The Purdue Model

Understanding Industrial Network Architecture and Segmentation

OT Security Learning Series

Document 010 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

The **Purdue Enterprise Reference Architecture** (PERA), commonly known as the **Purdue Model**, is a reference model for industrial control system (ICS) network segmentation. Originally developed in the 1990s at Purdue University, it has become the de facto standard for designing secure OT network architectures.

Information

The Purdue Model provides a hierarchical framework that separates industrial networks into distinct levels, each with specific functions and security requirements. This separation is fundamental to implementing defense-in-depth strategies in OT environments.

1.1 Why the Purdue Model Matters

In modern industrial environments, the convergence of IT and OT systems creates significant security challenges:

- Legacy OT systems were designed for reliability, not security
- Flat networks allow lateral movement during attacks
- IT-based threats can now reach physical processes
- Regulatory frameworks (IEC 62443, NIST) reference this model

Key Point

The Purdue Model helps organizations understand **where** security controls should be placed and **what** traffic should flow between different parts of the industrial network.

2 The Purdue Model Levels

The model defines six primary levels (0-5), plus a demilitarized zone (DMZ) between the OT and IT networks.

2.1 Level 0 – Physical Process

Level 0 Physical Process

Function: The actual physical equipment and processes
Components:
- Sensors (temperature, pressure, flow, level)
- Actuators (valves, motors, pumps)
- Physical machinery and production equipment

Security Considerations:
- No network connectivity at this level
- Physical security is paramount
- Tampering detection mechanisms

2.2 Level 1 – Basic Control

Level 1 Basic Control

Function: Direct control of the physical process
Components:
- Programmable Logic Controllers (PLCs)
- Remote Terminal Units (RTUs)
- Intelligent Electronic Devices (IEDs)
- Variable Frequency Drives (VFDs)

Protocols: Modbus, PROFINET, EtherNet/IP, DNP3
Security Considerations:
- Often lacks authentication mechanisms
- Firmware updates require careful planning
- Network isolation is critical

2.3 Level 2 – Area Supervisory Control

Level 2 Area Supervisory Control

Function: Supervising and controlling the physical process
Components:
- Human-Machine Interfaces (HMIs)
- SCADA systems
- Engineering Workstations
- Local operator consoles

Security Considerations:
- User authentication required
- Application whitelisting recommended
- USB and removable media controls

2.4 Level 3 – Site Operations

Level 3 Site Operations

Function: Site-wide monitoring, optimization, and data collection
Components:
- Data Historians
- OPC servers
- Batch management systems
- Manufacturing Execution Systems (MES)
- Asset management systems

Security Considerations:
- Database security and access controls
- Secure remote access configuration
- Integration point with business systems

2.5 Level 3.5 – Industrial DMZ

DMZ Industrial Demilitarized Zone

Function: Buffer zone between OT and IT networks
Components:
- Data diodes (unidirectional gateways)
- Jump servers / Bastion hosts
- Patch management servers
- Antivirus update servers
- Remote access gateways

Security Considerations:
- No direct connectivity between IT and OT
- All traffic must be proxied through DMZ
- Strict firewall rules on both sides

Warning

The DMZ is **critical** for protecting OT networks. Never allow direct connections from Level 4/5 to Levels 0-3. All data exchange should pass through DMZ services.

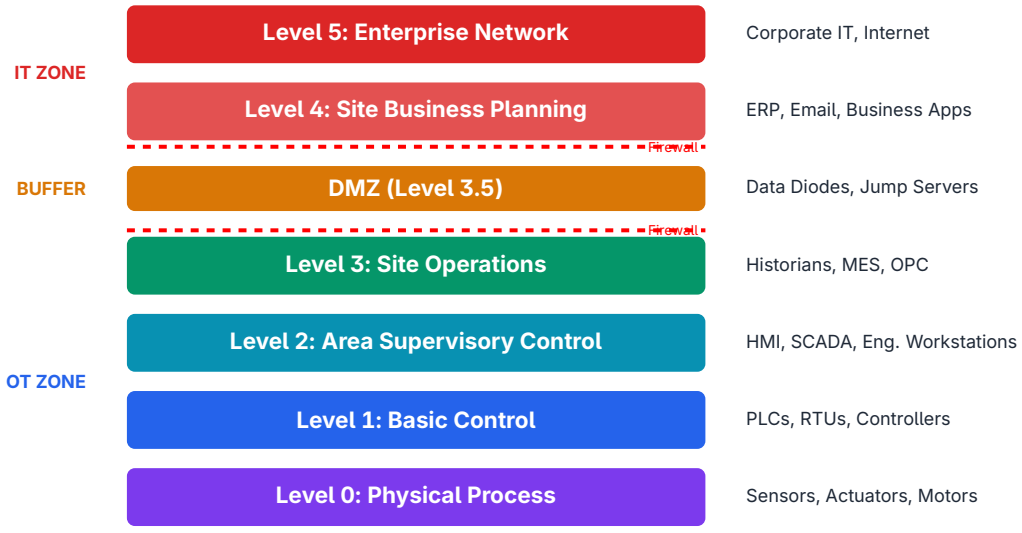
2.6 Levels 4 & 5 – Enterprise

Level 4/5 Enterprise Network

Function: Business operations and enterprise IT
Level 4 – Site Business:
- Site email and intranet
- ERP system interfaces
- Business reporting

Level 5 – Enterprise Network:
- Corporate network
- Cloud services
- Internet connectivity
- External business partners

3 Purdue Model Diagram



4 Implementing the Purdue Model

4.1 Key Principles

1. **Network Segmentation:** Each level should be on separate network segments/VLANs
2. **Traffic Control:** Firewalls between levels with strict rule sets
3. **Data Flow:** Information flows up; commands flow down
4. **No Bypass:** Never skip levels (e.g., no direct Level 5 to Level 1 connection)

4.2 Common Mistakes to Avoid

Critical

Flat Networks: Many legacy OT environments have flat networks where all devices can communicate directly. This allows attackers to move laterally from compromised IT systems directly to PLCs.

Warning

Direct Remote Access: Allowing VPN connections directly into Level 2 or below bypasses the DMZ protection and creates significant risk.

4.3 Firewall Rules Example

Basic firewall policy between DMZ and Level 3:

- **Allow:** Historian replication (specific ports, specific hosts)
- **Allow:** Patch downloads from DMZ server to Level 3
- **Deny:** All inbound connections from IT to OT
- **Deny:** Direct database queries from IT
- **Log:** All denied traffic for analysis

5 Summary

Key Takeaways

Level 0	Physical process – sensors and actuators
Level 1	Basic control – PLCs, RTUs
Level 2	Supervisory – HMI, SCADA
Level 3	Operations – Historians, MES
DMZ	Buffer zone – data diodes, jump servers
Level 4-5	Enterprise – IT and business systems

Tip

When assessing an OT environment, start by mapping the existing network to the Purdue Model. This helps identify gaps in segmentation and areas where security controls are missing.

6 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 Series** – Industrial Automation and Control Systems Security
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **ISA-95 / IEC 62264** – Enterprise-Control System Integration
  https://www.isa.org/isa95

Resources

- **CISA** – ICS Security Recommended Practices
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS** – Industrial Control Systems Security Resources
  https://www.sans.org/industrial-control-systems-security/
- **Purdue Enterprise Reference Architecture** – Original Williams Paper (1992)
  Reference: Williams, T.J. "The Purdue Enterprise Reference Architecture"

Books

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

Part of the OT Security Learning Series