process customer data and have unique security requirements, such as:

- **Fraud prevention.** In addition to physical meter tampering, utilities must ensure that meters are not replaced by rogue devices, and that meter data cannot be manipulated.
- **Grid integrity.** In the event that field devices are compromised, the grid must protect the “upstream” network from unauthorized commands, access to the network, and denial of service attacks.
- **Privacy.** Customer energy usage patterns can reveal personal information and vulnerabilities, such as whether an electric car is plugged into the house, or whether a family is away on vacation. Utilities must ensure that customers’ energy usage information remains private both in transit to the utility and in storage in the utility data center.

To provide this level of security, access to home systems and to the data gathered by them must be limited to authorized people and devices. To do this, customer energy management systems must be able to assure integrity of command and meter data, authenticate devices, and protect the grid from compromised devices.

The Corporate Security Zone

The corporate security zone includes all of the features and functions of the customer operations security zone plus security for IT functions vital to a business, such as email, Internet, telephony, messaging, and a wide variety of corporate applications.⁴

⁴ Learn more about enterprise security requirements at http://www.cisco.com/en/US/netso/ns170/networking_solutions_solution_segment_home.html

To meet these requirements, Cisco applies consistent security policies and across its entire product line in the smart grid to drive the industry toward open, interoperable network and security technologies, concentrating on the proven and secure IP architecture for network interoperability. Cisco's industry-leading enterprise security product portfolio is ideally suited to protect the corporate zone of the smart grid.

The Telemetry & Control Systems Security Zone

The smart grid gives utilities more tools to deliver power reliably and cost effectively. For example, utilities are installing sensors to automate distribution by monitoring and controlling the grid in near-real time. This enables them to detect faults early so they can take immediate action to isolate the fault and contain power outages. These sensors and devices—including circuit breakers, reclosers, and transformers—send grid performance information to remote terminal units (RTUs) that in turn transmit data to the utility companies' supervisory control and data acquisition (SCADA) systems to provide automatic, near-real-time electronic control of the grid. Thus monitoring and control systems are being extended from the distribution substations throughout the feeder network.

Another tool the smart grid gives utilities is automated substation maintenance. In the smart grid, the traditional substation maintenance strategy based on defined cycles is no longer effective or appropriate. With the smart grid, assets can and should be monitored continuously, and critical concerns can be identified in advance. And with new communications technologies, information about the condition of critical assets can be provided to field technicians so they can quickly address maintenance issues and fix problems. This new way of providing maintenance and troubleshooting can significantly increase the lifetime of assets and avoid expensive outages.

To secure substation automation, the smart grid must incorporate several key security features. Among these is providing protection from unauthorized access that could allow intruders to tamper with distribution devices. The smart grid security system must also ensure authentication of commands, and guarantee the integrity of telemetry data and commands, ensure data confidentiality, and protect upstream assets.

The telemetry and control systems security zone defines the processes that are used to manage the routing of energy from generation plant to consumer and the reliability of the energy delivery systems. This zone contains the data centers involved in the generation, transmission, and distribution of energy, and the intelligent end devices (IEDs) such as transformers, relays, feeder breakers, capacitors, voltage regulators, line switches, reclosers, and sensors/phasors that are used to control energy flow and ensure the reliability of the grid. This zone also contains energy substations that use SCADA systems to manage the grid. Information collected and processed in this zone supports equipment maintenance and troubleshooting, load capacity, and power re-routing in the case of outages. Because this information is crucial to the delivery of quality power to customers, the unique security requirements for this zone include:

Availability. System availability is the overarching priority of smart grid security. To maintain availability, security measures should be employed, including:

- Technician and device authorization
- Access control to network services by time of day and function for both users and devices
- Isolation, rerouting, and resilience in the event of a cyber security incident
- Protection from denial of service attacks

Data integrity. The integrity of telemetry data and control commands is critical to the proper functioning of the smart grid, and supports the availability requirement. Measures include:

- Technician and device authentication
- Computer health verification

- Integrity of telemetry data and SCADA commands
- Correlation of alarm data with other sensors to prevent false positives

Audit and confidentiality. To ensure regulatory compliance and enable forensic analysis, telemetry and control data must be collected and stored for time periods specified by regulating agencies. However, this information is very sensitive, and may reveal details that could be used to compromise the power grid. Therefore data encryption, intrusion prevention, and intrusion detection are essential.

Cisco's security vision for the telemetry and control systems zone includes rugged systems designed to ensure physical protection from elements and intruders, along with detection and troubleshooting mechanisms that will make re-routing power easy and rapid in the event of an outage, intrusion, or error.

Data Center Security and the Smart Grid

As mentioned earlier, the smart grid will capture and analyze real-time data about individual customer energy usage patterns. This will enable customers to adjust their power demands, and will enable utilities to adjust the power supply and design services to better meet customer needs. Such massive amounts of information require not only more data storage than utility companies have ever managed, but also the highest security to prevent unauthorized use and ensure safe, timely disposal in compliance with regulations.

All data centers must enable secure information sharing both within a specific data center and between data centers. For example, inter-zone communications would include information such as Internet customer portal access to energy use data, energy usage forecasting from customer operations to distribution operations for efficient routing of energy, and real-time commands issued by technicians to IEDs. On the other hand, intra-zone communications for the telemetry and control systems security zone would include information such as available power and energy use data. Information sharing among data centers has stringent security requirements, particularly because different types of data centers have different levels of security. Proper definition and enforcement of security policy ensures that appropriate access is granted, only authorized communication is granted between systems with different levels of trust, and that overall grid integrity is maintained.

Conclusion

Cisco is in a unique position to help energy organizations make the transformation to smart grids, starting with a foundation of converged IP networks and proven security principles. From a technology standpoint, the Cisco portfolio includes industry-leading networking equipment and software with integrated security capabilities that empower energy organizations to use Cisco's experience to build end-to-end, secure IP networks. The maturity, reliability, and success of these products and services can shorten the learning curve for power grid operations and allow energy companies to evolve their operations to meet developing standards and regulations.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLynX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)