ICS/OT Risk Assessment Framework

A Practical Guide for Industrial Environments

PROTISEC · 2026

Introduction

This framework provides a structured approach to assessing security risks in Industrial Control Systems (ICS) and Operational Technology (OT) environments. It is designed for:

- Plant managers and operations directors
- IT/OT convergence teams
- CISOs with industrial infrastructure responsibility
- Compliance officers (NIS2, ISA/IEC 62443)

Industrial environments face unique challenges: legacy protocols, real-time constraints, safety-critical operations, and convergence with IT networks. A generic IT security assessment will miss 80% of ICS/OT risks.

This document gives you the methodology, checklists, and scoring matrix to identify, prioritize, and remediate ICS/OT security gaps — before an incident forces the conversation.

---

1. ICS/OT Risk Assessment Methodology

1.1 Scope Definition

Before assessing, define boundaries:

Physical scope: - Which facilities? (plant, substation, warehouse) - Which control systems? (DCS, SCADA, PLC, RTU) - Which networks? (Level 0-5 per Purdue model)

Operational scope: - Safety Instrumented Systems (SIS)? - Fire and gas systems? - Emergency shutdown systems?

Regulatory scope: - NIS2 designation? (essential/important entity) - ISA/IEC 62443 compliance requirement? - Sector-specific regulations? (energy, water, transport)

1.2 Assessment Phases

Phase 1: Asset Discovery (1-2 weeks) - Inventory all industrial devices (PLCs, RTUs, HMIs, engineers' workstations) - Map network topology (VLANs, firewalls, DMZs) - Identify protocols in use (Modbus, DNP3, OPC-UA, Profinet) - Document firmware versions and patch levels

Phase 2: Threat Modeling (1 week) - Identify threat actors (script kiddies → nation-states) - Map attack surfaces (internet-facing HMIs, remote access, USB ports) - Assess adversary capabilities (MITRE ATT&CK ICS matrix) - Consider insider threats (operators, contractors, terminated employees)

Phase 3: Vulnerability Assessment (2-3 weeks) - Protocol-level analysis (clear-text Modbus, no authentication) - Network segmentation review (flat networks, missing DMZs) - Access control audit (default passwords, shared accounts) - Physical security assessment (unlocked cabinets, unsupervised HMIs)

Phase 4: Risk Scoring (1 week) - Apply risk matrix (likelihood × impact) - Prioritize by safety impact first, then operational, then financial - Document risk acceptance decisions

Phase 5: Remediation Roadmap (1-2 weeks) - Quick wins (password changes, network segmentation) - Medium-term (protocol hardening, monitoring deployment) - Long-term (full Purdue model implementation, ISA 62443 certification)

---

2. Purdue Model Reference

The Purdue Enterprise Reference Architecture (PERA) defines 6 levels for industrial network segmentation:

Level 4 — Enterprise Business Planning - ERP, MES, business logistics - Corporate IT network - Internet-connected

Level 3.5 — Industrial DMZ - Buffer zone between IT and OT - Historians, monitoring servers, patch management - **Critical control point** — all IT↔OT traffic passes here

Level 3 — Operations Management - HMI servers, engineering workstations - Operations management systems - No direct internet access

Level 2 — Supervisory Control - SCADA servers, DCS controllers - Real-time monitoring and control - Restricted access

Level 1 — Basic Control - PLCs, RTUs, standalone controllers - Direct process control - Safety-critical

Level 0 — Physical Process - Sensors, actuators, drives - Physical manufacturing process - No network stack (analog/electrical)

Segmentation Rules

1. **No direct Level 4 ↔ Level 0-2 connectivity.** All traffic routes through Level 3.5 DMZ.
2. **Unidirectional gateways** for Level 0-1 data extraction (data diodes).
3. **Industrial DMZ (Level 3.5)** hosts all cross-zone services (historians, jump hosts, patch servers).
4. **No internet-facing HMIs.** Remote access via VPN + jump host in DMZ.
5. **Separate VLANs per level** with firewall rules restricting lateral movement.

---

3. ISA/IEC 62443 Quick Checklist

ISA/IEC 62443 is the international standard for ICS security. Use this checklist for rapid gap analysis:

Foundational Requirements (Security Level 1)

SR 1 — Identification and Authentication Control - [ ] Unique user IDs for all operators - [ ] Password complexity enforced (min 12 chars, no defaults) - [ ] Multi-factor authentication for remote access - [ ] Account lockout after 5 failed attempts

SR 2 — Use Control - [ ] Role-based access control (RBAC) implemented - [ ] Least privilege principle (operators ≠ engineers ≠ admins) - [ ] Session timeout (15 min idle) - [ ] No shared accounts

SR 3 — System Integrity - [ ] Anti-malware on all Windows-based HMIs - [ ] Application whitelisting (no unauthorized executables) - [ ] File integrity monitoring on critical systems - [ ] Secure boot where supported

SR 4 — Data Confidentiality - [ ] Encrypted protocols (OPC-UA secure mode, not clear-text Modbus) - [ ] TLS 1.2+ for remote access - [ ] No clear-text credentials in configuration files - [ ] Data classification (public, internal, confidential, restricted)

SR 5 — Restricted Data Flow - [ ] Network segmentation per Purdue model - [ ] Firewall rules documented and reviewed quarterly - [ ] No direct internet access from Level 0-2 - [ ] Industrial DMZ (Level 3.5) enforced

SR 6 — Timely Response to Events - [ ] Centralized logging (SIEM or equivalent) - [ ] Alerting on security events (failed logins, configuration changes) - [ ] Incident response plan documented and tested - [ ] 24/7 monitoring for critical infrastructure

SR 7 — Resource Availability - [ ] Redundant controllers for critical processes - [ ] Uninterruptible power supply (UPS) for control systems - [ ] Backup and restore procedures tested annually - [ ] Disaster recovery plan with RTO/RPO defined

Advanced Requirements (Security Level 2-4)

- [ ] Security management system (ISMS) established
- [ ] Risk assessment conducted per IEC 62443-3-2

- [ ] Security levels assigned per zone and conduit
- [ ] IACS security policy documented and approved
- [ ] Third-party audit completed (certification body)

---

4. IT/OT Segmentation Assessment

Use this scoring rubric to evaluate current segmentation maturity:

Level 0 — Non-Existent (0 points)

- Flat network: IT and OT on same VLAN
- Direct internet access from HMIs
- No firewall between corporate and plant networks
- Shared accounts, default passwords

Level 1 — Basic (10-30 points)

- Some VLAN segmentation (IT vs OT)
- Firewall present but rules not reviewed
- Internet access restricted but not blocked
- Password policy exists but not enforced

Level 2 — Defined (40-60 points)

- Purdue model partially implemented (Level 3.5 DMZ exists)
- Firewall rules documented and reviewed annually
- Internet access blocked for Level 0-2
- RBAC implemented, MFA for remote access

Level 3 — Managed (70-85 points)

- Full Purdue model with unidirectional gateways for Level 0-1
- Industrial DMZ hosts all cross-zone services
- Network monitoring (IDS/IPS for OT protocols)
- Quarterly access reviews, annual penetration tests

Level 4 — Optimized (90-100 points)

- Zero Trust architecture for ICS (micro-segmentation)
- Continuous monitoring with anomaly detection (ML-based)
- Automated compliance reporting (ISA 62443)
- Incident response tested quarterly with OT-specific scenarios

Scoring Instructions

1. Rate each category (physical, network, access control, monitoring, incident response)
2. Calculate weighted average (network segmentation = 30%, access control = 25%, monitoring = 20%, incident response = 15%, physical = 10%)
3. Map to maturity level
4. Identify gaps and prioritize remediation

---

5. Risk Scoring Matrix

Likelihood (1-5)

1 — Rare - Attack requires physical access + insider knowledge - No known vulnerabilities in deployed systems - Network fully segmented, no internet exposure

2 — Unlikely - Vulnerability exists but requires complex exploit - Partial segmentation (some internet-facing assets) - Basic monitoring in place

3 — Possible - Known vulnerability with public exploit - Flat network, direct IT↔OT connectivity - No monitoring or alerting

4 — Likely - Actively exploited vulnerability (CISA KEV list) - Internet-facing HMIs or engineering workstations - Default credentials in use

5 — Almost Certain - Active compromise indicators (malware, unauthorized access) - No segmentation, no monitoring, no access control - Recent similar incidents in sector

Impact (1-5)

1 — Negligible - No safety impact - No production downtime - Financial impact < €10K

2 — Minor - Minor safety incident (first aid) - Production downtime < 4 hours - Financial impact €10K-100K

3 — Moderate - Lost-time injury - Production downtime 4-24 hours - Financial impact €100K-1M - Regulatory notification required

4 — Major - Serious injury or environmental release - Production downtime 1-7 days - Financial impact €1M-10M - NIS2 incident reporting triggered

5 — Catastrophic - Fatality or major environmental disaster - Production downtime > 7 days - Financial impact > €10M - Criminal liability, loss of operating license

Risk Score = Likelihood × Impact

1-4 — Low Risk - Accept or monitor - Include in next budget cycle

5-9 — Medium Risk - Mitigate within 6 months - Assign owner, track in risk register

10-15 — High Risk - Mitigate within 30 days - Escalate to CISO/plant manager

16-25 — Critical Risk - Immediate action required - Consider shutdown until remediated - Executive notification

---

6. Common ICS/OT Vulnerabilities

Protocol Vulnerabilities

Modbus TCP (no authentication) - Risk: Anyone on network can read/write registers - Impact: Unauthorized control changes, process disruption - Remediation: Deploy Modbus security gateways, network segmentation

OPC Classic (DA/HDA, DCOM-based) - Risk: DCOM vulnerabilities, no encryption - Impact: Lateral movement, data exfiltration - Remediation: Migrate to OPC-UA secure mode

Profinet / EtherNet/IP (no authentication) - Risk: Rogue devices can inject commands - Impact: Safety system bypass, equipment damage - Remediation: Port security, 802.1X, network access control

Network Vulnerabilities

Flat IT/OT networks - Risk: Corporate IT compromise → plant floor - Impact: Ransomware spreads from IT to OT - Remediation: Purdue model segmentation, industrial DMZ

Internet-facing HMIs - Risk: Direct attack vector from internet - Impact: Remote takeover of industrial processes - Remediation: Remove internet access, VPN + jump host

Wireless networks (Wi-Fi, Zigbee) - Risk: Eavesdropping, rogue access points - Impact: Unauthorized control, data theft - Remediation: WPA3-Enterprise, network segmentation, monitoring

Access Control Vulnerabilities

Default credentials - Risk: Trivial compromise - Impact: Full system control - Remediation: Password audit, change all defaults, MFA

Shared accounts - Risk: No accountability, cannot trace actions - Impact: Insider threat, compliance failure - Remediation: Unique user IDs, RBAC

No session timeout - Risk: Unattended workstations = open access - Impact: Unauthorized control changes - Remediation: 15-minute idle timeout, screen locks

Physical Security Vulnerabilities

Unlocked control cabinets - Risk: Physical access = game over - Impact: USB malware, hardware tampering - Remediation: Locked cabinets, access logs

Unsupervised HMIs - Risk: Unauthorized physical access - Impact: Process manipulation - Remediation: Access control, CCTV, kiosk mode

No visitor management - Risk: Contractors, vendors unmonitored - Impact: Malware introduction, espionage - Remediation: Visitor logs, escorted access, device scanning

---

7. Remediation Prioritization

Quick Wins (0-30 days)

1. **Change all default passwords** (PLCs, HMIs, network devices)
2. **Block internet access** for Level 0-2 systems
3. **Disable unused services** (FTP, Telnet, SMBv1)
4. **Patch Windows HMIs** (critical security updates only)
5. **Implement network segmentation** (VLANs, basic firewall rules)

Medium-Term (1-6 months)

1. **Deploy industrial DMZ** (Level 3.5)
2. **Implement RBAC** (role-based access control)
3. **Enable logging and monitoring** (SIEM integration)
4. **Migrate to secure protocols** (OPC-UA, Modbus security)
5. **Conduct operator training** (phishing, USB hygiene, incident reporting)

Long-Term (6-18 months)

1. **Full Purdue model implementation** (unidirectional gateways)

2. **Deploy OT-specific IDS/IPS** (protocol-aware monitoring)
3. **ISA/IEC 62443 certification** (Security Level 1-2)
4. **Incident response testing** (OT-specific scenarios)
5. **Continuous compliance monitoring** (automated reporting)

Prioritization Framework

Safety first: Any risk with safety impact (injury, environmental release) = critical priority.

Regulatory second: NIS2 essential entities have 2025-2026 compliance deadlines. ISA 62443 may be contractually required.

Operational third: Production downtime risk. Calculate cost per hour of downtime vs. remediation cost.

Financial fourth: Direct financial loss (ransomware, theft, fraud).

---

8. Next Steps

This framework gives you the methodology to assess ICS/OT security risks. Execution requires:

1. **Asset inventory** — you cannot protect what you cannot see
2. **Threat modeling** — understand your specific adversaries
3. **Gap analysis** — compare current state to ISA 62443 requirements
4. **Risk scoring** — prioritize by safety and operational impact
5. **Remediation roadmap** — quick wins first, then systematic improvement

How PROTISEC Can Help

PROTISEC specializes in ICS/OT security for critical infrastructure:

- **ISA/IEC 62443 assessment** — full gap analysis, Security Level determination
- **Purdue model implementation** — network segmentation design, industrial DMZ
- **OT anomaly detection** — AI-based monitoring for protocol deviations

- **Incident response** — ICS-specific playbooks, containment without production impact
- **Compliance** — NIS2, ISO 27001, sector-specific regulations

Contact us for a free 30-minute technical assessment: - Web: protisec.com/contact - WhatsApp: +34 XXX XXX XXX - Email: contact@protisec.com

---

About PROTISEC

PROTISEC is a boutique cybersecurity firm specializing in ICS/OT security, MLSecOps, and regulatory compliance (NIS2, ISO 27001, GDPR). We work with critical infrastructure operators, manufacturing, and energy companies across Spain and the EU.

Our team combines 30+ years of industrial automation experience with modern cybersecurity practices. We understand that in OT environments, availability and safety come first — security must enable operations, not disrupt them.

Certifications: ISO 27001 Lead Implementer, ISA/IEC 62443 Cybersecurity Expert, AEPD DPO Certified

---