

## Cisco Smart Grid Security Solutions Brief

### Meeting the Challenge of Smart Grid Security

Climate change, rising fuel costs, aging grid infrastructures, and new power generation technologies are driving the need for a new, more intelligent system to manage the electric grid. At the core of the smart grid transformation is the use of intelligent communication networks as the platform that enables grid instrumentation, analysis, and control of

Security based on established, open standards and regulatory compliance can help ensure the reliability and security, both physical and cyber, of the electrical power system.

utility operations from power generation to trading, to transmission and distribution, and to retail. One of the most important foundations of a smart grid is the interoperability that enables all of the required devices, technologies, applications, and agents (energy producers, consumers, and operators) to interact in the smart grid network.

Although smart grid communications can assist in transforming the energy industry, playing a critical role in maintaining high levels of reliability, performance, and manageability, they also introduce the need for an integrated security infrastructure. Many of the technologies being deployed to support smart grid projects—such as smart meters, sensors, and advanced communications networks—can increase the vulnerability of the grid to attack. Top security concerns for utilities migrating to an intelligent smart grid communications platform center on the following trends:

- Integration of distributed energy suppliers such as independent power producers, of renewable energy generation, and of distributed energy resources
- Proliferation of digital devices to enable automation, management, and control
- Regulatory mandates to comply with standards for critical infrastructure protection
- Migration to enhanced systems for outage management, distribution automation, condition-based maintenance, load forecasting, and advanced metering infrastructure
- Demand for new levels of customer service and energy management

This development of a diverse set of networks to support the integration of microgrids, open-access energy competition, and the use of network-controlled devices is driving the need for a converged security infrastructure for all participants in the smart grid, including utilities, commercial businesses, consumers, and energy service providers. Securing the assets of electric power delivery systems, from the control center to the substation, to the feeders and even to customer meters, requires an end-to-end security infrastructure that protects the myriad of communication assets (control center-based SCADA, RTUS, PLCs, power meters, digital relays, and bay controls) used to operate, monitor, and control power flow and measurement.

### Securing Grid Operations and Assets

Cisco combines long experience and deep domain knowledge in utility control systems with expertise in physical security and cybersecurity to help protect critical public infrastructure.

Cisco believes that modernization of the energy infrastructure requires a comprehensive security architecture that offers improved integration of diverse digital devices, increased use of sensors, and layers of

both physical security and cybersecurity management integrated across all operational aspects of the grid. Cisco® Grid Security solutions deliver an integrated, converged approach to security that provides critical infrastructure-grade security to grid systems, data, and assets; monitors the network while mitigating threats; and secures utility operational facilities.

By converging physical and logical security into an integrated security infrastructure, the Cisco Smart Grid solution enhances overall security while simultaneously making security easier and less costly to manage. This comprehensive and converged approach yields the following benefits:

- Reduced system vulnerability to physical attack or cyberattack
- Operating resiliency against security disruptions
- Secure access and data privacy for smart grid information
- Optimized network reliability, computing, and operational support for grid communications
- Establishment of a framework for compliance

Cisco helps utilities meet their smart grid security needs with:

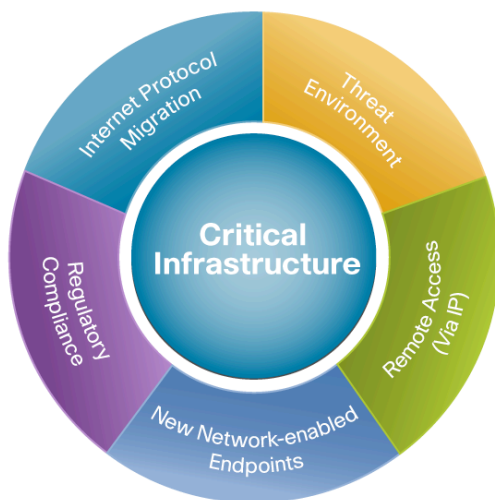
- A **solutions approach** to security, combining a comprehensive set of Cisco technologies, solutions, services, and partners to help utilities prevent, detect, and mitigate threats to the energy grid
- Deep experience helping utilities architect and build **end-to-end security architectures** that include physical security, cybersecurity, intrusion detection and prevention, data center security, and security management and control
- **Comprehensive lifecycle professional services** providing business strategy and requirements development; deep understanding of security technology solutions; and the ability to design, build, and operate grid physical and network security solutions

Cisco is uniquely positioned to help utilities make the transformation to smart grids by building end-to-end, secure communications networks that allow utilities to secure power grid operations with enhanced physical security and cybersecurity that meet developing standards and regulations through the use of Cisco security technologies, solutions, services, and ecosystem partners.

### Cisco Grid Security Solutions

Cisco has developed a set of grid security solutions (see Figure 1) that provide a secure communications platform for both business and control operations in support of generation networks, including bulk generation plants and renewable plant networks, as well as transmission and distribution networks supporting control centers, substations, and neighborhood area networks. This includes extending IT security to control centers and data centers that host critical operational applications, systems, and data while simultaneously complying with regulatory requirements.

**Figure 1.** Cisco Grid Security Solution



The Cisco Grid Security solutions include:

- Identity Management and Access Control
- Threat Defense
- Data Center Security
- WAN Security
- Security Monitoring and Management
- Physical Safety and Security
- Generation Plant Security
- Substation Security
- Utility Regulatory Compliance
- Cisco Services to plan, build, and run grid security solutions

## Identity Management and Access Control

Cisco's Identity Management solution is customized to meet the needs of grid operations and includes authentication and access control components. Authentication makes sure that access to control center, transmission, and distribution networks is granted only to authenticated users, groups, and services. The solution eliminates the arduous task of manually entering and changing authentication credentials for guest users and includes provisions for clientless authentication schemes and authentication for wireless users. Access control provides granular local and remote access to users and applications into diverse control center, data center, and substation networks.

The components of the Cisco Identity Management and Access Control solution include:

- Cisco Secure ACS: Provides centralized network identity and access control
- Cisco Network Admission Control (NAC): Enforces network security policies on devices seeking network access
- Cisco Identity-Based Network Services (IBNS): Offers authentication, access control, and user policies to secure network connectivity and resources
- Customized signatures for SCADA protocol firewalls: Provides access control at multiple levels for defense in depth

## Threat Defense

A threat defense solution is required to protect against vulnerabilities because it is often difficult to anticipate what form a new threat might take. Care should be taken to apply security principles broadly across the entire grid infrastructure to build an effective, layered defense. Cisco's Threat Defense solution for grid Security includes:

Proven network security systems will allow grid components to detect intrusion attempts and provide real-time monitoring and management of cybersecurity events.

- Network segmentation and access control to protect against denial-of-service (DoS) attacks
- Cisco Adaptive Security Appliances (ASAs): Integrates firewall, unified communications security, VPN, intrusion prevention system (IPS), and content security services
- Cisco IOS<sup>®</sup> Software Security: Offers a suite of security technologies including firewall, VPN, IPS, and content security on integrated services routers and WAN aggregation routers
- Cisco IPS: Delivers intelligent threat detection and protection to identify external threats attempting to enter the infrastructure as well as stop any attempts at internal propagation

## Data Center Security

The evolution of smart grid operations brings with it an immediate need to revisit utilities overarching information management strategy. The integration of operational computing and control systems with the utility's business systems is more critical today than ever before. Grid operations support systems (OSSs) will experience highly accelerated growth in terms of information storage, data retrieval, and application/systems interdependencies with the advent of smart grid communication. Additionally, regulatory requirements for disaster recovery require regular testing of the integrity and performance of backup control centers.

Securing information generated in a smart grid network requires that data center storage and access are secured and that diagnostics, telemetry, and control commands of intelligent devices in the utility control network are authenticated and protected.

This increased complexity of electrical power grid operations requires that a highly scalable, resilient, and secure data center network foundation is in place. Cisco's [Data Center Security](#) solution is the heart of securing utility operations. Using consolidation and virtualization technologies, Cisco Data Center solutions provide a robust set of tools that enable organizations to turn network, compute, and storage resources into a secure,

shared pool of resources that protects application and data integrity, secures communications between advanced business processes and applications within the utility, and secures connectivity to external resources such as providers of renewable energy.

The Cisco Data Center Security solution provides a comprehensive set of tools helping ensure security and privacy for smart grid storage, systems, and data and is based on the following design principles:

- A fully redundant, resilient data center design with no single point of failure
- [Server farm firewalls](#) to filter server farm ingress and egress traffic
- Data center firewalls to protect servers and secure segmentation of application traffic
- Cisco IPS appliances, IDS devices, and router and switch-based telemetry for threat detection, prevention, and mitigation
- Cisco ASAs providing integrated firewall, unified communication security, VPN, IPS, and content security services
- Secure Layer 2 connectivity, including access control lists (ACLs), Cisco Integrated Security Features (CISF), port security, netflow, dynamic ARP inspection, IP source guard, Encapsulated Remote Switched Port Analyzer (ERSPAN) QoS, and control-plane policing (CoPP)
- Server load balancing to mask servers and applications
- Cisco ACE Web Application Firewall: Combines deep web application analysis with Extensible Markup Language (XML) inspection to mitigate attacks based on cross-site scripting (XSS), HTTP, Structured Query Language (SQL), and XML
- Security management using Cisco Security Agent (CSA) host intrusion prevention system, firewalls, IPS, netflow, and syslog

Cisco [Services for the Data Center](#) help utilities build in security best practices, standards, and compliance in data center environments, including:

- **Data Center Facilities Assessment:** Includes a site security assessment to improve physical infrastructure security
- **Data Center Virtualization Assessment:** Analyzes security requirements and provides recommendations to improve data center security
- **Data Center Virtualization Planning and Design:** Provides a detailed design and implementation plan for virtualized data center environment, including security requirements for network, storage, and compute resources.

## Wide Area Network Security

Securing the wide area network (WAN) is critical since the WAN connects diverse utility networks, including field area networks, transmission and distribution (T&D) networks, service provider networks, and control center and data center networks for utility operations. The WAN network must be designed to help ensure the availability, security, and performance of all users, devices, and applications across utility networks and is based on the following design principles:

- Core network design for secure segmentation of traffic
- Cisco IOS Software Security: Security technologies (firewall, VPN, IPS, content security) on integrated services routers and WAN aggregation routers
- Secure WAN edge connectivity: VPN for traffic isolation (Dynamic Multipoint VPN [DMVPN]), Advanced Encryption Standard (AES) for strong encryption, and Public Key Infrastructure (PKI)

- Secure WAN edge protection: Edge QoS and rate limiting, uRPF, RFC-2827 antispoofing filtering, infrastructure protection ACLs, and routing security
- Secure transport of data to the data center, control center, and meter data center, including backhaul communications
- Identity management and access control of users and devices into each network segment

## Security Management and Monitoring

As an increasing number of grid assets used to generate and transmit electricity—such as substations, transformers, and power lines—are being connected to data networks, the mandate for enhancing security and operational resilience has compounded. NERC-CIP requires that automated tools and processes must be implemented to monitor security events.

Cisco's Security Management and Monitoring solution provides a broad set of capabilities for managing and monitoring grid assets, including:

- **CiscoWorks Network Compliance Manager (NCM):** Helps identify, manage, and counter security threats by managing configuration and software changes throughout a multivendor network infrastructure. and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements
- **Cisco Security Manager:** Enables consistent deployment and enforcement of security policies across Cisco routers, security appliances, and switch security capabilities.
- **Cisco LAN Management System (LMS):** Assists in disaster recovery and NERC CIP compliance (CIP 009) by configuration and image backups and easy rollback of configurations.

## Physical Security

Many of the assets used to generate and transmit electricity are vulnerable to terrorist attacks and natural disasters. Cisco's [Physical Security solutions](#) provide broad network-centric capabilities in video surveillance, IP cameras, and electronic access control along with technology that converges voice, data, and physical security in one integrated appliance for incident management across diverse media.

The components of Cisco's Physical Security solution include:

- **Electronic Access Control:** Cisco IP Access Gateways and Physical Security Access Manager restrict access to locations identified as critical infrastructure and provide the logging required by NERC-CIP for personnel access.
- **Video Surveillance:** Cisco offers an extensive suite of video surveillance solutions (IP cameras, video storage, and video analytics solutions) that can be deployed in utility control centers, as well as in multiple-site and remote-site facilities, including support for video across LAN/WAN to wireless connections and from indoor to harsh outdoor or mobile environments.
- **Communication, Collaboration, and Notification:** Cisco's IP Interoperability and Collaboration System (IPICS) solution enables data, voice, and video communications across a diverse set of devices and communication technology such as radios, voice over IP (VoIP) phone, land lines, and PCs.

## Generation Plant Security

An intelligent smart grid will allow utilities to integrate, manage, and control diverse energy sources for grid-load balancing so that energy deficits can be offset when conventional power plant output is insufficient. To achieve this, utilities networks must be designed to secure communications between conventional generation plants and to renewable plants that are utility controlled or owned by independent power producers. Cisco's Generation Plant Security solutions are based on the following design principles:

- Network segmentation (Layer 2 and Layer 3) for generation units and the generation site for zone and supervisory control
- Secure DMZ for generation plant management and security for operational functions such as patch management
- Secure local and remote network access to generation plants
- Centralized logging and event correlation at the generation plant
- Centralized authentication and authorization server for user access and authentication
- Security management for policy control across generation plants
- Physical security, including video surveillance and access control

### Substation Security

Substations are the core building blocks of utility power delivery networks. They provide connectivity to field area networks, metering networks, home area networks at distribution substations, and wide area measurement systems (WAMSs). Secure transport of data from substations to their multiple destinations poses significant challenges to the utility. Cisco's Substation Security solution is based on the following design principles:

- Unified WAN design incorporating security, resilience, and intelligence between substations and from the substation to the control center
- Router/firewall for establishing and protecting the electronic security perimeter (ESP)
- Integrated services routers (ISR) for integrated routing, switching, and security inside the ESP
- IPS module for the router/firewall for malware detection and prevention
- Security at the access layer for access within substations
- Identity management and access control for ESP user and device entry
- Protocol-based signatures for command-based firewalls and logging into the ESP
- Physical security, including video surveillance and access control for establishing and protecting the physical security perimeter

### Business Energy Management Security

The [Cisco Network Building Mediator](#) can access, measure, and help manage energy use by energy-consuming systems within commercial buildings. Built on a standards-based, open network platform that collects data from disparate building, IT, energy supply, and energy-consuming devices, the Cisco Network Building Mediator enables utilities to better predict and meet energy demand, optimize generation load, and better manage alternate sources of energy such as solar power.

Integration of the Cisco Building Mediator into an overall business energy management solution requires secure interoperability between building controllers and utility control networks, including connection of existing building automation equipment to the IP communications network. It also requires that robust security solutions are embedded to secure, high-quality delivery of integrated building and IT services.

The Cisco Business Energy Management Security solution is based on the following design principles:

- Hardened Cisco Network Building Mediator platform
- Isolation of building energy management systems from the corporate systems
- Secure pass through of building management protocols over the WAN
- Access control for building energy applications accessing end devices

- Secure communications via certificate encryption
- Identity management of users of building energy management networks

Cisco's Business Energy Management solution is delivered through a set of professional services that define utility smart grid requirements, develop customized building energy management solutions to meet these requirements, coordinate the deployment and integration of the solution, and then deliver support through ongoing optimization services.

## Utility Compliance

The network plays a governing role in operations risk and compliance management. Network security controls must be in place to monitor and report on business processes and the flow of information. If these controls are not properly implemented, the availability, integrity, and confidentiality of data and business-critical processes might be compromised. Securing utility networks for compliance not only helps utilities avoid potential penalties, but also increases consumer confidence and speeds adoption of smart technologies.

Cisco utility compliance solutions help utilities maintain compliance with government regulations while keeping investment costs low.

Compliance with NERC CIP 002-009 standards requires comprehensive cybersecurity solutions (segmentation, authentication, authorization, monitoring, logging, and training) and physical security solutions (access control and video surveillance). The Cisco Utility Compliance solution is based on the following design principles:

- Cisco's integrated services routers with integrated Cisco IOS firewall and VPN security and the IPS network module deployed inside substations (CIP 005)
- Cisco integrated services routers (ISR) at the control center with Multiprotocol Label Switching (MPLS ) and DMVPN support for segmentation and encryption at the core (CIP 002)
- Cisco Secure MARS at the control center for monitoring and logging of events for Cisco and third-party network devices (CIP 005)
- Cisco ISR with Cisco Secure Access Control Server (ACS) and Cisco Security Manager at the control center for user identity management and access control (CIP 003)
- Cisco IP-based access control and video surveillance solutions (CIP 006)

Cisco Services provide compliance assessment, design, deployment, and training services to help identify network compliance regulatory gaps, design a security solution that closes compliance gaps, and focus IT staff efforts on actionable security control remediation. Cisco Services for Utility Compliance include:

- NERC CIP Assessment: Assessment service to assess the gaps in the network for NERC CIP compliancy (CIP 007)
- NERC CIP Design and Deployment Services: Design services to develop and implement the corresponding security measures for NERC CIP compliance (CIP 007) and provide training on network device security (CIP 004)

## Cisco Grid Security Professional Services

Cisco Services for Grid Security offer a comprehensive approach to planning, designing, implementing, operating, and optimizing an integrated, utility security solution.

Cisco Services, with our ecosystem of partners, can help plan, build, and run networks that meet smart grid requirements for regulatory compliance and protection from cybersecurity and physical security threats. Cisco's Grid

Security Services are based on industry best practices and Cisco's proven methodology for planning, building, and running end-to-end security infrastructures that integrate Cisco and partner solutions. Cisco Services for Smart Grid Security include the following services:

- **Security Business Strategy and Architecture:** Prepare a multiyear security infrastructure transformation plan, including future-state business models, high-level designs, roadmaps, and recommendations on how to successfully manage the transformation
- **Security Assessments:** Assess the security posture of control system environments, perform physical site security assessments, evaluate the overall security architecture, and provide detailed recommendations to help meet NERC-CIP compliance requirements
- **Utility Compliance:** Improve risk management and satisfy compliance needs with NERC-CIP assessment, design, and deployment services
- **Physical Safety and Security:** Define overall physical security requirements, deliver site assessments, develop the future-state architectures, coordinate the deployment and integration of the solution, and deliver ongoing support through managed services
- **Data Center Security:** Make sure of data center operational efficiency, performance, and security with site security assessments, data center security architecture development, and detailed design and implementation services for improved data center security
- **Transmission and Distribution Security:** Increase the effectiveness of T&D security solutions while controlling integration costs with generation plant/substation requirements definition, future-state plant and substation security architecture development, and T&D security solution deployment services
- **Business Energy Management Security:** Securely integrate the Cisco Network Building Mediator into business energy management solutions with comprehensive strategy, architecture, design, and deployment services
- **Security Deployment:** Speed deployment of integrated security solutions with plan, design, and implementation services
- **Security Optimization:** Maintain a trusted, resilient security infrastructure with ongoing assessments, technology planning, and architecture reviews

Cisco's solutions-based approach and deep security expertise provide the foundation for solving the most complex grid security problems, enabling the secure, intelligent communications network that is required to provide utilities with near-real-time information to manage the entire electrical grid as an integrated system, actively responding to changes in power demand and renewable generation.



**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](http://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, iLX, 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)