ABB ICS Cyber Security Reference Architecture

The proven and consistent way to protect your Industrial Control Systems from cyber attacks

Industrial companies looking to avoid the devastating and costly impacts of cyber attacks need a proven and consistent approach.

They need a blueprint for planning, implementing and deploying industrial control system networks using industry best practices and IEC standards.

ABB ICS Cyber Security Reference Architecture is that blueprint.

ABB ICS Cyber Security Reference Architecture

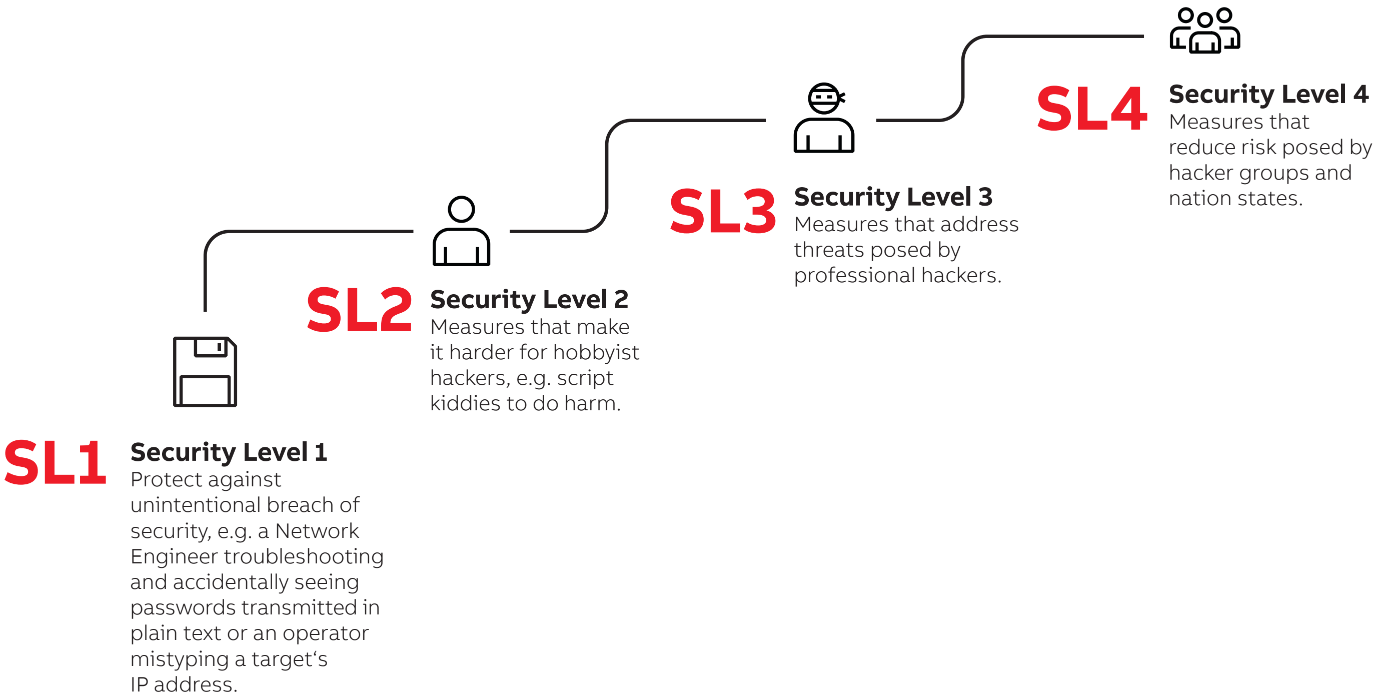
The ABB ICS Cyber Security Reference Architecture is a proven and consistent approach to planning, implementing, and deploying industrial control system networks using industry best practices and IEC standards. As a template solution, it provides a common vocabulary for discussing implementations, often with the aim of stressing commonality.

The ABB ICS Cyber Security Reference Architecture is vendor agnostic and based on the IEC 62443 control system security standard to create a secure area between the production and external systems.

While the architecture significantly improves cyber security posture, it is not a guarantee to pass external audits or that the system is secure.

Achieve Security Level 4

Use this reference architecture to develop a system to achieve Security Level 4. It helps you design an architecture that protects your production against the most basic cyber attacks right up to advanced, sophisticated attacks.



SL1 **Security Level 1**
Protect against unintentional breach of security, e.g. a Network Engineer troubleshooting and accidentally seeing passwords transmitted in plain text or an operator mistyping a target‘s IP address.

SL2 **Security Level 2**
Measures that make it harder for hobbyist hackers, e.g. script kiddies to do harm.

SL3 **Security Level 3**
Measures that address threats posed by professional hackers.

SL4 **Security Level 4**
Measures that reduce risk posed by hacker groups and nation states.

How it works

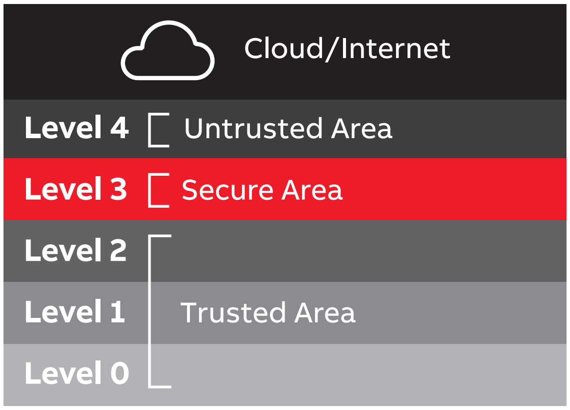
The ABB ICS Cyber Security Reference Architecture is based on the five levels found in the IEC 62443 reference model, as described in IEC 62443-1-1.

4	**Enterprise Systems:** Customers' local IT structure with office computers and other business-related systems	
3	**Operations Management:** Devices that add functionality but are not critical to the operation of the facility	**System Management:** Solutions that are used to manage the system's security but are not needed for operating the process.
2	**Supervisory Control:** Distributed Control System	
1	**Local or Basic Control:** Controllers, I/O and Fieldbus communication	
0	**Process:** Field instruments and devices that directly measure or control the process	

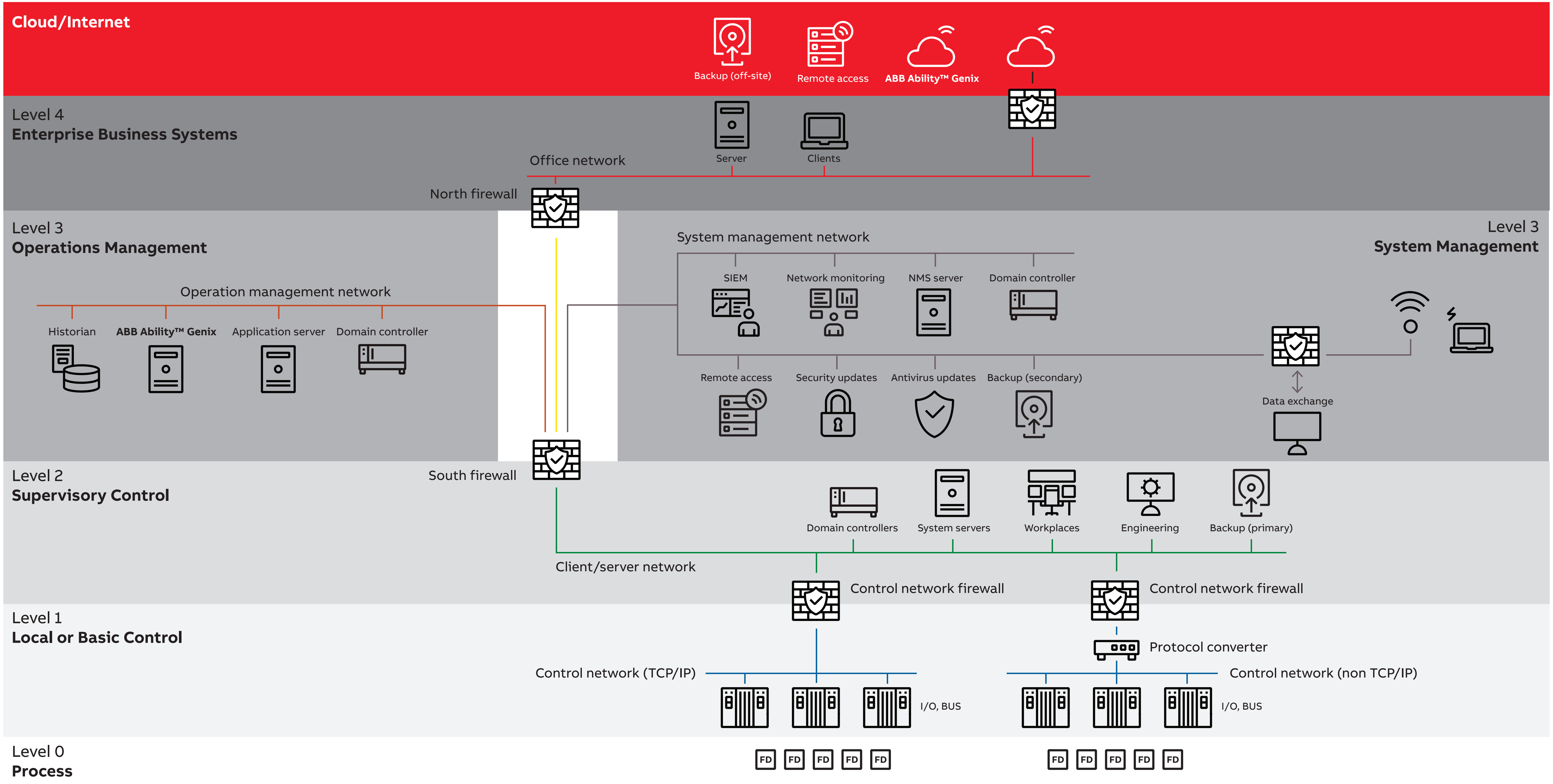
ABB's reference architecture adds a system management area in level 3 to help reduce complexity while maintaining security.

Separating the trusted from the untrusted
The ABB ICS Cyber Security Reference Architecture eliminates the need for an additional secure area, often called DMZ or Level 3.5, that separates the trusted area (Levels 0, 1, 2, 3) from the untrusted area (Levels 4, 5) by using Level 3 as the secure area between the trusted and untrusted areas.

This unique approach reduces complexity, keeps the Architecture consistent with IEC principles while not breaking from the 62443 model, and lets communication flow from trusted to untrusted areas while maintaining security.



Reference architecture



Use cases

Use Case 1: Remote Access

Customer challenge

“We realize that remote access is valuable, but we are concerned that our remote access isn’t secure, or that it will break our compliance.”

ABB solution

The ABB ICS Cyber Security Reference Architecture uses Level 3 as a data transfer zone between your untrusted and trusted area. This helps you deploy remote access without increasing your risk or breaking your compliance.

Use Case 2: Compliance

Customer challenge

“My CISO told me that I must get my control system certified by the end of the year. Will the ABB ICS Cyber Security Reference Architecture make me compliant?”

ABB solution

Implementing the ABB ICS Cyber Security Reference Architecture will not make you compliant. But it will help you meet some of the compliance requirements related to data control and architecture.

Minimize Your Cyber Security Risks

The ABB ICS Cyber Security Reference Architecture provides secure access to production data to enable better decisions, enable IIoT and maintain robust security.

To mitigate cyber security risks, you need a solid architecture for your OT systems. That's because your reference architecture is the keystone of OT security and your go-to document.

Make Better Decisions

Collects data from all devices without compromising security—so that you make better informed operational decisions.

Enable IIoT

Serves as an enabler for deployment of IIoT and digital services so that you continue on your path towards operational excellence.

Maintain Security

Enables you to create zones and conduits in accordance with 62243 and other standards for increased security.

Why ABB

People

ABB pioneered the development of electrical and automation technologies and has **years of experience helping customers protect control systems** and other automation assets.

Process

ABB's control systems are present globally across many industries. **We know the type of cyber threats our customers face and what needs to be done to mitigate risks.** We stay ahead of threats by investing heavily in research and development to continuously improve our security offerings.

Technology

ABB can support our customers throughout the lifecycle of their assets through our products, services and expert operations by making technology relevant to customers in industrial sector.

—

ABB
Operating in more than 100 countries

www.abb.com/cybersecurity