


VPN Security in Industrial Automation and Control Systems

Risks of Misconfiguration and Misuse, and Mitigation Measures Based on IEC 62443

Revision 1.0

Table of Contents

1. Overview 3

 1.1 Change History 3

 1.2 Purpose 3

 1.3 Definitions 3

 1.4 Abbreviations 4

 1.5 References 4

2. Threat Landscape: VPN in Industrial Environments 5

 2.1 Common VPN Vulnerabilities in IACS Contexts 5

 2.1.1 Outdated and Vulnerable VPN Gateway Software 5

 2.1.2 Weak or Shared Authentication Credentials 5

 2.1.3 Insufficient Network Segmentation and Overly Broad Access 5

 2.1.4 Permanent VPN Tunnels to Third-Party Sites 6

 2.1.5 Missing Session Control, Monitoring, and Audit Logging 6

 2.1.6 Insecure Cryptographic Configuration 6

 2.1.7 Application-Level Protocol Exposure 6

3. IEC 62443 Requirements and Mitigation Measures 7

 3.1 Zone and Conduit Model (IEC 62443-3-2) 7

 3.2 Identification, Authentication, and Access Control (SR 1.1, SR 1.2, SR 2.1) 7

 3.3 Session Control and Audit Logging (SR 2.6, SR 2.8, SR 3.2) 7

 3.4 On-Demand Access and Temporary Credentials 8

 3.5 Cryptographic Strength and VPN Gateway Hardening 8

 3.6 Application-Level Controls Beyond the VPN 8

4. Security Level Mapping 9

5. Audit Checklist 10

 5.1 Architecture and Network Design 10

 5.2 Authentication and Identity Management 10

 5.3 Session Control and Monitoring 10

 5.4 Cryptography and Patch Management 11

6. Conclusion 11

ANNEX 12

 A: Reference Architecture Diagram (Descriptive) 12

1. Overview

1.1 Change History

Version	Date	Author	Change Description
1.0	2026-02-23	M. Steinmetz	Initial version

1.2 Purpose

This document analyzes the risks arising from insecure VPN configurations and operational practices in Industrial Automation and Control Systems (IACS). It describes common vulnerability patterns, explains their potential impact on industrial operations, and provides guidance on how to mitigate these risks by applying the requirements defined in the IEC 62443 standard series. The document is intended for security engineers, system integrators, operators of IACS environments, and auditors assessing the security posture of industrial remote access solutions.

1.3 Definitions

Term	Definition
IACS	Industrial Automation and Control System: a collection of personnel, hardware, software and policies involved in the operation of an industrial process.
VPN	Virtual Private Network: an encrypted communication tunnel established over an untrusted network such as the Internet.
Conduit	As defined in IEC 62443-3-3: a logical grouping of communication channels that share the same security characteristics.
Zone	A logical or physical grouping of assets that share the same security requirements and policies (IEC 62443-3-2).
DMZ	Demilitarized Zone: a network segment placed between two firewalls that separates trusted internal networks from untrusted external networks.
Jump Host	A hardened, monitored server in a DMZ used as the sole access point for remote operators before connecting to production assets.
PAM	Privileged Access Management: a set of processes and tools for controlling and monitoring access by privileged users and service accounts.
SL	Security Level: a measure of confidence that an IACS zone or conduit is free from vulnerabilities (IEC 62443-3-3).

1.4 Abbreviations

Abbreviation	Meaning
ACL	Access Control List
CSMS	Cybersecurity Management System
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
IAM	Identity and Access Management
ICS	Industrial Control System
MFA	Multi-Factor Authentication
OT	Operational Technology
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
RBAC	Role-Based Access Control
SCADA	Supervisory Control and Data Acquisition
SL	Security Level
TLS	Transport Layer Security

1.5 References

Reference	Description
[IEC 62443-2-1]	IEC 62443-2-1:2010 - Security for industrial automation and control systems - Establishing an industrial automation and control system security program
[IEC 62443-3-2]	IEC 62443-3-2:2020 - Security risk assessment for system design
[IEC 62443-3-3]	IEC 62443-3-3:2013 - System security requirements and security levels
[IEC 62443-4-2]	IEC 62443-4-2:2019 - Technical security requirements for IACS components
[NIST SP 800-82]	NIST Special Publication 800-82 Rev. 3 - Guide to OT Security
[CISA ICS-CERT]	CISA Alerts and Advisories on ICS vulnerabilities, accessible at cisa.gov

2. Threat Landscape: VPN in Industrial Environments

Virtual Private Networks are a common and often indispensable technology for enabling remote access to Industrial Automation and Control Systems. Maintenance engineers, OEM service technicians, system integrators, and internal support staff routinely rely on VPN tunnels to perform diagnostics, apply patches, or carry out remote commissioning of IACS components. While VPN technology itself is a well-established security measure, the specific challenges of industrial environments frequently lead to configurations and operational practices that introduce serious vulnerabilities.

Unlike IT environments, IACS deployments operate under fundamentally different constraints. Availability and process continuity take precedence over security updates. Maintenance windows are rare and costly to arrange. Legacy components with decades-long lifecycles run protocols that were never designed with security in mind. These factors combine to create an environment where a VPN tunnel is often the last — and sometimes the only — security control standing between the open Internet and a production process.

When a VPN is misconfigured or misused in this context, the consequences extend far beyond a data breach. Unauthorized access to a SCADA system or programmable logic controller (PLC) can result in production shutdowns, damage to machinery, safety incidents, or in critical infrastructure sectors, threats to human life and public safety.

2.1 Common VPN Vulnerabilities in IACS Contexts

2.1.1 Outdated and Vulnerable VPN Gateway Software

VPN gateways are by definition internet-facing and represent one of the most attractive attack targets in any IACS environment. High-severity CVEs affecting major vendors — including Fortinet (CVE-2022-42475, CVE-2024-21762), Ivanti/Pulse Secure (CVE-2023-46805), and Cisco ASA — have been actively exploited in attacks against industrial operators. Because patching an IACS-connected VPN gateway often requires a maintenance window and involves risk to production continuity, these systems frequently remain unpatched for extended periods. An exploited VPN gateway grants an attacker direct access to the network segment it protects, potentially bypassing all other security controls.

2.1.2 Weak or Shared Authentication Credentials

In many industrial installations, VPN access for third-party maintenance is based on a single shared username and password distributed to all technicians of a given vendor. This approach violates the principle of individual accountability and makes it impossible to trace which person made specific changes during a remote session. Furthermore, such credentials are rarely rotated — they persist for years and continue to be valid after individual technicians have left the service provider. If the credentials are leaked, for example through a phishing attack on the vendor, the attacker gains the same level of access as any legitimate maintenance engineer. Single-factor authentication based on a simple password provides little resistance against credential stuffing and brute-force attacks targeting internet-exposed VPN gateways.

2.1.3 Insufficient Network Segmentation and Overly Broad Access

A VPN tunnel terminates at a network layer. Where it terminates and how much of the network is accessible from that termination point is a critical architectural decision. In many industrial installations, VPN tunnels terminate directly in the OT network or in a poorly segmented flat network, granting authenticated remote users

unrestricted Layer-3 access to all IACS components. This means that a single compromised VPN account provides lateral movement across PLCs, HMIs, engineering workstations, and historian servers without any further access control barrier. There is no need for the attacker to escalate privileges or pivot through additional systems — all assets are immediately reachable.

2.1.4 Permanent VPN Tunnels to Third-Party Sites

Many IACS operators maintain permanent site-to-site VPN tunnels to their machine builders, system integrators, or OEM service centers. The rationale is operational convenience: service requests can be addressed without delay because the tunnel is always available. However, a permanently active VPN tunnel is a permanently open attack surface. If the remote site — a vendor's office network — is compromised, the attacker inherits access to the industrial operator's network through the existing tunnel. This supply chain attack vector has been demonstrated in several real-world incidents and represents a severe risk that is often underestimated.

2.1.5 Missing Session Control, Monitoring, and Audit Logging

Remote sessions through a VPN give maintenance personnel direct access to sensitive IACS components. Without session monitoring and recording, there is no way to verify what actions were taken during a session, whether those actions were authorized, or whether a session was conducted by the legitimate user or an attacker. This absence of accountability makes forensic investigation of security incidents extremely difficult and means that unauthorized changes to IACS configurations may go undetected for extended periods. Even where logging is technically possible, many OT environments lack centralized log management and have no defined retention policy aligned with security requirements.

2.1.6 Insecure Cryptographic Configuration

Some deployed VPN solutions still use outdated or weak cryptographic algorithms. PPTP is cryptographically broken and should not be used under any circumstances. L2TP/IPsec with weak pre-shared keys, IKEv1 configurations without Perfect Forward Secrecy, and TLS-based VPNs using deprecated cipher suites (RC4, DES, 3DES) are also found in older IACS installations. Without Perfect Forward Secrecy, a compromise of the server's long-term private key allows retrospective decryption of all previously recorded sessions. In IACS environments where legacy systems limit upgrade options, weak cryptography often persists without a remediation plan.

2.1.7 Application-Level Protocol Exposure

VPN tunnels are transport-layer controls. They encrypt traffic in transit but do not filter or inspect the payloads flowing through them. Industrial protocols such as Modbus TCP, S7comm, OPC UA (without security profiles), and PROFINET often have no application-layer authentication. Once a VPN session is established, any IACS-specific commands can be issued freely. A compromised or misconfigured VPN client could be used to send unauthorized process commands to a PLC, change setpoints, or disable safety functions — all through the encrypted and seemingly legitimate VPN tunnel.

3. IEC 62443 Requirements and Mitigation Measures

The IEC 62443 standard series provides a comprehensive framework for securing Industrial Automation and Control Systems. The requirements it defines across its various parts directly address the vulnerabilities described in the preceding section. Applying these requirements systematically allows operators to significantly reduce the risk associated with remote VPN access to IACS environments.

3.1 Zone and Conduit Model (IEC 62443-3-2)

IEC 62443-3-2 requires that all IACS assets be assigned to security zones, and that communication between zones of different security levels be controlled through conduits. A VPN tunnel is itself a conduit and must be treated as such. This means it must have a defined and documented security policy specifying which assets and protocols are accessible through it, which users or systems are permitted to use it, and under what conditions the tunnel may be established.

The VPN gateway should terminate in a dedicated DMZ rather than directly in the OT zone. A jump host or bastion server in the DMZ serves as the controlled access point through which all remote operators must connect before reaching production assets. This architecture ensures that the conduit boundary is enforced at the network level and that no direct routing exists between the internet-facing VPN endpoint and IACS components. Access from the DMZ into the OT zone should be governed by restrictive access control lists and ideally by a dedicated industrial firewall capable of protocol-aware filtering.

3.2 Identification, Authentication, and Access Control (SR 1.1, SR 1.2, SR 2.1)

IEC 62443-3-3 System Requirement SR 1.1 mandates that all users, software processes, and devices be identified and authenticated before gaining access to any IACS zone. For remote access via VPN, this requires at minimum two-factor authentication combining a knowledge factor (password or PIN) with a possession factor (hardware token, certificate on a smart card, or a time-based one-time password). At Security Level 2, which represents the baseline for most industrial environments, simple password-only authentication is insufficient.

SR 2.1 (Authorization Enforcement) requires that access is granted only to the assets and functions for which a user has been explicitly authorized. This must be reflected in the VPN access policy: a field service technician responsible for one specific machine should have network-layer access only to that machine, not to all components on the OT network. Role-based access control enforced at both the VPN gateway and the internal firewall ensures adherence to the principle of least privilege.

For third-party access, the CSMS requirements of IEC 62443-2-1 mandate a formal process for granting, reviewing, and revoking access rights. Individual credentials must be issued for each technician, and a defined process must exist to ensure timely revocation when a technician leaves the service provider organization. Access should be granted for a defined time window and must be reviewed at regular intervals.

3.3 Session Control and Audit Logging (SR 2.6, SR 2.8, SR 3.2)

SR 2.6 (Remote Session Controls) requires that remote sessions be monitored and terminated after a defined period of inactivity. This prevents scenarios where a session remains open indefinitely after a maintenance activity has concluded, leaving an unmonitored access path into the OT environment. Automatic session timeouts,

combined with a requirement for explicit session re-authentication after a defined idle period, substantially reduce the window of exposure for any single remote access event.

SR 2.8 (Auditable Events) requires that security-relevant events be logged in a tamper-evident manner. For remote VPN access, this includes at a minimum: successful and failed authentication attempts, session start and end times, and the identity of the authenticated user. At higher security levels, session recording — capturing all commands executed and all changes made during a remote session — provides the level of accountability required for forensic investigation and regulatory compliance. A Privileged Access Management (PAM) solution installed in the DMZ can provide this capability without requiring changes to legacy IACS components.

3.4 On-Demand Access and Temporary Credentials

The principle of least privilege, which runs throughout the IEC 62443 framework, requires that access be available only for the duration it is needed. Applied to remote VPN access, this means that permanent site-to-site tunnels to vendor sites should be replaced with on-demand connections that are established only for approved maintenance activities and terminated immediately upon completion. A workflow-based access approval process — in which a remote access request is submitted and approved before the VPN account is enabled and valid credentials are issued — provides strong operational control and ensures traceability.

Privileged Access Management platforms support this model by providing time-limited credential issuance, automatic session recording, and centralized approval workflows. Even without a dedicated PAM system, simple procedural controls — such as requiring a change request number to be associated with every remote access event — significantly improve the operator's ability to monitor and control third-party access.

3.5 Cryptographic Strength and VPN Gateway Hardening

From a technical standpoint, VPN gateways protecting IACS environments should be configured with modern cryptographic standards: IKEv2 with ECDH key exchange, AES-256-GCM for encryption, and SHA-256 or stronger for integrity protection. Perfect Forward Secrecy must be enabled to ensure that compromise of long-term keys does not expose historical session traffic. PPTP and L2TP without strong IPsec profiles must not be used. Certificate-based authentication using a dedicated PKI is strongly preferred over pre-shared keys, as it supports individual credential management and revocation.

VPN gateways must be subject to the same patch management discipline as any other critical asset. Because these systems are directly internet-exposed, the window between public disclosure of a critical CVE and active exploitation is often measured in days. Operators should establish a process for monitoring vendor security advisories and applying critical patches to VPN gateways within a defined, risk-based timeframe. Where patching requires a maintenance window, compensating controls such as IP-based access restrictions or multi-stage authentication should be applied as interim measures.

3.6 Application-Level Controls Beyond the VPN

Because VPN provides only transport-layer security, application-layer controls must be implemented independently. Industrial firewalls or deep packet inspection (DPI) capable of understanding OT protocols should be deployed at the boundary between the DMZ and the OT zone. These systems can enforce allow-lists of permitted protocol types and function codes, blocking unauthorized commands even from authenticated VPN sessions. OPC UA connections should be configured with Message Security Mode SignAndEncrypt and use

dedicated certificates, not the None security profile. Where protocol-level security is not feasible for legacy systems, compensating controls such as unidirectional gateways for read-only traffic may be appropriate.

4. Security Level Mapping

The following table summarizes the remote access security requirements mapped against the Security Level targets defined in IEC 62443-3-3. Security Level 2 should be considered the minimum baseline for any IACS environment with remote access capability.

Requirement	SL 1	SL 2 (Minimum Baseline)	SL 3
Authentication	Password only	MFA (password + token or certificate)	MFA + hardware token + mutual TLS
Credential management	Shared accounts acceptable	Individual accounts, periodic review mandatory	Individual accounts, just-in-time issuance
Access scope	Network-wide after VPN login	Role-based, least privilege enforced	Microsegmentation, per-session scoping
Session timeout	Not required	Inactivity timeout mandatory	Inactivity timeout + re-authentication
Session recording	Not required	Full session logging	Real-time session monitoring + alerting
Audit trail	Basic event logging	Tamper-evident centralized logging	SIEM integration, automated anomaly detection
Network architecture	VPN terminates in OT network	VPN terminates in DMZ + jump host	VPN in DMZ + jump host + OT-level DPI firewall
Cryptography	Any IPsec/TLS profile	IKEv2, AES-128+, PFS enabled	IKEv2, AES-256, PFS, certificate-based auth
Patch management	No defined process	Regular review of security advisories	Critical patches within defined SLA
Third-party access	No formal process	Documented process, time-limited access	PAM workflow, automated revocation

5. Audit Checklist

The following checklist can be used by auditors and security assessors to evaluate the security posture of VPN-based remote access in an IACS environment. Each item maps to one or more IEC 62443 requirements.

5.1 Architecture and Network Design

Audit Question	IEC 62443 Reference	Finding
Is a documented Zone and Conduit model available that explicitly addresses remote VPN access?	IEC 62443-3-2	
Does the VPN tunnel terminate in a dedicated DMZ, not directly in the OT network?	IEC 62443-3-2, SR 5.1	
Is a jump host or bastion server deployed and used as the mandatory access point for all remote sessions?	IEC 62443-3-3 SR 5.2	
Is an industrial firewall or DPI-capable device deployed between the DMZ and OT network?	IEC 62443-3-3 SR 5.1	
Are IPv6 and split tunneling configured consistently with the security policy?	IEC 62443-3-2	

5.2 Authentication and Identity Management

Audit Question	IEC 62443 Reference	Finding
Is MFA enforced for all remote VPN users, including third-party service accounts?	SR 1.1, SR 1.2	
Are individual, non-shared credentials issued to each remote user?	SR 1.1, IEC 62443-2-1	
Is a documented process in place for granting, reviewing, and revoking third-party access?	IEC 62443-2-1	
Has an access rights review been conducted within the past 12 months?	IEC 62443-2-1	
Are all permanent VPN tunnels to third-party sites documented and risk-assessed?	IEC 62443-2-1, SR 1.3	

5.3 Session Control and Monitoring

Audit Question	IEC 62443 Reference	Finding
Is a session inactivity timeout configured on the VPN gateway and enforced?	SR 2.6	
Are remote sessions recorded and the recordings retained for a defined period?	SR 2.8	
Are audit logs stored in a tamper-evident, centralized system?	SR 2.8, SR 3.2	
Is there a defined process for reviewing remote access logs and investigating anomalies?	IEC 62443-2-1	

Is a kill switch or automatic tunnel termination implemented for VPN client software?	SR 2.6	
---	--------	--

5.4 Cryptography and Patch Management

Audit Question	IEC 62443 Reference	Finding
Is the VPN configured with IKEv2, AES-128 or stronger, and Perfect Forward Secrecy?	SR 4.3	
Are PPTP, L2TP without strong IPsec, and deprecated cipher suites explicitly disabled?	SR 4.3	
Is certificate-based authentication used instead of pre-shared keys?	SR 1.2	
Is there a defined patch management process for the VPN gateway covering critical CVEs?	IEC 62443-2-1	
When was the VPN gateway software last updated? Is it within vendor support lifecycle?	IEC 62443-2-1	

6. Conclusion

VPN technology provides an essential transport-layer security mechanism for remote access to industrial systems, but it is neither sufficient nor self-securing. The vulnerabilities that arise from misconfiguration and poor operational practices — including insufficient authentication, flat network architectures, permanent third-party tunnels, and absent monitoring — expose IACS environments to a level of risk that is incompatible with safe and reliable industrial operations.

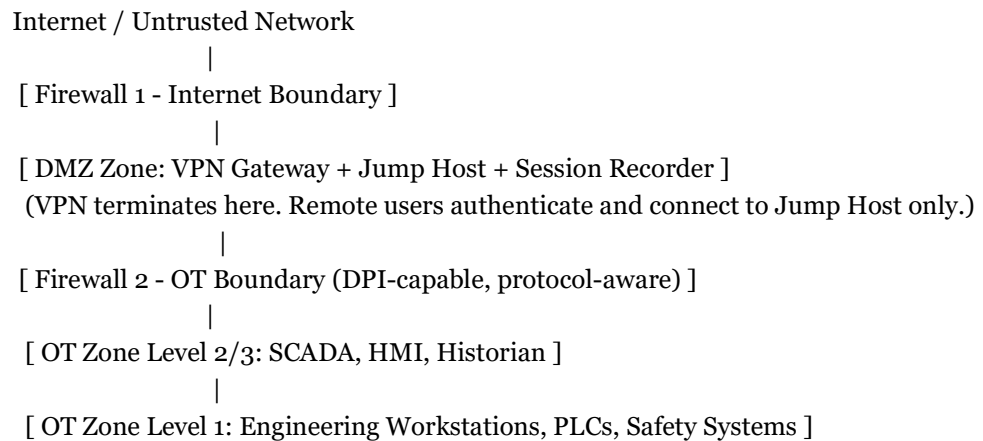
The IEC 62443 standard series provides a structured and internationally recognized framework for addressing these risks systematically. By applying the zone and conduit model, enforcing least-privilege access control, requiring multi-factor authentication, implementing session controls and audit logging, and maintaining VPN gateways as critical infrastructure assets subject to rigorous patch management, operators can achieve a level of protection appropriate for Security Level 2 and above.

A key insight from the IEC 62443 perspective is that a VPN tunnel is a conduit and must be governed accordingly. It requires a documented security policy, defined access rights, technical enforcement at both the network and application layer, and regular review. Security is not achieved by deploying a VPN — it is achieved by operating it correctly, within an architecture that limits the blast radius of any compromise and ensures that every remote access event is authenticated, authorized, and auditable.

ANNEX

A: Reference Architecture Diagram (Descriptive)

The following describes the target architecture for IEC 62443-compliant IACS remote access via VPN:



Key principles: (1) VPN never terminates directly in the OT zone. (2) All remote sessions pass through the Jump Host where they are authenticated, logged, and recorded. (3) The OT boundary firewall enforces protocol-level allow-lists. (4) Lateral movement within the OT zone from the DMZ is not possible without explicit firewall rules.