ZELLCHEMING Expo, 2019-06-26

Cyber Security in Pulp & Paper

Ragnar Schierholz, Head of Cyber Security, ABB Industrial Automation

Agenda

- Motivation: why do we care about cyber security in industrial control systems?
- ABB's approach to cyber security in a nutshell
- How to introduce a security management system for OT/IIoT?

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 the 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

Cyber security in power and automation

Why is cyber security an issue?

Stuxnet worm 'targeted high-value Iranian assets'

Hackers attack high-tech military contractor, break into submarine manufacturing plant

BlackEnergy crimeware coursing through US control systems

US CERT says three flavours of control kit are under attack

Active malware operation let attackers sabotage US energy industry

"Dragonfly" infected grid operators, power generators, gas pipelines, report warns.

Attackers poison legitimate apps to infect sensitive industrial control systems

Havex operators target mission-critical controllers around the world.

Computer intrusion inflicts massive damage on German steel factory

Blast furnace can't be properly shut down after attackers take control of network.

Ukraine power cut 'was cyber-attack'

Ukrainian blackout blamed on cyber-attack

Moller-Maersk puts cost of cyber attack at up to $300m

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

Cyber security

Common misconceptions

Myth 1 – Being Relevant

"Small companies and industries outside of media attention are not a relevant target"

False

- If it's worth having, it's worth stealing
- Attackers' business models are often built on economies of scale
- Critical infrastructure is often a network of smaller entities

Myth 2 – Waste of money

"Strong security is a waste of time and money"

False

- Compromised control systems are not reliable and trustworthy and can prevent the owner/operator from achieving its mission.
- Maloperations due to cyber events can become a safety issue.
- Business continuity insurance can become more expensive or even unavailable.

Myth 3 – Air-gapped

„Our system is air-gapped and has no connectivity to anything outside."

False

- Staff needs to get data into and out of the system
  - Production schedules, engineering updates, …
  - Production reports, emission reports, …
- Entirely isolated systems are extremely cumbersome and expensive to operate
  - If no communication is built-in, convenient workarounds are improvised, e.g. unapproved networks, temporary connections, portable media

Myth 4 – No Internet

"Our system does not have a direct connection to the Internet so attackers have no way in"

False

- Majority of incidents are staged attacks
  - (Spear)phishing to compromise legitimate user accounts
  - Compromise of perimeter networks first, e.g. DMZ, enterprise network
  - Lateral movement to reach more interesting targets

The Biggest Challenges

Addressing a unique set of requirements

	"Traditional" information technology	Power and automation technology
Object under protection	Information	Physical process
Risk impact	Information disclosure, financial loss	Safety, health, environmental, financial
Main security objective	Confidentiality, Privacy	Availability, Integrity
Security focus	Central Servers (fast CPU, lots of memory, …)	Distributed System (possibly limited resources)
Availability requirements	95 – 99% (accept. downtime/year: 18.25 - 3.65 days)	**99.9 – 99.999%** (accept. downtime/year: 8.76 hrs – 5.25 minutes)
System lifetime	3 – 10 Years	**5 – 25 Years**

Agenda

- Motivation: why do we care about cyber security in industrial control systems?
- ABB's approach to cyber security in a nutshell
- How to introduce a security management system for OT/IIoT?

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 about risk management

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 withour customers to address the new challenges."

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 addresses cyber security throughout the entire lifecycle and expects the same from our suppliers

IT/OT convergence as an overarching theme

Manage the culture clash

Mix of skills will be needed from both domains

- Typical IT background
  - profound cyber security expertise, understanding of threats and attacker TTPs*
  - security risk assessment methodology suited for „fuzzy“ risks

- Typical OT background
  - profound understanding of the respective domain (e.g. paper production) and critical processes
  - established change and risk management procedures and safety culture

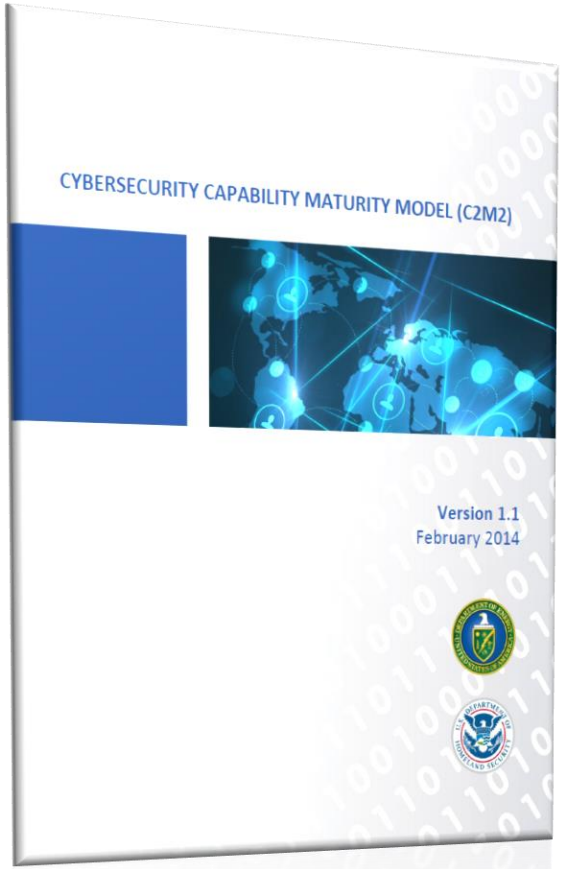
*TTPs: Techniques, tactics and procedures

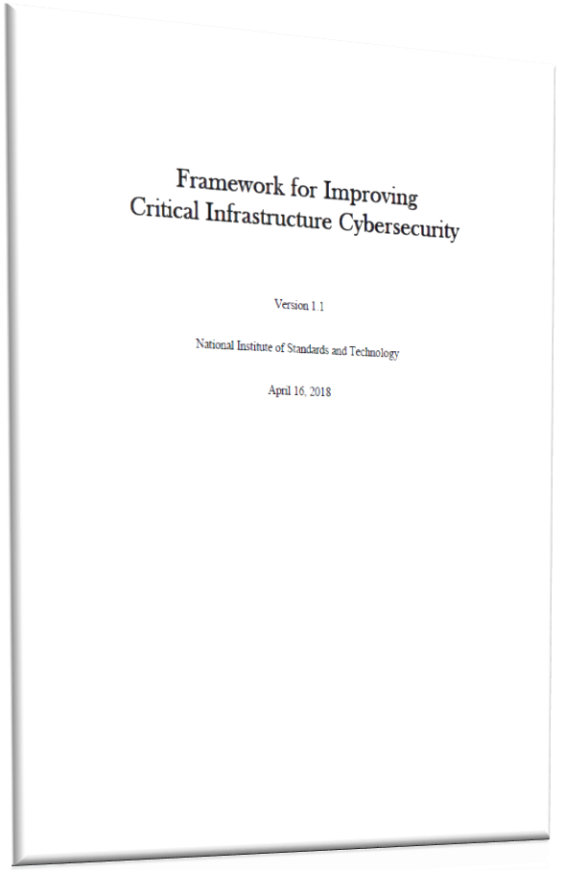
Agenda

- Motivation: why do we care about cyber security in industrial control systems?
- ABB's approach to cyber security in a nutshell
- How to introduce a security management system for OT/IIoT?

How to introduce a security management system?

Inspiration





Note:
IEC 62443-2-1 Ed 2.0 is still a work in progress and only available as draft from ISA

Two core concepts

Capability Maturity Indicator Levels

MIL 0: Generally, no practices are performed

MIL 1: Initial practices are performed but may be ad hoc

MIL 2: Practices are established

- Documented practices
- Stakeholder involvement
- Appropriate resources
- Relevant standards used

MIL 3: Practices are continuously managed

- Policies guide the practices, incl. compliance
- Continuous improvement
- Assigned responsibility and authority
- Role-specific training

Approach progression vs. **Institutionalization** progression

Cyber Security Capability Domains

ISO/IEC 62443-2-1

1. Risk Management
2. Information security policies
3. Organization of information security
4. Human resource security
5. Asset management
6. Access control
7. Cryptography
8. Physical and environmental security
9. Operations security
10. Communication Security
11. System acquisition, development and maintenance
12. Supplier relationships
13. Information security incident management
14. Information security aspects of business continuity management
15. Compliance

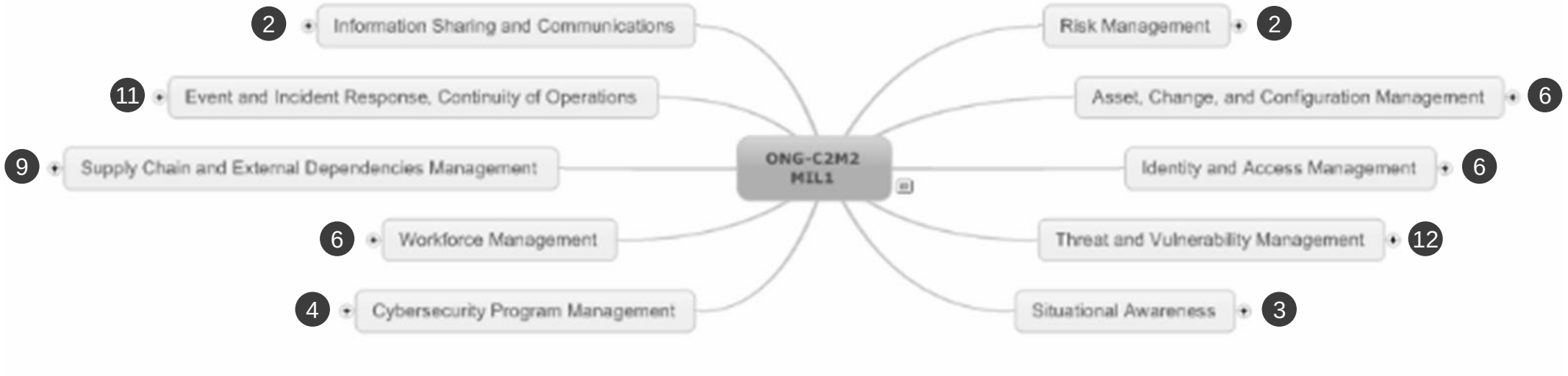
C2M2 (ONG & ES)

1. Risk Management
2. Asset, Change, and Configuration Management
3. Identity and Access Management
4. Threat and Vulnerability Management
5. Situational Awareness
6. Information Sharing and Communications
7. Event and Incident Response, Continuity of Operations
8. Supply Chain and External Dependencies Management
9. Workforce Management
10. Cybersecurity Program Management

Specific guidance from C2M2

Example: Reaching MIL-1

First step: Determine risk and define target maturity level for each domain



Moving from MIL 0 to MIL 1 is a fairly big step

Lean approach

Stage 0 – Getting started

Objectives

Raise awareness in management and other relevant levels of the organization

Identify areas of **biggest risk** generically

ABB Cyber Security Services

Awareness training

- Often more effective if done by external entities

Security assessment / fingerprint

- Doesn‘t have to be a very detailed audit
- Leverage general experience with regards to common causes of incidents
- Leverage general experience with regards to simple security countermeasures
- ABB Ability™ Cyber Security Fingerprint

Lean approach

Stage 1 – Introduce basic protection

Objectives

Establish a foundation for cyber security in operations

Mitigate the most common risks with countermeasures which the organization is capable of operating

Demonstrate risk reduction effectiveness by selected examples

Establish a context-specific, detailed **understanding of risk**

ABB Ability™ Cyber Security Services

Awareness training (continued)

ABB Ability™ Cyber Security Updates

ABB Ability™ Cyber Security Endpoint Protection

ABB Ability™ Cyber Security Hardening Services

ABB Ability™ Cyber Security Backup & Restore

ABB Ability™ Cyber Security Network Management (at least perimeter)

ABB Ability™ Cyber Security Analytics (basic security monitoring of the above practices)

ABB Ability™ Cyber Security Risk Assessment

Lean approach

Stage 2 – Defend your system

Objectives

Establish a security management system based on the risk assessment results

Establish security practices **systematically**

Reach **compliance to relevant standards**
(e.g. NERC-CIP IEC 62443-2-1)

ABB Cyber Security Services

Focused awareness training

Security policy & procedure development

ABB Ability™ Cyber Security Updates

ABB Ability™ Cyber Security Endpoint Protection

ABB Ability™ Cyber Security Hardening Services

ABB Ability™ Cyber Security Backup & Restore

ABB Ability™ Cyber Security Network Management

ABB Ability™ Cyber Security Access Management

ABB Ability™ Cyber Security Analytics
(basic security monitoring of the above practices)

ABB Ability™ Cyber Security Network Monitoring

ABB Ability ™ Cyber Security Incident Response

ABB Ability™ Cyber Security Risk Assessment

Lean approach

Stage 3 – Manage your risks

Objectives

Continuously adapt and **improve** the security management system based on evolving threat landscape

Maintain & document compliance with relevant standards

ABB Cyber Security Services

Security policy & procedure development
ABB Ability™ Cyber Security Updates
ABB Ability™ Cyber Security Endpoint Protection
ABB Ability™ Cyber Security Hardening Services
ABB Ability™ Cyber Security Backup & Restore
ABB Ability™ Cyber Security Network Management
ABB Ability™ Cyber Security Access Management
ABB Ability™ Cyber Security Analytics
(basic security monitoring of the above practices)
ABB Ability™ Cyber Security Network Monitoring
ABB Ability ™ Cyber Security Incident Response
ABB Ability™ Cyber Security Risk Assessment
Threat Intelligence*

ABB Ability™ Cyber Security Services

Customer focused

- ABBs cyber security solutions are all part of an overarching goal to help our customers address security more efficiently.
- These services can be applied to the customer's facility and used by the customer or managed through ABBs service centers.
- All services are developed to help the customer make better decisions, increase their cyber defenses and be a natural part of the customers regular routine.
- ABB Ability makes the suite of services work in harmony, and the customer gets the impression that it is truly one solution made for them.

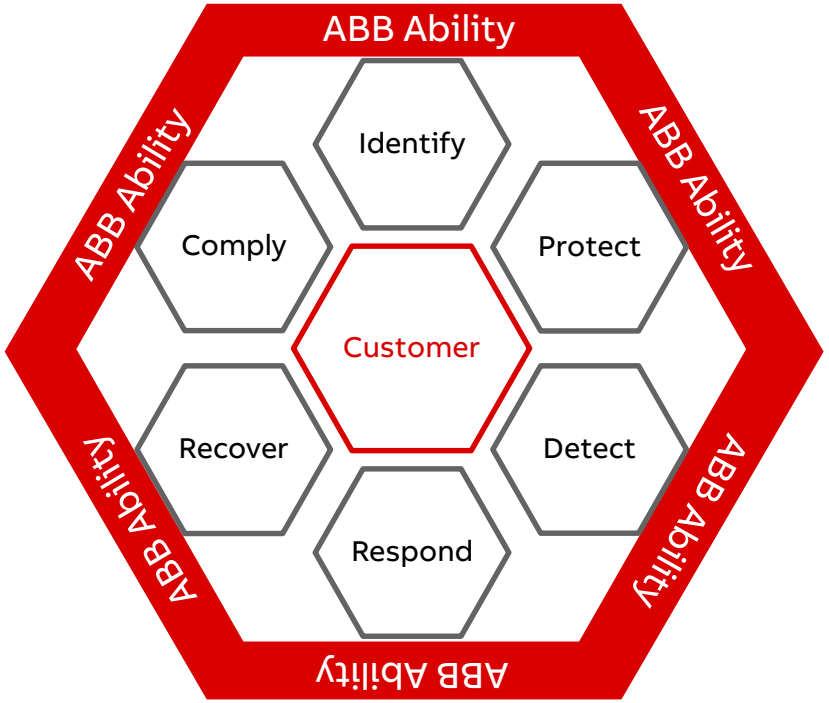


ABB Ability cybersecurity solutions developed for the customer

Summary

Subtitle

Step-by-step to cyber security maturity

Introducing cyber security management into control system operations is a major change and can be overwhelming

Early steps must work towards a solid understanding of context-specific risks and prioritize these

In parallel, basic controls can be introduced which experience shows will be part of any security management system

Competent partners are available on the market to bridge transition periods or continuously provide services

**Don‘t be the deer in headlights –
get started with small steps and look for partners!**

Dichotomy of attack / incident types

Generic attacks / “White noise”

Typical attack vectors & techniques

- Internet ➔ Enterprise IT / personal devices ➔OT
- (Spear-)Phishing / social engineering
- Generic malware from the IT world / the Internet based on known vulnerabilities & exploits

Typical consequences

- Limited to moderate damage (may aggregate to large damage)
- Little or no public attention

Targeted attacks / “APT”

Typical attack vectors & techniques

- Internet ➔ Enterprise IT / personal devices ➔OT
- (Spear-)Phishing / social engineering
- Custom malware often based on 0-day vulnerabilities, specific design of the target environment

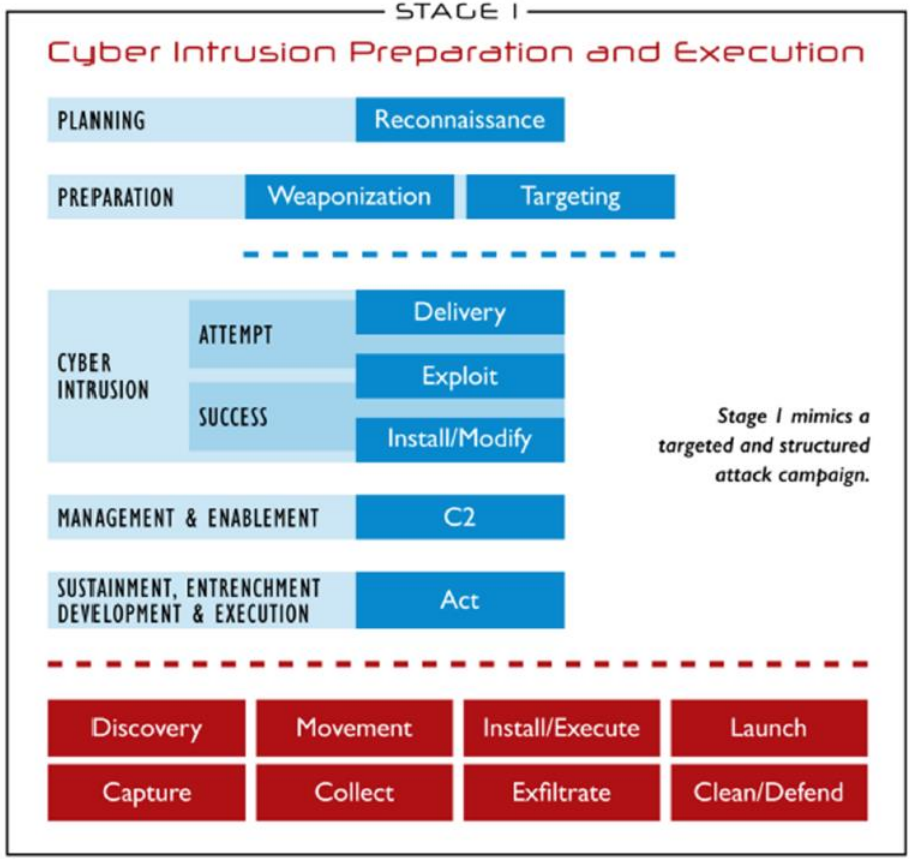
Typical consequences

- Moderate to large damage (usually concentrated on very few victims)
- Potentially large public attention (depending on the nature of the victim)

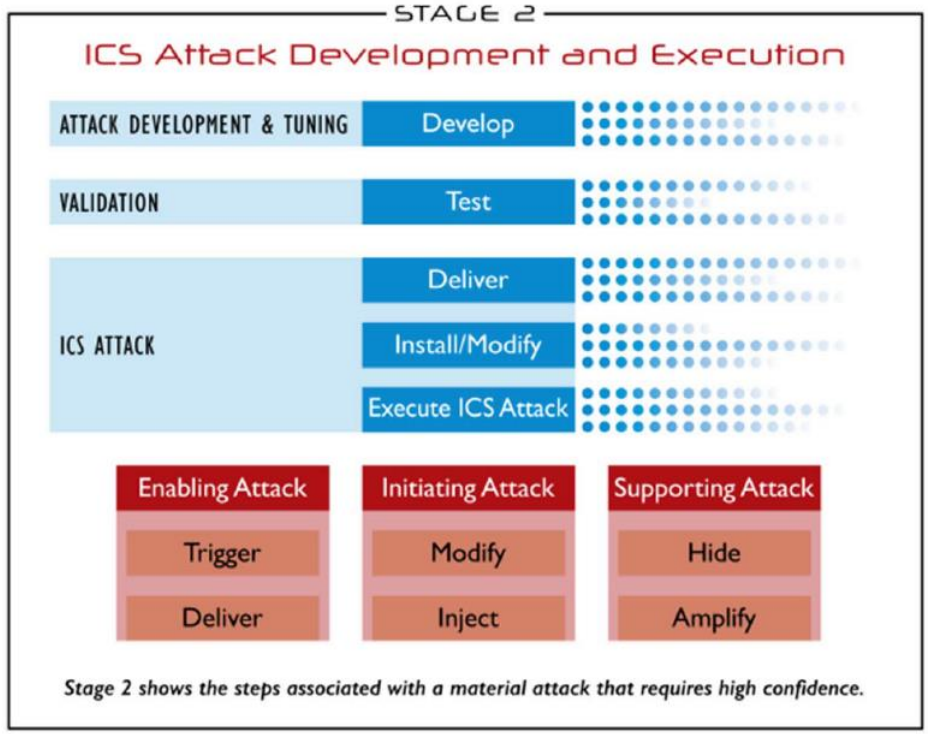
Anatomy of a targeted attack against ICS

Observable e.g. in the cases of Stuxnet, Industroyer or Triton/Trisis

Stage 1

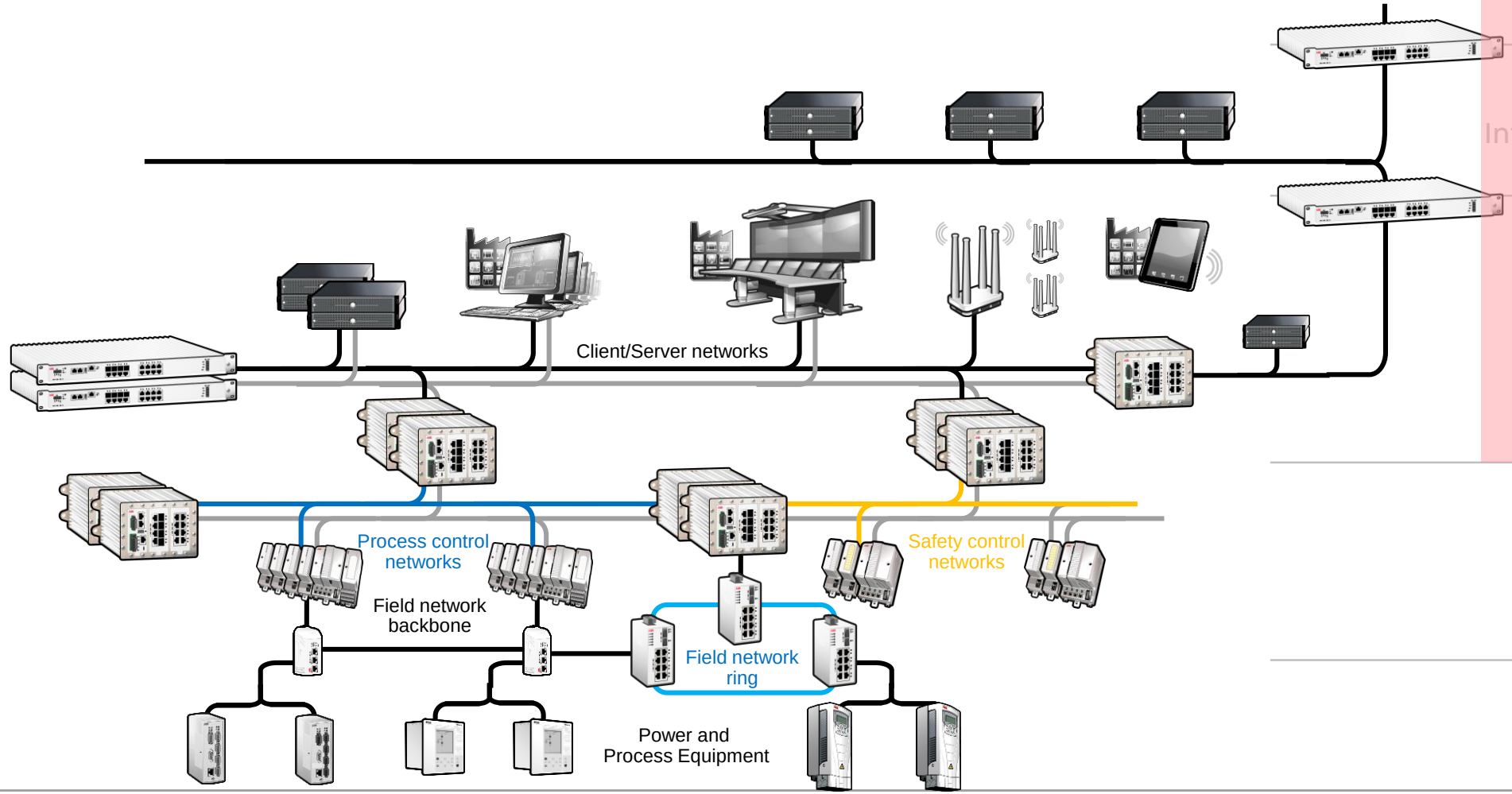


Stage 2



Typical ICS architecture / network topology

A refresher



White noise scope

APT scope

Level 4+ IT Plant Management

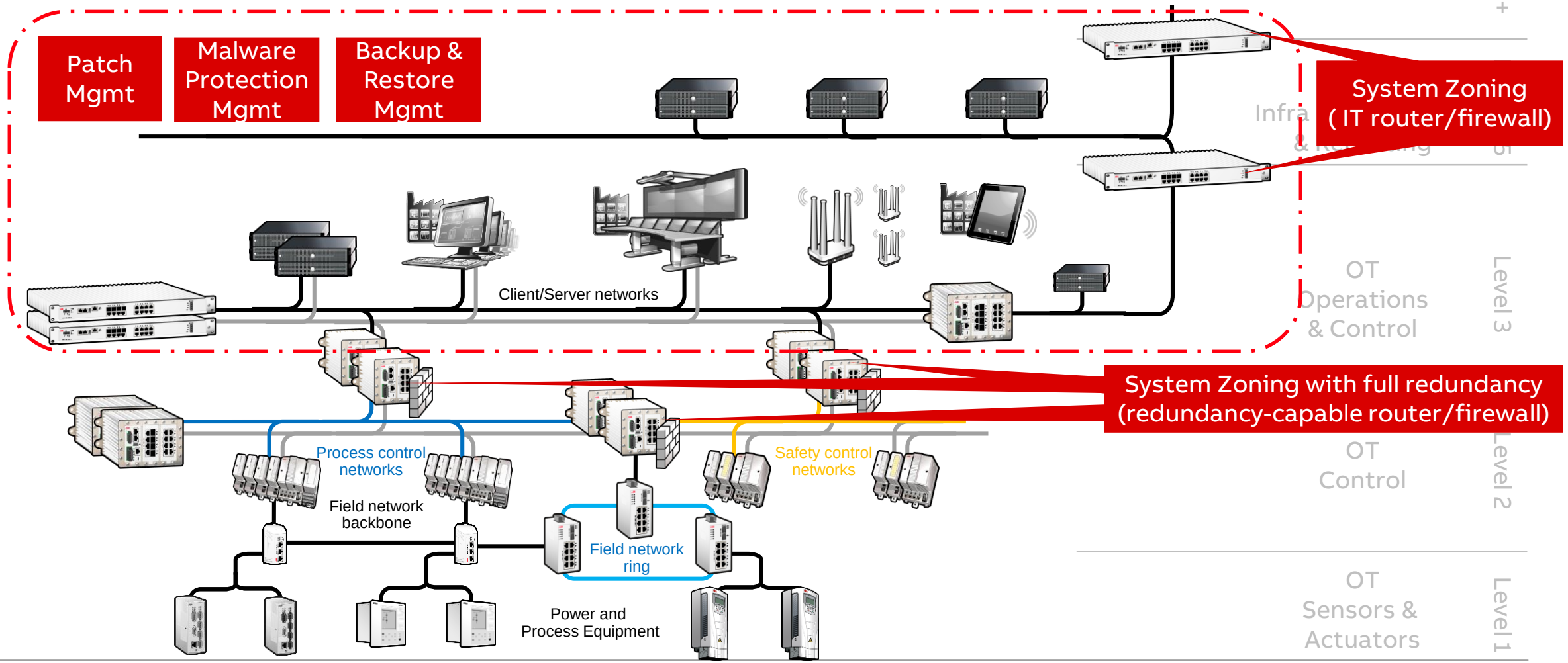
Level 3.5 OT & IT Infra Management & Reporting

Level 3 OT Operations & Control

Level 2 OT Control

Level 1 OT Sensors & Actuators

How to protect against attacks like WannaCry and NotPetya



ICS Cyber Kill Chain

Opportunities to disrupt with appropriate countermeasures