# Industrial DMZ Design

## Secure Buffer Zone Architecture for OT Networks

OT Security Learning Series

Document 302 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

# Contents

# 1 Introduction

An Industrial Demilitarized Zone (IDMZ) is a network segment that acts as a secure buffer between enterprise IT networks and operational technology (OT) networks. It provides controlled connectivity while preventing direct communication between business and control systems.

**Information**

The IDMZ is one of the most critical security controls in OT environments. A properly designed DMZ can prevent lateral movement from compromised IT systems to critical control networks.

## 1.1 Why IDMZ Matters

- **Isolation:** Prevents direct IT-to-OT communication paths
- **Control point:** Centralizes security monitoring and enforcement
- **Data exchange:** Enables safe sharing of operational data
- **Defense-in-depth:** Adds critical security layer

# 2 DMZ Concepts

## 2.1 Traditional IT DMZ vs Industrial DMZ

| Aspect | IT DMZ | Industrial DMZ |
|---|---|---|
| Primary purpose | Expose services to internet | Separate IT from OT |
| Traffic direction | Inbound from untrusted | Bidirectional, controlled |
| Services hosted | Web, email, DNS | Historians, jump servers |
| Trust model | Internet is untrusted | IT is semi-trusted |
| Availability needs | High | Critical (production impact) |

## 2.2 Purdue Model Context

In the Purdue Model, the IDMZ sits between Levels 3 and 4:

**DMZ in Purdue Architecture**

- **Level 4/5:** Enterprise network (IT)
- **Level 3.5:** Industrial DMZ (IDMZ)
- **Level 3:** Site operations (OT)
- **Levels 0–2:** Control and field devices

# 3 Architecture Patterns

### 3.1 Single-Firewall DMZ

The simplest pattern uses one firewall with three zones:

- Enterprise zone (IT network)
- DMZ zone (shared services)
- Control zone (OT network)

**Warning**

Single-firewall designs create a single point of failure. If the firewall is compromised, attackers gain access to all zones. Use only for small, low-risk environments.

### 3.2 Dual-Firewall DMZ

The recommended pattern uses two firewalls:

**Key Point**

**Dual-Firewall Architecture:**

- **Outer firewall:** Faces enterprise network
- **DMZ segment:** Between the firewalls
- **Inner firewall:** Protects OT network
- **Different vendors:** Prevents single vulnerability from compromising both

### 3.3 Data Diode Integration

For highest security, add hardware-enforced unidirectional gateways:

- **Outbound data diode:** OT to DMZ (historian replication)
- **No inbound path:** Physically prevents attacks from IT
- **Use cases:** Nuclear, critical infrastructure, high-security environments

## 4 DMZ Services

### 4.1 Typical DMZ Components

| Service | Purpose |
|---|---|
| Historian Mirror | Read-only copy of process data for business access |
| Jump Server | Secure remote access point for OT administration |
| Patch Server | Staging area for tested updates before OT deployment |
| AV/Update Server | Antivirus definitions and software updates |
| File Transfer | Secure exchange of files between IT and OT |
| Remote Access Gateway | VPN termination for authorized remote users |
| Log Collector | Aggregation point for OT security logs |

### 4.2 Service Placement Rules

**Tip**

**Key principles for DMZ service placement:**

- No service should have simultaneous connections to IT and OT
- Data should "break" in the DMZ (no direct tunnels)
- OT systems should initiate connections outbound to DMZ
- IT systems connect only to DMZ, never directly to OT

## 5 Traffic Flow Design

### 5.1 Allowed Traffic Patterns

| Source | Destination | Purpose |
|---|---|---|
| OT → DMZ | Historian mirror | Push process data for replication |
| OT → DMZ | Log collector | Send security events |
| DMZ → OT | Patch server | Pull tested updates (scheduled) |
| IT → DMZ | Historian mirror | Query operational data |
| IT → DMZ | Jump server | Remote administration access |

### 5.2 Prohibited Traffic

**Critical**

**Never allow these traffic flows:**

- IT directly to OT (any protocol)
- OT directly to IT (any protocol)
- Internet directly to DMZ or OT
- Broad "any-any" rules through the DMZ

## 6 Firewall Configuration

### 6.1 Rule Design Principles

1. **Default deny:** Block all traffic not explicitly permitted
2. **Least privilege:** Allow only required ports and protocols
3. **Specific sources/destinations:** No "any" in rules
4. **Application awareness:** Use OT-aware deep packet inspection
5. **Logging:** Log all traffic, especially denied connections

### 6.2 Example Rule Structure

| # | Source | Dest | Port | Purpose | Action |
|---|---|---|---|---|---|
| 1 | OT-Historian | DMZ-Mirror | 1433 | DB replication | Allow |
| 2 | IT-Analysts | DMZ-Mirror | 443 | Data queries | Allow |
| 3 | Admins | DMZ-Jump | 3389 | Remote admin | Allow |
| 4 | Any | Any | Any | Default | Deny |

## 7 Monitoring and Management

### 7.1 Security Monitoring

- **Traffic analysis:** Monitor for anomalous patterns
- **IDS/IPS:** Deploy at DMZ boundaries
- **Log correlation:** Aggregate logs from all DMZ systems
- **Alerting:** Immediate notification of policy violations

### 7.2 Change Management

**Information**

All DMZ changes should follow strict change control:
- Document business justification for rule changes
- Test changes in non-production environment
- Require approval from both IT and OT stakeholders
- Maintain audit trail of all modifications

## 8 Further Reading

### Standards and Guidelines

- **IEC 62443-3-2** – Security Risk Assessment and Zone Design
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **NIST SP 800-82 Rev. 3** – OT Security Guide
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

### Resources

- **CISA** – Recommended Practices for OT
  https://www.cisa.gov/topics/industrial-control-systems

### Books

- Pascal Ackerman – *Industrial Cybersecurity* (Packt)