OT Risk Assessment

Assessing Cybersecurity Risk in Industrial Environments

OT Security Learning Series

Document 700 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Risk assessment in OT environments must consider factors beyond traditional IT security—including physical safety, environmental impact, and operational continuity. The goal is to identify, analyze, and prioritize risks to enable informed security decisions.

Information

OT risk assessment bridges cybersecurity and process safety. It requires collaboration between security professionals, engineers, and operations staff to accurately evaluate threats and their potential consequences.

1.1 OT vs IT Risk Considerations

Factor	IT Focus	OT Focus
Primary concern	Data confidentiality	Safety and availability
Impact scope	Business operations	Physical world effects
Threat actors	Cybercriminals, APTs	Nation-states, insiders
Asset lifetime	3–5 years	15–25+ years
Patching	Regular updates	Constrained by operations

2 Risk Fundamentals

2.1 Risk Equation

Risk Calculation

$$\textbf{Risk} = \textbf{Threat} \times \textbf{Vulnerability} \times \textbf{Consequence}$$

- **Threat:** Who might attack and how likely?
- **Vulnerability:** What weaknesses can be exploited?
- **Consequence:** What is the impact if successful?

2.2 Consequence Categories

OT risk assessment must consider multiple impact types:

- **Safety:** Potential for injury or loss of life
- **Environmental:** Spills, emissions, contamination
- **Operational:** Production loss, equipment damage
- **Financial:** Direct costs and business impact
- **Reputational:** Customer and public trust
- **Regulatory:** Fines, compliance violations

3 IEC 62443 Risk Assessment

3.1 Zone and Conduit Model

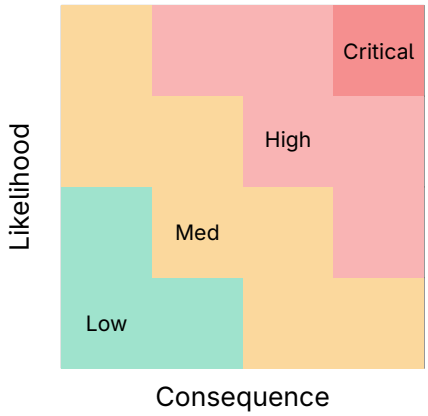
IEC 62443-3-2 defines a systematic approach:

1. **Identify system under consideration (SUC)**
2. **Perform initial risk assessment**
3. **Partition into zones and conduits**
4. **Assign target security levels (SL-T)**
5. **Document security requirements**

3.2 Security Levels

SL	Threat Level	Description
SL 1	Casual/Accidental	Protection against unintentional errors
SL 2	Intentional (simple)	Low skill, limited resources, general motivation
SL 3	Intentional (sophisticated)	Moderate skill, moderate resources, specific target
SL 4	Intentional (nation-state)	High skill, extensive resources, highly motivated

3.3 Risk Matrix



4 Assessment Process

4.1 Step 1: Scope Definition

- Define boundaries of assessment (facility, system, zone)
- Identify stakeholders and their concerns

- Gather existing documentation (diagrams, procedures)
- Establish assessment criteria and risk tolerance

4.2 Step 2: Asset Identification

- Inventory all assets in scope
- Classify by criticality and function
- Map communication flows and dependencies
- Identify data flows crossing zone boundaries

4.3 Step 3: Threat Assessment

- Identify relevant threat actors (nation-state, criminal, insider)
- Consider threat capabilities and motivations
- Review industry-specific threat intelligence
- Assess likelihood of targeting your organization

4.4 Step 4: Vulnerability Assessment

Warning

OT vulnerability assessment considerations:

- Avoid active scanning of production systems
- Use passive methods and configuration review
- Consider architectural weaknesses, not just CVEs
- Assess compensating controls effectiveness

4.5 Step 5: Risk Evaluation

- Calculate risk for each threat-vulnerability pair
- Consider existing controls and their effectiveness
- Prioritize risks based on consequence severity
- Document assumptions and uncertainties

5 Risk Treatment

5.1 Treatment Options

Option	Description
Mitigate	Implement controls to reduce likelihood or consequence
Transfer	Insurance, contractual arrangements with vendors
Accept	Document acceptance with management approval
Avoid	Eliminate the risk source (remove system, change process)

5.2 Control Selection

Prioritize controls that:

- Address highest risks first
- Are compatible with operational requirements
- Can be implemented without safety impact
- Provide defense in depth

6 Documentation

6.1 Required Outputs

- **Asset inventory** with criticality ratings
- **Zone and conduit diagram** with security levels
- **Risk register** with ratings and treatment plans
- **Security requirements** for each zone
- **Residual risk statement** with management sign-off

6.2 Review Cycle

- **Annual review:** Full reassessment recommended
- **Trigger-based:** After incidents, major changes, new threats
- **Continuous:** Update as new vulnerabilities discovered

7 Further Reading

Standards

- **IEC 62443-3-2** – Security Risk Assessment for System Design
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **ISO 27005** – Information Security Risk Management
  https://www.iso.org/standard/80585.html

Resources

- **NIST Cybersecurity Framework**
  https://www.nist.gov/cyberframework