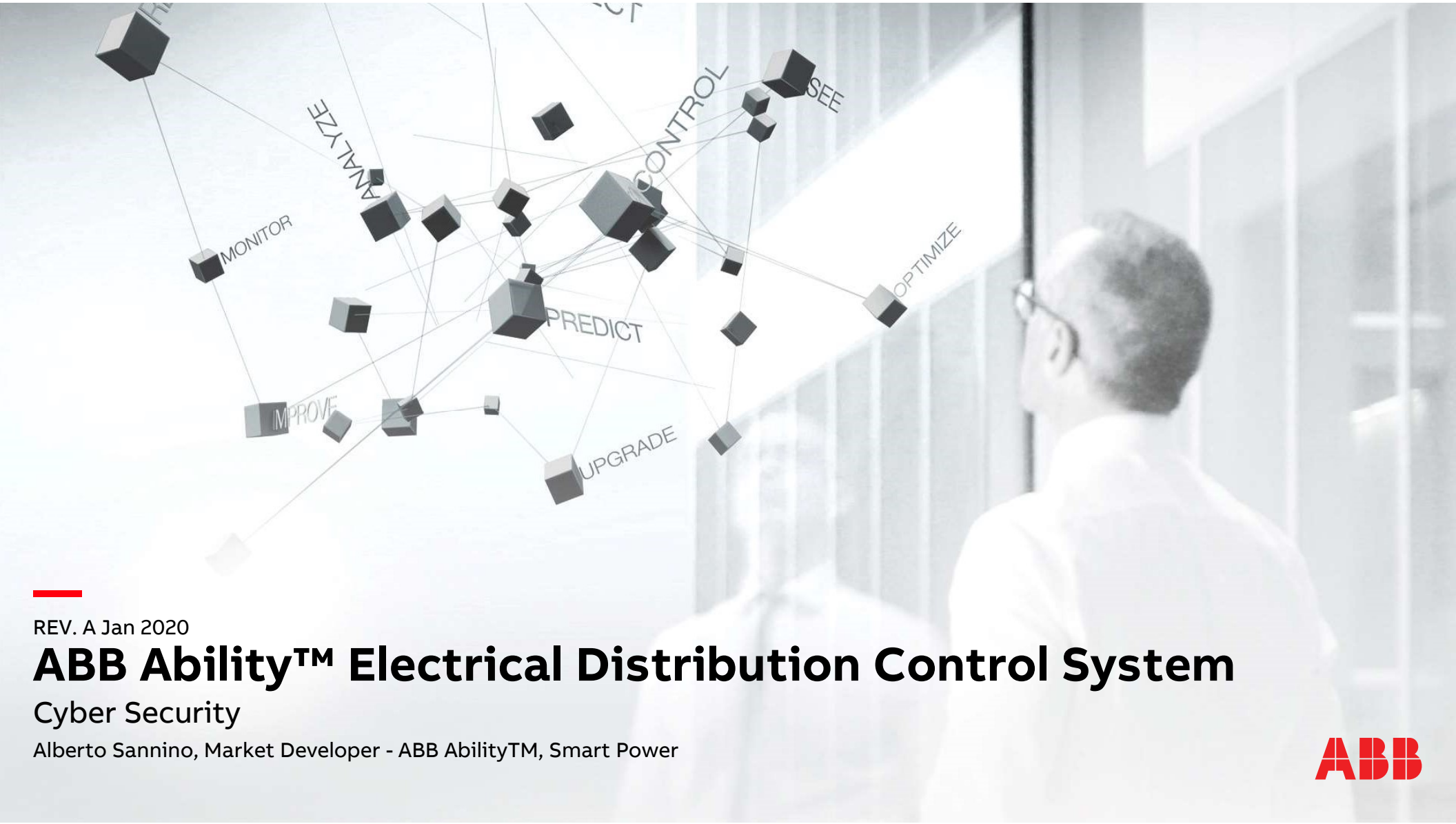


REV. A Jan 2020

ABB Ability™ Electrical Distribution Control System

Cyber Security

Alberto Sannino, Market Developer - ABB AbilityTM, Smart Power

Digital Megatrends

Mobility

Pervasive and affordable communication
Remote access
User-driven interfaces

Connectivity

Within 2020, over 33bn devices will be conntected worldwide
Strategy Analytics Study

Cloud

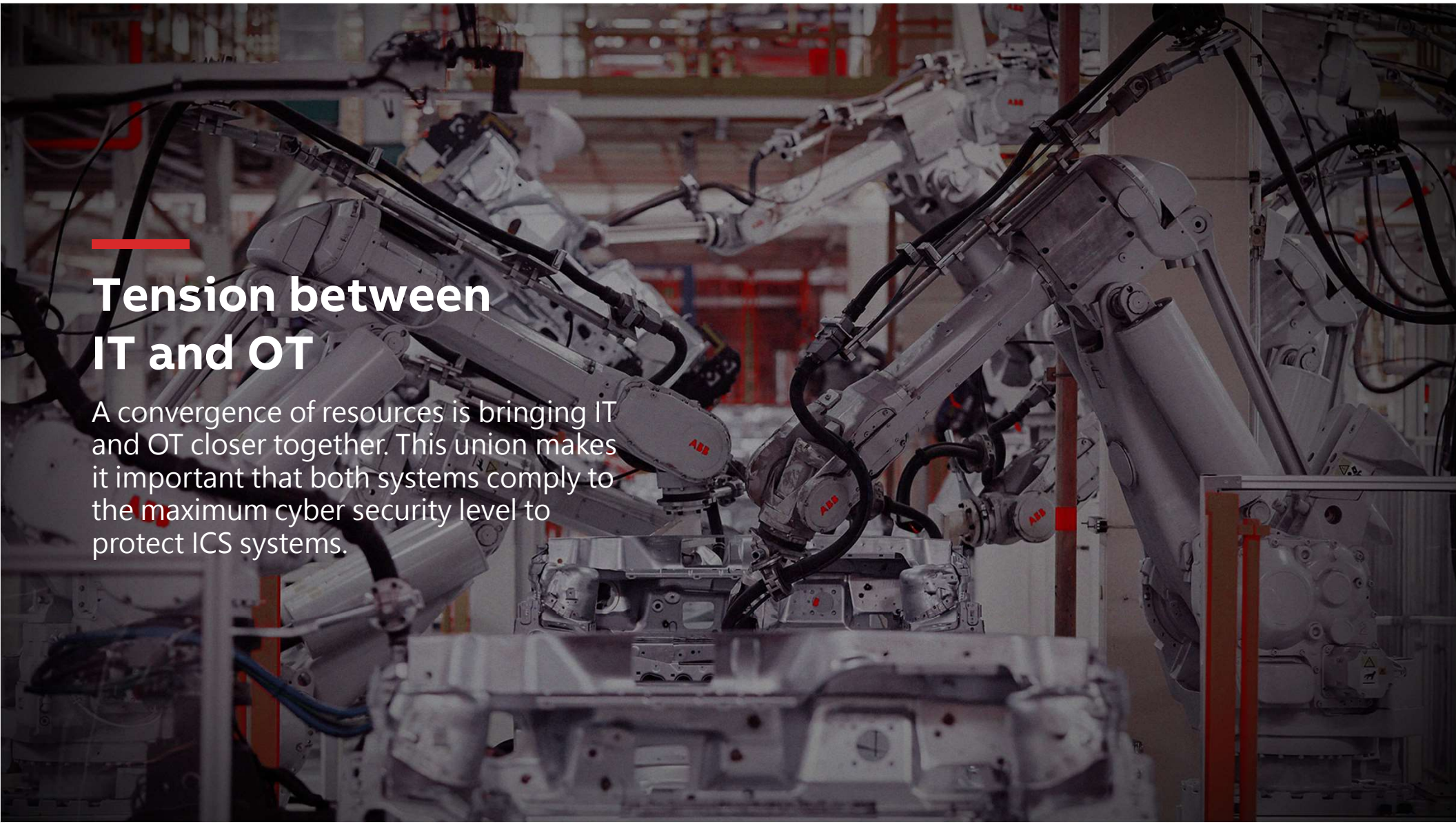
Massive aggregation of data
Data access by specialists
Industrial application developer ecosystem

Analytics

Cognitive applications
Artificial intelligence optimizing performance at all levels

Growth in IIoT connected devices creates opportunity – and risks.

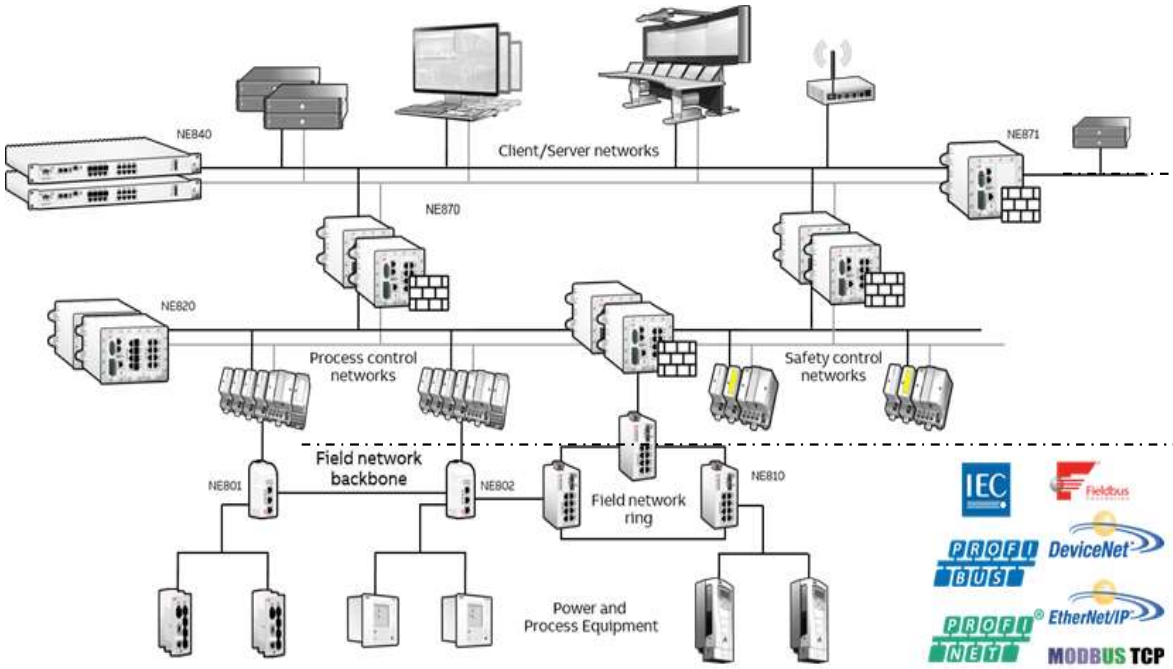
Cyber Security is everywhere



Tension between IT and OT

A convergence of resources is bringing IT and OT closer together. This union makes it important that both systems comply to the maximum cyber security level to protect ICS systems.

Cyber Security
In Power and Automation



General enterprise network protocols

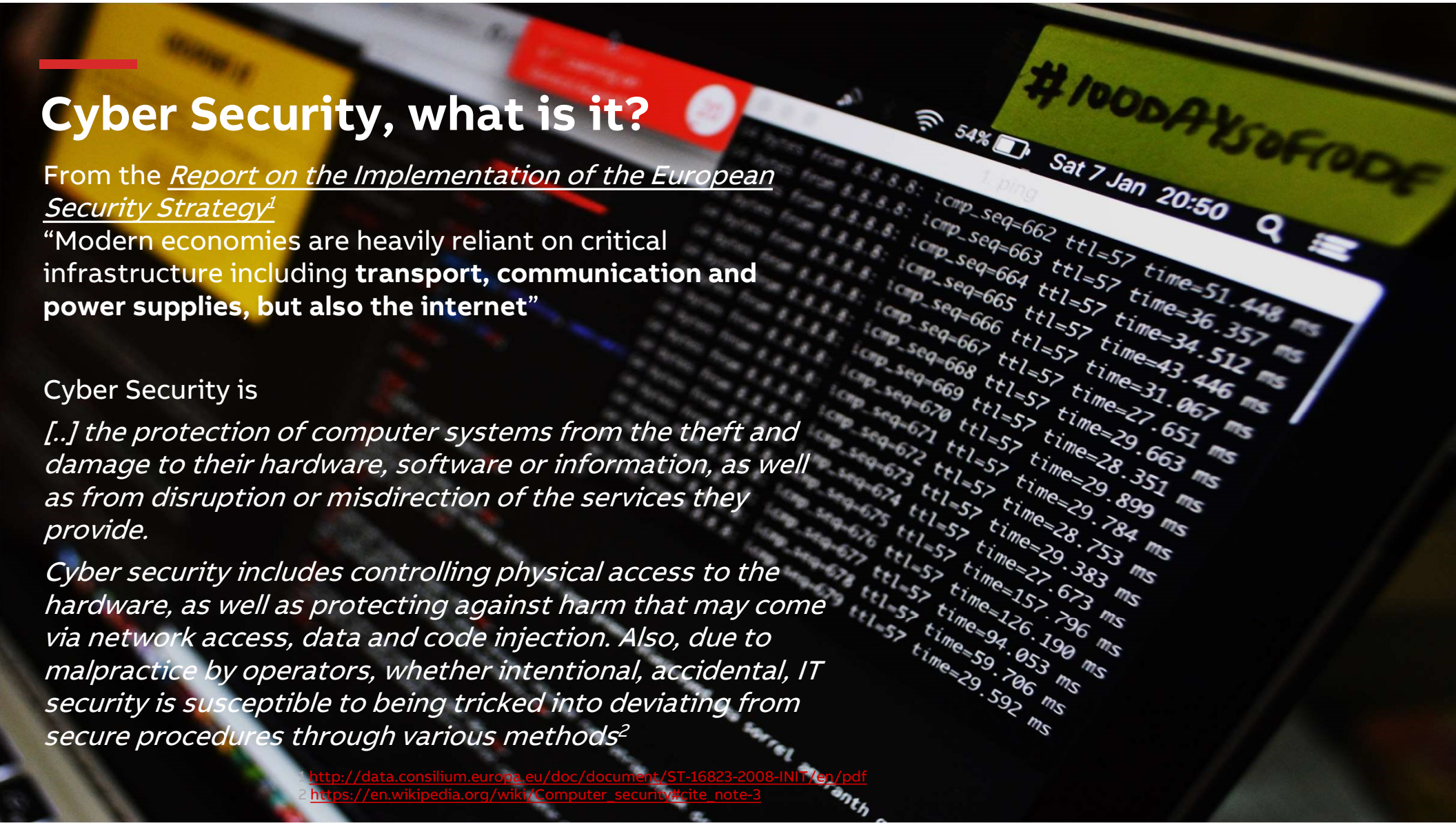
- DNS, DHCP,
- SMTP, HTTP, SMB

IP-based autotmation protocols

- OPC, Modbus/TCP, KNXnet/IP, IEC 61850 MMS

Ethernet-based fieldbus protocols

- Modbus TCP, PROFINET, EtherCAT, IEC 61850 SV, IEC 61850 GOOSE



Cyber Security, what is it?

From the *Report on the Implementation of the European Security Strategy*[1]
"Modern economies are heavily reliant on critical infrastructure including **transport, communication and power supplies, but also the internet**"

Cyber Security is

[..] the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. Also, due to malpractice by operators, whether intentional, accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods[2]

1 http://data.consilium.europa.eu/doc/document/ST-16823-2008-INIT/en/pdf
2 https://en.wikipedia.org/wiki/Computer_security#cite_note-3

Cyber Security

Threats

Intentional

With the use of standard internet technologies also come standard internet threats-viruses and hackers.
These are new threat sources to wich industrial control systems have historically not been exposed.

9.4%
of Security Threats come from **Hackers** and **Terrorists**

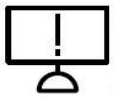
10.6%
of Security Threats come from **Insiders**

HACKERS | TERRORISTS | INSIDERS

Unintentional

Scarily, most cyber security threats and incidents are unintenional and occur 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 Failure**

HUMAN ERROR | MALWARE | DEVICES

Source: Industrial Internet Consortium www.iiconsortium.org/wc-security

What ABB does for Cyber Security applied to EDCS

Cyber Security @ ABB

Group Cyber Security Council and Cyber Security Organization

PUBLIC

ABB Group Cyber Security Council

Core Team

- Electrification
- Industrial Automation
- Motion
- Power Grids
- Robotics & Discrete Automation
- Digital ABB
- Cyber Security Program Management

Extended Team

IS security

Legal

Communication

Corporate security

Insurance risk management

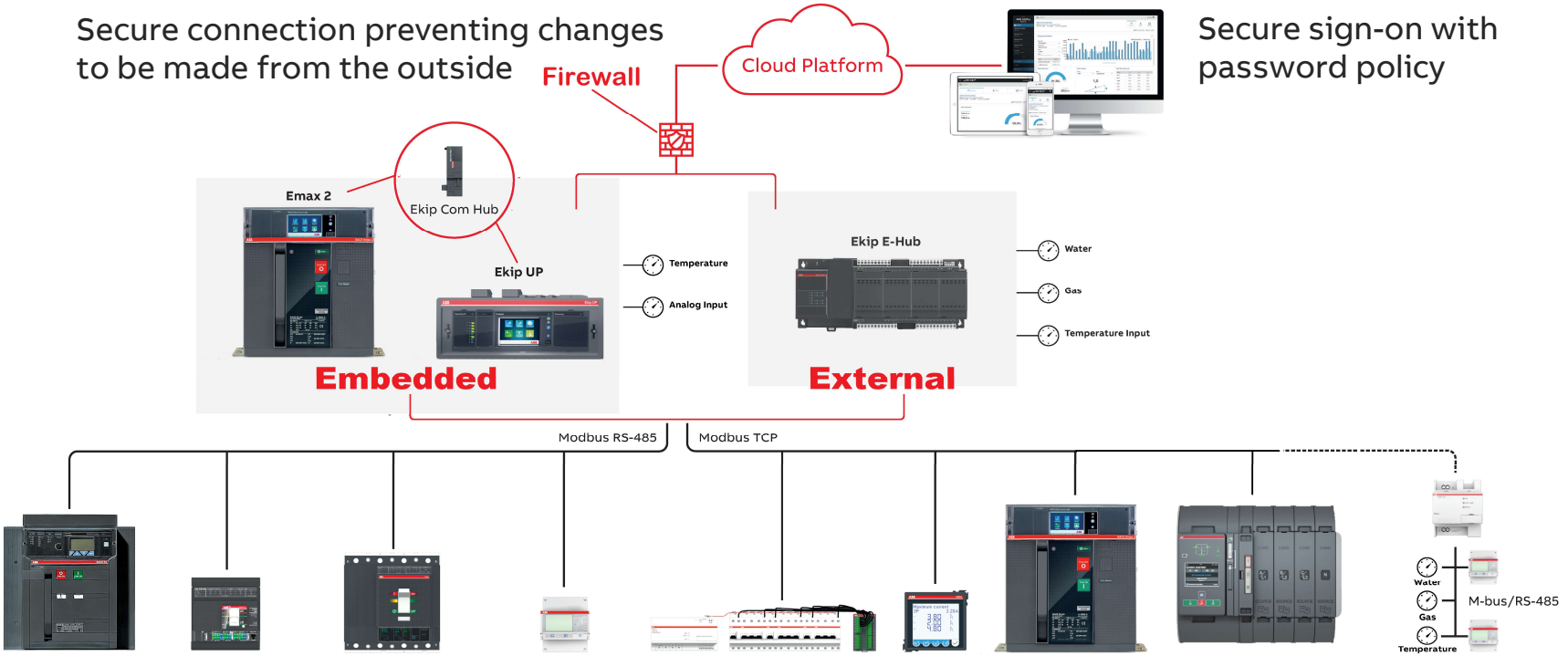
HR

- ABB Group Cyber Security Council: https://go.insideplus.abb.com/cybersecurity/groupcouncil
- Cyber security organization: https://go.insideplus.abb.com/cybersecurity/organization

Electrical Distribution Control System

A quick overview

Secure connection preventing changes to be made from the outside



Secure sign-on with password policy

Only the devices you choose to monitor send data to the cloud. You are therefore in control of the data getting sent

Cyber Security

The CIA Triad, what about EDCS?

Confidentiality

- Data is transmitted to and from the cloud through encrypted channels. No one is able to sniff the exchanged data
- EDCS portal implements proper authentication and authorization controls in order to restrict access to authorized entities only
- Azure storage services rely on cryptography to store data in a secure way
- Certificate validation ensures that data is sent only to ABB services

Integrity

- Data is checked for corruption and stored with redundancy
- Firmware is digitally signed by ABB to ensure field devices can install only genuine software

Availability

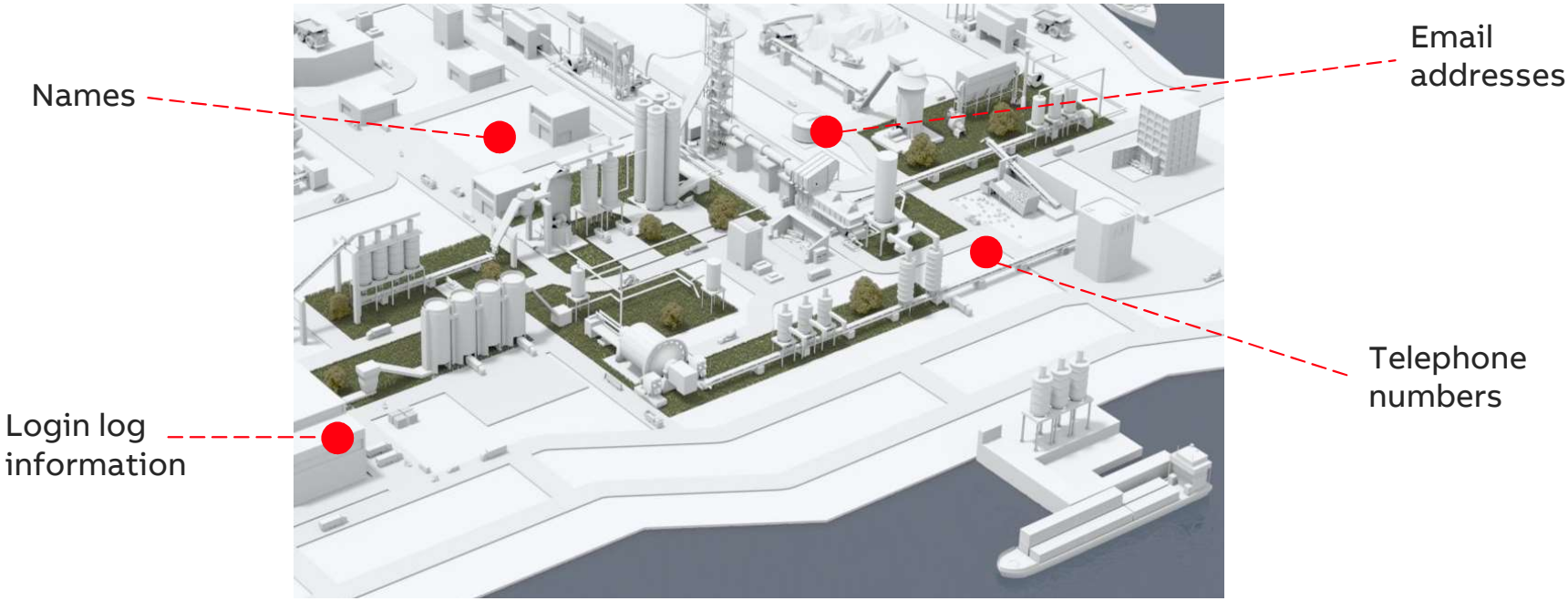
- Data redundancy
- Auto scaling allows services to expand the resources depending on the actual needs
- Microsoft Azure DDoS Protection

ABB adopted different solutions and strategies to implement the CIA paradigm

©ABB

ABB Ability is committed to complying with its obligations under the GDPR

PERSONAL DATA COLLECTED BY SUBPROCESSORS



HOSTING SERVICES SUBPROCESSORS: Microsoft Azure

©ABB

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

You own your IP:

$$f(x)=\$$$

No loss of intellectual property when using ABB Ability™ solutions

ABB intellectual property position

Azure Platform

Strong partner to ensure data security

Microsoft Azure is a public cloud service platform that supports:

- ISO27001 certified
- A broad selection of operating systems, programming languages, frameworks, tools, databases, and devices
- Three types of Storage (blob storage, azure storage, document DB)
- Azure Monitor: a feature to monitor the resources part of the subscription for performance and health
- Azure DDoS protection
- Azure Firewall
- Azure networking

©ABB

ABB Ability™ Electrical Distribution Control System

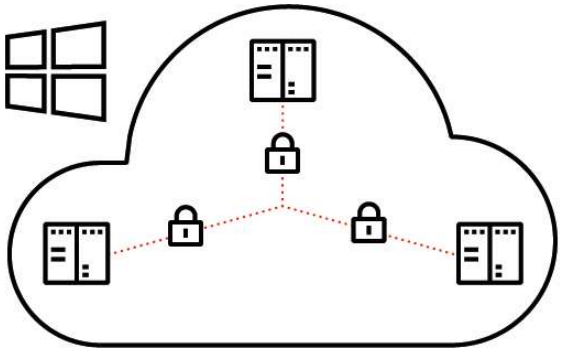
End-to-end process

Device to cloud

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

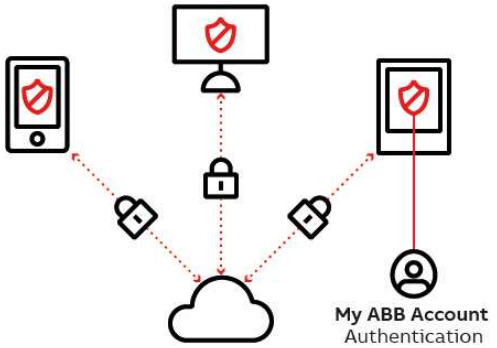
In the cloud

- Microsoft **Azure** security → link
- 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

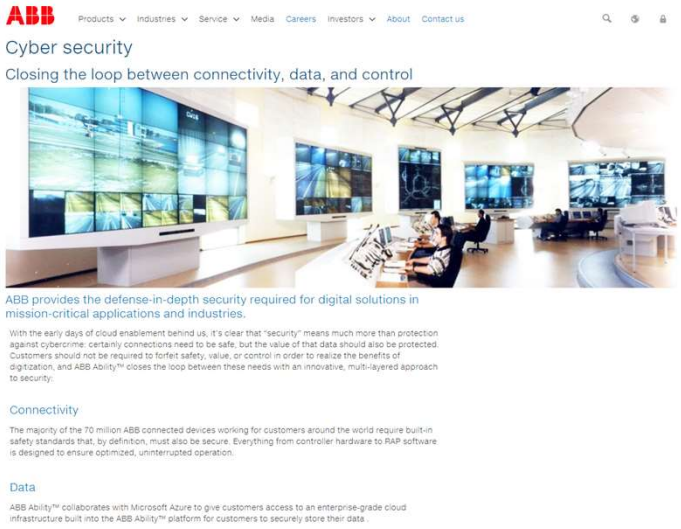


©ABB

External Cyber Security Portal

PUBLIC

Cyber Security portal	https://www.abb.com/cybersecurity
Alerts and Notifications	https://new.abb.com/about/technology/cyber-security/alerts-and-notifications
Supplier requirements	https://new.abb.com/about/supplying/cyber-security
Contacts	Group email: cybersecurity@ch.abb.com



ABB