

Securing Critical Utility Infrastructure

Medeco Intelligent Key Systems

medeco
ASSA ABLOY

ASSA ABLOY, the global leader
in door opening solutions

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources



Power Utilities Vulnerability

Medeco Intelligent Key Systems

Power Utilities Vulnerability

[FERC Overview](#)

[NERC Overview](#)

[CIP Standards](#)

[Intelligent Keys
Overview & Benefits](#)

[XT Features](#)

[XT Data Analytics](#)

[CLIQ Features](#)

[Applications & CIP
Compliance](#)

[Competitive
Comparisons](#)

[Frequently Asked
Questions](#)

[Resources](#)

The Vulnerability of Power Utilities

Utility executives and federal energy officials have long worried that power utilities are vulnerable to sabotage by both physical and cyber attacks. 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 local and even national electrical power supply and utility generation and transmission.

Unfortunately, many power utility components are often in remote, unattended locations and protected by little more than cameras and chain-link fences. As a result, there are numerous instances of equipment tampering and destruction due to the ease of accessing facilities:



London (2003) - 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.



Utah (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. Instead, they managed to cut power to nearly 4,000 homes and businesses.



Massachusetts (2006) - teenagers affected Blackstone'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 storage tank.



California (2013) - the PG&E Metcalf Transmission Substation near San Jose came under attack. Armed gunman shot up 17 electrical transformers and caused over \$15 million worth of damage. 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.



Power Utilities Vulnerability

Medeco Intelligent Key Systems

Power Utilities Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

The Vulnerability of Power Utilities: San Diego Gas & Electric



To date, the largest deployment of Medeco XT at a utility is at San Diego Gas & Electric (SDG&E).

There were two main factors that drove the sale:

SDG&E Needed A Backup System For Their EAC System

- The utility facility suffered from a power outage a few years prior and, as a result, their EAC system shut down. They were unable to access substations until power was restored. With Medeco XT, SDG&E not only has access to stations during a power outage, but also has continued audit accountability and system management.

SDG&E Wanted To Limit Exposure Of Lost Keys

- Medeco XT allows credentials to expire regularly and quickly – allowing facility managers to respond quickly to security threats, lost or stolen keys, or personnel changes.



What is FERC?

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Federal Energy Regulatory Commission (FERC)

The Federal Energy Regulatory commission, or FERC, is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. It's primary purpose is to evaluate the environmental, cultural, geological, land use, and socioeconomic aspects of construction, activities, and services related to power utilities.

Additional responsibilities include:

- Review mergers and acquisitions and corporate transactions by electricity companies
- Regulate the transmission and wholesale sales of electricity in interstate commerce
- License and inspect private, municipal, and state hydroelectric projects
- Monitor and investigate energy markets
- Enforce FERC regulatory requirements



In 2014, FERC “ordered the imposition of mandatory physical security standards (for substations)” and 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.

What is NERC?

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

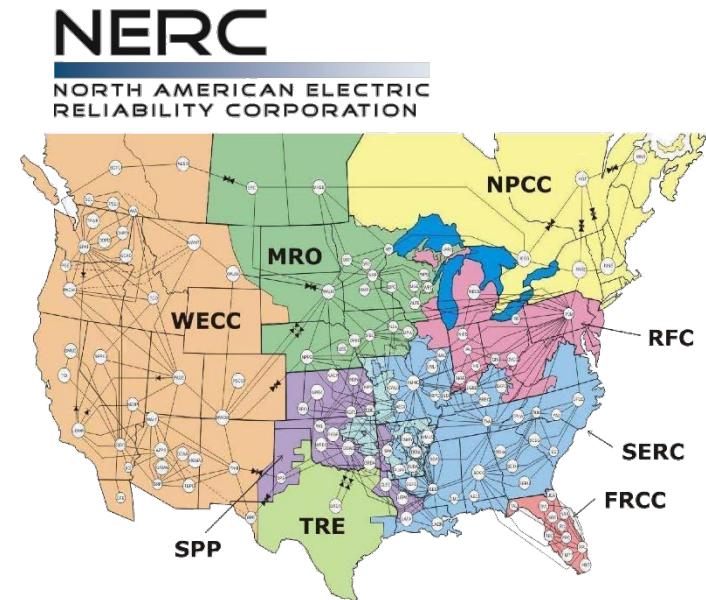
Resources

North American Electric Reliability Corporation (NERC)

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the North American bulk power system. It develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.

After the Energy Policy Act of 2005, it became the electric reliability organization for North America, meaning it is subject to oversight by FERC and has the ability to enforce standards and penalize non-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 and Bulk Electric Systems from cyber attacks.



CIP Standards

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Critical Infrastructure Protection (CIP) Standards

As the number of cyber attack incidents increase, NERC's CIP standards help protect the North American Bulk Electric system from security vulnerabilities. Of the original eight standards set by NERC, two are specific to physical security:

Standard CIP-006-3c was established to ensure the implementation of a physical security program for the protection of critical cyber assets.

Standard CIP-006-5 was established to manage physical access to Bulk Electric System cyber systems by specifying a physical security plan to protect against compromise that could lead to misoperation or instability.

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 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 ninety days.



CIP Standards

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Why Comply With CIP Standards?

NERC has the authority to levy monetary penalties and non-monetary sanctions against owners, operators, and users of the bulk electric system.

Complying with standards allow facilities to avoid fines – which can be applied for each day that a violation continues. The chart below shows the range of fines relative to the violations risk factor and severity level:

	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	\$1,000	\$3,000	\$2,000	\$7,500	\$3,000	\$15,000	\$5,000	\$25,000
Medium	\$2,000	\$30,000	\$4,000	\$100,000	\$6,000	\$200,000	\$10,000	\$335,000
High	\$4,000	\$125,000	\$8,000	\$300,000	\$12,000	\$625,000	\$20,000	\$1M



CIP Standards

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

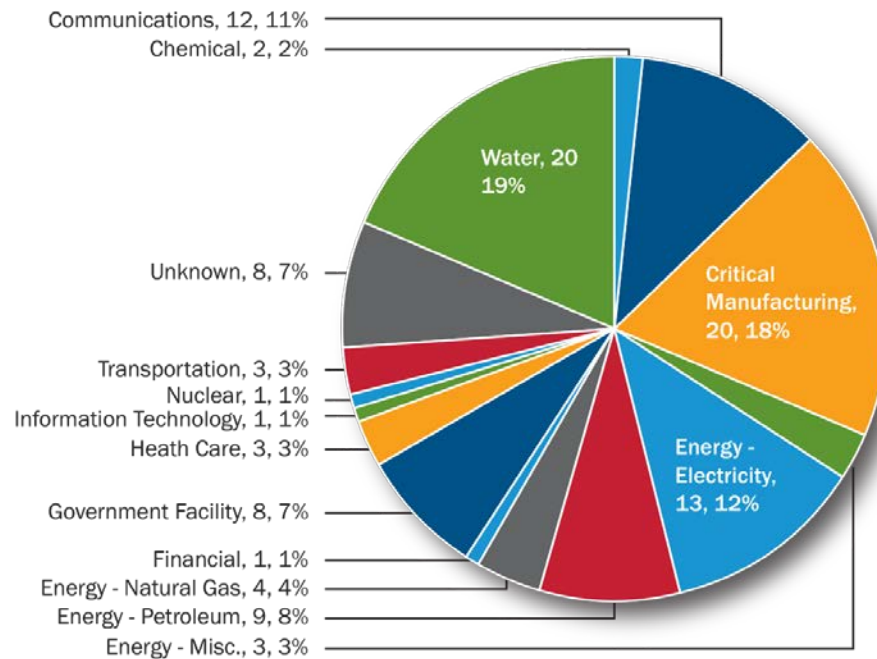
Frequently Asked
Questions

Resources

Why Comply With CIP Standards?

CIP standards help maintain the reliability of the bulk electric system from physical and cyber attacks.

- 108 cybersecurity incidents reported between October 2014 and April 2015*
- 12% energy related and 19% water related



*Source = ISC-CERT Monitor May/June 2015

Intelligent Keys Overview & Benefits

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Medeco Intelligent Key System

In response to the compliance requirements of CIP Standards 006-3c and 006-5, utilities have deployed various tactics including physical access control systems, electronic access control systems, cameras, security locks, fences, and more.

However, there is a solution that is far more efficient and effective. A utility can become complaint on many openings by simply replacing its outdated and uncontrolled mechanical master key system with a Medeco Intelligent Key System.

Controlled Access - Keys are electronically programmed to open only specific locks during a designated schedule. Schedules may also contain an expiration point to completely disable the key until it is audited and reprogrammed.

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.

Electronic Rekeying & Scheduling - Respond quickly to security threats, lost or stolen keys, or personnel changes without the added cost of changing your locks and keys.

Easy Installation - Intelligent key systems 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 ecylinder.

Physical Security - Medeco ecylinders 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.



Medeco XT Features

Medeco Intelligent Key Systems

medeco
ASSA ABLOY

ASSA ABLOY, the global leader
in door opening solutions

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Medeco XT Features

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



Uses Existing Hardware - Medeco XT key provides all power to the cylinder, eliminating the need for any hardwiring or power supply. Simply remove the existing mechanical cylinder and install the XT cylinder.



Reduce Risk of Lost Keys - Respond quickly to security threats, lost or stolen keys, or personnel changes without the added cost of changing your locks and keys.



Efficient System Management - Medeco XT software contains tools that will help you manage your security more efficiently. Flexible programming, scheduled access and full audit reports are offered with the convenience of stand-alone, network, WEB, or mobile programming options.



Unlimited Applications - Medeco XT cylinders are available to fit nearly any application or hardware type for enhanced security and accountability.



Indoor/Outdoor Use - With no outside power source, the XT system can be deployed in all interior and exterior climates - from office spaces to outside perimeters to remote access areas.



Small, Robust Key - XT electronic keys are convenient, portable, and built to withstand the toughest environments. They feature stainless steel housing and rechargeable batteries, with up to 1,800 openings per charge.



XT Data Analytics

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

XT Data Analytics

Security Analysis In Seconds

Depending on the size of the utility, thousands - perhaps millions - of data records are created by a Medeco XT Intelligent Key System on a daily or weekly basis. That information is critical, yet can be overwhelming when it comes to analysis.

Security administrators need to know at a glance, “What is out of the ordinary?” and “Who is accessing (or trying to access) specific locks and when?” Medeco XT utilizes sophisticated software called *Data Analytics* to provide immediate visual analysis, allowing administrators to quickly identify problem areas.

It immediately pinpoints the “actionable data” from all the system’s data – putting a spotlight on trends and potential security issues. This visual dashboard approach represents a huge advantage over complex data tables because it immediately illustrates important metrics for security administrators. It also provides new ways of utilizing audit data to comply with the latest CIP Standards.

The *Data Analytics* software program is without rival. In fact, it was awarded the Security Industry Association’s 2016 New Product Showcase Award for “Best Access Control Software and Controller.”



CLIQ Features

Medeco Intelligent Key Systems

medeco
ASSA ABLOY

ASSA ABLOY, the global leader
in door opening solutions

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Medeco M³ and X4 CLIQ Features

M³ & X4 CLIQ merge the flexibility of electronics with reliable mechanical technology - all in a retrofit cylinder. They offer end users audit trail, user access schedules and the ability to quickly and remotely change key authorizations. Both install with no wiring in a matter of minutes and digital keys and digital cylinders reprogram for instant changes.



Uses Existing Hardware - CLIQ intelligent key provides all power to the cylinder, eliminating the need for any hardwiring or power supply. CLIQ can be keyed in with Medeco mechanical systems featuring Medeco³ or BiLevel, Original or X4.



Reduce Risk of Lost Keys- Respond quickly to security threats, lost or stolen keys, or personnel changes utilizing expiring intelligent key validation intervals and remote programming.



Web Manager- This robust and versatile system allows administrators the ability to manage CLIQ intelligent keys and cylinders from anywhere with internet access.



Efficient System Management - CLIQ technology contains tools that will help you manage your security more efficiently. Flexible programming, scheduled access and full audit reports are offered with the convenience of web, remote, and mobile programming options.



Unlimited Applications - M³ and X4 cylinders are available to fit nearly any application or hardware type for enhanced security and accountability.



Indoor/Outdoor Use – cylinder and key are rated for -20 degrees Fahrenheit to 122 degrees Fahrenheit



Applications & CIP Compliance

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Applications & CIP Compliance

A Medeco Intelligent Key System is ideal for bringing access-control functionality to a wide variety of applications. As a simple cylinder retrofit, there is no need for costly modification or hard wiring, making it flexible enough for facilities and remote installations. The ease of installation makes this a solution worth considering for a facility quickly seeking compliance.

CIP-003-3 R1 Cyber Security Policy

The responsible entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.

Intelligent Key Systems represent technology that both controls and monitors physical access, including unsuccessful attempts. All aspects can be controlled based on level of threat, and all activity audited.

CIP-003-3 R1.1

The cyber security policy addresses the need for emergency situation provisions.

Intelligent keys can be programmed via mobile programming devices to grant extraordinary access rights in the event of an emergency. If access must be denied, programming can be applied to the cylinders to deny any or all key access.

CIP-003-3 R5: Access Control

The responsible entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

Intelligent Key Systems allow dynamic access management without burdensome infrastructure and eliminates legacy problems of lost or mis-applied keys.



Applications & CIP Compliance

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

**Applications & CIP
Compliance**

Competitive
Comparisons

Frequently Asked
Questions

Resources

Applications & CIP Compliance

CIP-003-3 R5.1

The responsible entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

Intelligent Key management allows assignment of system administrators who have well defined authority within the software, and immediate access to all key holder information and access information.

CIP-003-3 R5.2

The responsible entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the responsible entity's needs and appropriate personnel roles and responsibilities.

Unlike mechanical key systems, Intelligent Key Systems contain all access information and roles for straightforward compliance.

CIP-003-3 R5.3

The responsible entity shall assess and document at least annually the processes for controlling access privileges to protected information.

Because Intelligent Key Systems are “self-healing” when configured properly, the process for compliance can be as simple as referencing the Intelligent key system capabilities.

CIP-005-3a R1: Electronic Security Perimeter

The responsible entity shall ensure that every critical cyber asset resides within an Electronic Security Perimeter. The responsible entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

This is easily accomplished in the management software and pairs access points with audit information.



Applications & CIP Compliance

Medeco Intelligent Key Systems



ASSA ABLOY, the global leader
in door opening solutions

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

**Applications & CIP
Compliance**

Competitive
Comparisons

Frequently Asked
Questions

Resources

Applications & CIP Compliance

CIP-005 R2: Electronic Access Controls

The responsible entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s)

Easily accomplished within the software and allows rapid review and access change in the event of an unauthorized entry.

CIP-005-3a R2.1

These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

Keys can be programmed to expire quickly or, with the use of cameras for visual identification, guards can verify personnel prior to granting access.



Applications & CIP Compliance

Medeco Intelligent Key Systems

medeco
ASSA ABLOY

ASSA ABLOY, the global leader
in door opening solutions

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

**Applications & CIP
Compliance**

Competitive
Comparisons

Frequently Asked
Questions

Resources

Applications & CIP Compliance



Competitive Comparisons

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

**Competitive
Comparisons**

Frequently Asked
Questions

Resources

	Traditional EAC	Intelligent Key System ★	Other eCylinders
Easy Installation	✗	✓	✓
Key Control	✗	✓	✗
Battery Operated	✗	✓	✓
Key Security	Electronic Only	Electromechanical & Electronic	Electronic Only
Audit Trail	✓	✓	✓
Maintenance	Challenging	Easy	Moderate
Retrofit Capability	✗	✓	✓
Ergonomic Key Design	✓	✓	✗



Frequently Asked Questions

Medeco Intelligent Key Systems

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

I don't have any contact in my local utility... where should I start?

Work with your team and local channel partners. Many are probably already doing some business with local utilities. LinkedIn is another helpful tool to make a warm introduction. Also, consider getting involved with your local industry chapters, such as ASIS, to network and meet contacts.

What happens if the utility does not follow the regulations?

A utility that does not follow regulations is subject to monetary penalties and non-monetary sanctions from NERC. Fines can range anywhere from \$1,000 to \$1,000,000 per day for each day that the violation continues.

Can eCylinders be used in padlocks for utility fencing?

Yes – Medeco allows eCylinders to be incorporated into all of our padlocks, including the Protector II, G8R Series, Hockey Puck, and System Series.

Who is the decision maker within the utilities?

Each utility will be different, but it will most likely be a group consisting of a Security Director, Project Manager, Maintenance Director, etc. It is very important to ASK who will be involved in the decision making process.

Can Medeco Intelligent Keys be copied?

No, unlike traditional mechanical keys, Intelligent Keys cannot be copied.

What happens if Intelligent Keys are lost or stolen?

Electronic scheduling and rekeying allows for immediate response when keys go missing.



Resources

Medeco Intelligent Key Systems



ASSA ABLOY, the global leader
in door opening solutions

Power Utilities
Vulnerability

FERC Overview

NERC Overview

CIP Standards

Intelligent Keys
Overview & Benefits

XT Features

XT Data Analytics

CLIQ Features

Applications & CIP
Compliance

Competitive
Comparisons

Frequently Asked
Questions

Resources

Medeco Website

XT: <http://www.medeco.com/en/site/medeco/technology/ecylinder/medeco-xt1/>

XT Data Analytics: <http://www.medeco.com/en/site/medeco/technology/ecylinder/medeco-xt1/medeco-xt3/>

M3 and X4 CLIQ: <http://www.medeco.com/en/site/medeco/technology/ecylinder/medeco3-cliq1/>

Classic CLIQ: <http://www.medeco.com/en/site/medeco/technology/ecylinder/medeco-cliq/>

Online Brochures



Videos

XT Product Overview: <https://www.youtube.com/watch?v=61cLVPclsd0>

XT Data Analytics Tutorial: <https://www.youtube.com/watch?v=UV1sFZwFl08>

