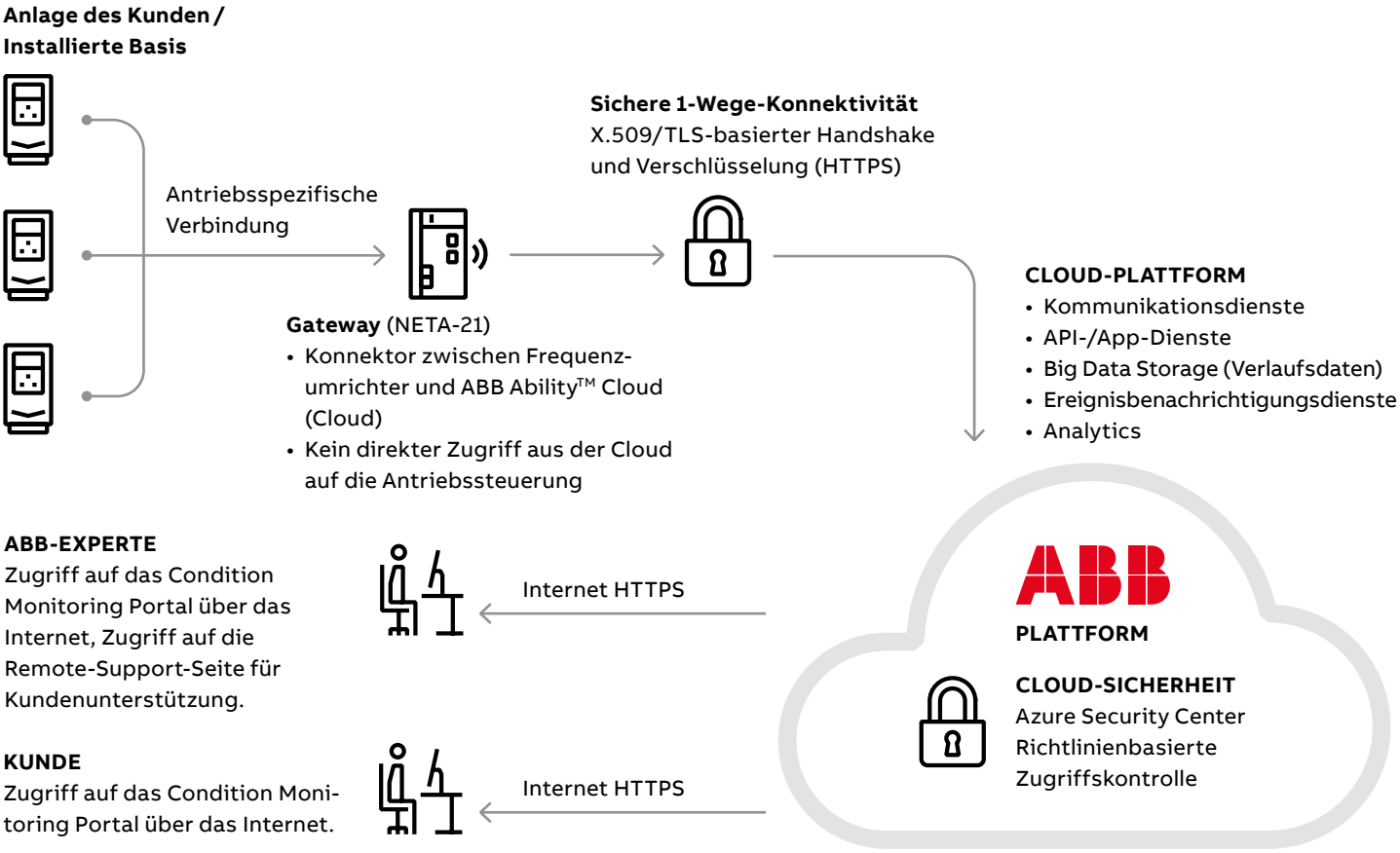
ABB MOTION SERVICES

ABB Ability™ Digitale Services für Frequenzumrichter

Cloud-Cybersicherheit

Bedenken hinsichtlich der Cybersicherheit sind häufig, wenn Daten von Industrieanlagen über Netzwerke kommuniziert werden. Für den Fall, dass zentralisierte Daten in die Cloud hochgeladen werden, wird der Prozess unten beschrieben. ABB wendet modernste Prozesse an, um die Sicherheit von Daten und Geräten zu gewährleisten. Aber auch Kunden müssen sicherheitsbewusst sein, falls ihre Systeme Teil der Monitoring-Datenübertragung sind.



Wie man mit Cybersicherheit umgeht

Sicherheitsprozesse von ABB

- Unter https://new.abb.com/about/technology/cyber-security/alerts-and-notifications können ABB-Cybersicherheitswarnungen und -benachrichtigungen angezeigt und abonniert werden
- Meldungen können über die E-Mail-Adresse cybersecurity@ch.abb.com direkt an das Cybersecurity Response Team (CERT) von ABB übermittelt werden, das als offizielles CERT von ABB fungiert
- Patch-Management und Schwachstellenüberwachung werden kontinuierlich für die Softwareversionen durchgeführt
- Secure Development Lifecycle (SDL)-Praktiken werden befolgt
- Sämtliche Software wird vor der Freigabe von mehreren Antivirenprogrammen geprüft
- Ein Hauptmerkmal des Angebots von ABB ist das unabhängige Device Security Assurance Center (DSAC), in dem alle ABB-Produkte modernsten Sicherheitstests unterzogen werden, bevor sie auf den Markt gebracht werden.
- Dieser Prozess misst Robustheit und Sicherheitsintegrität und umfasst Port-Scanning, Network Flooding, Vulnerability Scanning und Protocol Fuzzing.
- Cybersicherheitsschulungen sind für alle Benutzer, die an der Entwicklung und dem Betrieb von Diensten beteiligt sind, obligatorisch
- ABB verlangt von seinen Lieferanten die Einhaltung einer Reihe von Regeln, und ABB befolgt intern sogar noch strengere Regeln.
- Weitere Informationen finden Sie unter: https://new.abb.com/about/supplying/cyber-security

Verwaltung von Kundendaten

- ABB Ability™ Data Manifesto definiert, wie Kundendaten verwendet werden
- Kundendaten und IP bleiben vertraulich
- Kunden wissen, was wir mit ihren Daten machen
- Wir geben Kundendaten nicht ohne deren Zustimmung weiter.
- Sicherstellen, dass Daten/IP nicht mit Wettbewerbern geteilt oder zum Vorteil von Wettbewerbern verwendet werden

Antriebsspezifische Verbindung

- Verschiedene ABB-Antriebe können angeschlossen werden via:
  - Glasfaser
  - Panelbus (anstatt einem Panel)
  - Ethernet-Feldbusmodul am Antrieb
- NETA-21-Gateway kann als lokale Webseite für den Umrichterzugriff verwendet werden
- Das Schreiben auf Umrichter aus der Cloud ist nicht möglich. Nur die lokale NETA-21-Web-UI kann verwendet werden, um Antriebsparameter zu ändern, wenn ein bestimmtes Benutzerkonto konfiguriert ist.
- Auf der NETA-21-Webbenutzeroberfläche muss ein sicheres Passwort festgelegt werden, um die lokale Schnittstelle zu schützen
- Für Servicezwecke benötigt das Gateway keine eingehende oder VPN-Verbindung
- Die Sicherheit vor Ort liegt in der Verantwortung des Kunden. Lokale Firewalls müssen so konfiguriert werden, dass nur der notwendige Datenverkehr zugelassen wird.
- Eine Mobilfunkverbindung kann dabei helfen, die Antriebsmonitoringverbindung vom lokalen Steuernetzwerk zu isolieren

Sicherer Datenfluss in eine Richtung

- Daten und Ereignisse werden einseitig in die Cloud gepusht (über HTTPS)
- WebSocket auf einen anderen Server als HTTP-Push bietet begrenzte Befehle zum Anfordern von Daten und Aktualisieren von NETA-21 (kein Schreiben auf Umrichter)
- Updates werden nur von ABB-Servern (ABB Library) geholt und auf gültige Signatur geprüft
- Cloud-verbundene Softwarekomponente in NETA-21 hat keine Berechtigung zum Schreiben auf Umrichter
- Zwischen Gateway und Cloud wird TLS v1.2 mit sicheren Chiffren verwendet
- Die Zertifikatsvalidierung stellt sicher, dass Daten nur an legitime Clouds gesendet werden
- Das Gateway sollte hinter der Firewall platziert werden. Ausgehender Port TCP:443 zur Cloud ist erforderlich.
- Wenn das Kundennetzwerk nicht verwendet werden kann, kann ein Mobilfunkrouter verwendet werden, um die Internetverbindung bereitzustellen. Der Mobilfunkrouter bietet auch eine Firewall gegen den Zugriff auf die NETA-21-Webschnittstelle.
- Einige Modems bieten eine optionale VPN-Funktion für den Fernzugriff auf die NETA-21-Webschnittstelle. Dies wird nur bei Bedarf in Sonderfällen und nach Absprache mit dem Kunden aktiviert.
- Die Massendatenoption (Datenübertragung von der SD-Speicherkarte zum Cloud-Portal) ist eine Alternative

Gateway-Web-UI

- Das Gateway übernimmt die Protokollkonvertierung, Datenaggregation und mehrere Sicherheitsebenen
- Das Gateway führt nur signierte Original-ABB-Software aus. Der Benutzer kann keine zusätzliche Software auf dem Gateway installieren.
- Gateway-Software kann sowohl lokal als auch zentral über die Cloud aktualisiert werden
- ABB Ability™ Cloud-Gateways sind verifiziert, um nicht benötigte Verbindungstypen zu blockieren
- Alle Aktionen werden im Gateway zu Audit-Trail-Zwecken protokolliert und an die Cloud gesendet
- Die lokale Webschnittstelle von NETA-21 kann hinter der Firewall belassen oder mithilfe des Mobilfunkmodems für externen Zugriff blockiert werden
- Die Daten werden signiert, um unerwünschte Änderungen zu verhindern
- Physische Sicherheit (z. B. verschlossener Schrank oder überwachter Zugang zum Elektroraum) wird vorausgesetzt, um unerwünschten lokalen Zugriff zu verhindern

Portalsicherheit

- Portale verwenden sichere Verbindungen (HTTPS) und moderne reaktive Schnittstellen
- MyABB bietet Single Sign-On für alle ABB-Dienste
- Benutzerkonten werden von zentralen Regeln im zentralen Active Directory verwaltet
- Zwei-Faktor-Authentifizierung ist verfügbar
- Alle Benutzerkonten sind persönlich (keine Gruppen- oder Firmenkonten) und das Konto wird auf inaktiv gesetzt, wenn es nicht verwendet wird.
- Der Kunde muss die ABB-Kontaktperson darüber informieren, dass das Konto entfernt werden muss
- Um ein Konto zu entfernen, gibt die ABB-Kontaktperson ein Ticket in das ABB-Ticketsystem ein, das den Genehmigungsprozess und die Löschung des Kontos auslöst

Cloud-Sicherheit

- Alle gespeicherten Daten werden in der Cloud verschlüsselt
- Für die sichere Speicherung werden Best Practices wie Azure Key Vault verwendet
- Identitäts- und Zugriffsverwaltung sowie Multi-Faktor-Authentifizierung werden in der Cloud verwendet
- Cloud-Assets werden vor Bedrohungen geschützt und überwacht
- Cloud-Dienste führen Audit-Trails aller Aktionen

Weitere Informationen erhalten Sie von Ihrer ABB-Vertretung oder im Internet:

new.abb.com/drives/de/service/advanced-service/remote-condition-monitoring

Änderungen vorbehalten. Bei Bestellungen gelten die vereinbarten Einzelheiten. ABB übernimmt keinerlei Verantwortung für mögliche Fehler oder evtl. in diesem Dokument fehlende Angaben.

9AKK106930A8297 REV E DE 03.2022