# System 800xA Cyber Security

Maximizing cyber security in process automation

# If it is valuable to you, it is probably valuable to someone else

In critical infrastructure the protection goes beyond intellectual property and covers the availability of the asset that could be diminished under an attack. 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 inter-operability of systems.

# 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, relying on 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.

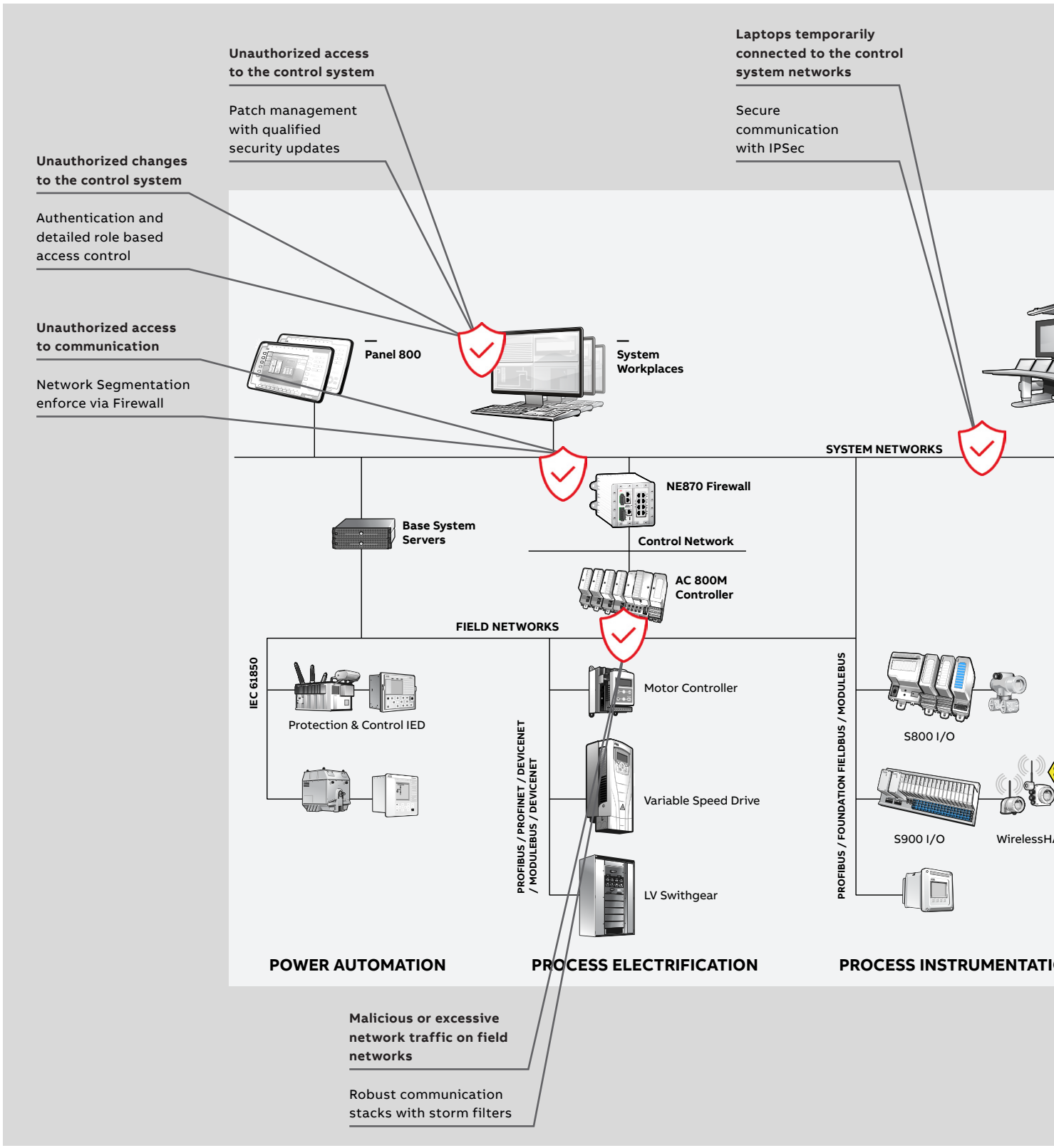
**Optimal compliance**

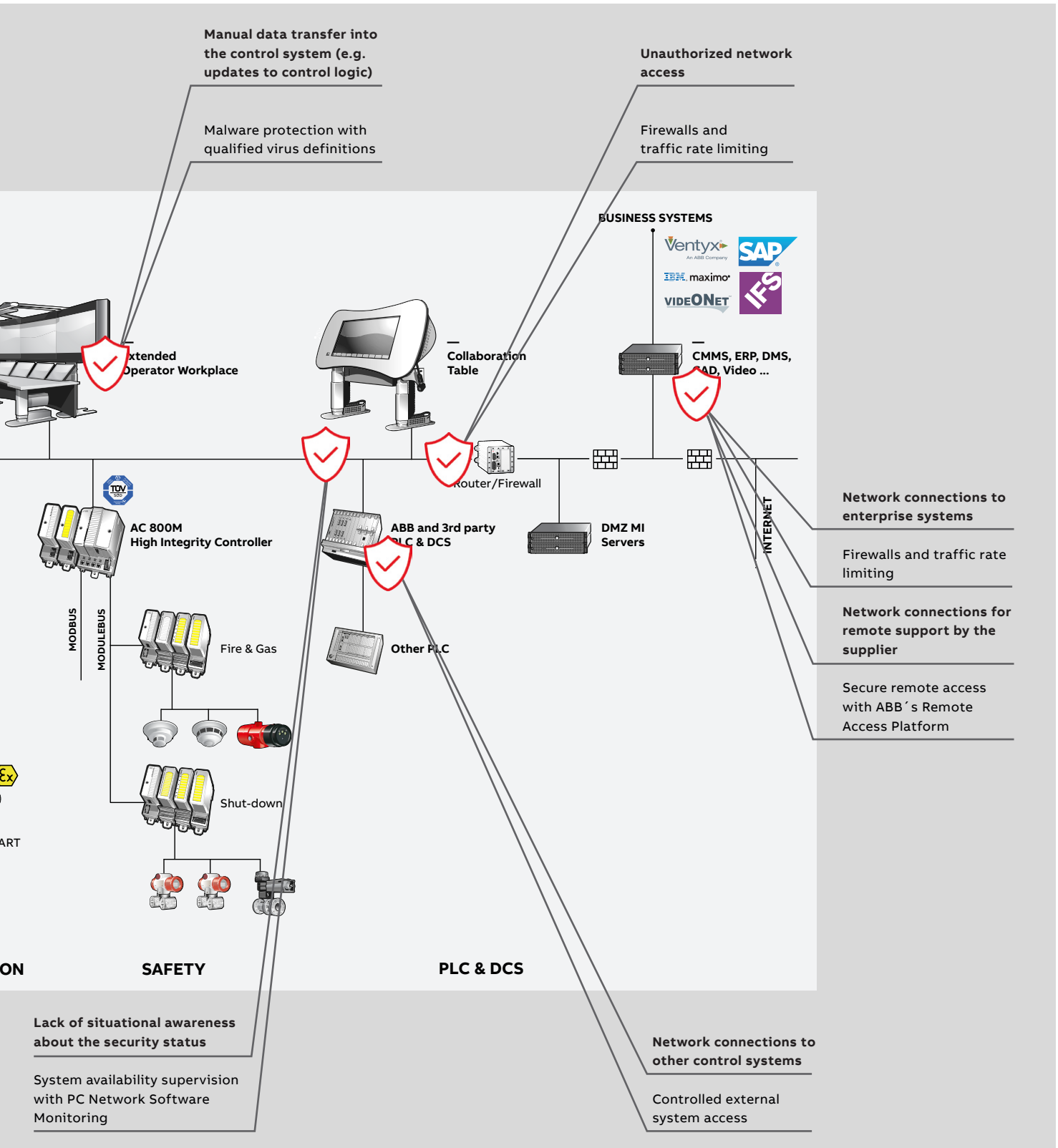
We also do our part when it comes to cyber security standards. ABB is an active member and driver of industry initiatives, including active involvement in ISA, IEEE, Cyber Security Standard Committees and IEC. Our involvement also allows the security councils to ensure that ABB products and systems are 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




Manual data transfer into the control system (e.g. updates to control logic)
Malware protection with qualified virus definitions
Unauthorized network access
Firewalls and traffic rate limiting
BUSINESS SYSTEMS
Ventyx
SAP
IBM maximo
VIDEONET
IFS
xtended Operator Workplace
Collaboration Table
CMMS, ERP, DMS, CAD, Video ...
Router/Firewall
AC 800M High Integrity Controller
ABB and 3rd party PLC & DCS
DMZ MI Servers
INTERNET
MODBUS
MODULEBUS
Fire & Gas
Other PLC
Shut-down
Network connections to enterprise systems
Firewalls and traffic rate limiting
Network connections for remote support by the supplier
Secure remote access with ABB´s Remote Access Platform
ON
SAFETY
PLC & DCS
Lack of situational awareness about the security status
System availability supervision with PC Network Software Monitoring
Network connections to other control systems
Controlled external system access

# 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 SD³+C Security Framework (created by Microsoft) to ensure and improve security in system components.

**Secure by Design**
The goal here is to make sure that security bugs or vulnerabilities are not present in new software. To accomplish this, cyber security must be a factor from the very start of product design. And through all phases, from creating the specification, through writing the code, and testing the product.

A secure-by-design philosophy manifests itself as security training, code reviews and walkthroughs, threat analysis, and robustness testing of products. Security is integrated in ABB's quality management system. Formal threat analysis and threat modelling provide the basis for security requirements and design principles for the system. Security checkpoints at project gates ensure that security objectives are met.

One key element of this process is our independent robustness test lab, the ABB Device Security Assurance Center, where our products are tested. This laboratory is run by dedicated personnel who are not part of any product development team. They use several specialized security testing tools, for example Wurldtech's Achilles Satellite Unit and Mu Dynamics Mu8000. In addition to our adoption of SD³+C Security Framework and extensive internal testing performed by ABB's Device Security Assurance Center (DSAC), ABB has embraced third party security certification to IEC62443 standard by ISA Secure Certification Institute (ISCI) for selected models of the AC 800M controller family.

System 800xA security features are designed to meet regulatory requirements, such as by FDA. User account management and authentication is based on Windows Active Directory, or Windows Workgroups for small systems.

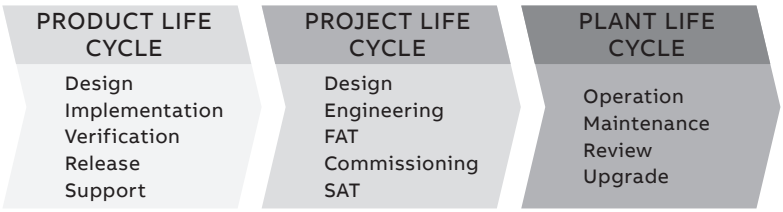
**Secure by Default**
The goal in this phase is to create default product installations and configurations that are more resistant to attack, by reducing the attack surface (the number of points a hacker can attempt to exploit).

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.




— Cyber security is an important factor in all phases of the system life cycle

## System 800xA gives you peace of mind

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.

**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.
  (AC 800M has earned Achilles Communication Certification.)
- Network protection filters and storm protection for controllers and communication modules.
- Detailed role-based access control.
- Fast operator log over.
- HW-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.
- **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.

**Overview of optional security features through our partners:**

- **Malware protection: AntiVirus**
  ABB recommends that a virus scanner is used on all System 800xA servers and workplaces.
  - McAfee VirusScan® Enterprise and McAfee Endpoint Security have been tested and qualified for optimal performance with System 800xA's operation and performance.

- **Malware protection: Whitelisting**
  - McAfee Application Control is also the preferred/validated whitelising solution for 800xA.

- Application whitelisting
  - Designed to prevent the execution of unauthorized and malicious programs.

# Cyber Security service offerings for System 800xA

## ABB service offerings:

### Foundation

- **Assessements**, gain an understanding of the cyber security posture of your system
- **Security Controls**, defend against fundamental threats by implementing cyber security controls
- **Training**, reduce incidents by equipping your team with cyber security insight

### Services

- **Maintenance**, ensure continuous protection of your automation systems using our skilled industrial cyber security engineers
- **Consulting**, perform system hardening or implement your cyber security projects using our global network of industrial cyber security experts.

### Operations

- **Collaborative Operations**, leverage our global network of experts trough ABB Collaborative Operations Centers for 24/7 continuous monitoring and support

For more information please visit our **ABB Ability Cyber Security Services web**

## If the worst happens, nothing is lost

**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, McAfee Endpoint Security 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.

**solutions.abb/800xA**
**abb.com/controlsystems**



3BSE074956 en F