SECURING POWER FACILITIES

Protecting Vulnerable Security Points At Power Centers

CyberLock

CyberLock, Inc. 1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501 • www.cyberlock.com • sales@cyberlock.com • support@cyberlock.com
CyberLock and CyberKey are registered trademarks of Videx, Inc. in the United States and other countries.

SECURING POWER FACILITIES

Protecting Vulnerable Security Points At Power Centers | by CyberLock

The U.S. government has defined 16 critical infrastructure sectors in an effort to assess and eliminate the security risks and vulnerabilities within each one. The energy sector, in particular, is vital to nearly every aspect of our lives. Indeed, the other 15 sectors rely heavily on the energy sector's ubiquitous infrastructure. With an annual consumption exceeding 4,000 terawatt hours (TWh), the United States is the world's second largest electricity consumer. Thousands of electrical power utilities are responsible for ensuring that our power generation and distribution facilities are capable of meeting this enormous demand. Collectively, these utilities face a monumental task. Even brief disruptions in supply can wreak havoc at a local or regional level. To say that security within the energy sector is imperative may even be an understatement.

EVEN BRIEF DISRUPTIONS IN SUPPLY CAN WREAK HAVOC AT A LOCAL OR REGIONAL LEVEL.

While many of today's security policies focus on cyber security, in 2014 the Federal Energy Regulatory Commission (FERC) recognized the need for increased physical security standards. The North American Electric Reliability Corporation (NERC), under the direction of FERC, defined a set of Critical Infrastructure Protection (CIP) reliability standards that include both physical and cyber security plans for monitoring and managing access to critical infrastructure sites. For electrical power utilities, demonstrating compliance with mandatory CIP standards requires administrators to confront a variety of physical security challenges. At the core of nearly every physical security plan is a set of locking devices designed to control user access. From padlocked gates at remote sites, to doors, cabinets, and even server racks, power utilities rely on locking devices throughout their facilities. However, not all locking devices are created equal. In this paper, we explain why certain locks may not be suitable for CIP compliance.

Mechanical Locks and Keys

With seemingly limitless variety, simple installation, and appealing prices, mechanical locks and keys offer an entry-level security solution. However, mechanical systems lack important features available in high-security locking systems, many of which are essential for power utilities pursuing CIP compliance. Notably, mechanical locks and keys lack the ability to track who was where, and when. CIP-006-6 expressly requires that access details be logged for each person entering a Physical Security Perimeter. While posting a guard at every perimeter access point would technically meet this requirement, manned checkpoints are not a feasible option for medium to large-scale organizations with numerous remote sites. Deploying security cameras is a popular alternative, however memory, bandwidth, and power limitations can cause recurring administrative headaches.To truly provide accurate documentation, cameras must generally be paired with complex facial recognition or biometric scanners,potentially exposing an organization to high-stakes privacy regulations.Additionally,a camera does not physically protect against unauthorized access, it merely satisfies the need to have a time-stamped record of the entry.

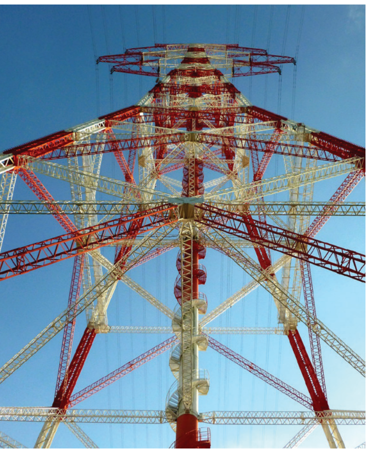
A SINGLE ROGUE KEY HAS THE ABILITY TO UNDERMINE AN ORGANIZATION'S PHYSICAL SECURITY ALTOGETHER. WITH SO MUCH AT STAKE, ELECTRICAL POWER UTILITIES HAVE TO ADDRESS COMMON KEY CONTROL INCIDENTS

Beyond CIP compliance, the risks associated with a lost, stolen, or readily copied mechanical key are immeasurable. With few practical ways to determine when a key is copied or trace its use after it was reported lost or stolen, facilities can easily lose control of keys in circulation. A single rogue key has the ability to undermine an organization's physical security altogether. With so much at stake, electrical power utilities have to address common key control incidents with costly, and often temporary, fixes. With a mechanical system in place, organizations may find themselves repeatedly re-keying their locks just to maintain the integrity of their security system. Re-keying a single facility can be cost-prohibitive, let alone a network of infrastructure sites spread across multiple states. In addition to widespread key control issues, mechanical locks are susceptible to picking and keyway vandalism, rendering them either ineffective or inoperable. Simply put, mechanical locks and keys are not sophisticated enough to meet the growing demands of critical infrastructure.

Remote access control CyberLock solutions

Electronic Security Systems

Electronic security systems, such as numeric pin pads, RFID card readers, and biometric scanners are commonly used in facilities that require electronic tracking and precise, scheduled control over who has access. While most electronic security systems provide enhanced security features compared to a mechanical solution, the installation costs, potential structural modifications, and networking requirements are significant drawbacks, particularly at remote or isolated sites. Like cameras, electronic security systems have inherent bandwidth, connectivity, and power limitations that present challenges for many applications. Moreover, electronic solutions are vulnerable to power and network outages, leaving critical sites inaccessible or, worse yet, unsecured during emergency situations. The cost and time associated with installing a hardwired access control system is also notably higher than that of a mechanical lock and key system. While electronic security systems are a sensible choice in certain industries, for many power utilities these types of access control solutions are impractical.



WHILE MOST ELECTRONIC SECURITY SYSTEMS PROVIDE ENHANCED SECURITY FEATURES COMPARED TO A MECHANICAL SOLUTION, [THERE] ARE SIGNIFICANT DRAWBACKS, PARTICULARLY AT REMOTE OR ISOLATED SITES

NERC Reliability Standards

NERC is a non-profit regulatory authority committed to reducing risks that threaten the reliability and security of the power grid. In the United States, all bulk power system owners, operators, and users must comply with NERC-approved reliability standards. Two of the CIP reliability standards, CIP-006-6 and CIP-014-2, set forth mandatory physical security controls to guard against attacks that could compromise the integrity of the grid.

CIP-006 aims to manage access to Bulk Electric System (BES) facilities by specifying a physical security plan to protect against vulnerabilities that could lead to disruption or instability within the BES. Among the mandates of CIP-006, an organization must demonstrate that it has implemented a documented physical security plan that includes controls limiting physical access to only authorized individuals. Notably, CIP-006 also requires that entry of each individual into a Physical Security Perimeter is documented, whether electronically or otherwise, with such records being maintained for at least 90 days.

While CIP-014 also addresses physical security controls, it is focused specifically on protecting those transmission stations and transmission substations that, in the event of an attack, are at risk of instability, uncontrolled separation, or a cascading failure. CIP-014 mandates that organizations must implement a physical security plan with measures designed to deter, detect, delay, communicate, and respond to potential physical threats to transmission stations, substations, and associated control centers.

FOR POWER UTILITIES IN PARTICULAR, IT IS IMPORTANT TO CONSIDER AN ACCESS CONTROL SYSTEM THAT IS COMPATIBLE WITH A WIDE VARIETY OF DOOR HARDWARE.

The most critical element of any physical security plan is implementing a means for effectively preventing unauthorized access to secured areas. For power utilities in particular, it is important to consider an access control system that is compatible with a wide variety of door hardware. After all, most facilities comprise a varied mix of physical access points, from office doors to gate padlocks, even remote equipment enclosures.

Key-Centric Access Control

Key-centric access control systems offer a versatile solution that is ideal for electrical power utilities. Importantly, key-centric systems can help organizations implement a physical security plan that meets CIP-006 and CIP-014 standards. Although less familiar than mechanical locks and keys, or even electronic security systems, key-centric access control systems combine the precision of electronic systems with the simple installation, affordability, and ease of use of a mechanical system. Key-centric systems allow users to retrofit their existing mechanical lock hardware with an electronic version that gives administrators complete control and visibility of their critical assets. With all of the power for the system provided by the key, organizations don't need to manage periodic battery replacements for locks scattered throughout their facilities. Personalized access permissions can be scheduled via the electronic keys. When a user attempts to access a site outside of his or her scheduled time, the lock won't open. Every access attempt, whether successful or not, can be recorded in both the lock and the key, providing detailed documentation for every system event. Additionally, key-centric access control systems are designed for convenient installation in nearly any lock hardware, allowing facilities to implement a CIP-compliant physical security plan that fits their specific needs.

CYBERLOCK PROVIDES FULL-FEATURED, CABLE-FREE ACCESS CONTROL TO EVERY LOCKING POINT IN AN ORGANIZATION.

One key-centric solution with proven success in the energy sector is the CyberLock® access control system. CyberLock provides full-featured, cable-free access control to every locking point in an organization. CyberLock's durable electronic cylinders are easily deployed on doors, but also on gates, trucks, shipping containers, and other mobile and remote assets. The battery in a CyberKey smart key energizes the CyberLock cylinder during an access event, bypassing the need to install and maintain network or power cables. As the cylinders are installed without any wiring, setup and installation is quick, easy, and affordable. Keys are programmed with access permissions for each individual user, limiting access to authorized personnel. Each lock and key holds a memory of every access attempt, allowing management to view an audit trail showing who accessed or attempted to access specific locations. With IP68-rated CyberLock padlocks, power utilities can use this detailed audit trail to automatically track access events at remote and temporary Physical Security Perimeters, helping meet CIP entry log requirements at virtually any entry point in the organization.

To minimize key control risks, expiration dates can be set to prevent keys from operating beyond their authorized life. For added security, when a CyberKey is lost or stolen, administrators can simply flag the missing key in the software. Instead of undergoing a costly re-keying process, CyberLock lets utilities quickly distribute lost key instructions

Remote access control CyberLock solutions

to their locks, ensuring any rogue keys are rendered inoperable. In addition to the access control and reporting capabilities essential to CIP compliance, CyberLock offers a multitude of productivity enhancing features with an industry-leading range of connected smart keys. Personnel can receive access permission updates in the field, eliminating time-consuming trips back to the office. With CyberLock, power utilities are no longer forced to choose between compliance and productivity.

ELECTRIC POWER UTILITIES PLAY A FUNDAMENTAL ROLE IN NEARLY EVERY ASPECT OF OUR LIVES. THE STRICT SECURITY GUIDELINES AND PROTECTIVE MEASURES HELP ENSURE THE CONTINUED, SAFE OPERATION OF OUR POWER GRID

Conclusion

Electric power utilities play a fundamental role in nearly every aspect of our lives. The strict security guidelines and protective measures help ensure the continued, safe operation of our power grid. Both mechanical locks and keys and traditional hardwired access control systems struggle to meet the needs of this industry. Key-centric access control systems offer the benefits of both systems, delivering an ideal solution for a wide range of power facilities. With over 20 years of proven success, CyberLock systems are built exclusively in the U.S.A. to exceed the demanding expectations of the energy sector.