3625 Alleghany Drive
Salem, VA 24153
1-800-675-7558
www.medeco.com

Access Control and Tracking at Utilities and Power Grid Facilities to Comply with FERC and NERC Standards

August 15, 2008

By Jennifer Riley
Medeco High Security Locks

Abstract

The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) govern the nation's energy industry and ensure the reliability of the U.S. and Canadian bulk electric power systems, respectively.

In 2007, FERC granted NERC the authority to enforce reliability standards on companies and individuals involved in the use, ownership and/or operation of the North American power grid, and made compliance with those standards mandatory.[1]

Several of the standards focus specifically on the security of physical assets and electronic data related to the power grid, as well as to public utility generation and delivery systems.

Individuals and organizations responsible for security at facilities that fall under FERC and NERC jurisdiction need to understand what the reliability standards are and how they relate to security, and whether their current security initiatives ensure compliance with said standards.

This paper will examine the FERC and NERC standards that focus specifically on access control, discuss the risks inherent in traditional security measures designed to protect physical plants and electronic data, and offer specific security solutions that help ensure compliance with the reliability standards through access control and tracking.

Introduction

Established in 1977, FERC regulates the interstate transmission of electricity, natural gas, and oil. Similarly, NERC, established in 1968 and only later becoming subject to both FERC and Canadian government oversight, is "committed to ensuring the reliability of the bulk power system in North America"[2] by maintaining the U.S. and Canadian electric power grids. In simpler terms, NERC President and CEO Rick Fergel describes NERC as the "'electric reliability organization' as defined in the Energy Policy Act of 2005."[3]

Each organization established and adopted enforceable security requirements aimed at preventing attacks, both physical and electronic, that could impact the reliability of the energy and utility delivery and generation systems.

Managing access to electronic data and the equipment it's housed on and access to hard assets, such as generating plants, equipment, transmission facilities or networks, not surprisingly focuses on controlling and tracking physical access and attempted access by individuals to these assets.

NERC and FERC – Specific Standards Related to Physical Security

NERC submitted to FERC and FERC subsequently approved in January, 2008, eight critical infrastructure protection (CIP) reliability standards. CIP-006-1 is of particular interest for purposes of a discussion on securing electronic assets as it addresses the physical security of the critical cyber assets identified in Reliability Standard CIP-002-1.

Specifically, CIP-006-1

> *"requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter also reside within an identified physical security perimeter. The physical security plan must be approved by senior management and must contain processes for identifying, controlling, and monitoring all access points and authorization requests. The Reliability Standard also requires that the logging of physical access must occur at all times, and the information logged must be sufficient to uniquely identify individuals"*[4]

FERC, meanwhile, addresses security through its Title 18: Conservation of Power and Water Resources, Section § 3a.41 Access Requirements. The Access Requirements section discusses physical access to classified materials broadly. Essentially, it states access to classified materials is determined by clearance level and need for access. The person responsible for the security of these items or areas determines a seeker's level of need. Most importantly, the individual accessing a classified area can only have admittance during the time of need. The law states that, "When a staff member no longer requires access to classified information or material in connection with performance of official duties," their clearance will be withdrawn.[5]

Unauthorized Access – A Real and Recurring Problem

Whether the threats are posed by terrorists, a disgruntled former employee or even teenagers who mistakenly view their actions as a harmless prank, the end result of unauthorized access and tampering at a power or utility facility is the same – a disruption of local and even national electrical power supply and utility generation and transmission. And, it matters little if the improper access is for purposes of gaining entrance to the facility's computer assets or to its other physical assets.

Perhaps the most well publicized incident of an intrusion into a power-generating facility to date was not, thankfully, unauthorized at all. In what is now known as the "Aurora" vulnerability, the Energy Department's Idaho National Laboratory, working for the Department of Homeland Security, was able to remotely change the settings on a small generator, causing the generator to shudder, emit black smoke and ultimately shut down because it suffered damage. The task was accomplished completely over the Internet and was designed to show that vulnerabilities to power grid equipment do indeed exist, whether criminals gain access remotely or by accessing a facility's computer server rooms.

NERC President and CEO Rick Fergel, in discussing attacks gained by accessing computers, grid vulnerabilities, and the public interest they generate, mentioned media reports that claimed hackers from China were responsible for two separate incidents that resulted in blackouts to a U.S. electric grid.[6] While those rumors have never been proven, the media attention they and the Aurora incident generated, demonstrate the potential for abuse, and the need to protect access to critical infrastructure electronic assets, such as computer server rooms.

The threats to the nation's energy and utility infrastructure aren't limited solely to attacks launched by gaining physical access to a utility's server room or over the Internet. An equally devastating threat lies in individuals or groups gaining unauthorized physical

access to facilities for purposes of tampering with or destroying equipment. This threat might be viewed as even more pressing and disturbing because there are numerous instances of it having already occurred, and because it could possibly be accomplished with less sophistication, knowledge and skill as compared to a cyber-based attack.

For example, in London in 2003, a group of 30 anti-nuclear protestors broke into the central control building of a nuclear power plant to demonstrate the facility's lack of security and its vulnerability to a terrorist attack.[7]

In Morgantown, West Virginia, thieves illegally accessed an Allegheny Power substation and stole copper wiring from the grounding towers.[8] In neighboring Ohio, more than $2,000 worth of copper was stolen from an American Electrical Power substation that was broken in to.[9]

In Utah in 2006, an individual or group accessed electrical power facilities in Salt Lake Valley and attempted to shut down the power grid over a wide area.[10] Instead, they managed to cut power to nearly 4,000 homes and businesses. A similar break-in occurred at a much larger power facility nearby a short while later, but this time a back up generator prevented what would have been an even more widespread power outage.

In Blackstone, Mass., teenagers affected the town's water supply for more than 9,000 people when they broke into a water facility and accessed the city's 1.3-million-gallon-water holding tank.[11]

Traditional Security Systems and Why They Are Inadequate

Mechanical locks are often the first line of defense for utility companies attempting to control physical access to certain areas of their facilities and to their computer systems responsible for helping operate those facilities, and understandably so. They're quick, easy, and inexpensive to install. There's a certain comfort level associated with this familiar security system used countless times daily to protect homes, vehicles, offices and other valuables. They don't require users to memorize access codes or carry electronic access cards, and traditional locks are cosmetically unobtrusive. Unfortunately, most locks are also woefully inadequate when it comes to protecting a corporation's most valuable assets.

The traditional lock and key system is a good solution in situations where there is only one person using the key, where tracking access isn't important, and where the need to add or delete keys from a system isn't a concern. But even this "one user, one key" situation, while fairly uncommon in today's environment, is fraught with risk. What happens if the key is lost or stolen, or worse yet, copied without the owner's knowledge?

This risk, however, can be mitigated to a degree by using a high-security mechanical system. Often employing patented keys and locks that are extremely difficult to bypass, these high-security mechanical systems do offer a significant level of protection and control as compared to standard systems, albeit without an audit and tracking feature.

A traditional mechanical masterkey system, particularly one that isn't defined as high-security, simply doesn't offer enough protection, flexibility and data needed to control access to data and to provide tracking features that enable the utility to maintain compliance with FERC and NERC standards.

When compared with other security options, traditional, non-high security mechanical masterkey systems come with other inherent risks and weaknesses, including:

- No ability to track who is accessing or attempting to access a door, how often, and when.
- No ability to limit access to certain times of the day or night to correspond to employees' scope of work.
- No ability to quickly add or delete keys from a system when a key is lost, stolen, or an employee is no longer part of the organization.
- Unpatented or otherwise restricted keys can be copied and locks easily bypassed without leaving physical evidence to serve as an indicator of a security breach.
- Users need multiple keys to access different locks.

Electronic security systems that employ security cards, alpha-numeric codes or biometrics, provide heightened levels of protection when compared to a traditional mechanical masterkey systems but also bring with them a set of drawbacks separate from mechanical keys and locks, inluding:

- Expense to install, both from a time and materials standpoint.
- Installation locations dependent on the availability of power and network lines.
- Installation requires significant modifications to the door or frame, or both.

In certain environments, either a mechanical- or an electronic-based security system can be the appropriate solution to asset protection. Neither system by itself, however, is the right solution for securing and controlling access to power grid facilities and public utilities, many of which are often in remote, unattended locations.

Solutions

CIP 006 requires the implementation of physical access methods, such as card keys or special locks, including but not limited to, locks with 'restricted key' systems. CIP 006 also requires methods for "logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week."[12] In other words, a locking device with an audit trail is required in the absence of a full-time attendant to log access to every covered entrance.

A viable, cost-effective solution to fullfilling these and other FERC and NERC requirements lies in combining the best attributes and features of mechanical and electronic door locking systems.

Medeco High Security Locks designed and introduced Logic – a new electromechanical product line that consists of digital lock cylinders and digital keys – as an answer to security and access tracking needs by using the most desirable characteristics that both mechanical and electronic sytems offer.

Logic offers functionality similar to that of sophisticated electronic security systems, including audit trails, scheduling and the ability to add and delete users easily, but installs without any wiring, door or frame modifications or additional hardware.

Logic's digital cylinder and digital key look much like a traditional lock and key. The key is virtually indistinguishable from most car keys, with the exception of a small display screen, as is the cylinder. The difference lies in the digital technology contained in both the self-powered key and the cylinder, which is powered by the key.

Logic's digital cylinder retrofits into existing hardware, enabling the replacement of an existing cylinder and mechanical key with the electro-mechanical Logic cylinder in less than five minutes. This upgrade results in a stronger mechanical system, and the ability to both electronically audit access and change accessibility features, such as times and authorized users, quickly.

With Logic, any key can be programmed to work or not work on any cylinder, without being limited by a mechanical hierarchy like on a mechanical masterkeying system.

Knowing who is accessing or attempting to access facilities is a key element in protecting the power grid and other utilities. Logic systems allow up to 1,000 audit trails to be pulled from both the key and the cylinder, showing who is entering the protected area, how often, and when, thanks to time and date stamps. This data enables administrators to regularly evaluate and assert that the internal controls are operating efficiently, and helps companies comply with key FERC and NERC requirements related to access control and logging.

Lost keys can simply be electronically deleted from the system to maintain security. And, any time a new user key is needed, it can be quickly and easily added.

Additionally, unauthorized key copying is removed from the equation because replacement keys are cut and issued only by the Medeco factory and because of the patented electronic technology in Medeco keys – two features that, combined, offer superior protection against unauthorized key copying.

Instant rekeying is another Logic benefit as keys and cylinders can be instantly and easily deactivated or reprogrammed with different access permissions or schedules, either by Medeco dealers or by end-users who choose to self manage their systems with an optional programming device and software.

While Logic's auditing and tracking features that show who is accessing or attempting to access a facility's secure areas and its technology that prevents unauthorized access are compelling by themselves, the installation benefits shouldn't be overlooked.

Traditional electronic security systems, including card readers, biometric systems, or keypads, usually require electricity in order to operate, and if the system is being installed as a retrofit, significant installation expense in both time and materials. Logic cylinders simply retrofit existing mechanical cylinders and leverage the use of existing door hardware without any door or hardware modifications. No electricity, hardwiring, phone, or Internet connection is necessary. This also means that the system is portable and can be moved as easily as changing a traditional cylinder so when security needs change, the system can adapt quickly and easily. And, unlike many stand-alone systems, Logic cylinders blend discretely into existing hardware and architectural designs, and are available in most common architectural finishes.

Logic provides a straightforward, cost-effective security solution where a mechanical masterkey system simply doesn't offer enough flexibility to keep up with utilities' ever increasing demands, and the ever-changing methods individuals are employing to gain unauthorized access to data and the physical plant.

Logic offers strong physical security with the flexibility of schedules, audit trails, the ability to easily add and delete user keys, and unlike electronic systems, a retrofit cylinder that blends unobtrusively into existing hardware.

Conclusion

Threats to the power grid and utilities aren't going to disappear, nor are the regulations designed to protect them. In today's environment, physical and electronic data security isn't a question of whether protection is needed but rather what type of protection is the best choice. The added complexities of ensuring compliance with FERC and NERC standards addressing control and tracking, make that security decision even murkier.

Both mechanical and electronics-only locking systems have their limitations when it comes to securing utility facilities and providing the data and control needed to comply with governmental regulations.

A viable, cost-effect solution to protection and FERC and NERC data and physical control requirments is a security system that combines the best attributes of both the mechanical and electronic systems.*

- 0 -

*For more information, please contact Joseph Kingma, Director of Business Development at Medeco High Security Locks: 1-800-675-7558 ext. 1683 or jkingma@medeco.com

References

1. www.NERC.com

2. www.NERC.com

3. Rick Sergel, President & CEO of NERC, NARUC Summer Meetings 2008 Remarks, July 20, 2008

4. www.NERC.com

5. Electronic Code of Federal Regulations

6. Rick Sergel, President & CEO of NERC, NARUC Summer Meetings 2008 Remarks, July 20, 2008

7. Associated Press, "So Much for Security…Greenpeace Protestors State Break-in at Nuclear Power Plant," January 14, 2003.

8. WBOY-TV, Morgantown, W.Va., Karen Kiley, "Sheriff's Deputies Say Thieves Were After Copper," March 5, 2008.

9. Zanesville (Ohio) Times Recorder, Staff Reports, "$2,000 Worth of Copper Stolen from AEP Substation," July 22, 2008.

10. KSL.com, John Lollenhorst, "Break-Ins at Power Substations Investigated," February 13, 2006.

11. Associated Press, Ray Henry, "Teens Arrested in Water Facility Break-In," March 29, 2006.

12. www.NERC.com