# OT Security fundamentals

**Márton Bor**

E-mail: international@budapestwaterworks.hu
Web: www.budapestwaterworks.hu


## INTRODUCTION

Critical infrastructures are being targeted by different threat actors including nation-state actors or hacktivists for various reasons. Defending against the emerging threat is not a simple task. Traditional IT based preventive measures might not work or cannot be applied in an OT environment therefore a unique approach is required. OT is not IT. OT (Operational Technology) also suffers from vulnerabilities from historical reasons.
The number of OT related cyber-attacks are increasing. Unfortunately, we live in a time when critical infrastructures are being targeted by nation-state threat actors or hacker groups. A good example is the recent attack (2025 December) against the Polish energy sector. The targets were heath and power plants, renewable energy facilities. The aim was to destabilize the energy supply of Poland. Unfortunately, drinking water suppliers are also being targeted. According to DWI (Drinking Water Inspectorate) between 2024 January 1 and 2025 October 20 hackers launched five cyberattacks against Britain's drinking water suppliers. Water utilities must prepare and defend themselves against this emerging threat.[1][2][3][4]

By applying industry-proven best practices, design guides, and proven models, you can significantly reduce risks. The designs and strategies outlined below provide a quick introduction to the core concepts of OT security. For a deeper dive, refer to the resources listed at the end of the presentation.

## OT VS IT

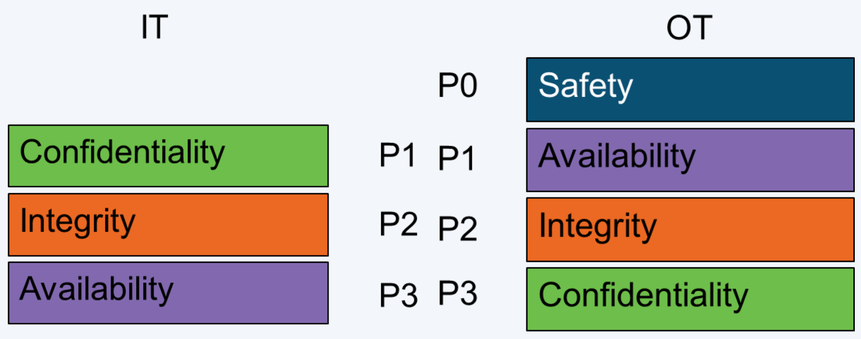


Figure 1 – IT VS OT priorities

IT and OT have different priorities and consequences.

In IT, the CIA triad is a well-known term. Its three priorities: confidentiality, integrity, and availability are listed in that order.

In IT a cyber threat could result in, for example, information loss (financial, intellectual property, personal (employee or customer)), downtime, loss of reputation. All of these impacts usually translate into direct monetary losses.

In OT an ICS controls physical processes. Therefore, the results can be physical too.
The priorities are **Safety, Availability, Integrity, Confidentiality.**
In an OT environment a cyber threat can result in catastrophic physical consequences. For example: no drinking water, injury of employees, loss of human life, damage to the environment.

The operational environment is usually different too. IT devices work in a controlled environment such as a datacentre or office. In an OT environment, devices often have to operate under harsh conditions such as extreme heat, dust, high humidity, and vibration. Therefore, ruggedized devices are being used. The lifecycle of devices is also different.
In IT there are usually well documented or open protocols, in OT there are many proprietary hardware or protocols where interoperability between different manufacturers can be challenging.[5]

## DEFENCE IN DEPTH

Multiple, layered, and overlapping security controls. Holistic approach to protect assets.

- Policies, education
- Lock, key card
- FW, ACL, AAA
- Hardening, Patch
- SDLC, AAA
- Hardening, Lifecycle [5][8]

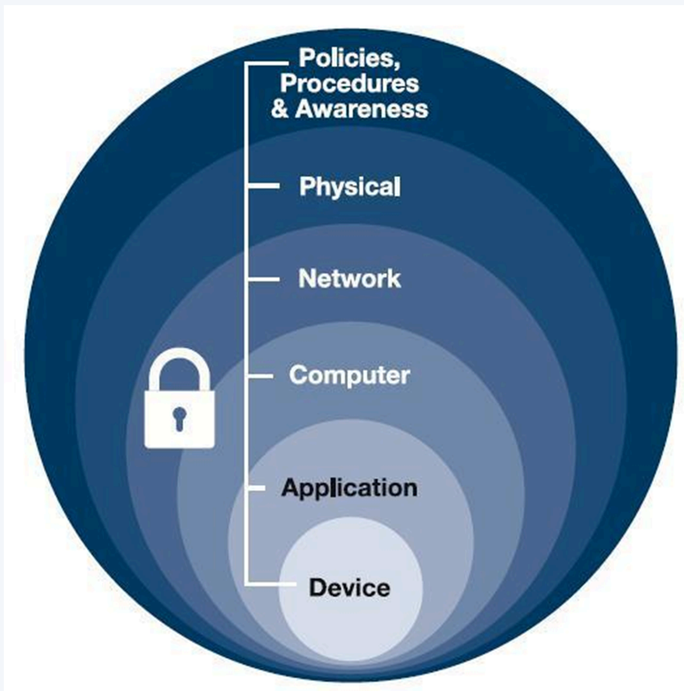


Figure 3 – Defense In Depth [8]

## PURDUE MODEL

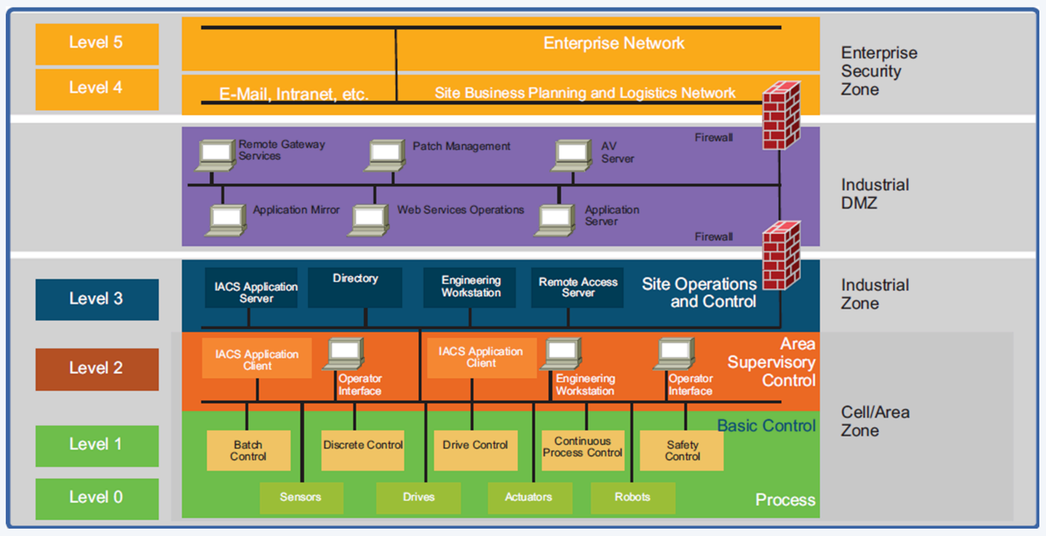


Figure 2 – Purdue model [6]

The Purdue model is a reference architecture available in several versions that provides a structured framework for planning.

**Levels of the model**
Level 0 Process: sensors, actuators, valves, devices related to the basic industrial process
Level 1 Basic Control: controllers that manipulate the manufacturing process
Level 2 Area Supervisory Control: Cell/Area Zone supervision and operation
Level 3 Site Operations and Control: Applications related to the site operation for example DNS, NTP, Site-level operations management, Historian, Workstation
Level 3.5 Industrial DMZ: Separates Industrial and Enterprise zone. Mirrored services, Remote access, Patch management, AV, Application mirror

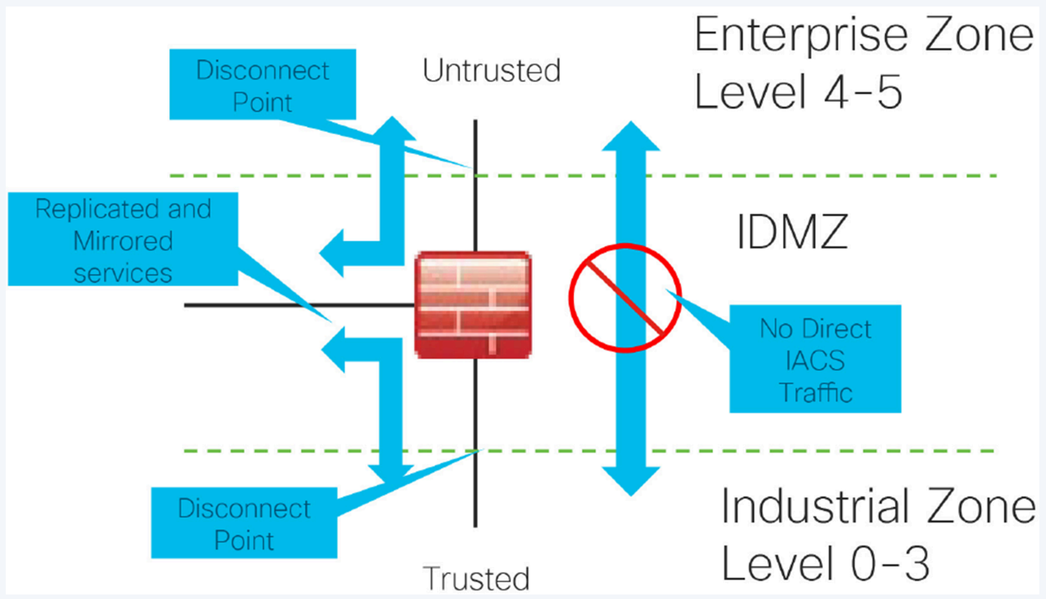


Figure 3 – iDMZ [6]

Level 4/5 Enterprise Security Zone: Services provided by Enterprise network. Internet access, SAP, ERP, E-mail, Intranet

SIS Safety Instrumented System: Last line of defence, prevent accidents, independent, airgap

You can also define multiple industrial zones where it makes sense for instance, to separate water and wastewater systems if they are not interrelated.[6][7]

## USEFUL RESOURCES

- SANS, CISA, Dragos ICS recommendations, OT specific trainings
- Cisco, Fortinet and other manufacturers OT specific design guides
- Defense In Depth: CISA "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies"
- Industrial Cybersecurity: Efficiently secure critical infrastructure systems ISBN 1788395158
- Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment ISBN 1800202091

References:
[1] Journal: SANS Institute 2025 survey finds OT cybersecurity incidents rising as ransomware and remote access risks grow - Industrial Cyber
[2] Journal: Hackers are attacking Britain's drinking water suppliers | The Record from Recorded Future News
[3] Journal: Operational Technology Security Trends And Risks In 2026 | Netwitness
[4] Report: Energy Sector Incident Report - 29 December 2025 | CERT Polska
[5] Book: Industrial Cybersecurity: Efficiently secure critical infrastructure systems ISBN 1788395158
[6] Design Guide: Networking and Security in Industrial Automation Environments Design and Implementation Guide - Networking and Security in Industrial Automation Environments [Network Security] – Cisco
[7] Design guide: Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense - Chapter 2: System Design Considerations [Design Zone] - Cisco
[8] Journal: Defence in Depth | Openpracticelibrary

Gold Standard for Utility Perfomance