



SERVICE@ANTREIBEN.DE

SERVICES FÜR DIE ANTRIEBSTECHNIK

ABB Ability™ Digitale Services für Drives

Cloud Cybersicherheit



Bedenken bei der Cybersicherheit sind weit verbreitet, wenn Daten von Industrieanlagen über Netzwerke übermittelt werden. Das Hochladen zentralisierter Daten in die Cloud erfolgt mit dem nachfolgend beschriebenen Verfahren. ABB wendet Prozesse nach dem neuesten Stand der Technik an, um die Sicherheit der Daten und Anlagen zu gewährleisten. Kunden müssen allerdings auch ein Sicherheitsbewusstsein haben, wenn ihre Systeme in die Übertragung von Überwachungsdaten eingebunden sind.

Beim Kunden/ installierte Einheiten

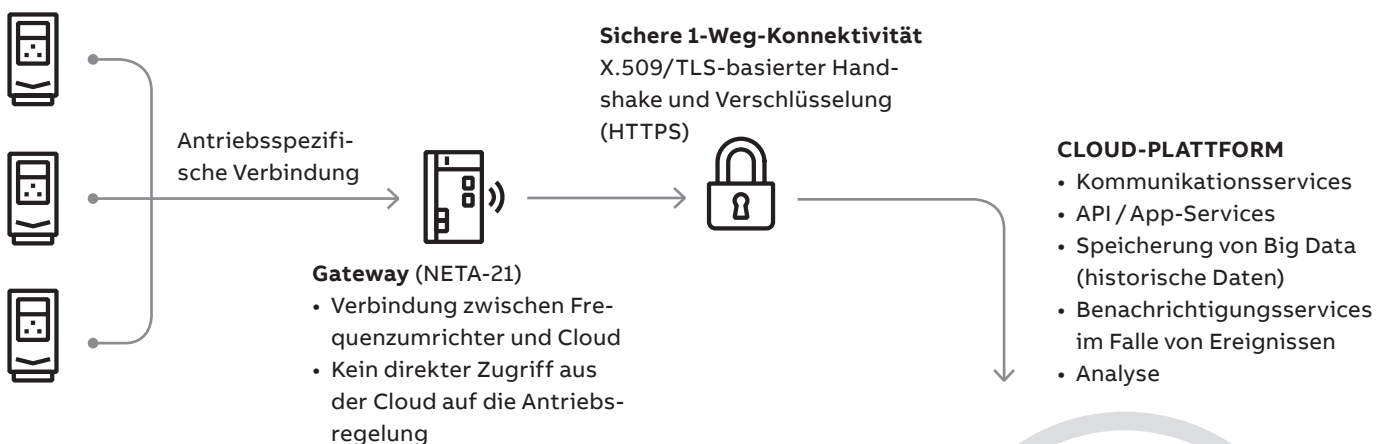


ABB-EXPERTE

Zugriff auf das Condition Monitoring Portal über das Internet, Zugriff auf die Hilfeseite zur Unterstützung der Kunden.



KUNDE

Zugriff auf das Condition Monitoring Portal über das Internet.



Umgang mit dem Thema Cybersicherheit



Sicherheitsprozesse bei ABB

- Über den folgenden Link können Sie Warnungen und Benachrichtigungen im Rahmen der ABB Cybersicherheit anzeigen und abonnieren:
<https://new.abb.com/about/technology/cyber-security/alerts-and-notifications>
- Berichte können direkt an das Cybersecurity Response Team von ABB gesendet werden, das als offizielles ABB CERT agiert und über die folgende E-Mail-Adresse erreichbar ist: cybersecurity@ch.abb.com
- Das Patch-Management und die Überwachung auf Schwachstellen erfolgt für die Software-Versionen kontinuierlich.
- Die Praktiken des Secure Development Lifecycle (SDL) werden befolgt.
- Die gesamte Software wird vor der Freigabe durch mehrere Virenschutzprogramme überprüft.
- Ein wesentliches Merkmal des Angebots von ABB ist das unabhängige Device Security Assurance Center (DSAC), in dem sämtliche ABB-Produkte einer Sicherheitsprüfung nach dem neuesten Stand der Technik unterzogen werden, bevor sie auf den Markt gebracht werden. Hierbei werden die Robustheit und Sicherheitsintegrität überprüft. Die Prüfung beinhaltet Port-Scanning, Netzwerküberflutung, Schwachstellenüberprüfung sowie Protokoll-Fuzzing.
- Eine Schulung in Cybersicherheit ist für alle Nutzer verpflichtend, die an der Entwicklung und Nutzung der Services beteiligt sind.
- ABB verpflichtet seine Lieferanten zur Einhaltung der Regeln und wendet intern noch strengere Regelungen an. Weitere Informationen siehe: <https://new.abb.com/about/supplying/cyber-security>

Verwaltung der Kundendaten

- Das ABB Ability™ Datenmanifest legt die Verwendung der Kundendaten fest
- Kundendaten bleiben Eigentum der Kunden
- Die Kunden wissen, was wir mit ihren Daten machen
- Wir geben Kundendaten nicht ohne Zustimmung des Kunden preis
- Es wird sichergestellt, dass Daten/IP nicht mit Mitbewerbern geteilt oder zu deren Vorteil verwendet werden.



Antriebsspezifischer Anschluss

- ABB Frequenzumrichter können angeschlossen werden über:
 - LWL
 - Panelbus (durch Ersetzen des Bedienpanels)
 - Ethernet über FENA-x1
- Der NETA-21 Gateway kann als lokale Zugriffsmöglichkeit auf den Frequenzumrichter verwendet werden.
- Die Standardzugriffsberechtigung erlaubt keine Konfiguration des Frequenzumrichters, kann allerdings lokal aktiviert werden.
- Für die NETA-21 Internetschnittstelle muss ein sicheres Passwort eingerichtet werden, um den böswilligen Zugriff aus dem lokalen Netzwerk zu verhindern.
- Zu Wartungszwecken benötigt NETA-21 keinen Eingang oder VPN-Anschluss.
- Die Sicherheit vor Ort liegt in der Verantwortung des Kunden. Der lokale Ethernet-Zugang sollte begrenzt sein, und Firewalls müssen so konfiguriert werden, dass nur der notwendige Datenverkehr zulässig ist.
- Mit einem Mobilfunkmodem für den Internetzugang kann die Verbindung zur Antriebsüberwachung von dem lokalen Steuerungsnetzwerk getrennt werden.



Sichere 1-Weg-Verbindung

- Beim Senden von Daten an die Cloud handelt es sich um einen reinen HTTPS Push. Daten werden also nur gesendet.
- Der zusätzliche WebSocket-Kanal ermöglicht eine begrenzte Anzahl von Befehlen z. B. zur Anforderung bestimmter Protokolldateien, dem Neustart des Gateway (nicht des Frequenzumrichters) und zur Bereitstellung der neuesten Software Updates.
- Updates werden nur vom ABB Library Download Center bezogen und auf eine gültige Signatur überprüft.
- Interne Benutzerkonten des Gateway verhindern das Schreiben auf den Frequenzumrichter als Standard- bzw. Cloud-Nutzer.
- Modernste Verschlüsselungsmethoden wie TLSv1.2 mit X.509 Zertifikaten werden zur Sicherstellung der Vertraulichkeit der Daten während der Übertragung verwendet.
- Die Überprüfung des Zertifikats stellt sicher, dass Daten nur an die legitime ABB Ability™ Cloud gesendet werden.
- Der Gateway sollte sich hinter der Firewall befinden. Der Ausgangsanschluss TCP:443 von NETA-21 zur Cloud ist ausreichend. Eingangsanschlüsse sind nicht notwendig.
- Wenn das Kundennetzwerk nicht verwendet werden kann, kann ein Mobilfunk-Router wie eWON Cosy 131 zur Bereitstellung der Internetverbindung verwendet werden. Der Mobilfunk-Router stellt eine Firewall und eine optionale VPN-Schicht bereit (VPN ist kein Standardbestandteil des Service-Angebots und sollte nur aktiviert werden, wenn dies unbedingt notwendig ist).
- Die Massendatenoption (Datenübertragung von der SD-Speicherkarte an das Cloud-Portal) ist eine Alternative, um eine direkte Internetverbindung zu vermeiden.



Gateway-Gerät

- Das Gateway-Gerät NETA-21 wird für die Protokollkonvertierung, Datenverdichtung und die Verwaltung der mehrstufigen Sicherheitsvorkehrungen eingesetzt.
- NETA-21 führt nur signierte Original-Software-Images von ABB aus. Der Anwender kann auf diesem Gerät keine weitere Software installieren.
- Die Gateway-Software kann sowohl lokal als auch zentral über die Cloud aktualisiert werden.
- NETA-21 verfügt über eine interne Firewall, die nicht benötigte Verbindungstypen blockiert.
- Sämtliche Aktionen werden im internen Speicher und auf einer SD-Karte protokolliert. Außerdem werden Ereignisse an die Cloud gesendet.
- Die lokale Internetschnittstelle des NETA-21 kann (nach der Verbindung mit der Cloud), falls erforderlich, komplett deaktiviert werden.
- Die Daten auf der SD-Speicherkarte haben eine Signatur, um unerwünschte Änderungen zu verhindern.
- Es ist ein physischer Schutz (z. B. ein abgeschlossener Schrank) notwendig, um das Löschen von Daten von der SD-Karte zu verhindern.



Sicherheit des Portals

- Portale verwenden sichere Verbindungen (HTTPS) und moderne, reaktive Schnittstellen.
- MyABB ermöglicht eine einzige Anmeldung für alle ABB Serviceleistungen.
- Benutzerkonten werden nach zentralen Regeln in einem zentralen Active Directory verwaltet.
- Eine Zwei-Faktor-Authentifizierung ist verfügbar.
- Alle Benutzerkonten sind personenbezogen (keine Gruppen- oder Unternehmenskonten) und werden gelöscht, wenn sie nicht genutzt werden.
- Der Kunde muss dem Ansprechpartner bei ABB mitteilen, dass ein Konto gelöscht werden soll.
- Um ein Konto zu löschen, gibt der Ansprechpartner bei ABB ein Ticket in das ABB-interne System (MyIS) ein, das (nach einem Genehmigungsverfahren) den Prozess der Konto-löschung einleitet.



Cloud-Sicherheit

- Alle in der Cloud gespeicherten Daten sind verschlüsselt.
- Zur sicheren Speicherung werden Best Practices wie Azure Key Vault verwendet.
- Identitäts- und Zugangsmanagement sowie die Multi-Faktor-Authentifizierung werden in der Cloud verwendet.
- Cloud Assets sind geschützt und werden auf Bedrohungen überwacht.
- Sämtliche Aktionen werden von den Cloud Services protokolliert.

—
Weitere Informationen erhalten Sie
von Ihrer ABB-Vertretung:



Dolomitstrasse 7
D-37431 Bad Lauterberg / OT Barbis
Phone +495524922811
Email: service@antreiben.de
www.antreiben.de

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

—
Ä

Für dieses Dokument und den darin dargestellten Gegenstand sowie darin enthaltene
Abbildungen behalten wir uns alle Rechte vor. Vervielfältigung, Bekanntgabe an Dritte
oder Verwertung seines Inhalts – ganz oder in Teilen – ist ohne schriftliche Zustimmung
von ABB verboten.
Copyright © 2019 ABB. Alle Rechte vorbehalten.