Symphony Plus
Cyber security for the power and water industries
Symphony Plus
Cyber security for the power and water industries
ABB addresses cyber security in every respect

Industrial automation and control systems have evolved significantly over the past decade thanks to many technological advancements and breakthroughs. 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, IEC 60870-5-104, DNP 3.0, 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 security risks were inherited by adopting open IT standards, but fortunately so were the cyber security mechanisms that were developed in a large number of enterprise environments to address those risks. These mechanisms enable the design and development of cyber security solutions that are specifically for industrial automation and control systems, and which utilize proven technology.

ABB fully understands the importance of cyber security, and its responsibility to advance the security of control systems used by the power and water industries. ABB customers can rely on system solutions where reliability and security have the highest priority.

Systematic approach to ensure cyber security

Over the past few years, the global power and water 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.

ABB has identified cyber security as a key requirement and is committed to providing customers with products, systems and services that clearly address this issue. ABB takes a systematic approach to cyber security through its operations on a global level. For instance, ABB has established the Power Systems Security Council to keep track of the global needs and requirements of cyber security. The mandate of the council is to ensure that products and solutions used in power systems meet the expectations of customers. Besides continuously adapting security requirements to keep up with changing demands, the security council drives proactive R&D efforts to support future trends, and ensures fast and efficient security improvements.

ABB also recognizes the importance of cyber security standards, and is an active member and driver of various industry initiatives, including active involvement in ISA, IEEE and IEC.
Cyber security is embedded in ABB products
Cyber security is embedded in ABB’s product life cycle, and is an integral part of our industrial automation and control solutions. This means that cyber security is addressed at each stage of our product portfolio life cycle, from design and development to maintenance. Threat modeling and security design reviews, security training of software developers, and in-house and external security testing are examples of the numerous actions ABB is taking to ensure reliable and secure solutions for its customers. Individual user accounts and detailed security event logs are just two instances of built-in security features available in our products. ABB’s industrial automation and control systems are available with firewalls, hardening and pre-defined antivirus software. System deliveries follow our strict guidelines on the handling of cyber security.

Cyber security without compromise
Evolving technologies like Ethernet and industry-specific standards such as OPC, PROFINET and IEC 61850 are enablers for information exchange that support higher system reliability. Additionally, it is important to safeguard interoperability, which allows information exchange between different vendors’ compliant products and systems. Ensuring reliability and interoperability are two of the main goals when designing and engineering industrial automation and control systems. Supporting availability, reliability and interoperability, while at the same time addressing cyber security, is a challenging task. ABB is committed to providing its customers with solutions that address all these aspects without compromise.

Cyber security addressed throughout the system life cycle
ABB provides products and solutions that enable end users to fulfill the requirements of cyber security standards such as NERC CIP. We view cyber security not only as a single, one-time activity, but as an integrated part of different phases of the product and system life cycle, as well as of the processes that support the products and systems in operation both now and in the future. Among the key elements of these processes are our security patch test center and our independent robustness test center, where all our products are tested using current state-of-the-art security testing tools.
A centralized security testing process applying up-to-date and rigorous test procedures guarantees a common and best practice approach. The test centers conduct regular regression tests on ABB products and systems to ensure a high level of robustness against cyber security attacks.

ABB is also constantly extending and improving security-related organizational processes such as those handling vulnerability. The proper and timely handling of software vulnerability is an important factor in helping our customers to minimize their risk exposure to cyber security threats.

**Cyber security on the client/server level**
Interactions between industrial automation and control systems, corporate networks and the outside world are usually handled on the client/server level, which means that ensuring a high level of security on this level is vital. ABB therefore uses best-in-class firewalls, intrusion detection or prevention systems, or virtual private network (VPN) technology. Additionally, ABB has built security mechanisms such as advanced account management and detailed security audit trails into its products. Systems can be divided into multiple security zones to further improve security. ABB’s system security approach is completed by robust control and field level devices supporting many security features.

The key requirements that need to be covered by a secure industrial automation and control system are:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td>Avoid denial of service</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Avoid unauthorized modification</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Avoid disclosure</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Avoid spoofing/forgery</td>
</tr>
<tr>
<td><strong>Authorization</strong></td>
<td>Avoid unauthorized usage</td>
</tr>
<tr>
<td><strong>Auditability</strong></td>
<td>Avoid hiding of attacks</td>
</tr>
</tbody>
</table>

**Cyber security features in Symphony™ Plus**
ABB is addressing all of these requirements, both on a system and on a product level. All communication from the outside world to an industrial automation and control system can, for instance, be protected by using a firewall and/or VPN-enabled communication. Verified antivirus software is supported to protect the system’s computers from attacks and viruses. Additionally, the system architecture can be designed using different security zones. Cyber security can be further improved by limiting the use of removable media in the system’s computers.
ABB’s Symphony Plus has been designed with cyber security in mind and to provide state-of-the-art functionality in this respect. This allows our customers to easily address NERC CIP requirements and maintain compliance according to these standards and beyond. All this can be done in an easy way using the security administration function in Symphony Plus Engineering Workbench.

Overview of security features:
- User authentication
- Role-based access control
- Event logging/Audit trails
- Backup/Restore
- Hardened hosts
- Host firewall configuration
- Antivirus
- Network zones
- Security patch validation

Optionally:
- Patch management
- Virus pattern management
- Host intrusion detection
- Host intrusion prevention
- Network intrusion detection
- Compliance management

Users and user roles
The Symphony Plus security model is based on IEC 62351-8. This allows for smooth integration with electrical systems and the smart grid. It supports the definition of rights and the roles for a user or user groups in the Symphony Plus system with definable granularity.

Authorization
Security controls a user’s authority to perform different operations on TAGs in accordance with several parameters:
- The user’s credentials, as provided by the lightweight directory access protocol (LDAP) server
- The node where the user is logged in. This makes it possible to give a user a different authority according to location, eg, close to the process equipment or in a control room
- The operation the user wants to perform

Access control
Basic access to the system is controlled by the user’s credentials entered during logon or log-over. Restrictions may be placed on factors such as password length, complexity, age and reuse.

Log-over
The log-over function enables a fast and temporary switch between users in a running workplace. For example, if an operation requires a right not held by an operator, another user (such as a supervisor) who holds the required right can log-over to perform that operation. The log-over changes the rights and user roles but keeps an open view on the process by retaining the workplace and its present contents, supporting automatic revert to the previous user.
Configuration change management
Symphony Plus supports configuration change management by defining each version area with three states of configuration data: design, release and running. These states can be archived and easily compared for differences. In addition, Symphony Plus maintains all used software and its versions for easy update management and comparison.

Audit trail
As required by regulations, Symphony Plus maintains an audit trail of changes made to process settings as well as configuration changes. In addition, all system and security events are collected in the Symphony Plus event management system.

Archive
The archive function of information management history services supports the permanent offline storage of historical data collected in property, message and report logs, as well as the operator workplace alarm and event message buffer, including audit trail messages. The archiving mechanism copies the contents of selected logs to a designated archive media.

System monitoring and diagnostics
Symphony Plus provides comprehensive diagnostic functions for determining the health of the process and control system. System status can also be displayed in the context of topology diagrams. This includes the status of the system infrastructure eg, controllers, I/O modules, switches, routers and firewalls. All events from these devices are collected, and alarms can be generated in the event of problems.

System hardening
System hardening can be deployed centrally from the administration console. This includes OS hardening, application hardening, host firewall configuration, and antivirus. It applies to servers, workstations and supported network equipment.

Disaster recovery
Numerous features of Symphony Plus 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 replaced easily by deploying all original software and configuration data in the new replacement node. Third-party software such as Acronis can be employed to restore a server- or workstation-based failure to a state in which a software and configuration deployment can be performed. Network equipment, such as routers and switches, can be backed up and loaded from the system's administration console.

Patch and service pack management
ABB evaluates security updates from third-party software such as Microsoft, McAfee and Adobe with respect to relevance to, and compatibility with, Symphony Plus. All relevant updates are validated. The goal is to communicate the validation plan for relevant updates within 24 hours of a security update release, and to communicate validation results for updates within seven days of release.
Contact us

ABB Inc.
Power Generation
Wickliffe, Ohio, USA
Phone: +1 440 585 3087
Email: powergeneration@us.abb.com

ABB AG
Power Generation
Mannheim, Germany
Phone: +49 621 381 3000
Email: powergeneration@de.abb.com

ABB Pte. Ltd.
Power Generation
Singapore
Phone: +65 6776 5711
Email: powergeneration@sg.abb.com

www.abb.com/powergeneration

© Copyright 2012 ABB
All rights reserved. Specifications subject to change without notice. Pictures, schematics, and other graphics contained herein are published for illustration purposes only and do not represent product configurations or functionality. User documentation accompanying the product is the exclusive source for functionality descriptions. Symphony is a registered or pending trademark of ABB S.p.A.