datacentrix

Operational Technology

Secure Remote Access

Confidential
This document is confidential and intended for the use of the distribution parties only. Any copying or dissemination of this document is strictly prohibited.
© 2026 Datacentrix (Pty) Ltd

Remote access to operational systems is now unavoidable. Vendors, integrators, engineers and OEMs require access to industrial environments to maintain uptime, resolve incidents and support modern operations. The risk is not remote access itself; the risk is uncontrolled, unmonitored and permanently open access pathways into production systems.

In many organisations, remote access has evolved organically:

- VPNs shared across teams;
- Jump hosts with excessive privileges;
- Vendor accounts that are never revoked; and
- Limited visibility into who accessed what, when and why.

This creates latent operational and liability risk that only becomes visible after an incident.

1. OT Reality: Why IT Virtual Private Networks (VPNs) Are Not Enough

Traditional IT remote access tools were not designed for operational environments where:

- Systems cannot tolerate scanning or disruption;
- Safety systems must remain isolated;
- Engineers require protocol-level access; and
- Regulatory traceability is mandatory.

OT secure remote access respects these constraints while still enabling speed and efficiency.

2. A Modern, Identity-Centric Model for OT Secure Remote Access

Imagine an OT environment where access to engineering applications and control systems is delivered through a secure, browser-based portal, without the need for traditional VPNs, jump hosts, or direct network exposure to the industrial environment. In this model, access is granted to assets and applications, not to networks.

Engineers, operators and external original equipment manufacturers (OEMs) are authenticated through a central identity platform and presented only with the specific engineering tools or control interfaces they are authorised to use. They never gain visibility of the underlying network, operating system, or infrastructure supporting those assets.

2.1 Identity linked directly to industrial assets

Access is governed through identity-to-asset mapping, where each user is explicitly authorised to interact with defined systems, applications, or functions. This removes broad network access and replaces it with precise, purpose-driven connectivity.

As a result:

- There is no lateral movement across the OT network;
- Compromise of one user or supplier does not expose adjacent systems; and
- Access paths are reduced to the absolute minimum required.

This approach fundamentally alters the OT risk profile by eliminating the attack surface created by flat VPN access and shared jump environments.

2.2 Elimination of credential exposure

External vendors and OEMs never receive local usernames or passwords for programmable logic controllers (PLCs), human-machine interfaces (HMIs), or engineering workstations. Authentication is performed centrally using enterprise identity services, such as active directory or secure remote access (SRA) credentials, enforced with multi-factor authentication.

The underlying system credentials remain:

- Hidden;
- Rotated centrally; and
- Never shared outside the organization.

This significantly reduces supply-chain risk and prevents credential reuse across customers or environments.

2.3 Built-in security and accountability

Every remote session is:

- Explicitly approved;
- Time-bound; and
- Fully logged and auditable.

All actions are recorded, providing a defensible audit trail that supports regulatory compliance, forensic investigation and vendor accountability. Access can be revoked instantly without touching the OT system itself.

3. Fortify Your Operational Resilience

Contact our industrial OT specialists today to discuss how we can implement secure remote access solutions to elevate your risk management and control. Email Karina Geyser, Business Unit Manager: Infrastructure Solutions and Operational Technology at Datacentrix on kgeyser@datacentrix.co.za.

4. National Contact Details

Corporate office
Tel: +27 87 741 5000

Corporate Park North
238 Roan Crescent, 1685
Old Pretoria Road, Midrand

PO Box 50722
Randjiesfontein
Midrand, 1683

Logistics centre
Tel: +27 12 657 5000

26 Landmarks Avenue
Kosmosdal, Extension 11
Samrand, Midrand

PO Box 50722
Randjiesfontein
Midrand, 1683

Coastal

Cape Town office
Tel: +27 21 529 0700

18 Oxbow Crescent
The Estuaries
Century City, 7441

PO Box 181
Century City
Cape Town, 7446

East London office
Tel: +27 43 705 8000

Suite 2, 11 Cavendish Road
Vincent
East London, 5217

PO Box 19066
Tecoma
East London, 5214

Gqeberha office
Tel: +27 41 391 0200

Southern Life Gardens
Ground Floor, Block B, 70 2nd Avenue
Newton Park, Gqeberha

PO Box 63657
Greenacres, 6057

Durban office
Tel: +27 31 389 0500

1st Floor, 30A The Boulevard
Dawncliffe, Westville
Durban, 3629

PO Box 1645
Westville, Durban, 3630

Middle East

Doha office
Tel: +974 4007 1793

Eighteen Tower
Zone 69, Street 303, Building 230
19th Floor, Office 1972
Lusail, Doha, Qatar
PO Box 23107

Rest of Africa

Datacentrix deploys technologies and provides support services to customers across 45 countries in the rest of Africa.

www.datacentrix.co.za