Cyber Security

ABB takes cyber security extremely seriously – for the security of our products, systems, services, as well as our customer’s and ABB’s data.

With the early days of cloud enablement behind us, it’s clear that “security” means much more than protection against cybercrime: some connections need to be safe, but the value of that data should also be protected. Customers should not be required to forfeit safety, value, or control to realize the benefits of digitization, and ABB Ability closes the loop between these needs with an innovative, multi-layered approach to security:

Connectivity
The majority of the 70 million ABB connected devices working for customers around the world require built-in safety standards that, by definition, must also be secure. Everything from controller hardware to software is designed to ensure optimized, uninterrupted operation.
**Data**
Naveo®Pro Smart Monitoring System uses Google Cloud to give customers access to an enterprise-grade cloud infrastructure platform to securely store their data. ABB has adopted global data protection standards to ensure a standardised and high level of protection of Personal Data which is processed by ABB Group Companies worldwide.

**Standards**
ABB innovates digital security via its Group Cyber Security Council and participates in standardization efforts such as Platform Industrie 4.0 and Industrial Internet Consortium. It also works with dozens of universities and brings together leading minds annually for its Global Technology Forum.

Google Cloud Platform is certified as ISO/IEC 27001 compliant.

**Multi-factor authentication (MFA)**
MFA is a multi-layered security system that verifies the identity of our users applying additional security measures.

**Product Cybersecurity Tests carried out by our Device Security Assurance Center (DSAC)**
A dedicated, independent security test center has been established where ABB products are subject to security and robustness tests. A detailed test report and analysis is shared with the development teams to help them rectify detected vulnerabilities, if any.

The objective of the Device Security Assurance Center is to provide continuous protocol-stack robustness and vulnerability assessments of embedded devices, enabling:

- ABB to supply customers with products that meet the highest robustness standards
- ABB products and devices to comply with existing and forthcoming governmental and industrial regulations
- ABB to stay ahead of technology in device security

[DSAC Whitepaper link](#)