ABLOY SOLUTIONS PAPER

LOCKING IN CRITICAL INFRASTRUCTURE PROTECTION AT A LARGE ENERGY UTILITY

Congressional Research Service
Informing the legislative debate since 1914

Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations

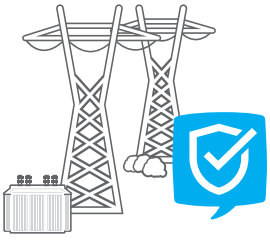
Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

June 17, 2014

SECURING THE ELECTRIC GRID

On April 16, 2013 the PG&E Metcalf Transmission Substation near San Jose, California came under sniper attack. An armed gunman destroyed 17 electrical transformers before disappearing into the night. The damage to the substation was significant — over $15 million dollars. One former federal regulator called the event a planned terrorist attack that, if replicated across the country, could have blacked-out much of the country.

Utility executives and federal energy officials have long worried that the electric grid is vulnerable to sabotage. This problem is compounded by the fact that there are increasingly sophisticated ways for people without authorization to gain access to transmission substations.



THE FEDERAL GOVERNMENT STEPS IN

A July 2014 report from the Congressional Research Service entitled, Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations, repeatedly cited the Metcalf attack and noted that, "…in the wake of the Metcalf incident, the Federal Energy Regulatory Commission (FERC) has ordered the imposition of mandatory physical security standards (for substations) in 2014."

FERC directed the North American Electric Reliability Corporation (NERC) to submit proposed reliability standards. Those standards would require utilities with critical assets to take steps, or to demonstrate that they had taken steps, to address physical security risks and vulnerabilities. Today, NERC's Critical Infrastructure Protection (CIP) Standards require all electric utilities to have a physical security plan and program in place to monitor and manage physical access to protect critical infrastructure, cyber assets, and Bulk Electric System cyber systems.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC CIP STANDARDS

Established to specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

To learn more, visit: www.nerc.com

HOW A MAJOR UTILITY BUILT A CULTURE OF COMPLIANCE

In response to the compliance requirements of CIP Standards, utilities have deployed various tactics including physical access control systems, electronic access control systems, cameras, security locks, fences and other means.

However, in a plant environment or substation, the assets are all over the yards, or they're situated all over a plant site. And utilities might have thousands of substations, each with multiple gates to be secured and monitored. So, what approach should utilities take to provide access control on traditional fencing and gates?

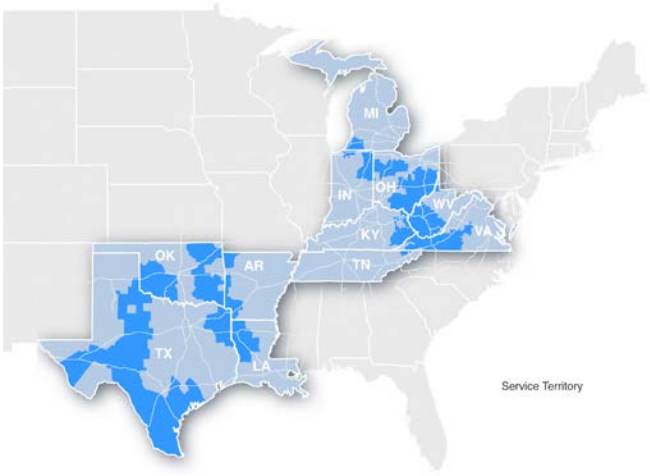
Here's how one Director of Security for a large utility headquartered in the Midwest secured his infrastructure with 4,000-plus locations in his transmission environment: "We took the compliance aspect of the standards and we used them as the minimum guidelines. We don't just do the minimum, we do what's right for security."

REPLACING AN OUTDATED AND UNCONTROLLED MECHANICAL MASTER KEY SYSTEM

In the energy transmission world, It's primarily fences and gates that are usually locked with a padlock and a chain. OSHA requires that the gates be locked, so no one gains access or gets hurt in a substation. Traditionally that's what utilities have done and continue to do because of the sheer amount of assets that need to be secured in the field. In many facilities, a manager might have a drawer full of keys and could give them to anybody he wanted. Before the regulations came into effect, there was no centralized logging, no centralized documentation.

To comply with the new NERC CIP standards, the utility needed to define operational or procedural controls to restrict physical access at its sites. Now, for authorized individuals requiring physical access to critical infrastructure or physical security perimeters, the utility needed to:

- Implement a minimum of one physical access control system, although two or more control measures are recommended.
- Monitor unauthorized access through all physical access points.
- Maintain records (automated or manual) of entry — with time and date — for each individual with authorized access, unescorted access, or unauthorized access to physical access points.
- Issue an alarm or alert within 15 minutes if unauthorized access is gained through physical access points.
- Keep physical access logs capturing date and time of individual's access for a minimum of 90 days.



"We looked at the benefits that the PROTEC2 CLIQ® system could give us and as long as we set up a program that requires people to sync on a periodic basis, even if we lose a key, we can send the command to shut it off, or if that key is found and someone tries to re-synced it, we can turn it off. We have an audit trail and now we're starting from scratch issuing keys and now we know who they are assigned to."

—Director of Security for Large Midwest Utility.

EXPERIENCED SECURITY INTEGRATOR LEADS THE IMPLEMENTATION

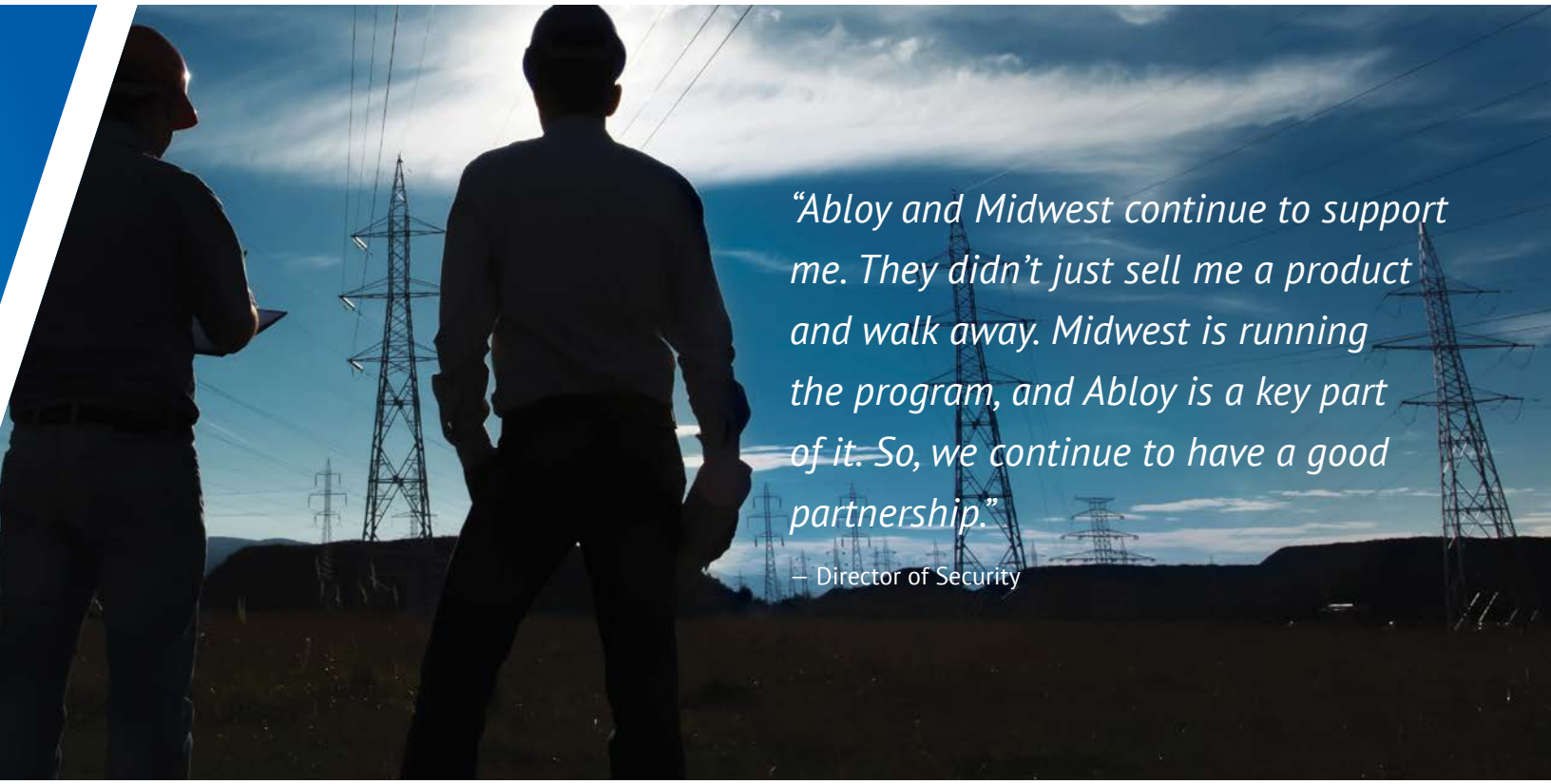
To assist them in developing a new, more compliant physical security footprint this utility turned to Midwest Security Products, Inc. This high security solutions provider and consulting firm has years of experience helping utilities, corporations, government and military installations harden their facilities and meet new regulatory environments. With its 40-person staff, including an engineering team and onsite data center, Midwest Security has become an industry leader in industrial and door lock hardware solutions.

To help its customer meet the new NERC CIP regulations, Midwest Security recommended upgrading to the PROTEC2 CLIQ® system by ABLOY® USA. This system combines high security super weatherproof padlocks that are virtually bump proof and pick proof, and keys with a mechatronic access control system that can be administered remotely.

"Previously, the person managing the keys for a utility might have had a drawer full of them and gave them away to anybody who needed one," said Mark Imhoff, Key Account Manager at Midwest Security Products. "In this case, there was no centralized logging and no centralized documentation of who had a key or when they used it. Some keys had been lost or stolen over the years, and since everyone in a region was keyed the same, this presented security risks across the network."

The utility partnered with Midwest on establishing a strategic plan to meet or exceed NERC CIP regulations. The company worked with managers in the field to build the keying systems, manage access rights and set the implementation schedule to secure thousands of locking points spread out over an eleven-state geographic area.

midwest
Security Products



"Abloy and Midwest continue to support me. They didn't just sell me a product and walk away. Midwest is running the program, and Abloy is a key part of it. So, we continue to have a good partnership."

— Director of Security

MINIMIZING RISK ASSOCIATED WITH LOST KEYS

With the system in place, they are now able to re-sync keys on a regular basis with remote access control. If a key is lost or stolen, it can be deactivated, and keys that aren't re-synced in a certain timeframe won't work anyway. Security administrators are able to issue keys in an organized and documented manner.

"The ability to control access from a central location is more convenient than the older versions of electronic keys, which in the past had required direct access to the lock," added Imhoff.

Audit trails can be pulled to find out who the keys are assigned to, and who has gained access to facilities. This is invaluable in maintaining compliance. While regulations allow power companies to self-report audits, the NERC audits security once every three years and can audit any other time, at their discretion. If a problem in auditing is reported, that can trigger a fine. If a problem in auditing isn't reported but is discovered later, that could also lead to an even bigger fine.

A SECURE COMMITMENT TO COMPLIANCE

Management at the utility was so impressed with the system, they made it the standard at all transmission stations and generation sites. This standardization across the board and centralized access control improves security and results in a more streamlined process. All told, this large utilities company will be able to meet NERC CIP regulations and benefit from a more efficient, safe and effective high security locking system for its critical infrastructure.

Imhoff added, "Their partnership is actually with both Midwest Security and ABLOY USA, because it's essential to develop a productive relationship with the security products manufacturer and also the integrator servicing the utility in the field."

WE'VE BUILT SUPERIOR LOCKS SINCE DAY ONE

One of the leading manufacturers of locks, locking systems, architectural hardware, and the world's leading developer of products in the field of electromechanical locking technology, ABLOY Security has been the symbol of high security and superior performance since 1907. As a brand of the ASSA ABLOY Group, we satisfy the most demanding security applications for a wide range of customer industries, from casino gaming, health clubs and locker space, OEM and parking meters, to public utilities, transportation, U.S. Government and vending.

Abloy 1907

CONTACT US AT 800.367.4598 OR VISIT ABLOYUSA.COM

ABLOY®

ABLOY secures people, property, and business operations on land, at sea, and in the air – in all circumstances.

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.

Wahlforssinkatu 20
P.O. Box 108
FI-80101 Joensuu | Finland
Tel. +358 20 599 2501
WWW.ABLOY.COM

ABLOY Security
6005 Commerce Drive #330
Irving, TX 75063
Tel. 972 753 1127
800 367 4598
Canada: +1 514-335-9500
info@abloyusa.com
WWW.ABLOYUSA.COM

PEFC PEFC/02-31-151

An ASSA ABLOY Group brand ASSA ABLOY