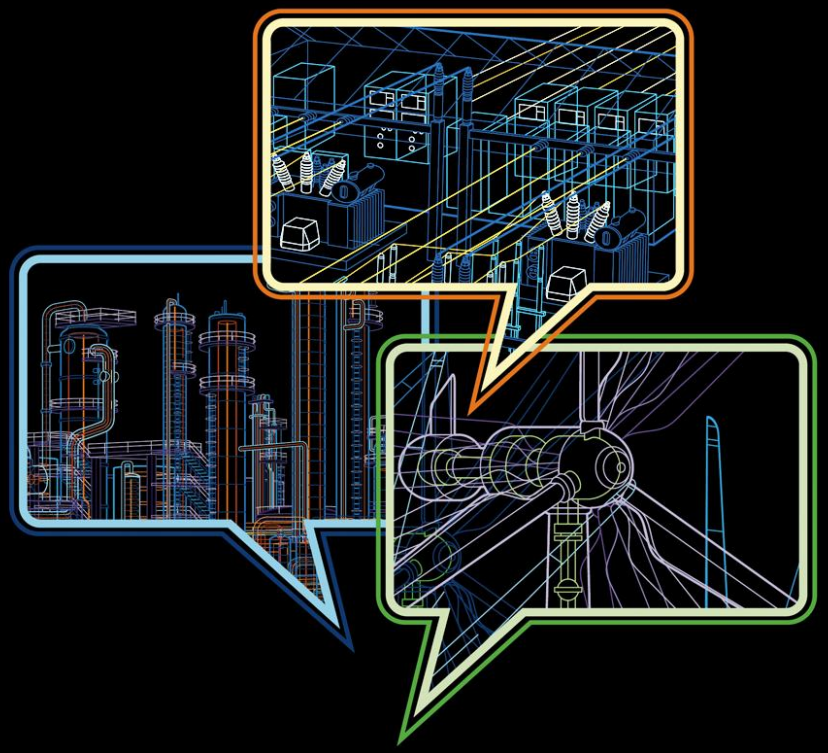


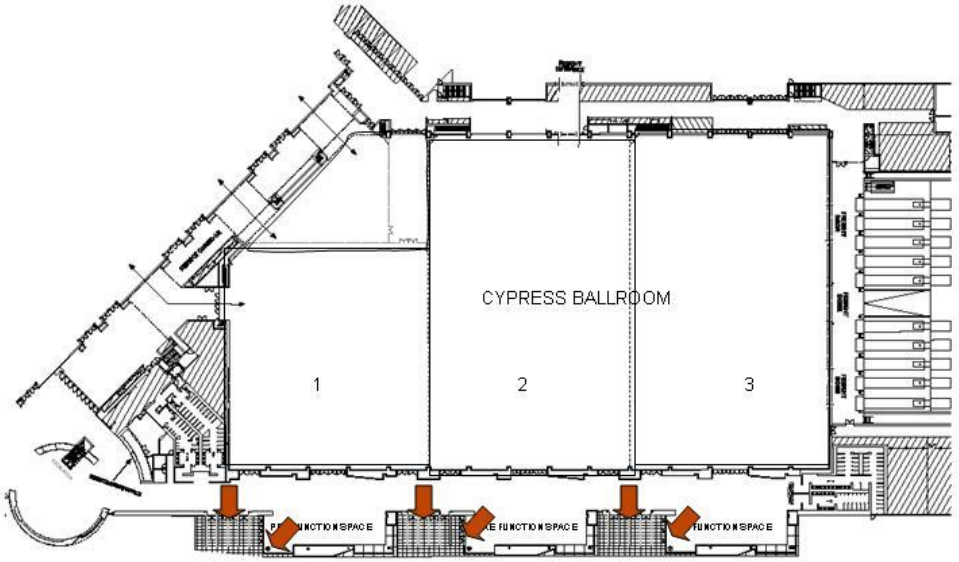
ABB Automation & Power World: April 18-21, 2011

WSE-106-1
Cyber Security in the System Lifecycle - ABB's commitment

Your safety is important to us
Please be aware of these emergency procedures

- In the event of an emergency please dial ext. 55555 from any house phone. Do not dial 9-1-1.
- In the event of an alarm, please proceed carefully to the nearest exit. Emergency exits are clearly marked throughout the hotel and convention center.
- Use the stairwells to evacuate the building and do not attempt to use the elevators.
- Hotel associates will be located throughout the public space to assist in directing guests toward the closest exit.
- Any guest requiring assistance during an evacuation should dial “0” from any house phone and notify the operator of their location.
- Do not re-enter the building until advised by hotel personnel or an “all clear” announcement is made.

Your safety is important to us
Convention Center exits in case of an emergency



Know your surroundings:

- Identify the meeting room your workshop is being held in
- Locate the nearest exit

WSE-106-1
Cyber Security in the System Lifecycle
- ABB's commitment

- Speaker name : Akilur Rahman
- Speaker title : PA Division Cyber Security Manager
- Company name : ABB
- Location : Switzerland

- Speaker name : Markus Braendle
- Speaker title : Head of Group Cyber Security
- Company name : ABB
- Location : Switzerland

- Speaker name : Bart de Wijs
- Speaker title : PS/PP Division Cyber Security Manager
- Company name : ABB
- Location : The Netherlands

Cyber Security in the System Lifecycle
ABB's Commitment

Cyber Security is About
- People
- Organizations
- Processes
- Technology & Solutions.

- Cyber Security addressed through the entire system lifecycle
  - Early design and development
  - Commissioning and installation
  - Throughout operations.

Many steps ABB is taking to ensure that cyber security is addressed in all phases of a system's lifecycle.

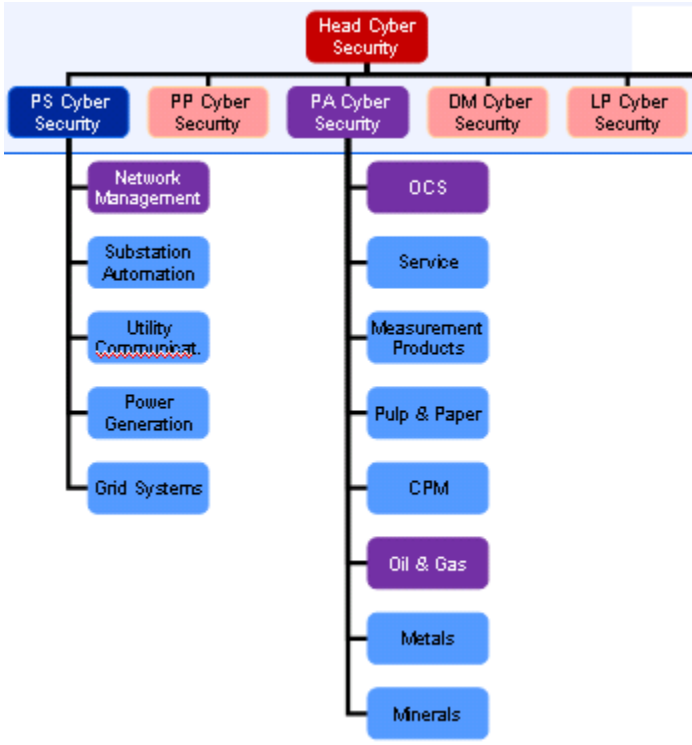
How our systematic approach addresses
- Product and system security
- How it benefits our customers

Cyber Security in the System Lifecycle
ABB's Organization

Group Cyber Security Council

Division Level Security Council

Business Unit Security Team



- Help customers to reduce their business & compliance risks due to Cyber Security
- Enable Business Units to reduce business risks (financial, quality, compliance and market image) due to Cyber Security
- Create enhanced service/consulting offerings to customers in Cyber Security

by

- Capturing and analyzing security requirements from the market & customers
- Developing common security policy, best practices, guidelines, processes and specifications to support Product & Plan Lifecycle
- Raising awareness, developing skills/competencies & knowledge sharing in Cyber Security

Cyber Security in the System Lifecycle
ABB's Preparedness

- External Engagements
  - ABB has established Security Councils acting as the Computer Emergency Response Team (CERT) for ABB
  - Established contacts with ICS-CERT and NERC
  - Expanding network of engaged third-party security researchers, including Idaho National Labs
- Engagement in cyber-security related standards
  - ISA99: Full membership
  - IEC62351: Full membership
  - NERC-CIP: Reviewing member
  - NIST SGIP-CSWG: Full membership
- Strategic partnership with Industrial Defender

Cyber Security in the System Lifecycle
ABB's Objectives

Cyber security embedded

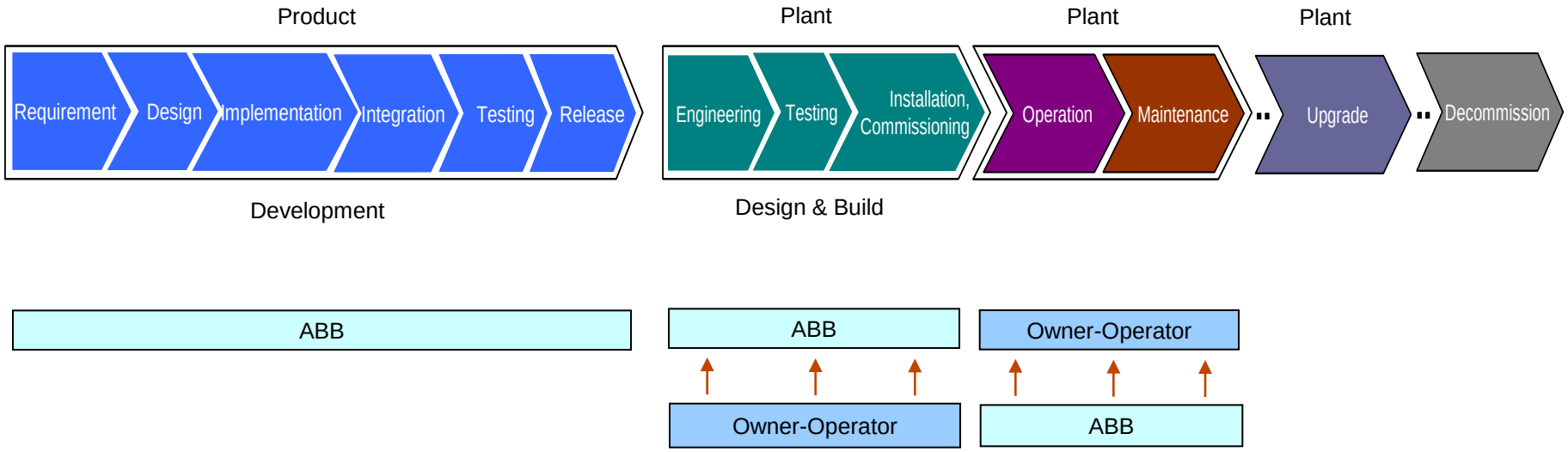
- Embedded in the product lifecycle
- Embedded in our organization
- Embedded in our products and systems

Cyber security without compromises

- No compromise on reliability
- No compromise on interoperability
- No compromise on security

Cyber security - Addressed throughout the system life cycle

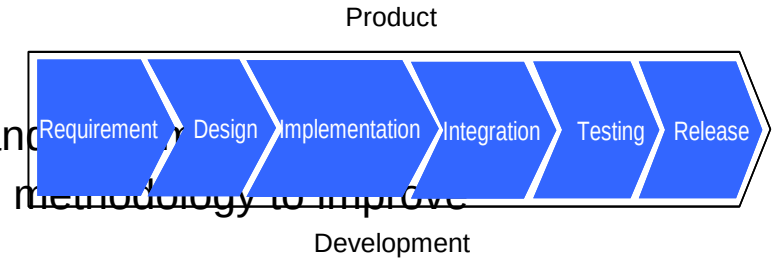
Cyber Security in the System Lifecycle
From our Product Lifecycle to your Plant Lifecycle



Cyber Security in the System Lifecycle
Security in Product Design & Development

Requires understanding of threats

- Security assessments of products and
- Development of new tool-supported methodology to improve and formalize threat modeling

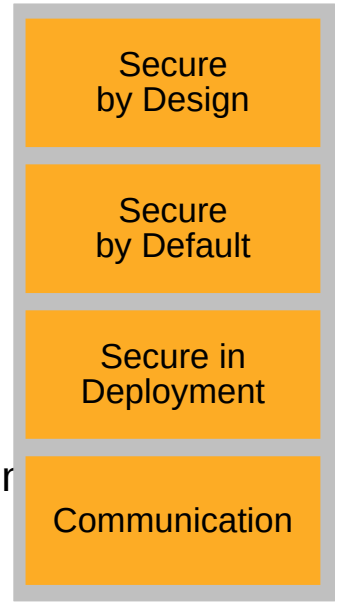


Secure development requires know-how

- Security training for developers

Security design and development for

- Products (e.g. security features)
- Systems (e.g. network architecture)
- As early as possible for new products
- As feasible as possible for existing solutions



Security is an integrated but explicit part of our design development processes

Cyber Security in the System Lifecycle
Product Requirements

Continuously Capturing Requirements from

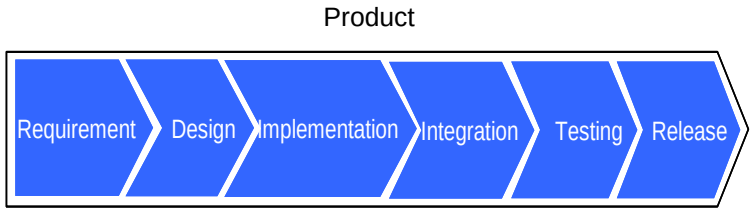
- Customers
- Industry groups
- Regulatory Bodies
- Standardization Bodies

To develop Products with enhanced security

Cyber Security in the System Lifecycle
Product Requirements

Continuously evaluating Products for measurable Improvements based on

- Standards
- Specifications



3.00 supported system-wide in an integrated fashion
2 supported in most parts of the system, but not integrated
1 supported in some parts of the system, but not integrated
0 not supported
n/a not applicable (needs strong justification!)

ISA 99.03.03 System Security Requirements Evaluation — Rating: 2.82

1. Access Control — Rating: 3.00
Identify and authenticate IACS users (incl. human users, processes, and devices), assign them to a pre-defined role, and allow them access to the system or assets.
- 1.1 IACS User Identification and Authentication — Comments: 3.00
- 1.2 Account Management — Comments: 3.00
- 1.3 Access Enforcement — Comments: 3.00
- 1.4 Indentifier Management — Comments: 3.00
- 1.5 Authenticator Management
- 1.6 Authenticator Feedback
- 1.7 Unsuccessful Login Attem
- 1.8 System Use Notification
- 1.9 Previous Logon Notificati
- 1.10 Session Lock
- 1.11 Remote Session Terminat
- 1.12 Remote Access
- 1.13 Device Identification and

2. Use Control
Enforce the assigned privileges of an
to perform the requested action on t
monitor the use of these privileges.

3. Data Integrity
Ensure the integrity of information o

3. Data Integrity — Rating: 3.00
Ensure the integrity of information on communication channels and in data repositories to prevent unauthorized manipulation.

4. Data Confidentiality — Rating: 3.00
Ensure the confidentiality of information on communication channels and in data repositories to prevent dissemination.

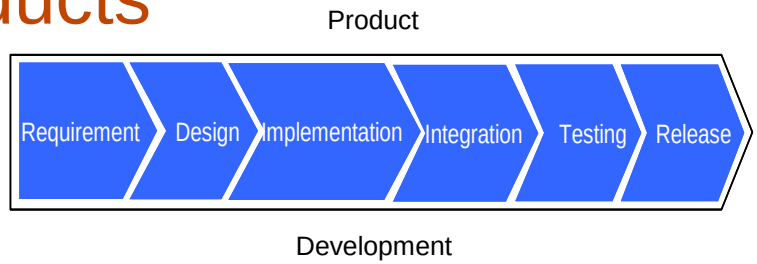
5. Restrict Data Flow — Rating: 3.00
Segment the system via zones and conduits to limit the unnecessary flow of data.

6. Timely Response to Events — Rating: 2.50
Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and taking timely corrective action when incidents are discovered.

7. Network Resource Availability — Rating: 2.54
Ensure the availability of the system or assets against the denial of essential services.

Cyber Security in the System Lifecycle
Technology Applications in Products

- Identify/Develop Core Technologies in-house
- Partnering with Industry Security Leader: Industrial Defender
- Adaptation/validation of other 3rd party Technology & Solutions for enhanced security



Integrate security solutions from Enterprise IT
e.g. IPSec, AV, …

Integrate specialized, tailored or modified security solutions,
e.g. FW, IDS, …

Develop built-in security features,
e.g. authentication, access control, network filter, storm filter, data diodes, …

Test & Verify

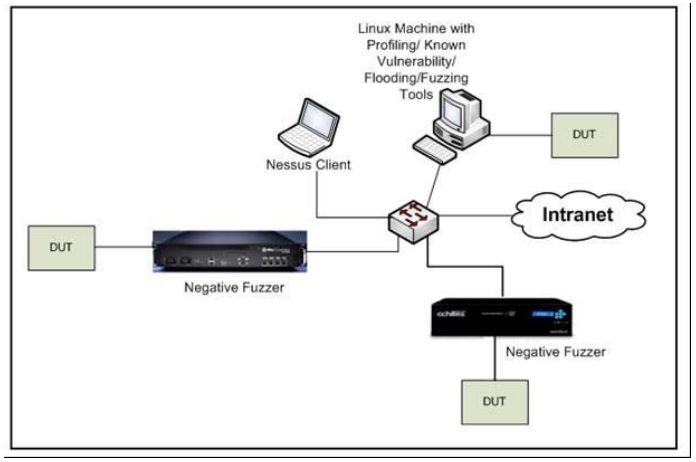
Cyber Security in the System Lifecycle
ABB's device security assurance center

Product

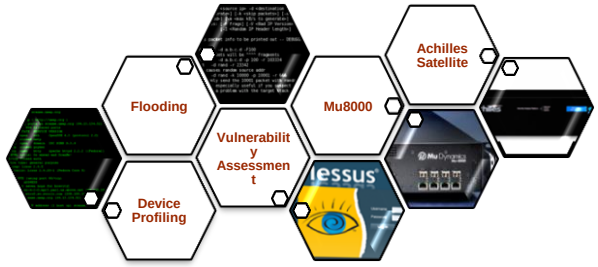
Development

Product Robustness Testing

- Assures consistent approach in carrying-out security/robustness testing for devices
- Formalized part of all device development
- Strengthen quality of communication stacks
- Verify and enhance the security posture of devices
- Around 200 tests planned in 2011
- Results also in guidelines for developers

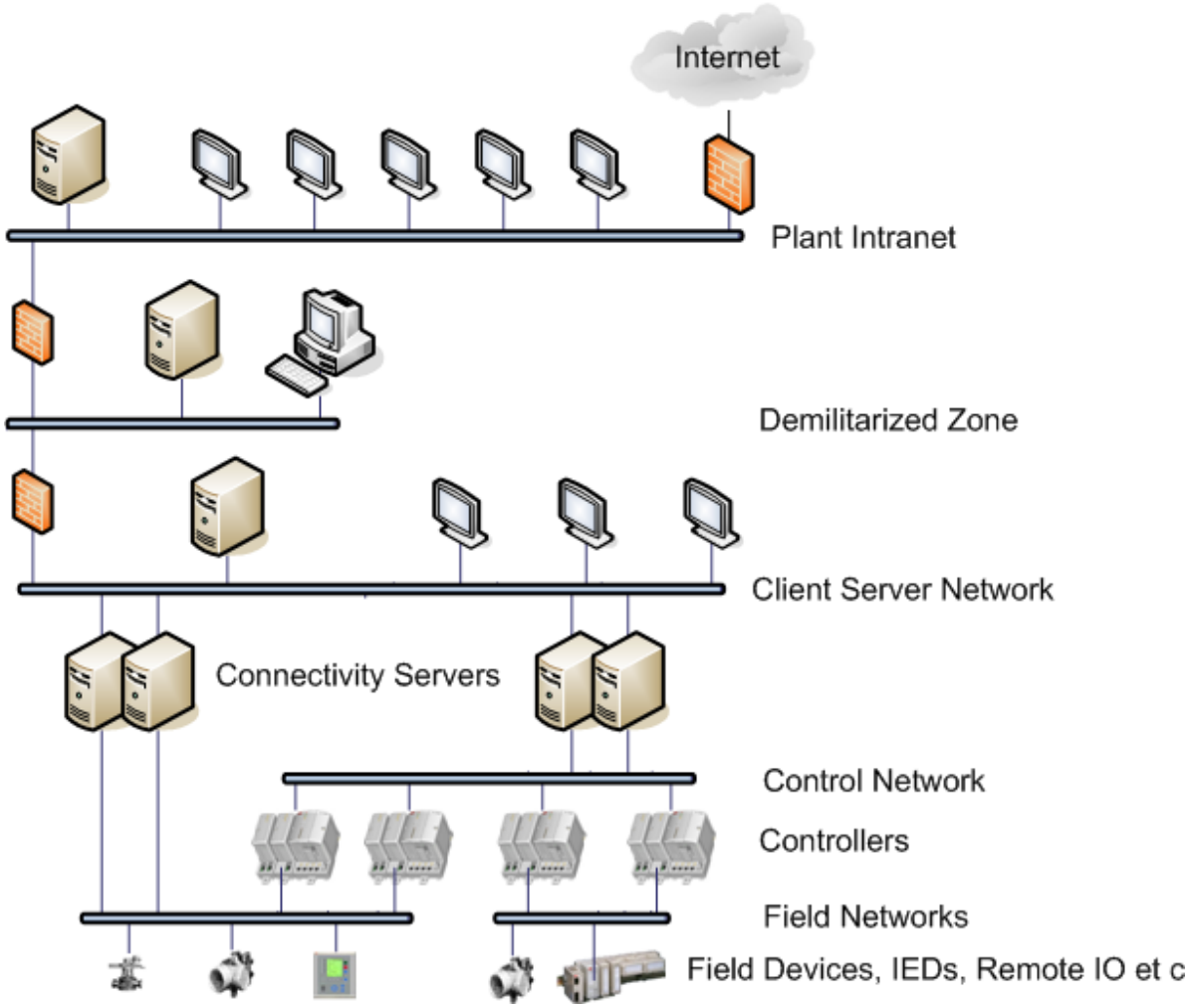


Testing in System Environment (Simulated/Typical Configuration)



Cyber Security in the Plant Lifecycle
Product to Plant System Design (System 800xA)

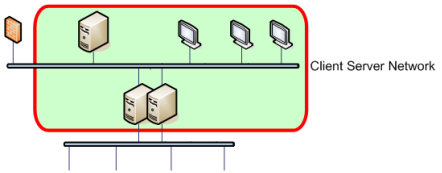
Security Zones: Multiple Network layers



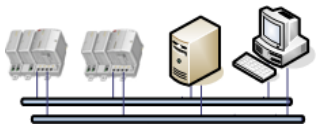
Plant

Design & Build

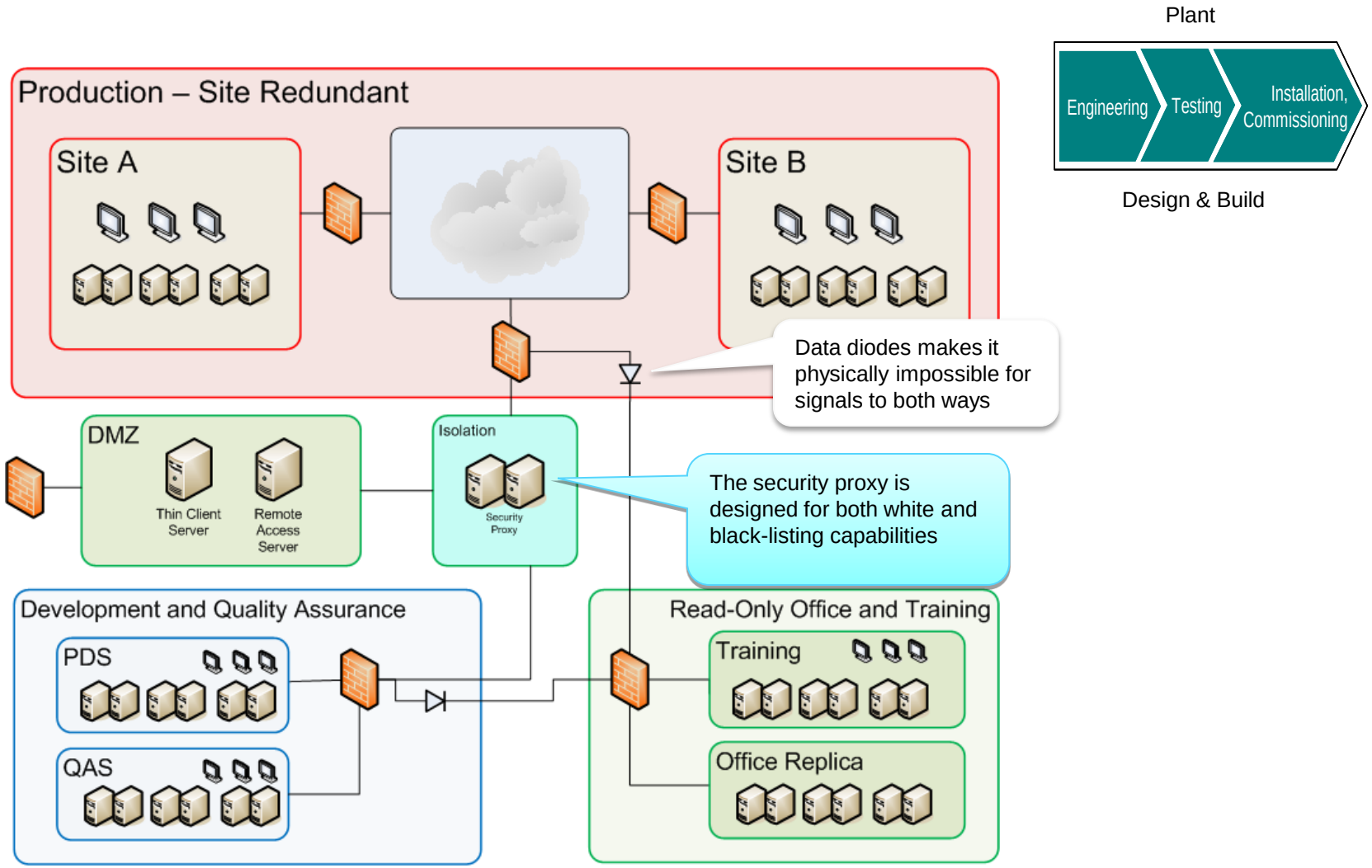
IPSec
protection



Redundancy with
Separated networks



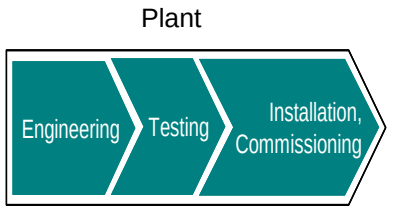
Cyber Security in the Plant Lifecycle
Product to Plant System Design (Network Manager)



Cyber Security in the Plant Lifecycle
Installation & Deployment

Installation/Deployment Guidelines to ensure system is properly configured using available security

- Capabilities
- Features
- Support



System 800xA
Network Configuration

Section 5 - Network Security

Establish a Network Security Policy
The Onion Approach
Firewalls
Connections to 800xA Systems through Firewalls
Connect Inside-out Instead of Outside-in
Network Address Translation in Firewalls
Single Firewall or a Demilitarized Zone
Connecting a single Firewall to a Redundant Network
Using an Extra Network for Remote Access
Redundant connection to external network
Virtual Private Networks (VPN) for Secure Connections

Section 6 - Domain Setup and Name handling

Node name handling and DNS
Choosing Names for Domains and PCs
Allocating 800xA Systems to Domains
Configuring Name Resolution and DNS
Which Nodes use host names
Location of Domain Controllers
Maintaining Redundant Domain Controllers
DcDiag: Domain Controller Diagnostics
Backups of Domain Controllers
Recovering after a Crash of the First Installed Domain Controller

Cyber Security Installation Guide

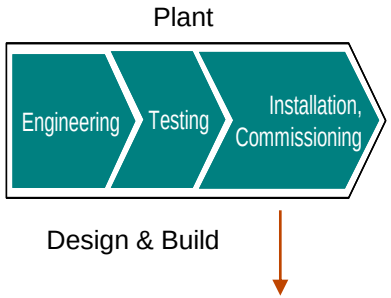
Implementation Manual

2 Prepare and Plan Installation
2.1 Determine network architecture
2.2 Typical zones
2.2.1 The Main Trusted Zone
2.2.2 The DMZ
2.3 IP Plan
2.4 Determine Name Resolution Strategy
3 Software Preparation
3.1 Windows Server Version
3.2 Support Tools
3.2.1 Active Directory Tools
3.2.2 SSH Tools
4 Active Directory
4.1 First Time Install
4.1.1 Installation of primary Domain Controller
4.1.2 Scrubbing the primary Domain Controller
4.1.3 Installation of secondary Domain Controller
4.1.3.1 Setup the Acti
4.1.3.2 Setup Read-C
4.2 Install UNIX Ident
4.3 Install and Config
4.4 Population of Act
4.4.1 Install Security C
4.4.2 Run Security Cor
4.4.3 Completion of the
4.4.3.1 Authentication
4.4.3.2 Setting Acces
4.5 Windows Integrat
4.5.1 Configure Name
4.5.2 Install MIT Kerbe
4.5.3 Configure Kerber
4.5.4 Increase Ticket L
4.5.5 Test configuratio
4.6 Increase Ticket L
5 Network Partitioning (Zones)
5.1 Overview
5.2 SpiConf Considerations
5.3 Security Configuration Tool Considerations
5.4 Kerberos Considerations
5.5 Setting up Trust between Domain Controllers
5.5.1 Verify DNS Settings
5.5.2 Configure Trust
6 Network Time Configuration
6.1 Overview
6.2 Configuration of Windows Time Service (WTS)
7 Base Level Hardening
7.1 Vulnerability Scanning – Before
7.2 Hardening of Windows hosts
7.3 Hardening of Linux hosts
7.4 Installation of OSSEC
7.5 Vulnerability Scanning – After
8 Troubleshooting
8.1 Configuration Verification Checklist
8.2 Problems during installation of Domain Controller and/or roles
8.2.1 OS Version not Standard Edition
8.2.2 OS Version not R2
8.2.3 OS Version not Service Pack 2
8.2.4 Other hosts are unable to connect to the Domain Controller
8.3 Problems related to UNIX Identity Management integration
8.3.1 The getent command does not return expected information

Cyber Security in the Plant Lifecycle
Installation & Deployment

Checklist for Project & Services to ensure Installation is done

- Following Installation/Deployment Guidelines
- Based on Security Policy
- With proper hand-over to Owner-Operator for Secured Operation & Maintenance



2.1 Deployment in Projects & Services

Item #	OK: checked and ok NO: checked and not ok NA: not applicable Blank not checked	Status	Reference
1	**Process Engineering**		
1.1	Does the customer have a Security Policy document for process control systems, and has this document been reviewed? If yes, can it be used as is or is there a need to make a specific document with exceptions or additions for this project?		
1.2	Have all project members been trained in basic IT security as specified by this checklist, or in the Security Policy provided by the customer?		
1.3	Have you checked for any relevant international process control security standards that need to be complied with in the project? If yes, provide a list of references.		
1.4	Has a security risk assessment been carried out and a mitigation plan been made?		

2	**Detailed Engineering**	
2.1	Is security addressed & described in a design specification document? If yes, provide a reference to the document(s).	
2.2	Is all communication between different systems, devices and domains well defined? Are there security perimeter protection devices (e.g. firewalls) in place to segregate the systems and control the communication?	
2.3	Have common mechanisms for clock	

3	**Build**	
3.1	Has anti-virus software been installed and configured according to the guidelines from the system manufacturer? Is there a strategy for handling updates of this system?	
3.2	Has a patch management system been installed	

4	**Testing (FAT/SAT)**	
4.1	Have you verified that the functions for protection against malicious code (e.g. viruses) work without affecting the system's normal functionality?	
4.2	Has a complete scan of the system been	

5	**Commissioning**	
5.1	Have all mechanisms for automatic update, patching and remote access been reconfigured to use the operations solutions, rather than the engineering solutions?	
5.2	Are there any temporary solutions that has been	

6	**Customer Handover**	
6.1	Have you identified an ABB security contact to interact with the customer on IT security issues and providing the customer with: - timely information about cyber security vulnerabilities - timely support and advice to the customer in the event of cyber security incidents If yes, please provide the contact information for reference	

Confirmation:

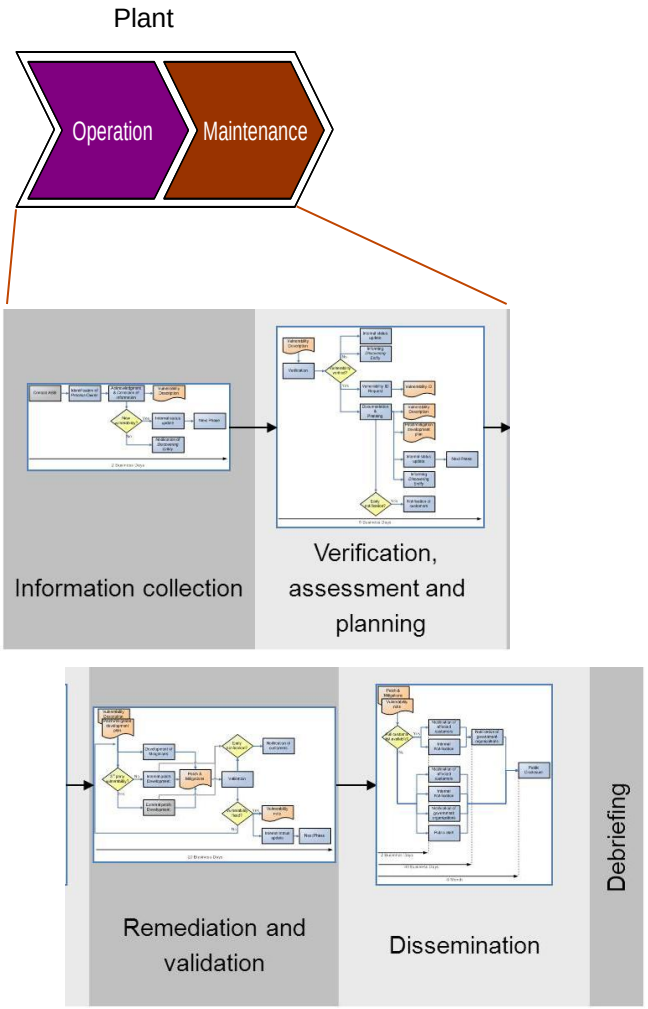
Date :	<ABB>	<Customer>	<Other supplier>
	Signature	Signature	Signature
	Printed name	Printed name	Printed name

Cyber Security in the Plant Lifecycle
Vulnerability/Incident Response

Provide Response & Mitigation measures to customers/discovering entities with

- Plan for analysis, validation and mitigation measures for the vulnerability
- Security advisory (general and/or product/service specific)
- Product/service bulletin/alert/update
- Security validation status of products/services with respect to related 3rd party system/software
- Security update on specific customer/use-case
- Update of ABB product/service with fixes/mitigation measures
- Final closure of the vulnerability case

ABB has an Emergency Response team with all necessary skills and authorities to respond to any critical Cyber Security vulnerability or incident and to provide faster mitigation measures.



Cyber Security in the Plant Lifecycle
Enhancing/Maintaining Security

Diagnose (Fingerprints)

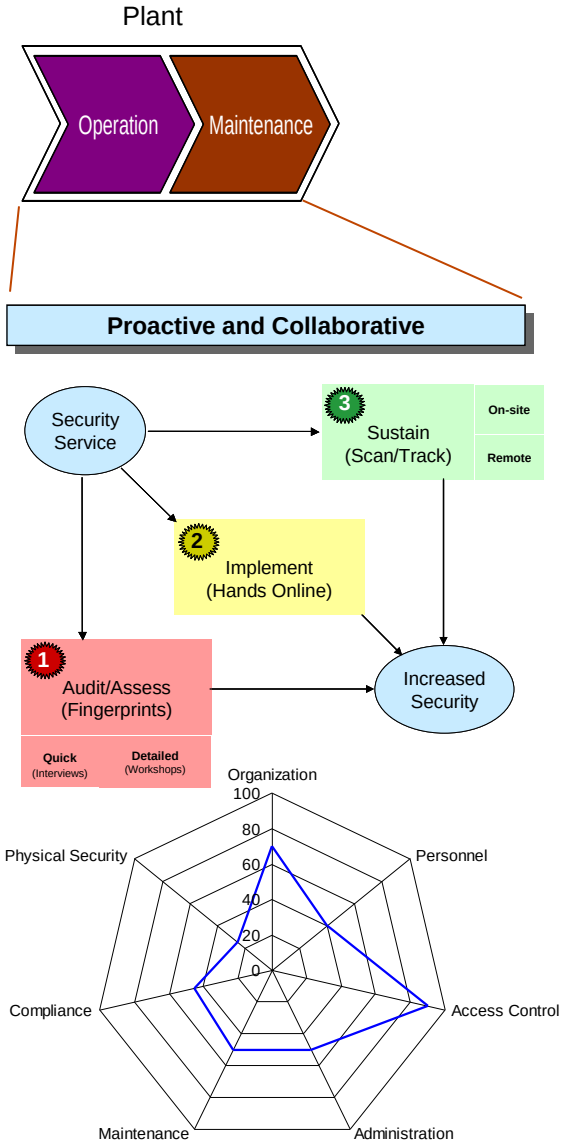
- Benchmark policy: define gap
- Forecast compliance
- Define action plan

Implement

- Apply action plan: fix gap
- Define monitor plan

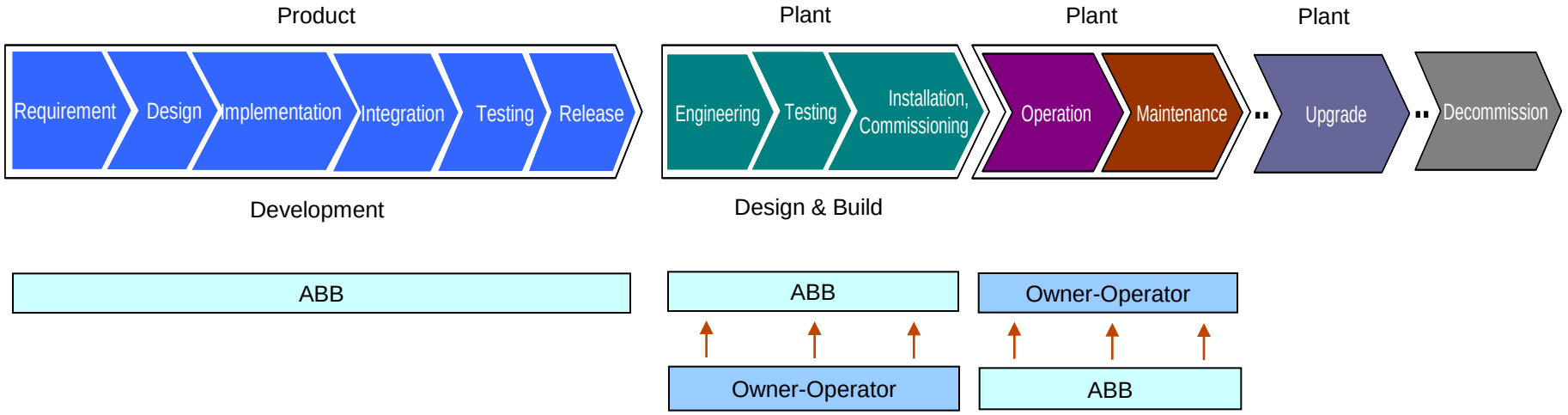
Sustain (Scan/Track)

- Maintain compliance: keep fixed
- Proactive improvements
- Define vulnerability triggers
- Vulnerability-triggered improvements



Cyber Security in the System Lifecycle
ABB's Commitment

- As technology leader, ABB fully understands the importance of and its role in Cyber Security for industrial control systems.
- ABB is actively anticipating the security challenges imposed by the changing landscape of the markets.
- ABB is constantly adapting its systems to the latest developments in security and is engaging with external partners for security testing and consulting.
- ABB has been involved in cyber security for control systems for over a decade - long before the hype.



Reminders
Automation & Power World 2011

- Please be sure to complete the workshop evaluation
- Professional Development Hours (PDHs) and Continuing Education Credits (CEUs):
  - You will receive a link via e-mail to print certificates for all the workshops you have attended during Automation & Power World 2011.
  - BE SURE YOU HAVE YOUR BADGE SCANNED for each workshop you attend. If you do not have your badge scanned you will not be able to obtain PDHs or CEUs.

Power and productivity
for a better world™