SECURE REMOTE MAINTENANCE!

Around 70% of operators and OEMs still neglect regular patching.

Remote access, firewalling, and data access—transparent, documented, and scalable. Patching, updating, securing—standardized, plannable, and audit-proof.

Why secure remote maintenance?

Secure remote maintenance makes production service both accepted and scalable. Instead of 'just VPN,' you get explicit on-device approvals, transparent logs, and outbound-only connections that comply even with strict IT policies. Technicians work directly in the browser—no extra client—while roles, evidence, and reports simplify audits. Whether it's a single machine or a global rollout: the same portal, the same principles, with your choice of cloud or on-prem. With security by design, patching becomes plannable, access is traceable—and your systems stay online, but under control.

MB CONNECTLINE

Top 10 reasons for secure remote maintenance with MB Connect Line products:

- **On-site authorization:** Remote access only when the key allows it—visible, traceable, and accepted.
- **Outbound-only connections:** No open ports in the plant—significantly reducing the attack surface.
- **Fully documented:** Who, when, how long, and for what—tamper-proof audit logs and reports.
- **Roles over sprawl:** Fine-grained permissions down to device, port, and protocol.
- **Patching becomes plannable:** Automate tasks, generate evidence—closing gaps consistently.
- **Browser-based access:** RDP, VNC, HTTP/HTTPS, and SSH directly via mbWEB2go—no client needed.
- **Security by design:** Secure Boot, Secure Element, and signed firmware included by default.
- **Multi-tenant:** Clean separation of plants, lines, and service providers—ideal for corporate structures.
- **Cloud or on-prem:** Operate according to compliance requirements—with flexible switching and scalability.
- **IIoT-ready:** OPC UA, Modbus, MQTT, and Node-RED—data flows without DIY workarounds.

CONSOLIDATED INFORMATION—A FOUNDATION FOR EFFICIENCY AND SUCCESS

ypical use cases

- **Remote maintenance & programming:** TIA Portal, Step7, TwinCAT, RSLogix—'as if on site' via VPN.
- **Patching & updates:** Central maintenance windows with task scheduler and approvals.
- **Remote diagnostics & support:** Temporary REM approvals, fully documented and traceable.
- **Data access & IIoT:** OPC UA/Modbus/MQTT, Node-RED flows, and cloud connectivity.

Facts and figures:

- **VPN:** OpenVPN/IPsec
- **Connectivity:** LTE EU/US (bands by type), Wi-Fi 2.4 GHz 802.11 b/g/n
- **I/Os:** typ. 4× DI, 2× DO (galv. getrennt) bei HW06
- **Seriell/Fieldbus:** RS-232/485, MPI/PROFIBUS (Optionen)
- **nstallation/environment:** DIN rail, IP30, −40…+75°C (by type)
- **Compliance:** CE, UL (model-dependent), EU/UKCA conformity
- **Operation:** Cloud oder On-Prem (mymbCONNECT24.virtual)

Device overview:

mbNET (HW06):
- mbNET (HW06): 4x LAN, 1x WAN, 4x DI, 2x DO, USB; options: RS-232/485, MPI/PROFIBUS, LTE/Wi-Fi.
- OpenVPN/IPsec
- Typical temperature range −40…+75°C, DIN rail, IP30.

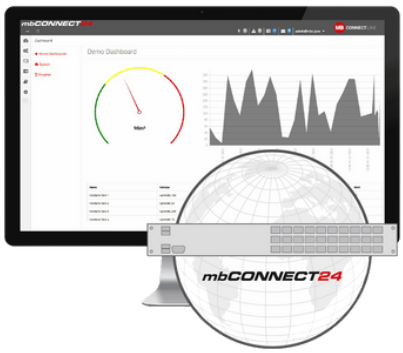
mbNET.rokey (HW06):
- Like mbNET, plus a physical key switch with OFF/ONL/REM (recommended by BSI/ENISA).
- Explicit on-site authorization: Internet can be physically disconnected; remote access only in REM mode.

mbNET.mini (HW02/03):
- Kompakt, 3–4× LAN, 1× WAN; Optionen LTE/WLAN; OpenVPN (typ. 1 tunnels).For machines/M2M access—cost-efficient and quick to integrate.

Note: Exact interfaces and temperature ranges per type/variant as specified in the technical datasheets.

Core elements:

- **Router family:** mbNET, mbNET.rokey, mbNET.mini—from control cabinet to compact edge.
- **Portal:** (my)mbCONNECT24—VPN server, multi-tenant, roles, reporting, alerting, mbWEB2go (RDP/VNC/HTTP/SSH)
- **Security by design:** Secure Boot, Secure Element, signed firmware, stateful firewall, 802.1x/SNMPv3 (model-dependent).
- **IIoT options:** Node-RED, OPC UA/Modbus/MQTT, Docker/Portainer (license-dependent).



Request your proof of concept now and test our remote maintenance solution directly in your own environment—with optional hands-on support

Industrial Automation GmbH
AT-6020 Innsbruck
Technikerstraße 1 - 3

Tel.: +43 512 27 22 71-00
office@automation.team

Industrial Automation Suisse GmbH
CH-8808 Pfäffikon SZ
Churerstraße 16

Tel.: +41 55 56 002-00
office.ch@automation.team

Büro Italien
IT-39032 Campo Tures
Via Unterwalburgen 15B

Tel.: +39 0474 86 93 00-30
office@automation.team

www.scada.online