THE REQUEST

Secured remote ad-hoc support when the machine stops.

When a machine stops, your equipment supplier needs access on short notice: usually to diagnose the fault in the machine's programming software, sometimes to a machine with no running operating system. This brief describes how that access works using BifrostConnect and what your site is asked to approve.

1 Reaching machines that have no operating system

Direct Native Access is a browser console straight to the hardware: pre-OS, BIOS and serial. For faults diagnosed in the programming software, Direct Tunnel Access opens a tunnel scoped to that machine and time-bound to that session.

2 Zero supplier access left behind

The unit is carried in for the job and unplugged after it. No appliance on your network to inventory, patch, scan or defend, no account to deprovision, and nothing to decommission in three years.

3 Your network is not part of the deployment

The unit has its own built-in 4G/LTE connection. No firewall change, no VLAN, no address, no route and no change request: you are approving a device at one machine, not a change to your infrastructure.

The Manager
Central control: Your approval, Your time limit, Your audit trail.

YOUR SITE
OT network, unchanged

The stopped machine
PLC, drive or engineering station

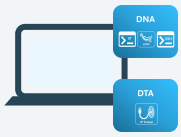
HDMI / USB / Ethernet / serial

Bifrost Unit
Carried in, plugged in, unplugged again

Outbound only, port 443

No inbound path

OUTSIDE
Your supplier's engineer



Two ways in
Both brokered by the Manager

Closed by default. The unit calls out and never receives. Between sessions there is no path into your network.

You are approving

- ✓ One session per stoppage, on a named machine.
- ✓ Console access that works with no operating system running: pre-OS, BIOS and serial.
- ✓ A scoped, time-bound tunnel only where the fault needs IP.
- ✓ A named engineer your site approves for that session.
- ✓ A complete audit record of every session: who, what, when and for how long.

Not part of the request

- ✗ A standing account or a supplier identity in your directory.
- ✗ Inbound ports, firewall changes or perimeter rules.
- ✗ Software agents on your network.
- ✗ A connection to your network. The unit has a built-in 4G/LTE uplink.
- ✗ An always-on link. Unplug the unit and access is gone.

SECURITY BRIEF

Technical facts
for your IT security review.

The unit connects to the equipment by HDMI, USB, Ethernet or serial, and every session is authorized by the BifrostConnect Manager. Access exists only for the duration of that session, scoped to the endpoints you approve.

IDENTITY AND ACCESS CONTROL

- Operator identity via Auth0 (SOC 2 Type 2, ISO 27001 / 27018).
- Mandatory multi-factor authentication on every interactive session, no opt-out.
- Role-based access control with group scoping; just-in-time and time-bounded policies.

CRYPTOGRAPHY

- TLS 1.2 minimum, TLS 1.3 supported, AEAD ciphers only (AES-GCM, ChaCha20-Poly1305).
- Console sessions: DTLS-SRTP end to end. Tunnel sessions: WireGuard with ChaCha20-Poly1305, Curve25519, BLAKE2s.
- Relays forward ciphertext only. No production data is stored in, or readable from, the cloud.

NETWORK

- Outbound TCP/443 only; no inbound ports or firewall rules required.
- Optional out-of-band path: built-in LTE / 4G modem, independent of your network.
- No changes to your network, no software on your OT endpoints, no persistent connection.

DATA RESIDENCY

- EU-region cloud service.
- Manufactured and supported from Denmark. GDPR-aligned, DPA available.

HARDWARE POSTURE

- Hardened industrial embedded Linux, stripped to the BifrostConnect service only.
- Signed firmware, updated only over the air, with atomic A/B rollback.
- No listening services, no local users, no SSH, no local administration interface, no physical debug ports.
- Cannot boot from alternative storage; unique, revocable device keys.

CERTIFICATION AND ASSURANCE

- RED 2014/53/EU: EN IEC 62368-1:2020, EN IEC 62311:2020 / EN 50665:2017, EN 18031-1:2024.
- Independent penetration tests by Nixu, ICS Range and Devoteam.
- Compliance documentation available under NDA.

MAPS TO

- IEC 62443-2-1 NET 3.2 and 3.3, USER 1.9. IEC 62443-3-3 SR 2.1, SR 2.6, FR 6.
- NIS2 Article 21(2)(d), 21(2)(j) and 21(3). NIST SP 800-207 tenets 3 and 6.
- Aligned with NIS2, IEC 62443, CRA, CER and BEK 260.

Contact us for any further questions or need for clarification: sales@bifrostconnect.com