Secure Remote Access

Implementing Safe Remote Connectivity to Industrial Systems

OT Security Learning Series

Document 301 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Remote access to OT environments is increasingly necessary for operations, maintenance, and vendor support. However, improperly implemented remote access has been the entry point for numerous high-profile attacks on industrial systems.

Critical

Remote access was the attack vector in the Ukraine power grid attacks (2015/2016). Attackers used hijacked VPN credentials to access SCADA systems and open circuit breakers remotely.

1.1 Business Drivers

- **Centralized operations:** Monitor multiple sites from control center
- **Vendor support:** Third-party maintenance and troubleshooting
- **Expert access:** Specialists supporting remote facilities
- **Emergency response:** After-hours incident support

Warning

Every remote access connection is a potential attack path. The convenience must be balanced against the risk of unauthorized access to critical systems.

2 Architecture Principles

2.1 Key Requirements

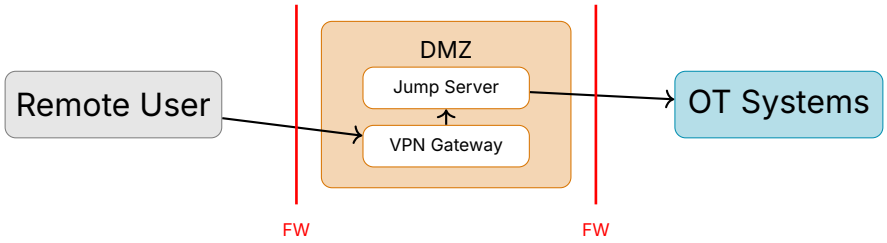
Key Point

Secure remote access must provide:

1. **Strong authentication:** Multi-factor, not just passwords
2. **Encrypted transport:** Protect data in transit
3. **Access control:** Limit what users can reach
4. **Session monitoring:** Record and audit all activity
5. **Controlled entry point:** Single, monitored gateway

2.2 DMZ-Based Architecture

Remote access should terminate in the Industrial DMZ, never directly into OT:



3 Key Components

3.1 Jump Servers (Bastion Hosts)

Jump Server Functions

- **Single entry point:** All remote sessions pass through
- **Session brokering:** Connects users to authorized systems
- **No direct OT access:** Users cannot bypass the jump server
- **Hardened system:** Minimal services, fully patched

3.2 VPN Technologies

Type	Considerations
IPsec	Strong encryption, complex configuration, site-to-site or client
SSL/TLS VPN	Easier deployment, browser-based options, client-based
WireGuard	Modern, lightweight, good performance

3.3 Multi-Factor Authentication (MFA)

- **Something you know:** Password, PIN
- **Something you have:** Hardware token, mobile app, smart card
- **Something you are:** Biometrics (less common in OT)

Tip

MFA is essential for remote access. Password-only authentication is insufficient—stolen credentials were used in the Ukraine attacks.

4 Access Control

4.1 Principle of Least Privilege

- **Role-based access:** Define roles with specific permissions
- **System-level restrictions:** Limit which systems each role can access

- **Time-based access:** Restrict access to business hours or maintenance windows
- **Purpose-specific accounts:** Separate accounts for different functions

4.2 Vendor Access Management

> **Warning**
>
> **Third-party access requires additional controls:**
> - Dedicated vendor accounts (no shared credentials)
> - Access enabled only when needed, disabled by default
> - Explicit approval workflow for each session
> - All sessions monitored and recorded

5 Monitoring and Audit

5.1 Session Recording

- **Video recording:** Capture screen activity for review
- **Keystroke logging:** Record commands entered
- **File transfer logging:** Track all files moved
- **Retention:** Store recordings per compliance requirements

5.2 Real-Time Monitoring

- **Active session visibility:** See who is connected now
- **Anomaly detection:** Alert on unusual activity patterns
- **Session termination:** Ability to kill suspicious sessions
- **Geographic restrictions:** Block access from unexpected locations

5.3 Audit Trail

- **Authentication logs:** All login attempts (success and failure)
- **Authorization logs:** Access requests and approvals
- **Activity logs:** Actions performed during sessions
- **Log integrity:** Protect logs from tampering

6 Common Mistakes

Critical

Remote access security failures:

- **Direct VPN to OT:** Bypassing DMZ and jump servers
- **Shared credentials:** Multiple users with same account
- **No MFA:** Password-only authentication
- **Always-on access:** Vendor connections left enabled
- **No monitoring:** Sessions not recorded or reviewed
- **Forgotten access:** Former employees/vendors still enabled

7 Implementation Checklist

Key Point

Secure remote access checklist:

- ☐ Remote access terminates in DMZ, not directly in OT
- ☐ Jump server required for all OT system access
- ☐ Multi-factor authentication enforced
- ☐ Role-based access control implemented
- ☐ All sessions recorded and logged
- ☐ Vendor access disabled by default, enabled per-request
- ☐ Regular access reviews conducted
- ☐ Incident response plan includes remote access scenarios

8 Further Reading

Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security (Chapter 5)
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443-3-3** – System Security Requirements
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Resources

- **CISA** – Remote Access Guidance
  https://www.cisa.gov/resources-tools/resources

- **SANS ICS** – Securing Remote Access
  https://www.sans.org/blog/