NIST SP 800-82

Guide to Operational Technology Security

OT Security Learning Series

Document 111 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

NIST Special Publication 800-82 is the primary U.S. government guidance document for securing Operational Technology (OT) systems, including Industrial Control Systems (ICS), SCADA systems, and Distributed Control Systems (DCS).

Information

NIST SP 800-82 Revision 3 (2023) represents a significant update, expanding scope from ICS to all OT systems and aligning with the NIST Cybersecurity Framework and SP 800-53.

1.1 Document Evolution

Version	Year	Key Changes
Original	2006	Initial ICS security guidance
Revision 1	2011	Updated threats, expanded controls
Revision 2	2015	Risk management, ISA/IEC 62443 alignment
Revision 3	2023	OT scope, supply chain, cloud, CSF alignment

1.2 Why NIST 800-82 Matters

- **Authoritative:** Primary U.S. federal guidance for OT security
- **Comprehensive:** Covers threats, vulnerabilities, and countermeasures
- **Practical:** Provides implementation guidance and overlay controls
- **Referenced:** Used by regulators, auditors, and industry worldwide

2 Document Structure

NIST SP 800-82 Rev. 3 is organized into six main sections:

Document Organization

1. **Introduction:** Purpose, scope, and document structure
2. **OT Overview:** System types, architectures, and components
3. **OT Risk Management:** Risk assessment and management approaches
4. **OT Security Program:** Governance, policies, and procedures
5. **OT Security Architecture:** Network design and segmentation
6. **Security Controls:** OT-specific control recommendations

3 OT System Overview

3.1 System Types Covered

System Type	Description
SCADA	Supervisory Control and Data Acquisition for distributed assets
DCS	Distributed Control Systems for process manufacturing
PLC/RTU	Programmable controllers for local automation
SIS	Safety Instrumented Systems for emergency shutdown
BAS/BMS	Building Automation and Management Systems
IIoT	Industrial Internet of Things devices and sensors

3.2 Key Differences: IT vs OT

Warning

NIST 800-82 emphasizes that OT environments have different priorities:

- **Availability** is typically the highest priority (not confidentiality)
- **Safety** considerations may override security decisions
- **Legacy systems** often cannot be patched or upgraded
- **Real-time requirements** limit security control options

4 Risk Management

4.1 Risk Assessment Process

NIST 800-82 recommends a structured risk assessment approach:

1. **System characterization:** Identify OT assets and boundaries
2. **Threat identification:** Determine relevant threat sources
3. **Vulnerability identification:** Assess system weaknesses
4. **Impact analysis:** Evaluate consequences of compromise
5. **Risk determination:** Calculate risk levels
6. **Control recommendations:** Select appropriate mitigations

4.2 Threat Sources

Threat Source	Characteristics
Nation-states	Advanced capabilities, strategic objectives, persistent
Cybercriminals	Financial motivation, ransomware, extortion
Hacktivists	Political/social motivation, publicity-seeking
Insiders	Authorized access, knowledge of systems
Terrorists	Disruption and destruction goals

5 Security Architecture

5.1 Defense-in-Depth

NIST 800-82 advocates for layered security:

Key Point

Defense-in-Depth Layers:

- Physical security (access control, surveillance)
- Network security (segmentation, firewalls, DMZ)
- Host security (hardening, whitelisting, patching)
- Application security (secure coding, input validation)
- Data security (encryption, integrity checking)

5.2 Network Segmentation

The document recommends network architecture based on zones:

- **Enterprise Zone:** Corporate IT network
- **DMZ:** Buffer zone with shared services
- **Control Zone:** OT network with control systems
- **Safety Zone:** Isolated safety systems

Tip

NIST 800-82 recommends using the Purdue Model or IEC 62443 zone concepts for network architecture design.

6 Security Controls

6.1 OT Overlay

NIST 800-82 provides an OT overlay for SP 800-53 controls, with tailored guidance for:

Family	Name	OT Considerations
AC	Access Control	Physical and logical access, remote access
AU	Audit	Logging without performance impact
CM	Configuration Mgmt	Change control, baseline configurations
CP	Contingency Planning	Backup, recovery, continuity
IA	Identification/Auth	Account management, strong authentication
IR	Incident Response	OT-specific procedures, coordination
MA	Maintenance	Secure remote maintenance, vendor access
SC	System/Comm Protection	Network segmentation, encryption

6.2 Key Control Recommendations

Critical

High-Priority Controls for OT:

- Network segmentation and traffic filtering
- Secure remote access with multi-factor authentication
- Application whitelisting on critical systems
- Comprehensive logging and monitoring
- Regular vulnerability assessments
- Incident response planning and testing

7 Implementation Guidance

7.1 Phased Approach

NIST 800-82 recommends implementing security in phases:

1. **Assessment:** Inventory assets, assess current state
2. **Planning:** Develop security plan, prioritize actions
3. **Implementation:** Deploy controls incrementally
4. **Operations:** Monitor, maintain, and improve

7.2 Integration with Other Standards

Information

NIST 800-82 aligns with and references:
- NIST Cybersecurity Framework (CSF)
- ISA/IEC 62443 series
- NERC CIP (for electric utilities)
- ISO 27001/27002

8 Further Reading

NIST Publications

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **NIST Cybersecurity Framework 2.0**
  https://www.nist.gov/cyberframework
- **NIST SP 800-53 Rev. 5** – Security Controls
  https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Related Standards

- **ISA/IEC 62443** – Industrial Automation Security
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards