Bart de Wijs, Head of Cyber Security, ABB Power Grids

Cyber-Physical Security and Resilience in SmartGrid

Cyber Security Landscape from a vendor’s perspective

Guiding principles

Reality	There is no such thing as 100% or absolute security
Process	Cyber security is not destination but an evolving target – it is not a product but a process
Balance	Cyber security is about finding the right balance – it impacts usability and increases cost

Cyber security is all about risk management

Cyber Security
A definition ***in the context of power and automation technology***

Traditional

*Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack**

Power and automation technology

Measures taken to protect the reliability, integrity and availability of power and automation technologies against unauthorized access or attack

*Merriam-Webster's dictionary

Cyber security in power and automation

Why is cyber security an issue?

Power and automation today

- 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
  - Based on software (> 50% of ABB offering is software-related)

Cyber security issues

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

Attacks are real and have an actual safety, health, environmental, and financial impact

ABB Cyber Security
A word from ABB's CEO

Ulrich Spiesshofer, CEO ABB

"ABB recognizes the importance of cyber security in control-based systems and solutions for infrastructure and industry, and is working closely with our customers to address the new challenges."

Importance of Software for ABB

Majority of offering with software content today

ABB software business – some facts

Embedded software: core of our electronics offering

Automation system software: a leading DCS[1] player

Application software: for design, operations, and services

> 50% of offering is software-related

> 2’600 software developers

Smallest software application

3-pole contactor

~100 lines of software code

Large software application

Network Manager

>5 mn lines of software code

Same size as avionics and control system of Boeing 787

ABB - a leading industrial software player

ABB Group Cyber Security Council
Representation

Group Cyber Security Council - Representation

Divisions

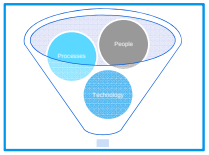
Power Grids

Discrete Automation and Motion

Process Automation

Electrification Products

Cross Functions



Software Development

IT Security

Legal

Communication

Corporate Security

Service

Insurance Risk Management

Research

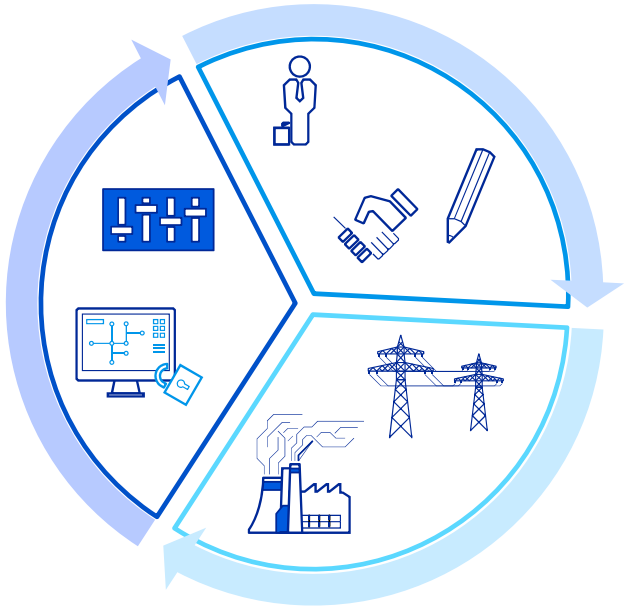
ABB has a formally established cyber security organization reporting to top management

Cyber Security in the System Lifecycle

Product Lifecycle to Plant Lifecycle and back

Product

Design
Implementation
Verification
Release
Support



Project

Design
Engineering
FAT
Commissioning
SAT

Plant

Operation
Maintenance
Review
Upgrade

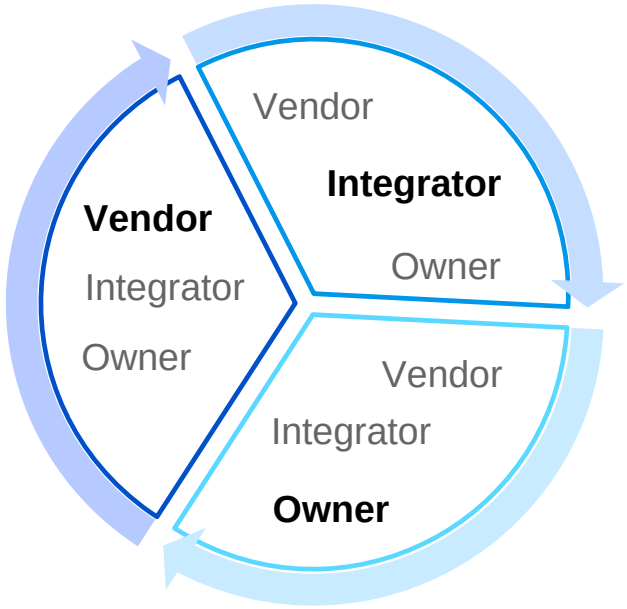
"Security is a process, not a product" (B. Schneier)

Cyber Security in the System Lifecycle

Product Lifecycle to Plant Lifecycle and back

Product

Design
Implementation
Verification
Release
Support



Project

Design
Engineering
FAT
Commissioning
SAT

Plant

Operation
Maintenance
Review
Upgrade

Addressing the security challenges effectively requires collaboration

Cyber Security in the System Lifecycle
Tendering and contracts

Recommendations

Address cyber security explicitly in tenders and contracts

- Be specific but practical

Consider the entire lifecycle

- Product, Project and Plant

Be transparent and establish clear expectations

- What is included in delivery
- What comes with additional cost
- Who is responsible for what
- When do responsibilities shift

Examples for R&D

Security Development Lifecycle ☺

Independent Validation

Certification ☹

Examples for Processes

Awareness & training ☺

Background investigations ☹

Vulnerability handling ☺

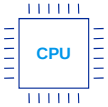
Examples for Information Security

Protection of customer data ☺

(Sub) Contractor information security policies

Security considerations in products and systems

Hardware



Capabilities for security operations

Dedicated security chips

Trusted modules (tampering)

Long-term deployment

OS

Security needs and functionalities

Addition security features (anti-virus, whitelisting)

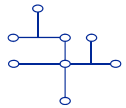
Lifecycle and support

Application

Security capabilities (access control secure comm.)

Security as SW quality requirement: SDL

Network and System



DMZ, perimeter protection, zone and conduits

Firewalls

IDS and IPS

Monitoring

Infrastructure for Service

Secure remote access

Monitoring & asset management

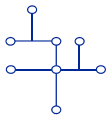
Access control

Patch management

Incident management

Security considerations in system design, engineering and operations

Architecture

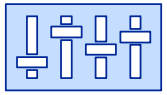


Network topology (e.g., DMZ, zone and conduits)

System security controls (e.g., firewalls, logging, directories)

Remote access and system connectivity

Management



Software updates

Malware protection

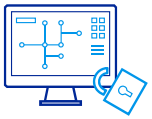
System hardening

Backup and recovery

Security monitoring and diagnostics

Incident management

Access



Roles and permissions

Account management

Policy enforcement

User authentication

Documentation

System and software inventory

Network diagram

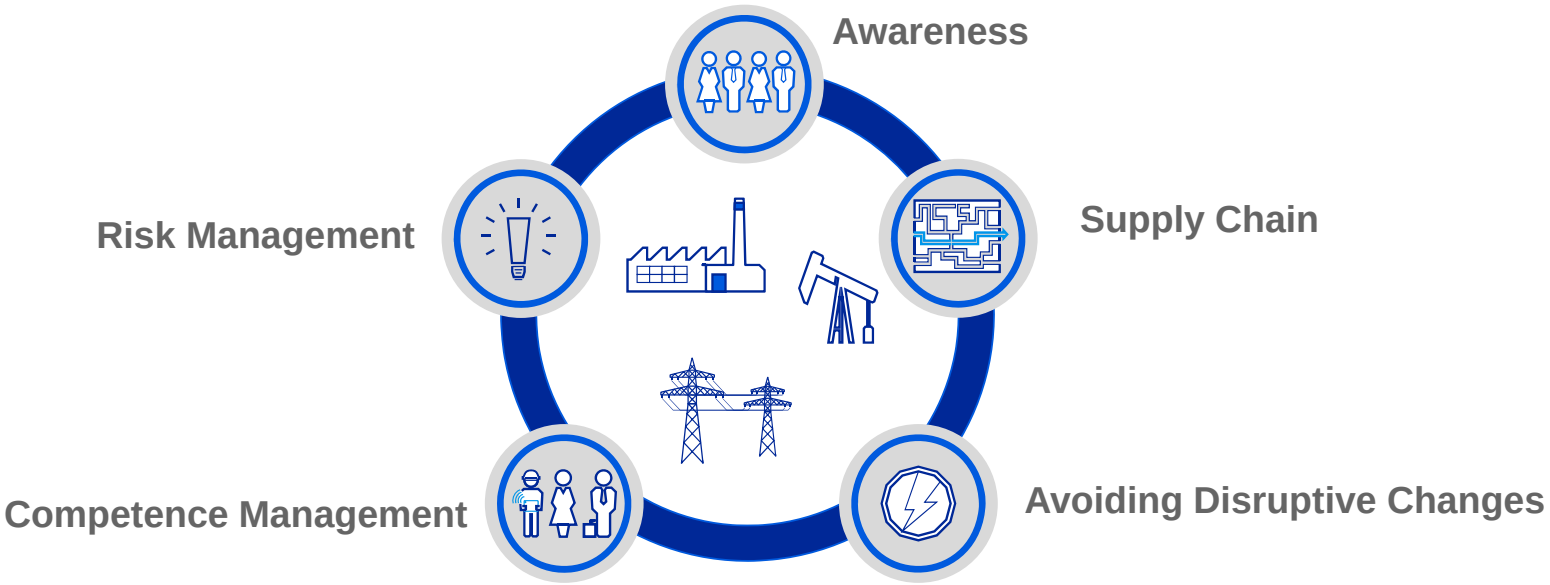
Used / required ports and services

Hardening settings

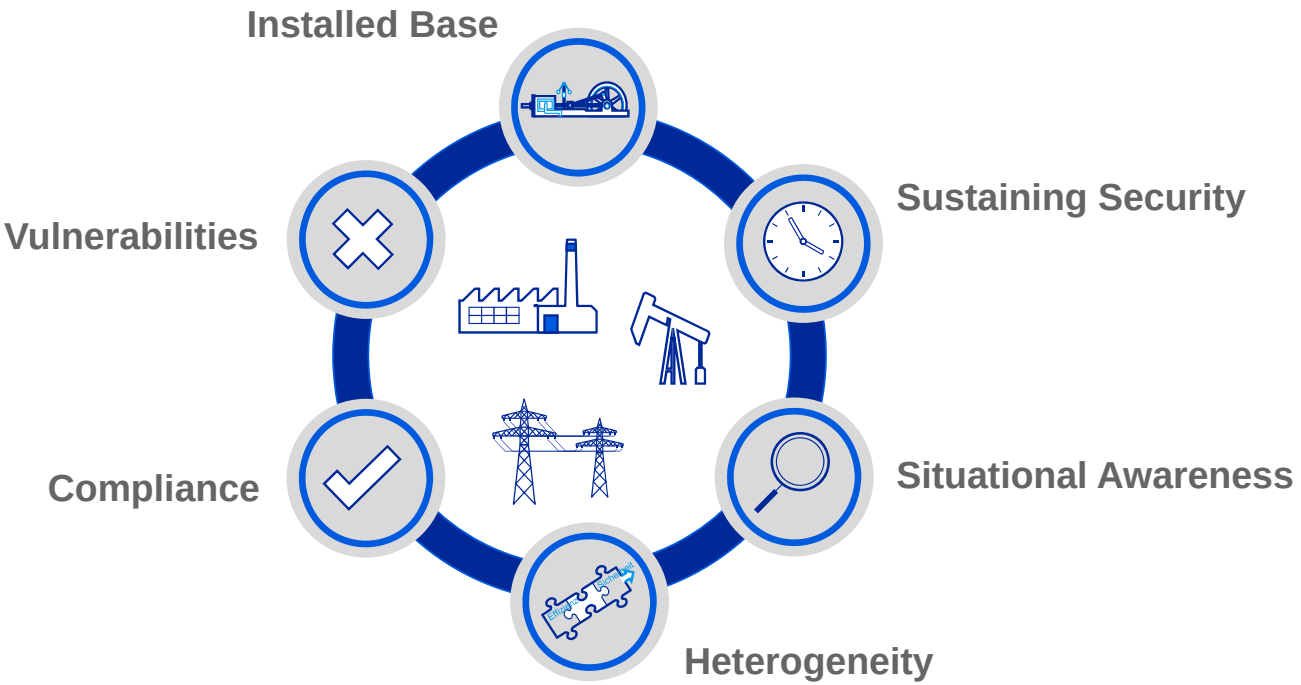
User and system accounts

Biggest challenges for asset owners

Operational and Organizational



Biggest challenges for asset owners
Technical



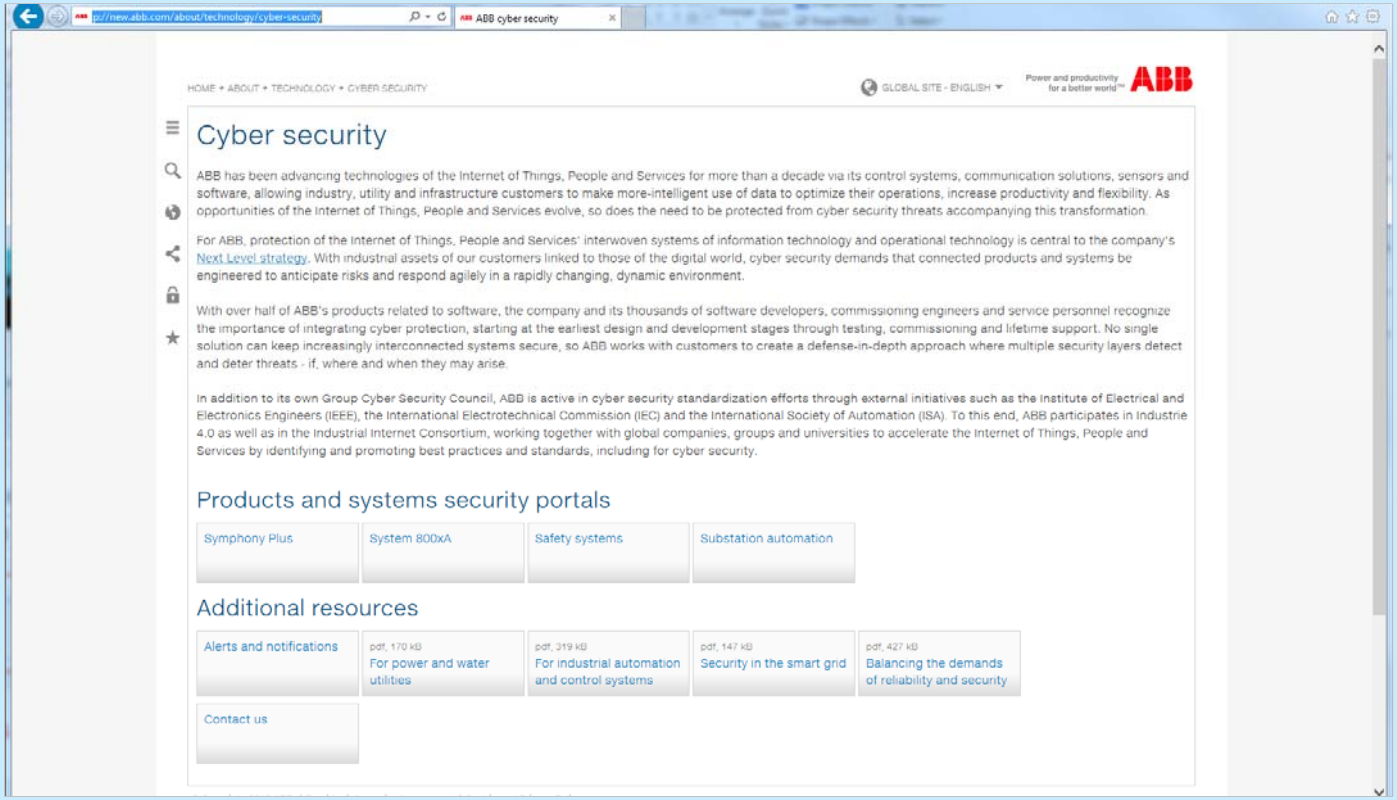
What the future holds

Software	Importance of IT and SW will increase ▪ Use of COTS components ▪ Cloud based offerings ▪ Wireless technologies
Demand	Importance of and demand for cyber security will increase ▪ in all corners of the world ▪ for all industries
Success	Keys for success ▪ Joint effort by all stakeholders, e.g. asset owners, vendors, governments ▪ True integration with automation technology, bringing end-to-end security ▪ Better integration of cyber security into organization and operational processes

External Cyber Security Portal

Links

- Web: http://www.abb.com/cybersecurity
- Email: cybersecurity@ch.abb.com



Power and productivity
for a better world™

April 12, 2016