EXECUTIVE BRIEF:
POWER UTILITIES
Physical Security Regulatory Compliance
Why Medeco Intelligent Key Systems are an Efficient & Effective Solution

medeco®
ASSA ABLOY

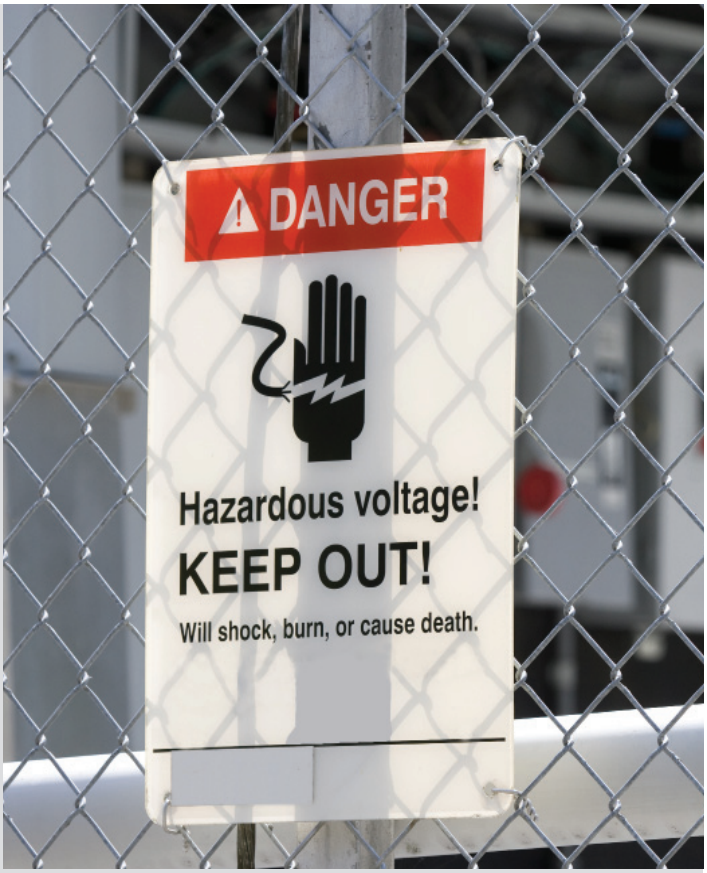
ASSA ABLOY, the global leader
in door opening solutions

How Vulnerable are U.S. Utilities?

Securing the electric power grid is among the highest priorities for critical infrastructure protection in the United States. In the past, power grid facilities have had varying degrees of access control and surveillance depending upon the facility type and location.

These measures were largely focused on public safety (reflecting liability concerns) and preventing vandalism and theft. More recently, federal agencies, Congress, and the utility industry have focused greater attention on the vulnerability of the power grid, especially the high voltage transmission (bulk power) system, to terrorist attacks which could cause widespread, extended blackouts.

Until 2013, the emphasis of analysts and policymakers was on power grid cybersecurity—protecting the computer controls and communication systems used to operate the grid. However, a 2013 rifle attack on an electric transmission substation in Metcalf, CA, shifted more attention to the physical security of power grid critical assets. Since 2014, security risks to the power grid have become an even greater concern in the electric utility industry.



The Federal Government Steps in to Ensure Physical Security

Whether the threats are posed by terrorists, disgruntled former employees, or teenagers performing a prank, the end result of unauthorized access and tampering at a utility facility is the same – a disruption of electrical power supply and utility generation and transmission.

In response to the Metcalf attack, as well as other incidents from utility security exercises, Congress passed new legislation to strengthen power grid physical security and to facilitate recovery in the event of a successful attack. 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.

Achieving and Maintaining Physical Security Regulatory Compliance

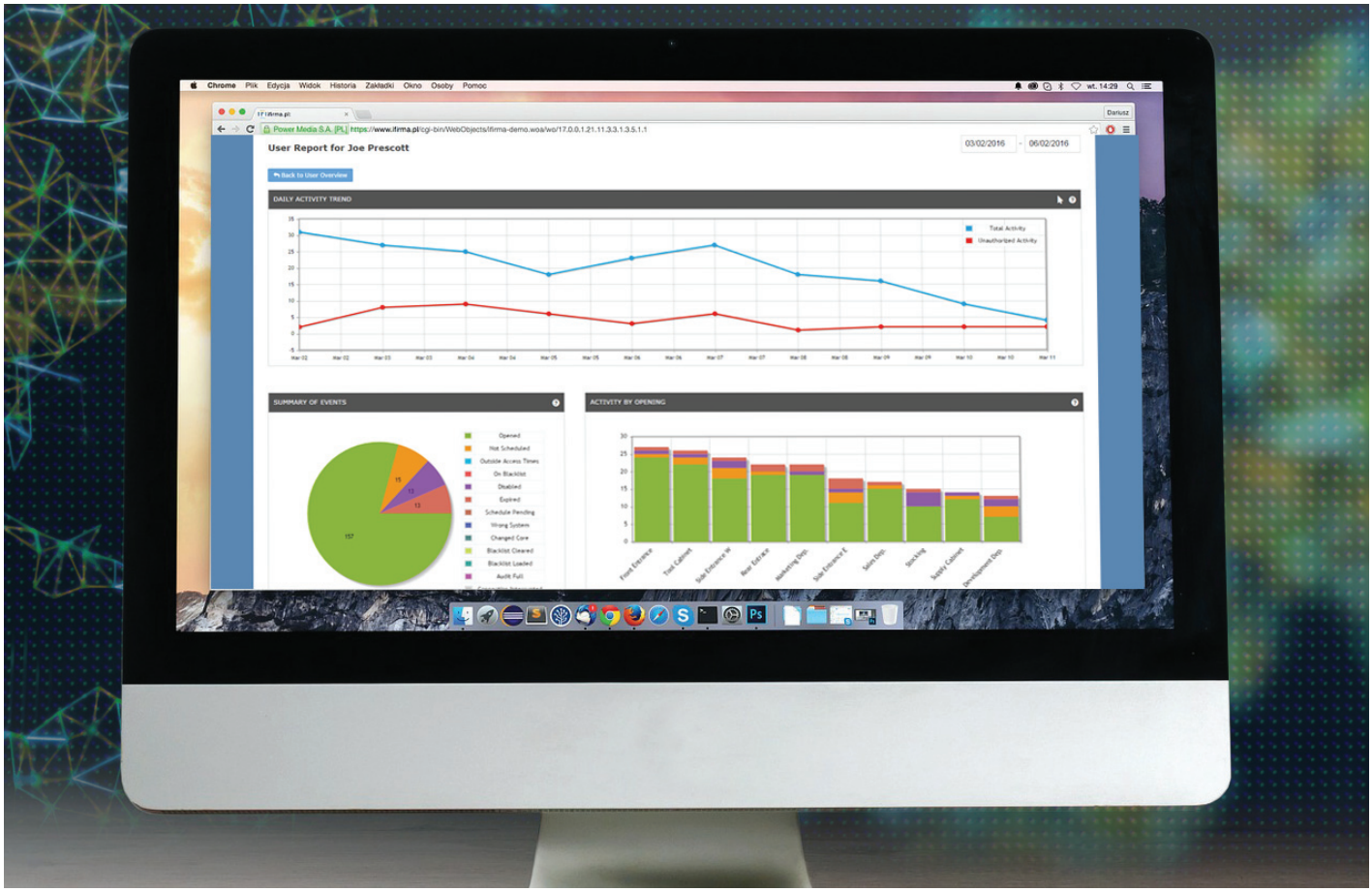
Today, NERC's Critical Infrastructure Protection (CIP) Standards require all electric utilities to have a physical security plan and program in place to monitor and manage physical access to protect critical infrastructure, cyber assets, and Bulk Electric System cyber systems.

To comply with these standards, utilities must define operational or procedural controls to restrict physical access. For authorized individuals requiring physical access to critical infrastructure or physical security perimeters, utilities should:

- 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 if unauthorized access is gained through physical access points.
- Keep physical access logs capturing date and time of individual's access.

Standard CIP-006
has been established to manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

Standard CIP-014
has been established to identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

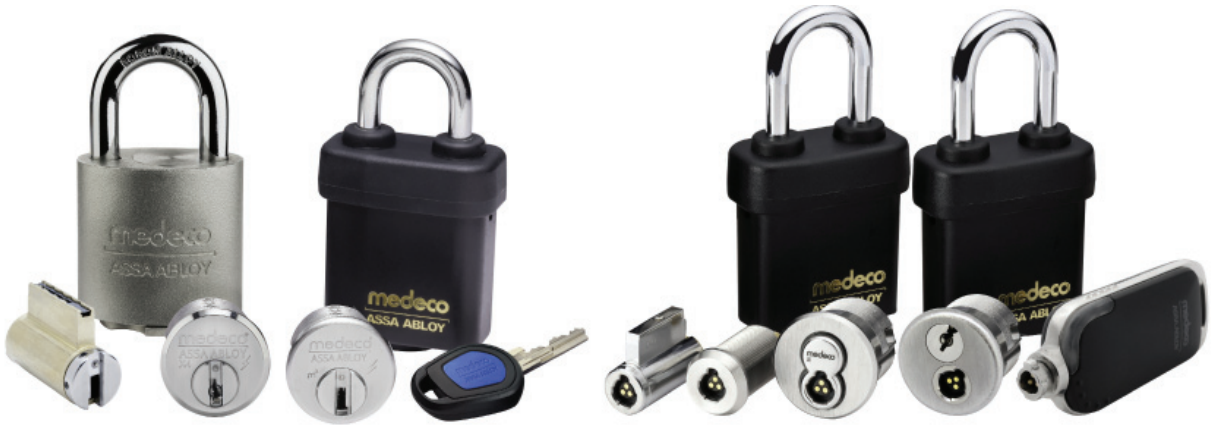


Role of Locking Systems in Critical Infrastructure

Utilities need to support the established resiliency strategies to assess, prevent, detect and recover. This strategy not only includes perimeter hardening but also encompasses cyber security, communications and equipment redundancy, hardening the System Operations Center, protecting critical substation assets, and recovery from all events — both man-made and natural.

As a tool to address the complex security scenarios facing critical infrastructure, secure locks are indispensable. For internal uses, locking devices on doors, elevators, machines, shutters, cupboards, cabinets and switchgears prevent unauthorized access. In critical infrastructure environments, locks are often required to be resistant to extreme temperatures, dust and toxic substances, fire and explosions.

For outdoor infrastructure sites, locks must perform in environments that are even more challenging, including ice, snow, rain and manipulation. Here, locking equipment secures outdoor gates, fences, doors, shutters, switchgears and key safes.



Critical infrastructure facilities tend to operate across large geographic areas, to have multiple and remote locations, and to have a large number of people needing to access those sites. Critical infrastructure companies often work with third-party companies and/or contractors who may need temporary access to a remote site. Locking systems must accommodate these challenges, too.

Specifically, critical infrastructure facilities can benefit from a high-security locking system that combines electronic and mechanical security; in effect, providing an intelligent combination of both.

Programmable keys are powered by replaceable or rechargeable batteries which energize the lock cylinder once the key is inserted. Communication between the cylinder and the key is encrypted to ensure the highest levels of security. Programmable cylinders for different applications do not require any wiring, so installation is fast and on-site maintenance requirements are minimal.

When the key is inserted into the lock, an audio indication is given and LED indicators inform the user whether or not the key has the necessary access rights.

Key management software and programming devices allow administrators to program, amend or delete keys remotely and instantly.

A key can be given a short authorization time-window, thus minimizing risks associated with lost keys. Security managers can generate time-stamped audit trails for any lock or key, and trace access workflows.

This is the kind of locking system that critical infrastructure — and its users — demand.

In Summary, Utilities are Looking for:

- Flexible access and key management for:
  - Permanent staff
  - Part-time staff
  - Third-party contractors
- Interior and exterior locking and access points supporting
  - Doors, elevators, machines, windows, shutters, cupboards, cabinets
  - Gates, fences, switchgears
- Global access to management software, with minimum IT investment and support
- Multiple administration possibilities, several roles (office receptionist handing out keys, security manager managing access rights and read audit trails), minimum administration time
- Easily support NERC CIP audits for physical security
- Easy key and access management for different users and their requirements
- Health and safety, works for existing processes
- Integration possibilities with HR systems, access control systems, task management software

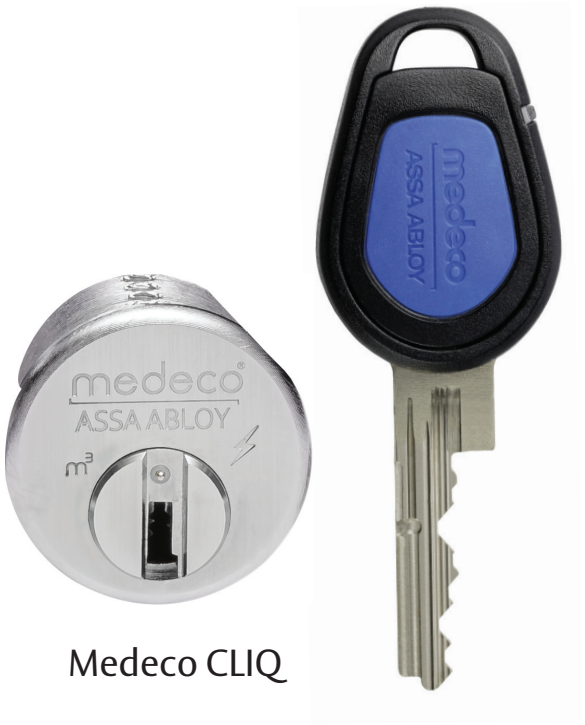
Medeco Intelligent Key Systems are a Smart Business Decision

In response to the compliance requirements of CIP Standards 006, Utility companies have deployed various solutions including physical access control systems, electronic access control systems, cameras, security locks, fences and other means. CIP-014 is not so prescriptive in the security measures they require that each owner or operator must install for compliance. The specific security plan is left open for the utility to determine what is appropriate.

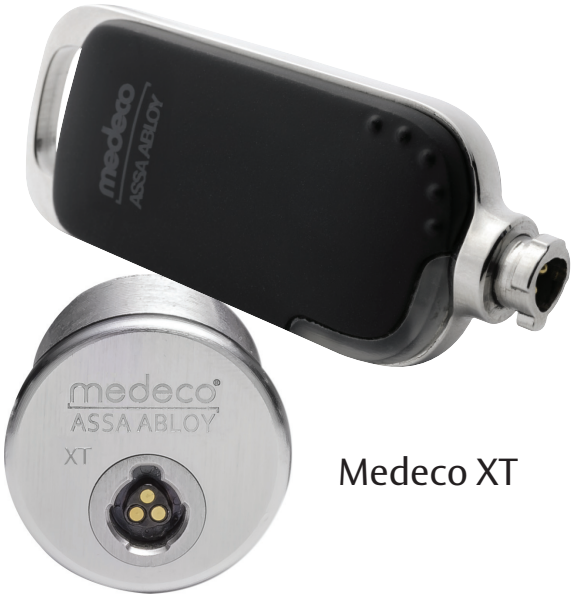
Medeco offers several solutions to help you adhere to these compliance requirements. Both the Medeco XT electronic locking system or the Medeco CLIQ electro-mechanical locking system provide controlled Access, accountability, physical security, and system management. Medeco Intelligent Key Systems provide many of the same benefits as an electronic access control system and the cylinders in both of these Intelligent Key Systems retrofit a facility's existing hardware without hardwiring, reducing installation time and providing a significant cost savings.

Medeco Intelligent Key Systems provide outstanding physical security, which is the hallmark of Medeco security locks. Medeco locks are built to the highest standards, provide strong protection against forced entry and include tamper-proof features in an attack-resistant design.

Some utilities have gone the route of an elaborate Electronic Access Control (EAC) system to provide physical security. The major drawback of an EAC system is the cost to install. Hardwiring is needed throughout the system which means cabling and construction expense, delays and lost time. The power for a Medeco Intelligent Key System resides in the electronic keys—there is no hardwiring required which means the system continues working even during a power failure. Medeco XT Intelligent Keys use rechargeable batteries that hold enough power for 1,800 openings per charge. Medeco CLIQ Intelligent Keys use replaceable coin cell batteries with a 20,000 cycle battery life. Because there is no outside power source, either key system can be deployed in all interior and exterior climates— from office spaces to outside perimeters that use padlocks.



Medeco CLIQ



Medeco XT

Compared with an EAC or other system, installation of a Medeco Intelligent Key system is a snap. The installer simply removes the old cylinder and drops in the new cylinder. That means deployment is fast and efficient, good news for a utility that needs to be in compliance with CIP Standards.

Trusted Security for Critical Infrastructure

Medeco Intelligent Key Systems offer the following benefits to owner or operator:

- **Key Management and Access Control**

  - Respond quickly to security threats, lost or stolen keys, or personnel changes utilizing expiring intelligent key validation intervals and remote programming.
  - One key can access doors, cabinets, gates and many outdoor areas .
  - Improved security due to flexible access, electronic scheduling and key management, e.g., the right person (employees, consultants and service crews) at the right location at the right time.
  - Freedom to easily administer the system anytime and anywhere.

- **Access Control for Mobile Workforce**

  - Bluetooth connectivity with an iOS or Android mobile phone allows a user to update keys (access rights) wirelessly anywhere and anytime.

- **Audit Accountability**

  - Audit information recorded in both the lock and key shows a time-and-date stamped record of every event, including authorized accesses and unauthorized attempts.
  - Customized software integration possibilities to third party solutions or with customers' own IT systems through XML/SOAP Web Services interface offered in CLIQ Intelligent Key System.

- **Physical Security**

  - Both Medeco XT and Medeco CLIQ Intelligent Key System products add a wide variety of intelligent features without compromising on physical security. Attack-resistant design and tamper-proof features provide strong protection against forced entry.

- **Reduce Costs**

  - Cost effective solutions from eliminating the need to return to the administrator to update keys or replace batteries.

  - Reduced operational costs due to use of existing hardware, easy wire-free installation, Medeco intelligent keys provide all power to the cylinder, eliminating the need for any hard wiring or power supply. Simply remove the existing mechanical cylinder and install the Medeco XT or CLIQ intelligent cylinder.

  - Access control for mobile workforce - Bluetooth connectivity with an iOS or Android mobile phone allows a user to update keys (access rights) wirelessly anywhere and anytime.

  - Reduced IT infrastructure costs due to Medeco hosted software as a service (SaaS) solution using Amazon web services (AWS) or AWS GovCloud. AWS GovCloud (US) gives vetted government customers and their partners the flexibility to architect secure cloud solutions. Medeco, has achieved ISO/IEC 27001:2013 certification, affirming that Medeco's Salem, Virginia operation adheres to the internationally-recognized standards for information security management in the production and sale of Intelligent Key (electronic locking) systems.

  - Service availability: Medeco offers 24/7, High-availability environment (SLA 99.9%, excluding planned maintenance).
    - All services are monitored 24/7
    - Optional professional support available 24/7

The CIP Compliance Solution that is Easy and Cost-Effective

We live in a world where disruptive events occur without notice. Utility security is a huge concern. The federal government has taken action and in turn, all North American power utilities must now comply with a rigid set of regulations that enforce physical security measures.

One of the most cost-effective and efficient ways a utility can meet and sustain compliance with several key NERC CIP Standards is to simply replace a vulnerable mechanical key system with a Medeco Intelligent Key System. There is no need for expensive hardwiring. It provides all the benefits of an electronic access control system without the high cost.

Medeco Intelligent Key Systems offer a significant component in a power utility's quest to dramatically lower the cost and complexity of CIP physical security compliance.

Numerous small, medium and large utility customers from the U.S.A. and Canada are using Medeco Intelligent Key solutions (CLIQ and XT) to protect and provide compliance to physical security.

For more information about Medeco Intelligent Key Systems, contact:

Andy Hummel
US Business Development Manager
Medeco Security Locks, Inc.,
andy.hummel@assaabloy.com
(919) 740-3433.

medeco
ASSA ABLOY

LT-942003-10 Rev2

ASSA ABLOY, the global leader in door opening solutions