Securing Critical Infrastructure: A Guide to Smart Grid Security

Today's electrical utilities face the demands of a rapidly transforming industry, including increasingly stringent security regulations and power grid management requirements. On top of this, they must also assure 24x7 reliability and availability of power. To meet these needs, utilities are increasingly turning to smart grid technologies, which in turn introduce another set of challenges: the need for visibility and security controls.

When building out a smart grid, electrical utilities must actively address security concerns. Security through obscurity is not going to cut it when it comes to protecting critical infrastructure. Its reliance on design or implementation secrecy as the main method of providing security actually makes the grid more vulnerable. A connected grid with a thoughtful defense-in-depth approach to connectivity, operations, and management is best practice.

This paper provides a guide to smart grid security – read on to learn more.

What is a smart grid?

A smart grid refers to an electrical power grid that's integrated with digital technology and a two-way communication network. The smart grid incorporates controls, computers, automation, and other technologies and equipment, which work with the grid to respond to changes in power consumption.

Benefits of a smart grid

- More efficient transmission of electricity
- Quicker restoration after power disturbances
- Improved reliability and safety via connected assets
- Reduced operations and management costs
- Lower power costs for consumers

The evolution of the power grid

The dynamic nature of power is forcing the electric grid to evolve. In the past, electricity flowed from the generator, to the grid, to hardware, to users. Utilities could easily plan for generation and distribution and look at past consumption trends to reasonably predict spikes in demand to ensure reliability and availability.

With the trend toward renewable energy, the power flow has fundamentally changed – and continues to do so. Power is now flowing in the opposite direction; consumers are generating power and sending it back to the grid. The dynamic nature of consumption is putting new stress on the grid, and balancing consumption and generation is becoming much more complex. If consumption and generation are not balanced, the grid becomes unreliable.

Utilities need better visibility into the grid. They need to know how much power is being generated, and how much is actually being consumed. Power companies can then make real-time, data-driven decisions to make the grid reliable and efficient. That's where the smart grid comes in.

A smart grid refers to an electrical power grid that's integrated with digital technology and a two-way communication network. The smart grid incorporates controls, computers, automation, and other technologies and equipment, which work with the grid to respond to changes in power consumption.

The smart grid offers a number of benefits for both power companies and their customers, such as a more efficient transmission of electricity as well as quicker restoration after power disturbances. The smart grid also improves reliability and safety of the electric transmission and distribution grid via connected assets. Utilities benefit from reduced operations and management costs, which in turn means lower power costs for consumers. The smart grid also integrates with customer-owned power generation systems, including renewable energy systems.

Smart grid security challenges

Of course, nothing is foolproof – smart grid included. Connecting critical infrastructure to a communication network increases cybersecurity risk. An attacker can gain access to the control network via the corporate network using credentials stolen or provided by an authorized user. Or, an attacker can access a control center LAN and from there gain visibility and even access to hundreds of remote terminal units. Multiple entry points require layered controls to provide defense in depth.

Security incidents range from non-targeted attacks like user errors or malware and natural disasters to targeted cyberattacks, like those described above. Threat groups such as Thrip and Triton have created a cyber warfare battleground and are vested in compromising operational and industrial control systems (Symantec). According to Accenture, the top four cybercrime consequences are information loss, business disruption, revenue loss, and equipment damages – in that order.

3 stakeholders in smart grid security

1. Operational technology (OT)
2. The IT department
3. The Security Operation Center (SOC)

To successfully secure the grid, all three parties must work together. Each stakeholder possesses institutional knowledge that is required for the other to achieve their objectives: operations understands the industrial environment – the devices, their protocols, and the business processes, IT understands the IP network, and the SOC understands threats and vulnerabilities.

Nevertheless, power utilities are required to maintain compliance with regulatory requirements, particularly NERC-CIP (North American Electric Reliability Corporation-Critical Infrastructure Protection) and EU NIS (European Union Network and Information Security Directive). These requirements range from critical cyber asset identification and segmentation, zone segregation, remote access, and malware detection and mitigation, to security practices and processes.

Looking for guidance on applying Cisco security solutions to enable NERC-CIP? Review the table at the end of this paper.

Securing the grid to assure reliability and availability is no small task. Grid operations have expanded over time. A patchwork of non-interoperable control and business environments includes aging infrastructure that poses a threat to grid reliability. Assets have been added over multiple decades, some of which have fallen off of inventory lists and yet continue to operate. In addition, harsh environments affect transmission and delivery equipment.

The scale of utility grids also poses a challenge. Grids are distributed over widely dispersed territories covering thousands of square miles. Substations require monitoring, but sites are unattended, and space is scarce. Operators lack visibility into remote locations' equipment and physical security, as well as access to information flowing to and from control and data centers.

And then there are internal operational issues. Three stakeholders are typically vested in smart grid security: 1) operational technology (OT), 2) the IT department, and 3) the Security Operation Center (SOC). OT is responsible for ensuring that industrial processes keep running. Their objective is to reduce downtime with operational insights that help track activities in the industrial process. OT wants more efficiency, more predictability, and more scalability. To achieve these outcomes, the network must be secure, and OT requires visibility to better understand what's on the network and how devices are operating.

IT is responsible for implementing and managing the security infrastructure. A traditional security solution requires security appliances deployed throughout the environment, an ever-growing SPAN collection network, or a combination of the two. With these types of solutions, the total cost of ownership (TCO) increases as the environment grows. Not only does the organization need to invest in more appliances and a SPAN network to support the additional traffic, but it also incurs additional operational costs. IT simply doesn't have the resources to support a sprawling security infrastructure in the OT environment while maintaining the IT environment.

Meanwhile, the SOC's number one priority is to protect the business against threats using the strongest suite of industrial application-aware integrated security solutions. The SOC wants visibility into the OT environment so that it can see the assets, threats, and vulnerabilities as they relate to the whole organization. This context is critical to understanding how to write security policies to best protect those assets. Simply quarantining a compromised

Four steps to secure the grid

1. Asset discovery
2. Network segmentation
3. Live threat detection
4. Integrated IT/OT SOC

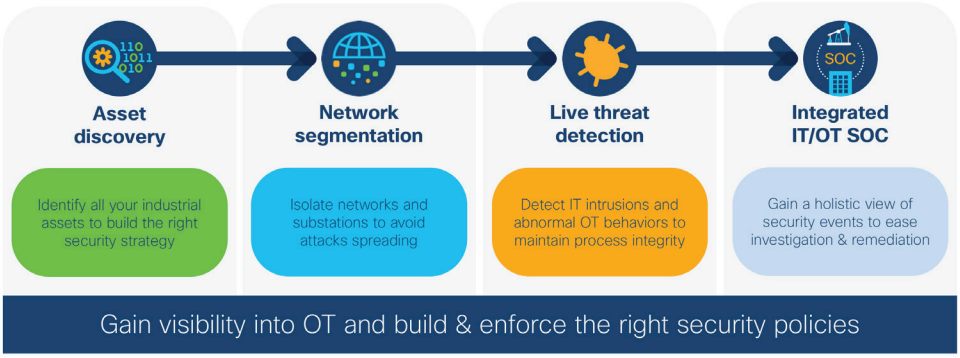
To address challenges and effectively secure the grid, leverage these four steps. While it's a journey, there is no defined beginning or end. It's an iterative process that requires continual adjustments – the most important thing is to start wherever you happen to be today.

asset to prevent an attack from spreading through the network can cause an entire process to come to a grinding halt due to the interdependency of the systems in the operational environment.

To successfully secure the grid, all three parties must work together. Each stakeholder possesses institutional knowledge that is required for the other to achieve their objectives. Operations understands the industrial environment – the devices, their protocols, and the business processes. IT understands the IP network, and the SOC understands threats and vulnerabilities. OT, IT, and the SOC must work together effectively to achieve a common goal: securing the smart grid.

The four-step journey to secure the grid

Securing the modern smart grid doesn't have to be as complex as it seems. Organizations can address the concerns of all the vested parties while implementing the controls needed to reduce risk with a simple four-step journey.



The four-step journey can begin with either asset discovery or network segmentation. It's not as important where you start as much as it is that you fully address each step. That may mean going back to a previous step.

For many power companies, the journey begins with asset discovery. Utility grids grow over many decades, and organizations rarely have full visibility into the assets on the OT network. In order to build and enforce the right security policies, you need to know what devices are on the network, how they communicate, and what devices they are communicating to, so this is a logical first step. The solution you use for asset discovery must understand grid protocols you use, such as IEC 101/104, IEC 61850, GOOSE, SV, MMS, Modbus, DNP3, etc.

Alternatively, organizations may begin with network segmentation. This is the practice of isolating portions of the network to prevent attacks from spreading throughout the environment by using firewalls designed to meet the constraints of a power grid network: a ruggedized enclosure that can be deployed in harsh industrial environment, support for challenging electromagnetic conditions, understanding of grid protocols, ability to be managed remotely, etc.

Ready to get started?

Learn more

Contact us

Organizations that start here and then conduct an asset discovery often find that their findings warrant another level of segmentation – micro-segmentation. You may want to segment off applications or partners that talk between the process bus and the station bus, for example. Or there may be multiple iterations of segments of the process bus and station bus depending on multicast traffic and who they talk to.

Once the network is adequately segmented and an asset discovery has been completed, the next step is implementing live threat detection. Smart grid processes tend to be stable and unchanging, as reflected by a baseline assessment of the network traffic (often included as part of an asset discovery). With this baseline, it's possible to identify anomalies that likely indicate suspicious activity. You can detect unusual access and traffic to OT systems, identify configuration changes, and block malicious traffic, for example.

The last step is integrating the data from the previous steps with the tools used by the Security Operations Center (SOC) to provide a holistic view of security events. With this end-to-end view, security professionals can more quickly and effectively investigate and remediate OT threats.

How Cisco can help

At Cisco, we've simplified the four steps above with integrated network and security solutions that provide defense in depth. These can be implemented with the help of the Cisco Grid Security CVD together with Cisco Cyber Vision and the ISA3000 Industrial Security Appliance. The Cisco Validated Design (CVD) is a blueprint for an integrated security architecture designed to help reduce risk and minimize the burden of regulatory compliance. The CVD aims to simplify implementation and lower operating costs for utilities while providing comprehensive protection through defense in depth.

Cisco Cyber Vision brings IT and OT together in partnership and provides best-of-breed IT security practices with all the requirements wrapped around the OT environment. The holistic security platform provides a detailed map of the protocols, end devices, and hosts in the OT environment, including where they talk and who they talk to on a frequent basis. Cyber Vision also provides 24/7 live threat detection and integrates into the SOC. Its integration and centralized management significantly reduce operational costs, time, and exposure to the utility as a whole, key benefits of one system versus integrating numerous point products from multiple vendors.

Implementing defense in depth to secure the smart grid can feel like a monumental task – but it doesn't have to be. Cisco brings network security and industry experience together to help electrical utilities make the transition to a secure smart grid. If you'd like to learn more, watch the webinar "Building a Modern Grid Security Architecture" or contact us.

Looking for guidance on applying Cisco security solutions to enable NERC-CIP? Review the table to the right.

Appendix

NERC-CIP Compliance & Solution Mapping

Requirements	Summary	Solution Coverage	Solution Mapping
CIP-002-5.1a	Cyber Security – Critical Cyber Asset Identification	✔	Cisco Cyber Vision Cisco Stealthwatch
CIP-003-8	Cyber Security – Security Management Controls	✔	ISA3000 & FMC Cisco ISE
CIP-005-5	Cyber Security – Electronic Security Perimeter(s)	✔	ISA3000 IR800 & IR1101 CGR2010 IE4000 Switches IE5000 Switches
CIP-006-6	Cyber Security – Physical Security of Critical Cyber Assets	✔	IoT Threat Defense and Grid Security Architecture
CIP-007-6	Cyber Security – Systems Security Management	✔	FMC, ISE
CIP-008-5	Cyber Security – Incident Reporting and Response Plan	✔	Cisco Cyber Vision, ISE, FMC
CIP-010-2	Cyber Security – Configuration Change Management and Vulnerability Assessments	✔	Cisco FMC, Cisco Cyber Vision, Stealthwatch, ISE
CIP-011-2	Cyber Security – Information Protection	✔	Segmentation with ISA3000, Encryption, TrustSEC
CIP-013-1	Supply Chain Management	✔	IEC 62443-4-1 & 62443-4-2 Certifications
CIP-014-2	Physical Security	✔	Meraki MV72 Outdoor Camera & Analytics