HORIZONSHIELD ORIGINALS · BOOK 18

OT & ICS Security Fundamentals

Securing Industrial Control Systems & Critical Infrastructure

Operational technology and ICS security covering the Purdue model, IEC 62443, SCADA vulnerabilities, OT network monitoring, and incident response for industrial environments.

HORIZONSHIELD

SPECIALIZED

CONFIDENTIAL — © 2026 HorizonShield

Contents

CONFIDENTIAL — © 2026 HorizonShield

CHAPTER 01

OT/ICS Security Fundamentals

Operational Technology (OT) and Industrial Control Systems (ICS) run the physical world — power grids, water treatment, manufacturing, pipelines. Attacks on OT can cause physical damage, safety incidents, and loss of life. Security principles from IT must be adapted carefully for OT environments.

IT vs OT Security Priorities

Priority	IT (Information Technology)	OT (Operational Technology)
1st	Confidentiality	**Safety**
2nd	Integrity	**Reliability/Availability**
3rd	Availability	**Integrity**
4th	Security patching (fast)	Confidentiality (lower priority)
Key concern	Data breach, ransomware	Physical damage, safety incident
Patch tolerance	Patch frequently, restart OK	Patching may require production downtime
Uptime expectation	99.9% — some downtime tolerated	99.999% — 5 minutes/year maximum

The Purdue Reference Model (ICS Architecture)

```
Level 5 — Enterprise Network (IT)
  Business systems, ERP, corporate email
Level 4 — Site Business Network
  Historian servers, engineering workstations
──────── DEMILITARIZED ZONE (DMZ) ────────
Level 3 — Site Operations
  SCADA servers, HMI servers, data historians
Level 2 — Area Control
  Supervisory HMI, local historians, batch managers
Level 1 — Basic Control
  PLCs, DCS controllers, RTUs
Level 0 — Physical Process
  Sensors, actuators, drives, valves
```

IT/OT Convergence Risk: Modern OT networks are increasingly connected to IT networks for data analytics, remote monitoring, and business integration. Every IT/OT connection is a potential attack path from the internet to physical systems. The DMZ is your most critical security control — protect it with extreme care.

CONFIDENTIAL — © 2026 HorizonShield

CHAPTER 02

OT Threat Landscape & Notable Attacks

OT cyberattacks have escalated dramatically. Nation-state actors, criminal groups, and hacktivists target critical infrastructure with increasingly sophisticated tools designed specifically for industrial protocols.

Notable OT/ICS Attacks

Attack	Year	Target	Impact	Vector
Stuxnet	2010	Iran nuclear centrifuges	Destroyed 1,000+ centrifuges	USB drop, Siemens PLC exploit
Ukrainian Power Grid	2015	Ukrainian electricity	230,000 customers lost power	Spear phishing, BlackEnergy
Triton/TRISIS	2017	Saudi petrochemical plant	Safety systems targeted (near explosion)	IT pivot to Safety Instrumented System
Oldsmar Water	2021	Florida water treatment	NaOH increase 111x — caught by operator	TeamViewer remote access
Colonial Pipeline	2021	US fuel pipeline operator	Fuel shortages; $4.4M ransom paid	VPN credential compromise

OT Security Controls

- **Network segregation:** Air gap or DMZ between IT and OT — no direct connections
- **Unidirectional gateways:** Data diodes for historian data to IT (physically one-way)
- **Asset inventory:** Know every PLC, RTU, HMI — OT asset management is often nonexistent
- **Passive monitoring:** Nozomi Networks, Claroty, Dragos — OT-safe passive IDS
- **Remote access controls:** Jump server with MFA; no direct vendor VPN to OT
- **Patch management:** Vendor-approved patches only; test in non-production first

CONFIDENTIAL — © 2026 HorizonShield

CHAPTER 03

IEC 62443 Compliance Framework

IEC 62443 is the international standard series for industrial cybersecurity. It defines requirements for asset owners, system integrators, and product suppliers — covering the entire ICS supply chain.

IEC 62443 Security Levels

Level	Protection Against	Typical Zone
SL 0	No specific requirements	Non-critical systems
SL 1	Casual/unintentional violation	General industrial zones
SL 2	Intentional violation with simple means	Most operational zones
SL 3	Sophisticated attack with moderate resources	Critical operational zones
SL 4	Nation-state level sophisticated attack	Safety-critical systems only

```
# IEC 62443 Zone and Conduit Model
Zone: Logical grouping of assets with same security level
Conduit: Communication path between zones — each conduit
         must be explicitly authorized and protected

Example Zone Design:
  Zone A (SL2): SCADA servers, HMI — protected by NGFW
  Zone B (SL3): Critical PLCs — isolated, one-way comms
  Zone C (SL4): Safety Instrumented System — air-gapped

Conduit A-B: One-way data diode (Zone A reads Zone B data)
Conduit B-C: No electronic connection — hardwired interlock only
```


CONFIDENTIAL — © 2026 HorizonShield

CHAPTER 04

OT Incident Response

OT incident response differs fundamentally from IT IR. Containment actions that are standard in IT (network isolation, system shutdown) can cause physical damage, safety incidents, or production loss in OT environments.

OT IR Decision Framework

```
Before ANY containment action in OT, ask:
  1. SAFETY: Does this action risk physical injury or environmental harm?
  2. PRODUCTION: Will this stop a physical process mid-operation?
  3. SAFETY SYSTEMS: Are Safety Instrumented Systems (SIS) affected?
  4. OPERATOR: Is the control room operator aware and ready?

NEVER in OT:
  - Isolate a PLC controlling an active physical process without operator
  - Restart OT systems without change management and operator consent
  - Apply patches to production OT without vendor approval
  - Block network traffic without understanding physical impact

OT-Specific IR Steps:
  1. Notify OT operations team BEFORE taking any technical action
  2. Assess physical process state (is anything dangerous happening?)
  3. Ensure safety systems (SIS) are independent and functioning
  4. Engage OT vendor and ICS-CERT before changes
  5. Prefer monitoring over blocking in active OT incidents
```

>

ICS-CERT: For significant OT incidents, contact CISA ICS-CERT immediately: 1-888-282-0870 or report at ics-cert.us-cert.gov. ICS-CERT provides free technical assistance and has OT-specific expertise not available in most private IR firms.

CONFIDENTIAL — © 2026 HorizonShield

HS

HORIZONSHIELD ORIGINALS

Complete Security Library

HorizonShield Originals are practitioner-written guides designed for real-world implementation — from SMB security foundations to advanced threat hunting, cloud architecture, and regulatory compliance.

AVAILABLE IN THIS SERIES

01 SMB Cybersecurity Guide 2026
02 Penetration Testing Checklist
03 Incident Response Playbook
04 DORA Compliance Guide
05 Cloud Security Hardening
06 Zero Trust Architecture
07 Threat Hunting SOC Operations
08 DevSecOps Implementation
09 Web Application Security
10 Network Security Fundamentals
11 Linux & Systems Security
12 Social Engineering & Human Hacking
13 Malware Analysis & Reverse Engineering
14 Digital Forensics & Incident Response
15 Applied Cryptography
16 Compliance Audit & Risk Management
17 AI & LLM Security Guide
18 OT & ICS Security
19 Mobile Security
20 Kubernetes Security
21 Bug Bounty Methodology
22 Security Architecture for Startups

horizonshield.net/library

Download all 16 books · Access labs · Track your progress

© 2026 HorizonShield. All rights reserved.

horizonshield.net