OT Security Standards Overview

A Global Perspective on Industrial Cybersecurity Regulations

OT Security Learning Series

Document 100 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

The increasing convergence of IT and OT systems, combined with the rise of cyber threats targeting critical infrastructure, has led to the development of numerous cybersecurity standards and regulations worldwide. Understanding these standards is essential for organizations operating in multiple regions or sectors.

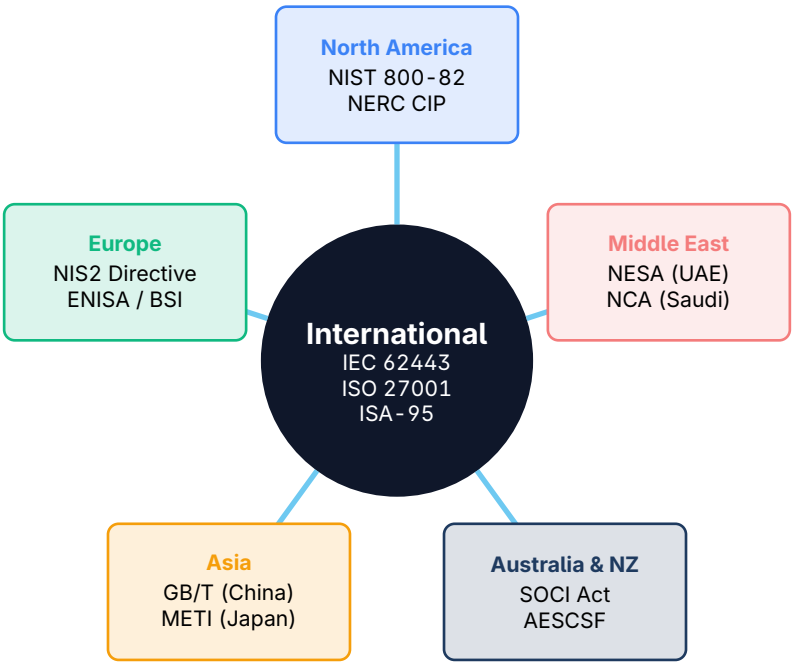
Information

This document provides an overview of the major OT security standards and regulations across different regions. Standards vary in their scope, requirements, and enforcement mechanisms.

1.1 Types of Standards

- **International Standards:** Developed by international bodies (ISO, IEC, ISA) for global adoption
- **Regional Regulations:** Legal requirements within specific regions (EU, North America)
- **National Standards:** Country-specific guidelines and frameworks
- **Sector-Specific:** Standards for particular industries (energy, water, manufacturing)

2 Global Standards Overview



Region	Key Standards	Mandatory
International	IEC 62443, ISO/IEC 27001, ISA-95	No
North America	NIST SP 800-82, NERC CIP, TSA Directives	Partial
Europe	NIS2, CRA, BSI IT-Grundschutz, ENISA	Yes
Asia-Pacific	GB/T 30976 (CN), METI (JP), TR64 (SG)	Partial
Australia & NZ	SOCI Act, AESCSF, Essential Eight	Yes
Middle East	NESA (UAE), NCA (Saudi Arabia)	Yes

Key Point

IEC 62443 is referenced by regulations worldwide and serves as the common foundation for OT security compliance across all regions.

3 International Standards

3.1 IEC 62443

IEC 62443 – Industrial Automation and Control Systems Security

Scope	Comprehensive framework for IACS security
Publisher	International Electrotechnical Commission (IEC)
Adoption	Worldwide, referenced by many national regulations
Key Parts	62443-2-1 (Policies), 62443-3-3 (System Requirements), 62443-4-2 (Components)

Key Point

IEC 62443 is the most widely recognized international standard for OT security. It provides a common framework and language for asset owners, integrators, and vendors.

3.2 ISO/IEC 27001

ISO/IEC 27001 – Information Security Management

Scope	Information security management systems (ISMS)
Publisher	ISO/IEC Joint Technical Committee
Adoption	Worldwide, certifiable standard
OT Relevance	General framework, often combined with IEC 62443 for OT

3.3 ISA-95 / IEC 62264

ISA-95 – Enterprise-Control System Integration

Scope	Integration between enterprise and control systems
Publisher	International Society of Automation (ISA)
Adoption	Worldwide, manufacturing focus
OT Relevance	Defines functional hierarchy, basis for Purdue Model

4 North America

4.1 United States

4.1.1 NIST SP 800-82

NIST SP 800-82 – Guide to OT Security

Scope	Guidance for securing industrial control systems
Publisher	National Institute of Standards and Technology
Status	Recommended practice (voluntary for most sectors)
Current Version	Revision 3 (2023)

4.1.2 NERC CIP

NERC CIP – Critical Infrastructure Protection

Scope	Bulk electric system cybersecurity
Publisher	North American Electric Reliability Corporation
Status	**Mandatory** for bulk power system owners/operators
Enforcement	Significant financial penalties for non-compliance

Warning

NERC CIP violations can result in penalties up to $1 million per violation per day. Compliance is mandatory for registered entities operating bulk electric system assets.

4.1.3 Other U.S. Frameworks

- **NIST Cybersecurity Framework (CSF)** – Risk-based framework applicable to all sectors
- **CISA Guidelines** – Sector-specific guidance for critical infrastructure
- **TSA Security Directives** – Pipeline and rail cybersecurity requirements
- **CFATS** – Chemical facility anti-terrorism standards

4.2 Canada

- **CSA Z246.1** – Security Management for Petroleum and Natural Gas
- **NERC CIP** – Applicable to interconnected power systems
- **CCCS Guidelines** – Canadian Centre for Cyber Security guidance

5 Europe

5.1 European Union

5.1.1 NIS2 Directive

NIS2 Directive – Network and Information Security

Scope	Essential and important entities across EU
Publisher	European Parliament and Council
Status	**Mandatory** (Member states must transpose by Oct 2024)
Sectors	Energy, transport, health, water, digital infrastructure, manufacturing

Critical

NIS2 significantly expands the scope of the original NIS Directive. More organizations are now subject to mandatory cybersecurity requirements, including many manufacturing companies.

5.1.2 Cyber Resilience Act (CRA)

- Mandatory cybersecurity requirements for products with digital elements
- Affects manufacturers, importers, and distributors
- Applies to both hardware and software, including OT components

5.1.3 ENISA Guidelines

The European Union Agency for Cybersecurity (ENISA) publishes sector-specific guidelines:

- Good Practices for Security of Smart Manufacturing
- Railway Cybersecurity Guidelines
- Smart Grid Security Recommendations

5.2 Germany

BSI IT-Grundschutz

Scope	Comprehensive IT/OT security methodology
Publisher	German Federal Office for Information Security (BSI)
Status	Mandatory for federal agencies, recommended for KRITIS
OT Module	IND – Industrial Control Systems

- **IT-Sicherheitsgesetz 2.0** – Legal requirements for critical infrastructure
- **KRITIS Verordnung** – Defines critical infrastructure thresholds

5.3 United Kingdom

- **NIS Regulations** – UK implementation (post-Brexit maintained)
- **Cyber Assessment Framework (CAF)** – NCSC guidance for OT
- **OG86** – Offshore oil and gas cybersecurity guidance

5.4 France

- **LPM** – Military Programming Law for critical infrastructure
- **ANSSI Guidelines** – National cybersecurity agency recommendations

6 Asia-Pacific

6.1 China

Chinese Cybersecurity Standards

GB/T 22239	– Information Security Technology Baseline
GB/T 30976	– Industrial Control System Security
Cybersecurity Law	– Mandatory requirements for critical information infrastructure

Warning

China has mandatory data localization and security review requirements for critical infrastructure operators. Foreign companies operating in China must comply with local regulations.

6.2 Japan

- **METI Guidelines** – Cyber-Physical Security Framework
- **NISC Guidelines** – Critical infrastructure protection
- **JPCERT/CC** – Incident response and security guidance

6.3 South Korea

- **KISA Guidelines** – Korea Internet and Security Agency
- **K-ISMS** – Korean Information Security Management System

6.4 Singapore

- **Cybersecurity Act** – Critical information infrastructure requirements
- **CSA Guidelines** – Cyber Security Agency of Singapore
- **TR64** – Technical reference for ICS security

7 Australia & New Zealand

7.1 Australia

Australian Energy Sector Cyber Security Framework (AESCSF)	
Scope	Energy sector cybersecurity maturity
Publisher	Australian Energy Market Operator (AEMO)
Status	Voluntary self-assessment framework
Alignment	Maps to NIST CSF and IEC 62443

- **SOCI Act** – Security of Critical Infrastructure Act (mandatory)
- **Essential Eight** – ASD security baseline controls
- **ISM** – Information Security Manual

7.2 New Zealand

- **NZISM** – NZ Information Security Manual
- **NCSC Guidelines** – Critical infrastructure guidance

8 Sector-Specific Standards

Certain industries have developed specialized standards:

Sector	Standard	Description
Power Grid	NERC CIP	North American bulk electric system
Oil & Gas	API 1164	Pipeline SCADA security
Oil & Gas	IEC 62443	Commonly adopted in O&G
Water	AWWA Guidance	American Water Works Association
Nuclear	NRC 10 CFR 73.54	US Nuclear cybersecurity rule
Nuclear	IEC 62645	Nuclear I&C security
Maritime	IMO MSC.428	Maritime cyber risk management
Rail	EN 50129	Railway safety-related systems
Automotive	ISO/SAE 21434	Road vehicle cybersecurity

9 Standards Comparison

Standard	Mandatory	Certifiable	OT Focus	Region
IEC 62443	No	Yes	Yes	International
ISO 27001	No	Yes	No	International
NIST 800-82	No	No	Yes	USA
NERC CIP	Yes	No	Yes	North America
NIS2	Yes	No	Partial	EU
GB/T 30976	Yes	No	Yes	China
AESCSF	No	No	Yes	Australia

Tip

When operating across multiple regions, use IEC 62443 as a baseline framework and map it to regional requirements. This approach provides a common foundation while ensuring local compliance.

10 Summary

Key Takeaways

- **IEC 62443** is the leading international OT security standard
- **Regulations are expanding** – NIS2, SOCI Act, and others bring mandatory requirements
- **Sector matters** – Critical infrastructure faces stricter requirements
- **Regional compliance** – Multinational organizations must address local regulations
- **Convergence trend** – Many regional standards reference or align with IEC 62443

11 Further Reading

Standards Organizations

- **IEC** – International Electrotechnical Commission
  https://www.iec.ch/
- **ISA** – International Society of Automation
  https://www.isa.org/
- **NIST** – National Institute of Standards and Technology
  https://www.nist.gov/cyberframework

Regulatory Bodies

- **ENISA** – European Union Agency for Cybersecurity
  https://www.enisa.europa.eu/
- **CISA** – Cybersecurity and Infrastructure Security Agency
  https://www.cisa.gov/
- **BSI** – German Federal Office for Information Security
  https://www.bsi.bund.de/
- **NERC** – North American Electric Reliability Corporation
  https://www.nerc.com/

Books

- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)
- Macaulay, T. & Singer, B. – *Cybersecurity for Industrial Control Systems* (CRC Press)