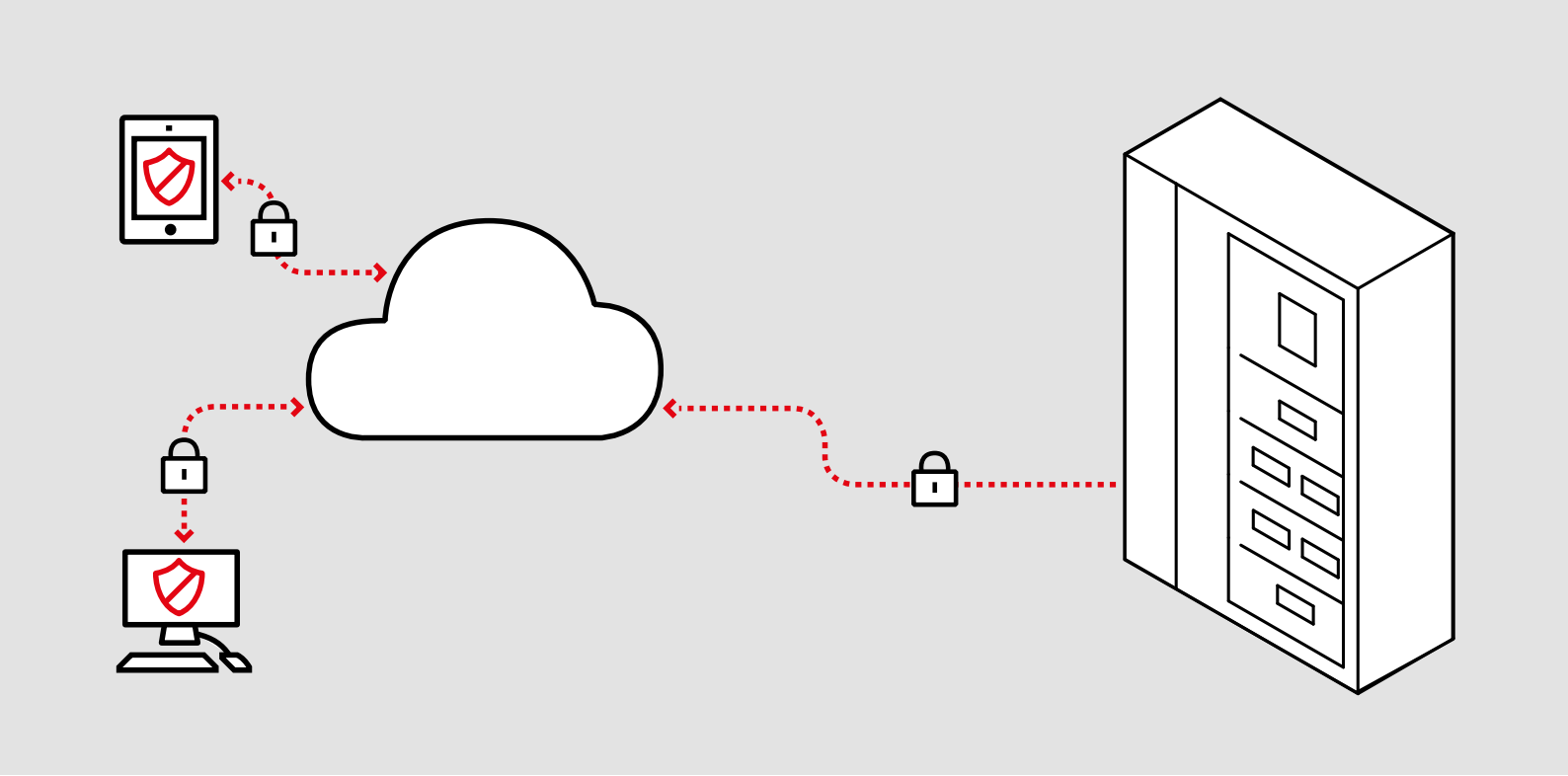
KONNEKTIVITÄT

Wie man Cyber Security angeht

ABB Ability™ Electrical Distribution Control System



Wir, unsere Dinge und Geräte werden über das Internet immer mehr vernetzt. Unsere digitale Erfahrung wird zunehmend grösser.

Dies gilt auch für die «industriellen» Komponenten und bringt grosse Vorteile für die Darstellung und Überwachung aus der Ferne, sowie eine performante Analyse der vorhandenen Infomationen.

Durch den zunehmenden Einsatz von Automatisierungs- und Überwachungssystemen für Anlagen, Gebäude und industrielle Prozesse wird die Implementierung von Kommunikationsnetzwerken zunehmend wichtiger, um Erkenntnisse aus den verfügbaren Daten des elektrischen Systems zu gewinnen.

Diese Daten können entscheidend sein für eine optimale Verwaltung des Energieverbauchs und der physischen Anlagen.

Darüber hinaus ist die Vernetzung, geprägt durch den Trend der Industrie 4.0, zu einer entscheidenden Herausforderung geworden. Das Internet der Dinge, Mikronetze und Big Data sind die Schlüsselmerkmale, die diese Herausforderung zu einer echten Chance machen. Andererseits kann dies die Teilnehmer der Internet der Dinge einer erhöhten Bedrohung durch Cyber-Angriffe aussetzen.

Was ist Cyber Security?

Cyber Security = Risikomanagement
- Es gibt keine 100%ige oder absolute Sicherheit
- Cyber Security ist kein Ziel oder Produkt, sondern ein dynamischer Prozess
- Bei Cyber Security dreht sich alles um das Risikomanagement

Cyber Security in der Energieautomatisierung
Moderne Automatisierungs-, Schutz- und Prozessleitsysteme sind hochspezialisierte IT-Systeme:
- Einsatz kommerzieller Standard-IT-Komponenten
- Verwendung standardisierter, IP-basierter Kommunikationsprotokolle
- Sind verteilt und stark vernetzt
- Verwendung mobiler Geräte und Speichermedien
- Sind softwarebasiert (> 50 % des ABB-Angebots basieren auf Softwarelösungen)

Probleme in der Cyber Sicherheit
- Erhöhte Angriffsfläche im Vergleich zu älteren, isolierten Systemen
- Kommunikation mit externen (Nicht-OT-)Systemen
- Angriffe aus der/über die IT-Welt

Wir, unsere Dinge und Geräte werden immer mehr vernetzt, unsere digitale Erfahrung wird zunehmend grösser. Das gilt auch für industrielle Komponenten, die Cyber-Bedrohungen stärker ausgesetzt werden. Cyber-Angreifer zielen darauf ab, persönliche oder sensible Informationen zu beschaffen und Systeme zu hacken, mit der Absicht, sich wirtschaftliche, politische oder militärische Vorteile zu verschaffen.
Selbst ein eigenständiges oder isoliertes System kann nicht als 100 % sicher definiert werden: Während der Installation oder neuer Updates ist dieses System gewissen Cyber-Bedrohungen ausgesetzt.
Cyber Security sollte als ein Verfahren im Risikomanagement betrachten werden, denn wir müssen uns der Bedrohungen durch Cyberangriffe bewusst sein und alle verfügbaren Massnahmen und Werkzeuge zur Schadensbegrenzung implementieren: also eine kontinuierliche Überwachung sicherstellen und Schwachstellen vermeiden.

Bedrohungen in der Cyber Security

Absichtliche Angriffe

Mit den standardmässigen Internettechnologien erfolgen auch standardmässig Bedrohungen und zwar in Form von Viren und Hacker-Angriffen.
Dies sind die neuen Bedrohungen, denen industrielle Prozessleitsysteme in der Vergangenheit nicht ausgesetzt waren.

9,4 %
der Sicherheitsbedrohungen gehen von **Hackern** und **Terroristen**aus

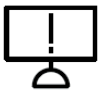
10,6 %
der Sicherheitsbedrohungen gehen von **Insidern**aus

HACKER | TERRORISTEN | INSIDER

Unbeabsichtigt

Die Sicherheitsbedrohungen und Vorfälle im Cyber-Bereich sind erschreckenderweise unbeabsichtigt und treten in industriellen Netzwerken auf.

11,2 %
der Sicherheitsbedrohungen resultieren aus **menschlichem Versagen**



30,4 %
der Sicherheitsbedrohungen gehen von **bösartiger Software** aus

38,4 %
der Sicherheitsbedrohungen kommen von **Geräte- und Softwarefehlern**

MENSCHLICHES VERSAGEN | MALWARE | GERÄTE

Antwort von ABB
Unsere digitalen Lösungen werden seit jeher lokal vor Ort («on premise») eingesetzt, wobei wir zunächst mit Angeboten «am Rand des Netzwerks», der so genannten Edge angefangen haben.
Heute wird dies zunehmend als «Fog Computing» bezeichnet (weil «Fog», also Nebel, im Gegensatz zur «Cloud», also Wolke, näher am Boden, also am Rand der Cloud liegt).

ABB verfügt über umfangreiche Erfahrung im Aufbau unternehmenskritischer Automatisierungssysteme, die sich vor Ort befinden. Viele unserer Systeme werden nun mit einer Verbindung zu unserer cloudbasierten ABB-Plattform Ability™ erweitert.

ABB Ability™ bezieht sich sowohl auf eine Reihe von digitalen Branchenlösungen als auch auf die Plattform, auf der sie aufgebaut sind.
Wir bieten diese Branchenlösungen in unseren drei Hauptmärkten an: Versorgungsunternehmen, Industrie sowie Transport und Infrastruktur.

Die Plattform ABB Ability™ umfasst eine Reihe von Technologien, mit denen ABB diese Lösungen schneller und effizienter entwickeln kann.
Die Plattform ist auf branchenführenden Technologien aufgebaut und nutzt unter anderem Microsoft Azure als Clouddienst, Watson von IBM für maschinelles Lernen und KI und die Big Data-Abfragetools von SAP HANA.

Die Cloudtechnologie bietet die Möglichkeit, die Skalierbarkeit und Flexibilität von Entwicklung und Wartung in jeder neuen Lösung deutlich zu erhöhen und gleichzeitig die globale Reichweite von veralteten und lokal installierten Systemen zu erhöhen.
Darüber hinaus können authentifizierte und autorisierte Eigentümer von überall und zu jeder Zeit auf ihre Daten zugreifen.

Das Sichern industrieller Systeme ist anspruchsvoller als der Schutz von Laptops oder Mobiltelefonen.
Neben der Sicherung von Kommunikation und Daten müssen wir ausserdem sicherstellen, dass Programme nicht manipuliert werden können.
Wir müssen die Geräte beim Start (Boot) schützen.
Wir müssen sicherstellen, dass Software-Updates von seriösen Quellen stammen und nicht verändert wurden und dass wir Bedrohungen erkennen und behandeln können, sobald sie auftreten.

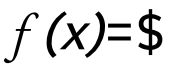
ABB Ability™: Sicherheit, Daten und IP
Lösungen und Daten für geschäftskritische Anwendungen sicher machen

Wir schützen Ihre Systeme:
Sicherer Betrieb
Bedrohungserkennung
Sichere Kommunikation
Sichere Updates
Sicherer Start

Cybersicherheit nach ABB-Standards

Die Daten gehören Ihnen:
Identität
Messdaten
Sie wissen, was wir mit Ihren Daten machen
Wir geben Daten nur mit Ihrer Zustimmung weiter

ABBs IoT-Datenmanifest



Die IP gehört Ihnen:
Kein Verlust des geistigen Eigentums bei der Nutzung der Lösungen von ABB Ability™

ABBs Position im Bereich geistigen Eigentums

Daten, die von den Einrichtungen unserer Kunden stammen, sind wertvoll und sollten nicht ohne deren informierte Einwilligung an andere weitergegeben werden.

Die Lösungen von ABB Ability™ stellen sicher, dass Kunden auch dann Eigentümer ihrer Daten und der IP ihrer Systeme bleiben, wenn Lösungen von ABB eingesetzt werden.

ABB Ability™ Electrical Distribution Control System – Fallbeschreibung

Das ABB Ability™ Electrical Distribution Control System EDCS ist die innovative Cloud-Computing-Plattform zur Überwachung, Optimierung, Kontrolle und Vorhersage des Zustands elektrischer Systeme.

Es basiert auf einer hochmodernen Cloudarchitektur für die Datenerfassung, -verarbeitung und -speicherung. Die Cloudarchitektur von ABB Ability™ wurde gemeinsam mit Microsoft entwickelt, damit die Leistung gesteigert und höchste Zuverlässigkeit und Sicherheit gewährleistet werden kann.

Dank ABB, Microsoft und einem kompetenten Partner für IT-Sicherheit kann **ABB Ability™ EDCS** modernste Cybersicherheit garantieren:

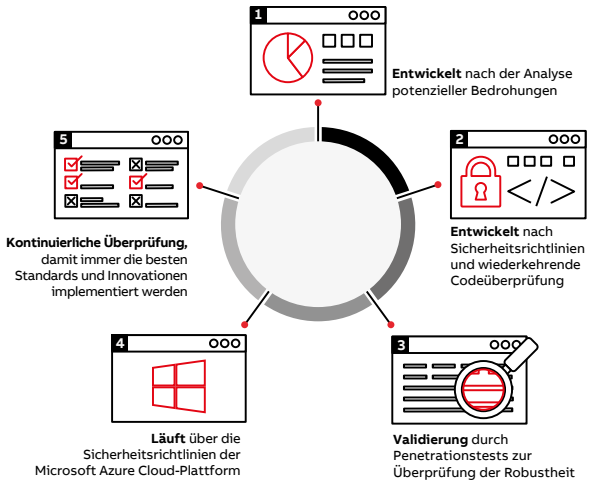
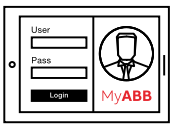


ABB Ability™ EDCS

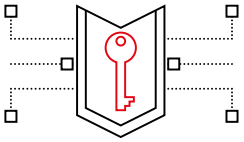
Grundpfeiler für die Cyber Security

Identität



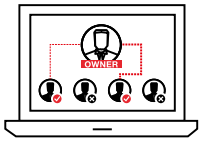
Authentifizierung über ein eindeutiges **MyABB-Konto**

Sicherheit



Verschlüsselter Kommunikationskanal, mit dem gleichen Protokoll wie bei Banken und anderen wichtigen Anwendungen

Datenschutz



Nur der Eigentümer kann auf die Daten initial zugreifen und die Rollen anderer Benutzer mit einem Profil versehen

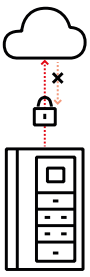
Digitale Signatur

Jedes angeschlossene Gerät ist **eindeutig identifiziert**

End-to-End-Prozess

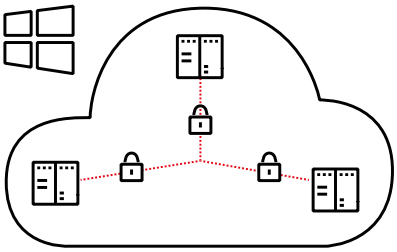
Gerät zu Cloud

- **Whitelist** zur eindeutigen Identifizierung
- Inbetriebnahme **vor Ort**
- **Keine Befehle**
- **Verschlüsselter** Kommunikationskanal



In der Cloud

- Microsoft Azure-Sicherheit
- Datenspeicherung in zertifizierten **Rechenzentren** mit modernsten Cyber Security-Standards
- **Verschlüsselter** Kommunikationskanal



Über den Browser

- Eindeutige **Authentifizierung** über ABB Single-Sign-On
- Zugriff auf die Daten nur nach erfolgreicher **Autorisierung**
- **Keine Schaltbefehle**
- **Verschlüsselter** Kommunikationskanal

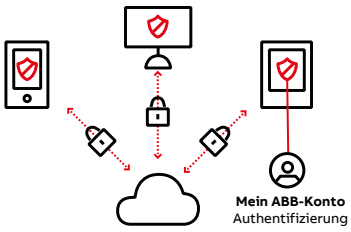


ABB Schweiz AG
Electrification
Bruggerstrasse 66
CH-5400 Baden
Tel. +41 58 586 00 00
Fax +41 58 586 06 01

ABB Suisse SA
Electrification
Rue du Sablon 2-4
CH-1110 Morges
Tél. +41 58 588 40 50
Fax +41 58 588 40 95

solutions.abb/ch-tmax-xt

9AKK107680A7153 – Mai 2020