FOR YOUR IT DEPARTMENT · AS OF OCTOBER 2026

What leaves your plant. And what does not.

An edge box on the machine reads data from the CNC control and the vibration sensor, calculates features on site and sends only these, encrypted, to our platform in data centres in Germany. The box never writes to your CNC control and accepts no inbound connections.

01 Firewall rules

DIRECTION	DESTINATION	PORT	PURPOSE
Box to CNC control	IP of the CNC control	`4840 · OPC UA`	Read only, encrypted
Box to platform	Provided at project start	`8883 · MQTT/TLS, otherwise 443`	Send features
Box to update server	Provided at project start	`443 · HTTPS`	Fetch signed updates
Outside to box	none	`none`	No connection possible

If port 8883 is blocked, the box sends via MQTT over WebSockets with TLS on port 443. If your firewall uses TLS inspection, the box needs an exception. Otherwise mutual certificate validation fails and nothing is transmitted. That is intentional.

02 Data scope

STAYS WITH YOU

- NC programs and tool offsets
- Drawings, CAD and CAM data
- Workpiece geometry and part dimensions
- Order, customer and costing data
- Operator and shift data
- Raw vibration signals

TRANSMITTED ENCRYPTED

- Calculated vibration features of the spindle
- Speed and, where available, load from the CNC control
- Machine status and CNC control alarms
- Timestamps and machine identifier
- Health reports of the box

The box calculates the features on site and transmits only the result. No production content can be reconstructed from these values. We record machine data, not data about operators.

03 Protecting your machine: read-only, four independent safeguards

A **No write function**
The software contains no code that writes to a CNC control.

B **Upstream block**
Every OPC UA request passes an allow-list. Only read, browse, subscribe and session set-up are permitted. Write, method calls, add and delete are blocked before anything is sent.

C **Automated checks**
With every change to the software, tests verify that no write path has been introduced.

D **Read-only user on the CNC control**
A dedicated user with read rights only, for SINUMERIK for example only SinuReadAll and AlarmRead. We set up users and certificates only with your approval.

- OPC UA signed and encrypted, security policy Basic256Sha256. The CNC control's certificate is mandatory. Without it the box does not establish an encrypted connection.
- Certificate fingerprints are compared on site at the CNC control.
- Polling once per second by default, technically limited to at most every 0.1 seconds.

YOUR CONTACT
Sascha P. Forbach
Founder, managing director and software architect

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

Graf-Adolf-Strasse 41
40210 Düsseldorf, Germany
Forbach and Partners Ltd, Paphos (Cyprus)

04 Transmission and device identity

- MQTT over TLS 1.2 or higher with mutual certificate validation. No password login. Unencrypted only to localhost for testing, enforced by the configuration.
- Each box's private key is generated on the box and never leaves it.
- The device certificate is issued by our offline device CA, only for registered boxes and valid for at most two years. The box reports the remaining validity and warns from 30 days.
- Each box may only send under its own device ID. Which customer it belongs to is decided by the platform alone.
- During network outages the box buffers at least 7 days and then sends on without gaps or duplicates. Buffered data is deleted only after the platform has confirmed receipt.

05 Signed updates

- The box only installs updates with a valid digital signature (Ed25519). The public key is pinned on the box.
- Expired update manifests and older versions are rejected, even after a restart.
- Checksum (SHA-256) and file size are verified before installation. Updates are fetched via HTTPS only.

06 Platform, access and your data

- Processing and storage exclusively in data centres in Germany.
- Tenant separation in the database itself (row level security), not just in the user interface.
- Roles administrator, maintenance and read-only. Permissions are checked on the server with every request.
- Dashboard login with password and mandatory two-factor authentication (authenticator app).
- Feedback on alerts, re-learning of the baseline and data exports are logged.
- Your data belongs to you: export at any time in an open format (JSON Lines). When the contract ends we delete it verifiably, after a full export and with a report of the deleted records.

07 Security process

- Aligned with IEC 62443-4-1 and 4-2 and the EU Cyber Resilience Act. A threat model is documented.
- All libraries used are automatically checked for known vulnerabilities with every change.
- Software bill of materials (SBOM, CycloneDX format) on request.
- The vulnerability reporting process under the Cyber Resilience Act is documented.

08 Requirements on the CNC control

Siemens SINUMERIK 840D sl, 828D, ONE

- Option “Access MyMachine /OPC UA”
- Read-only user with SinuReadAll and AlarmRead
- Network access to the CNC control (port 4840)

HEIDENHAIN TNC 640, TNC 620, TNC7

- OPC UA NC Server (software options)
- Each connected client uses one licence
- Read-only role in user administration

iTNC 530 and TNC 320 have no OPC UA NC Server: checked case by case. FANUC is planned. The connection uses the OPC UA interface that Siemens and Heidenhain themselves offer. Nothing is modified and nothing is written to the CNC control.

TECHNICAL CALL

We go through this datasheet with your IT lead in 20 minutes, technically and without a sales pitch. We provide the addresses of the platform and the update server at project start.

YOUR CONTACT

Sascha P. Forbach

Founder, managing director and software architect

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

Graf-Adolf-Strasse 41
40210 Düsseldorf, Germany
Forbach and Partners Ltd, Paphos (Cyprus)