End-to-end cyber security solutions for Grid Automation
Securing your systems and products

- Compliance to international cyber security standards
- Designed and configured according to best practices
- Large range of cyber security measures applied
Compliance to international cyber security standards

Cyber security is not a single solution for one problem, but more like an evolving battle requiring multiple approaches and solutions. ABB has developed a range of products, solutions and services to help operate and safeguard your digitalized infrastructure.

Today’s automation systems interconnect with multiple networks, systems and locations, and have increased operational efficiencies tremendously. However, this process has also introduced cyber security concerns previously known only to office or enterprise IT systems. ABB end-to-end cyber security solutions confront the risks wherever they arise, from control centers to communications networks to substation automation.

We define the digitalization and develop highly secure, trusted cyber security solutions for industrial, infrastructure and mission critical environments. ABB’s innovative product and system solutions place the highest priority on reliability and security.

Integral to the lifecycle of all ABB products, cyber security is incorporated into ABB grid automation systems, which follow industrial best practice guidelines outlined in such standards as IEC 62443, IEC 62351, NERC-CIP, IEEE 1686, as well as the BDEW white paper recommendations. Compliance with international cyber security standards is very important, and ABB is an active member in several industry initiatives relating to cyber security, including the IEEE and IEC.

This ensures the needs of ABB customers are considered as new standards are developed, and helps ABB remain abreast of new cyber security developments. This is important because the interoperability that ensures devices can communicate with each other is an essential part of ABB product design. By incorporating the latest cyber security standards into its products and systems, ABB can provide grid automation products and systems that help customers comply with all local laws and regulations.

Key cyber security initiatives driven or supported by ABB.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Main Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>NERC CIP</td>
<td>Cyber Security regulation for North American power utilities</td>
</tr>
<tr>
<td>IEC 62351*</td>
<td>Data and Communications Security</td>
</tr>
</tbody>
</table>
| IEEE 1686          | IEEE Standard for Substation Intelligent Electronic Devices (IEDs)  
|                    | Cyber Security Capabilities                    |
| IEC 62443*         | Industrial Automation and Control System Security (formerly known as ISA S99) |
| BDEW Whitepaper    | Requirements for Secure Control and Telecommunication Systems |

* Standards are still in development

Defense in depth approach

Cyber security measures help to monitor, manage and protect systems and products, ensuring they comply with industrial standards and follow the defense in depth approach. All grid automation systems from ABB are designed and configured according to best practices and provide a broad range of cyber security measures, which are grouped into three main categories:

1. **Monitor**  
   Monitoring features provide real-time security and monitor the health and activity of assets across grid automation systems, including networks and applications.

2. **Manage**  
   Managing features help users monitor and manage critical activity, including configurations, changes and patches across grid automation systems.

3. **Protect**  
   Protecting features defend grid automation systems against unauthorized access, attacks, exploits and malware that compromise system availability, performance, security and compliance.
ABB's Grid Automation end-to-end cyber security solutions

Security levels according to IEC 62443

From substation automation to the control center, ABB Grid Automation solution secures your system and products all the way from process level over the communication level to the network level.
ABB’s Grid Automation
cyber security offering

By adding multiple layers of security controls throughout your system you can build your defense in depth. Our cyber security feature groups will help you to ensure your system security.

**Secure communications**
Our solutions use the latest encryption technology according to the IEC 62351 Industry standard. Examples are https, VPN tunneling for remote access, secure IEC 60870-5-104, and secure DNP 3.0 communication according to IEC 62351. In addition, ABB utilizes Quantum-safe solutions for highly secure end-to-end encryption and long-term protection in business-critical communication networks.

**Zoning & perimeter protection**
Stateful firewalls protect the network perimeter, separating it into security (demilitarized) zones that ensure an infected system does not compromise the entire network. For deeper inspection, next generation firewalls (NGFW) including an intrusion detection system (IDS) can be included to improve the monitoring and protection capacity of an industrial control system.

**Backup & recovery**
Complete system backups enable quick recovery and restoration of an entire system. ABB offers backup solutions to address data loss, hardware and software failures, and security attacks that enable users to always be prepared for the worst.

**Malware protection**
Malware and intrusion protection solutions protect grid automation systems from viruses, Trojans and other types of malware. In addition, an application whitelisting solution can be added to prevent potentially harmful unauthorized applications from running.

**Zoning & perimeter protection**
Stateful firewalls protect the network perimeter, separating it into security (demilitarized) zones that ensure an infected system does not compromise the entire network. For deeper inspection, next generation firewalls (NGFW) including an intrusion detection system (IDS) can be included to improve the monitoring and protection capacity of an industrial control system.

**Account management**
Our systems provide extensive user account management capabilities based on Role Based Access Control (RBAC). To manage large numbers of devices, we offer a central user account management solution based on IEC 62351-8, in which the user defines password complexity. In addition, two-factor authentication can be included for remote access.

**Patch management**
Patch management is an essential step towards securing a system and protecting a business, and one of the most important layers of cyber security protection in modern digital systems. To ensure strong security throughout a system lifecycle, ABB delivers comprehensive patch management solutions.

**Security logging & monitoring**
Detailed audit trails (log files) of all security-relevant user activities are created. These security events can be sent to a central security manager for further analysis, which enables customers to monitor and respond to security events in real time.

**Product & system hardening**
All ABB products are successfully verified at our Independent Device Security Assurance Center (DSAC). During engineering and testing the delivered system will be hardened according to well-known best-practice guides.
Cyber security protection over system life cycles

We address cyber security at all stages of the system life cycle. Cyber security is considered from design and development to operations and maintenance.

Cyber security is an integral part of product life cycles at ABB, and has been carefully incorporated into the products and systems for grid automation customers. The ABB Security Development Lifecycle (SDL) program addresses cyber security needs at all phases of the development process.

Threat modelling and security design reviews, security training for software developers, and in-house and external security testing are some of the multiple actions ABB takes to deliver reliable, secure customer solutions. Individual user accounts and detailed security event logs are just two examples of built-in security features available in our products.

A key feature of ABB’s offering is the Independent Device Security Assurance Center (DSAC), where all ABB products undergo state-of-the-art security testing before they are released to the market. This process measures robustness and security integrity, and includes port scanning, network flooding, vulnerability scanning and protocol fuzzing. Centralized security testing ensures a common, best-practice approach and a robust defense against cyber security attacks.

Quantum-Safe Cyber Security Solutions for Mission Critical Communication

The rising threat of cyber-attacks to mission critical infrastructures – such as electricity and powers grids and new threat vectors, like a quantum computer, means that these networks urgently need improved protection.

This is leading to a re-thinking of security. ABB offers the industry’s first Quantum-Safe solution for highly secure MPLS-TP end-to-end encryption and taking into account the specific needs of mission critical applications in terms of communication performance (e.g. jitter, wander, latency), but also considering the availability and long-time protection of the communication infrastructure. Quantum technologies improve the overall safety of critical infrastructure by improving cryptographic key generation with Quantum Random Number Generators (QRNG).
ABB is continually expanding and improving security-related processes to ensure new vulnerabilities are handled quickly and correctly. A timely response is essential to help customers minimize exposure to cyber security threats. All findings can be reported informally via email.

ABB is focused on maintaining and increasing cyber security in the installed base of ABB grid automation systems. In addition to technical solutions, ABB can provide training, consulting and cyber security risk assessment solutions for an installation. The assessment provides technical as well as organizational analysis, and proposes optimized measures to reduce cyber security risks at the installation.
Contact your local service and sales support team to discuss your requirements further.

To report security findings send an email to: cybersecurity@ch.abb.com

For further information visit: abb.com/cybersecurity