



Installations- und Bedienhandbuch

openXEdge

Industrie-PC für die Prozessdatenerfassung an der Maschine



Brinkhaus GmbH

Version 2026.10.21

Datum: 10.2026

Technische Änderungen jederzeit vorbehalten!



Inhalt

1 Erste Schritte	3
1.1 Einführung	3
1.2 Erste Inbetriebnahme	3
2 Anleitungen	9
2.1 Firmware aktualisieren	9
2.2 Firmware offline per USB installieren	11
2.3 Von einem anderen Rechner zugreifen (HTTPS)	12
2.4 Passwort ändern	16
2.5 Sprache der Bedienoberfläche wählen	17
2.6 Netzwerk konfigurieren	20
2.7 Firewall konfigurieren	21
2.8 Benutzer verwalten	24
2.9 Diagnose lesen	27
2.10 IDEA-4S-Gerät konfigurieren	29
2.11 IO-Link-Master konfigurieren	35
2.12 Messdaten nach Excel exportieren	38
3 Referenz	40
3.1 Diagnose-Codes	40
3.2 IDEA-4S – Signalnamen im DataStore	44
4 Hintergrund	46
4.1 Das Gerät	46
4.2 Anschlüsse der Edge	48
4.3 Wie Updates funktionieren	49
4.4 Grafana-Dashboards	52
4.5 Ressourcen-Anzeige	55
4.6 Fleet-Anbindung	57
4.7 Sicherheit und Support	60
5 Notizen	66



1 Erste Schritte

1.1 Einführung

Die openXEdge arbeitet als Industrie-PC direkt an der Maschine. Die Edge erfasst Messdaten, speichert sie auf dem Gerät und zeigt sie im Browser an — an jedem ihrer Netzwerkanschlüsse, ohne Verbindung ins Internet. Sie läuft unbeaufsichtigt: Zieht jemand ein Netzkabel oder fällt eine Gegenstelle aus, verbinden sich die Dienste selbstständig neu, sobald die Gegenstelle wieder erreichbar ist. Firmware-Updates installiert die Edge selbst und kehrt bei einem Fehler zum vorherigen Stand zurück.

1.1.1 Wie dieses Handbuch aufgebaut ist

Die Seitenliste links führt durch das ganze Handbuch, von oben nach unten:

- **Tutorial** — die erste Inbetriebnahme Schritt für Schritt. Wer ein neues Gerät auspackt, beginnt mit Erste Inbetriebnahme (Kap. 1.2).
- **Anleitungen** — einzelne Aufgaben im Betrieb: Firmware aktualisieren, Netzwerk und Firewall einstellen, Benutzer verwalten, Diagnose lesen.
- **Referenz** — Nachschlagelisten, etwa alle Diagnose-Codes (Kap. 3.1).
- **Konzepte** — Hintergrund: wie Updates ablaufen, wie die Edge angeschlossen wird, was sie für Sicherheit und Support tut.

Oben rechts wechseln Sie die Sprache; Sie bleiben dabei auf derselben Seite.

1.2 Erste Inbetriebnahme

Dieses Tutorial führt Sie vom ausgepackten Gerät bis zum ersten erfolgreichen Login durch alle nötigen Schritte. Sie benötigen dafür einen Laptop mit LAN-Anschluss oder einen Bildschirm und eine Tastatur an der openXEdge sowie etwa 10 Minuten Zeit.

1.2.1 Voraussetzungen

- openXEdge ist montiert und mit Strom versorgt
- Etikett oder Lieferschein des Geräts mit **Seriennummer** (z. B. SN00100) und **Initialpasswort** liegen bereit
- Ein Laptop mit LAN-Anschluss und Browser und ein LAN-Kabel — oder ein Bildschirm (HDMI) und eine USB-Tastatur, direkt an der Edge angeschlossen

1.2.2 Schritt 1: Zugang zur Edge herstellen

Vor der Anmeldung zeigt die Edge ihre IP-Adressen nirgends an, weder am Bildschirm noch im Browser. Für die erste Anmeldung nutzen Sie deshalb einen Anschluss mit fester Werksadresse oder



melden sich direkt am Gerät an. Welcher Anschluss welcher Port ist, zeigt Anschlüsse der Edge (Kap. 4.2).

1.2.2.1 Empfohlen: über den Service-Port

Port 3 (Eth3) hat ab Werk die feste Adresse 172.16.10.250/24 und ist für genau diesen Zweck da.

1. Verbinden Sie Ihren Laptop per LAN-Kabel direkt mit Port 3.
2. Geben Sie dem Laptop eine feste Adresse im selben Netz, z. B. 172.16.10.10/24, ohne Gateway.
3. Die Edge ist jetzt unter 172.16.10.250 erreichbar. Weiter mit Schritt 2.

Port 1 (Eth1, 172.16.9.112/24) gehört dem IO-Link-Master; schließen Sie den Laptop dort nicht an.

1.2.2.2 Direkt am Gerät: Bildschirm und Tastatur

Schließen Sie einen Bildschirm an einen HDMI-Anschluss und eine Tastatur an einen USB-Anschluss der Edge an. Nach dem Start zeigt der Bildschirm die Anmeldeseite; melden Sie sich dort wie in Schritt 2 beschrieben an.

Tastaturlayout: Im Auslieferungszustand tippt die Tastatur im Layout der Sprache, die an der Edge eingestellt ist — ab Werk Deutsch. Wählen Sie auf der Anmeldeseite über die Weltkugel eine andere Sprache, ändert sich nur die Anzeige, nicht das Tastaturlayout. Umstellen lässt sich das Layout erst nach der Anmeldung (siehe Sprache wählen (Kap. 2.5)). Bei einer Tastatur, die nicht deutsch beschriftet ist, liegen deshalb z. B. y, z und der Bindestrich des Initialpassworts auf anderen Tasten.

1.2.2.3 Über das Firmennetz

Port 2 (Eth2) bezieht seine Adresse per DHCP aus Ihrem Firmennetz. Welche Adresse er bekommen hat, weiß Ihr DHCP-Server bzw. Ihre IT-Abteilung; die Edge selbst zeigt sie erst nach der Anmeldung.

Nach der Anmeldung finden Sie die aktuellen Adressen aller Ports unter **Einstellungen** → **Netzwerk** — auch die, die Port 2 per DHCP bekommen hat.

1.2.3 Schritt 2: Anmelden mit dem Passwort vom Etikett

Öffnen Sie im Browser <http://<edge-ip>:5000/>, über den Service-Port also <http://172.16.10.250:5000/>. Am Bildschirm der Edge ist nichts zu öffnen. Ein Gerät mit Seriennummer braucht keine Aktivierung: Beim ersten Start übernimmt es Seriennummer, Kundenzuordnung und Initialpasswort von selbst, auch ohne Internetverbindung. Der Browser zeigt deshalb direkt die Anmeldeseite:

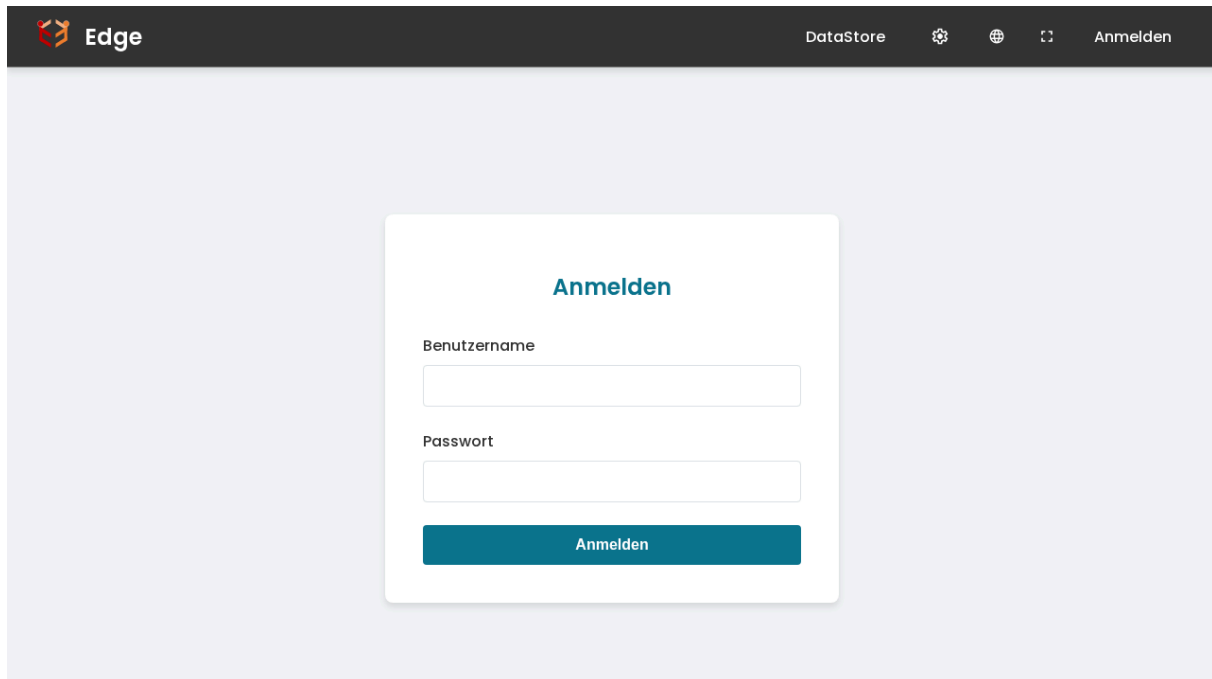


Abbildung 1: Login-Seite der Brinkhaus GmbH openXEdge

Melden Sie sich mit dem Benutzernamen `admin` und dem **Initialpasswort vom Etikett bzw. Lieferschein** an. Geben Sie es genau so ein, wie es dort steht, mit den Bindestrichen: drei Vierergruppen aus Kleinbuchstaben und Ziffern. Es enthält nur die Ziffern 2 bis 7 — was wie eine 1 aussieht, ist ein kleines **l**, was wie eine 0 aussieht, ein kleines **o**.

△ **Wichtig:** Das Initialpasswort lässt sich nicht aus der Seriennummer ausrechnen — es steht nur auf Etikett und Lieferschein. Bewahren Sie beides auf wie einen Schlüssel. Nach dem ersten Login mit dem Initialpasswort führt das Gerät Sie direkt zum Passwortwechsel; erst mit einem eigenen Passwort geht es weiter. Das Passwort vom Etikett wird dabei nicht wieder angenommen (siehe auch Passwort ändern (Kap. 2.4)).

Zeigt der Browser statt der Anmeldeseite einen Aktivierungs-Bildschirm, wurde Ihr Gerät ohne Seriennummer ausgeliefert. Aktivieren Sie es dann einmalig selbst, wie unter Geräte ohne Seriennummer: Aktivierung (Kap. 1.2.5) beschrieben, und kommen Sie danach zu Schritt 3 zurück.

1.2.4 Schritt 3: Die Hauptansicht

Nach der Anmeldung landen Sie auf der Startseite **Hauptfunktionen**:

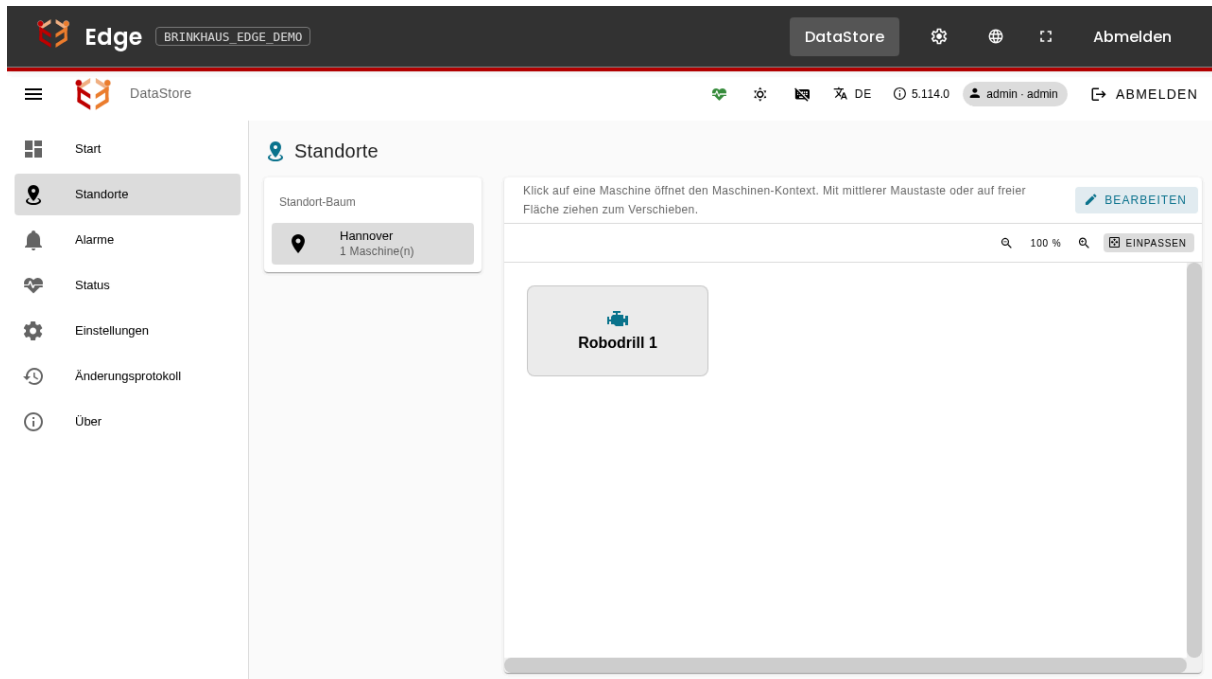


Abbildung 2: Startseite Hauptfunktionen mit den fünf Hauptanwendungs-Kacheln

Die fünf Kacheln entsprechen den fünf eingebetteten Anwendungen:

- **Grafana** — Dashboards und Diagramme der gesammelten Messdaten
- **IDEA4SBridge** — Übersicht und Konfiguration der angeschlossenen IDEA-4S-Sensorik
- **IO-Link-Master-Konfiguration** — Konfiguration des IFM-IO-Link-Masters
- **DataStore** — interne Datenbasis
- **AppStore** — installierbare Erweiterungen über FLECS

Über das Zahnrad-Symbol oben rechts erreichen Sie die Einstellungen.

1.2.5 Geräte ohne Seriennummer: Aktivierung

Geräte, die ohne Seriennummer ausgeliefert wurden und noch nie aktiviert waren, fragen beim ersten Aufruf von `http://<edge-ip>:5000/` einmalig nach einer Maschinen-ID. Bereits aktivierte Geräte sind davon nicht betroffen: Sie behalten ihre Maschinen-ID und ihr Passwort, auch nach einem Firmware-Update.



Abbildung 3: Geräteaktivierungs-Bildschirm der Brinkhaus GmbH openXEdge

Geben Sie die **Maschinen-ID** ein (z. B. WERK1_M01_GMN, eindeutig in Ihrer Flotte) und klicken Sie auf **Gerät aktivieren**. Diese ID identifiziert das Gerät später in der Flottenverwaltung; sie wird gleichzeitig zur Ableitung des Initialpassworts verwendet.

Nach der Aktivierung erscheint einmalig das Initialpasswort:

Abbildung 4: Aktivierung abgeschlossen — Anzeige des einmaligen Initialpassworts



△ **Wichtig:** Notieren Sie das Passwort jetzt. Nach dem Verlassen dieser Seite wird es nicht erneut angezeigt. Standard-Benutzername ist `admin`. Das Passwort lässt sich aus der Maschinen-ID durch berechtigtes Personal jederzeit erneut herleiten — ändern Sie es deshalb direkt nach dem ersten Login (siehe Passwort ändern (Kap. 2.4)).

Klicken Sie auf **Weiter zur Anmeldung**, melden Sie sich mit `admin` und dem soeben angezeigten Passwort an und lesen Sie bei Schritt 3 (Kap. 1.2.4) weiter.

1.2.6 Welche Seite die Edge zuerst zeigt

Ab Werk führt der erste Weg auf die Übersicht mit den Kacheln — außer Ihr Gerät wurde ab Werk auf eine bestimmte Anwendung eingestellt. Auf den GMN-Geräten ist das **Grafana**: Sowohl der Bildschirm am Gerät als auch der Browser öffnen zuerst die Dashboards, weil das im Betrieb der häufigste Grund ist, das Gerät anzusehen.

Sie können das jederzeit selbst ändern: **Einstellungen** → **Seiten** → **Startseite**. Zur Auswahl stehen die Übersicht und jede Anwendung, die dieses Gerät hat. Die Einstellung gilt für beide Wege gleichzeitig — den Bildschirm am Gerät und den Browser. Mit **Automatisch** verhält sich das Gerät wie vor dieser Einstellung: am Bildschirm die erste Hauptanwendung, im Browser die Übersicht.

Zur Übersicht kommen Sie immer zurück, indem Sie oben links auf das Logo oder den Gerätenamen daneben klicken. Und wer eine Anwendung nicht öffnen darf, landet weiterhin auf der Übersicht statt auf einer Absage.

1.2.7 Nächste Schritte

- Passwort ändern (Kap. 2.4)
- Netzwerk konfigurieren (Kap. 2.6)
- Firmware aktualisieren (Kap. 2.1)
- Zum Verständnis: Wie Updates funktionieren (Kap. 4.3)



2 Anleitungen

2.1 Firmware aktualisieren

Sie wollen eine neue Firmware-Version auf einer einzelnen openXEdge installieren.

2.1.1 Voraussetzungen

- Sie sind als **admin** (oder ein Benutzer mit Settings-Berechtigung) angemeldet
- Die Edge hat eine funktionierende Internet- oder mindestens VPN-Anbindung an `update.brinkhaus-gmbh.de`

2.1.2 Schritte

1. Klicken Sie oben rechts auf das Zahnrad-Symbol → Sie landen in den Einstellungen.
2. Wählen Sie links **Update**.
3. Sie sehen oben die aktuell installierte Version, darunter die Versionen aller laufenden Docker-Services und unten die Liste der verfügbaren Versionen vom Update-Server.

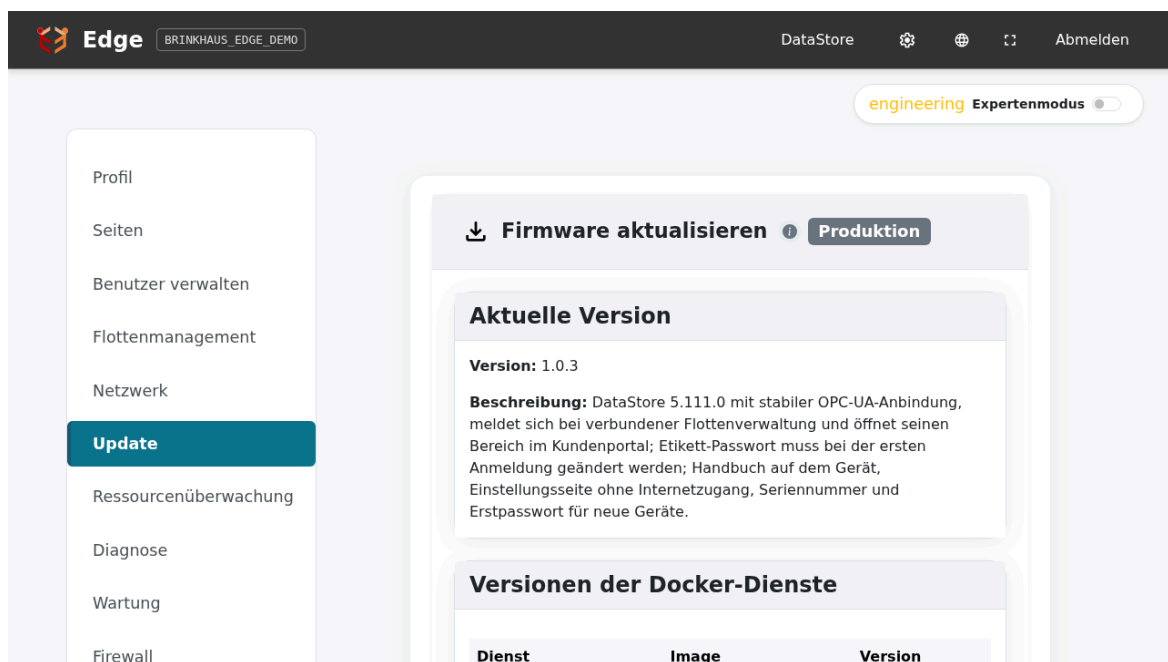


Abbildung 5: Einstellungen → Update — aktuelle Version, Service-Tabelle, verfügbare Versionen

4. Suchen Sie die Zielversion (i. d. R. die neueste). Die Liste zeigt standardmäßig nur Versionen **derselben Hauptversion** wie die installierte Firmware (eine 2.x-Edge sieht nur 2.x-Versionen). Über den Schalter „**Alle Versionen anzeigen**“ im Kopf der Versionsliste lassen sich auch andere Hauptversionen einblenden — Sprünge über eine Hauptversionsgrenze erfordern jedoch eine ausdrückliche Bridge-Version und sollten nur nach Rücksprache erfolgen.



5. Über den Button **Versionshinweise** lesen Sie die Änderungen aller Versionen des Streams; Notizen zu Versionen, die neuer sind als die installierte Firmware, sind abgesetzt dargestellt.
6. Klicken Sie **Upgrade** (oder bei niedrigeren Versionen **Downgrade**).
7. Die Edge lädt die signierte Compose-Datei vom Update-Server, prüft die Ed25519-Signatur, stellt die Dateien für den UpdateService bereit, und startet anschließend automatisch den Update-Prozess.
8. Während des Updates zeigt ein Fortschrittsbildschirm die aktuelle Phase an (Validierung, Signaturprüfung, Dienste stoppen, Images laden, ...). Die Bedienoberfläche ist dabei **kurzzeitig nicht erreichbar**. Nach erfolgreichem Health-Check (typisch 1–2 Minuten) sind Sie wieder eingeloggt; bei einem Fehler erfolgt automatisch ein Rollback auf die vorherige Version — auch das Ergebnis des Rollbacks (erfolgreich / fehlgeschlagen) wird auf dem Fortschrittsbildschirm angezeigt.

2.1.3 Ohne Internetverbindung (USB)

Steht keine Verbindung zum Update-Server zur Verfügung, kann eine Firmware-Version auch per USB-Stick installiert werden (Kap. 2.2) — mit derselben Signaturprüfung und demselben Rollback-Verhalten.

2.1.4 Aus der Ferne (FleetManager)

Firmware-Updates können auch zentral aus dem FleetManager ausgelöst werden (Befehl „Firmware-Version installieren“). Die Edge lädt die gewählte Version dann selbst signiert vom Update-Server und installiert sie über den normalen Update-Mechanismus inklusive Rollback-Schutz.

2.1.5 Was tun bei Problemen?

- **Update bleibt im „wird heruntergeladen“ hängen** → Internet-Verbindung prüfen, Edge bei Bedarf neu starten und Vorgang wiederholen.
- **Nach dem Update ist eine Anwendung dauerhaft auf „Rollback“ gesprungen** → in **Einstellungen** → **Diagnose** nachsehen, welcher Dienst die Ursache war; die einzelnen Codes sind unter Diagnose-Codes (Kap. 3.1) aufgeschlüsselt.
- **Verfügbare Versionen erscheinen nicht** → **Expertenmodus** oben rechts aktivieren und prüfen, ob im Feld **URL des Update-Servers** der richtige Update-Server eingetragen ist; üblich ist <https://update.brinkhaus-gmbh.de>.

2.1.6 Verwandte Themen

- Wie Updates funktionieren (Kap. 4.3) — Hintergrund zum 7-Phasen-Flow und der Rollback-Logik
- Diagnose-Codes (Kap. 3.1) — Bedeutung aller Codes, die in der Diagnose erscheinen



2.2 Firmware offline per USB installieren

Die openXEdge kann Firmware-Updates auch **ohne Internetverbindung** von einem USB-Stick installieren (verfügbar ab Firmware 2.10.0). Signaturprüfung, Fortschrittsanzeige und automatisches Rollback verhalten sich identisch zum Online-Update.

2.2.1 Was auf den Stick gehört

Im **Stammverzeichnis** des USB-Sticks müssen liegen:

Datei	Zweck
docker-compose.yml	Die Firmware-Definition der Zielversion
eine *.sig-Datei	Ed25519-Signatur der Compose-Datei (beliebiger Name mit Endung .sig)
eine *.pem-Datei	Öffentlicher Schlüssel für die Signaturprüfung (beliebiger Name mit Endung .pem)
description.json	optional — Versionsbeschreibung

Das Paket erhalten Sie von Brinkhaus bzw. aus dem Kundenportal.

2.2.2 Schritte

1. Melden Sie sich an der Edge an und öffnen Sie **Einstellungen** → **Update**.
2. Klappen Sie am Ende der Seite den Bereich „**Offline update**“ auf.
3. Stecken Sie den USB-Stick ein. Der Stick wird beim Scan **automatisch eingebunden** — manuelles Mounten ist nicht nötig. Erkannte Sticks mit gültigem Firmware-Paket erscheinen in der Liste; bei mehreren Paketen ist das mit der höchsten Version vorausgewählt.
4. Starten Sie die Installation. Die Edge prüft die Ed25519-Signatur **lokal**; nur bei gültiger Signatur wird das Paket für den UpdateService bereitgestellt.
5. Der weitere Ablauf entspricht dem Online-Update: Fortschrittsbildschirm mit Phasenanzeige, Health-Check, bei Fehlern automatisches Rollback auf die vorherige Version.

2.2.3 Was tun bei Problemen?

- **Stick wird nicht erkannt** → Stick abziehen, neu einstecken und den Offline-Update-Bereich erneut öffnen; ggf. einen anderen Stick (FAT32/exFAT) verwenden.
- **„Signatur ungültig“** → Das Paket wurde verändert oder gehört zu einem anderen Stream. Nicht installieren; Paket neu beziehen. Siehe Diagnose-Codes (Kap. 3.1) (Code 2008).

2.2.4 Verwandte Themen

- Firmware aktualisieren (Kap. 2.1) — der normale Online-Weg
- Wie Updates funktionieren (Kap. 4.3)



2.3 Von einem anderen Rechner zugreifen (HTTPS)

Direkt am Gerät (Kiosk-Bildschirm) läuft die Bedienoberfläche über `http://localhost:5000`. Von **anderen Rechnern im Netzwerk** erreichen Sie dieselbe Oberfläche zusätzlich verschlüsselt:

```
https://<edge-ip>:5443
```

Beide Zugänge zeigen dieselbe Anwendung mit denselben Benutzern und Rechten.

2.3.1 Warum HTTPS auf einem eigenen Port?

Einige eingebettete Anwendungen benötigen im Browser einen sogenannten *sicheren Kontext*. Der ist bei `http://localhost` auf dem Gerät selbst gegeben, bei einem Zugriff über eine LAN-IP jedoch nur mit HTTPS. Die Edge stellt deshalb **beide** Zugänge bereit (im Stream für GMN seit Firmware 2.1.1): HTTP auf Port 5000 (lokal/Kiosk) und HTTPS auf Port 5443 (Fernzugriff).

2.3.2 Das Zertifikat der Edge

Edges haben meist keinen Internetzugang; ein Zertifikat einer öffentlichen Zertifizierungsstelle kommt deshalb nicht in Frage. Die Edge bringt stattdessen ihre **eigene Zertifizierungsstelle** mit, die *Edge-CA*. Sie entsteht beim ersten Start, bleibt für die Lebensdauer des Geräts dieselbe und stellt das Zertifikat für Port 5443 aus. Dieses Zertifikat deckt alle privaten IP-Adressen der Edge ab; es läuft ein gutes Jahr und wird von der Edge selbst rechtzeitig erneuert, ebenso beim nächsten Start, wenn eine IP-Adresse hinzugekommen ist.

Solange Ihr Rechner der Edge-CA nicht vertraut, zeigt der Browser beim Aufruf eine Warnung („Verbindung ist nicht privat“). Sie haben drei Möglichkeiten:

1. **Warnung bestätigen** („Erweitert“ → „Weiter zu ...“) — genügt für einen gelegentlichen Zugriff.
2. **Der Edge-CA einmal vertrauen** — danach keine Warnung mehr, auch nicht nach einer Erneuerung oder einem IP-Wechsel. Siehe unten.
3. **Ein Zertifikat Ihrer Firmen-CA installieren** — wenn Ihre IT eine eigene Zertifizierungsstelle betreibt, der Ihre Rechner ohnehin vertrauen. Siehe Eigenes Zertifikat (Kap. 2.3.3).

2.3.2.1 Der Edge-CA vertrauen

Die Edge-CA kann **nur für private Adressen und lokale Namen bürgen** (10.x, 172.16–31.x, 192.168.x, Namen auf .local, .lan, .internal, .intranet, .intern, .corp, .home.arpa). Das ist im Zertifikat selbst festgeschrieben und wird vom Browser geprüft. Selbst wer an ihren Schlüssel käme, könnte damit keine Website im Internet vortäuschen.

1. Melden Sie sich als Administrator an und öffnen Sie **Einstellungen** → **HTTPS-Zertifikat**.
2. Notieren Sie den **Fingerabdruck (SHA-256)** und klicken Sie auf **Edge-CA herunterladen**. Sie erhalten die Datei `edge-ca.crt`.



3. Installieren Sie die Datei auf dem Rechner als vertrauenswürdige Stammzertifizierungsstelle:

- **Windows** (gilt für Edge und Chrome): Doppelklick auf `edge-ca.crt` → **Zertifikat installieren** → **Lokaler Computer** → **Alle Zertifikate in folgendem Speicher speichern** → **Vertrauenswürdige Stammzertifizierungsstellen**. Vor dem Abschluss zeigt Windows den Fingerabdruck an — vergleichen Sie ihn.
- **Viele Rechner auf einmal**: Ihre IT kann die Datei per Gruppenrichtlinie verteilen (*Computerkonfiguration* → *Richtlinien* → *Windows-Einstellungen* → *Sicherheitseinstellungen* → *Richtlinien für öffentliche Schlüssel* → *Vertrauenswürdige Stammzertifizierungsstellen*).
- **macOS**: Datei öffnen → Schlüsselbund **System** → im Zertifikat unter **Vertrauen** „SSL“ auf **Immer vertrauen** stellen.
- **Firefox** (eigene Zertifikatsverwaltung): **Einstellungen** → **Datenschutz & Sicherheit** → **Zertifikate anzeigen** → **Zertifizierungsstellen** → **Importieren** und „Dieser CA vertrauen, um Websites zu identifizieren“ ankreuzen.

4. Browser neu starten und `https://<edge-ip>:5443` aufrufen — ohne Warnung.

Jede Edge hat ihre eigene CA. Bei mehreren Edges vertrauen Sie jeder einzeln — oder Sie verwenden für alle ein Zertifikat Ihrer Firmen-CA.

2.3.2.2 Hostnamen

Rufen Sie die Edge statt über ihre IP über einen Namen auf (etwa `edge01.local` oder einen Eintrag im DNS Ihrer Firma), tragen Sie ihn unter **Einstellungen** → **HTTPS-Zertifikat** → **Hostnamen** ein.

Namen mit den oben genannten lokalen Endungen nimmt die Edge sofort in ihr Zertifikat auf. Für andere Namen, etwa `edge01.firma.de`, darf die Edge-CA nicht bürgen; sie landen nur in Zertifikatsanforderungen — für solche Namen brauchen Sie ein Zertifikat Ihrer Firmen-CA.

2.3.3 Eigenes Zertifikat Ihrer Firmen-CA

Betreibt Ihre IT eine eigene Zertifizierungsstelle (zum Beispiel Active Directory Certificate Services), können Sie ein Zertifikat von ihr verwenden. Die Edge kennt zwei Wege.

2.3.3.1 Weg 1: Zertifikatsanforderung (empfohlen)

Der private Schlüssel entsteht auf der Edge und verlässt sie nie.

1. **Einstellungen** → **HTTPS-Zertifikat** → **Eigenes Zertifikat**: Hostnamen eintragen (durch Kommas getrennt), bei Bedarf **IP-Adressen dieser Edge aufnehmen** ankreuzen und die Organisation angeben.
2. **Zertifikatsanforderung erstellen**, dann **Anforderung herunterladen** (`edge.csr`) oder **In die Zwischenablage kopieren**.
3. Ihre IT stellt daraus ein **Webserver-Zertifikat** aus. Bei einer Windows-CA zum Beispiel:

```
certreq -submit -attrib "CertificateTemplate:WebServer" edge.csr edge.cer
```



4. Auf derselben Seite die erhaltene Datei auswählen (.cer, .crt, .pem oder die Kette als .p7b) und **Prüfen und installieren** klicken. Die Edge ordnet das Zertifikat dem wartenden Schlüssel zu.

Solange eine Anforderung offen ist, zeigt die Seite sie an. **Anforderung verwerfen** löscht den wartenden Schlüssel; ein dafür ausgestelltes Zertifikat lässt sich danach nicht mehr installieren.

2.3.3.2 Weg 2: Zertifikat mit Schlüssel importieren

Hat Ihre IT Zertifikat und Schlüssel schon erzeugt, laden Sie beides hoch:

- **PKCS#12** (.pfx, .p12) — Passwort ins Feld daneben eintragen.
- **PEM** — Zertifikat, Zwischenzertifikate und privater Schlüssel, in einer oder mehreren Dateien; ein verschlüsselter Schlüssel braucht sein Passwort.

2.3.3.3 Was die Edge vor dem Aktivieren prüft

Ein Zertifikat wird nur aktiviert, wenn es funktionieren kann. **Abgelehnt** wird es, wenn

- der private Schlüssel fehlt oder nicht zum Zertifikat passt,
- es abgelaufen oder noch nicht gültig ist (dann auch Datum und Uhrzeit der Edge prüfen),
- es ein CA-Zertifikat ist, keinen Hostnamen nennt (*Subject Alternative Name*) oder nicht für Server bestimmt ist,
- der Schlüssel zu schwach ist (RSA unter 2048 Bit) oder es mit SHA-1 signiert ist,
- die mitgelieferte Kette nicht zusammenpasst.

Eine **Warnung** — das Zertifikat wird trotzdem installiert — erscheint, wenn es keine Adresse und keinen eingetragenen Hostnamen der Edge abdeckt, eine Zwischenzertifizierungsstelle zu fehlen scheint, es länger als 825 Tage gilt oder keinen Verwendungszweck nennt (Apple-Geräte lehnen die beiden letzten ab), oder wenn es in weniger als 30 Tagen abläuft.

Nach **Prüfen und installieren** gilt das Zertifikat ab der nächsten Verbindung, ein Neustart ist nicht nötig. Laden Sie die Seite neu.

2.3.3.4 Welcher Rechner welches Zertifikat bekommt

Die Edge entscheidet je Verbindung:

- Aufruf über einen **Namen**, den Ihr Zertifikat nennt (auch über einen Platzhalter wie *.firma.de) → Ihr Zertifikat.
- Aufruf über eine **IP-Adresse** → Ihr Zertifikat nur, wenn es **alle** IP-Adressen der Edge enthält; sonst das Edge-Zertifikat. Der Browser verrät bei einem Aufruf per IP nicht, welche Adresse er gewählt hat; ein Zertifikat mit nur einer davon würde auf allen anderen Anschlüssen eine Warnung erzeugen.
- alles andere → das Edge-Zertifikat.



Soll Ihr Zertifikat auch beim Aufruf per IP gelten, kreuzen Sie bei der Anforderung **IP-Adressen dieser Edge aufnehmen** an — oder rufen Sie die Edge über einen Namen auf, den das Zertifikat nennt.

2.3.3.5 Ablauf und Erneuerung

30 Tage vor Ablauf meldet die Diagnose den Code **1012**; bei angebundener Flottenverwaltung erscheint die Meldung auch dort. Erneuern Sie wie beim ersten Mal (neue Anforderung oder Import). Ein abgelaufenes Zertifikat liefert die Edge weiter aus: der Browser warnt, Sie kommen aber auf die Oberfläche, um ein neues zu installieren.

Lässt sich Ihr Zertifikat einmal nicht laden, verwendet die Edge automatisch wieder ihr eigenes und meldet **1013. Wieder das Edge-Zertifikat verwenden** entfernt Ihr Zertifikat dauerhaft. Dieselbe Meldung erscheint, wenn die Edge ihr eigenes Zertifikat nicht speichern oder erneuern konnte; dann arbeitet sie mit einem vorläufigen Zertifikat weiter und versucht es selbst erneut.

2.3.4 Unverschlüsselten Zugang schließen

Port 5000 (HTTP) bleibt ab Werk offen. Möchten Sie im Netzwerk nur verschlüsselte Zugriffe zulassen, schließen Sie ihn unter **Einstellungen** → **Firewall** — siehe Firewall konfigurieren (Kap. 2.7). Der Kiosk-Bildschirm greift lokal zu und ist davon nicht betroffen.

2.3.5 Mehrere Netzwerk-Anschlüsse

Eine openXEdge hat bis zu drei LAN-Ports mit eigenen IP-Adressen (typisch: Büronetz, Anlagen-Subnetz, Service-Port). Die Oberfläche — einschließlich aller eingebetteten Anwendungen — ist über **jede** dieser Adressen erreichbar; verwenden Sie einfach die IP des Ports, mit dem Ihr Rechner verbunden ist. Die Zuordnung der Ports beschreibt Anschlüsse und Verkabelung (Kap. 4.2).

2.3.6 Was tun bei Problemen?

- **Seite lädt nicht** → Sind Sie im richtigen Subnetz? Die IP-Adressen aller Ports zeigt **Einstellungen** → **Netzwerk** nach der Anmeldung, auch am Bildschirm der Edge.
- **Eingebettete Ansicht bleibt leer (nur bei HTTP über LAN-IP)** → Verwenden Sie den HTTPS-Zugang `https://<edge-ip>:5443`.
- **Warnung trotz installierter Edge-CA** → Browser ganz neu starten. Rufen Sie die Edge über eine öffentliche IP oder einen Namen ohne lokale Endung auf, kann die Edge-CA dafür nicht bürgen; die Seite **HTTPS-Zertifikat** nennt solche Adressen. Firefox verwaltet Zertifikate getrennt von Windows.
- **Warnung nach einem Firmware-Update von einer Version vor der Edge-CA** → Einmalig: Die Edge hat ihr altes selbstsigniertes Zertifikat durch eines der Edge-CA ersetzt. Vertrauen Sie der Edge-CA wie oben beschrieben.



2.4 Passwort ändern

Sie wollen Ihr eigenes Passwort ändern — typischerweise direkt nach der ersten Inbetriebnahme.

Wir empfehlen, das **Initialpasswort beim ersten Login zu ersetzen**. Es steht auf Etikett und Lieferschein (bei älteren Geräten: aus der Aktivierung); wer eines davon in die Hand bekommt, kann sich sonst anmelden. Geräte mit Seriennummer führen nach dem ersten Login mit dem Passwort vom Etikett direkt zum Wechsel; ältere Geräte erzwingen ihn nicht.

2.4.1 Schritte

1. Oben rechts auf das Zahnrad-Symbol klicken → Sie sind in den Einstellungen.
2. Links **Profil** wählen.
3. Im Formular **Profil ändern** ein neues Passwort eintragen, im zweiten Feld bestätigen. Unter dem Feld steht, was die Passwortrichtlinie verlangt, ab Werk mindestens 10 Zeichen und nicht den Benutzernamen.

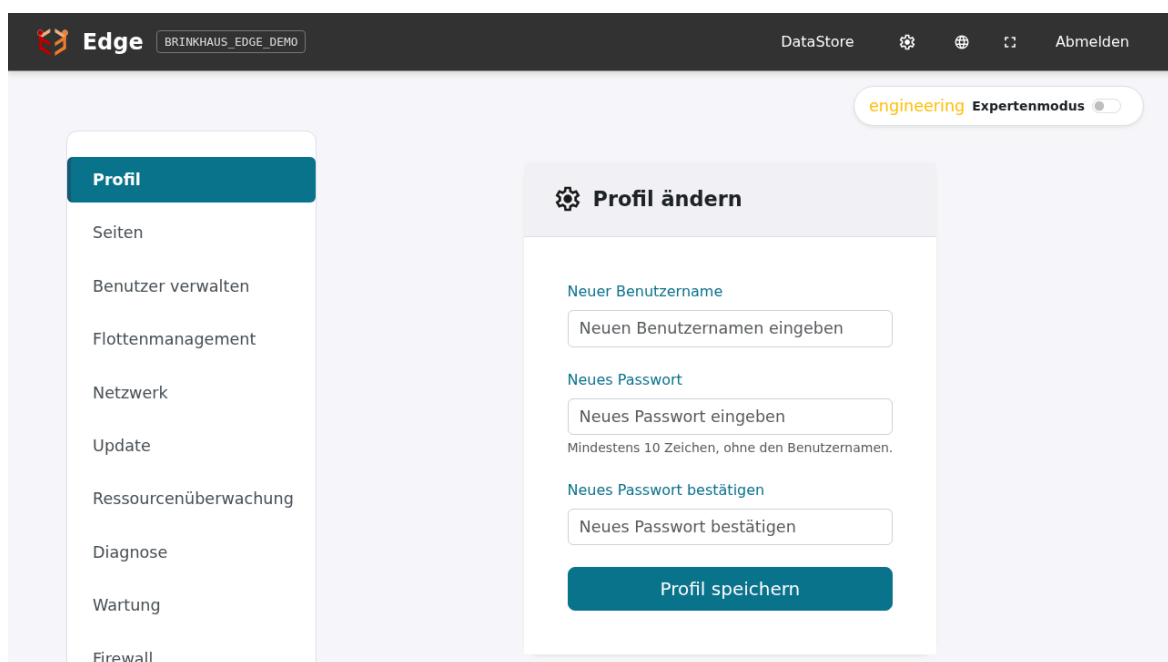


Abbildung 6: Einstellungen → Profil → Profil ändern

4. Optional: auch den Benutzernamen ändern.
5. **Profil speichern** klicken.

Beim nächsten Login verwenden Sie den (eventuell neuen) Benutzernamen und das neue Passwort.

2.4.2 Hinweise

- Erfüllt das neue Passwort die Richtlinie nicht, bleibt das alte gültig, und oben erscheint der Grund. Die Richtlinie legt ein Admin unter Benutzer verwalten (Kap. 2.8) fest.



- Sobald Sie ein eigenes Passwort gesetzt haben, gilt das Initialpasswort für Ihr Konto nicht mehr — weder das vom Etikett noch das aus der Maschinen-ID hergeleitete. Sie sind danach selbst dafür verantwortlich.
- **Was die Flottenverwaltung erfährt:** nur, *ob* das Initialpasswort geändert wurde — nie das Passwort selbst, weder das alte noch das neue. Als geändert gilt es erst, wenn **kein** Konto des Geräts mehr das Initialpasswort vom Etikett verwendet; ändert nur ein Bediener seines, `admin` aber nicht, bleibt es „unverändert“. Die Flotte erfährt die Änderung nicht sofort, spätestens nach dem nächsten Neustart des Geräts. Bei Geräten, die über die Maschinen-ID aktiviert wurden (auch mit nachträglich zugewiesener Seriennummer), kann die Edge das nicht feststellen und meldet es nicht.
- Verlieren Sie Ihr Passwort, kann ein Benutzer mit `network-configuration`- oder anderer Admin-Berechtigung in **Einstellungen** → **Benutzer verwalten** ein neues setzen.
- Geht der Zugriff komplett verloren, kann Brinkhaus-Personal das Initialpasswort erneut herleiten: bei Geräten mit Seriennummer aus der Seriennummer und einem Schlüssel, der nie auf dem Gerät liegt, bei älteren Geräten aus der Maschinen-ID. Das hilft nur, solange noch ein Konto das Initialpasswort verwendet.
- Ist auch das Initialpasswort schon geändert, setzt der Brinkhaus-Service über die Flottenverwaltung ein **Einmalpasswort** für Ihr Konto. Das Gerät muss dafür mit der Flottenverwaltung verbunden sein. Das Passwort reist verschlüsselt, nur Ihr Gerät kann es lesen. Wer sich damit anmeldet, wird wie beim Etikett-Passwort zuerst aufgefordert, ein eigenes zu wählen; das Einmalpasswort selbst wird dabei abgelehnt.
- **Die Maschinen-ID steht ab gmn-2.34.0 in der Kopfzeile**, rechts neben dem Anlagennamen — sie sagt Ihnen, auf welcher Anlage Sie gerade sind. Auf schmalen Bildschirmen wird sie ausgeblendet. Sie erscheint erst **nach** dem Anmelden, und das mit Absicht: Bei Geräten, die über die Maschinen-ID aktiviert wurden, wird aus ihr das Initialpasswort hergeleitet. Auf einer Anlage, deren Passwort seit der Inbetriebnahme nicht geändert wurde, stünde sie auf der Anmeldeseite jedem offen, der die Anlage im Netz erreicht. Bei Geräten, die mit Seriennummer ausgeliefert wurden, steht dort die Seriennummer in Kleinbuchstaben (z. B. `sn00100`); aus ihr allein lässt sich das Passwort nicht herleiten. Geräte, die über die Maschinen-ID aktiviert wurden, zeigen weiter ihre Maschinen-ID, auch wenn sie später eine Seriennummer bekommen haben.

2.5 Sprache der Bedienoberfläche wählen

Sie wollen die Bedienoberfläche der Edge in einer anderen Sprache sehen, oder festlegen, in welcher Sprache sie an der Anlage erscheint.

Die Bedienoberfläche spricht 33 Sprachen, dieselben wie der DataStore. Ab Werk ist sie **deutsch**. Ältere Firmware-Stände zeigen sie nur auf Englisch.

Zwei Einstellungen wirken zusammen:



- **Die Sprache Ihres Browsers** wählen Sie in der Kopfzeile. Sie gilt nur für den Browser, in dem Sie sie gewählt haben, und bleibt dort erhalten, auch über das Abmelden hinaus.
- **Die Vorgabe der Anlage** legt ein Administrator in den Einstellungen fest. Sie gilt für jeden Browser, der keine eigene Sprache gewählt hat, auch für den Bildschirm am Gerät.

2.5.1 Sprache für Ihren Browser wählen

1. In der Kopfzeile oben rechts auf das **Weltkugel-Symbol** klicken. Das geht auch schon auf der Anmeldeseite.
2. In der Liste die Sprache wählen. Jede Sprache steht dort in ihrer eigenen Schreibweise, etwa *English*, *Français* oder *Polski*.

Die Seite lädt neu und erscheint in der gewählten Sprache.

Ist das Fenster schmal und die Kopfzeile zu einem Menü (☰) zusammengeklappt, steht die Weltkugel in diesem Menü, zusammen mit dem Kürzel der aktuellen Sprache, etwa **DE**.

Andere Browser und andere Rechner sind davon nicht betroffen: Eine Kollegin im Büro kann die Oberfläche auf Englisch sehen, während der Bildschirm an der Anlage deutsch bleibt.

2.5.2 Vorgabe der Anlage festlegen

Nur als Administrator.

1. Oben rechts auf das Zahnrad-Symbol klicken → Sie sind in den **Einstellungen**.
2. Links **Seiten** wählen.
3. In der Karte **Sprache** die gewünschte Sprache auswählen.
4. Unten auf **Seiten speichern** klicken.

Die Vorgabe gilt ab dem nächsten Laden einer Seite für jeden Browser, der in der Kopfzeile keine eigene Sprache gewählt hat: für den Bildschirm am Gerät ebenso wie für Bildschirme, die mit einem Kiosk-Link (Kap. 2.8) angemeldet sind. Diese zeigen keine Weltkugel. Ein Browser, in dem schon eine eigene Sprache gewählt wurde, behält sie, auch der Bildschirm am Gerät, wenn dort jemand die Weltkugel benutzt hat.

2.5.3 Tastaturlayout am Gerät

Eine Tastatur, die direkt an der Edge steckt, tippt im Layout der Vorgabesprache der Anlage: bei Deutsch im deutschen Layout, bei Englisch im US-Layout. Sprachen mit nicht-lateinischer Schrift, etwa Russisch oder Griechisch, bekommen das US-Layout, damit sich das Passwort eintippen lässt. Die Sprache Ihres Browsers in der Kopfzeile ändert das Layout nicht.

Passt die Tastatur nicht zur Sprache, etwa eine spanische Tastatur bei englischer Oberfläche, legen Sie das Layout fest. Nur als Administrator:



1. **Einstellungen** → links **Seiten**.
2. In der Karte **Sprache** unter **Tastaturlayout** das Layout wählen. Ab Werk steht dort **Automatisch (folgt der Sprache)**.
3. Unten auf **Seiten speichern** klicken.

Die Änderung erreicht die Tastatur innerhalb einer Minute. Der Bildschirm am Gerät wird dabei einige Sekunden dunkel und zeigt danach wieder die Bedienoberfläche. Lässt sich das Layout nicht setzen, meldet die Edge die Diagnose 6006 und versucht es jede Minute erneut.

2.5.4 Was der Sprache folgt und was nicht

Mit der Sprache wechseln alle Seiten der Bedienoberfläche: Anmeldung, Kopfzeile, Übersicht, Einstellungen und die Hinweise auf dem Bildschirm. Hebräisch wird von rechts nach links dargestellt.

Der DataStore folgt der Sprache der Bedienoberfläche ab DataStore 5.115.0; mit einer älteren Version wählen Sie die Sprache im DataStore selbst. Wählen Sie im DataStore eine andere Sprache, gilt sie bis zum nächsten Mal, an dem Sie den DataStore aus der Bedienoberfläche öffnen. Dann zeigt er wieder die Sprache der Bedienoberfläche.

Grafana folgt ebenfalls, mit seinen Menüs, Knöpfen und dem Zeitwähler, in den Sprachen, die Grafana kennt: Deutsch, Englisch, Französisch, Spanisch, Portugiesisch, Italienisch, Niederländisch, Schwedisch, Polnisch, Tschechisch, Ungarisch, Russisch, Türkisch, Japanisch und Chinesisch. Bei allen anderen Sprachen zeigt Grafana Englisch. Die Inhalte der Dashboards, etwa Panel-Titel und Achsen, bleiben, wie sie angelegt sind. Grafana merkt sich die Sprache für Ihr Benutzerkonto: Öffnen Sie Grafana mit demselben Konto in einem Browser mit anderer Sprache, wechselt es dorthin.

Ihre eigene Sprache behalten:

- der **AppStore** und die darüber installierten Anwendungen,
- die **IDEA-4S-Bridge**,
- die Konfigurationsseite des **IO-Link-Masters**, die das Gerät selbst liefert.

Diagnosemeldungen und Protokolle übersetzt die Bedienoberfläche nicht: Die Meldungen der Edge selbst bleiben in jeder Sprache englisch.

2.5.5 Hinweise

- Fehlt in einer Sprache noch ein Text, erscheint er in einer verwandten Sprache oder auf Englisch, etwa Norwegisch zuerst auf Dänisch. Deutsch ist vollständig.
- Ihr Browser merkt sich die Wahl für die Adresse, unter der Sie die Edge geöffnet haben. Erreichen Sie dieselbe Edge über eine andere ihrer IP-Adressen, etwa über den Service-Port, wählen Sie die Sprache dort noch einmal. Löschen Sie die Browserdaten, gilt wieder die Vorgabe der Anlage.



2.6 Netzwerk konfigurieren

Sie passen die Netzwerkschnittstellen einer openXEdge an Ihre Werks-Topologie an. Eine Edge hat bis zu drei LAN-Ports, die Sie unabhängig statisch oder per DHCP konfigurieren können.

2.6.1 Voraussetzungen

- Sie sind als Benutzer mit `network-configuration`-Berechtigung angemeldet.
- Sie haben die geplanten IP-Adressen, Gateway und gegebenenfalls DNS-Server bereit.
- **Wichtig:** nach dem Speichern startet die Edge neu — planen Sie ein kurzes Wartungsfenster ein.

2.6.2 Schritte

1. Oben rechts Zahnrad → Einstellungen → links **Netzwerk**.
2. Sie sehen den **Netplan-Konfigurator**: pro Schnittstelle (z. B. `enp1s0`, `enp2s0`) ein Block mit Methode (DHCP / Statisch), Adresse (CIDR), Gateway und Nameservern.

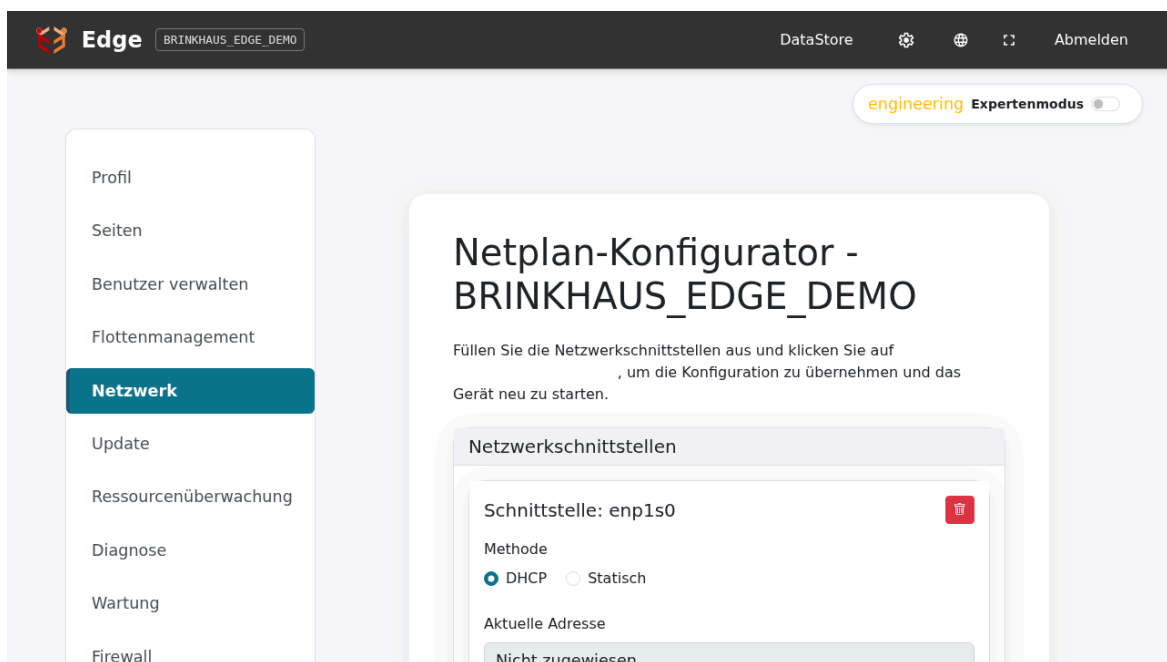


Abbildung 7: Einstellungen → Netzwerk → Netplan-Konfigurator

3. Felder anpassen:
 - **DHCP:** keine weiteren Felder nötig.
 - **Statisch:** Adresse als CIDR (z. B. `192.168.10.20/24`); optional Gateway und Nameserver.
4. **Speichern & neu starten** klicken — die Edge übernimmt die neue Konfiguration und startet automatisch neu.
5. Nach dem Neustart erreichen Sie die Bedienoberfläche unter der neuen IP-Adresse.



2.6.3 Hintergrund

Die openXEdge unterstützt bis zu drei gleichzeitige Netzwerkschnittstellen, da sie typischerweise gleichzeitig im Werksnetz, in einem Maschinen- oder Sensor-Subnetz und ggf. einem dritten Netz hängt. Die MainUI ist von **jeder** dieser Adressen aus erreichbar; das HTTPS-Zertifikat enthält alle drei IPs als SAN. Eine eigene Erklärungs-Seite zur Multi-IP-Architektur folgt — bis dahin: für Spezialfälle den Brinkhaus-Service kontaktieren.

2.6.4 Was tun, wenn ich mich ausgesperrt habe?

- Über einen anderen LAN-Port verbinden, falls noch erreichbar.
- Falls alle Adressen unbekannt: Bildschirm und Tastatur an die Edge anschließen, dort anmelden und unter **Einstellungen** → **Netzwerk** nachsehen. Vor der Anmeldung zeigt die Edge keine Adressen an.
- In Notfällen kann ein Brinkhaus-Servicetechniker per VPN oder vor Ort Netplan zurücksetzen.

2.7 Firewall konfigurieren

Die openXEdge nimmt aus dem Netz nur Verbindungen auf Ports an, die auf ihrer Freigabeliste stehen. Alles andere wird verworfen — auch Dienste, die auf dem Gerät zwar laufen, aber von außen nichts zu suchen haben: die eigene Oberfläche des AppStores, die von AppStore-Anwendungen geöffneten Ports, die IDEA-4S-Bridge, das IO-Link-Relais und der Druckdienst, der mit dem Kiosk-Browser mitkommt. Auf dem Gerät selbst und zwischen seinen Diensten ändert die Firewall nichts.

Sie brauchen diese Seite, wenn Sie einen der Systemports aus dem Netz sperren wollen, oder wenn eines Ihrer Systeme einen Port erreichen soll, der nicht ohnehin offen ist — etwa die Weboberfläche einer Anwendung aus dem AppStore oder das IO-Link-Relais für einen DataStore außerhalb der Edge.

2.7.1 Systemports

Das sind die Ports, die die Edge absichtlich anbietet. Im Auslieferungszustand sind sie alle offen; die Seite **Einstellungen** → **Firewall** zeigt sie unter *Systemports* mit ihrem Zweck.

Port	Wofür	Sperren
22/tcp	Wartungszugang für den Brinkhaus-Service	nur mit Bestätigung
5000/tcp	Bedienoberfläche, unverschlüsselt	ohne Rückfrage
5443/tcp	Bedienoberfläche, verschlüsselt	nur mit Bestätigung
1883/tcp	MQTT-Broker	nur mit Bestätigung

2.7.2 Einen Systemport sperren

1. Melden Sie sich als Administrator an und öffnen Sie **Einstellungen** → **Firewall**.



2. Schalten Sie in der Zeile des Ports *Offen fürs Netz* aus. Bei Ports, deren Verlust etwas kostet, nennt die Edge die Folge und fragt nach — ohne 22 kommt der Brinkhaus-Service nicht mehr aus der Ferne auf das Gerät, ohne 5443 gibt es keine verschlüsselte Bedienung aus dem Netz, ohne 1883 keine MQTT-Abnehmer.
3. Klicken Sie **Speichern und anwenden**.

Einer der beiden Bedienports 5000 und 5443 bleibt immer offen; die Edge lässt nicht beide zugleich sperren, sonst wäre sie nur noch am eigenen Bildschirm bedienbar. Öffnen geht jederzeit ohne Rückfrage.

Wenn Sie sich ausgesperrt haben: Über die Flottenverwaltung gibt es die Aktion *Firewall: Systemports wieder öffnen*. Sie öffnet alle gesperrten Systemports wieder und lässt Ihre eigenen Regeln unangetastet; sprechen Sie Ihren Ansprechpartner an.

2.7.3 Einen Port oder Port-Bereich freigeben

1. Melden Sie sich als Administrator an und öffnen Sie **Einstellungen** → **Firewall**.
2. Klicken Sie unter *Von Ihnen geöffnet* auf **Regel hinzufügen**.
3. Wählen Sie das Protokoll (TCP oder UDP) und tragen Sie den ersten und den letzten Port des Bereichs ein. Für einen einzelnen Port lassen Sie *Bis Port* leer.
4. Optional: Beschränken Sie die Freigabe mit *Quellnetz* auf ein Netz in CIDR-Schreibweise, zum Beispiel 192.168.0.0/24. Leer bedeutet: von überall.
5. Ein Kommentar hilft, die Regel später wiederzuerkennen.
6. Klicken Sie **Speichern und anwenden**. Die Regel gilt sofort und bleibt nach einem Neustart erhalten.

Eine Regel entfernen Sie mit dem ☐ in ihrer Zeile und **Speichern und anwenden**.

Beispiel: Ein DataStore auf einem anderen Rechner mit der Adresse 192.168.0.50 soll den IO-Link-Master über das Relais der Edge lesen. Dafür braucht es zwei Dinge: die Adresse in der Freigabeliste des Relais (siehe IO-Link-Master konfigurieren (Kap. 2.11)) und hier eine Regel TCP, Port 8082, Quellnetz 192.168.0.50/32.

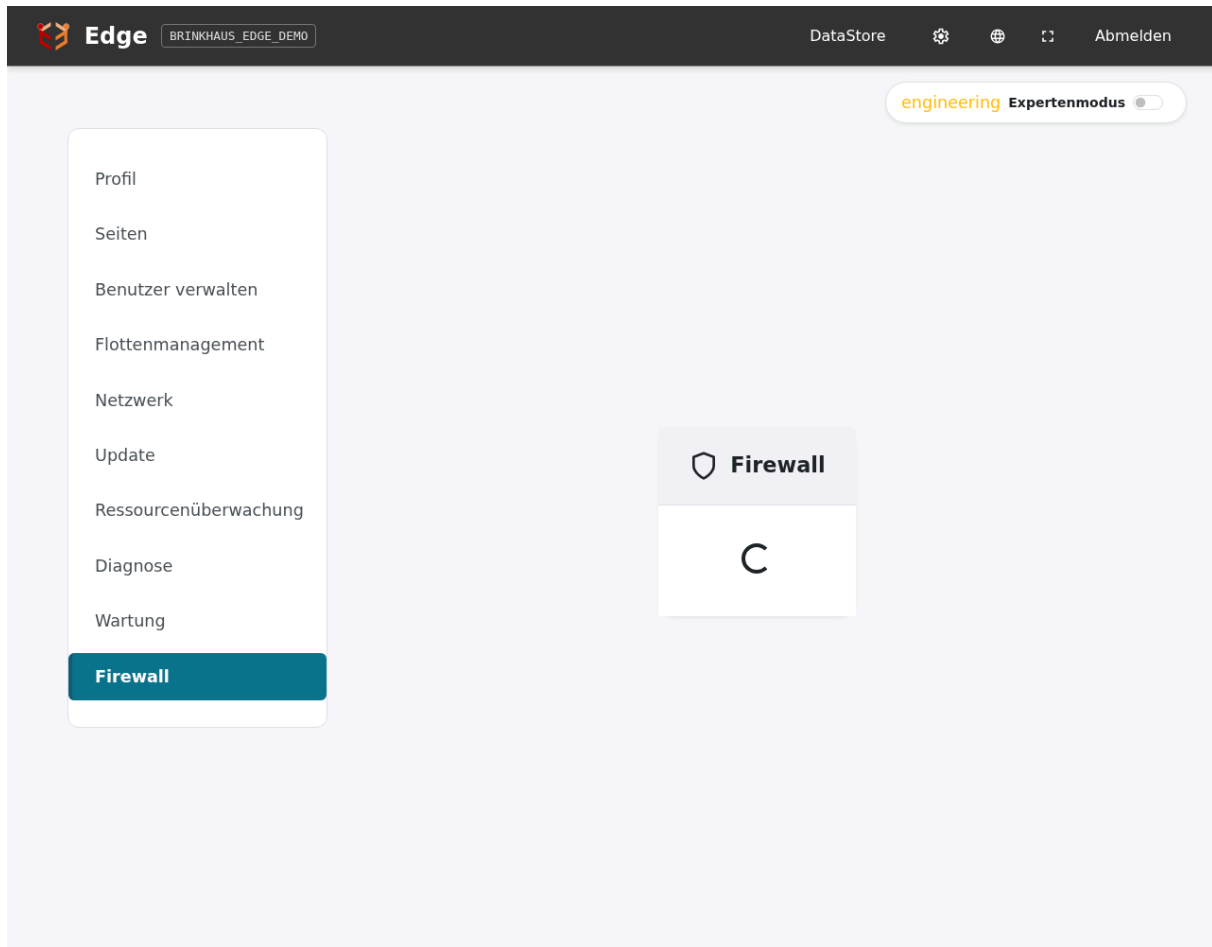


Abbildung 8: Einstellungen → Firewall

2.7.4 Wenn eine Regel abgelehnt wird

Die Edge prüft jede Regel, bevor sie etwas ändert: Ports müssen zwischen 1 und 65535 liegen, der erste Port darf nicht größer sein als der letzte, das Quellnetz muss eine gültige CIDR-Angabe sein. Bei einem Fehler bleibt die bisherige Freigabeliste unverändert; die Meldung nennt die betroffene Regel.

2.7.5 Firewall abschalten

Mit dem Schalter **Firewall aktiv** und **Speichern und anwenden** schalten Sie die Firewall ganz ab. Die Edge antwortet dann wieder auf allen Ports, so wie vor Einführung der Firewall. Das ist für die Fehlersuche gedacht, nicht für den Dauerbetrieb.

2.7.6 Gut zu wissen

- Der Zustand der Firewall (aktiv, zuletzt angewendet, letzter Fehler) steht oben rechts auf der Seite. Schlägt das Anwenden fehl, meldet die Edge das auch in der Diagnose (Code 6005) und versucht es beim nächsten Start erneut.



- Anwendungen aus dem AppStore, die Sie direkt über ihren Port erreichen wollen, brauchen ab dieser Firmware eine Regel. Über die Bedienoberfläche der Edge bleiben sie ohne Regel erreichbar, und untereinander sowie mit der IDEA-4S-Bridge sprechen sie weiterhin ohne Freigabe.
- Zeigt die Seite an, dass der Wartungsdienst zu alt ist, fehlt der Edge noch die Firmware mit der Firewall — dann ist auch noch nichts gesperrt.

2.8 Benutzer verwalten

Sie wollen weitere Personen Zugriff auf die Bedienoberfläche der openXEdge geben — typischerweise einen Wartungs- und einen Werker-Account zusätzlich zum bestehenden `admin`.

2.8.1 Voraussetzungen

- Sie sind als Benutzer mit `settings`-Berechtigung angemeldet (in der Werksauslieferung der `admin`).
- Sie haben sich überlegt, **welche Bereiche** der oder die neue Benutzer*in sehen darf.

2.8.2 Bestehende Konten ansehen

1. Oben rechts auf das Zahnrad → Einstellungen → links **Benutzer verwalten**.
2. Sie sehen die Tabelle aller Konten mit den Berechtigungs-Spalten:

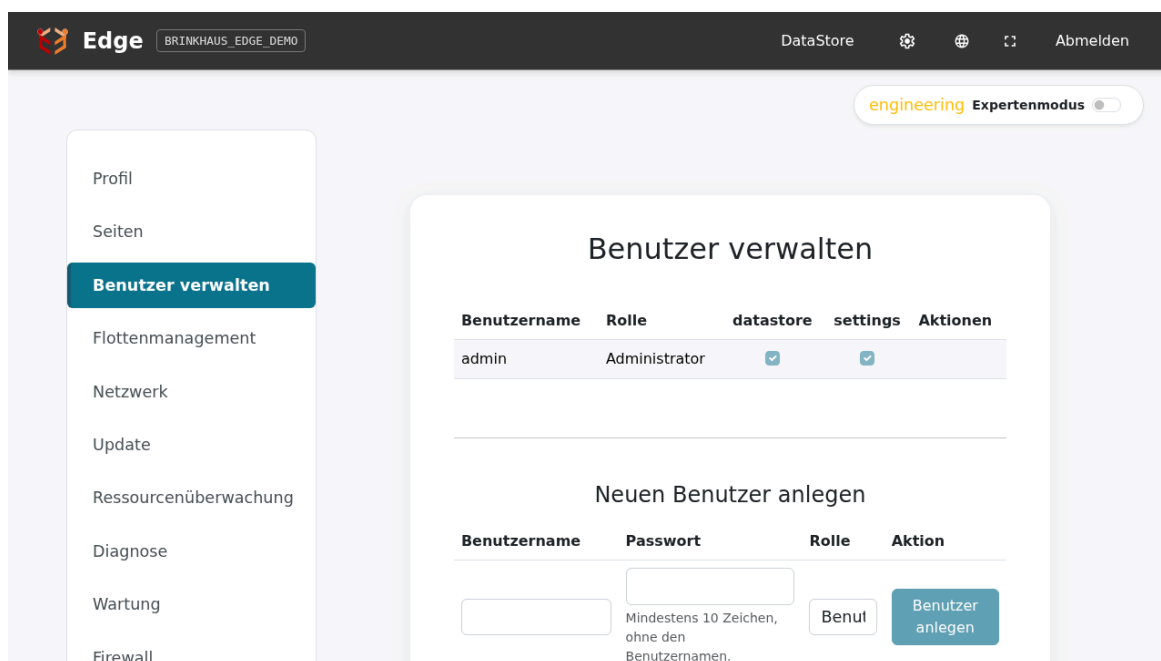


Abbildung 9: Einstellungen → Benutzer verwalten mit Berechtigungs-Tabelle und Anlage-Formular

Spalte	Bedeutung
network-configuration	Darf Netplan ändern (in Einstellungen → Netzwerk) — die Edge wird beim Speichern neu gestartet.



Spalte	Bedeutung
grafana	Sieht die Grafana-Kachel auf der Startseite und erreicht das Dashboard.
idea4s-bridge	Darf den IDEA-4S-Sensor und seine Parameter sehen und bearbeiten.
datastore	Sieht die DataStore-Kachel und kommt in die interne Datenbank-Oberfläche.
settings	Darf den kompletten Einstellungs-Bereich sehen, inkl. anderer Benutzerkonten und Update.

admin hat per Definition alle Berechtigungen.

2.8.3 Neuen Benutzer anlegen

Im Block **Neuen Benutzer anlegen** unten:

1. **Benutzername** eintragen (frei wählbar, eindeutig).
2. **Passwort** setzen. Unter dem Feld steht, was die Passwortrichtlinie verlangt, ab Werk mindestens 10 Zeichen und nicht den Benutzernamen.
3. **Rolle** wählen — **Benutzer** für eingeschränkte Konten, **Administrator** für volle Rechte.
4. Auf **Benutzer anlegen** klicken.

Der neue Eintrag erscheint sofort in der Tabelle. Pflegen Sie die Berechtigungs-Häkchen so, dass die Person genau die Bereiche sieht, die sie braucht — z. B. ein Werker-Konto erhält nur `grafana` und `idea4s-bridge`, nicht `settings`.

Erfüllt das Passwort die Richtlinie nicht, wird kein Konto angelegt, und oben erscheint der Grund.

2.8.4 Passwortrichtlinie festlegen

Im Block **Passwortregeln** legen Sie fest, was ein neues Passwort erfüllen muss:

Feld	Bedeutung	ab Werk
Mindestlänge	Mindestlänge, 8 bis 64 Zeichen	10
Geforderte Zeichenarten	Wie viele der vier Zeichenarten vorkommen müssen: Kleinbuchstaben, Großbuchstaben, Ziffern, sonstige Zeichen	beliebig
Darf den Benutzernamen nicht enthalten	Das Passwort darf den Benutzernamen nicht enthalten	an

Mit **Passwortregeln speichern** gilt die Richtlinie sofort. Sie gilt für neue Konten und für jedes Passwort, das ab jetzt geändert wird. Bestehende Passwörter bleiben gültig, niemand wird ausgesperrt. Das Passwort aus der Erstinbetriebnahme und ein Zurücksetzen durch Brinkhaus-Personal sind ausgenommen.

Länge schützt besser als vorgeschriebene Zeichenarten. Ein langer Satz aus mehreren Wörtern ist sicherer und leichter zu merken als ein kurzes Passwort mit Sonderzeichen.



2.8.5 Berechtigungen ändern

Häkchen direkt in der Tabelle setzen oder entfernen — die Änderung wird sofort wirksam beim nächsten Seitenaufruf des betroffenen Kontos.

2.8.6 Konto löschen

Spalte **Aktionen** → Lösch-Schaltfläche. **Hinweis:** Das letzte verbleibende Admin-Konto kann nicht gelöscht werden — sonst ist der Zugriff verloren.

2.8.7 Kiosk-Link: eine App ohne Anmeldung auf einem Hallenmonitor zeigen

Ein fest montierter Bildschirm soll eine App wie den DataStore dauerhaft anzeigen, ohne dass jemand nach jedem Neustart ein Passwort eingibt. Dafür gibt es unterhalb von **Neuen Benutzer anlegen** den Block **Kiosk-Links**.

1. Bei der gewünschten App auf **Link erzeugen** klicken.
2. Den angezeigten Link kopieren (**Kopieren**) und als Startadresse des Monitor-Browsers eintragen.

Wer den Link öffnet, wird automatisch als **Betrachter** angemeldet und sieht **nur diese eine App** — ohne Navigationsleiste, ohne Einstellungen, ohne Möglichkeit, etwas zu ändern oder zu quittieren. Der DataStore öffnet dabei direkt in seiner Kiosk-Anzeige; in seinem Protokoll erscheinen solche Sitzungen als Benutzer `kiosk`.

Schaltfläche	Wirkung
Link erzeugen / Neuer Link	Erzeugt einen (neuen) Link. Ein alter Link wird dabei ungültig; Bildschirme, die ihn noch verwenden, landen beim nächsten Laden auf der Anmeldeseite.
Widerrufen	Zieht den Link zurück.
Kopieren	Kopiert den Link in die Zwischenablage.

Hinweise

- Der Link ist ein Zugang: Wer ihn kennt, sieht die Daten dieser App. Geben Sie ihn nur an Personen weiter, die sie auch sehen dürfen, und erzeugen Sie ihn neu, wenn er in falsche Hände geraten sein könnte.
- Der angezeigte Link trägt die Adresse, über die Sie gerade angemeldet sind. Jede andere Adresse der Edge funktioniert genauso; nur der Teil ab `/share/` zählt.
- Angeboten werden nur Apps, die selbst eine reine Lese-Rolle kennen (DataStore, Grafana). IDEA-4S-Bridge und IO-Link-Master lassen sich nicht freigeben.

2.8.8 Wie lange eine Anmeldung gilt

Eine Anmeldung gilt **72 Stunden nach dem letzten Aufruf** und verlängert sich mit jeder Nutzung. Eine Anzeige, die ständig läuft, etwa ein Hallenmonitor, bleibt also angemeldet. Ein vergessener Browser-Tab meldet sich drei Tage nach der letzten Nutzung selbst ab. Die Anmeldung übersteht auch



einen Neustart des Browsers. Kiosk-Links laufen nicht ab. Sie gelten, bis Sie sie zurückziehen oder neu erzeugen.

2.8.9 Nach mehreren falschen Passwörtern

Nach **fünf falschen Passwörtern innerhalb von fünf Minuten** nimmt die openXEdge von dieser Netzwerkadresse, meist also von diesem Rechner, **eine Minute lang keine Anmeldung** an, auch nicht mit dem richtigen Passwort. Die Anmeldeseite zeigt dann „Zu viele Fehlversuche“ und die Wartezeit. Warten Sie diese Zeit ab und melden Sie sich dann normal an. Folgen innerhalb von fünf Minuten nach der Wartezeit wieder fünf falsche Passwörter, verdoppelt sie sich jedes Mal, bis höchstens 15 Minuten. Eine erfolgreiche Anmeldung setzt die Zählung zurück.

Gesperrt wird nur die Netzwerkadresse, von der die Fehlversuche kamen, nie das Konto. Rechner, die die openXEdge über dieselbe Fernwartungsverbindung oder denselben Router erreichen, teilen sich eine Sperre. Am Bildschirm der openXEdge oder von einem Rechner mit eigener Adresse aus können Sie sich sofort anmelden. Ein Neustart der openXEdge hebt die Wartezeit ebenfalls auf.

2.8.10 Wenn Sie sich aussperren

- Andere Person mit `settings`-Berechtigung kann das Passwort in der Manage-Users-Tabelle zurücksetzen.
- Geht das nicht, kann Brinkhaus-Personal das Initialpasswort neu herleiten (bei Geräten mit Seriennummer steht es auch auf Etikett und Lieferschein) — siehe Erste Inbetriebnahme (Kap. 1.2). Es gilt aber nur noch für Konten, deren Passwort nie geändert wurde.

2.9 Diagnose lesen

Sie haben einen Hinweis auf ein Problem (keine neuen Messdaten, Update klappt nicht, ...) und wollen wissen, **welcher Dienst** der Edge das Problem auslöst.

2.9.1 Schritte

1. Oben rechts Zahnrad → Einstellungen → links **Diagnose**.
2. Sie sehen eine Liste aller Edge-Dienste Ihres Geräts (etwa `main-ui`, `datastore`, `postgres`, `update-service` und — je nach Ausstattung — `grafana`, `idea4sbridge`, `iolink-proxy`, `mosquitto`, `usb-service`, `flecs`) — jeder mit einem Status-Punkt und einem **N messages**-Klappfeld:

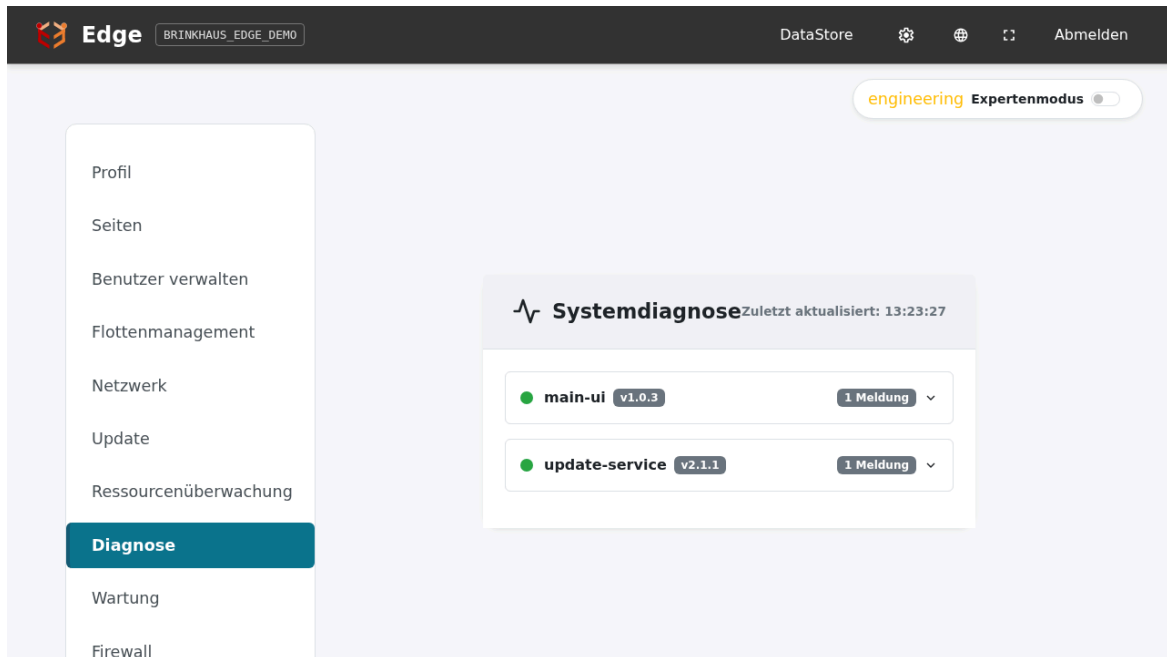


Abbildung 10: Einstellungen → Diagnose mit grünen Status-Punkten

3. Status lesen:

- ● grün → keine offenen Meldungen, Dienst hält seine Selbstdiagnose für gesund.
- ● gelb → mindestens eine Warnung. Dienst läuft weiter, aber etwas ist auffällig.
- □ rot → mindestens ein Fehler. Dienst kann eingeschränkt oder ausgefallen sein.

4. Bei nicht-grünem Punkt das Klappfeld **N messages** öffnen — die einzelnen Meldungen erscheinen mit ihrem **Code** und einem Erklärtext.
5. Code in der Tabelle Diagnose-Codes (Kap. 3.1) nachschlagen — dort steht, was die Meldung bedeutet und welche Maßnahme passt.

2.9.2 Häufige Muster

- **Alle grün, aber Grafana zeigt keine Daten:** häufig ein Datenfluss-Problem unterhalb der Schwelle für Diagnose-Meldungen. IO-Link-Master prüfen (siehe IO-Link-Master konfigurieren (Kap. 2.11)), MQTT-Subscriptions prüfen.
- **update-service rot kurz nach einem Update:** das Update wurde zurückgerollt — der vorherige Stand läuft wieder; siehe Diagnose-Codes 2xxx (Kap. 3.1).
- **datastore meldet Code 7002 (FleetManager nicht erreichbar):** ein Hinweis, kein Fehler — der DataStore arbeitet normal weiter. Typisch für ein Gerät ohne Internetzugang oder direkt nach der Erstinstallation, bevor das Gerät in der Flotte bekannt ist — siehe Fleet-Anbindung (Kap. 4.6).



2.9.3 Wenn Sie nicht weiterkommen

Brinkhaus-Personal kann die Diagnose der Edge zentral einsehen, sobald sie an den FleetManager angebunden ist (siehe Fleet-Anbindung (Kap. 4.6)). Schicken Sie der Hotline die Seriennummer (bei älteren Geräten die Maschinen-ID) und die Beschreibung — die Codes liest die Hotline parallel mit.

2.10 IDEA-4S-Gerät konfigurieren

Sie wollen den IDEA-4S-Sensor an Port 1 des IO-Link-Masters einsehen oder pflegen — ohne IFM-Spezialsoftware, direkt aus der openXEdge-Bedienoberfläche.

2.10.1 Voraussetzungen

- Sie sind als Benutzer mit `idea4s-bridge`-Berechtigung angemeldet.
- Der IDEA-4S ist physisch verkabelt (siehe Anschlüsse der Edge (Kap. 4.2)) und wird in der oberen Geräte-Liste angezeigt.

2.10.2 Schritte

1. Oben rechts Zahnrad → Einstellungen → links **IDEA-4S-Geräte**.
2. Sie sehen pro angeschlossenes Gerät einen Untereintrag (z. B. **IDEA-4S 0**). Wählen Sie den passenden.
3. Die Werteliste lädt alle Parameter vom Sensor (Anzeige „Werte werden geladen: x/y“, bei größeren Geräten mit dem gerade gelesenen Abschnitt davor). Das dauert je nach Gerät etwa eine halbe bis eine Minute — länger, wenn gleichzeitig etwas anderes mit dem Sensor spricht. Direkt darunter wechseln Sie zwischen fünf Reitern:

Status	Name	Value	Type
Green	VendorName Read-only	GMN Paul Müller Industrie GmbH & Co. KG	StringT
Green	VendorText Read-only	www.gmn.de	StringT
Green	ProductName Read-only	IDEA-4S Advanced	StringT
Green	ProductID Read-only	1211488	StringT
Green	ProductText Read-only	Integrated Data Evaluation and Acquisition for Spindles	StringT
Red	SerialNumber Read-only		StringT
Green	Unique Resource Token Of The Product Read-only	416726; 416726_GMN2825	StringT
Green	IDTA Nameplate		
Green	Nameplate Semantic ID Read-only	[IRI] https://admin-shell.io/zvei/nameplate/2/0/Nameplate	StringT

Abbildung 11: Einstellungen → IDEA-4S-Geräte → IDEA-4S 0 → Identifikation



Reiter	Inhalt	Bearbeitbar?
Identifikation	Hersteller, Produktname, Seriennummer, IDTA-Nameplate-Felder.	Bis auf ein Feld nur lesen. Application Specific Tag ist der frei vergebbare Geräte name und ab gmn-2.30.0 beschreibbar (32 Zeichen, ab gmn-2.33.0 nur als Administrator); die übrigen Felder stammen aus dem Werks-Datensatz des Sensors und ändert nur der Elektromontage-Platz.
Parameter	Mess-, Schwellen- und Konfigurationswerte des Sensors — der Hauptbereich für Anpassungen.	Ja , je nach Feld — ab gmn-2.33.0 nur als Administrator.
Diagnose	Lebenszeit, Fehlerzähler, Temperaturfenster, technische Eigenschaften.	Lesen.
Sonstiges	Reserviert für künftige IODD-Erweiterungen.	Bei aktueller Firmware leer.
Werkseinstellungen	Der Werks-Datensatz des Sensors — der Stand, auf den er bei „Werkseinstellungen wiederherstellen“ zurückfällt. Er spiegelt fast jeden Betriebsparameter unter demselben Namen; bis gmn-2.27.2 waren diese Felder über die anderen Reiter verstreut und sahen dort wie Dubletten aus.	Ab gmn-2.33.0 für Administratoren , siehe unten. Bis dahin für niemanden.

Welcher Wert in welchem Reiter steht, bestimmt der Sensor, nicht die Edge: Seine Gerätebeschreibung legt die drei Bereiche *Identifikation*, *Parameter* und *Diagnose* selbst fest, und ab gmn-2.32.0 folgt die Anzeige dieser Angabe. Vorher hat die Edge sie aus den Feldnamen erschlossen — auf der Prüfanlage standen dadurch 347 von 920 Zeilen im falschen Reiter, und zusammengehörige Bereiche wie *Temperature Bearing 1* waren über alle drei verteilt. **Wenn Sie Werte an anderer Stelle finden als gewohnt, ist das diese Umstellung.** Die Gliederung folgt damit derselben Quelle wie das Auswertewerkzeug ifm moneo, das GMN als Referenz beige stellt hat: der Gerätebeschreibung selbst.

2.10.2.1 Die Spalten

Spalte	Bedeutung
Status	Ampel: gelesen, geändert (noch nicht geschrieben), oder nicht gelesen.
Name	Bezeichnung aus der Gerätebeschreibung; die Einrückung zeigt die Gliederung.
Wert	Der Wert im Sensor. Bearbeitbare Felder sind Eingabefelder, mit ↓ zum Neulesen und ↑ zum Schreiben. Befehle stehen als Schaltflächen dort (siehe unten).



Spalte	Bedeutung
Bereich	Zulässiger Bereich in derselben Einheit wie der Wert, etwa 0,00 - 19,60 mm/s. Bei Textfeldern die Anzahl Zeichen. Ab gmn-2.32.0.
Beschreibung	Erläuterung aus der Gerätebeschreibung. Ab gmn-2.32.0.

Auf schmalen Bildschirmen wird **Beschreibung** ausgeblendet und steht dann im Tooltip der Zeile, zusammen mit dem Standardwert aus der Gerätebeschreibung, Pfad, Bezeichner und Adresse. **Bis gmn-2.32.0** hatte die Tabelle zwei weitere Spalten, *Default* und *Type*; der Standardwert ist jetzt nur noch im Tooltip zu finden.

2.10.2.2 Befehle sind Schaltflächen

Ab gmn-2.33.0, sichtbar für Administratoren. Manche Zeilen tragen kein Eingabefeld, sondern eine Reihe von Schaltflächen — etwa *Store Factory Settings*, *Service Reset*, *Reset Error Memory* im Reiter **Werkseinstellungen** oder *Application Reset*, *Restore Factory Settings* und *Back-to-Box* im Reiter **Diagnose**. Das sind keine Werte, sondern Befehle: Ein Klick löst die genannte Aktion im Sensor aus, ohne Rückfrage. Was eine Schaltfläche bewirkt, steht in ihrem Tooltip. Welche Zeilen so dargestellt werden, legt die Gerätebeschreibung fest.

Back-to-Box unterbindet die Kommunikation des Sensors bis zum nächsten Einschalten der Anlage. Danach ist der Sensor erst wieder erreichbar, wenn er stromlos war — an der Anlage, nicht aus der Ferne.

Ob der Befehl angekommen ist, sehen Sie an der Zeile (ab gmn-2.34.0): Die Ampel wird grün, wenn das Gerät den Befehl angenommen hat, und rot, wenn es ihn abgelehnt hat. Unter den Schaltflächen steht kurz, was war — etwa „*Vom Gerät abgelehnt (Code 531)*“; der ganze Satz mit dem Hinweis, woran es liegt, erscheint, wenn Sie mit der Maus über diese Zeile Text oder über die Ampel fahren. Der Hinweis oben rechts verschwindet nach wenigen Sekunden, die Angabe an der Zeile bleibt. Häufigster Grund für Code 531: Das Werkspasswort ist nicht oder falsch gesetzt.

2.10.2.3 Bedienerrolle

Über dem Reiter lässt sich die IO-Link-Bedienerrolle wählen — *Observer*, *Maintenance* oder *Specialist*, soweit die Gerätebeschreibung sie kennt. Jede Rolle öffnet einen anderen Umfang an Feldern; *Observer* zeigt am wenigsten. Vorausgewählt ist *Maintenance*: der Umfang, den diese Seite immer gezeigt hat. Wer nichts umstellt, sieht also weiterhin dieselbe Liste.

Das Auswahlfeld gibt es ab gmn-2.39.0. Vorher war es nicht zu sehen — die Oberfläche fragte die verfügbaren Rollen an einer Adresse ab, die es nicht gab, und blendete das Feld daraufhin aus. Die Angabe „ab gmn-2.31.0 wirkt die Auswahl“ betraf die Weitergabe der Rolle an das Gerät, nicht das Auswahlfeld.

Ebenfalls ab gmn-2.39.0 gehören die angezeigten Werte zur ausgewählten Rolle. Jede Rolle nummeriert ihre Zeilen für sich, und gelesen wurde bis dahin immer in der Nummerierung von



Maintenance. Unter *Observer* hätte deshalb rund die Hälfte der Zeilen den Wert eines anderen Parameters getragen — ohne Fehlermeldung, weil so ein Wert genauso aussieht wie der richtige.

2.10.3 Wenn der Ladevorgang fertig ist

Am Ende steht eine Zeile mit dem Ergebnis, etwa „**Alle 760 Werte gelesen. 13 davon sind leer – das Gerät hat geantwortet und dort keinen Wert.**“ oder, wenn wirklich etwas fehlt, „**x von y Werten gelesen – z ließen sich nicht lesen.**“ Wie groß y ist, hängt vom Sensor ab; die Prüfanlage führt 760 Zeilen.

Drei Zustände sind zu unterscheiden, und die Oberfläche zeigt sie ab gmn-2.31.0 auch getrennt an:

Anzeige	Bedeutung
Wert im Feld, grüne Ampel	Gelesen.
Leeres Feld , grüne Ampel	Gelesen — der Sensor hält an dieser Stelle nichts . Das betrifft Felder, die bei der Inbetriebnahme nie ausgefüllt wurden: Herstellername, Herkunftsland, Firmenname, Einbauort, Maschinenummer, Ein- und Ausbaudatum. Keine Störung.
nicht gelesen , rote Ampel	Nicht gelesen. Der Sensor hat auf diese Stelle nicht geantwortet.

Bis gmn-2.30.0 stand in der zweiten Zeile ebenfalls **not read** mit roter Ampel, und die Ergebniszeile zählte diese Felder als Verlust — auf einem typischen Gerät waren das 13 von 760. Wer daraufhin nach einem Fehler suchte, suchte etwas, das es nicht gab.

Bleiben Felder rot, drücken Sie „**Fehlende Werte erneut lesen**“: gelesen wird dann nur noch das Fehlende. Bleiben dieselben Felder rot, liefert dieses Gerät sie nicht.

2.10.4 Welche Felder darf ich ändern?

Ab gmn-2.33.0 ändert Werte nur, wer als Administrator angemeldet ist — die ganze Ansicht, nicht nur einzelne Reiter. Wer das nicht ist, sieht über der Liste einen entsprechenden Hinweis, alle Felder nur lesend und keine Befehls-Schaltflächen. Der Grund sind die Befehle: *Back-to-Box* etwa nimmt den Sensor bis zum nächsten Einschalten der Anlage aus dem Verkehr, und der Sensor fragt vorher nichts.

Auch als Administrator sind nicht alle Felder aktiv. Neben dem Namen steht, was der Sensor über das Feld sagt:

Hinweis	Bedeutung
Nur lesbar	Der Sensor gibt dieses Feld nicht zum Schreiben frei — eine Eigenschaft des Sensors, nicht der Edge.
Nur schreibbar	Das Feld nimmt einen Wert an, gibt ihn aber nicht zurück. Es bleibt daher immer leer, und seine Ampel ist grau.

Bearbeitbare Felder erkennen Sie an aktivem Eingabefeld und einem Speichern-/Schreib-Pfeil rechts.



2.10.4.1 Den Werks-Datensatz ändern

Ab gmn-2.33.0, nur für Administratoren. Der Reiter **Werkseinstellungen** zeigt den Stand, auf den der Sensor bei „Werkseinstellungen wiederherstellen“ zurückfällt. Bis gmn-2.32.0 war er gesperrt.

Werte dieses Reiters nimmt der Sensor unmittelbar an — ein Passwort verlangt er dafür nicht. Am Prüfgerät nachgemessen (ADVANCED 1.0.1.5): Das Schreiben eines Werks-Wertes wird sofort bestätigt.

Die Befehle dieses Reiters verlangt er dagegen freigeschaltet. *Store Factory Settings*, *Service Reset* und *Reset Error Memory* weist er ab, solange sein Werkspasswort nicht gesetzt ist — die Meldung nennt dann den Gerätecode 531. Das Passwort tragen Sie im Feld **FactoryPassword** desselben Reiters ein und schreiben es mit ↑; danach führt er die Befehle aus. Es erhalten Sie vom Brinkhaus-Service; es steht bewusst nicht in dieser Anleitung.

Was hier steht, ist der Rückfallstand des Sensors. Eine Änderung überlebt jedes „Werkseinstellungen wiederherstellen“ und jedes Restore — sie ist durch eine Sicherung **nicht** rückgängig zu machen, weil ein Restore diesen Bereich bewusst unangetastet lässt.

- Wenn Sie nicht sicher sind, ob eine Änderung sicher ist, ziehen Sie **vor** der Änderung ein Backup (siehe unten) — Sie können den Stand jederzeit zurückspielen.

2.10.5 Backup und Restore

Oben rechts auf der IDEA-4S-Seite finden Sie zwei Schaltflächen:

- **Sicherung** — liest alle Parameter noch einmal vom Sensor und lädt sie als JSON-Datei herunter. Datei-Name z. B. `idea4s_device_0_backup.json`. Das dauert rund eine Minute; Sie können es starten, während die Werteliste oben noch lädt — beide sprechen dasselbe Gerät an und brauchen dann länger.
- **Wiederherstellen** (nur für Administratoren) — schreibt eine zuvor heruntergeladene JSON-Datei wieder auf das Gerät. Geschrieben werden die Bedieneinstellungen; der Werks-Datensatz bleibt unangetastet. Die Werte überstehen einen Stromausfall des Sensors: Er speichert Geschriebenes von sich aus dauerhaft, ein zusätzlicher Sicherungsschritt ist nicht nötig. Der Werks-Datensatz des Sensors bleibt dabei unberührt — ein späteres „Werkseinstellungen wiederherstellen“ führt weiterhin auf den Auslieferungszustand zurück (bis gmn-2.27.1 war das anders, siehe Versionshinweise zu 2.27.2).

Der Werks-Datensatz bleibt bei Backup und Restore außen vor — daran ändert auch gmn-2.33.0 nichts. Er lässt sich nur einzeln von Hand ändern (siehe oben) und deshalb auch nur einzeln von Hand zurücksetzen.

Ein Backup ist entweder vollständig, oder es entsteht keine Datei. Konnte auch nach Wiederholung ein Parameter nicht gelesen werden, meldet die Oberfläche das mit Zahlen und lädt



nichts herunter — versuchen Sie es dann erneut. Die Erfolgsmeldung nennt, was in der Datei steht, z. B. „700 Werte gelesen, 62 vom Gerät nicht geliefert“: die zweite Zahl sind Parameter, die dieses Gerät grundsätzlich nicht liefert. Sie sind in der Datei namentlich aufgeführt, so dass sich zwei Backups desselben Sensors vergleichen lassen.

△ Restore überschreibt **alle** in der Backup-Datei enthaltenen Felder mit deren damaligen Werten. Nehmen Sie die Datei daher immer von **demselben** Sensortyp und derselben Firmware.

△ Backup-Dateien aus Firmware vor gmn-2.26.0 können Lücken enthalten, ohne dass das damals sichtbar war. Der Restore lehnt sie ab und nennt die Zahl der fehlenden Parameter. Sie können den Rest trotzdem einspielen — die Rückfrage sagt genau, wie viele Parameter dabei ihren jetzigen Wert behalten. Besser ist ein frisches Backup.

2.10.6 Eine neue IODD einspielen

Die gesamte Parameterliste — welche Felder es gibt, wie sie heißen, welche Einheit und welche Grenzen sie haben — stammt aus der **IODD**, der Gerätebeschreibungsdatei des Sensors. Die Edge bringt die IODDs mit, die zum Zeitpunkt ihrer Auslieferung bekannt waren. Ein Sensor mit einem neueren Firmware-Stand ist dort nicht beschrieben: Er erscheint dann gar nicht in der Geräteliste, und im DataStore fehlen seine Messwerte.

Ab gmn-2.31.0 spielen Sie die passende IODD selbst ein, ohne Firmware-Update:

1. Zahnrad → Einstellungen → **IDEA-4S-Geräte** → das betroffene Gerät.
2. Oben rechts **IODD hochladen**.
3. Wählen Sie die Datei. Beides geht: die einzelne ...-IODD1.1.xml oder das **komplette ZIP-Paket von GMN** — daraus werden nur die Gerätebeschreibungen übernommen, Bilder und Firmware-Dateien nicht.
4. Bestätigen Sie die Rückfrage. Die Datei geht an die IDEA-4S-Bridge **und** an den DataStore; anschließend startet die Bridge neu und die Parameterliste lädt erneut.

Über **Hochgeladene IODDs** sehen Sie, was eingespielt ist, und können es wieder entfernen — dann gilt wieder die mitgelieferte Beschreibung.

△ Starten Sie keinen Upload, während ein Backup läuft: der Neustart der Bridge bricht es ab.

Eine eingespielte IODD **verdrängt** die mitgelieferte für dasselbe Gerät und denselben Firmware-Stand. Eine falsche Datei macht die Parameterliste damit unbrauchbar — sie ist über **Entfernen** aber jederzeit wieder weg.

Steht nach dem Einspielen alles im Reiter **Parameter** und sind *Identifikation* und *Diagnose* leer, nennt die eingespielte Datei die drei Bereiche nicht (RoLeMenuSet). Alle Beschreibungen von GMN tun das; eine Datei anderer Herkunft muss es nicht. Die Werte sind vollständig da und in der richtigen Reihenfolge, nur nicht auf die Reiter verteilt.



Nur für Administratoren.

2.10.7 Die Startseite: welche Sensoren angezeigt werden

Unter **IDEA4SBridge** zeigt die Edge je Sensor eine Karte mit dem aktuellen Wert, dem beobachteten Bereich, den Alarm- und Fehlergrenzen und den Überschreitungszählern. **Welche Karten es gibt, bestimmt die Gerätebeschreibung (IODD) des Sensors:** Jeder Kanal, für den sie Statistiken oder Grenzen führt, bekommt eine. Beim IDEA-4S ADVANCED kommen so Verlagerung und Verlagerungstemperatur dazu, beim ADVANCED ENC die Encoder-Kanäle (Luftspalt, vRMS, aPeak, Encoder-Temperatur, -Schwingung und -Drehzahl).

Über die Schaltfläche **Sensors** oben in der Leiste wählen Sie aus, welche Karten erscheinen, und speichern mit **Save**. Die Auswahl gilt **für diese Edge**: Kiosk-Bildschirm und alle Büro-Browser zeigen dieselben Karten. Solange nichts gewählt ist, erscheinen alle Karten außer Kanälen, die im Sensor ausgeschaltet sind. Wie viele Karten ausgeblendet sind, steht unter dem Kartenraster und auf der Schaltfläche.

2.10.8 Wenn ein Feld nicht erscheint

Die Aufteilung in **Identifikation / Parameter / Diagnose** wird automatisch aus der IODD-Beschreibung des Sensors abgeleitet. Erscheint ein Feld nicht oder im falschen Reiter, passt die mitgelieferte IODD nicht zum Firmware-Stand des Sensors — spielen Sie die zum Gerät gehörende IODD ein (siehe oben). Hilft das nicht, Brinkhaus-Service kontaktieren mit Gerätetyp und FW-Stand (steht im Reiter Identifikation).

2.11 IO-Link-Master konfigurieren

Sie wollen einstellen, **welche** Sensorwerte der IO-Link-Master aktiv per MQTT publiziert (oder bestehende Subscriptions löschen). Die openXEdge bindet dafür die Konfigurations-Oberfläche des IFM-Geräts direkt ein — ohne Kabel umzustecken oder ein zweites Tool zu öffnen.

2.11.1 Was wird hier eingebunden?

Wenn Sie auf der Startseite die Kachel **IO-Link-Master-Konfiguration** anklicken, lädt die openXEdge intern die Adresse `/web/subscribe` der **ifm IoT Core**-Firmware Ihres IO-Link-Masters (Beispielgerät AL1304, FW 2.6.x). Das ist die Standard-**Notification**-Seite des IFM-Geräts:

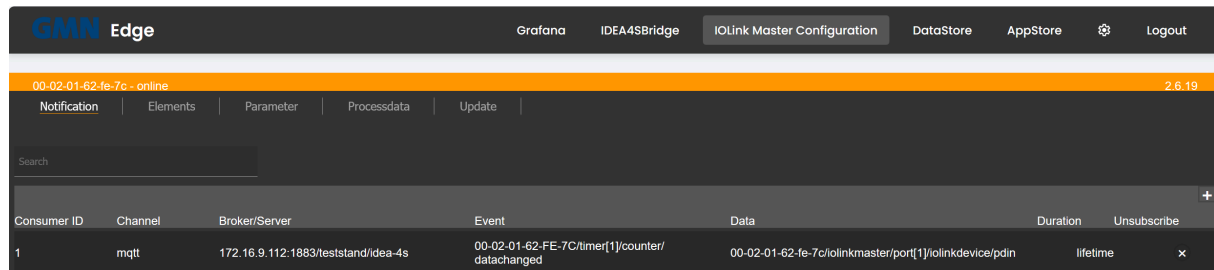


Abbildung 12: IFM IoT Core — Notification-Seite mit MQTT-Subscription

Die Reiter darüber (Notification, Elements, Parameter, Processdata, Update) sind originale IFM-IoT-Core-Reiter — die openXEdge zeigt sie 1:1, sie wirken direkt auf das IO-Link-Gerät.

2.11.2 MQTT-Subscription anlegen

Auf der **Notification**-Seite mit dem + rechts oben eine neue Zeile anlegen, dann pro Subscription:

Feld	Bedeutung
Channel	Transport — typisch <code>mqtt</code> .
Broker/Server	Adresse + Port + Topic-Präfix des MQTT-Brokers. Auf der openXEdge selbst läuft Mosquitto auf Port 1883 ohne Login. Beispiel: <code>172.16.9.112:1883/teststand/idea-4s</code> .
Event	Welches Ereignis am Master oder Gerät der Auslöser ist — z. B. <code>00-02-01-62-FE-7C/timer[1]/counter/datachanged</code> für jeden Tick eines internen Timers.
Data	Welche Datenpunkte mitgesendet werden — z. B. <code>00-02-01-62-fe-7c/iolinkmaster/port[1]/iolinkdevice/pdin</code> für die Process-Data-In des Sensors an Port 1.
Duration	<code>lifetime</code> (bleibt bis zum Löschen aktiv) oder eine Zeitbegrenzung.

Die Konfiguration wird **im IFM-Gerät** gespeichert — nicht in der openXEdge. Das Gerät behält die Subscriptions auch nach einem openXEdge-Neustart bei. Sie sind Teil der „Ports im Gerät“ und überleben Power-Off.

2.11.3 Subscription löschen

Spalte **Unsubscribe** → das **x** klicken. Die Zeile verschwindet sofort und das IFM-Gerät hört auf zu publizieren.

2.11.4 Ein System außerhalb der Anlage den Master mitlesen lassen

Ein DataStore, der nicht auf dieser Anlage läuft, braucht zweierlei, um den Sensor als Maschine zu zeigen: die Live-Werte vom MQTT-Verteiler der Anlage und den Master selbst über HTTP-JSON-RPC. Der zweite Weg ist ab Werk zu — die Anlage reicht den Master auf Port **8082** durch, lässt dort aber nur ihre eigene Bedienoberfläche und die Adressen durch, die Sie eintragen.

Eingetragen wird auf der Anlage, im Einstellungsordner, als `/home/gmn-service/docker/data/web-ui/settings/iolink_master.json`:



```
{
  "host": "172.16.9.110",
  "port": 80,
  "allow_from": ["172.16.0.229"]
}
```

host/port sind die Adresse des Masters (können entfallen, wenn er auf der Werkseinstellung 172.16.9.110:80 steht); allow_from nimmt einzelne Adressen oder ganze Bereiche in CIDR-Schreibweise. Danach das Relais neu starten: `sudo docker restart docker-iolink-proxy-1`. Die Datei übersteht Aktualisierungen.

Der Mitleser wird anschließend auf <Adresse der Anlage>:8082 gerichtet statt auf die Adresse des Masters.

Der Mitleser braucht auch die IODD. Die Anlage führt nachgelieferte IODD-Dateien für ihre eigene Erfassung mit; ein DataStore anderswo bekommt davon nichts. Ohne die zur Geräteerkennung passende IODD entschlüsselt er **keinen einzigen** Messwert, obwohl die Daten sichtbar fließen — bei einem IDEA-4S Basic ist das der Regelfall, weil dem DataStore keine Basic-Revision beiliegt. Dieselbe IODD gehört dort ebenfalls eingespielt. Alles, was nicht auf der Liste steht, wird mit 403 abgewiesen und als Diagnose-Code **3004** gemeldet, der die abgewiesene Adresse nennt — ein fehlender Eintrag sieht damit nicht wie ein totes Kabel aus.

Nur ein Betrachter gleichzeitig. Der IO-Link-Master beantwortet immer nur einen; ein Mitleser von außen teilt ihn sich mit dieser Konfigurationsseite, der Sicherung und dem DataStore der Anlage.

Ein Versuch von der Anlage selbst aus führt über diesen Port nicht zum Ziel — eine Anfrage aus der Kommandozeile der Anlage erreicht das Relais mit einer internen Adresse und wird abgewiesen, wie jeder andere, der nicht auf der Liste steht. Das ist so gewollt. Prüfen Sie von dem Rechner aus, der mitlesen soll, oder über diese Seite.

2.11.5 Wann brauchen Sie das?

- Beim ersten Aufbau einer Edge: einmalig die Subscription für den IDEA-4S-Sensor anlegen, damit Daten in DataStore und Grafana ankommen.
- Bei einem **leeren Grafana**-Dashboard: prüfen, ob die Subscription noch existiert (manche IFM-Firmware-Updates leeren die Liste). Falls ja, Status prüfen; falls nein, neu anlegen.
- Wenn Sie zusätzliche Größen mitschicken wollen — z. B. Diagnose-Werte des IO-Link-Masters selbst.

2.11.6 Hinweise

- Die ifm-IoT-Core-Oberfläche wird vom Masters direkt geliefert — wenn sie nicht erscheint, ist meist die LAN-Verkabelung oder Stromversorgung des IO-Link-Masters fehlerhaft. Die



openXEdge meldet das in **Einstellungen** → **Diagnose** unter `iolink-proxy` mit Code 3001 (siehe Diagnose-Codes (Kap. 3.1)).

- Eine ausführliche Doku der einzelnen IFM-Felder finden Sie in der **ifm IoT Core**-Anleitung zu Ihrem Mastermodell — die openXEdge-Doku konzentriert sich auf den Teil, der die Edge betrifft.

2.12 Messdaten nach Excel exportieren

Sie wollen Messwerte aus einem Zeitraum in Excel auswerten — etwa um einen Hochlauf nachzurechnen oder eine Aufzeichnung an Dritte weiterzugeben. **Jedes** Panel in Grafana gibt seine Daten als CSV heraus; die Arbeit steckt danach im Excel-Import.

2.12.1 1. Zeitraum wählen

Stellen Sie **zuerst** oben rechts den Zeitraum ein, den Sie exportieren wollen. Exportiert wird immer genau das, was das Panel gerade anzeigt.

Halten Sie den Zeitraum klein. Bei den IDEA-4S-Signalen kommen pro Stunde einige zehntausend Werte zusammen — die Datenbank liefert das in Sekundenbruchteilen, aber die Tabelle im Browser darzustellen kostet auf der Anlage spürbar Zeit. Für einen ganzen Tag exportieren Sie besser mehrere Stunden nacheinander.

2.12.2 2. CSV herunterladen

1. Auf die drei Punkte oben rechts am Panel klicken.
2. **Überprüfen** → **Daten** wählen.
3. Unter **Datenoptionen** den Schalter **Download for Excel** einschalten (diese Beschriftung ist auch in der deutschen Oberfläche englisch).
4. **CSV herunterladen** klicken.

Der Schalter ist der Grund, warum es in Excel gutgeht: Grafana schreibt dann eine Kennzeichnung des Trennzeichens in die erste Zeile, an der sich Excel beim Öffnen orientiert.

2.12.3 3. In Excel importieren

Öffnen Sie Excel mit einem **leeren** Arbeitsblatt und holen Sie die Datei über **Daten** → **Aus Text/CSV** herein — nicht per Doppelklick auf die Datei.

Im Fenster *Daten transformieren* achten Sie auf zwei Dinge:

- **Trennzeichen** muss auf Komma stehen.
- Der Schritt **Geänderter Typ** rechts unter *Angewendete Schritte* rät die Spaltentypen aus dem Gebietsschema. Grafana schreibt Zahlen mit **Punkt** als Dezimaltrennzeichen; ein deutsches Excel rät daher falsch und macht aus 12.5 den 12. Mai oder die Zahl 125. Löschen Sie den Schritt



über das Kreuz; alle Spalten kommen dann als Text herein, und Sie setzen die Typen anschließend selbst.

2.12.4 4. Die Zeitachse

Welche Spalten Sie bekommen, hängt vom exportierten Panel ab. Die Zeitreihen-Panels des ausgelieferten Dashboards liefern eine Spalte **time** mit Datum und Uhrzeit und daneben je eine Wertespalte (etwa `value_temperature_bearing_1`). Damit können Sie direkt arbeiten: Spalte als *Datum/Uhrzeit* typisieren, fertig.

Manche selbst gebauten Tabellen-Panels geben die Zeit stattdessen als **Zahl** heraus — Sekunden seit dem 1.1.1970. Daraus wird in einer neuen Spalte eine Datums-Achse (Zeitspalte hier B):

```
=B2/86400 + DATUM(1970;1;1)
```

Oder eine **relative Zeitachse** in Sekunden ab Aufzeichnungsbeginn — meist die bessere Wahl für einen Hochlauf:

```
=B2 - $B$2
```

2.12.5 5. Diagramm

Nehmen Sie ein **Punktdiagramm (XY) mit Linien**, kein Liniendiagramm: Das Liniendiagramm behandelt die Zeit als gleichmäßig verteilte Beschriftung und verzerrt jede Lücke in der Aufzeichnung. Formatieren Sie die X-Achse anschließend mit Rechtsklick → **Achse formatieren** → **Zahl**, entfernen Sie den Haken bei *Mit Quelle verknüpft* und geben Sie das gewünschte Format ein.

2.12.6 Warum manche Zellen leer bleiben

Wenn ein Panel mehrere Signale in eine gemeinsame Tabelle legt, fallen Lücken auf. Die Signale kommen unterschiedlich schnell an — der Sensor meldet **bei Änderung**, nicht in einem festen Takt. Auf einer Anlage über zwei Stunden gemessen (Abstand zwischen zwei Werten, Median): Schwinggeschwindigkeit 0,1 s, Lager- und Kühlmitteltemperaturen 0,2 s, Drehzahl 30 s bei stehender Spindel. In den Zeilen dazwischen bleibt die langsamere Spalte deshalb leer. Das ist kein Fehler in der Aufzeichnung. Für eine durchgehende Kurve filtern Sie in Excel auf die Zeilen, in denen die Spalte belegt ist.



3 Referenz

3.1 Diagnose-Codes

Alle Edge-Dienste schreiben strukturierte Diagnose-Meldungen in eine zentrale Übersicht (**Einstellungen** → **Diagnose**). Jede Meldung trägt einen vierstelligen Code.

Bereich	Dienst	Codebereich
1xxx	MainUI	1001–1099
2xxx	UpdateService	2001–2099
3xxx	IOLinkMasterProxy	3001–3099
4xxx	USBService	4001–4099
7xxx	Flottenanbindung — meldet aus jedem Dienst, der sie nutzt	7000–7999
—	DataStore	1000–2504, siehe unten

Die Nummer allein genügt nicht. Der DataStore bringt rund 150 eigene Codes mit, deren Nummern sich mit denen von MainUI und UpdateService **überschneiden**. Maßgeblich ist deshalb der **Dienstname**, unter dem die Meldung in der Diagnose-Ansicht steht — nicht die Ziffernfolge.

3.1.1 MainUI (1xxx)

Code	Bedeutung	Übliche Maßnahme
1001	Update-Server nicht erreichbar	Internet-Verbindung der Edge prüfen; ggf. VPN.
1002	IDEA4S-Schnittstelle nicht erreichbar	IDEA4S-Bridge-Dienst prüfen (Diagnose-Detail); Edge ggf. neu starten.
1003	Netplan-Konfiguration fehlgeschlagen	Eingegebene IP-Konfiguration prüfen, Edge neu starten.
1004	Konfigurationsdatei beschädigt	Service-Techniker hinzuziehen — Edge fällt auf Defaults zurück.
1005	Docker-Socket nicht erreichbar	Edge neu starten; bei Wiederholung Service-Techniker.
1006	Service-URL nicht erreichbar	Welche URL ist betroffen — siehe Detail-Meldung in der Diagnose.
1007	Container nicht gesund	Diagnose-Tab des betroffenen Service prüfen.
1008	Docker-Befehl fehlgeschlagen	Service-Techniker.
1009	Update-Signatur ungültig	Nicht installieren — Brinkhaus-Support kontaktieren.
1010	Schlüssel des Update-Servers passt nicht zum hinterlegten	Der Update-Server hat einen anderen Signaturschlüssel geliefert als den, den die



Code	Bedeutung	Übliche Maßnahme
		Edge kennt, und keinen gültigen Nachweis für einen Schlüsselwechsel. Das Update wurde nicht geladen, die laufende Version ist unverändert. Nicht wiederholen — Brinkhaus-Support kontaktieren.
1011	UpdateService-Update abgelehnt: Abbildung aus nicht zugelassener Quelle	Die neue Fassung des UpdateService nannte eine Container-Abbildung aus einer Quelle, die diese Edge nicht akzeptiert; sie wurde nicht installiert, der bisherige Dienst läuft weiter. Brinkhaus-Support kontaktieren.
1012	Eigenes HTTPS-Zertifikat läuft bald ab oder ist abgelaufen	Erneueres Zertifikat installieren — siehe Fernzugriff (HTTPS) (Kap. 2.3.3.5).
1013	HTTPS-Zertifikat nicht nutzbar	Nennt die Meldung Ihr eigenes Zertifikat : Die Edge verwendet stattdessen ihr Edge-Zertifikat; installieren Sie es unter Einstellungen → HTTPS-Zertifikat neu oder entfernen Sie es. Nennt sie ein vorläufiges Zertifikat , eine fehlgeschlagene Erneuerung oder einen HTTPS-Start: Die Edge versucht es selbst erneut; bleibt die Meldung stehen, Service-Techniker hinzuziehen.

3.1.2 UpdateService (2xxx)

Code	Bedeutung	Übliche Maßnahme
2001	Update-Verzeichnis fehlt	Service-Techniker.
2002	Backup vor Update fehlgeschlagen	Festplattenplatz prüfen, dann erneut versuchen.
2003	<code>docker compose up</code> fehlgeschlagen	Diagnose-Detail prüfen, ggf. Rollback durchführen.
2004	Health-Check nach Update fehlgeschlagen	Update wird automatisch zurückgenommen — Logs prüfen.
2005	Rollback gestartet	Informativ — kein Eingriff nötig.
2006	Rollback erfolgreich	Informativ — Edge läuft wieder.
2007	Rollback fehlgeschlagen	Service-Techniker sofort.
2008	Update-Signatur-Prüfung fehlgeschlagen	Nicht installieren — Support kontaktieren.
2009	Signaturprüfung übersprungen (Legacy-1.x-Update)	Informativ — tritt nur während der Migration von 1.x-Edges auf; ab 2.x ist die Signaturprüfung immer aktiv.
2010	Update-Abbildungen fehlen auf dem Gerät	Die Meldung nennt die betroffenen Abbildungen: sie konnten nicht geladen werden



Code	Bedeutung	Übliche Maßnahme
		und liegen auch nicht auf dem Gerät. Das Update wurde deshalb nicht gestartet; ein Gerät, auf dem bereits eine Version läuft, kehrt zu dieser zurück (siehe 2005–2007). Netzwerkzugang des Geräts zur Registry prüfen und Update erneut anstoßen.
2011	Update abgelehnt: Abbildung aus nicht zugelassener Quelle	Das Update nannte eine Container-Abbildung aus einem Repository, das dieses Gerät nicht akzeptiert; es wurde nichts installiert, die laufende Version ist unverändert. Nicht mit demselben Paket erneut versuchen — Support kontaktieren: entweder ist das Release fehlerhaft oder jemand hat es verändert.

3.1.3 IOLinkMasterProxy (3xxx)

Code	Bedeutung	Übliche Maßnahme
3001	IO-Link-Master nicht erreichbar	LAN-Kabel zum IFM-Master prüfen, IFM-Gerät neu starten.
3002	Hohe Fehlerrate beim Proxyieren	IFM-Master oder Netzwerk hat Probleme — Logs prüfen.
3003	HTTP-Fehler vom IO-Link-Master	IFM-Konfiguration prüfen.
3004	Zugriff auf den IO-Link-Master abgewiesen	Ein Gerät wollte den IO-Link-Master lesen und darf das nicht. So gewollt — es sei denn, es ist ein von Ihnen eingerichteter Mitleser: dann seine Adresse in der Master-Konfigurationsdatei der Anlage unter <code>allow_from</code> eintragen.

3.1.4 USBService (4xxx)

Code	Bedeutung	Übliche Maßnahme
4001	USB-Mount fehlgeschlagen	Stick neu einstecken; ggf. anderen Stick versuchen.
4002	Dateiübertragung fehlgeschlagen	Stick neu einstecken.
4003	MainUI nicht erreichbar	Edge selbst hat ein Problem — siehe Diagnose-Codes 1xxx.
4004	USB erkannt, aber kein Gerät	Stick neu einstecken.
4005	CSV-Dateien zur Übertragung anstehend	Stick einstecken.
4006	Container startet neu	Informativ.
4007	Kein USB mit übertragbaren Dateien	Informativ.
4008	Letzte Kopie erfolgreich	Informativ.



3.1.5 DataStore

Führt Ihre Anlage einen **DataStore**, kommen dessen eigene Codes hinzu. Die vollständige Liste steht im Handbuch des DataStore, das Sie beim Brinkhaus-Service anfordern können; hier stehen die drei, die im Alltag auffallen. Alle drei betreffen die **Aufbewahrung** — also wie lange die Anlage Messwerte behält. Der Meldungstext in der Diagnose-Ansicht nennt jeweils den betroffenen Datenbestand.

Code	Bedeutung	Übliche Maßnahme
1513	Die automatische Datenbereinigung kommt nicht nach — es läuft mehr ein, als sie abträgt.	Aufbewahrungsgrenzen prüfen (DataStore → Einstellungen → Verhaltensparameter → <i>Aufbewahrung</i>); hält es an, Brinkhaus-Service informieren.
1517	Hinweis (kein Fehler): Nach einem Update wird der vorhandene Bestand einmalig eingeteilt.	Keine. Auf großen Anlagen dauert das Stunden; solange räumt die Bereinigung bei den Messwerten nur ab, was schon eingeteilt ist.
1522	Notstillstand: Die Anlage hat die Datenerfassung angehalten , weil ein Bestand seine Not-Grenze erreicht hat — meist, nachdem eine Größengrenze zu klein gesetzt wurde.	Grenze im DataStore anpassen oder abwarten, bis aufgeräumt ist. Die Meldung bleibt danach stehen, bis sie mit einem „ Kleinen Neustart “ in der DataStore-Oberfläche quittiert wird.

3.1.6 Wo sehe ich die Codes?

In **Einstellungen** → **Diagnose** rollen Sie pro Service ein Klappfeld auf — die einzelnen Meldungen mit Code und Beschreibung erscheinen darunter:

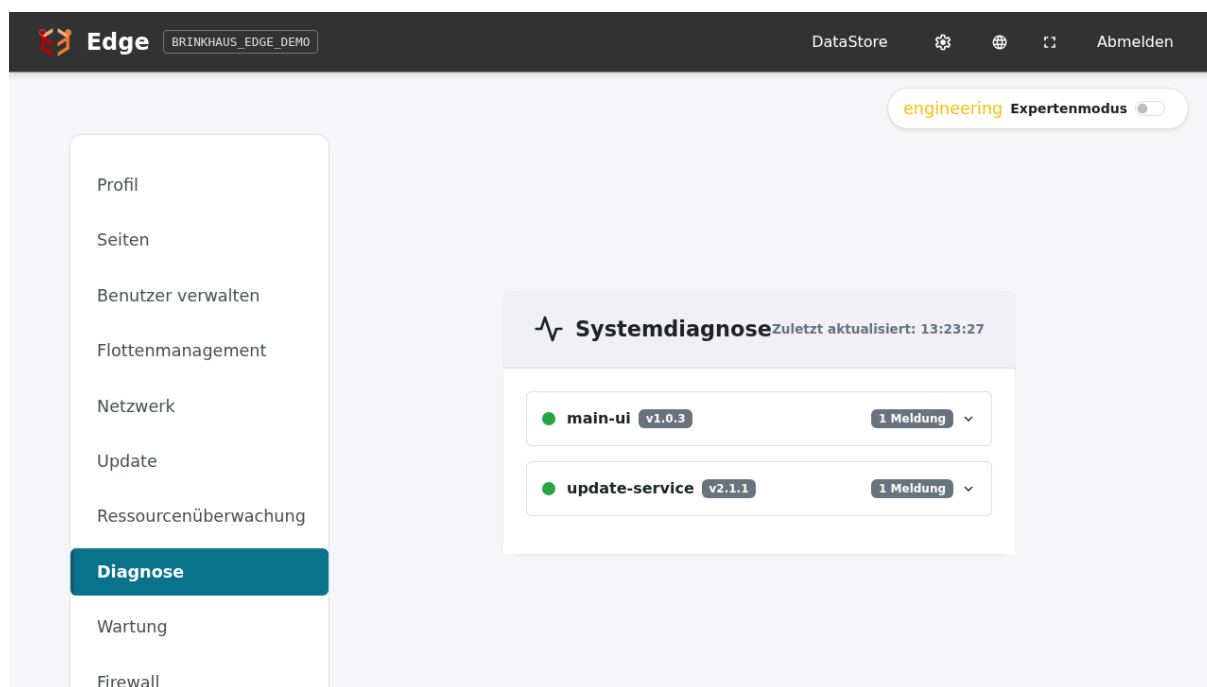


Abbildung 13: System-Diagnose-Panel mit grünen Status-Punkten und Versions-Badges



Über die Flottenanbindung können dieselben Diagnose-Codes auch zentral im FleetManager ausgewertet werden — die zugehörige Erklärungs-Seite folgt.

3.2 IDEA-4S – Signalnamen im DataStore

Wenn Sie ein eigenes Grafana-Panel bauen, fragen Sie die Tabelle `historicValues` nach einem `signal_name`. Trifft der Name nicht, bleibt das Panel **leer** — **ohne Fehlermeldung**. Diese Seite listet die Namen, wie sie auf einer GMN-Anlage tatsächlich in der Datenbank stehen.

3.2.1 Messwerte

Diese zehn Signale enthalten eine Zahl:

Signalname	Größe
VibVeloXDirection	Effektive Schwinggeschwindigkeit, X-Achse
VibVeloYDirection	Effektive Schwinggeschwindigkeit, Y-Achse
VibVeloZDirection	Effektive Schwinggeschwindigkeit, Z-Achse
TempBearing1 ... TempBearing4	Lagertemperaturen 1 bis 4
TempCoolantInlet	Kühlmitteltemperatur am Eintritt
RotSpeed	Drehzahl
operatingHours	Betriebszeit als Rohzähler , nicht in Stunden

Zwei Namen sind die häufigste Fehlerquelle:

- Die Drehzahl heißt **RotSpeed**, nicht **Speed**. Eine Abfrage auf `Speed` liefert nichts und sieht dabei aus wie eine Anlage ohne Drehzahlsignal.
- **operatingHours** ist ein Zähler in Schritten von rund einer Zehntelsekunde. Die Umrechnung in Stunden macht die Kachel im DataStore mit dem Gerätekenwert aus der IODD; in einer eigenen Abfrage müssen Sie sie selbst vornehmen.

3.2.2 Status-Signale

Zu den meisten Messwerten gibt es ein gleichnamiges Signal mit dem Zusatz **Status** (`RotSpeedStatus`, `TempBearing1Status`, ...), dazu `DeviceStatus`, `ClampingStatus`, `DisplacementStatus`, `DisplacementTempStatus`, `DrawbarPositionStatus`, `HydraulicPiston` und `ReleaseStroke`.

Diese Signale enthalten **keine Zahl, sondern ein Objekt**. Deshalb gehört in jede eigene Abfrage die Zeile

```
AND jsonb_typeof(hv.value) = 'number'
```

Ohne sie bricht die Abfrage ab, sobald ein solcher Wert in die Auswahl gerät — `invalid input syntax for type double precision`.



3.2.3 Histogramm-Klassen

Die übrigen 51 Signale (`wearEdge...`, `wearTime...`) sind die Klassen der Verweildauer-Histogramme, je Achse durchnummeriert. Sie werden von den Histogramm-Kacheln ausgewertet und sind für eigene Zeitreihen-Panels nicht gedacht.

3.2.4 Die Maschine treffen

Alle Signale hängen an der importierten IDEA-4S-Maschine. Deren Nummer steht nicht fest — sie ändert sich, wenn die Maschine neu angelegt wird. Fragen Sie sie deshalb mit `ab`, statt eine Zahl einzutragen:

```
WHERE hv.machine_id = (SELECT id FROM "machines"
                        WHERE import_type = 'idea4s' ORDER BY id LIMIT 1)
```

`ORDER BY id LIMIT 1` ist kein Beiwerk: Steht mehr als eine IDEA-4S-Maschine im DataStore — etwa nach einem erneuten Import —, bricht die Abfrage ohne diese Zeile ab.



4 Hintergrund

4.1 Das Gerät

Die openXEdge besteht aus zwei Teilen: einem lüfterlosen Industrie-PC für den Schaltschrank und der Firmware, die auf ihm läuft. Die Firmware hält sich selbst aktuell (siehe Wie Updates funktionieren (Kap. 4.3)); der PC bleibt derselbe.

4.1.1 Wofür die openXEdge da ist

Die openXEdge ist die Plattform für Anwendungen an der Maschine: Sie bringt die Bedienoberfläche, die Updates, die Diagnose und die Anbindung an die Flottenverwaltung mit. Welche Anwendungen auf einer Edge laufen, hängt von ihrer Ausführung ab; die Handbücher der einzelnen Ausführungen beschreiben sie.

4.1.2 Der Industrie-PC

Die openXEdge wird auf dem Embedded-Computer **NET-III 2I640DW** von LEX COMPUTECH ausgeliefert, in der Ausführung mit Intel-Atom-Prozessor (-E13).

4.1.2.1 Technische Daten

Hersteller, Modell, Prozessor, Arbeits- und Datenspeicher wie ausgeliefert, die übrigen Werte nach dem Datenblatt des Herstellers.

Merkmal	Wert
Hersteller	LEX COMPUTECH Co., Ltd. (Taiwan)
Modell	NET-III 2I640DW-E13, lüfterloser Embedded-Computer
Prozessor	Intel Atom x6413E (Elkhart Lake), vier Kerne, 2,7 GHz
Arbeitsspeicher	8 GB DDR4 (ein SODIMM-Steckplatz, bis 32 GB)
Datenspeicher	128 GB, M.2
Sicherheitschip	TPM 2.0
Netzwerk	3 × 2,5 Gbit/s Ethernet (Intel I225 oder I226, je nach Baujahr)
USB	2 × USB 3.0
Bildschirm	2 × HDMI
Seriell	2 × RS-232/422/485 (COM)
Stromversorgung	9–24 V DC über eine zweipolige Klemme, alternativ externes Netzteil 100–240 V AC
Abmessungen	135 × 110 × 35 mm, mit Hutschienehalter 142,45 mm hoch und 40 mm breit
Gewicht	0,75 kg
Montage	Hutschiene (Halter mit 3 × M4) oder flach über 4 × M4 im Raster 75 × 75 mm
Betriebstemperatur	–20 bis +60 °C bei voller Prozessorlast (Herstellerangabe) ¹
Lagertemperatur	–20 bis +70 °C



Merkmal	Wert
Luftfeuchte	bis 95 % bei 40 °C, nicht kondensierend

¹ Laut Hersteller mit Arbeitsspeicher und Datenspeicher für den erweiterten Temperaturbereich.

4.1.2.2 Anschlüsse am Gehäuse

- **Vorderseite**, von oben nach unten: Ein-/Ausshalter, Nano-SIM-Schacht, drei LAN-Buchsen (oben Eth3, in der Mitte Eth2, unten Eth1), daneben zwei USB-Buchsen, darunter zwei HDMI-Buchsen.
- **Oberseite**: zwei COM-Anschlüsse (9-polig).
- **Unterseite**: Klemme der Stromversorgung.

Ab Werk sind die LAN-Ports so eingestellt:

Port	Werkseinstellung
Eth1	fest 172.16.9.112/24
Eth2	DHCP
Eth3	fest 172.16.10.250/24 (Service-Port)

Wofür jeder Port gedacht ist, beschreibt Anschlüsse der Edge (Kap. 4.2).

4.1.2.3 Maßzeichnung

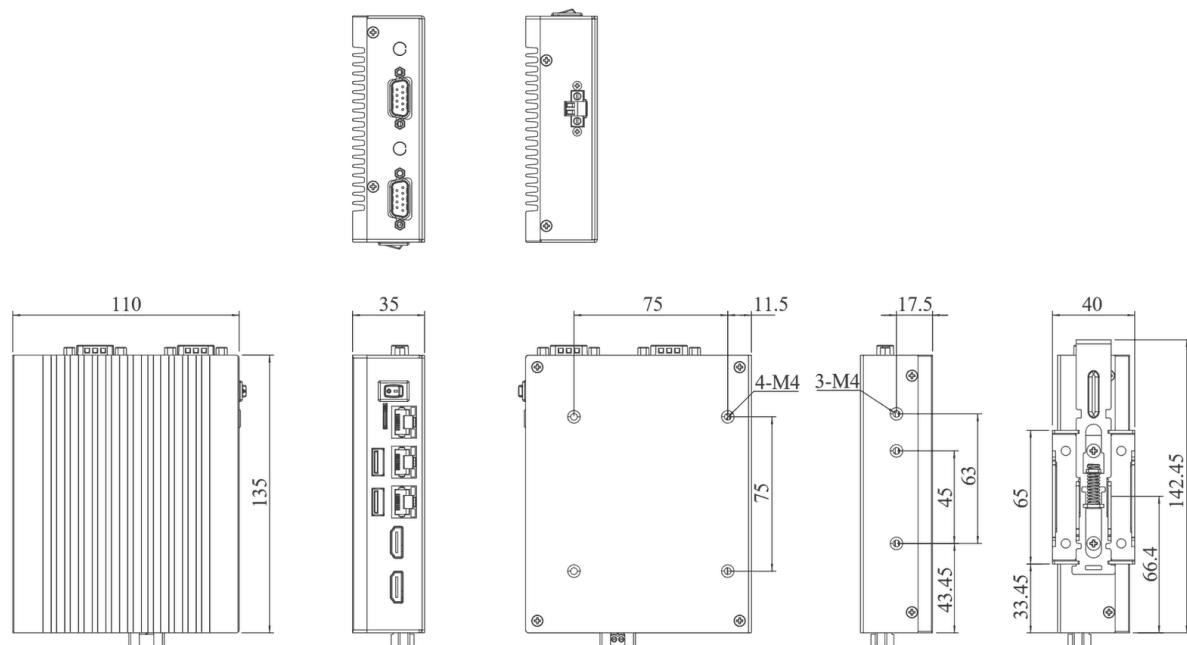


Abbildung 14: Maßzeichnung des LEX NET-III 2I640DW mit Gehäusemaßen, Anschlüssen und Hutschienenhalter (Maße in mm)

4.2 Anschlüsse der Edge

Die openXEdge hat drei LAN-Ports auf der Vorderseite. Sie sind in der Werksauslieferung **fest** auf drei verschiedene Aufgaben vorbereitet — wer das einmal verstanden hat, weiß auch, wo Service-Personal an die Edge kommt und wohin der Sensorbus verkabelt gehört.

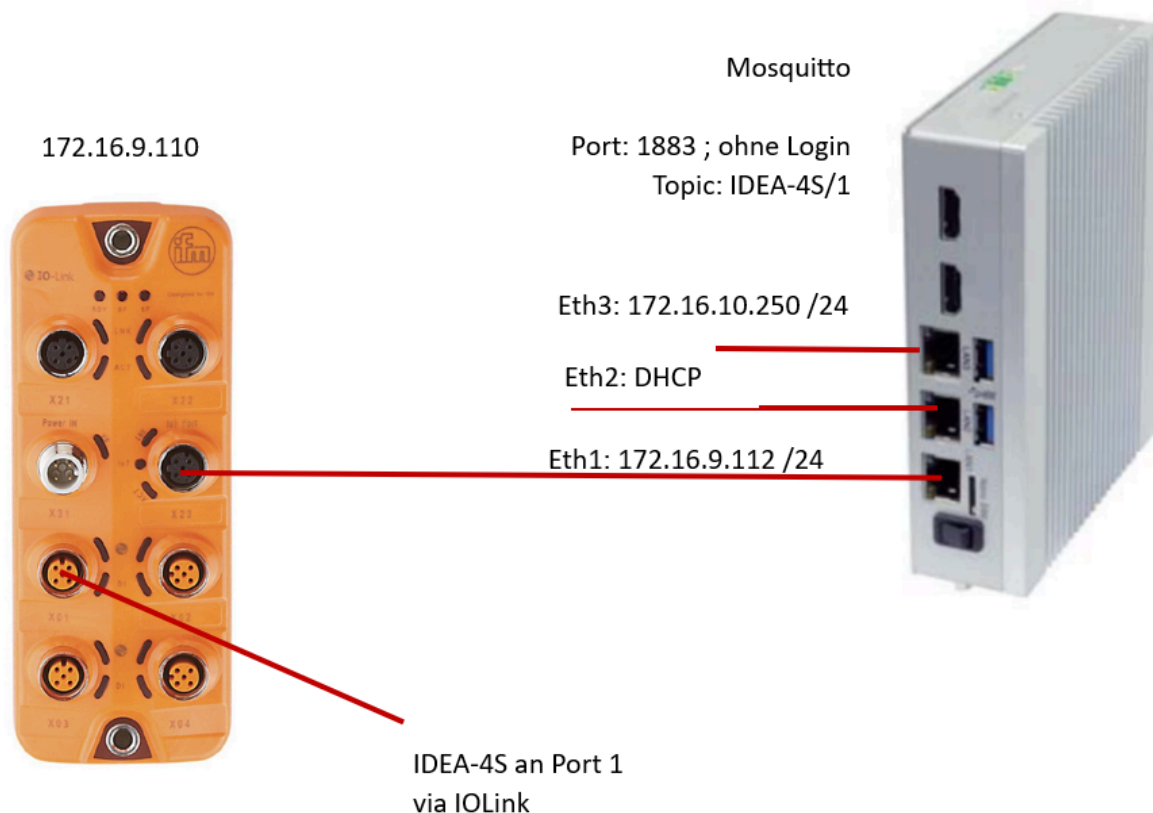


Abbildung 15: Verkabelungsübersicht: IO-Link-Master, Edge-Ports, Mosquitto

4.2.1 Die drei Ports

Von oben nach unten am Gerät:

Port	Aufgabe	Werks-IP
Eth3 (oben)	Service-Port für Brinkhaus-Service / IT-Wartung. Statisch vergeben, nicht im Werksnetz.	172.16.10.250/24
Eth2 (Mitte)	Firmennetz — DHCP-Client. Über diesen Port holt sich die Edge ihre Firmen-IP, kommt ins Internet, erreicht den Fleet-Manager.	DHCP
Eth1 (unten)	IO-Link-Master -Anschluss. Statisch im Master-Subnetz.	172.16.9.112/24



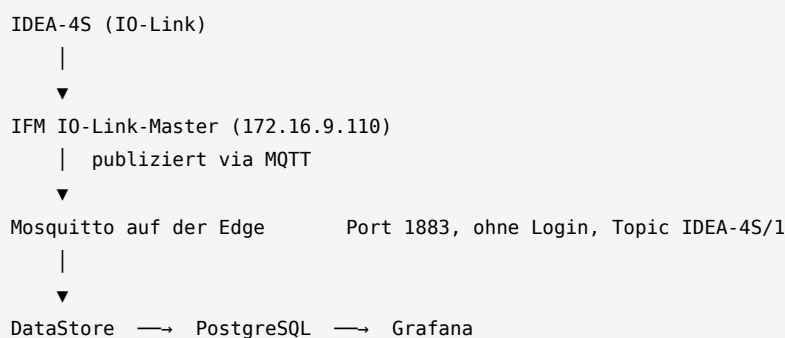
Eth1 zeigt damit fest auf den IFM-IO-Link-Master — werksseitig auf 172.16.9.110. Der **IDEA-4S**-Sensor hängt physisch an **Port 1** dieses Masters via IO-Link und schickt seine Werte über das IO-Link-Protokoll.

4.2.2 Wieso drei getrennte Netze?

Die Trennung macht zwei Dinge möglich:

1. **Maschinen-Bus bleibt ungestört** — der IO-Link-Master und sein Sensorstrang sind in einem eigenen kleinen Subnetz (172.16.9.0/24). Der Datenverkehr dort liegt im einstelligen kbit-Bereich und wird durch Office-Last nicht beeinflusst.
2. **Firmennetz bleibt sauber** — alles, was die Welt erreichen soll (Updates aus dem Internet, Anbindung an den FleetManager, Browser-Zugriff vom Werker-PC), läuft ausschließlich über Eth2.

4.2.3 Datenfluss kurzgefasst



Mehr zur Visualisierung in Grafana-Dashboards (Kap. 4.4), mehr zur MQTT-Subscription in IO-Link-Master konfigurieren (Kap. 2.11).

4.2.4 Praktische Konsequenzen

- **Anlage in Betrieb nehmen:** Eth1 zum IO-Link-Master, Eth2 ins Firmennetz mit DHCP, Eth3 erst stecken, wenn ein Service-Techniker da ist.
- **Vor Ort am IDEA-4S messen:** Ihr Service-Laptop kommt über Eth3 ins Service-Subnetz oder über Eth2 von der Office-Seite.
- **IP der Edge ändern:** nur über die Bedienoberfläche (siehe Netzwerk konfigurieren (Kap. 2.6)) — niemals über das Betriebssystem selbst, Sie würden die nächste Update-Konfiguration brechen.

4.3 Wie Updates funktionieren

Wenn Sie in **Einstellungen** → **Update** auf **Upgrade** oder **Downgrade** klicken, läuft ein mehrstufiger Prozess. Dieses Dokument erklärt, was im Hintergrund passiert — nützlich, wenn etwas nicht wie erwartet abläuft.



4.3.1 Beteiligte Komponenten

- **MainUI** — die Bedienoberfläche, die den Klick entgegennimmt und die Update-Dateien herunterlädt.
- **BOS Update Server** (<https://update.brinkhaus-gmbh.de>) — die zentrale Quelle aller Firmware-Versionen, signiert mit einem Ed25519-Schlüssel.
- **UpdateService** — ein eigener Hintergrund-Container auf der Edge, der den eigentlichen Austausch orchestriert. Er läuft in einem **separaten Compose-Stack** als der Haupt-Stack — denn er muss den Haupt-Stack neu starten können, ohne sich selbst zu beenden.

4.3.2 Phase 1: Auswahl und Download (durch MainUI)

1. MainUI ruft die verfügbaren Versionen vom Update-Server ab.
2. Sie klicken auf eine Version → MainUI lädt drei Dateien in genau dieser Reihenfolge:
 1. `public-key.pem` — der öffentliche Signaturschlüssel
 2. `docker-compose.yml.sig` — die Signatur über die neue Compose-Datei
 3. `docker-compose.yml` — die eigentliche Compose-Datei (zuletzt!)
3. MainUI verifiziert die Ed25519-Signatur. Bei Fehlschlag → Diagnose-Code 1009, Update wird abgebrochen.
4. Die drei Dateien liegen jetzt unter `/home/gmn-service/docker/updates/data/`. Das Schreiben der Compose-Datei ist das Trigger-Ereignis für den UpdateService.

4.3.3 Phase 2: 7-Phasen-Deploy (durch UpdateService)

Der UpdateService prüft das Staging-Verzeichnis im 10-Sekunden-Takt. Sobald er eine neue `docker-compose.yml` findet, läuft folgender Ablauf:

Phase	Aktion
1	Validierung — gestagete Compose-Datei vorhanden und syntaktisch gültig?
2	Backup — aktuelle Compose-Datei und <code>description.json</code> ins Backup-Verzeichnis kopieren.
3	Stop — <code>docker compose stop</code> + <code>docker compose rm -f</code> für den Haupt-Stack (nicht <code>down</code> , damit das gemeinsame <code>bos-internal</code> -Netz erhalten bleibt).
4	Deploy — atomares Kopieren der neuen Dateien an den Live-Speicherort. <code>config.json</code> wird nicht überschrieben (MainUI merkt neue Defaults beim Start).
5	Start — <code>.env</code> neu generieren (für die aktuelle Multi-IP-Liste), <code>docker compose pull</code> , <code>docker compose up -d</code> .
6	Health-Check — Container-Stabilität (≥ 10 s laufend, keine Restart-Loops) und HTTP-Probe gegen <code>http://localhost:5000/api/version</code> <i>im Container</i> .
7	Cleanup (bei Erfolg) oder Rollback (bei Misserfolg).

Während des gesamten Vorgangs ist die Bedienoberfläche **nicht erreichbar**.



4.3.4 Phase 3: Rollback (nur bei Misserfolg)

Wenn der Health-Check innerhalb von 90 Sekunden nicht grün wird, springt der UpdateService automatisch zurück:

1. Stack mit der neuen Version stoppen.
2. Backup-Compose und -Description an den Live-Speicherort kopieren.
3. Stack mit der alten Version wieder starten.
4. Diagnose-Codes 2005 (Rollback gestartet), dann 2006 (erfolgreich) oder 2007 (fehlgeschlagen) absetzen.

□ **One-cycle backwards-compatibility:** der **vorherige** UpdateService führt den Health-Check während eines Upgrades durch — die neue MainUI muss daher mindestens einen Update-Zyklus lang noch genauso auf `http://localhost:5000/api/version` antworten, wie es der alte UpdateService erwartet. Diese Regel galt nicht in 2.1.0 — alle Upgrades von 2.0.x rollten zurück; 2.1.1 hat es korrigiert.

4.3.5 Was bedeuten die Versionen in der Service-Tabelle?

In **Einstellungen** → **Update** sehen Sie nicht nur die Firmwareversion (z. B. 2.2.1), sondern auch die individuellen Versionen jedes Docker-Containers:

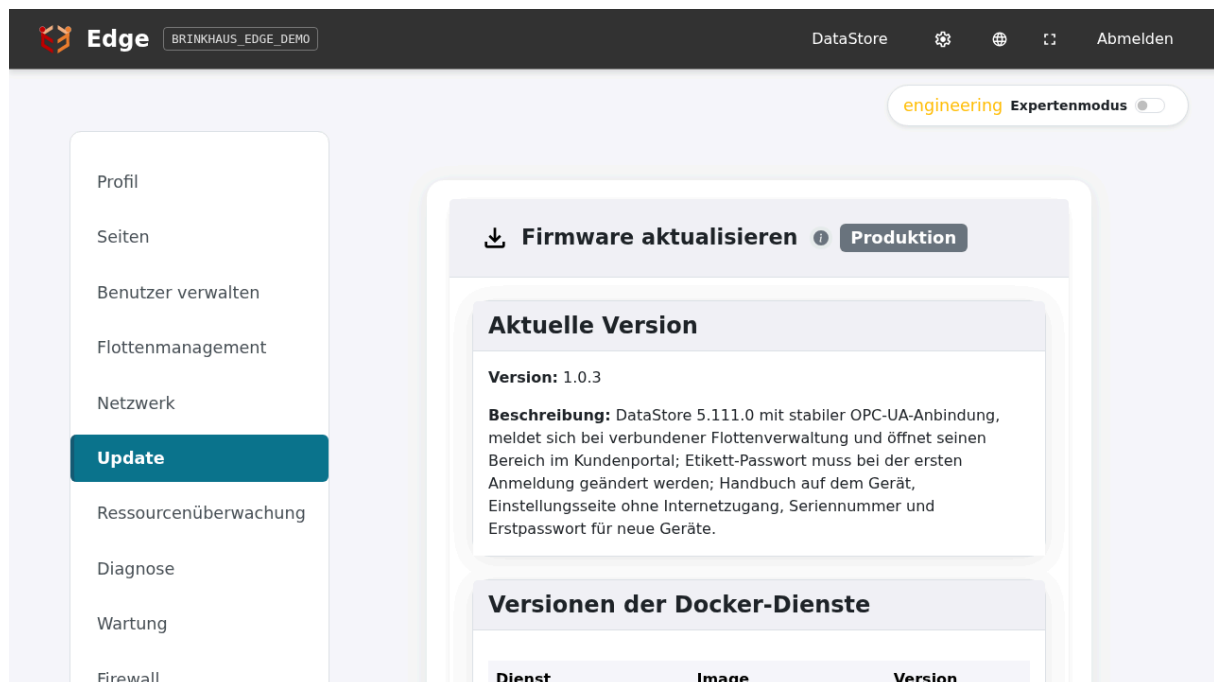


Abbildung 16: Service-Versionen-Tabelle in der Update-Ansicht

Eine Firmware-Version ist eine **Sammlung** kompatibler Service-Versionen, festgelegt in der ausgelieferten `docker-compose.yml`. Updates ersetzen also nicht nur ein Image, sondern stellen eine geprüfte Kombination aller Container des Streams her.



4.3.6 Verwandt

- Firmware aktualisieren (Kap. 2.1) — die Schritte am Bildschirm
- Diagnose-Codes (Kap. 3.1) — was bedeuten Update-Fehlermeldungen (Bereich 2xxx)

4.4 Grafana-Dashboards

Wenn Sie auf der Startseite die Kachel **Grafana** anklicken, landen Sie auf einem vorkonfigurierten Dashboard. Es zeigt das Wichtigste über den angeschlossenen IDEA-4S-Sensor in einem Blick.

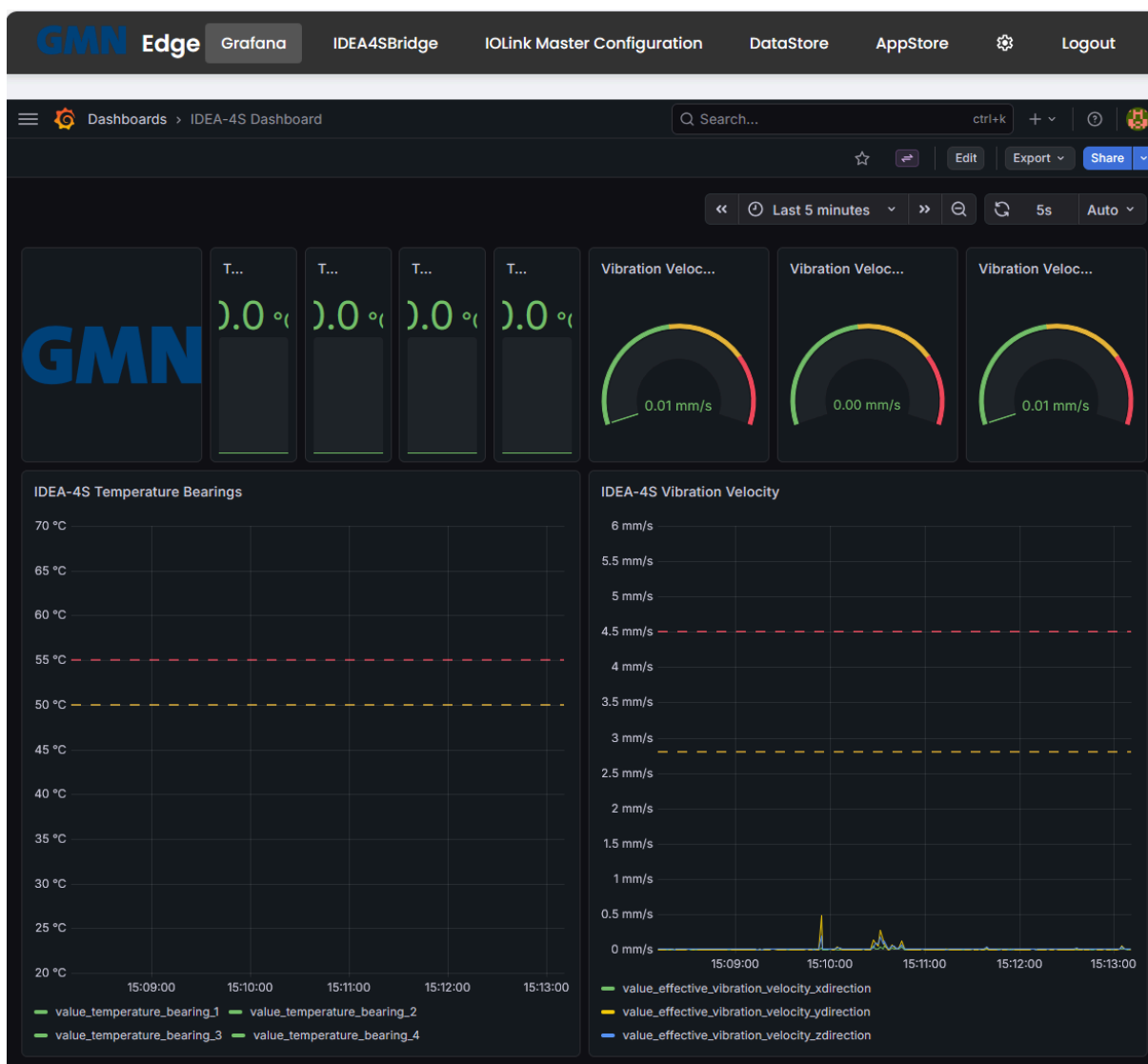


Abbildung 17: IDEA-4S-Dashboard in Grafana mit Lagertemperaturen, Vibrationen und Zeitreihen

4.4.1 Aufbau des Dashboards

- **Vier Lagertemperatur-Kacheln** oben links: Bearing 1 bis Bearing 4, Anzeige in °C. Bei vorliegenden Rohwerten leuchten die Kacheln entsprechend der hinterlegten Schwellenwerte.

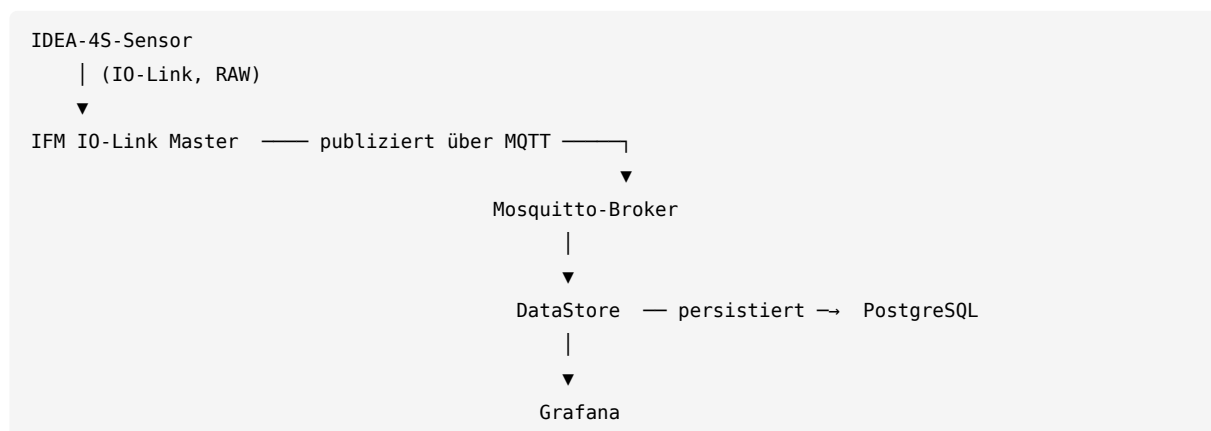


- **Drei Vibrationsgeschwindigkeits-Gauges** oben rechts: X-, Y-, Z-Achse, in mm/s. Die Skala beginnt grün und geht über gelb zu rot, sobald sich Werte den im IODD definierten Schwellen nähern.
- **Zeitreihenpanel „IDEA-4S Temperature Bearings“** unten links: alle vier Lager über den gewählten Zeitraum. Die rote gestrichelte Linie ist die Alarmschwelle, die gelbe die Warnschwelle.
- **Zeitreihenpanel „IDEA-4S Vibration Velocity“** unten rechts: die drei Achsen über den gewählten Zeitraum.

Beide Zeitreihenpanels zeichnen eine durchgezogene Linie, auch wenn ein Lager in einem Zeitabschnitt nichts gemeldet hat (ab **gmn-2.34.1**). Die vier Lager melden nicht im selben Augenblick; früher brach die Linie eines Lagers an jeder solchen Stelle ab, und übrig blieben verstreute Punkte. Zwischen zwei gemessenen Werten wird dabei nur eine gerade Verbindung gezogen — kein Wert erfunden. Fällt ein Sensor tatsächlich aus, ist das deshalb **nicht** als Lücke in der Kurve zu sehen, sondern an den Kacheln darüber und auf der Diagnoseseite.

Über die Zeitspannen-Auswahl oben rechts (im Beispiel: „Last 5 minutes“) wechseln Sie zwischen Live-Ansicht und historischer Auswertung.

4.4.2 Wo kommen die Daten her?



- Der IO-Link-Master liest den IDEA-4S zyklisch aus und sendet jede Änderung als MQTT-Nachricht. Welche Topics konfiguriert sind, sehen Sie in **IO-Link-Master-Konfiguration** → **Notification**.
- Der **DataStore** abonniert diese Topics, prüft sie gegen das hinterlegte Schema und schreibt die Werte in die lokale **PostgreSQL** auf der Edge.
- **Grafana** liest aus der PostgreSQL und visualisiert. Das Dashboard ist mit der Edge ausgeliefert; Sie können Kopien anlegen und anpassen.



4.4.3 Anmeldung: Sie sind schon angemeldet

Grafana hat kein eigenes Passwort. Die Bedienoberfläche der Edge meldet Sie dort mit **Ihrem eigenen Benutzernamen** an — oben rechts steht Ihr Name, und was Sie ändern, wird unter diesem Namen protokolliert. Wenn Sie sich an der Bedienoberfläche abmelden, endet damit auch der Zugriff auf Grafana.

Was Sie dort dürfen, richtet sich nach Ihrer Rolle in der Bedienoberfläche:

Ihre Rolle	In Grafana
Administrator	Dashboards ansehen, bearbeiten und speichern
Benutzer	Dashboards ansehen

Ändert ein Administrator Ihre Rolle, wirkt das in Grafana sofort — mit dem nächsten Seitenaufruf.

4.4.4 Eigene Dashboards

Als **Administrator** klicken Sie in der linken Grafana-Seitenleiste auf **Dashboards** → **New** oder duplizieren das mitgelieferte Dashboard, um eigene Auswertungen zu bauen. Eigene Dashboards bleiben beim Firmware-Update erhalten — sie werden nicht durch das Repo-Seed überschrieben.

Fehlt Ihnen die Schaltfläche zum Speichern, sind Sie an der Bedienoberfläche nicht als Administrator angemeldet.

4.4.5 Ein eigenes Dashboard als Startseite

Welches Dashboard der Reiter **Grafana** öffnet, stellen Sie unter **Einstellungen** → **Seiten** → **Standardseiten** ein. Wählen Sie das Dashboard dort aus der **Liste** — sie zeigt genau die Dashboards, die auf dieser Anlage vorhanden sind.

Wenn Sie die Adresse stattdessen von Hand eintragen, achten Sie darauf, **welchen Teil** Sie kopieren:

```
/grafana-proxy/d/c10732a9-2e02-47cd-a033-059fb6f34344/idea-4s-dashboard-vwbaunatal  
      Kennung      Name
```

Grafana sucht das Dashboard **allein über die Kennung** und ersetzt den Namen dahinter beim Aufruf durch den eigenen. Eine Adresse mit dem Namen Ihres Dashboards und der Kennung eines anderen führt deshalb zum anderen Dashboard — sie wird gespeichert, sie funktioniert, sie zeigt nur etwas anderes. Kopien tragen oft sehr ähnliche Kennungen, die sich erst in den letzten Zeichen unterscheiden.

Die Bedienoberfläche prüft die eingetragene Adresse beim Speichern gegen die vorhandenen Dashboards und sagt Ihnen, wenn Kennung und Name zu zwei verschiedenen Dashboards gehören.



4.4.6 Wie oft die Anzeige aktualisiert wird

Das Aktualisierungsintervall stellen Sie in Grafana oben rechts neben der Zeitspanne ein. Die kürzeste Einstellung, die die Anlage zulässt, ist **eine halbe Sekunde**; angeboten werden 500 ms und 1 s allerdings nur von Dashboards, die diese Werte in ihrer eigenen Intervall-Liste führen — die ausgelieferten tun das.

Schneller als die Werte ankommen wird die Anzeige davon nicht. Über zwei Stunden auf einer Anlage gemessen, als Abstand zwischen zwei Werten (Median): Schwinggeschwindigkeit 0,1 s, Lager- und Kühlmitteltemperaturen 0,2 s — dort lohnt der Sekundentakt. Die Drehzahl kam nur alle 30 Sekunden, weil die Spindel stand: Der Sensor meldet bei Änderung, im Betrieb liegen auch hier 0,1 s zwischen zwei Werten.

Für ein flüssiges Bild bei einem Wert, der sich gerade nicht ändert, ist der Haken **Live-Dashboards aktualisieren** (in den Dashboard-Einstellungen) der bessere Weg — er lässt die Zeitachse durchlaufen, ohne die Abfragen häufiger zu stellen.

4.4.7 Wenn das Dashboard leer bleibt

Sehen Sie nur Achsen ohne Daten, ist meist die Datenquellen-Kette unterbrochen:

1. In **Einstellungen** → **Diagnose** prüfen, ob `datastore`, `postgres` und `mosquitto` grün sind.
2. In **IO-Link-Master-Konfiguration** → **Notification** prüfen, ob mindestens eine MQTT-Subscription auf `172.16.9.112:1883/teststand/idea-4s` steht (Beispiel-Topic).
3. Falls beides OK ist, aber Grafana trotzdem leer: kann ein bekannter „Gedächtnisverlust“-Fall sein — siehe interne Dokumentation oder kontaktieren Sie den Brinkhaus-Service.

4.5 Ressourcen-Anzeige

Unter **Einstellungen** → **Ressourcenüberwachung** sehen Sie auf einen Blick die Auslastung der Edge-Hardware. Die Werte werden direkt vom Betriebssystem (`psutil`) abgefragt; der Knopf **Aktualisieren** holt aktuelle Zahlen.

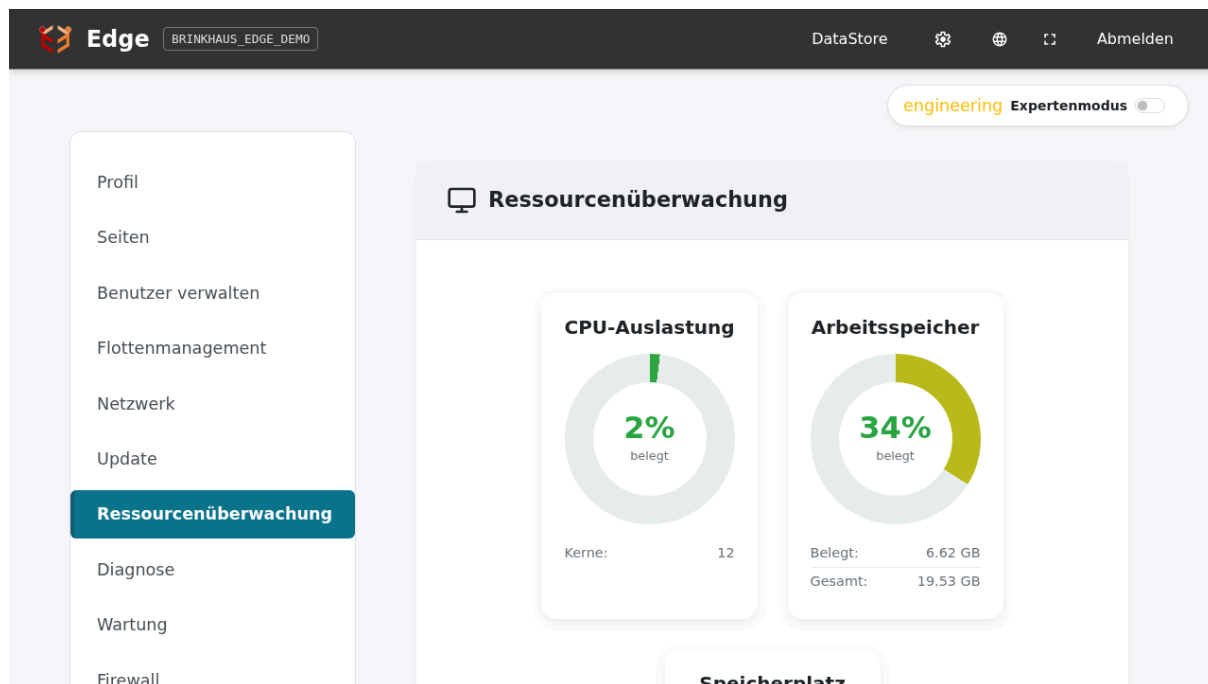


Abbildung 18: Ressourcenüberwachung mit drei Donut-Diagrammen

4.5.1 Was die drei Diagramme bedeuten

Anzeige	Bedeutung
CPU-Auslastung	Aktuelle Auslastung aller Prozessorkerne (Momentaufnahme). Der Wert „Kerne“ zeigt, wie viele Kerne die Edge hat.
Arbeitsspeicher	Belegter RAM gegenüber dem insgesamt verfügbaren. „Belegt“ und „Gesamt“ sind in MB / GB ausgegeben.
Speicherplatz	Belegung der internen SSD/eMMC. Die Edge-Firmware schreibt in der Regel nur Logs und gemessene Sensordaten — schnelles Wachstum bedeutet meist eine fehlkonfigurierte Anwendung.

4.5.2 Was sind „normale“ Werte?

Im Leerlauf bei laufender Messdatenerfassung:

- **CPU:** typisch 1–5 %. Spitzen beim Start oder während eines Updates sind normal.
- **Memory:** 15–25 %. Steigt langsam, weil Container-Caches voll werden — bis ~70 % unkritisch.
- **Disk:** 5–15 % je nach Laufzeit und Datenmenge. Pro Monat wachsen die Postgres-Daten um wenige hundert MB.

4.5.3 Wann sollten Sie reagieren?

- **CPU dauerhaft > 80 %:** meist eine Endlosschleife in einer FLECS-App oder in einem Custom-Dashboard. AppStore prüfen, App ggf. beenden.



- **Arbeitsspeicher > 85 %:** eine App leakt — die Edge wird sich selbst nicht abstürzen lassen, aber neue Container starten langsamer. Edge neu starten oder Brinkhaus-Service.
- **Speicherplatz > 90 %:** Logs aufräumen oder ältere Postgres-Tabellen prunen — Brinkhaus-Service kontaktieren, niemals selbst Dateien auf der Edge löschen.

4.5.4 Wo werden die Daten erfasst?

Die Werte stammen vom Betriebssystem der Edge selbst, nicht aus den Containern. Eine einzelne Anwendung mit hoher CPU verursacht hier den Anstieg, ohne dass Sie sehen, *welche* — dafür schauen Sie in **Einstellungen** → **Diagnose**, wo jeder Service einzeln gemeldet wird.

4.6 Fleet-Anbindung

4.6.1 Was es ist

Jede openXEdge ist ab Werk so vorbereitet, dass sie sich beim **FleetManager** meldet, sobald sie ins Internet kommt. Das ist die Grundlage für alles, was Sie aus der Ferne unterstützen lassen wollen — Fern-Diagnose, Update-Empfehlungen, Notfall-Reparatur.

4.6.2 Voraussetzungen

Damit es funktioniert, müssen drei Dinge gleichzeitig erfüllt sein:

1. **24 V Strom** an der Edge.
2. Eth2 (mittlerer Port) hängt an einem **DHCP-Server**, der eine Firmen-IP vergibt und Internet-Zugriff erlaubt — typisch ein Office-Switch hinter Ihrem Firmen-Router.
3. Die Edge hat ihre **Kennung**: Geräte mit Seriennummer bringen sie ab Werk mit; ältere Geräte bekommen ihre Maschinen-ID bei der Aktivierung (Kap. 1.2.5).

Sind alle Bedingungen erfüllt, schickt die Edge alle paar Minuten ein **Heartbeat** an den FleetManager mit Versionen, IP-Adressen und Selbstdiagnose. Brinkhaus-Personal sieht Ihre Edge dann in der zentralen Übersicht:

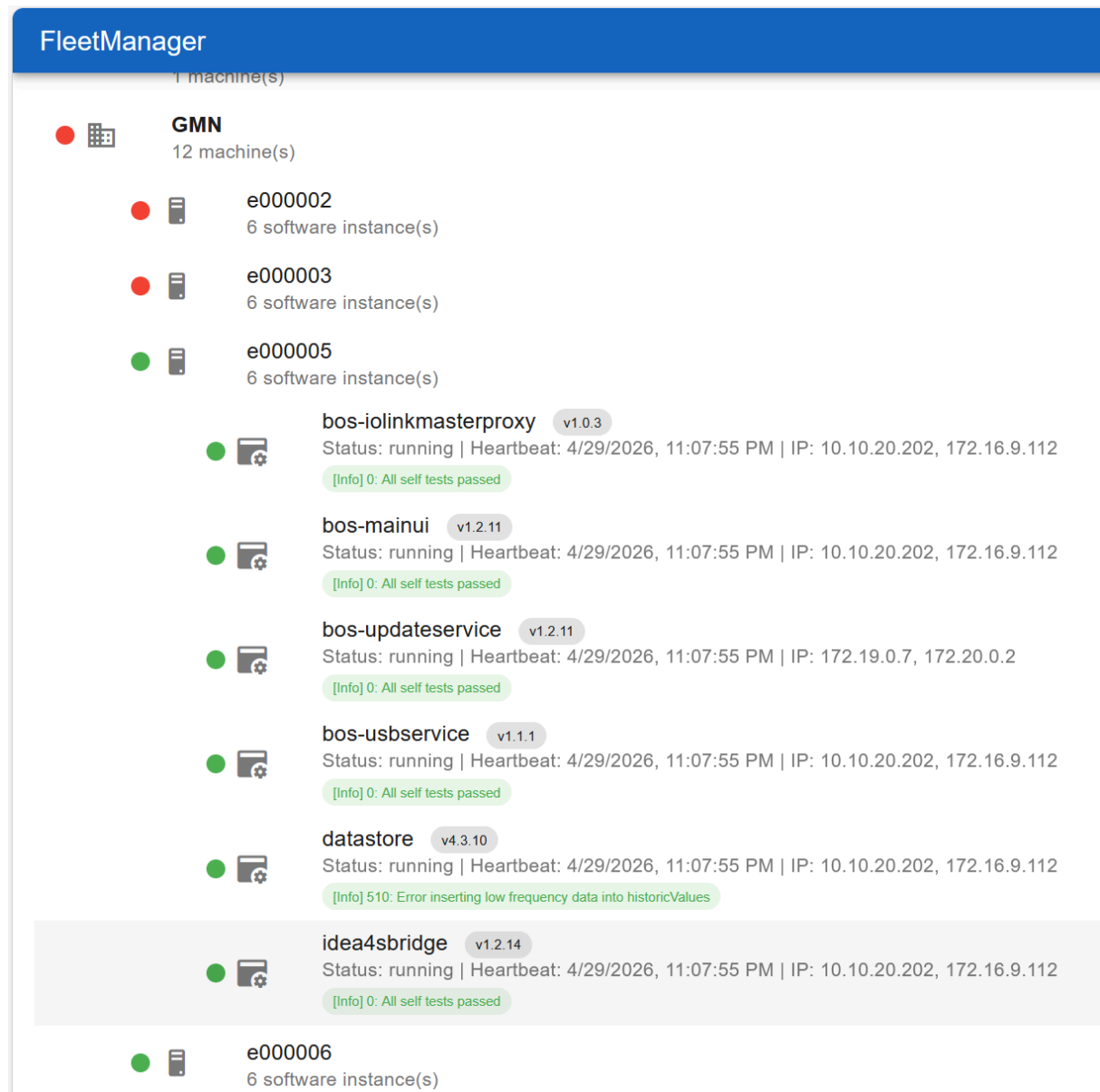


Abbildung 19: FleetManager mit Brinkhaus GmbH-Knoten und einer ausgeklappten Edge

4.6.3 Seriennummer, Geräte- und Inventarnummer

Jede neu ausgelieferte Edge trägt eine **Seriennummer** (z. B. SN00100); sie steht auf Etikett und Lieferschein. Unter dieser Nummer führt die Flottenverwaltung das Gerät. Die Seriennummer wird bei der Erstkonfektionierung vergeben und lässt sich auf der Edge nicht ändern — so bleibt ein Gerät in der Flotte immer dasselbe, auch wenn Sie es umbenennen oder an einen anderen Ort stellen.

Wie Sie das Gerät nennen, bestimmen Sie selbst, mit zwei freien Feldern:

- **Geräte-Name** — der Name, unter dem das Gerät in der Flottenverwaltung angezeigt wird (z. B. „Drehmaschine 1“). Umbenennen ändert nur die Anzeige; es entsteht kein zweites Gerät.



- **Inventarnummer** — Ihre eigene Inventar- oder Maschinennummer, damit Sie das Gerät in Ihren Unterlagen wiederfinden.

Beide Felder sind optional.

Ältere Geräte ohne Seriennummer werden weiter unter ihrer Maschinen-ID aus der Aktivierung geführt und behalten sie. Solange sie an die Flottenverwaltung angebunden sind, kann ihnen der Support dort nachträglich eine Seriennummer zuweisen. Maschinen-ID, Passwort und bisheriger Verlauf bleiben dabei erhalten; auf der Edge erscheint danach die Seriennummer statt des Felds **Maschine**.

4.6.4 Was Brinkhaus-Personal damit sehen kann

Pro Edge in der zentralen Sicht:

- **Status-Punkt** (grün/gelb/rot) — auf einen Blick, ob die Edge noch online ist und ob sie Probleme meldet.
- **Versionsstände** aller laufenden Container (bos-mainui, bos-updateservice, datastore, idea4sbridge, ...).
- **Letzter Heartbeat-Zeitpunkt** — wenn der älter als ein paar Minuten ist, ist die Edge offline oder hat keinen Internetzugriff mehr.
- **Alle aktuellen IP-Adressen** der Edge — hilfreich, wenn die Office-IP per DHCP wechselt.
- **Selbstdiagnose-Meldungen** — dieselben Codes, die Sie auch unter Diagnose lesen (Kap. 2.9) sehen.

4.6.5 Was die Edge selbst überträgt

Die Inhalte sind absichtlich knapp:

- Versionsstände, IPs, Heartbeat-Zeit, Selbstdiagnose-Codes.
- Seriennummer, Gerätename und Inventarnummer.
- Ob das Initialpasswort geändert wurde — **nie** das Passwort selbst (siehe Passwort ändern (Kap. 2.4)).
- **Keine** Sensormesswerte, **keine** Prozessdaten, **keine** persönlichen Daten.

Heißt: der FleetManager ist eine Wartungsebene für die Edge selbst, **nicht** ein Datenarchiv für Ihre Produktion. Ihre Messwerte bleiben in der Edge (und in dem, was Sie darüber per Datenexport aktiv hinausschicken).

4.6.6 Edge-seitig kontrollieren

Auf der Edge sehen Sie Ihren Anteil unter **Einstellungen** → **Flottenmanagement**:

- **Kundenname** — read-only, gibt an, zu welchem Kunden die Edge in der Flotte gehört.



- **Seriennummer** — read-only, nur bei Geräten mit Seriennummer. Sie identifiziert die Edge in der Flotte.
- **Maschine** — nur bei Geräten ohne Seriennummer: die Maschinen-ID aus der Aktivierung (Kap. 1.2.5), die diese Edge in der Flotte identifiziert.
- **Gerätename, Inventarnummer und Aufstellungsort** — frei wählbar.

Änderungen übernehmen Sie mit **Flottenmanagement-Einstellungen speichern**. In der Flottenverwaltung erscheinen Gerätename, Inventarnummer und Aufstellungsort erst nach dem nächsten Neustart des Geräts.

4.6.7 Wenn die Edge offline geht

In der zentralen Sicht (Bild oben) sind Edges, deren letzter Heartbeat zu lange her ist, mit einem **roten** Status-Punkt markiert (im Beispiel `e000002` und `e000003`). Brinkhaus-Personal sieht das sofort und meldet sich proaktiv — sofern die Edge an die Flottenverwaltung angebunden ist. Typische Ursachen sind ausgefallene Switches, vergessene Stromzufuhr oder ein Firmen-DHCP, der den Pool gewechselt hat.

4.6.8 Hilfe anfragen

Geben Sie der Hotline:

1. die **Seriennummer** (auf Etikett und Lieferschein, auf der Edge unter **Einstellungen** → **Flottenmanagement**) oder, bei älteren Geräten ohne Seriennummer, die **Maschinen-ID** (ebenda),
2. den groben Symptomsatz („Grafana leer“, „Update bricht ab“),
3. die zuletzt versuchte Aktion.

Ist die Edge an die Flottenverwaltung angebunden, kann die Hotline parallel die Diagnose im FleetManager mitlesen — meist ist das schon genug, um das Problem zu lokalisieren, ohne dass jemand vor Ort sein muss.

4.7 Sicherheit und Support

Diese Seite fasst zusammen, was Sie zum sicheren Betrieb der openXEdge wissen müssen: wohin Sie eine Sicherheitslücke melden, wie lange es Updates gibt, was bei Inbetriebnahme und Außerbetriebnahme zu tun ist, welche Netzwerk-Ports offen sind und welche Daten das Gerät verarbeitet.

4.7.1 Eine Schwachstelle melden

Wenn Ihnen an der openXEdge etwas auffällt, das ein Sicherheitsproblem sein könnte, melden Sie es bitte an:



security@brinkhaus-gmbh.de

Hilfreich ist alles, was das Nachstellen erleichtert: die Firmware-Version (steht in den Einstellungen unter **Update**), die Seriennummer (bei älteren Geräten die Machine-ID), was Sie getan haben und was dabei passiert ist.

Unsere Zusage. Wer uns gutgläubig auf eine Schwachstelle hinweist, hat von uns keine rechtlichen Schritte zu befürchten. Wir bestätigen den Eingang, halten Sie über den Stand auf dem Laufenden und nennen Sie auf Wunsch, wenn wir die Lücke schließen. Bitte geben Sie uns Zeit für eine Korrektur, bevor Sie Einzelheiten veröffentlichen.

Daran können Sie uns messen:

- Sie erhalten eine **Eingangsbestätigung binnen 5 Arbeitstagen**.
- Binnen **15 Arbeitstagen** sagen wir Ihnen, ob die openXEdge betroffen ist, wie schwer wir die Lücke einschätzen und wie wir vorgehen wollen.
- Einzelheiten veröffentlichen Sie bitte **frühestens 90 Tage nach Ihrer Meldung oder sobald die Korrektur ausgeliefert ist**, je nachdem, was früher eintritt.

Wenn Sie den Verdacht haben, dass eine Lücke bereits ausgenutzt wird, schreiben Sie das bitte ausdrücklich dazu — dafür gelten kürzere Fristen.

4.7.2 Wie lange es Sicherheitsupdates gibt

Brinkhaus stellt für die openXEdge ab Lieferung des einzelnen Geräts **fünf Jahre** lang Sicherheitsupdates für die Firmware und den mitgelieferten Container-Stack über den signierten Aktualisierungskanal bereit.

Dazu im Einzelnen:

- Der Zeitraum beginnt mit der **Lieferung Ihres Geräts**, nicht mit dem Marktstart des Produkts. Zwei Geräte können also unterschiedliche Enddaten haben.
- Bei einem **Gerätetausch** beginnt für das Ersatzgerät ein eigener Zeitraum.
- Umfasst sind die Firmware und die mitgelieferten Dienste. **Nicht** umfasst sind Anwendungen, die Sie selbst über den AppStore installieren — dafür gilt die Zusage des jeweiligen Anbieters.
- Die Zusage gilt für Firmware ab Version 2. Geräte auf dem alten Stand 1.1 sind davon ausgenommen und sollten umgestellt werden; sprechen Sie uns an.

4.7.3 Wie Sicherheitsupdates ankommen

Updates kommen über denselben Weg wie alle Firmware-Aktualisierungen: Sie wählen in den Einstellungen eine Version aus, die Edge lädt sie vom Update-Server und prüft vor der Installation die **digitale Signatur**. Passt sie nicht, wird nichts installiert. Schlägt die Installation fehl, kehrt die Edge selbsttätig auf den vorherigen Stand zurück.



Den Ablauf im Einzelnen beschreibt Wie Updates funktionieren (Kap. 4.3). Wenn Ihre Edge keine Verbindung zum Update-Server hat, geht es auch per USB-Stick (Kap. 2.2) — mit derselben Signaturprüfung.

Sicherheitsrelevante Änderungen kennzeichnen wir in den Versionshinweisen, die Sie vor der Installation lesen können.

4.7.4 Sichere Inbetriebnahme

Zwei Dinge sollten Sie gleich beim ersten Mal erledigen:

1. **Startpasswort ändern.** Jede Edge bekommt ein eigenes Startpasswort. Bei Geräten mit Seriennummer steht es auf dem Etikett bzw. Lieferschein und lässt sich aus der Seriennummer allein nicht ausrechnen. Bei älteren Geräten zeigt die Aktivierung es einmal an; es ist aus der Machine-ID abgeleitet und damit kein Geheimnis: Wer das Verfahren und die Machine-ID kennt, kann es nachrechnen. Ändern Sie es in beiden Fällen bei der ersten Anmeldung. Geräte mit Seriennummer verlangen das nach dem ersten Login mit dem Etikett-Passwort; ältere Geräte erzwingen es **nicht**. → Passwort ändern (Kap. 2.4)
2. **Eigene Benutzerkonten anlegen** statt gemeinsam ein Konto zu benutzen. Nur dann sagt das Protokoll hinterher, wer etwas geändert hat. Jedes Passwort, das jemand vergibt, muss der Passwortrichtlinie genügen (im Stream für GMN ab gmn-2.45.2), ab Werk mindestens 10 Zeichen. Ein Admin kann sie dort verschärfen. → Benutzer verwalten (Kap. 2.8)

Darüber hinaus setzt der sichere Betrieb voraus, dass die Edge **im geschützten Firmen- oder Anlagennetz** steht und **nicht aus dem Internet erreichbar** ist. Richten Sie keine Portweiterleitung auf das Gerät ein. Für den Fernzugriff gibt es den verschlüsselten Weg (Kap. 2.3).

4.7.5 Sichere Außerbetriebnahme

Wenn ein Gerät stillgelegt, zurückgegeben oder weitergegeben wird:

1. **Daten löschen.** Alle erfassten Messwerte, Einstellungen und Zugangsdaten liegen auf der eingebauten Platte. Eine Neuinstallation vom USB-Stick schreibt ein vollständiges Abbild auf diese Platte und überschreibt sie dabei. Muss der Datenträger **nachweislich rückstandsfrei** gelöscht werden — etwa bei Rückgabe an einen Dritten —, reicht das nicht aus; sehen Sie dann ein vollständiges Überschreiben oder die physische Zerstörung des Datenträgers vor. Wir unterstützen Sie dabei.
2. **Abmeldung aus der Flottenverwaltung anfordern.** Das Gerät kann sich nicht selbst abmelden. Schreiben Sie an security@brinkhaus-gmbh.de oder an Ihren Ansprechpartner; wir entfernen den Eintrag und die zugehörigen Protokolldaten.
3. **Zugänge prüfen.** Wenn Sie den Edge-Zugang in eigene Systeme eingetragen haben (etwa einen MQTT-Abgriff auf Port 1883), entfernen Sie diese Einträge.



4.7.6 Offene Netzwerk-Ports

Diese Ports sind im Auslieferungszustand von außen erreichbar. Alle anderen Dienste — Datenbank, Grafana, DataStore, Aktualisierungsdienst — sind **nur gerätintern** erreichbar und von außen nicht ansprechbar. Ab dem Softwarestand mit Wartungsdienst 1.22 (GMN: Firmware 2.45) sorgt dafür eine **Firewall auf dem Gerät**: Sie verwirft jede Verbindung auf einen Port, der nicht auf der Freigabeliste steht. Die Systemports 22, 5000, 5443 und 1883 können Sie selbst sperren, weitere Ports selbst freigeben — siehe Firewall konfigurieren (Kap. 2.7).

4.7.6.1 Ihre Produktfunktionen

Port	Wofür	Anmerkung
5000/tcp	Bedienoberfläche, unverschlüsselt	Auch der Kiosk-Bildschirm nutzt ihn
5443/tcp	Bedienoberfläche, verschlüsselt	Empfohlener Weg; Zertifikat von der geräteeigenen Edge-CA oder Ihrer Firmen-CA, siehe Fernzugriff (HTTPS) (Kap. 2.3).
8050/tcp	IDEA-4S-Bridge	Aus dem Netz durch die Firewall gesperrt; gedacht für die Anwendungen auf dem Gerät. Wer lesen und wer schreiben darf, entscheidet der Dienst zusätzlich anhand der Absenderadresse.
8082/tcp	IO-Link-Relais	Aus dem Netz durch die Firewall gesperrt, bis Sie es für einen DataStore außerhalb der Edge per Regel öffnen; das Relais prüft die Absenderadresse zusätzlich gegen seine Freigabeliste.
1883/tcp	MQTT-Broker	Ohne Anmeldung und ohne Verschlüsselung. Wer den Port erreicht, kann alle Messwerte mitlesen und eigene einspeisen. Die Schnittstelle ist bewusst offen, damit Ihre eigenen Systeme mitlesen können — sie gehört deshalb in ein geschütztes Netz.

4.7.6.2 Dienste des Basissystems

Port	Wofür
22/tcp	Wartungszugang für den Brinkhaus-Service, Anmeldung nur mit Schlüssel

Diese Dienste des Basissystems laufen auf dem Gerät, sind aber von außen **durch die Firewall gesperrt**; sie werden nur gerätintern gebraucht:

Port	Wofür
80, 443/tcp	Verteiler des AppStores auf die installierten Anwendungen — die Bedienoberfläche bindet den AppStore über ihren eigenen Port ein.
8951/tcp	AppStore-Dienst.
8085/tcp	Selbstdiagnose des Sicherheits-Agenten, gelesen von der Bedienoberfläche.



Port	Wofür
631/tcp	Druckdienst. Er kommt als Beipack des Kiosk-Browsers mit und wird für den Betrieb der Edge nicht benötigt

Anwendungen aus dem AppStore öffnen eigene Ports. Auch die sind von außen gesperrt, bis Sie sie in der Firewall freigeben; über die Bedienoberfläche der Edge erreichen Sie die Anwendungen ohne Freigabe. Vor dem Wartungsdienst 1.22 (GMN: Firmware 2.45) gab es die Firewall nicht — auf solchen Geräten sind die hier als gesperrt genannten Ports offen.

4.7.7 Welche Daten die Edge verarbeitet

Auf dem Gerät liegen die Messwerte Ihrer Sensorik und Maschinen, die Einstellungen und die Benutzerkonten der Bedienoberfläche. Wie lange Messwerte aufbewahrt werden, stellen Sie selbst ein.

An die Flottenverwaltung gehen ausschließlich Betriebsdaten: Versionsstände, IP-Adressen, der Zeitpunkt des letzten Lebenszeichens, Selbstdiagnose-Codes, Seriennummer, Geräte- und Inventarnummer sowie ob das Startpasswort geändert wurde (nie das Passwort selbst). **Keine** Sensormesswerte, **keine** Prozessdaten, **keine** personenbezogenen Daten. Die Verbindung geht immer von der Edge nach außen; von außen wird kein Port geöffnet.

Mehr dazu: Anbindung an die Flotte (Kap. 4.6).

4.7.8 Was das Produkt ist und wogegen es geschützt ist

Die openXEdge dient der **Zustandsüberwachung** von Fertigungsmaschinen. Die Edge erfasst Sensor- und Prozesswerte, speichert sie und stellt sie dar. Sie **steuert die Maschine nicht** und ist kein Teil einer Sicherheitskette.

Wir schützen dabei vier Dinge, in dieser Rangfolge:

1. **Die Erfassung läuft weiter** — auch wenn das Netz ausfällt, ein Stecker gezogen wird oder ein Dienst abstürzt.
2. **Auf das Gerät kommt nur unsere Software** — jede Aktualisierung ist signiert und wird vor der Installation geprüft.
3. **Zugangsdaten bleiben auf dem Gerät.**
4. **Eingriffe sind nachvollziehbar** — An- und Abmeldungen und Änderungen werden protokolliert.

Wo Verfügbarkeit und Härting in Konflikt geraten, gewinnt die Verfügbarkeit: Ein Gerät, das nicht mehr misst, nützt in der Fertigung niemandem. Diese Abwägungen sind schriftlich festgehalten und begründet.

Stückliste der Software (SBOM). Zu jeder ausgelieferten Version führen wir eine vollständige Liste aller enthaltenen Software-Bestandteile im CycloneDX-Format. Sie bekommen sie auf Anfrage an



security@brinkhaus-gmbh.de innerhalb von zehn Arbeitstagen; nennen Sie dabei bitte die Firmware-Version Ihres Geräts.

Konformitätserklärung. Die Lieferantenerklärung zu Ihrem Gerät finden Sie als eigene, druckbare Seite in dieser Dokumentation.

Die vollständige EU-Konformitätserklärung und die technische Dokumentation stellen wir auf Anfrage bereit.

Version 2026.10.21

Datum: 10.2026

© 2026 Brinkhaus GmbH, Isernhagen



Brinkhaus GmbH

Schneekoppenweg 6
30916 Isernhagen

Support

E-Mail: edge-support@brinkhaus-gmbh.de