White Paper

Advancing Electric Utility Security

The nature of electricity generation, consumption, delivery, and the electrical grid itself have been changing rapidly and will continue to change. In addition to challenges posed by these changes, utilities face serious difficulties from increased cyber and physical security threats. For both types of security threats, The American Public Power Association (APPA) recommends that electric utilities use risk management programs to prioritize facilities and equipment, develop contingency plans, and employ defense-in-depth security techniques to "keep the lights on."[1]

However, across the electric utility industry, there are two categories of utility companies – *federally regulated* and *state & locally regulated* – between which are huge differences in the approaches to security, in large part due to the nature of their ownership and their regulatory environments. Table 1 below presents overview information provided by the U.S. Energy Information Administration for 2016, based upon electric utility reports to the administration.[2]

Table 1. Chief Categories of Utilities

Ownership	Count	Regulation	Customer Count	Customer %
Investor-Owned	61	Federal	101.75 million	63%
Cooperative	867	Federal or State & Local	19.44 million	12%
Municipal	1841	Federal or State & Local	15.29 million	10%
Other*	517	Federal or State & Local	23.96 million	15%

**Includes Customer-Owned, Community Choice Aggregator, Federal, Marketers and Marketing Authorities, Political Subdivision, and State*

The Cooperative and Municipal categories of ownership are together referred to as the Publicly Owned Utilities (POUs), in contrast to the Investor-Owned Utilities (IOUs). While there are estimated to be many more POUs (2,708) compared to IOUs (61), according to the U.S. Department of Energy, the IOUs account for nearly 80 percent of electrical transmission and the POUs and Federal power agencies account for almost all the remaining transmission. Although the POUs are characteristically smaller than most of the IOUs, and have facility management challenges on a smaller scale, they face the same types of security threats as the IOUs face.

Publicly owned utilities (POUs) and investor-owned utilities (IOUs) can take different approaches when implementing security solutions. This is because for IOU and some POU sites, federally-approved industry regulations specify the security approaches to take as prescribed in the NERC-CIP security standards. IOUs and some POUs are subject to rigorous audits and substantial fines for non-compliance to NERC-CIP mandates. Penalties for physical security deficiencies can range from $10,000 to $1,000,000 per day of violation.

---

[1] American Public Power Association, "Grid Security", Issue Brief July 2018, p. 1. Retrieved July 21, 2018 from: https://www.publicpower.org/system/files/documents/Grid%20Security_1.pdf

[2] Energy Information Administration. "Electric power sales, revenue, and energy efficiency Form EIA-861 detailed data files." Washington D.C.: U.S. Department of Energy, October 2016. Retrieved August 21, 2018 from: https://www.eia.gov/electricity/data/eia861/zip/f8612016.zip. (Frame_2016.xlsx.)

For POUs that are not subject to federal regulation or provided formal guidance on security from state and local regulatory commissions, many have different approaches to security programs. Key portions of the NERC-CIP standards can be applied very effectively by IOUs and these POUs to reduce security risks, especially CIP-014, the standard for Physical Security, which establishes the requirement to deter, detect, delay, assess, communicate and respond to physical security threats.

Security Obligations

All utilities have the need to protect their electric utility infrastructure – whether generation, transmission or distribution – including personnel, property and control/operations functions. Historically, public utilities have utilized traditional physical security measures, such as access control, intrusion detection and CCTV video surveillance with access to command and control functions in a security operations center (SOC) and/or Emergency Operations Center (EOC). Due to finite financial resources and the lesser capabilities of earlier generations of physical security technology, utilities are not likely to have all of the physical security capabilities that are available now to protect assets.

Thanks to the continually accelerating advancement of today's technologies, the capabilities of electronic physical security systems to deter, detect, delay, assess, communicate and respond to physical security threats far surpass those of even a few years ago. Today, advanced video and audio analytics, high-resolution network video cameras, multi-technology 3D intrusion detection, and improved systems integration capabilities provide highly accurate threat detection and classification.

Many current-technology video-based applications include the ability to securely share video and other data with first responders as well as security personnel in the field through mobile device support. With new technology, faster person and vehicle detection can be performed with 90% or greater accuracy.

Aligning Protection Measures with Current Risks

To make best use of security funding, security architects must prioritize what assets are critical, how they are at risk, and plan how to use people, process and technology measures to best *deter, detect, delay, assess, communicate and respond to threat actions* according to sound security practices and guidance. The NERC-CIP standards and guidance can be applied successfully for the protection of non-regulated assets, which – while they are not part of the bulk power system – are critical to the local distribution of electric energy.

Facility Threats

Today's electric utility facility threats include theft of materials for scrap resale, destruction of property and systems in political or social protest, cyber-attacks on data networks and information systems, and other events intended to damage or interrupt power service. There are over 55,000 substations in the U.S., many of which are particularly attractive targets because of the important function they perform and the fact that they are typically unstaffed and often located in remote and open settings. Many of those that are monitored for intrusion or surveillance have communication lines that are vulnerable to being cut, leaving security personnel unaware of what is happening.

Increasing substation automation and integration means that many substations will be getting improved and more robust communications capabilities, which will support improved security system communications including redundant communication paths and immediate notification of communications loss. As a result, not only can the original intentions of NERC-CIP regarding physical security be fully achieved with effective planning

and technology deployment, POUs that are not federally regulated can selectively apply the relevant portions of NERC-CIP to focus their security improvement efforts and ensure that their security technology fully addresses their needs for risk mitigation and security operations capabilities.

There is every reason to take action on further addressing security risks now, if action is not already well under way.

Utility Security Improvement

Two NERC CIP standards, CIP-006 and CIP-014, provide concepts, perspectives and requirements for electric utility physical security. The following important concepts are found in the CIP requirements and guidance. These concepts have been proven to be key factors in establishing and maintaining a strong physical security profile for electric utility sites.

Developing and Implementing a Security Plan

CIP-006 provides three tables that specify minimum requirements and measures for a security plan or program. The three requirements tables address:

- Physical Security
- Visitor Control Program
- Physical Access Control System Maintenance and Testing Program

CIP-014 specifies:

- Initial and subsequent risk assessments
- Third-party risk assessment verification
- Threat and vulnerability evaluation of transmission facilities, substations and control centers, considering:
  - Site unique characteristics
  - Prior history of physical security events
  - Intelligence or threat warnings received from law enforcement, governmental agencies and other resources
- Develop and implement a physical security plan that includes:
  - Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified in assessments
  - Law enforcement contact and coordination
  - Timeline for executing the physical security enhancements and modifications specified in the physical security plan
  - Provisions to evaluate evolving physical threats, and their corresponding security measures
- Third-party review of the threat and vulnerability evaluation and physical security plan

The approach outlined by NERC CIP can be applied by any electric utility to any of its sites to develop and implement security plans and specific security measures that are appropriate for the threats and vulnerabilities that each site faces. Going beyond the physical protection of electric energy delivery systems, there are also broader impacts to consider, such as utility reputation and community support, which can result from security incidents. These can be easily considered as part of the above approach.

Key Security Design Concepts

CIP-014 Identifies *security operations capabilities* (deter, detect, delay, assess, communicate and respond to physical security threats) that are most effectively achieved using *layered security protection to achieve defense in depth* as described in CIP-006. Site threat and vulnerability evaluation involves the consideration of risk scenarios against which sites must be protected. Layered security addresses the possibility that one or more security measures may be bypassed or defeated; it helps assure that the set of security measures can still be effective in addressing the threat. The purpose for such security planning is to establish a security program with security operations capabilities that reduce the site security risks to acceptable levels, at an acceptable cost. That is much easier to accomplish given the capabilities of today's security technologies.

Most utilities will have many security measures in place, and can review the effectiveness, efficiency and manageability of the measures in place in light of what new technologies offer – especially the cybersecurity features built into the new technologies.

Electronic Physical Security Systems Are Cyber Assets

For more than 15 years, the U.S. federal government has considered electronic security, access control and digital video systems to be Information Technology (IT) systems, to be subject to all the protections and design criteria applicable to IT systems in the Federal space.[3]

Electronic security systems contain a mix of *standard information technology* (such as servers, workstations, networks and radios) and *Internet of Things technology* (such as video cameras, intrusion sensor systems, credential-based physical access control, intercoms, and alarm systems). Electronic physical security systems are cyber assets that require both physical and cyber protective measures to assure the confidentiality, integrity and availability of real-time security technical capabilities and the evidence information collected by the security systems. Thus, cybersecurity is an important consideration in the design of electronic physical security measures.

Continuous Improvement

Electric utility facilities and systems are continually changing and evolving, as are their security threats. Thus, leading utilities have found it most practical to develop security programs – and implement security technology infrastructure – that can be easily sustained and continually improved in accordance with these changes. The *continuous improvement* approach is a very practical one, because it is not financially or operationally feasible to implement all desired security improvements at the same time. Risk-based prioritization of security measures, as outlined by NERC-CIP standards and guidance, provides the most security-effective path for risk reduction and supports continuous security improvement. Current-day electronic security technology makes this approach very feasible.

For more information about security solutions for utilities and other critical infrastructure sites, contact:

Jeff Fields
Business Development Manager
Bosch Security and Safety Systems
Phone: 315-310-1133
Email: jeff.fields@us.bosch.com

[3] Security Industry Association, "Homeland Security Presidential Directives (HSPDs) and their effect on the Security Industry", SIA Quarterly Technical update, Jun. 2005.