If its valuable to you, it is a target 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 – but also 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, ransomware 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 confident knowing that we are protecting you with best-in-class security solutions.

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.
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 utilize open standards, such as OPC, IEC 61850, IEC 60870-5-104, DNP 3.0, 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’s systematic approach ensures cyber security

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. On a global level, ABB takes a systematic approach to cyber security throughout design, development and delivery of its automation products. 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 adapting to the latest threats and testing with best-in-class tools to ensure products can meet today’s cyber security requirements.

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

Cyber security is embedded in all phases of ABB’s system life cycle. Security for Symphony Plus adheres to the SD3+C Security Framework (created by Microsoft) to ensure and improve security in system components. This means that cyber security is addressed at each stage of our system life cycle, from design and development to maintenance.

- **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.

- **Secure by Default**
  - Symphony Plus 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 configured to only enable necessary communication ports. Symphony Plus 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 Symphony Plus 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. Systems in operation are kept secure with monthly security patch updates and daily anti-virus updates.

Symphony Plus security features are designed to meet regulatory requirements and includes features to help enable compliance such as user account management, role-based access control, user authentication, audit trail, etc.

- **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.

Symphony Plus 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 Symphony Plus. It is reassuring to know you have done all you can to protect your company’s know-how, ideas and operations.

ABB is engaged with the wider ICS-Cybersecurity community which includes security researchers and analysts. There is an open channel of communication with the community and customer base regarding cyber security issues. This may entail working with third parties specialized in security assessment and penetration testing of ICS technologies. When a potential vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. The goal is to provide customers with advice for workaround or mitigation strategies that minimize the potential risk of a vulnerability as much as possible. These findings are then addressed by product development and made available to improve overall product cyber security.

Occasionally these activities result in the need to publish an external Cybersecurity Advisory which demonstrates part of ABB’s commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed. Cybersecurity Advisories which are released can be found on our public facing websites.

An overview of the security features provided with Symphony Plus:
- 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
- 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
- Digital signature to ensure data is kept unchanged after approval
- Advanced access control for secure interaction and inactivity log-out
- Audit trail for logging of all user-initiated actions in a system

Overview of optional security features through our partners:
- Malware protection: Antivirus accomplished with McAfee Endpoint Security on all Symphony Plus servers and workstations
- Malware protection: Allowlisting accomplished with McAfee Application Control
- Backup and restore for disaster recovery

A secure-by-default 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 Achilles Test Platform and Nessus scanners.

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), see www.iaisecure.org.

Backup and restore for disaster recovery

Malware protection: Allowlisting accomplished with McAfee Application Control

Peace of mind tends to come when you have less to worry about. And that is a fact when you operate Symphony Plus. It is reassuring to know you have done all you can to protect your company’s know-how, ideas and operations.
Strengthen your resilience with a complete portfolio of cyber security services

ABB provides a range of cyber security services to support you on your cyber security journey. Uniquely developed for industrial systems like yours, ABB Cyber Security Services mitigate cyber risks by identifying potential threats, automating compliance efforts and defending against cyber-attacks.

**Do something rather than nothing.**
Investing in cyber security is necessary to protect your company’s future. Companies that fail to address known risks are viewed poorly when cyber attacks expose lack of proper management.

Cyber security is not a one-time event, but an ongoing process. To guide you on this journey, we offer a stepwise and practical service approach that lowers cyber risk by taking the necessary steps to identify what must addressed, actively protect automation assets, detect security breaches, respond to cyber-attacks and establish backup and recovery plans.

ABB’s cyber security portfolio includes services and solutions to match your requirements. These include:

- **Assess**: A strong cyber security posture is important to defend against cyber-attacks. ABB Cyber Security Assessment services help you understand the strengths, weaknesses, gaps and risks in your cyber security posture so that you can determine the right strategy for your business.

- **Plan**: Whether you need help implementing a cyber security control, making changes to your architecture, or writing a security policy, leverage ABB’s experience with industrial cyber security and process to design your cyber security plan.

- **Implement**: In addition to basic controls, such as system hardening, applying security updates, applying antivirus software and ensuring backup, a comprehensive asset inventory is critical to manage your cyber security controls. ABB’s Asset Inventory helps you detect unauthorized changes to your cyber security policy and computer settings so that you can take action to strengthen your systems.

- **Maintain**: The implemented cyber security controls must be maintained to continue to be effective. Depending on what your maintenance needs are, the ABB team can work remotely or on-site. By delivering some services remotely, we can reduce costs and increase efficiency without affecting production.

- **Detect and respond**: Once you’ve implemented your cyber security foundation, depending on risk factors and regulations, you may need to strengthen your cyber defenses with ABB advanced cyber security services such as network and event monitoring.

ABB can help monitor your defenses on a 24x7 model to quickly alert you of any threat to your production. When an abnormal event or malicious behavior is detected and alerted, ABB experts analyze the event and respond as needed.

In the event of a cyber security breach, ABB’s experts spring into action and restore your production as quickly as possible. Afterwards, ABB provides an after-action report and consults with strategy to prevent future incidents.

For more information, please visit our ABB Ability™ Cyber Security Services web.
We reserve the right to make technical changes to the products or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not assume any responsibility for any errors or incomplete information in this document.

We reserve all rights to this document and the items and images it contains. The reproduction, disclosure to third parties or the use of the content of this document – including parts thereof – are prohibited without ABB’s prior written permission.

Copyright © 2021 ABB. All rights reserved. ABB Ability is a trademark of ABB. Symphony and Symphony Plus are registered or pending trademarks of ABB. SIMPLE, SCALABLE, SEAMLESS, SECURE is a registered or pending trademark of ABB. All rights to other trademarks reside with their respective owners.