IT vs OT

Understanding the Fundamental Differences

OT Security Learning Series

Document 001 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 Definitions **3**
2.1 Information Technology (IT) . . . 3
2.2 Operational Technology (OT) . . . 3
2.3 Industrial Control Systems (ICS) . . . 4

3 Key Differences **4**
3.1 Priority: CIA vs AIC . . . 4
3.2 Comparison Table . . . 5
3.3 System Lifecycles . . . 5
3.4 Communication Protocols . . . 5

4 IT/OT Convergence **6**
4.1 What is Convergence? . . . 6
4.2 Convergence Challenges . . . 6
4.3 The Air Gap Myth . . . 6

5 Security Implications **7**
5.1 Why OT Security is Different . . . 7
5.2 Common Mistakes . . . 7
5.3 Real-World Incidents . . . 7

6 Bridging the Gap **7**
6.1 Organizational Approaches . . . 8
6.2 Technical Approaches . . . 8

7 Summary **8**

8 Further Reading **8**

1 Introduction

The worlds of Information Technology (IT) and Operational Technology (OT) have traditionally been separate domains with distinct priorities, technologies, and cultures. However, increasing digitalization and connectivity are driving convergence between these two worlds, creating new challenges for security professionals.

Information

Understanding the fundamental differences between IT and OT is essential for anyone working in industrial cybersecurity. Applying IT security practices directly to OT environments without adaptation can lead to operational disruptions or safety incidents.

2 Definitions

2.1 Information Technology (IT)

Information Technology (IT)

IT encompasses the hardware, software, and networks used to process, store, and transmit **data and information**. IT systems support business operations, communication, and data management.

Examples:

- Servers, workstations, laptops
- Enterprise applications (ERP, CRM, email)
- Databases and data centers
- Corporate networks and internet connectivity

2.2 Operational Technology (OT)

Operational Technology (OT)

OT encompasses the hardware, software, and networks used to monitor and control **physical processes, devices, and infrastructure**. OT systems directly interact with the physical world.

Examples:

- Programmable Logic Controllers (PLCs)
- SCADA systems and HMIs
- Distributed Control Systems (DCS)
- Industrial robots and machinery
- Building automation systems

2.3 Industrial Control Systems (ICS)

Industrial Control Systems (ICS)

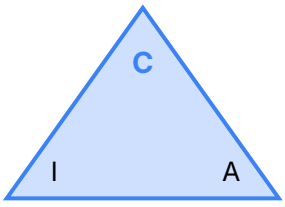
ICS is a subset of OT that specifically refers to the control systems used in industrial environments. The term encompasses SCADA, DCS, PLCs, and other control system components.

3 Key Differences

3.1 Priority: CIA vs AIC

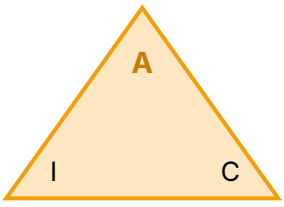
The most fundamental difference between IT and OT lies in the prioritization of security objectives.

IT Priority



Confidentiality (top)
Integrity **A**vailability

OT Priority



Availability (top)
Integrity **C**onfidentiality

Why Availability is King in OT

- **Safety:** System downtime can endanger human lives
- **Physical consequences:** Processes cannot simply be "restarted"
- **Financial impact:** Production downtime costs can be enormous
- **Environmental:** Failures can cause environmental damage

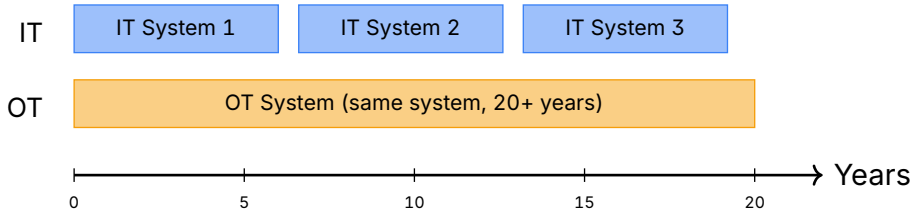
3.2 Comparison Table

Aspect	IT	OT
Primary Goal	Process data	Control physical processes
Top Priority	Confidentiality	Availability / Safety
Downtime Tolerance	Minutes to hours acceptable	Seconds can be critical
System Lifecycle	3–5 years	15–25+ years
Patching	Regular, often automated	Rare, requires planning
Change Management	Agile, frequent updates	Rigid, infrequent changes
Environment	Climate-controlled offices	Harsh industrial conditions
Protocols	TCP/IP, HTTP, SQL	Modbus, DNP3, OPC, Profinet
Real-time Requirements	Generally not critical	Often millisecond precision
Security Testing	Penetration testing common	Can cause physical damage
Vendor Dependency	Multiple vendors, standards	Proprietary, vendor lock-in
Staff Background	Computer science, IT	Engineering, process control

3.3 System Lifecycles

Warning

OT systems often run for 15–25 years or longer. It is common to find Windows XP, Windows 7, or even older systems still operating critical infrastructure because the control system vendor only supports those platforms.



3.4 Communication Protocols

Protocol Differences

IT Protocols:

- TCP/IP, HTTP/HTTPS, TLS
- Built-in security features (encryption, authentication)
- Well-documented, standardized

OT Protocols:

- Modbus (1979), DNP3, BACnet, Profinet, EtherNet/IP
- Often no built-in security (designed for isolated networks)
- Proprietary variations common

Critical

Many OT protocols were designed decades ago when networks were physically isolated. They lack authentication, encryption, and integrity checking. A single packet can command a PLC to perform dangerous actions.

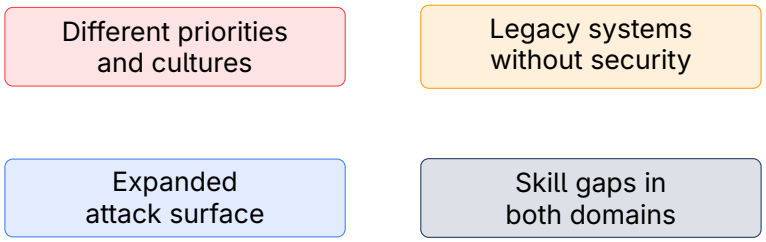
4 IT/OT Convergence

4.1 What is Convergence?

IT/OT convergence refers to the increasing integration of IT and OT systems, driven by:

- **Industry 4.0 / IIoT:** Connected sensors, cloud analytics, digital twins
- **Business requirements:** Real-time data for decision making
- **Remote operations:** Centralized monitoring and control
- **Cost reduction:** Shared infrastructure and standard technologies

4.2 Convergence Challenges



Warning

Convergence increases the attack surface. Attackers can now potentially reach OT systems through IT networks, email phishing, or compromised vendor connections.

4.3 The Air Gap Myth

Tip

The belief that OT networks are "air-gapped" (physically isolated) is often false. Studies show most OT environments have some connection to IT networks or the internet, whether intended or not.

Common connectivity paths:

- Historian servers replicating to business networks
- Remote access for vendors and operators
- USB drives and laptops moving between networks
- Dual-homed engineering workstations

- Cloud-based monitoring and analytics

5 Security Implications

5.1 Why OT Security is Different

1. **Safety first:** Security controls must not compromise safety systems
2. **No downtime for patching:** Systems run 24/7/365
3. **Testing limitations:** Cannot test on production systems
4. **Vendor dependencies:** Changes may void warranties or certifications
5. **Long lifecycles:** Must secure systems for decades
6. **Physical consequences:** Cyber attacks can cause real-world harm

5.2 Common Mistakes

Critical

Applying IT practices directly to OT can be dangerous:

- Automatic updates may crash control systems
- Antivirus scans can cause CPU spikes and missed deadlines
- Active vulnerability scanning may disrupt PLCs
- Network segmentation can break process dependencies

5.3 Real-World Incidents

Notable incidents demonstrating IT/OT security failures:

- **Stuxnet (2010):** Malware crossed IT/OT boundary to destroy centrifuges
- **Ukraine Power Grid (2015):** IT compromise led to OT manipulation
- **TRITON/TRISIS (2017):** Targeted safety instrumented systems
- **Colonial Pipeline (2021):** IT ransomware caused OT shutdown
- **Oldsmar Water (2021):** Remote access exploit to manipulate chemicals

6 Bridging the Gap

6.1 Organizational Approaches

Key Point

Successful IT/OT security requires collaboration, not competition. Neither team can secure converged environments alone.

- **Joint governance:** Combined IT/OT security committees
- **Cross-training:** IT staff learn process safety; OT staff learn cybersecurity
- **Shared responsibility:** Clear RACI for converged systems
- **Unified policies:** Adapted for both environments

6.2 Technical Approaches

- **Network segmentation:** Purdue Model, DMZ between IT and OT
- **Secure remote access:** Jump servers, MFA, session recording
- **OT-specific tools:** Passive monitoring, OT-aware firewalls
- **Asset inventory:** Know what's connected before securing it
- **Compensating controls:** When patching isn't possible

7 Summary

Key Takeaways

- **IT manages data**; **OT controls physical processes**
- OT prioritizes **availability and safety** over confidentiality
- OT systems have **much longer lifecycles** (15–25+ years)
- IT/OT **convergence is increasing**, expanding the attack surface
- **Direct application of IT security** to OT can cause harm
- Successful security requires **collaboration** between IT and OT teams

8 Further Reading

Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443** – Industrial Automation Security
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Resources

- **CISA** – ICS Security Resources
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS** – Industrial Control Systems Security
  https://www.sans.org/industrial-control-systems-security/

Books

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