Control System IT Security Executive Overview
Control System IT Security is the practice of defending the control system IT assets and database from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Control System IT Security is about closing the ‘gaps‘ through which ‘intruders‘ can get into the control system environment.

Control System IT Security is about early planning to integrate IT security measures in the Functional Design Specifications of the control system. It is that important nowadays.
Control system IT security
Myths and Facts

Myth: My control system is not connected to the Internet. I do not have to worry and there is no need for any security measures.

Myth: Virus Scanners slow down my control system. I do not need them because they slow down my system performance.

Myth: My control system is redundant at all levels and it can tolerate the breakdown of any single component. There is no need for any further security measures.

Fact: Control systems are no longer considered as ‘Islands’ on their own. They have, in most cases, to communicate with other equipment on the outside.

Fact: Networking is on the march. There is no way to reverse this trend.
Fact: Control System built-in defense against cyber attacks is not enough on its own. There is a strong need to supplement such a cyber defense with additional products and measures.

Fact: A large number of installed control systems are old and are rarely updated. They are vulnerable in one way or another.

Fact: IT security costs money and needs human resources.

Fact: IT security is a control system life cycle issue. Regular verification and updates is a must.

Fact: 100% security is not possible. There is not such a thing.
Control system security
A defense strategy

All aspects of control system security must be considered and addressed for a meaningful and comprehensive defense strategy.
Control system security
The threats

- Unauthorized access to the control system
- Unauthorized changes to the control system
- Laptops temporarily connected to the field networks
- Unexpected or excessive network traffic on field networks
- Manual data transfer from the control system (e.g., history)
- Manual data transfer into the control system (e.g., updates to control logic)
- Laptops temporarily connected to the control system networks
- Network connections to enterprise systems
- Network connections for remote support by the supplier
- Network connections to other control systems
- Manual data transfer from the control system (e.g., history)
- Manual data transfer into the control system (e.g., updates to control logic)
- Laptops temporarily connected to the control system networks
- Network connections to enterprise systems
- Network connections for remote support by the supplier
- Network connections to other control systems
- Unexpected or excessive network traffic on field networks
Control system security
The Protection Measures

- Unauthorized access to the control system
- Unauthorized changes to the control system
- Network connections to enterprise systems
- Network connections for remote support by the supplier
- Network connections to other control systems
- Secure remote access platform

Control and monitoring of portable media device usage

Manual data transfer from the control system (e.g., history)

Manual data transfer into the control system (e.g., updates to control logic)

Secure network architectures with zoning concepts and managed interfaces

Firewalls and traffic rate limiting

Patch management for timely deployment of security updates

Authentication and authorization on user and device level

Unauthorized changes to the control system

Laptops temporarily connected to the control system networks

Laptops temporarily connected to the field networks

Secure communication with IPSec

Secure remote communication with IPSec

Strict change and configuration management

Network connections to the field networks

Redundancy with separated networks

Robust communication stacks with rate limiting

Security information and event management (SIEM)

Malware protection with antivirus and application whitelisting

Secure network architectures with zoning concepts and managed interfaces

Firewalls and traffic rate limiting

Network connections to enterprise systems

Network connections for remote support by the supplier

Network connections to other control systems

Secure remote access platform

Patch management for timely deployment of security updates

Authentication and authorization on user and device level

Unauthorized changes to the control system

Laptops temporarily connected to the control system networks

Laptops temporarily connected to the field networks

Secure communication with IPSec

Secure remote communication with IPSec

Strict change and configuration management

Network connections to the field networks

Redundancy with separated networks

Robust communication stacks with rate limiting

Security information and event management (SIEM)
ABB understands the importance of IT Security for Industrial Automation customers and is offering the following services under the Automation Sentinel program:

- Daily Verification Reports for Antivirus Scanners. This service is included in Automation Sentinel Agreement.

- Microsoft Security Patches testing and validation. This service is included in Automation Sentinel Agreement.

- A monthly delivery service of MS Security patches and Antivirus scanners verification reports to customer sites on suitable media. This service can be obtained by means of an Add-on to the Automation Sentinel Agreement.

- Industrial Defender (ID) for System 800xA and Cryptzone "800xA whitelisting SE46“ are new software options released as part of the System 800xA V5.1 FP4. Software updates for these System 800xA license options are covered through an Add-on to the Automation Sentinel Agreement.
Control system security
Virus Scanners

- To remain protected, ABB systems must update the latest DAT files of the Virus Scanner software on regular basis.
- McAfee and Symantec release updates at regular intervals, usually several times a week.
- ABB verifies these updates for selected ABB control systems and selected software versions as soon as they are available to ensure that the virus scanner does not detect legal code as a ‘false positive’.
- A ‘false positive’ means that an Anti-virus update on a particular date is impacting the control system operations in an adverse way. Once identified, a product bulletin is issued and appropriate measures are taken.
- The document “System daily verification of updates” is regularly updated and published through the ABB Solutionsbank and lists the DAT file version which have been verified for the ABB control system in question.
Microsoft Security Patches Testing Service

- Microsoft security patches are compatibility tested and validated for selected ABB control systems at selected software versions.
- Security patches management solutions
  - Testing Security patches with monthly updates
  - Testing results are published in Solutionsbank
- Security patches deployment solutions
- Response in case of product vulnerability
  - Field communication security bulletin or safety report or product alert if safety impact
- Microsoft security patches testing and validation service is covered under *Automation Sentinel subscription*. 
Validated security patches and documentation are delivered to customer site on suitable media.

ABB Microsoft Security Patch Delivery Service simplifies the process and reduces the risk of updating security patches.

This service is monthly and it includes security patches and bulletins for the current month.

McAfee Virus Scan patches, scan engine, and virus definition file updates are also included with the delivery.

Security Patch Delivery Service is available as an add-on for all Automation Sentinel agreements.
Power and productivity for a better world™