

No. 99

CYBERSECURITY

OT and Industrial Security

Protecting the systems that run factories, utilities and infrastructure

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 99

OT and Industrial Security

Protecting the systems that run factories, utilities and infrastructure

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

OT and Industrial Security

Protecting the systems that run factories, utilities and infrastructure

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product, company and threat group names mentioned in this book are trademarks or names of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · UNDERSTANDING OT

1 What OT is 5
2 IT versus OT 6
3 Components of industrial systems 8
4 How control works 10
5 Industrial network architecture 12

PART II · THREATS

6 Landmark incidents 15
7 OT threats by the numbers 17
8 Who attacks OT 19
9 How attackers get in 21
10 Why OT is hard to secure 22
11 Buildings, hospitals and smaller sites 23

PART III · DEFENCES

12 The five critical controls 26
13 Segmentation and architecture 27
14 Secure remote access 28
15 Asset inventory 29
16 Monitoring and detection 31
17 Vulnerability management 33
18 Endpoints, accounts and backups 35
19 Safety systems and security 36
20 Vendors and supply chain 37

PART IV · PROGRAMME

21 Standards and regulation 39
22 Incident response in OT 41

FREE SAMPLE · ojayo.com

23 Exercises and resilience 42
24 People and culture 43
25 Emerging trends 44
26 A starter roadmap 45
Checklists 46
Glossary 47
Further reading 48

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Operational technology (OT) is the hardware and software that monitors and controls physical processes: power grids, water treatment, oil and gas pipelines, factories, building systems, hospitals' equipment and transport. When OT is attacked, the result is not just lost data; it can be stopped production, damaged equipment, environmental harm or danger to people.

OT security has become one of the most important areas in cybersecurity. Ransomware increasingly disrupts industrial operations, and state-sponsored groups have been found positioning themselves inside critical infrastructure. This book explains OT and industrial security for beginners, including IT professionals moving into industrial environments and engineers new to cybersecurity.

What this book covers

- What OT is, how it differs from IT, and its key components.
- Landmark incidents, today's threats and how attackers reach industrial systems.
- Defences: the five critical controls, segmentation, remote access, asset inventory, monitoring and vulnerability management.
- Standards such as IEC 62443 and NIST SP 800-82, incident response and building a programme.

Who this book is for

- **IT and security staff** supporting industrial sites.

FREE SAMPLE · ojayo.com

- **Engineers and operators** who want to understand cyber risk.
- **Managers** in manufacturing, utilities and infrastructure.

How the book is organized

- **Part I — Understanding OT** (Chapters 1–5): what OT is, IT versus OT, components, control loops, and architecture.
- **Part II — Threats** (Chapters 6–11): landmark incidents, the numbers, who attacks OT, how they get in, why OT is hard to secure, and buildings and smaller sites.
- **Part III — Defences** (Chapters 12–20): the five critical controls, segmentation, secure remote access, asset inventory, monitoring, vulnerabilities, endpoints and backups, safety systems, and supply chain.
- **Part IV — Programme** (Chapters 21–26): standards and regulation, incident response, exercises and resilience, people and culture, emerging trends, and a roadmap.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks at a real site.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on safety and screens

Never test or change live industrial systems without the plant's engineers and proper approval: cyber actions can have physical consequences. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Understanding OT

These chapters explain what operational technology is, how it differs from IT, its main components and how industrial networks are organized.

FREE SAMPLE · ojayo.com

CHAPTER 1

What OT is

OT is technology that interacts with the physical world.

Definition

Operational technology covers the systems that detect or cause changes in physical processes by monitoring and controlling equipment. You will also hear **industrial control systems (ICS)**, **SCADA** and **cyber-physical systems**.

Where OT is found

- **Energy**: power generation, transmission and distribution.
- **Water**: treatment plants and pumping stations.
- **Manufacturing**: assembly lines, robots, chemical processes.
- **Oil and gas**: pipelines and refineries.
- **Transport**: rail signalling, ports, airports.
- **Buildings**: heating, ventilation, lifts and access control.
- **Healthcare**: building systems and some medical equipment.

Why it matters

Society depends on OT. Disruption can affect thousands or millions of people, which is why many OT operators are designated as **critical infrastructure** with specific legal duties.

KEY IDEA

In OT, a cyber incident can have physical consequences.

FREE SAMPLE · ojayo.com

CHAPTER 2

IT versus OT

IT and OT have different priorities, lifetimes and constraints.

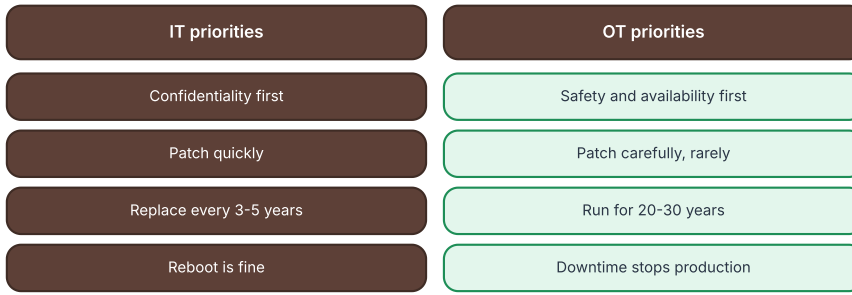


Figure 2.1 IT and OT see the world differently

Priorities

IT security often puts **confidentiality** first. OT puts **safety** and **availability** first: the plant must keep running safely.

Lifetimes

Industrial equipment may run for 20 to 30 years. Some systems still use old operating systems that no longer receive security updates.

Change is risky

Patching or rebooting a controller can stop production or, in the worst case, affect safety. Changes need testing, planning and often a scheduled shutdown.

FREE SAMPLE · ojayo.com

Convergence

IT and OT are increasingly connected for remote monitoring, analytics and efficiency. That brings benefits, and also IT's threats into OT.

WATCH OUT

Applying IT security tools to OT without care, such as aggressive network scanning, can crash fragile devices.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security (you are reading this)
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

OT and Industrial Security

Enjoyed it? The full book has 53 pages and 26 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.