OT Security Maturity Models

Measuring and Improving Industrial Cybersecurity Capability

OT Security Learning Series

Document 740 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Security maturity models provide a structured framework for assessing an organization's cybersecurity capabilities against defined benchmarks. For OT environments, maturity assessments help identify gaps, prioritize investments, and track improvement over time.

Information

This document introduces security maturity models applicable to OT environments. It covers common frameworks, maturity levels, assessment approaches, and how to use maturity assessments to drive meaningful security improvements in industrial settings.

2 Why Maturity Models for OT

2.1 Benefits of Maturity Assessment

- **Baseline Establishment:** Understand current security posture objectively
- **Gap Identification:** Find weaknesses before adversaries do
- **Prioritization:** Focus resources on highest-impact improvements
- **Progress Tracking:** Measure improvement over time
- **Benchmarking:** Compare against industry peers
- **Communication:** Translate security status for executives and boards

2.2 OT-Specific Considerations

Factor	Impact on Maturity Assessment
Safety requirements	Security controls must not compromise safety systems
Legacy systems	Older systems may not support modern security practices
Availability focus	Downtime for security improvements is limited
Vendor dependencies	Third-party support affects achievable maturity
Regulatory environment	Compliance requirements set minimum baselines

Table 1: OT factors affecting maturity assessment

3 Common Maturity Models

3.1 Overview of Frameworks

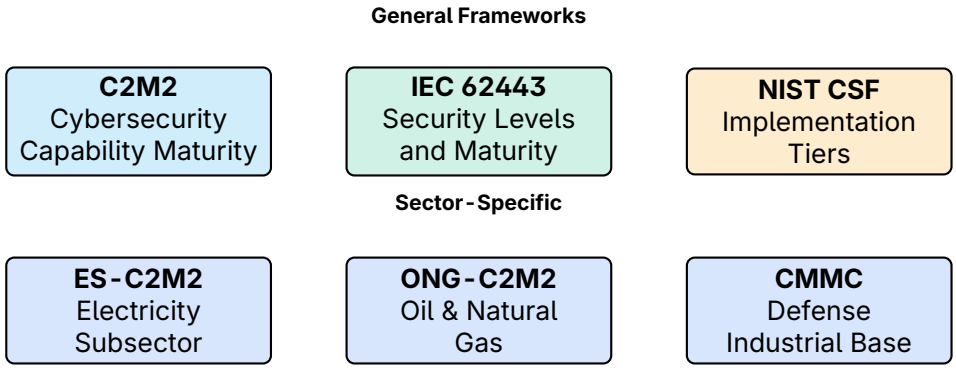

Figure 1: Common security maturity models for OT

3.2 C2M2 – Cybersecurity Capability Maturity Model

Developed by the U.S. Department of Energy, C2M2 is widely used in critical infrastructure:

- **10 Domains:** Risk management, asset management, access control, threat detection, incident response, etc.
- **4 Maturity Levels:** MIL0 (not performed) through MIL3 (optimized)
- **Self-Assessment:** Designed for organizations to assess themselves
- **OT Focus:** Includes IT and OT considerations throughout

3.3 IEC 62443 Security Levels

IEC 62443 defines both Security Levels (SL) and maturity concepts:

Level	Threat	Description
SL 1	Casual/coincidental	Protection against unintentional violations
SL 2	Intentional, low resources	Protection against intentional attack with limited means
SL 3	Intentional, moderate resources	Protection against sophisticated attack
SL 4	Intentional, extended resources	Protection against state-sponsored attack

Table 2: IEC 62443 Security Levels

3.4 NIST CSF Implementation Tiers

The NIST Cybersecurity Framework defines four implementation tiers:

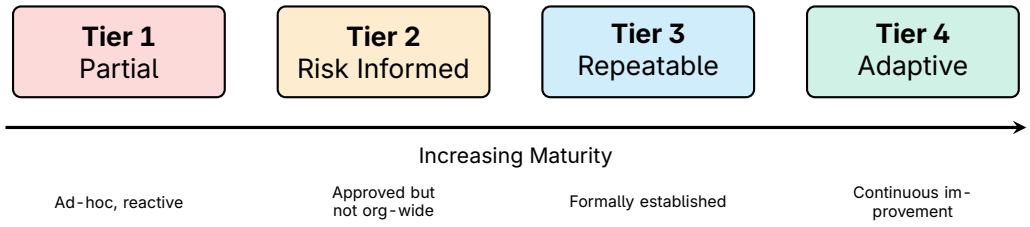

Figure 2: NIST CSF Implementation Tiers

4 Maturity Levels Explained

4.1 Generic Maturity Scale

Most models use similar progression concepts:

Level 0 – Not Performed: Practice not implemented or no evidence

Level 1 – Initial: Ad-hoc, reactive, dependent on individuals

Level 2 – Managed: Documented, practiced, but inconsistent

Level 3 – Defined: Standardized, organization-wide, measured

Level 4 – Optimized: Continuous improvement, adaptive

Figure 3: Generic maturity level progression

4.2 What Each Level Means in Practice

Level	Characteristics	OT Example
Initial	Reactive, heroic efforts	Firewall exists but rules undocumented
Managed	Documented for specific areas	Patch process defined for SCADA servers
Defined	Consistent across organization	All sites follow same access control policy
Optimized	Metrics-driven improvement	KPIs track and improve detection time

Table 3: Maturity levels with OT examples

Warning

Higher maturity is not always better. The target maturity level should align with risk appetite and business requirements. A Level 4 maturity for low-risk systems may waste resources that could protect critical assets.

5 Assessment Process

5.1 Assessment Approaches

Approach	Advantages	Disadvantages
Self-assessment	Low cost, internal ownership	May lack objectivity
Facilitated	Expert guidance, consistent	Requires skilled facilitator
Third-party audit	Independent, credible	Higher cost, less context
Continuous monitoring	Real-time, automated	Limited to measurable controls

Table 4: Maturity assessment approaches

5.2 Assessment Steps

Figure 4: Maturity assessment process

5.3 Evidence Collection

Gather evidence across multiple sources:

- **Documentation:** Policies, procedures, standards, network diagrams
- **Interviews:** Engineers, operators, security staff, management
- **Technical Review:** Configuration files, logs, tool outputs
- **Observation:** Site visits, process walkthroughs

Tip

Include both IT and OT stakeholders in assessments. OT engineers understand operational constraints while IT security brings assessment experience. Joint participation improves accuracy and buy-in.

6 Using Assessment Results

6.1 Gap Prioritization

Not all gaps are equal. Prioritize based on:

- **Risk Impact:** How much does this gap increase risk?
- **Compliance:** Is this gap a regulatory violation?
- **Dependency:** Do other improvements depend on this?
- **Feasibility:** Can this be addressed with available resources?
- **Quick Wins:** Low effort, high impact improvements

6.2 Roadmap Development

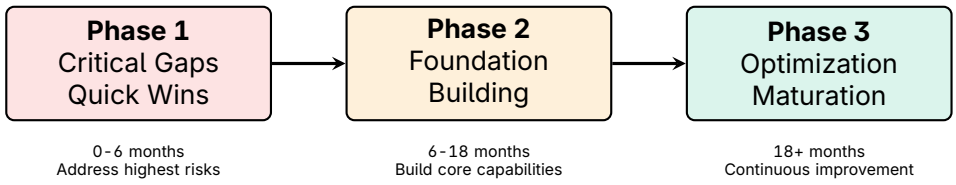

Figure 5: Phased improvement roadmap

6.3 Target State Definition

Key Point

Recommendation: Define target maturity levels per domain based on asset criticality. Safety-critical systems may require Level 3+ while support systems may only need Level 2. Not everything needs maximum maturity.

7 Common Pitfalls

- **Checkbox Mentality:** Focus on scoring rather than actual security improvement
- **Ignoring OT Context:** Applying IT maturity expectations to OT environments
- **One-Time Assessment:** Treating maturity as a project, not ongoing process
- **Unrealistic Targets:** Setting Level 4 targets for all domains
- **Siloed Assessment:** Excluding OT operations from the process
- **Documentation Focus:** Having policies without implementation

Critical

A documented policy without implementation scores higher on some assessments but provides no actual security. Verify that documented practices are actually followed in operations.

8 Summary

Key Takeaways

- **Structured Assessment:** Maturity models provide objective frameworks for measuring OT security capabilities
- **Framework Selection:** Choose models appropriate for your sector (C2M2 for energy, IEC 62443 for manufacturing)
- **Right-Sized Targets:** Target maturity should align with risk—not everything needs Level 4
- **Evidence-Based:** Gather evidence from documentation, interviews, technical review, and observation
- **Prioritized Improvement:** Focus on high-risk gaps and quick wins before comprehensive maturation
- **Continuous Process:** Reassess periodically to track progress and identify new gaps
- **OT Context:** Include operational constraints and OT stakeholders throughout the process

9 Further Reading

Maturity Models

- **C2M2 Version 2.1** – Cybersecurity Capability Maturity Model
  https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
- **NIST Cybersecurity Framework 2.0**
  https://www.nist.gov/cyberframework
- **IEC 62443-2-1** – Security Program Requirements
  https://webstore.iec.ch/publication/7030

Resources

- **CISA** – Cross-Sector Cybersecurity Performance Goals
  https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- **SANS ICS** – Industrial Control Systems Security
  https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials

Books

- Caralli et al. – *CERT Resilience Management Model* (Addison-Wesley)
- Knapp, Eric D. – *Industrial Network Security* (Syngress)

Part of the OT Security Learning Series