ABB ICS Cyber Security Reference Architecture

Examining the benefits, challenges, and considerations when adopting a reference architecture for industrial systems
A reference architecture supports the whole company.

**Engineering**
Reduce engineering and auditing costs by documenting your systems in a consistent manner.

**Compliance**
Approach compliance and regulation with confidence, knowing that the network is cyber security enabled.

**Digitalization**
Approach new and evolving business needs confidently, knowing digital services are added without jeopardizing security.
A reference architecture is a document or set of documents that provides **recommended structures** and integrations of IT products and services to form a solution.

The reference architecture embodies accepted **industry best practices**, typically suggesting the optimal delivery method for specific technologies.
ICS Cyber Security Reference Architecture

**Level 0**: Process
- Field Devices

**Level 1**: Local or Basic Control
- Field Devices
  - Controllers, PLC, I/O, com bus

**Level 2**: Supervisory Control
- South Firewall
  - Domain controllers
  - System servers
  - Workplaces
  - Engineering
  - Backup server
  - Protocol converter

**Level 3**: Operations Management
- North Firewall
  - Remote access
  - Security updates
  - Malware protection
  - Backup server
  - Data exchange
  - Historian
  - IoT Gateway
  - Application server
  - Domain controller

**Level 4**: Enterprise Business Systems
- Cloud/Internet
  - ABB Ability™ Genix
  - Remote access
  - Servers
  - Clients

System Management
- Engineering
  - Workplaces
  - System servers
  - Domain controllers
  - Backup server
ICS Cyber Security Reference Architecture

**LEVEL 0**
Process

**LEVEL 1**
Local or Basic Control

**LEVEL 2**
Supervisory Control

**LEVEL 3**
Operations Management
- Historian
- IoT Gateway
- Application server
- Domain controller
- South Firewall

**LEVEL 4**
Enterprise Business Systems
- ABB Ability™ Genix
- Remote access
- Servers
- Clients
- North Firewall
- Remote access
- Security updates
- Malware protection
- Backup server
- Data exchange
- Historian
- IoT Gateway
- Application server
- Domain controller
- North Firewall
- Servers
- Clients
- Remote access
- Security updates
- Malware protection
- Backup server
- Data exchange

**LEVEL 5**
System Management
- Servers
- Clients
- Remote access
- Security updates
- Malware protection
- Backup server
- Data exchange
- Historian
- IoT Gateway
- Application server
- Domain controller
- North Firewall
- Servers
- Clients
- Remote access
- Security updates
- Malware protection
- Backup server
- Data exchange

**LEVEL 6**
Cloud/Internet

- Field Devices
- Controllers, PLC, I/O, com bus
- Protocol converter
- Field Devices
1. Customer provided a network architecture drawing that represents their typical ABB 800xA sv6.0 system implementation.

The next slide will transform this drawing into the ABB Reference Architecture format.
Customer Architecture
Transformed Architecture

2.

This is a transformation of a customer’s architecture into the ABB reference architecture format for easy comparison.

The next slide will show any gaps between the customer’s current architecture and ABB’s Reference Architecture.
Customer Architecture
Implementation View

3.

Step 1
A. Implement System Management area to have a place for current and future cyber solutions.

Step 2
B. Increase resilience by adding RNRP routing. Eliminating one of the single point of failures.

Step 3
C. Adding controller firewall
D. Remove Dual-Homed server
ABB ICS Cyber Security Reference Architecture
Use-case

IoT Gateways (or any buzzword)

YOU

“We see the value in [insert buzzword here], but don't think it can be done securely.”

ABB

We created the architecture with this in mind. Correctly implemented, you can reap the benefits of these new technologies with only negligible increased cyber risk.
ABB ICS Cyber Security Reference Architecture
Simplicity saves

Source: Cost of a data breach 2023 | IBM
Risk Reduction Roadmap
The Industrial Cyber Security Journey

1. Assess
   - Fingerprint
   - Risk Assessment

2. Plan
   - Consultancy
   - Reference Architecture

3. Implement
   - System Hardening
   - Asset Inventory
   - Malware Protection
   - Security Updates
   - Backup

4. Sustain
   - Application Allowlisting
   - Training
   - Asset Inventory

5. Detect
   - Network Monitoring
   - Event Monitoring
   - Maintenance

6. Monitor
   - Cyber Security Workplace™
   - Related Services
   - Application Allowlisting

7. Respond
   - Incident Response
   - Security Operations
   - Related Services
   - Maintenance
How to meet today’s cyber security challenges

Implement a defensible architecture
Control communication between devices, zones, and levels.

Deploy foundational security
Deploy protection against malware and known vulnerabilities.

Monitor for malicious activity
Detect malicious activity early and give yourself time to respond.