Kaspersky ICS Cybersecurity 2017, 2017-09-28

Cyber Security for Process Control Systems

ABB's view

Tomas Lindström, Cyber Security Manager, ABB Control Technologies

Agenda

Cyber security for process control systems
for vendors and system owners

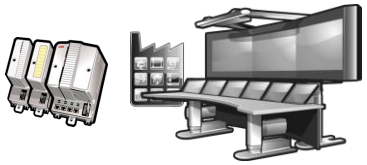
- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services

ABB: the pioneering technology leader

What (Offering)	**Pioneering technology**		
	Products 58%	Systems 24%	Services & software 18%
For whom (Customers)	**Utilities**	**Industry**	**Transport & Infrastructure**
	~35% of revenue	~40% of revenue	~25% of revenue
Where (Geographies)	**Globally**		
	Asia, Middle East, Africa 38%	Americas 29%	Europe 33%

~$35 bn revenue	~100 countries	~132,000 employees

ABB Ability™ System 800xA, the # 1 DCS in process control



The process information core

Plant-wide consolidation, collaboration and optimization

One system solution for process- , power automation and safety	Plant centric view – operational excellence
Seamless connectivity to value added systems and applications	Lower cost of ownership
Full scope asset monitoring	Streamline procedures and become more predictive
Integrated operations with embedded functionality	Operator effectiveness reducing downtime

Proven track record

10,000 systems

100 countries

45,000 controllers

40,000 workstations

30,000,000 I/Os

Agenda

Cyber security for process control systems
for vendors and system owners

- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services

Cyber Security @ ABB

Three 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

ABB Cyber Security Approach

Full lifecycle coverage

Product

Design
Implementation
Verification
Release
Support

Project

Design
Engineering
FAT
Commissioning
SAT

Plant

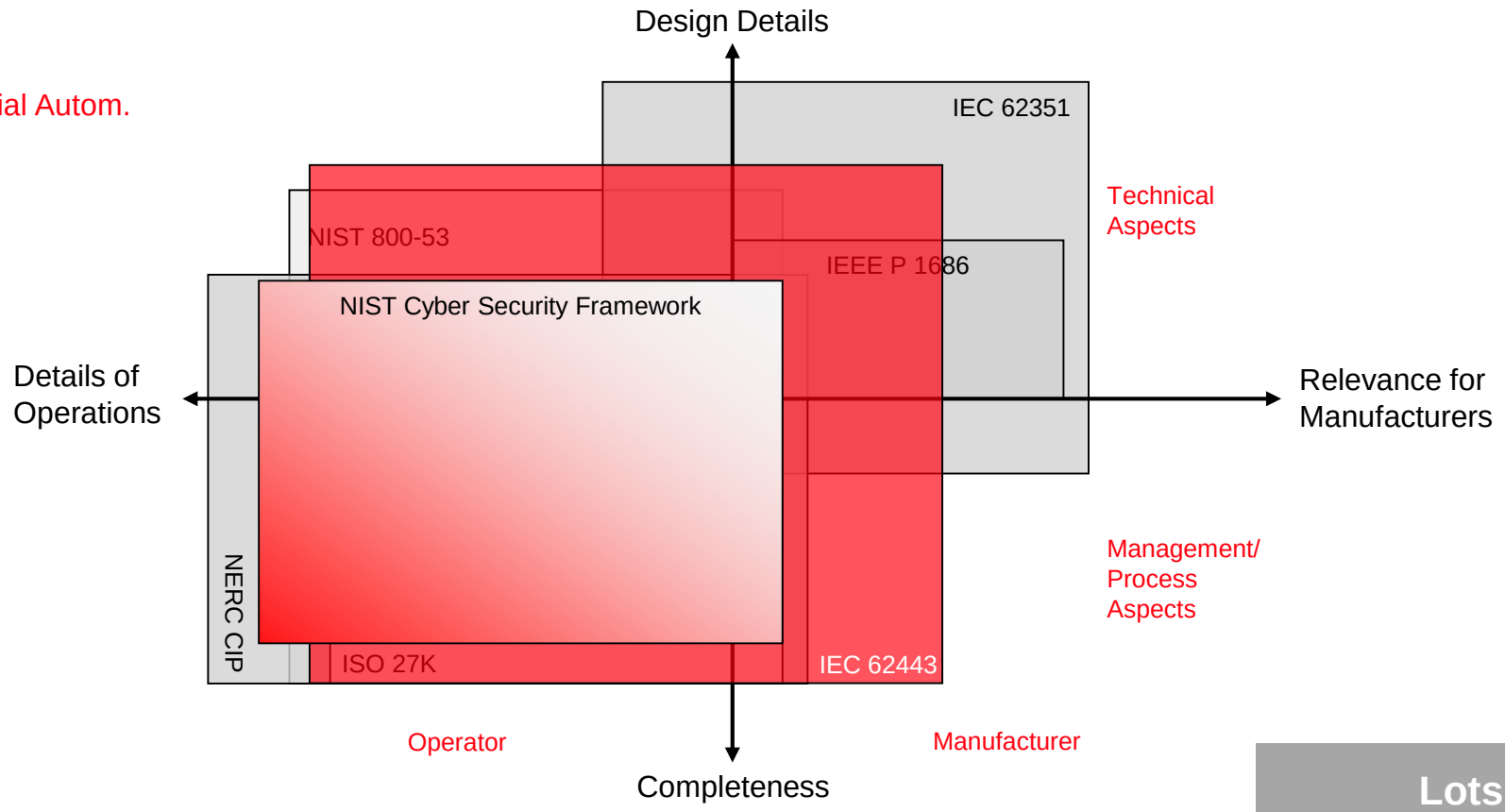
Operation
Maintenance
Review
Upgrade

ABB requires the same of our suppliers

Cyber Security Best Practices

International standards and guidelines

IT
Energy
Industrial Autom.

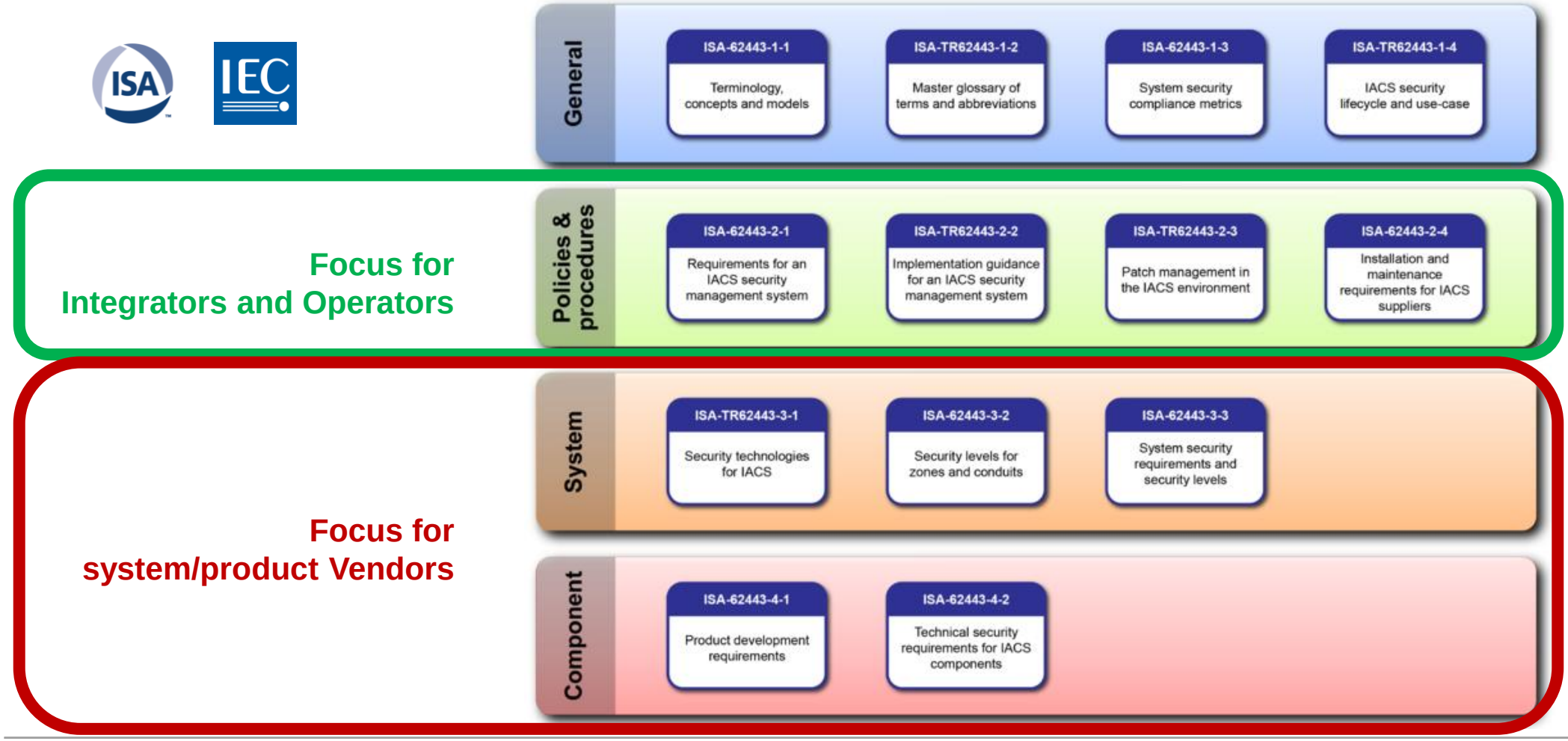


Lots of similar support available

Source: ESCoRTS Project (European network for the Security of Control and Real-Time Systems), with ABB additions.

Cyber Security Best Practices

The IEC 62443 standard



Agenda

Cyber security for process control systems
for vendors and system owners

- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services

Cyber security for the Product Lifecycle

The SD^3 + C Security Framework

Secure by Design	Security in the Product Development Process: Requirements, Design, Implementation, Verification
Secure by Default	Default installation and usage with minimal attack surface Built in functions for Defense in Depth
Secure in Deployment	Support for Secure Project and Plant Lifecycle Validation of 3rd party software and solutions
Communication	Correct information to those who need to know

Security in the Product Development Process

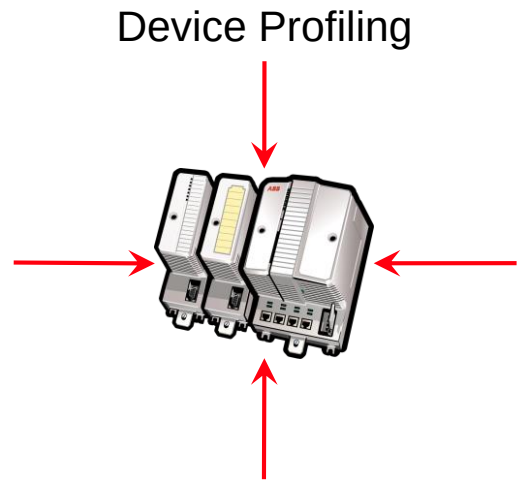
Security verification and validation

Overview

Product- / System Type Testing of security requirements

Robustness testing:
– by product R&D
– and product independent test center: DSAC

Testing by ABB's Device Security Assurance Center (DSAC)



Thorough vendor testing more effective than 3rd party certification

Communication

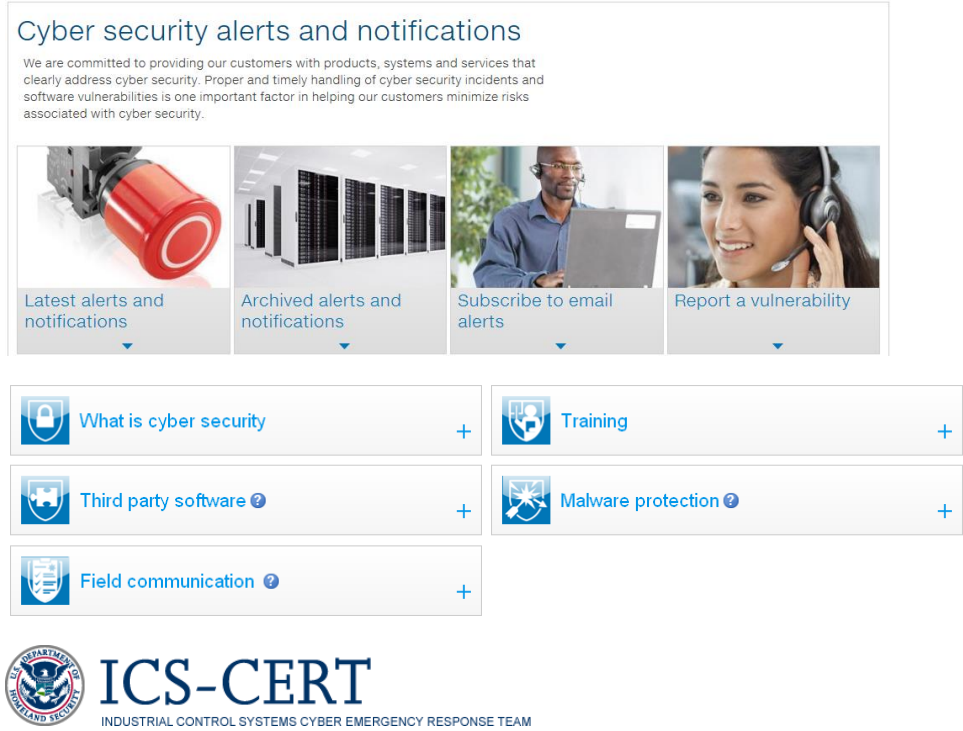
Inform those who need to know in case of problems

Reporting a suspected problem:

- ABB Customer: The regular ABB contact
- Others: www.abb.com/cybersecurity
  or cybersecurity@ch.abb.com

ABB's responses in case of product vulnerability:

- Responsible/Coordinated disclosure
- Field Communication:
  "Security Advisory" for customers via MyControlSystem
- If publically disclosed ➔ public response:
  ICS-CERT and www.abb.com/cybersecurity



Agenda

Cyber security for process control systems
for vendors and system owners

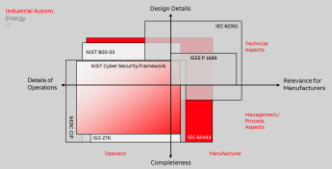
- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services

A Cyber Security Framework for system owners

Overview

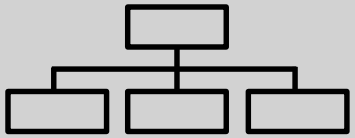
1

Standards: Guidelines

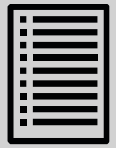


Risk Assessment

Management Buy-in



Security Policy



(IT⇔OT?)

2

Balance Security Measures:
- Value for me ⇔ Value for X ⇔ Mitigation cost

Combine measures:
- Defense in Depth

Work with system vendors
- Request selected measures

3

Incident response
Disaster recovery

Training for all staff

Audit policy compliance

4

Categories of Security Measures

The 7 Foundational Requirements of IEC 62443

FR 1 Identification and authentication control — Who

- User, software, & device authentication
- Account management

FR 2 Use control — What

- Authorization enforcement
- Auditable events

FR 3 System integrity — Protect

- Communication integrity
- Malicious code protection

FR 4 Data confidentiality — Protect

- Information confidentiality

FR 5 Restricted data flow — Protect

- Network segmentation

FR 6 Timely response to events — Detect

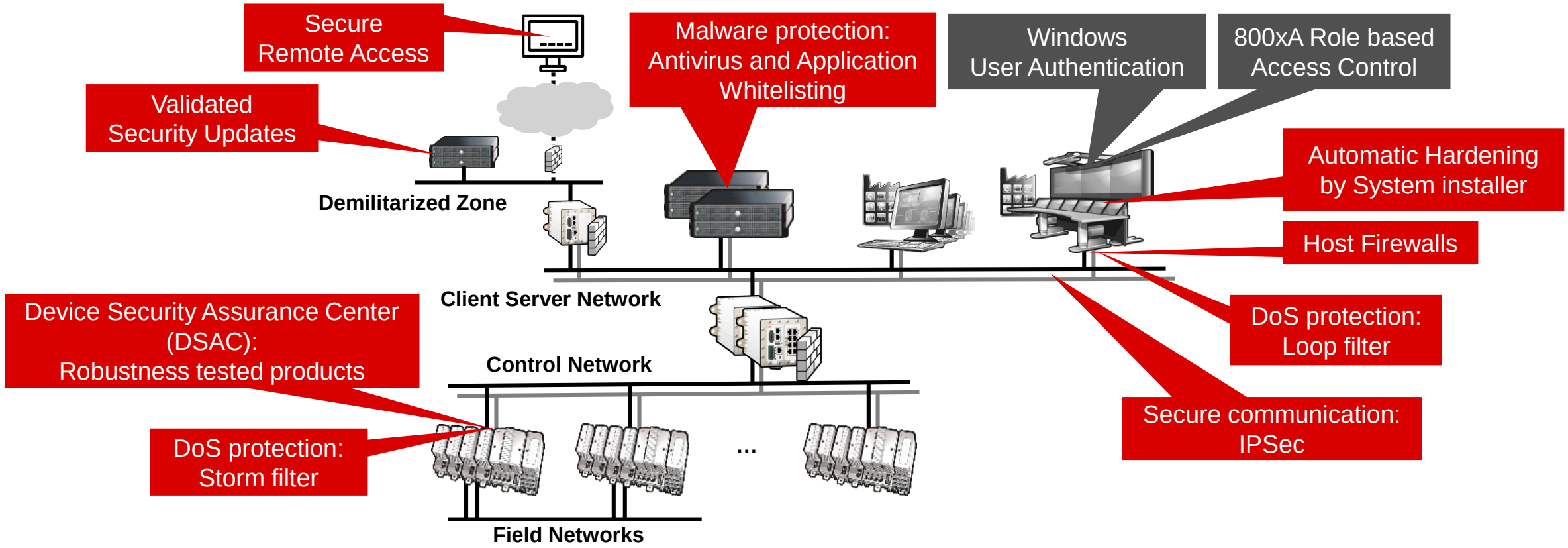
- Audit log accessibility
- Continuous monitoring

FR 7 Resource availability — Protect

- Denial of service protection
- Control system backup

Defense in Depth in 800xA

Who/What, Protect Hosts



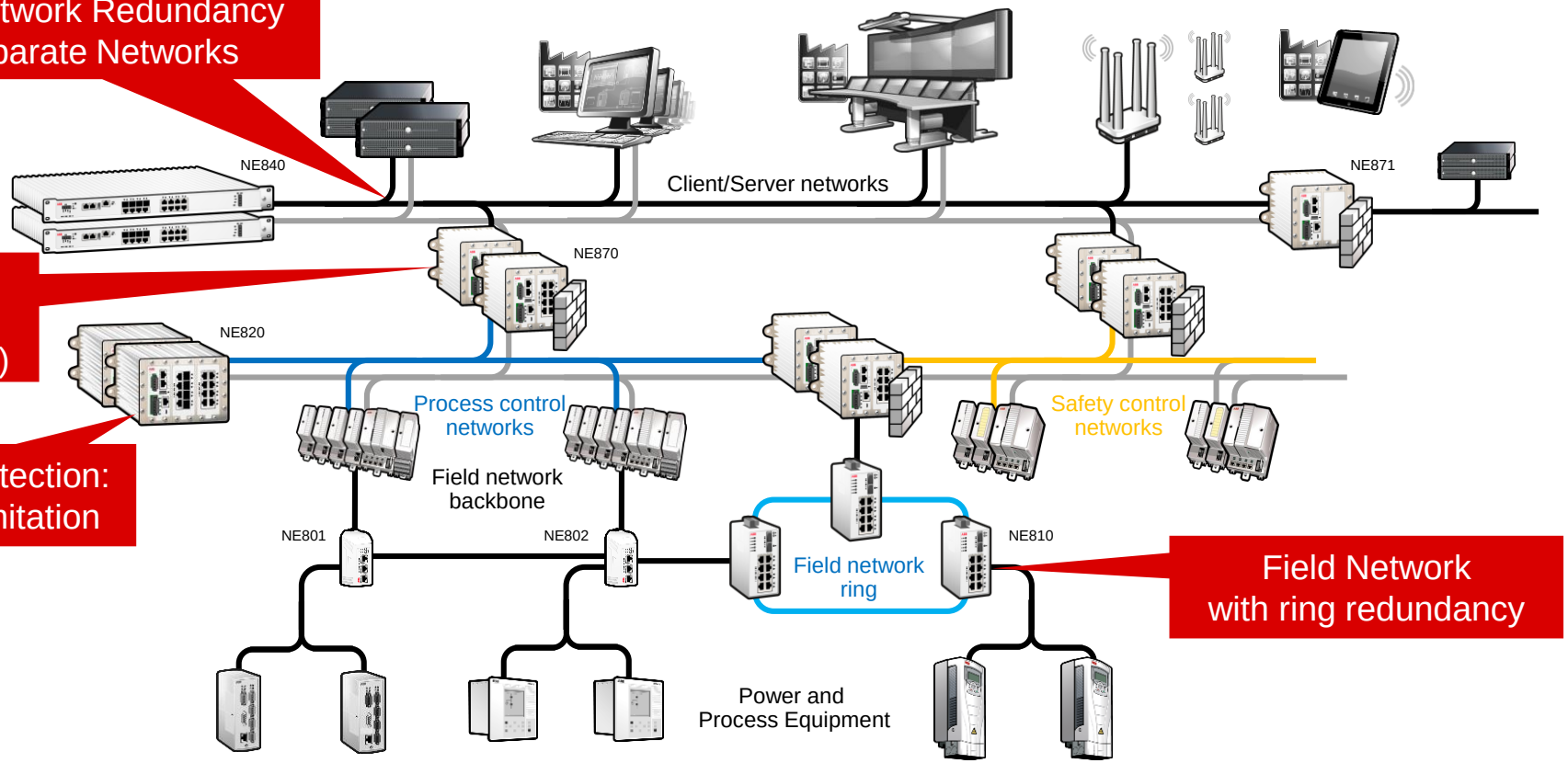
System 800xA Networks

Protect Networks

RNRP:
System Network Redundancy
with Separate Networks

System Zoning
with full redundancy
(RNRP router/firewall)

DoS protection:
Rate limitation



Field Network
with ring redundancy

Fieldbus
IEC
PROFIBUS
PROFINET
DeviceNet
EtherNet/IP
MODBUS TCP

Audit logging with System 800xA

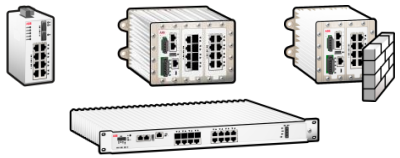
Detect 1, Create the information

Enable Logging/Audit Trail

– Operating system (Windows) events
– Control system events
– System User Actions
  800xA Audit Trail

System monitoring

– Control system built-in self-supervision
– Additional monitoring functions/log sources
  • Servers and Workstations
  • Network equipment
  • Add-on products (e.g. Malware protection)
– Collect via Windows Event Log, SNMP, SysLog
– More information from integrated equipment
  • ABB’s Network Equipment NE800
  • ABB’s PC Network Software Monitoring

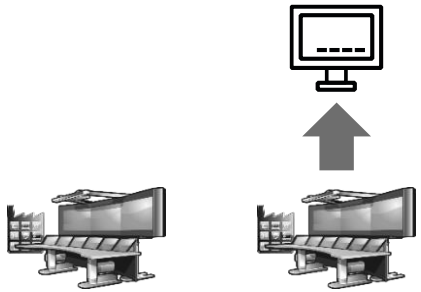


Security Information and Event Management

Detect 2, Analyze the information

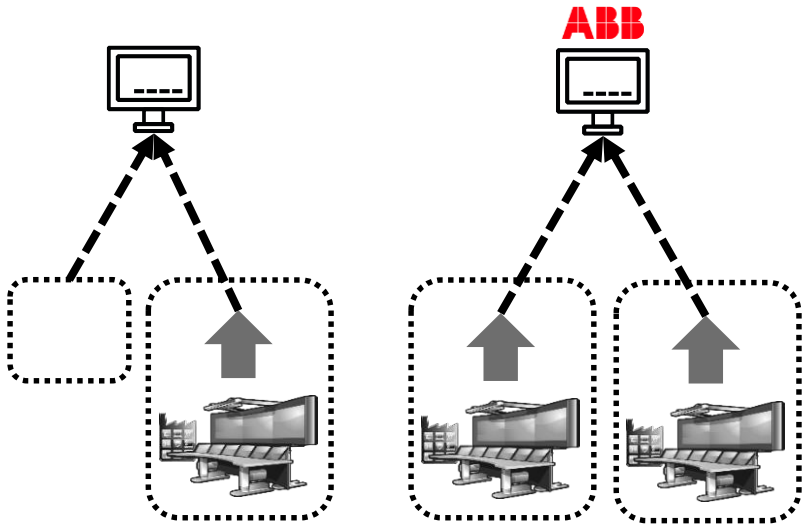
Collection/Storage

- Collection in the control system
- Dedicated SIEM
  Security
  Information and
  Event
  Management system



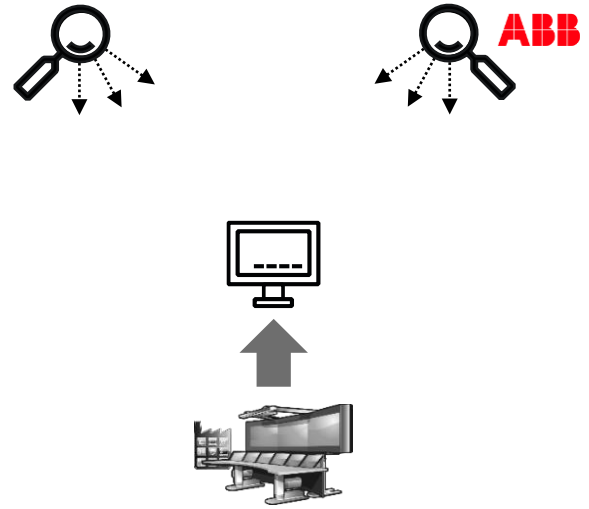
Centralization

- Infrastructure by system owner
- Infrastructure by system vendor



Monitoring/Analysis

- Performed by system owner
- Performed by system vendor

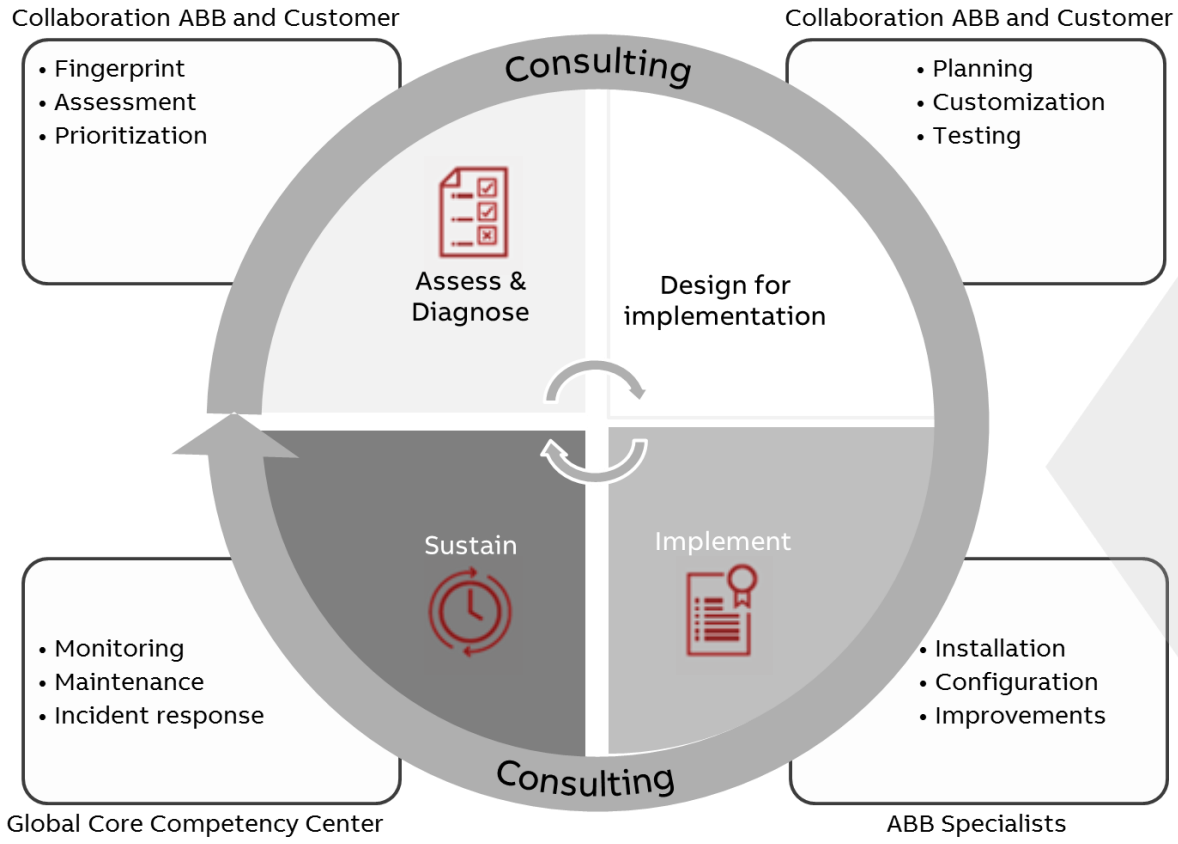


Agenda

Cyber security for process control systems
for vendors and system owners

- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services

Cyber Security Services



Service portfolio
Cyber Security Benchmark
Cyber Security Fingerprint
Cyber Security Assessment
Security Patch Management
Malware Protection Management
System Hardening
Backup and Recovery Management
Network Security Management
User and Access Management
Cyber Security Maintenance
Cyber Security Monitoring
Incident Response Retainer
Threat Intelligence
Cyber Security Risk Assessment
Cyber Security Training
Security Policies & Procedures

Cyber Security Services

Cyber Security Fingerprint

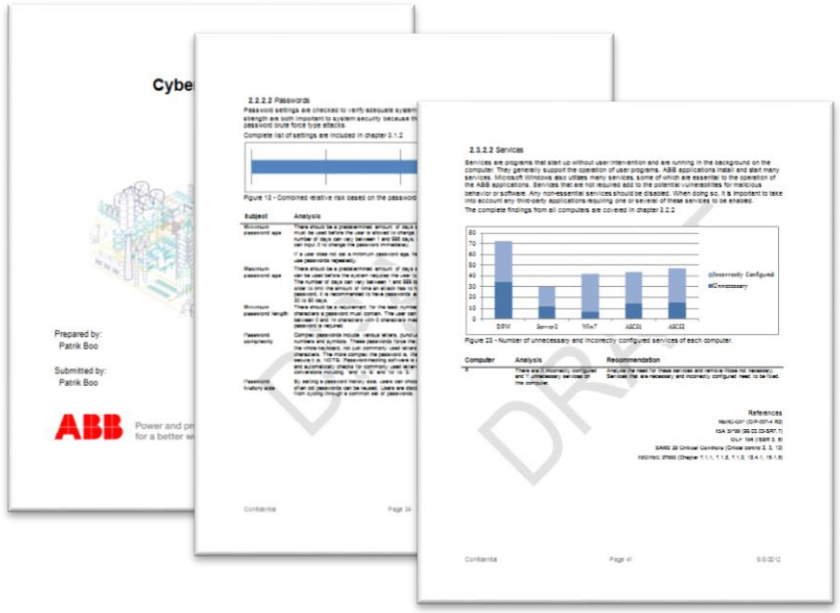
– Interview
  Data collection

– Analysis

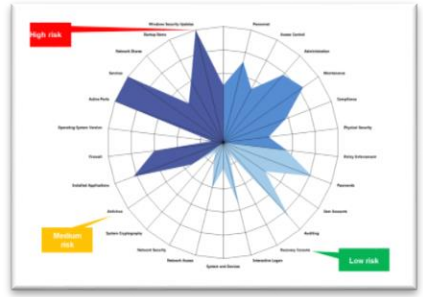
➔ Report with

- Cyber security status
  Identifies strengths and weaknesses
- Recommendations on improvements

– Based on widely accepted industry standards*

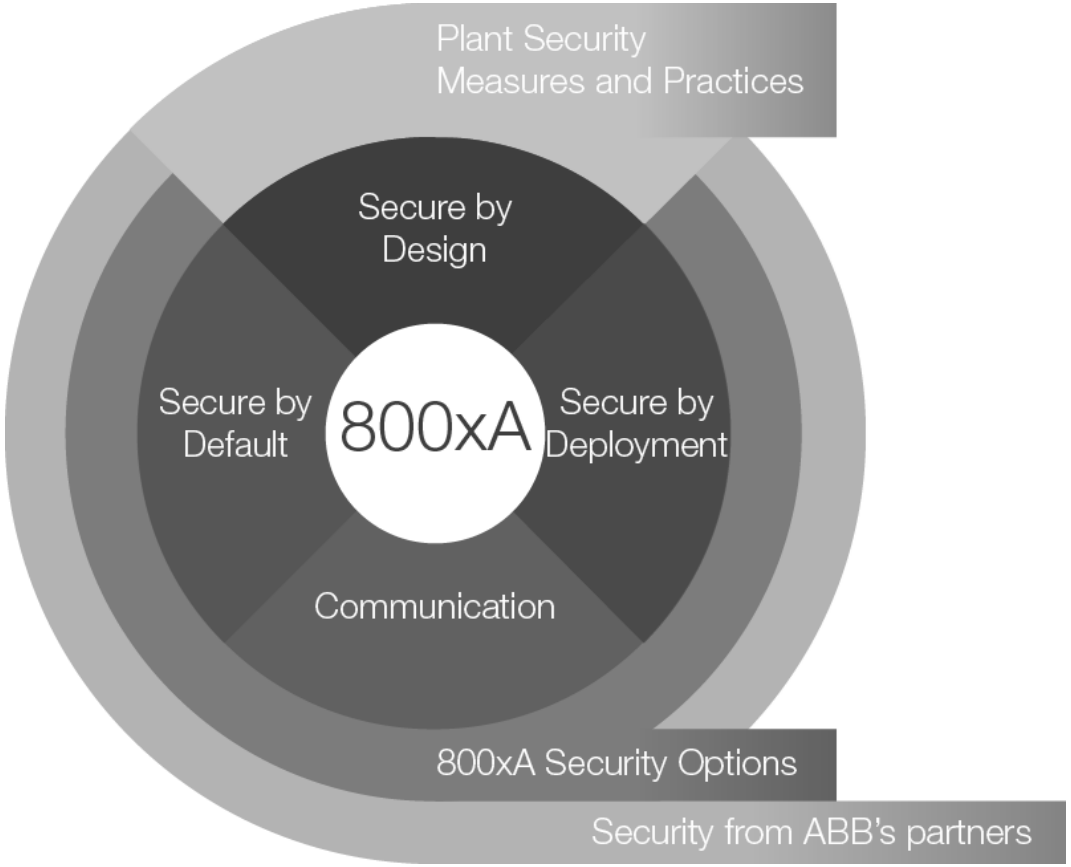


Cyber security
Risk Profile



*) Including, but not limited to: NERC-CIP, OLF-104, ISA-62443 (ISA99), ISO 27000

eXtended Security from ABB



Security for a Process Control System: We can make it if we cooperate!