# **ABB Ability™ solutions:**
Protecting data with unsurpassed industrial-strength cybersecurity


—

Bart de Wijs, Head of Cybersecurity, Digital ABB

**As a leader in digital technology for industries, ABB provides 360° cybersecurity data-protection capabilities. All ABB Ability™ solutions are designed with security and data protection top-of-mind from their inception, and deliver on that promise throughout their product lifecycle.**

# Table of contents


**04**-05 **The situation**

**06**-07 **ABB’s approach to cybersecurity**

**08** **How ABB protects against the full range of cybersecurity threats**

**09**-14 **ABB cybersecurity starts with the platform**

# The situation

The factory of the future is here now, enabled by potent arrays of digitally connected smart devices and sensors, building the Industrial Internet of Things (IIoT).

This new generation of digital Operational Technology (OT) is delivering transformational business insights that enable such business optimizations as highly flexible and customizable production lines, fully automated manufacturing processes and new business models.

The more sophisticated and interconnected these digital devices and processes become – moving data from inside factories and enterprises to the edge and then the public cloud/internet – the more crucial it is for companies and their industrial technology vendor-partners to deploy the most robust cybersecurity systems. Data is the lifeblood of companies, and the more sensitive the data, the more attractive it is to malicious actors intent on stealing or corrupting it.

—

As a leader in digital technology for industries, ABB provides 360° cybersecurity data-protection capabilities. All ABB Ability™ solutions are “secure by design” – developed and built with cyber-security and data protection top-of-mind from their inception to the end of every product’s lifecycle.

One key insight driving ABB’s IIoT cybersecurity strategy is that OT industrial companies undergoing digital transformation can leverage the hard-won, long-fought lessons of IT to leapfrog to an advanced state of IIoT security.

## Sophisticated threats countered by sophisticated ABB risk-mitigation

ABB's industrial customers live in a world of increasingly sophisticated threats, putting organizations at risk of potentially catastrophic losses to business continuity. As continuing waves of news reports attest, the number of cyberattacks harming businesses, consumers and governments has accelerated in frequency, ferocity and sophistication in recent years.

The global business value at risk from cybercrime over the next five years is US$5.2 trillion, according to Accenture's "2019 Cost of Cybercrime Study," which evaluated cybersecurity risk across 16 industries and 355 companies in 11 countries. Put another way, the amount of potential loss from cybercrime over the next five years is approximately twice the size of the entire annual economy of the United Kingdom. Manufacturers across all industries have become significant targets, while intruders have broadened their malicious behavior from corporate IT to industrial control systems in highly sensitive industrial OT.

Each extension of connectivity within OT environments and between OT and IT systems and the cloud opens new attack vectors for cyber-intruders bent on espionage, sabotage or the theft of company and customer data.

A prime element of ABB's relationship with its industrial customers is trust, which includes developing and providing comprehensive cybersecurity solutions.

ABB is passionately committed to its customers' cybersecurity and data protection.

—

ABB Ability™'s range of cybersecurity and data protection solutions empower customers to monitor and defend equipment and processes, anticipate and identify risks, detect vulnerabilities, protect company and customer data and respond quickly to enable rapid recovery and a return to profitable business operations.

# ABB's approach to cybersecurity

The balance of this paper will detail the elements of ABB's cybersecurity strategy, including:

- The role and significance of ABB Ability™ solutions
- Cybersecurity standards every ABB Ability™ solution must meet before release to customers
- How ABB protects against security threats to business, customer and personal data and business operations
- Edge communications and data protection
- Details of ABB's support for stringent global data privacy and protection standards
- How ABB provides cyber-protection throughout the product lifecycle
- Data-protection best practices

## ABB Ability™

ABB Ability™ is our unified, cross-industry digital offering — extending from device to edge to cloud — that connects ABB customers to the power of the Industrial Internet of Things (IIoT) with devices, systems, solutions, services and an open, flexible platform that enables our customers to know more, do more and do better, together. Drawing on ABB's deep domain expertise, ABB Ability™'s digital capabilities turn data insights into direct action that "closes the loop" and generates customer value in the physical world.

The ABB Ability™ **platform** is a set of common software technologies and services for the device, edge and cloud. It enables the rapid creation, extension, deployment and operation of secure industrial, cloud-based applications. The ABB Ability™ **Cloud**, a key component of the platform, utilizes Microsoft Azure to support connectivity and delivery of web services.

## Cybersecurity is a continuous process that's never complete

Cybersecurity is not one product or one technology that can be installed, switched on and forgotten. It's a commitment to a continuous process of improvement throughout products' entire lifecycles.

This principle is tightly integrated into ABB's global research & development organization and its product development teams. No ABB Ability™ solution is approved until it has passed rigorous testing to ensure compliance with a comprehensive and continually updated set of cybersecurity requirements.

Three of the key principles ABB applies to ensure secure protection of customer data – in a cloud or in transit between a cloud environment and customer sites:

- **Standards:** We adhere to relevant country and cybersecurity best practices and standards for data protection, such as ISO 27018. We pay close attention to evolving data ownership and stewardship standards, adhering to the regulatory framework pioneered by the European Union's General Data Protection Regulations (GDPR) and subsequently matched by jurisdictions including Japan, California and Canada.

- **Partners:** ABB has chosen Microsoft Azure as its cloud provider, as well as partnering with such innovative companies as Hewlett-Packard Enterprise (HPE), (edge), Dassault Systemes (Digital Twin), Ericsson (5G) and other trusted, best-in-class companies. One criterion for partnership: each partner organization must be as dedicated to the protection and security of their customers' intellectual property and data privacy as ABB.

- **IIoT Bill of Rights:** ABB supports Chief Digital Officer Guido Jouret's "Data Bill of Rights Manifesto," which calls on the IIoT industry – ABB, its partners, vendors and competitors – to clearly lay out what customer data is collected, why it is needed and used, how it is secured, how customers benefit from its use, and what IIoT providers will do with their data should they stop being customers.

# How ABB protects against the full range of cybersecurity threats

ABB's tactical approaches to cybersecurity risk-mitigation evolve in response to the "STRIDE" threat environment, pictured here. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS) attacks and Escalation of Privileges. Here are the threats, and how ABB/ABB Ability™ defends against them:

**TABLE A: Cybersecurity threats and ABB best-practice defenses**

| Threat | What it is | ABB defenses employed |
|---|---|---|
| **Spoofing** | The act of falsely disguising a communication from an unknown source as being from a known, trusted source to insert malicious data into an digital system, hijack a shared access signature (SAS) token or fake a user's identity to steal data from a solution. Spoofing can compromise emails, phone calls, websites, IP addresses, Address Resolution Protocols (ARP) or Domain Name System (DNS) servers. | • Enforcing strong authentication via X.509 public key certificates<br>• Preventing unauthorized copying of an SAS token by passing the token securely and assigning an expiration time<br>• Enforcing strong authentication requirements for all users of an ABB Ability™ solution |
| **Tampering** | Modifying or destroying data so the attacker can, among other things, add or remove some functional elements or change the purpose or operation of a solution or system. | • Ensuring the network transferring data uses a mutually authenticated Transport Layer Security (TLS) tunnel with the latest and most secure ciphers.<br>• In the case of tampering aimed at data stores in Microsoft Azure's cloud database, storing the database access keys in the Azure Key Vault. Additionally, ensuring the databases are part of the Azure Virtual Network (VNet), which prevents direct access to the databases from the Internet.<br>• When attackers attempt to tamper with data received at the application programming interfaces (APIs) in an ABB Ability™ solution, applying API gateways and web application firewalls to prevent meddling with the public APIs. |
| **Repudiation** | Attackers often try to hide their malicious activity to avoid being detected and blocked. They might try to repudiate actions they have performed; for instance, by erasing them from the logs, or by spoofing the credentials of another user. | ABB's tampering defense – from device to edge to cloud (where Microsoft Azure provides the same protection) – provides complete auditing/ monitoring of log files that record all system and application events to sense and investigate anomalies. |
| **Information Disclosure** | A common vulnerability that can lead to expensive and/or destructive data breaches – an attacker attempts to acquire information about a system. Typically, the attacker tries to capture data transferred across system and services interfaces when that data is moved by an ABB Ability™ solution, and then uses that information to gain malicious access. | ABB's Information Disclosure defense uses strong mutual authentication and encryption for all data transfers among interfaces, employs the Azure Virtual Network (VNet) and encrypts all data in the ABB Ability™ databases. |
| **Denial of Service (DoS)** | Attacks which flood a system with so many requests that the system on which a solution is running can no longer respond, and crashes. DoS attacks prevent regular users from accessing a system, typically as part of a ransomware extortion attempt. | ABB relies on the strong anti-DoS capabilities of the Microsoft Azure cloud platform on which ABB Ability™ solutions run. |
| **Escalation of Privilege** | Refers to malicious users acquiring higher-order privileges within a system to perform unauthorized, usually harmful, actions. This is sometimes done when users authorized to perform some lower-level functions spoof a user with higher privileges to gain those privileges. | ABB's Escalation of Privilege defense uses strong authorization techniques, including Ability Role-based Access Control (RBAC) Services and Azure's Active Directory (AD). Authentication establishes who you are, while authorization determines what you are allowed to do. |

# ABB cybersecurity starts with the platform

The Industrial Internet of Things generates superior business value when its components sense, communicate, store, analyze, derive insights and then act on data generated by connected devices in the physical and virtual worlds. This requires a platform for collecting and processing data from a diverse range of sources, turning data into insights that enable business-optimizing action.

ABB, unlike some other companies, has not built a platform from scratch. Instead, ABB uses its broad industrial experience to create a third generation IIoT platform – standards-based, flexible, reusable IT building blocks – atop Microsoft Azure, the most advanced Platform as a Service (PaaS) system. The ABB Ability™ platform provides a set of common software technologies and services at the device, edge and cloud levels.

ABB employs best-in-class technologies from multiple, trusted IT leaders, extended with domain expertise garnered by ABB over years of experience in the field. The company has partnered with Microsoft to harness its massive investment in Azure and the vibrant ecosystem Microsoft has established around it. Azure delivers a powerful foundation for cloud-based and hybrid-cloud applications.

Additionally, ABB is continually strengthening the ABB Ability™ platform by adding software from vendors that specialize in cybersecurity and privacy.

## Data protection at the vulnerable network edge

The rise of connected edge computing potentially increases cybersecurity threats as valuable company and customer data, formerly protected by isolation inside an organization's network, is transmitted to the edge and then to the cloud, where powerful analytics identify valuable, actionable business insights.

To mitigate risk, ABB has developed the ABB Ability™ Edge as a layer of defensive security that supports, manages and optimizes the connection between the company environment and cloud.

ABB Ability™ Edge is a gateway – a secure doorway – between the public internet and the easier-to-protect factory network. ABB Ability™ Edge protects OT networks from external access and from inadvertently exposing OT details to the cloud. Threats like botnets can therefore be avoided by preventing devices from connecting to the internet and/or cloud directly.

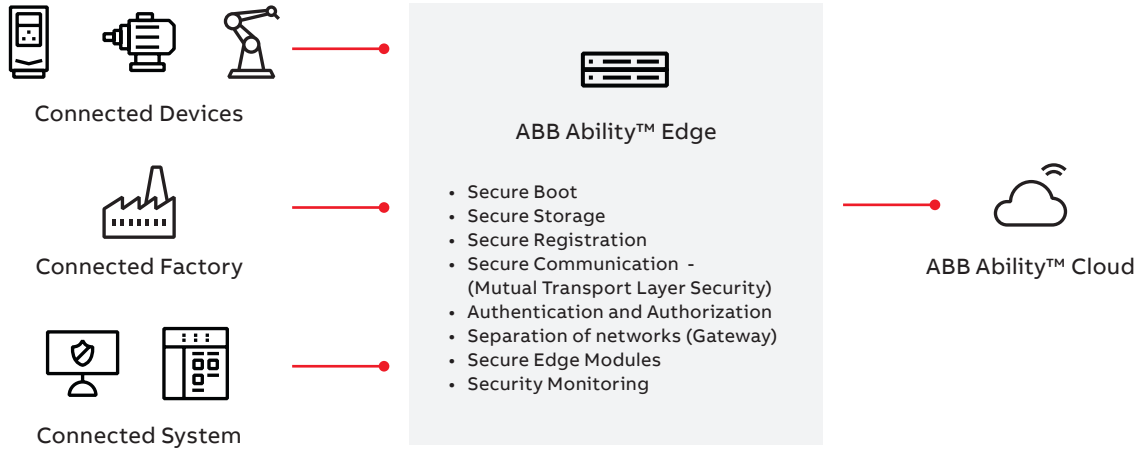


Figure 1: A secure gateway between the IT /internet and the easier-to-protect factory network

ABB Ability™ Edge also incorporates security to protect telemetry data from IIoT and smart sensors, access and control keys to ensure that only authorized users gain access, and device registration data for, to cite one example, field sensors that communicate with ABB Ability™ solutions.

Here are several of the major cybersecurity elements of ABB Ability™ Edge that, as part of ABB's "Security by Design" policy, are shared by all ABB Ability™ solutions:

- **Secure registration** assigns a unique identity to each device. (A number analogous to the unique device ID, called an IMED, which every smart-phone carries.) This number functions like a fingerprint to differentiate each device from every other device in the world. Hackers therefore can't attach random new devices to a network, because the network will only recognize those that are on its list of approved, registered devices.
  - Accordingly, all edge devices – e.g., sensors, motors, robots – must be registered before they are allowed to communicate across the gateway, and only those registered devices can communicate with the cloud, whether it's with each other on-premises or with other, geographically dispersed nodes of a customer's industrial automation network.
  - Registration also prevents identity impersonation through assigning each device a unique number. If a device has been compromised, it can be removed from the system by revoking its certificate. Thus, no future copycat – lacking the unique registration number – will be granted access.
- **Separation of networks.** ABB Ability™ Edge provides a key security element first developed in IT– separation between industrial automation networks and the outside world. OT devices cannot communicate directly to the cloud through ABB Ability™ Edge. Rather, devices communicate with ABB Ability™ Edge, and ABB Ability™ Edge in turn communicates with the cloud. This minimizes opportunities for cyber-attackers to enter OT networks from the internet.
- **Authentication.** Only mutually authenticated devices are allowed to communicate between edge devices and the cloud. Trust has to be established mutually between communication partners to guard against impersonation.
- **Authorization.** While authentication ensures users are who they claim to be, authorization ensures users get access only to the data for which they have permission, and nothing more.
- **Encryption**. All communication across the edge boundary is encrypted and integrity-protected by a mutually trusted connection. All data stored by ABB Ability™ solutions, and/or data stored in or managed by the ABB Ability™ platform, is also encrypted.
  - Encryption is important for both "data in motion" transported over an internal factory network and/or across the public internet, and for "data at rest," which is stored or inactive data, that's protected via encryption.
- **Secure Boot.** Secure Boot verifies the trustworthiness of all running software. Secure Boot uses a signed cryptographic key, which is itself protected against tampering, to provide continuous assurance that only authentic software which has not been tampered with is executed.
- **Secure Storage** provides hardware-based protection to guard data against both malicious as well as inadvertent leakage. Secure storage utilizes several methods to accomplish this, including setting aside a special, tamper-proof area where the data to be protected is both encrypted and isolated in a secure, "trusted" zone.
- **Secure Update** provides update and patch capabilities, where software is verified for authenticity and integrity prior to installation to assure the software has not been tampered with.

## Support for global data privacy and protection standards

ABB digital solutions adhere to ISO 27018, Platform Industrie 4.0 and the Industrial Internet Consortium's standards, as well as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act, two of the world's most stringent. ABB's cloud partner, Microsoft Azure, complies with the GDPR, as well as privacy regulations instituted by Japan, Argentina and federal and provincial authorities in Canada.

As noted above, ABB also campaigns for global adoption of a Data Bill of Rights.

In a similar manner, the various data privacy standards ABB supports require organizations that collect personal information from users to define why and what personal information is collected and how it is used. These regulatory frameworks often empower citizens to manage and remove their own data.

ABB solutions comply with the letter and spirit of the strictest global data protection and privacy standards by ensuring that use of personal data is minimized, anonymized when used and purged from systems after a period of time. All user information, including credentials, is stored in customer-owned directories rather than in the solutions themselves.

The table below details the regulatory compliance practices in all ABB Ability™ solutions.

—

**TABLE B: Data Protection Best Practices**

| | |
|---|---|
| Protection of user data | All ABB solutions provide the capability to purge all sensitive data, including user credentials, keys and personal data, upon decommission or when releasing the product from active service. |
| | Only relevant personal data is collected. |
| | ABB solutions minimize the use of personal data and, where used, is anonymized where possible. |
| | The underlying ABB Ability™ platform itself does not collect personal data. |
| | Data is securely deleted when no longer needed. |
| | Data can only be used for agreed-upon purposes. |
| | Storage is subject to access control. Storage encryption is used where appropriate. |
| | In addition to purging expired data from the solution, the infrastructure owner ensures that all sensitive data are purged upon customer, application or service decommission. |

## Data protection throughout the product lifecycle

ABB Ability™ solutions offer cybersecurity and data protection throughout products' complete lifecycles. The table below offers details.

—
**TABLE C: Cybersecurity and Data Protection Throughout the ABB Ability™ solution lifecycle**

| Governance | Implementation | Verification | Support throughout the product lifecycle |
|---|---|---|---|
| Cybersecurity and data protection must be formal, established parts of overall organization. | Cybersecurity and data protection are supported as major components of product development. | Cybersecurity and data protection capabilities must be verified throughout the product development lifecycle. | Cybersecurity and data protection efforts continue after product release throughout system lifecycle. |
| A formal cybersecurity and data protection organization is in place, supported by management at the highest levels. | Cybersecurity and data protection are supported as major components of product development. | Cybersecurity and data protection capabilities must be verified throughout the product development lifecycle. | Cybersecurity and data protection efforts continue after product release throughout system lifecycle. |
| | Cybersecurity and data protection training is mandated for all ABB software developers. | All critical source code is analyzed using state of the art technology. | ABB provides supporting material for proper installation and commissioning. |
| Established cybersecurity and data protection policies approved by ABB CEO mandating industry-standards minimum expectations for all products. | Formal process for capturing cybersecurity and data protection requirements. | ABB operates an industry leading, centralized security test center performing 200+ tests per year. | Continuous validation of 3rd party software dependencies. |
| Cybersecurity and data protection further enforced through integration into ABB development process. | Cybersecurity and data protection assessment done for all product and development efforts. | ABB complements internal verification with external security testing. | ABB has established processes to handle cybersecurity incidents, data breaches and software vulnerabilities. |
| | Use of common and standardized components is mandated. | Verification also includes interoperability testing. | |

## What we talk about when we talk about 'best practices'

True security can't be bolted onto an existing product. It must be a key element in every product's DNA, just as data protection and cybersecurity risk-mitigation is part of ABB's DNA. Every ABB Ability™ solution is "secure by design." Cybersecurity experts are involved with solution development and build from Day 1, and cybersecurity remains a key priority throughout every product and solution's lifecycle.

We live this philosophy through an internal Group Cybersecurity Council that brings together experts from R&D, IT infrastructure, Legal, Communications and Cybersecurity to collaborate in design and production and to educate one another on the discovery of new threats and how to defend against them.

The ABB Group Cybersecurity Council also works with such industry standards bodies as Platform Industrie 4.0 and the Industrial Internet Consortium, and insists that every supplier – and, of course, every partner – adheres to the same stringent cybersecurity levels as ABB.

Among the cybersecurity best practices designed into every ABB Ability™ solution:

- Stateless services design (services executed by software are kept separated from the data which keeps track of those services)
- Services-based implementation (software is run utilizing an applications container, isolating each service from other applications in the cloud for enhanced protection and security)
- Utilization of the least-required-privileges principle in access control (software processes are granted only those access rights essential to their operation)
- Logging only the minimum amount of data necessary for successful operation
- Separation of concerns between functional implementation and access control (large programs consist of separate software modules, each of which is separated and thus better protected).

The table below presents the additional threat protection – above and beyond the threats discussed earlier – that each ABB Ability™ solution must support before it is released.

**TABLE D: Cybersecurity Requirements for ABB Ability™ solutions (partial list)**

| Threat | Threat protection capabilities in ABB Ability™ solutions |
|---|---|
| Resistance to backdoor attacks | ABB Ability™ solutions do not have any accounts, passwords, secret or private keys or certificates that cannot be changed or removed by the authorized end-user. |
| Vulnerability handling | ABB Ability™ solutions do not have any accounts, passwords, secret or private keys or certificates that cannot be changed or removed by the authorized end-user. |
| Patch management/ Secure patching | ABB provides bespoke information and recommendations on patching software-based products while being fully aware that not all OT systems can be patched, in which case ABB suggests alternative approaches. ABB Ability™ solutions provide secure updating mechanisms for appropriate connected devices. |
| Credential Protection | Confidentiality and integrity guaranteed via identity credentials and cryptographic material (keys and certificates). |
| Secure Communication | Internet-facing communication is based on secure protocols and guarantees the following principles:<br>• Cryptographically strong mutual authentication based on digital certificates<br>• Data confidentiality and integrity<br>• Product-initiated outbound, bidirectional communication and discarding of all unsolicited inbound connections |
| Minimize exposed attack surfaces/ hardening | The attack surface is minimized by enabling only those ports and services specifically needed to support the main functionality of a solution. |
| Integrity and authenticity of software deliverables | All software delivered to customers is packaged in a way that allows the customer to verify the integrity and authenticity of the package. For internet-connected devices, integrity and authenticity are verified using secure boot mechanisms as well as applicable secure patching/ updating mechanisms. |
| Data protection | Data-at-rest and data-in-transit is guaranteed protected in accordance with all applicable regulations, customer policies and requirements, industry standards and ABB policies and standards.<br><br>Products provide the capability to purge all sensitive data including but not limited to credentials, keys, and personal data upon decommission or when releasing the product from active service. |
| Validation of input data | Data provided through external user interfaces, application program interfaces (APIs) or via network communication will be validated. |
| Logging and monitoring | All ABB Ability™ solutions provide mechanisms to log and monitor any anomalous behaviors and events. |

## It takes a Global Village

Realizing "it takes a Global Village" to optimize industrial cybersecurity in worldwide interconnected markets, in 2019 ABB was a leading force behind the founding of the Operational Technology Cyber Security Alliance, an international consortium of OT operators and their vendor communities to "build and support an understanding of OT cybersecurity challenges and solutions from the board room to the factory floor." Cybersecurity areas of focus for the OTCSA include:

- Industrial control system equipment, software and networks
- IT equipment and networks that are used in OT systems or provide functionality to OT systems
- Building management systems
- Facilities and control rooms access control systems
- CCTV systems
- Medical equipment

## In the end, it's all about trust

In this paper we've detailed how ABB Ability™ solutions deliver on the promise of protecting data and systems in Industrial Internet of Things networks that are driving the digital transformation of industries around the world. We've emphasized that cybersecurity and data protection are not individual products or "one and done" solutions, but a constant battle against intruders bent on mischief, thievery or sabotage.

ABB has made a company-wide commitment to live and breathe cybersecurity 24/7 as we help customers know more, do more and do better – together, and is proud to write the future with customers, partners and suppliers who are equally committed. What we value most of all is the trust of our customers. Earning and keeping that trust is our North Star as we develop ABB Ability™ solutions – including cybersecurity solutions – to keep our customers' businesses operating safely, securely, profitably and continuously.

—

Our promise to customers: ABB Ability™ digital solutions are today's leaders in the generation of optimal business insights with unsurpassed cybersecurity risk mitigation and privacy protection. And ABB will remain in the forefront of empowering our customers as the Industrial Internet of Things enables "business as unusual" through the digital transformation of industries around the world.

**ABB Inc.**
3055 Orchard Drive
San Jose, CA 95134
USA

**ability.abb.com**