Purdue Model Limitations

When Traditional Segmentation Meets Modern Connectivity

OT Security Learning Series

Document 309 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

The Purdue Enterprise Reference Architecture, developed in the 1990s, has guided OT network segmentation for decades. It assumes clear physical boundaries between hierarchical levels, with traffic flowing predictably between adjacent zones. However, modern technologies—cloud connectivity, software-defined networking, virtualization, and IIoT—challenge these fundamental assumptions.

Information

This document examines why the traditional Purdue Model is increasingly difficult to enforce in modern OT environments. It explores the technical and business drivers that break zone boundaries, and presents complementary security approaches for environments where strict hierarchical segmentation is not achievable.

2 Original Purdue Assumptions

2.1 Design Principles

The Purdue Model was built on assumptions that no longer hold true:

Assumption	Modern Reality
Physical network separation	Virtualized, software-defined networks
Air-gapped OT networks	Cloud connectivity, remote access requirements
Traffic flows between adjacent levels	Direct cloud connections bypass hierarchy
Static, well-defined boundaries	Dynamic workloads, containerization
On-premise systems only	Hybrid cloud, edge computing, SaaS
Predictable communication patterns	API-driven, event-based architectures

Table 1: Purdue assumptions vs. modern reality

2.2 The Hierarchical Model

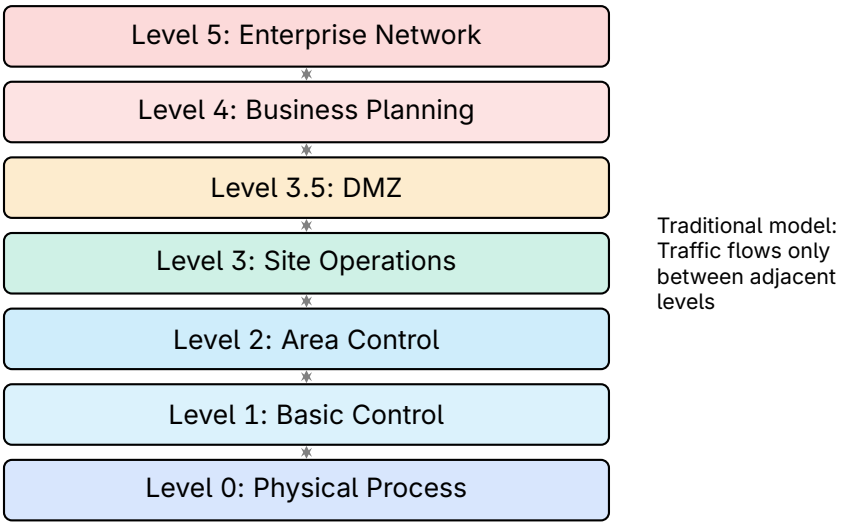

Figure 1: Traditional Purdue hierarchical traffic flow

3 Why Boundaries Break Down

3.1 Cloud Connectivity

Modern OT increasingly connects directly to cloud services:

- **Predictive maintenance** – Sensor data sent to cloud analytics
- **Remote monitoring** – Vendor dashboards and alerting
- **Edge-to-cloud** – IIoT gateways bypassing traditional hierarchy
- **Digital twins** – Real-time process simulation in cloud

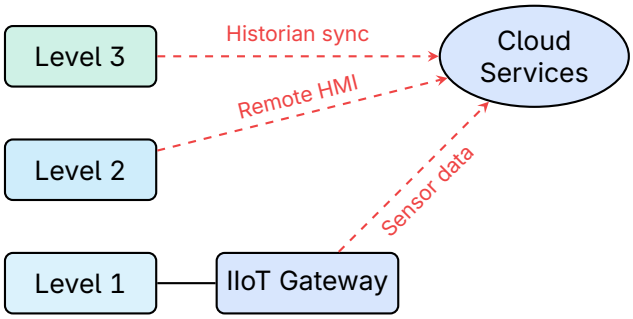

Figure 2: Cloud connections bypass Purdue hierarchy

Warning

Cloud connectivity creates direct paths from lower Purdue levels to the internet, bypassing the DMZ and enterprise layers entirely. Traditional perimeter controls cannot inspect or control this traffic.

3.2 Software-Defined Networking

SDN and virtualization abstract physical network boundaries:

- **Virtual switches** – Traffic between VMs may not traverse physical firewalls
- **Overlay networks** – Logical networks span physical infrastructure
- **Micro-services** – Workloads communicate across traditional boundaries
- **Container orchestration** – Dynamic IP assignments break static rules

3.3 Converged Infrastructure

Technology	Boundary Challenge
Hyperconverged systems	Multiple Purdue levels on single physical host
Virtualized PLCs	Control logic runs alongside IT workloads
Edge computing	Processing at Level 1 communicates directly with cloud
Unified namespaces	Data accessible across all levels simultaneously
API gateways	RESTful interfaces expose OT data to any consumer

Table 2: Converged technologies that blur boundaries

3.4 Remote Access Requirements

Business drivers demand connectivity that breaks isolation:

- **Vendor support** – Remote troubleshooting and maintenance
- **Distributed operations** – Central control rooms for multiple sites
- **Mobile workforce** – Engineers need access from anywhere
- **Third-party integration** – Supply chain and customer systems

4 Security Implications

4.1 Attack Surface Expansion

When boundaries blur, attack surfaces expand:

- Cloud credentials compromise can reach OT directly
- Lateral movement paths bypass zone firewalls

- Supply chain attacks through connected vendors
- Internet-exposed OT components become targets

Critical

A compromised cloud account or vendor VPN can provide direct access to Level 1-2 systems, bypassing all intermediate controls that the Purdue Model assumes exist.

4.2 Visibility Gaps

Traditional monitoring assumes traffic passes through chokepoints:

- East-west traffic within virtualized environments is invisible
- Encrypted cloud connections hide content from inspection
- API calls don't match traditional firewall rule patterns
- Dynamic workloads evade static monitoring rules

5 Complementary Security Approaches

5.1 Defense in Depth

When perimeter controls weaken, layer additional defenses:

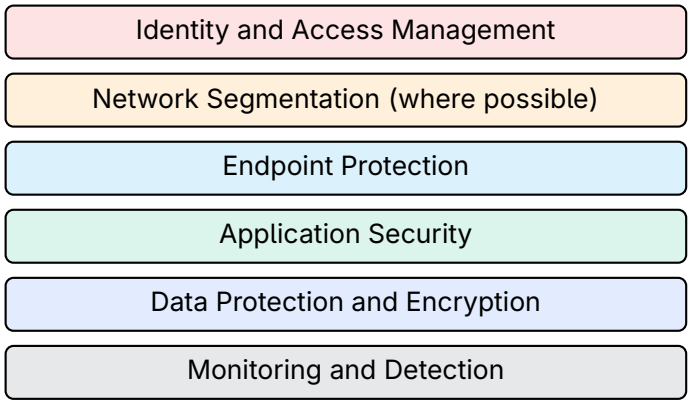

Figure 3: Defense in depth layers

5.2 Zero Trust Principles

Apply Zero Trust concepts to OT where boundaries are weak:

Principle	OT Application
Verify explicitly	Authenticate every connection, even within zones
Least privilege	Limit access to specific assets and functions
Assume breach	Monitor for lateral movement within OT networks
Micro-segmentation	Isolate critical assets regardless of zone

Table 3: Zero Trust principles for OT

5.3 Identity-Centric Security

When network location is unreliable, focus on identity:

- **Strong authentication** – MFA for all remote and privileged access
- **Service accounts** – Managed identities for machine-to-machine
- **Just-in-time access** – Temporary privileges for maintenance
- **Certificate-based auth** – Device identity for OT endpoints

5.4 Micro-Segmentation

Segment within zones, not just between them:

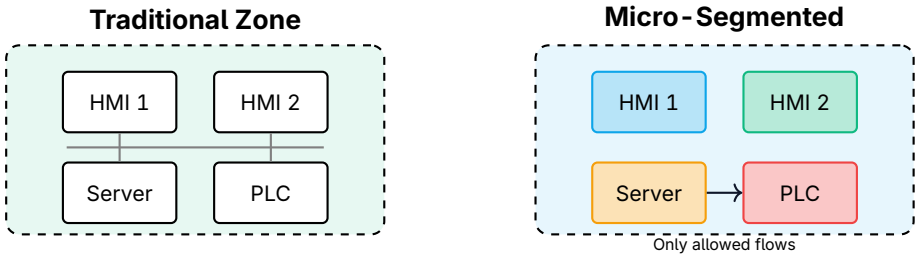

Figure 4: Traditional zone vs. micro-segmentation

Key Point

Recommendation: Identify crown jewel assets (safety systems, critical PLCs) and apply strict micro-segmentation regardless of their Purdue level. Protect what matters most, not just zone boundaries.

5.5 Enhanced Monitoring

Compensate for boundary weakness with detection:

- **Behavioral analytics** – Detect anomalies within zones
- **API monitoring** – Track cloud and integration traffic
- **Identity analytics** – Unusual access patterns
- **Encrypted traffic analysis** – Metadata-based detection

6 Practical Recommendations

6.1 Assessment First

Before implementing controls, understand your reality:

1. Map actual traffic flows, not assumed architecture
2. Identify all cloud connections and remote access paths
3. Document where virtualization spans zones
4. Inventory API integrations and data flows

6.2 Pragmatic Segmentation

Accept that perfect Purdue compliance may be impossible:

- Enforce strict segmentation where feasible (safety systems)
- Use compensating controls where boundaries are weak
- Prioritize protection of critical assets over zone purity
- Document exceptions and accepted risks

Tip

The goal is risk reduction, not architectural purity. A well-monitored, identity-controlled cloud connection may be more secure than an unmonitored "compliant" architecture with unknown shadow IT.

7 Summary

Key Takeaways

- **Model Limitations:** The Purdue Model assumes physical separation and adjacent-level traffic that modern technologies violate
- **Cloud and SDN:** Direct cloud connectivity, virtualization, and software-defined networking bypass traditional zone boundaries
- **Defense in Depth:** Layer multiple controls rather than relying solely on network segmentation
- **Zero Trust:** Apply identity verification and least privilege when network location is unreliable
- **Micro-Segmentation:** Protect critical assets individually, regardless of their Purdue level
- **Enhanced Monitoring:** Compensate for boundary weakness with behavioral detection and analytics
- **Pragmatic Approach:** Focus on risk reduction and asset protection rather than architectural compliance

8 Further Reading

Standards and Guidelines

- **NIST SP 800-207** – Zero Trust Architecture
  https://csrc.nist.gov/pubs/sp/800/207/final
- **IEC 62443-3-3** – System Security Requirements and Levels
  https://webstore.iec.ch/publication/7033

Resources

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

Books

- Knapp, Eric D. – *Industrial Network Security* (Syngress)
- Gilman & Barth – *Zero Trust Networks* (O'Reilly)

Part of the OT Security Learning Series