System 800xA Cyber Security
Maximizing cyber security in process automation
All businesses have intelligence worth protecting. In fact, the shape and size of your company’s future will be determined by your know-how, ideas and operations – and on your ability to protect them.

With so much at stake the big question is: How do you secure your company against cyber risks, like attacks from viruses, hackers and human errors?

ABB is committed to cyber security
Cyber security is important for every company. Without it, your company risks production disruptions, loss of intellectual property and data that cannot be recreated.

As for any ABB solution, we want you to be satisfied with the security solutions we provide you with.

We fully understand the importance of cyber security, and its responsibility to advance the security of control systems. You can rely on system solutions where reliability and security have the highest priority.

ABB helps secure your company’s future
The world of process automation is changing in the face of new technologies, opportunities and challenges. ABB remains committed to helping customers take advantage of technology advances while minimizing exposure to cyber risks.

Since ABB is a leading provider of control systems for a wide spectrum of industries, we can combine our technology strengths and domain expertise to provide a customer-focused solution that enhances asset productivity and efficiency.

The objective is to establish the necessary levels of cyber security, and maintain that level while preserving the availability and functional interoperability of systems.

If it is valuable to you, it is probably valuable to someone else
Why control system owners have to focus on cyber security

Industrial automation and control systems have evolved over the past decade thanks to technological advancements. At the heart of these advancements are specialized IT systems. To provide end users with comprehensive real-time information and allow for higher levels of reliability and control, these systems have become more and more interconnected.

The new generation of automation systems utilizes open standards, such as OPC, Profinet, FOUNDATION Fieldbus, IEC 61850, and commercial technologies, in particular Ethernet and TCP/IP-based communication protocols. They also enable connectivity to external networks, such as office intranet and the Internet. These changes in technology have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only in office or enterprise IT systems.

Cyber risks were inherited by adopting open IT standards. But fortunately, so were the cyber security mechanisms developed in enterprise environments to address those risks. These mechanisms enable the development of cyber security solutions tailored for industrial automation and control systems, and which utilize proven technology.

ABB fully understands the importance of cyber security, and its role to advance the security of control systems. ABB customers can rely on system solutions where reliability and security have the highest priority.

ABB’s systematic approach ensures cyber security

Over the past few years, the global industries have steadily increased their focus on cyber security for industrial automation and control systems. As a result, many different drivers and trends have emerged.

At ABB, we have always seen cyber security as a key requirement and are committed to provide products, systems and services that clearly address this vital issue. ABB takes a systematic approach to cyber security through its operations on a global level. For instance, ABB has established an organization with security councils on corporate and division level to keep track of the global needs and requirements concerning cyber security.

Optimal compliance

We also do our part when it comes to cyber security standards. ABB is an active member and driver of industry initiatives, including active involvement in ISA, IEEE and IEC. Our involvement also allows the security councils to ensure that ABB products and systems are compliant with, and support industry standards and regulations related to cyber security. We are constantly developing and improving products compliant with the latest cyber security standards.

System 800xA has been designed with cyber security in mind and provides state-of-the-art functionality. This allows you to easily address NERC CIP requirements and maintain compliance according to these standards and beyond.
All control systems are exposed to threats
System 800xA has the right protection mechanisms in place
Cyber security is embedded in System 800xA

Cyber security is embedded in all phases of ABB’s system life cycle (product, project, and plant life cycle), and is an integral part of System 800xA. This means that cyber security is addressed at each stage of our system life cycle, from design and development to maintenance. Threat modelling and security design reviews, security training of software developers, and in-house and external security testing are examples of actions ABB is taking to ensure reliable and secure solutions. System deliveries follow our strict guidelines on handling cyber security.

Security for System 800xA adheres to the SD lifecycle, and is an integral part of System 800xA. Cyber security is embedded in all phases of ABB’s system life cycle, from design and development to maintenance. Threat modelling and security design reviews, security training of software developers, and in-house and external security testing are examples of actions ABB is taking to ensure reliable and secure solutions. System deliveries follow our strict guidelines on handling cyber security.

Secure by Default

The goal in this phase is to create default product installations and configurations that are more resistant to attack, by reducing the attack surface (the number of points a hacker can attempt to exploit).

To accomplish this goal, software must be installed in its most secure configuration and must stay that way until the customer takes informed steps to loosen it.

When using the system installer, 800xA is installed in a predefined way, which makes the process easy and reliable, ensuring that settings are done in a consistent and repeatable way. Functions and features that are not needed are disabled or not installed, and Windows Firewall is automatically configured.

System 800xA gives control engineers a unique opportunity to manage access for each user. Access can be granted based on parameters such as who and where the user is, what the user wants to do, and on which aspect object.

Secure by Deployment

The goal here is to ensure that the products can be installed, configured, operated, and maintained in a secure way.

User documentation describes how to install and operate System 800xA at the highest level of security. Documentation includes recommendations on how to build secure system architecture using security zones and defense in depth. Security compliance project checklists make sure that all important steps are taken during project execution to ensure a secure deployment.

An overview of the security features embedded in System 800xA:

- Detailed system monitoring and diagnostics.
- Network protection with IPSec.
- Host firewalls for servers and workstations.
- Network loop protection in servers and workstations.
- Robustness tested products.
- Detailed role-based access control.
- Fast operator log over.
- HWI-based access control for safety systems.
- Data integrity with protected archives for historical data.
- Backup and restore for disaster recovery.

An overview of additional security features:

- Digital signature
  Makes it possible to digitally sign aspects to ensure that data is kept unchanged after approval.
- Advanced access control
  Reauthentication and double reauthentication for secure Interaction and inactivity logout.

Peace of mind tends to come when you have less to worry about. And that is a fact when you operate System 800xA. It is reassuring to know you have done all you can to protect your company’s know-how, ideas and operations.

ABB recommends that a virus scanner is used on all System 800xA servers and workplaces.

Overview of optional security features through our partners:

- Malware protection: AntiVirus
  McAfee VirusScan® Enterprise and Symantec Endpoint Protection have been tested and qualified for optimal performance with System 800xA’s operation and performance.

- Security event monitoring
  Situation awareness is required to maintain a high security level of a control system. 800xA offers centralized security event monitoring using Industrial Defender Monitor.

- Configuration compliance management
  ABB’s operation and performance.

- Audit trail
  Logging of all user-initiated actions in a system, like operator interactions, configuration changes and download to controllers, batch recipe editing and execution, start/stop of servers etc.
- 800xA for Industrial Defender
  800xA security events are sent to Industrial Defender Monitor for further security analysis.
- Application whitelisting by Cryptzone
  Provides advanced threat protection with whitelists of allowed software to execute on workplaces and servers.

800xA for Industrial Defender

800xA security events are sent to Industrial Defender Monitor for further security analysis.

Overview of optional security features through our partners:

- Malware protection: AntiVirus
  McAfee VirusScan® Enterprise and Symantec Endpoint Protection have been tested and qualified for optimal performance with System 800xA’s operation and performance.

- Security event monitoring
  Situation awareness is required to maintain a high security level of a control system. 800xA offers centralized security event monitoring using Industrial Defender Monitor.

- Configuration compliance management
  ABB’s operation and performance.

- Audit trail
  Logging of all user-initiated actions in a system, like operator interactions, configuration changes and download to controllers, batch recipe editing and execution, start/stop of servers etc.
- 800xA for Industrial Defender
  800xA security events are sent to Industrial Defender Monitor for further security analysis.
- Application whitelisting by Cryptzone
  Provides advanced threat protection with whitelists of allowed software to execute on workplaces and servers.

Overview of optional security features through our partners:

- Malware protection: AntiVirus
  McAfee VirusScan® Enterprise and Symantec Endpoint Protection have been tested and qualified for optimal performance with System 800xA’s operation and performance.

- Security event monitoring
  Situation awareness is required to maintain a high security level of a control system. 800xA offers centralized security event monitoring using Industrial Defender Monitor.

- Configuration compliance management
  ABB’s operation and performance.

- Audit trail
  Logging of all user-initiated actions in a system, like operator interactions, configuration changes and download to controllers, batch recipe editing and execution, start/stop of servers etc.
- 800xA for Industrial Defender
  800xA security events are sent to Industrial Defender Monitor for further security analysis.
- Application whitelisting by Cryptzone
  Provides advanced threat protection with whitelists of allowed software to execute on workplaces and servers.

Overview of optional security features through our partners:

- Malware protection: AntiVirus
  McAfee VirusScan® Enterprise and Symantec Endpoint Protection have been tested and qualified for optimal performance with System 800xA’s operation and performance.

- Security event monitoring
  Situation awareness is required to maintain a high security level of a control system. 800xA offers centralized security event monitoring using Industrial Defender Monitor.
Security monitoring, management and application whitelisting for 800xA systems

To help users achieve a proactive cyber security strategy for their 800xA-based systems, ABB has partnered with Industrial Defender to provide Automation Systems Manager (ASM), a centralised platform for security, compliance, and change management activities across control system operations. The integration and validation of Industrial Defender as part of System 800xA combines industry-leading technologies that enable users to better monitor and manage their critical control system operations.

In cooperation with Cryptzone, ABB has integrated the application whitelisting solution 800xA whitelisting SE46. This solution ensures that only trusted software is allowed to run on mission-critical machines and computer workstations.

Industrial Defender Automation Systems Manager includes software and hardware that automatically collects information from 800xA servers, workstations and network devices. It works by collecting system events, configuration, software, patches, and user information from nodes. This information is forwarded so it can be automatically processed and leveraged across various operational activities related to security, compliance, and change management.

Monitor
- Centralized monitoring of security events from 800xA servers, workstations, switches, routers, firewalls and RTUs.
- Correlation, prioritization and notification of security and performance events based on customer preference and policy.

Manage
- Change management for all system devices through the use of baseline exception reporting.
- Automated reporting of deviations with industry standards, internal policies, configuration settings, software patch levels and more.

Application whitelisting
- Designed to prevent the execution of unauthorised and malicious programs.
- Application whitelists are created in SE46 Studio and deployed on whitelisting agents on servers and workstations. Only software allowed by whitelists can execute on the servers and workstations.

If the worst happens, nothing is lost

System 800xA is on top of the game when it comes to disaster recovery. Numerous features assist in the recovery of a system failure. Total and selective backup and restores are possible through the system administration features. System nodes can be easily replaced by deploying all original software and configuration data in the new replacement node. Third-party software such as Industrial Defender’s monitor solution stores security logs that enable forensic analysis of what actually happened.

Systems are always up to date
Automation Sentinel is ABB’s subscription based control system lifecycle support program that allows systems owners to actively monitor their control system versions and software lifecycle costs.

For Automation Sentinel subscribers it is easy to keep systems up to date with the latest security updates and virus signature files.

ABB evaluates all third party software security updates for System 800xA, and tests all relevant updates for compatibility. The “ABB System 800xA Qualified Security Updates”, are available for download from ABB for Automation Sentinel subscribers.

Also updates for supported virus scanners, including virus definition files, are tested for compatibility with System 800xA to ensure that legitimate code is not wrongly classified as malware. ABB tests virus definition files for both McAfee VirusScan® Enterprise and Symantec Endpoint Protection each weekday.

Service that maximizes security
ABB has developed non-invasive tools to diagnose potential cyber security issues, offer solutions to maximize security, and provide support for the future.

Cyber Security Fingerprint services; diagnoses and offers solutions for potential security risks. It includes detailed recommendations to reduce vulnerability, and helps to develop a sustainable security strategy for control systems. This service is delivered by an ABB engineer at site.

Invest in cyber security now

Investing in cyber security is one of the best ways to invest in your company’s future. And it should never be an issue of waiting to see if something will happen. Who can afford that kind of chance taking?

Finally, and maybe most importantly, cyber security is not a one-time event, it is an ongoing process. At ABB, we are happy to help you with that process all the way.