FREE

CYBERSECURITY OT & NIS2

# OT vs IT — Fundamental Differences

*OT vs IT — air-gap myth, real protocols, why CIA inverts.*


· **Cybersecurity OT & NIS2** Lesson 1 of 10

Operational Technology (OT) controls physical processes — BMS, lifts, HVAC, security systems. IT processes data. They have different threat models, different priorities, different lifecycles.

This lesson sets the foundational distinction that makes OT cybersecurity its own discipline.

## Learning objectives

| | |
|---|---|
| Remember | Key concepts. |
| Understand | Why OT differs. |
| Understand | Frameworks and controls. |
| Apply | Recognise risk on a real project. |

## 1 · CIA triad inverts

IT prioritises Confidentiality, Integrity, Availability. OT prioritises Availability, Integrity, Confidentiality. Lift cannot stop because of a security update; data center cooling cannot pause for password rotation.

## 2 · Lifecycles differ

IT equipment refresh: 3–5 years. OT equipment: 15–25 years. Many BMS controllers in service from the 1990s-2000s. Patching constraints inherit from this.

## 3 · Protocols differ

IT: TCP/IP, HTTPS, modern encryption. OT: Modbus (1979, no auth), BACnet (limited security), Profinet, OPC UA. Many native OT protocols pre-date security as a concept.

## 4 · Air-gap myth

"OT is air-gapped" — typically isn't. BMS reaches the cloud for analytics, remote monitoring, mobile apps. Stuxnet (2010) crossed an actual air gap. NIS2 reports document multiple OT incidents in EU buildings 2024–2025.

## 5 · What this looks like on a real project

UK

### BMS exposed to internet

Shodan searches regularly find UK BMS controllers exposed without authentication. Building Safety Act 2022 doesn't directly cover cybersecurity but accountability is rising.

EU

### NIS2 brings buildings into scope

NIS2 expanded scope captures large building operators as essential / important entities. Compliance from 17 October 2024 / 2025 in member states.

### UAE TRA cybersecurity guidance

UAE Telecommunications Regulatory Authority publishes cybersecurity guidance increasingly applicable to building automation systems.

## 6 · Why this matters

OT and IT both have screens and ethernet but everything else is different — uptime priorities, lifecycles, threat models, patching tolerance. You can now explain the difference to leadership without simplifying it into a slogan. That clarity is the foundation for every later security decision.

## Quiz

**Your score** 0 / 5

**1. In OT, the priority is:**

a) C-I-A

b) A-I-C (availability first)

c) C-A-I

d) Random

**2. Modbus protocol dates from:**

a) 2010s

b) 1979

c) 2000

d) 1995

**3. Typical BMS controller lifecycle:**

a) 1 year

b) 15–25 years

c) 6 months

d) 100 years

---

**4. Stuxnet (2010) demonstrated:**

a) IT systems are unhackable

b) OT systems can be attacked even when air-gapped

c) Modbus is secure

d) Air gaps prevent all attacks

---

**5. NIS2 effective transposition deadline:**

a) 2020

b) 17 October 2024

c) 2030

d) Unspecified

---

**Answers (for print):** 1b · 2b · 3b · 4b · 5b

# Resources

**PRIMARY SOURCES**

- Directive (EU) 2022/2555 (NIS2).
- IEC 62443 series.

- NIST SP 800-82 (Industrial Control Systems Security).

### STANDARDS AND GUIDANCE

- ISO 27001 / 27002 (IT, mappable to OT).
- IEC 62443-2-1 (security management).

### INDEPENDENT COMMENTARY

- ENISA OT cybersecurity reports.
- CISA ICS advisories.

YOU'VE FINISHED A FREE SAMPLE

# Ready for the rest of the course?

The remaining lessons are where the working detail lives — the standards, the deadlines, the scenarios, the engineering judgment. All written from practice, with primary-source citations.

## Unlock all 97 lessons across 10 courses

Downloadable resources · Quiz tracking · Standards updates · 30-day refund

## Get Pro · £99 / yr

or £39 per single course · cancel anytime · 30-day money-back

**Continue at academy.novtriq.tech**