ABB Ability™ digital services for drives
Cloud cybersecurity

Cybersecurity concerns are common when data from industrial equipment is communicated over networks. In the event of centralized data being uploaded to the cloud, the process is described below. ABB follows state-of-the art processes to ensure security of data and equipment. However, customers also need to be security-aware if their systems are part of the monitoring data transfer.
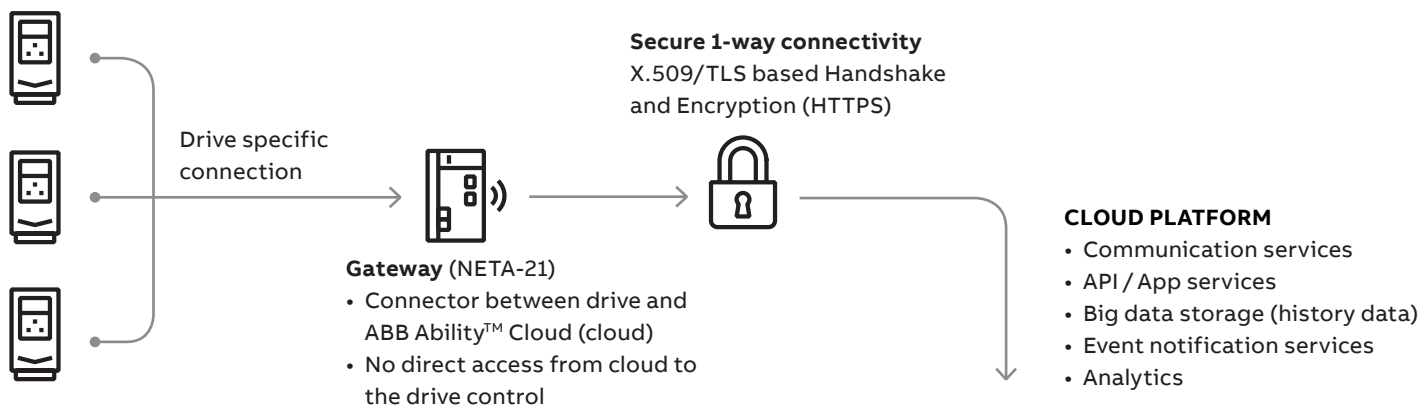
Customer's site/ Installed base

Drive specific connection

Secure 1-way connectivity
X.509/TLS based Handshake and Encryption (HTTPS)

Gateway (NETA-21)
• Connector between drive and ABB Ability™ Cloud (cloud)
• No direct access from cloud to the drive control

CLOUD PLATFORM
• Communication services
• API / App services
• Big data storage (history data)
• Event notification services
• Analytics

ABB EXPERT
Access to Condition Monitoring portal via internet, access to remote assistance page for customer assistance.

Internet HTTPS

CUSTOMER
Access to Condition Monitoring portal via Internet.

Internet HTTPS

PLATFORM

CLOUD SECURITY
Azure Security Center
Policy-Based Access Control

How to deal with cybersecurity

ABB's security processes

- It is possible to view and subscribe to ABB cybersecurity alerts and notifications at:
  https://new.abb.com/about/technology/cyber-security/alerts-and-notifications
- Reports can be submitted directly to ABB's Cybersecurity Response Team (CERT), that acts as the official
  ABB CERT, using the email address: cybersecurity@ch.abb.com
- Patch management and vulnerability monitoring is done continuously for the software versions
- Secure Development Lifecycle (SDL) practices are followed
- All software is checked by several anti-virus programs before release
- 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.
- Cybersecurity training is mandatory for all users involved in the development and operation of services
- ABB requires its suppliers to follow a set of rules, and internally ABB follows even stricter ones.
  For more information see: https://new.abb.com/about/supplying/cyber-security

Management of customer data

- ABB Ability™ Data Manifesto defines how customer data is used
- Customer's data and IP remains confidential
- Customers know what we do with their data
- We will not disclose customers' data without their consent
- Ensuring data/IP is not shared with or used for the benefit of competitors

Drive specific connection

- Various ABB drives can be connected with:
  - Optical fiber
  - Panel bus (by replacing panel)
  - Ethernet fieldbus module on drive
- NETA-21 gateway can be used as local web page for drive access
- Writing to drive from the cloud is not possible. Only local NETA-21 web UI can be used to modify drive parameters when specific user account is configured.
- Secure password must be set on the NETA-21 web UI to protect the local interface
- For service purposes, the gateway does not require any incoming or VPN connection
- On-site security is the customer's responsibility. Local firewalls must be configured to allow only necessary traffic.
- Cellular connection can help isolate drive monitoring connection from local control network

Secure one-way data flow

- Data and events are pushed 1-way to cloud (using HTTPS)
- WebSocket to different server than HTTP push provides limited commands to request data and update NETA-21 (no writing to drive)
- Updates are fetched only from ABB servers (ABB Library) and checked for valid signature
- Cloud connected software component in NETA-21 has no permission to write to drives
- TLS v1.2 with secure ciphers is used between gateway and cloud
- Certificate validation ensures that data is sent only to legitimate cloud
- Gateway should be placed behind firewall. Outbound port TCP:443 to cloud is required.
- If customer network cannot be used, cellular router can be used to provide the internet connection. Cellular router also provides firewalling against access to NETA-21 web interface.
- Some modems provide optional VPN feature for NETA-21 web interface remote access. This is enabled only if needed in special cases and agreed with customer.
- Bulk data option (data transfer from SD memory card to cloud portal) is an alternative to avoid direct internet connection

Gateway web UI

- The gateway handles protocol conversion, data aggregation and multiple layers of security
- The gateway runs only signed original ABB software. User cannot install any additional software on the gateway.
- Gateway software can be updated both locally, as well as centrally using the cloud
- ABB Ability™ cloud gateways are verified to block unneeded connection types
- All actions are logged in the gateway for audit trail purposes in addition to being sent to the cloud
- The local web interface of NETA-21 can be left behind firewall, or blocked from external access by using the cellular modem
- Data is signed to prevent unwanted modifications
- Physical security (e.g. locked cabinet or monitored access to electrical room) is assumed to prevent unwanted local access

Portal security

- Portals use secure connections (HTTPS) and modern reactive interfaces
- MyABB provides single sign-on for all ABB services
- User accounts are handled by central rules, in central Active Directory
- Two factor authentication is available
- All user accounts are personal (no group or company accounts) and the account will be set to inactive when not in use.
- Customer shall inform ABB contact person that account needs to be removed
- To remove an account, ABB contact person enters ticket to ABB ticketing system, which will trigger approval process and deletion of account

Cloud security

- All stored data is encrypted in cloud
- Best practices such as Azure Key Vault are used for secure storage
- Identity and access management, and multi-factor authentication are used in cloud
- Cloud assets are protected and monitored against threats
- Cloud services keep audit trail of all actions

—

For more information, please contact
your local ABB representative or visit

abb.com/drives
abb.com/drivespartners
abb.com/motors&generators

—

For other product documents

www.abb.com/drives/documents