FÜR IHRE IT-ABTEILUNG · STAND OKTOBER 2026

Was Ihr Werk verlässt. Und was nicht.

Eine Box an der Maschine liest Daten aus der Steuerung und vom Schwingungssensor, berechnet daraus vor Ort Kennwerte und sendet nur diese verschlüsselt an unsere Plattform in Rechenzentren in Deutschland. Die Box schreibt nie auf Ihre Steuerung und nimmt keine eingehenden Verbindungen an.

01 Firewall-Freigaben

RICHTUNG	ZIEL	PORT	ZWECK
Box zur Steuerung	IP der Steuerung	`4840 · OPC UA`	Nur lesen, verschlüsselt
Box zur Plattform	Wird bei Projektstart genannt	`8883 · MQTT/TLS, sonst 443`	Kennwerte senden
Box zum Update-Server	Wird bei Projektstart genannt	`443 · HTTPS`	Signierte Updates abholen
Von außen zur Box	keines	`keiner`	Keine Verbindung möglich

Ist Port 8883 gesperrt, sendet die Box über MQTT mit WebSockets und TLS auf Port 443. Setzt Ihre Firewall TLS-Inspektion ein, braucht die Box eine Ausnahme. Sonst schlägt die beidseitige Zertifikatsprüfung fehl und es wird nichts übertragen. Das ist so gewollt.

02 Datenumfang

BLEIBT BEI IHNEN

- NC-Programme und Werkzeugkorrekturen
- Zeichnungen, CAD- und CAM-Daten
- Werkstückgeometrie und Bauteilmaße
- Auftrags-, Kunden- und Kalkulationsdaten
- Bediener- und Schichtdaten
- Rohe Schwingungssignale

WIRD VERSCHLÜSSELT ÜBERTRAGEN

- Berechnete Schwingungskennwerte der Spindel
- Drehzahl und, soweit verfügbar, Last aus der Steuerung
- Maschinenstatus und Steuerungsalarme
- Zeitstempel und Maschinenkennung
- Zustandsmeldungen der Box

Die Box rechnet die Kennwerte vor Ort und überträgt nur das Ergebnis. Aus diesen Werten lässt sich kein Fertigungsinhalt rekonstruieren. Erfasst werden Maschinendaten, keine Daten über Bediener.

03 Schutz Ihrer Maschine: nur lesen, vierfach abgesichert

A Keine Schreibfunktion
Die Software enthält keinen Code, der auf eine Steuerung schreibt.

B Vorgelagerte Sperre
Jede OPC-UA-Anfrage läuft durch eine Positivliste. Erlaubt sind nur Lesen, Durchsuchen, Abonnieren und Sitzungsaufbau. Schreiben, Methodenaufrufe, Anlegen und Löschen werden blockiert, bevor etwas gesendet wird.

C Automatische Prüfung
Tests stellen bei jeder Änderung an der Software sicher, dass kein Schreibpfad entsteht.

D Lese-Benutzer an der Steuerung
Eigener Benutzer mit reinen Leserechten, bei SINUMERIK etwa nur SinuReadAll und AlarmRead. Benutzer und Zertifikate richten wir nur mit Ihrer Freigabe ein.

- OPC UA signiert und verschlüsselt, Sicherheitsprofil Basic256Sha256. Das Zertifikat der Steuerung ist Pflicht. Ohne es baut die Box keine verschlüsselte Verbindung auf.
- Die Fingerabdrücke der Zertifikate werden vor Ort an der Steuerung verglichen.
- Abfrage standardmäßig einmal pro Sekunde, technisch begrenzt auf höchstens alle 0,1 Sekunden.

ANSPRECHPARTNER
Sascha P. Forbach
Gründer, Geschäftsführer und Software-Architekt

Telefon +49 211 909 899 62
info@forbachandpartners.com
forbachandpartners.com

Graf-Adolf-Straße 41
40210 Düsseldorf
Forbach and Partners Ltd, Paphos (Zypern)

04 Übertragung und Geräteidentität

- MQTT über TLS 1.2 oder höher mit beidseitiger Zertifikatsprüfung. Kein Passwort-Login. Unverschlüsselt nur zu localhost für Tests, per Konfiguration erzwungen.
- Der private Schlüssel jeder Box entsteht auf der Box und verlässt sie nie.
- Das Gerätezertifikat stellt unsere offline betriebene Geräte-CA aus, nur für registrierte Boxen, mit höchstens zwei Jahren Laufzeit. Die Box meldet die Restlaufzeit und warnt ab 30 Tagen.
- Jede Box darf nur unter ihrer eigenen Geräte-ID senden. Welcher Kunde dazugehört, legt allein die Plattform fest.
- Bei Netzausfall puffert die Box mindestens 7 Tage und sendet danach ohne Lücken und ohne Doppelte nach. Gelöscht wird im Puffer erst nach Bestätigung durch die Plattform.

05 Signierte Updates

- Die Box installiert nur Updates mit gültiger digitaler Signatur (Ed25519). Der öffentliche Schlüssel ist auf der Box fest hinterlegt.
- Abgelaufene Update-Beschreibungen und ältere Versionen werden abgelehnt, auch nach einem Neustart.
- Prüfsumme (SHA-256) und Größe der Datei werden vor der Installation geprüft. Abgeholt wird nur über HTTPS.

06 Plattform, Zugriff und Ihre Daten

- Verarbeitung und Speicherung ausschließlich in Rechenzentren in Deutschland.
- Mandantentrennung in der Datenbank selbst (Row Level Security), nicht nur in der Oberfläche.
- Rollen Administrator, Instandhalter und Leser. Rechte werden bei jeder Abfrage auf dem Server geprüft.
- Anmeldung am Dashboard mit Passwort und verpflichtender Zwei-Faktor-Anmeldung (Authenticator-App).
- Rückmeldungen zu Meldungen, Neu-Lernen der Normallage und Datenexporte werden protokolliert.
- Ihre Daten gehören Ihnen: Export jederzeit in einem offenen Format (JSON Lines). Nach Vertragsende löschen wir sie nachweisbar, mit vorherigem Gesamtexport und Bericht über die gelöschten Datensätze.

07 Sicherheitsprozess

- Ausgerichtet an IEC 62443-4-1 und 4-2 sowie am EU Cyber Resilience Act. Ein Bedrohungsmodell ist dokumentiert.
- Alle verwendeten Bibliotheken werden bei jeder Änderung automatisch auf bekannte Schwachstellen geprüft.
- Software-Stückliste (SBOM im Format CycloneDX) auf Anfrage.
- Der Meldeweg für Schwachstellen nach Cyber Resilience Act ist beschrieben.

08 Voraussetzungen an der Steuerung

Siemens SINUMERIK 840D sl, 828D, ONE

- Option „Access MyMachine /OPC UA“
- Lese-Benutzer mit SinuReadAll und AlarmRead
- Netzwerkzugang zur Steuerung (Port 4840)

HEIDENHAIN TNC 640, TNC 620, TNC7

- OPC UA NC Server (Software-Optionen)
- Jeder verbundene Client belegt eine Lizenz
- Nur-Lese-Rolle in der Benutzerverwaltung

iTNC 530 und TNC 320 haben keinen OPC UA NC Server: Prüfung im Einzelfall. FANUC ist geplant. Die Anbindung nutzt die OPC-UA-Schnittstelle, die Siemens und Heidenhain selbst anbieten. Es wird nichts umgebaut und nichts in die Steuerung geschrieben.

> TECHNISCHES GESPRÄCH
>
> Wir gehen dieses Blatt in 20 Minuten mit Ihrem IT-Verantwortlichen durch, technisch und ohne Verkaufsgespräch. Die Adressen für Plattform und Update-Server nennen wir bei Projektstart.

ANSPRECHPARTNER
Sascha P. Forbach
Gründer, Geschäftsführer und Software-Architekt

Telefon +49 211 909 899 62
info@forbachandpartners.com
forbachandpartners.com

Graf-Adolf-Straße 41
40210 Düsseldorf
Forbach and Partners Ltd, Paphos (Zypern)