Cisco Services for Securing the Smart Grid

Security has become one of the top priorities for today's electric energy industry. Identified as critical national infrastructure by most nations, utilities are under pressure to assure 24x7 reliability and availability of the power grid. In the midst of a rapidly transforming environment, utilities must meet stringent new security regulations and grid management requirements, such as the NERC CIP standard in the United States. In response, utilities are looking for ways to assess and effectively mitigate risk associated with their operations.

The Cisco® Connected Grid Services team designs proven architectures to protect the smart grid against potential threats, including accidents, human error, national disaster, and malicious attack.

Our experts work closely with utilities to:

- Analyze business priorities and associated business functions
- Assess risk to understand the effects of threats that might undermine business priorities and functions
- Review the current architecture's ability to mitigate risk and identify security gaps
- Develop an architecture to address those security gaps
- Create implementation and operations strategies

The Challenges of Securing the Grid

Securing the grid to assure reliability and availability is a challenging task. Grid operations have expanded over time, leading to a patchwork of non-interoperable control and business environments. Distributed over widely dispersed territories covering thousands of square miles, the power grid is vulnerable to:

- An aging infrastructure that threatens grid reliability
- Lack of visibility into remote locations' equipment and physical security
- Lack of information access to and from control and data centers
- Harsh environments that affect transmission and delivery equipment
- Lack of compliance with evolving security standards
- The addition of intermittent renewable energy resources to the grid

Cisco Services for Grid Security

Cisco Services work with utilities to respond to these challenges by creating a unified network architecture that combines systems, data, and facilities into a secure services framework. This comprehensive approach reduces grid vulnerability to cyber or physical attack while improving overall operating resiliency. These secure designs are based on decades of experience with creating some of the largest networks in the world.

Multiple protections built into each product and solution enable the communications network itself to serve as a security mechanism. Cisco's approach supports utilities with:

- A multilayer defense that combines a comprehensive set of Cisco Services, Cisco solutions, and partner solutions
- Extensive experience in helping utilities plan and build end-to-end architectures that include physical security, cybersecurity, compliance, intrusion detection and prevention, data center security, and security management
- Expertise in developing business strategies and architectures; understanding compliance needs; and designing, building, and operating grid physical and network security solutions

Cisco Services for Securing the Smart Grid

The process of developing, deploying, and maintaining a secure architecture for a utility proceeds through five key stages:

Use Case Security Analysis
Cisco experts conduct a security assessment of the use cases the utility intends to pass through its environment. This assessment includes a threat and risk analysis, which is used to develop a set of primary requirements. These must be fulfilled to make sure that functionality is not disrupted by typical and atypical threats within the utility environment.

Secure Architecture Development
Based on the business case analysis, the same primary requirements are used to develop an architectural blueprint designed to protect the utility system against a range of cyber and physical threats. This integrated architecture includes routing/switching as an intelligent building block that provides built-in virtualization capabilities. The architecture may also encompass:

- Segmentation design across the network
- Authentication and authorization framework
- Host security
- Redundancy and device hardening
- Physical security, including video surveillance and access control for establishing and protecting the physical security perimeter
- Unified WAN design incorporating security, resilience, and intelligence between locations and from the location to the control center
- Unified control and data center design incorporating security, resilience, and intelligence between locations and the control and data centers

Architecture Assessment, Security Posture Assessment, and Roadmap
Cisco Services conduct a gap analysis between the utility's current architecture and the recommended architecture. This phase may also include a thorough security posture assessment to achieve a deeper understanding of the current architecture and its potential security issues. The results of these analyses are combined to build a comprehensive roadmap for achieving the utility's ultimate architectural vision.

Secure Design and Deployment
A detailed technology-focused design is developed based on the architectural gap analysis. Cisco Services offer the ability to stage and test solutions in lab environments before actual deployment.

Security Optimization
Cisco's Services organization supports the utility to evolve its security system over time to meet ever-changing threats and compliance requirements. This security optimization service employs a range of expertise, tools, and methodologies to proactively evaluate and strengthen the network's ability to prevent, detect, and mitigate threats.

Benefits

Cisco Connected Grid Services deliver clear and immediate benefits to the utility, cost-effectively controlling access to critical utility assets, monitoring the network, mitigating threats, and protecting physical facilities. Our open standards-based infrastructure enables a more scalable and secure substation network design. Benefits include:

- Increased grid utilization and reliability
- Reduced vulnerability to physical attack or cyberattack
- A comprehensive framework for meeting compliance requirements
- A new platform for clean energy policy
- New models for customer engagement
- New opportunities for innovation in operations and enterprise computing

Why Cisco?

Cisco brings more than 30 years of industry networking experience to each utility industry project. Our Connected Grid Services team has the experience, expertise, and portfolio of technology solutions to improve how the energy industry serve its customers and manage daily operations. By securing disparate networks across the utility, Cisco enables utilities to manage assets more efficiently throughout the grid, optimizing business functions and simplifying operations for the future.

C45-693105-00 1111