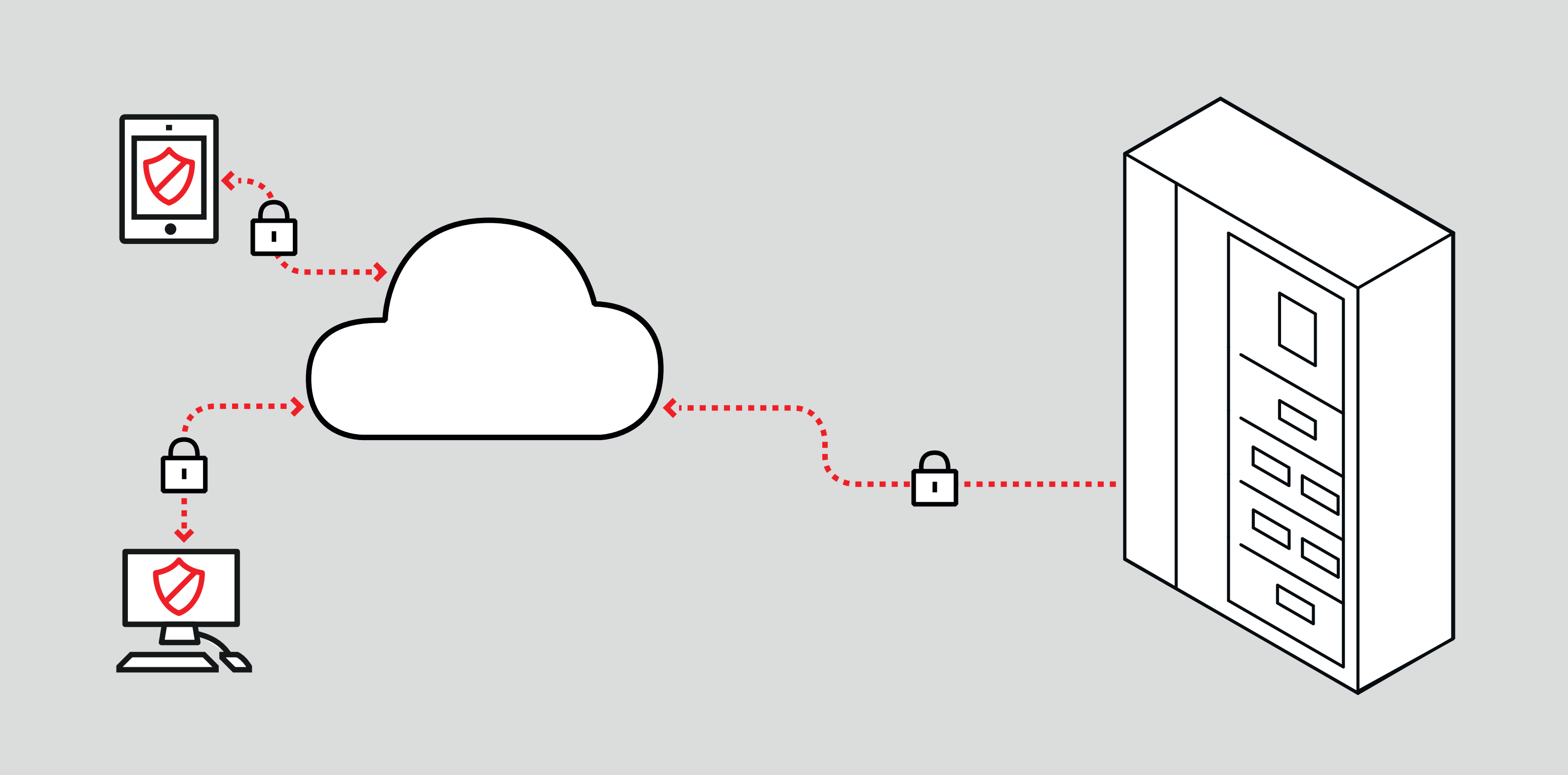
CONNECTIVITY

How to tackle Cyber Security

ABB Ability™ Electrical Distribution Control System



We are getting more and more interconnected in our human digital experience over the internet, as well as our things and devices are.

This applies also to the “industrial” components, with great benefits in terms of remote visibility and performance analytics.

Due to the growing use of automation and supervision systems for plants, buildings and industrial processes, the implementation of communication networks is everyday more and more important to retrieve insights from the data available in the electrical system.

These data could be crucial for an energy management or asset management solution.

Moreover, being connected has become a crucial challenge in the actual days strongly influenced by the trend of Industry 4.0. Internet of Things, micro-grid and big data are the key features to make this challenge a concrete opportunity.
On the other hand, this may increase the exposure to cyber threats.

What is Cyber Security

Cyber Security = Risk management

- There is no such thing as 100% or absolute security
- Cyber Security is not a destination but an evolving target – it is not a product but a dynamic process
- Cyber Security is all about risk management

Cyber Security in power automation

Modern automation, protection and control systems are highly specialized IT systems:

- Leverage commercial off-the-shelf IT components
- Use standardized, IP-based communication protocols
- Are distributed and highly interconnected
- Use mobile devices and storage media
- Are based on software (> 50% of the ABB offering is software-related)

Cyber Security issues

- Increased attack surface as compared to older, isolated systems
- Communication with external (non-OT) systems
- Attacks from/over the IT world

We are getting more and more interconnected in our digital experience, as well as our things and devices are. This applies also to industrial components, increasing the exposure to cyber threats. Cyber attackers target to acquire personal or sensible information and hack systems with the goal to get economical, political or military advantages.
Even a stand alone or isolated system cannot be defined as 100% secure. Let's think about software updates or new software installations: such things could result in exposures for the system.
We have to consider Cyber Security as a risk management procedure, since we must be aware of the threats of cyber attacks and put in place all the mitigation activities and implementations in order to prevent any harm: a continuous monitoring and prevention of vulnerability.

Cyber Security threats

Intentional attacks

Together with the use of standard internet technologies, you get also standard internet threats-viruses and hackers.
These are the new threats to which industrial control systems have not been historically exposed.

9.4%
of security threats come from **hackers** and **terrorists**

10.6%
of security threats come from **insiders**

HACKERS TERRORISTS INSIDERS

Unintentional

Scarily, most Cyber Security threats and incidents are unintentional and occur in industrial networks.

11.2%
of security threats come from **human error**

30.4%
of security threats come from **malware**

38.4%
of security threats come from **device and software failures**

HUMAN ERROR MALWARE DEVICES

ABB response

Our digital solutions have historically been deployed on premises, with offerings started “at the edge”. Today, this is increasingly being called “fog-computing” (because fog, unlike the cloud, is closer to the ground).

ABB has extensive experience in building mission-critical automation systems that reside onsite. Many of our systems are now being extended with a connection to our cloud-based ABB Ability™ platform.

ABB Ability™ refers to both a set of industry digital solutions and the platform that they are built on. We deliver these industry solutions in our 3 key markets: utilities, industry and transportation & infrastructure.

The ABB Ability™ platform is a set of technologies that enables ABB to build these solutions more quickly and efficiently.

We are building the platform from best-in-class industry technologies, such as Microsoft Azure cloud services, IBM Watson machine learning and AI, and SAP HANA’s big-data query tools.

Cloud technology offers the chance to significantly increase the scalability and flexibility of developments and maintenance in any new solution, while enhancing the global reach toward legacy and on premise systems.
Furthermore, data can be accessed by their authenticated and authorized owners from wherever they are and whenever they need.

Securing industrial systems is more challenging than protecting laptops or mobile phones.
In addition to securing communications and data, we need to make sure that programs cannot be tampered with.
We need to protect devices as they start up (boot), make sure that software updates come from reputable sources and have not been altered and that we can detect and deal with threats as they happen.

ABB Ability™: security, data and IP

Making solutions and data safe for mission-critical applications

We secure your systems:

Secure operations

Threat detection

Secure communications

Secure updates

Secure boot

ABB cybersecurity standards

You own your data:

Identity

Measurement data

You know what we do with your data

We only share data with your consent

ABB IoT data manifesto

ƒ (x)=$

You own your IP:

No loss of intellectual property when using ABB Ability™ solutions

ABB intellectual property position

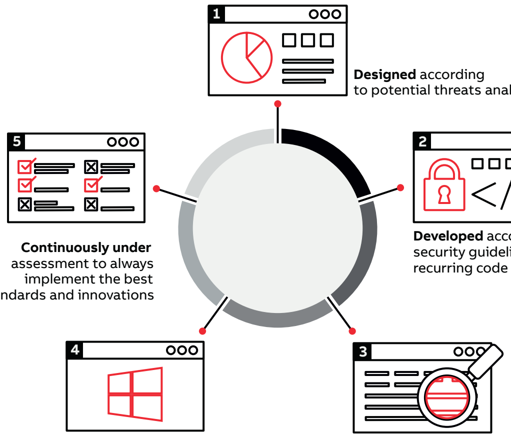
Data coming from our customer’s facilities is valuable and it should not go to others without their informed consent.

ABB Ability™ solutions ensure that the customers own their data and the IP of their systems even when ABB solutions are deployed.

The case of ABB Ability™ Electrical Distribution Control System
ABB Ability™ Electrical Distribution Control System is the innovative cloud-computing platform designed to monitor, optimize, control and predict the condition of the electrical system.

It is built on a state-of-the-art cloud architecture for data collection, processing and storage.
ABB Ability™ cloud architecture has been developed together with Microsoft in order to enhance performance and guarantee the highest reliability and security.

Thanks to ABB, Microsoft and an expert partner on IT security,
ABB Ability™ EDCS can guarantee state-of-the-art cybersecurity as it is:



Designed according to potential threats analysis

Developed according to security guidelines and recurring code review

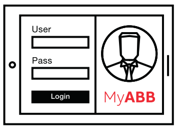
Validated by penetration tests to verify robustness

Relayed on Microsoft Azure cloud platform security policy

Continuously under assessment to always implement the best standards and innovations

ABB Ability™ EDCS
main pillars for Cyber Security

Identity

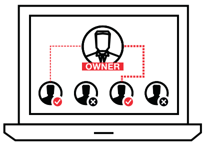


Authentication via unique **MyABB account**

Security

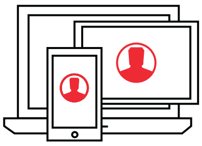
Encrypted communication channel, using the same protocol as banking and other important applications

Privacy



Only the owner has initial access to data and can profile other users' role

Digital Signature

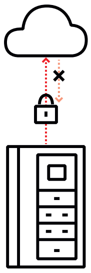


Each connected device is **uniquely identified**

End-to-end process

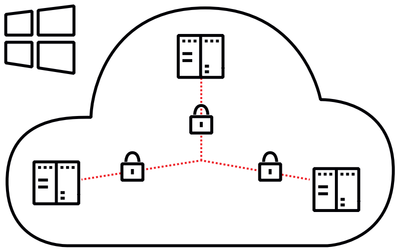
Device to cloud

- **Whitelist** for unique identification
- **Local** commissioning
- **No commands**
- **Encrypted** communication channel



In the cloud

- Microsoft **Azure** security
- Data storage in certified **data-centers** with state-of-the-art cyber security standards
- **Encrypted** communication channel



From the browser

- Unique **authentication** via ABB SSO
- Access to data only upon **authorization**
- **No commands**
- **Encrypted** communication channel

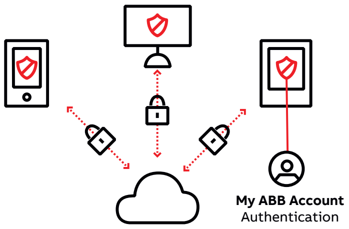


ABB SACE
A divison of ABB S.p.A.
L.V. Breakers
Via Pescaria, 5
24123 Bergamo - Italy
Phone: +39 035 395.111
Fax: +39 035 395.306-433
abb.com/lowvoltage

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.