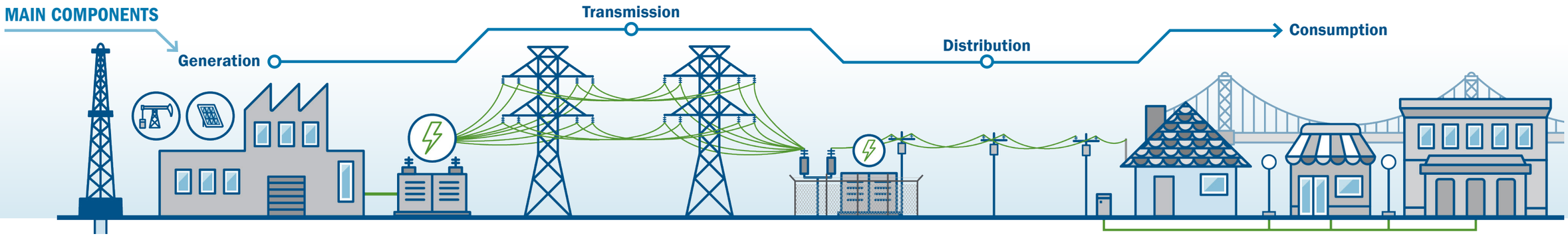
SECTOR SPOTLIGHT: **Cyber-Physical Security Considerations for the Electricity Sub-Sector**

The Nation's electricity grid could be vulnerable to increasing cyber threats that have physical consequences. New vectors for a disruptive attack on the Nation's grid and operations are emerging as monitoring and control technologies and connected devices become further integrated at the industrial and consumer levels.



AREAS OF RISK

CYBER:
Cybersecurity is an evolving security challenge for the electricity sub-sector. Cyberattacks pose a persistent threat to the electricity sub-sector and can cause severe physical and economic harm. Hackers can disrupt operations through ransomware attacks or by exploiting virtual private networks and gaining access to control systems responsible for critical operational components, such as tap changers on transformers. Malicious actors may continue to use cyber activity to bypass physical security measures.

PHYSICAL:
Physical security requirements for the electricity sub-sector are a complex challenge. For example, the diverse and disparate network of outdoor sub-stations are vulnerable to a number of physical attacks. Trespassers can damage transformers and compromise on-site control systems using firearms, explosives, and motor vehicles. Unauthorized persons are also increasingly using small Unmanned Aircraft Systems to bypass traditional security measures to conduct surveillance, damage transmission lines, and execute other nefarious actions.

SUPPLY CHAIN:
Managing the security and quality control of component acquisition is vital for the electricity sub-sector. A single compromised manufacturer or poorly secured component for Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), or software management systems, when broadly distributed across the electricity sub-sector, could compromise utility systems. Additionally, attacks on the sub-sector's supply chain for critical component manufacturers could delay the acquisition of key operational components.

PERIPHERAL DEVICES:
Electricity sub-sector operators are increasingly integrating Industrial Internet of Things (IIoT) devices with ICS to help monitor, regulate, and manage operating environments. These connected devices pose many of the same risks to enterprise security as traditional ICS. Inherent risks of IIoT devices include vulnerabilities in design, manufacturing, implementation, configuration, and disposal. For example, an IIoT device using outdated or unpatched software or firmware could be at greater risk of compromise and used to infiltrate enterprise networks, systems, and data stored in the cloud.

BEST PRACTICES FOR SECURING THE ELECTRICITY SUB-SECTOR

Protect Networks:
- Identify, minimize, and secure all network connections to ICS assets.
- Secure ICS and supporting systems by disabling unnecessary services, ports, and protocols. Enable security features and implement robust configuration management practices.
- Continuously monitor facility networks, applications, and other ICS and SCADA software systems.
- Develop facility-wide cybersecurity standards and implement cybersecurity best practices such as multi-factor authentication for system access. Regularly check, test, and implement ICS security patches.

Secure Vulnerable Infrastructure:
Develop a risk management framework to better understand how to secure vulnerable infrastructure. This framework can identify, analyze, and communicate risk. It can further instruct users on accepting, avoiding, transferring, or controlling risk to an acceptable level at an acceptable cost. The framework should do the following:[1]

- Assess the threats that are most likely to cause significant damage to components and operations.
- Prioritize vulnerability reduction efforts.
- Address physical features or operational attributes that make infrastructure elements open to exploitation.
- Mitigate the potential consequences of incidents proactively or prepare to mitigate them effectively if they do occur.

Formalize Collaboration across Organizational Security Functions:
Implement an integrated approach to security that aligns cybersecurity and physical security teams with grid operators. Cross train security personnel to enable a holistic understanding of cyber-physical threats and their impacts to grid operations and consider implementing an Insider Threat Mitigation Program. This collaboration can ensure personnel have the knowledge and tools to rapidly identify and respond to an incident with cross-sector impacts. See CISA's Cybersecurity and Physical Security Convergence Guide, which provides a framework for establishing formal collaboration between cybersecurity and physical security teams.

Update Outdated Infrastructure and Technology:
Invest in improvements to infrastructure and operational technology (OT) that are critical to daily operations. When installing new OT systems that are connected to information technology (IT) networks, ensure both systems can be readily secured and updated. Understand how OT is interacting with and connected to enterprise networks. Identify, logically isolate, and consider how obsolete or orphaned equipment is utilized in your environment and ensure risk management principles are applied.

Assess the Supply Chain:
Coordinate with individuals within the organization who engage in supply acquisition and management of security and compliance to ensure effective supply chain management practices. Establish protocols to assess already procured hardware and software components to understand which are used for critical functions and what systems have remote access capabilities to these systems. Consider how information and communications technology Supply Chain Risk Management (SCRM) and SCRM essentials integrate into each component to identify risks and vulnerabilities associated with the availability, integrity, and confidentiality of your ICS.

Secure Connected Devices:
Conduct an inventory of IIoT devices, understand how they communicate and link to the network, and disable any unnecessary internet connections, ports, and devices. Ensure connected devices connect only to intended systems. Separate the network supporting IIoT devices from the main IT and OT networks. Consider whether the IIoT device for acquisition supports software updates or security patches. Educate system administrators on the importance of cybersecurity and integrator/vendor collaboration in a connected IIoT environment.

1. CISA, A Guide to Critical Infrastructure Security and Resilience (November 2019), https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience.

SECTOR SPOTLIGHT: **Cyber-Physical Security Considerations for the Electricity Sub-Sector**

MAINTAINING RESILIENCY

REPORT:

Adhere to industry reporting requirements and establish internal processes for voluntary reporting of incidents and intrusions to the proper authorities. Leverage available tools, such as CISA's cyber incident reporting mechanism. Timely reporting enables rapid dissemination of actionable intelligence to sector partners and stakeholders, resulting in greater visibility of industry-wide threats. It creates a common operating picture among industry security stakeholders to facilitate the deployment of detective and preventative technologies that minimize the impacts of identified threats. Incident reporting also informs the process for developing threat-based products and initiatives and supports information sharing efforts that connect public and private sector partners with each other and with resources to help identify, prevent, mitigate, and recover from cyber incidents.

ASSESS:

Conduct periodic, detailed assessments of cyber and physical components to identify dependencies and interdependencies. Understand current threats and known exploited vulnerabilities. Finally, determine potential impacts of a successful cyber or physical attack. These assessments help stakeholders inform risk management plans to analyze threats to, vulnerabilities of, and consequences to critical infrastructure.

COLLABORATE:

Connect with law enforcement and federal, state, local, tribal, and territorial partners to stay informed of the current threat landscape. Collaborate with these partners to understand the layers of defense that should be adopted, develop security plans, and understand the latest tactics, techniques, and procedures used by adversaries. Additionally, communicate with operators of independent critical functions and resources to understand the cascading impacts of a cyber or physical attack.

PLAN FOR CONTINGENCIES:

Develop primary, alternate, contingency, and emergency plans to mitigate the most severe effects of prolonged grid disruptions, including the ability to operate power systems manually without the aid of control systems in the event of a compromise. Ensure redundancies of critical components and data systems to prevent single points of failure that could produce catastrophic results. Conduct exercises to provide personnel with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures.

TOOLS

CISA Regional Advisors:

CISA collaborates with sector partners and stakeholders through a robust network of subject matter experts including Protective Security Advisors, Cybersecurity Advisors, and Interagency Security Committee Regional Advisors. These on-the-ground resources connect with organizations nationwide to provide comprehensive security expertise, guidance, and support, including risk assessments, security planning, training, and exercises.

Cybersecurity Capability Maturity Model (C2M2):

The C2M2 helps organizations accurately gauge investment and improvements to their cybersecurity programs and strengthen their operational resilience. The C2M2 tool focuses on implementation and management of cybersecurity practices associated with IT and OT assets and the environments in which they operate.

Incident Reporting:

CISA provides a secure, web-enabled mechanism that facilitates reporting of pertinent information such as date, time, organization, and incident description when a ransomware or other cyber incident occurs. This enables rapid response capabilities as a security incident unfolds and real-time security analysis to understand potential cascading impacts across multiple critical infrastructure sectors. Examples of incidents to report to the proper authorities include phishing emails, unauthorized access attempts to systems, malware, and unauthorized changes to systems, firmware, or software characteristics.

Cybersecurity Operational Technology Environment (CyOTE™):

CyOTE is a DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) investment to enhance the electricity sector's threat detection of anomalous behavior that may indicate malicious cyber activity in OT networks. The initiative aims to develop tools and capabilities that can provide electricity asset owners and operators with timely alerts and actionable information.

Cybersecurity Risk Information Sharing Program (CRISP):

CRISP is a public-private partnership between DOE and the Electricity Information Sharing and Analysis Center. CRISP collaborates with energy sector partners to facilitate the timely bidirectional sharing of cyber information, enhancing the sector's ability to protect critical electric infrastructure.

Cyber Testing for Resilient Industrial Control Systems (CyTRICS):

CyTRICS partners across stakeholders to identify high priority OT components, perform expert cyber testing, share test results, and inform on improvements in design of components. CyTRICS leverages best-in-class testing capabilities at four DOE National Laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners.

RESOURCES

Critical Infrastructure Vulnerability Assessments: cisa.gov/critical-infrastructure-vulnerability-assessments

Cybersecurity Advisors: cisa.gov/stakeholder-risk-assessment-and-mitigation

Cybersecurity and Physical Security Convergence Guide: cisa.gov/publication/cybersecurity-and-physical-security-convergence

Cybersecurity Best Practices for Industrial Control Systems: cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

Cyber Hygiene Services: cisa.gov/cyber-hygiene-services

Incident Reporting System: cisa.gov/forms-report

Insider Threat Mitigation: cisa.gov/insider-threat-mitigation

National Cyber Awareness System: cisa.gov/uscert/ncas

Protective Security Advisors: cisa.gov/protective-security-advisors

Ransomware Guide: cisa.gov/stopransomware/ransomware-guide

SCRM Essentials: cisa.gov/sites-supply-chain

Shields UP: cisa.gov/shields-up

Training & Exercises: cisa.gov/cybersecurity-training-exercises

Using and Sharing Protected Critical Infrastructure Information: cisa.gov/using-and-sharing-pcii

For more information or to seek additional help contact us at **Central@cisa.gov**.

C2M2: energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

CESER: energy.gov/ceser/articles/ceser-releases-supply-chain-assessment-digital-components

CyOTE: energy.gov/ceser/cybersecurity-operational-technology-environment-cyote

CRISP: energy.gov/sites/prod/CRISP

CyTRICS: inl.gov/cytrics