Zone & Conduit Model

IEC 62443 network segmentation architecture

OT Security Learning Series

Document 303 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 Core Concepts **3**
2.1 Zones . . . 3
2.2 Conduits . . . 3

3 Zone Architecture **4**

4 Zone Types **4**
4.1 Common Zone Classifications . . . 5
4.2 Zone Sizing Considerations . . . 5

5 Conduit Design **5**
5.1 Conduit Security Controls . . . 5
5.2 Conduit Rules . . . 5
5.3 Conduit SL Requirements . . . 6

6 Implementation Steps **6**

7 Common Mistakes **6**

8 Summary **7**

9 Further Reading **7**

1 Introduction

Information

The Zone and Conduit Model is the foundational architecture concept in IEC 62443 for segmenting industrial control systems. It provides a structured approach to grouping assets by security requirements and controlling communication between groups.

Key principles:

- Group assets with similar security requirements into **zones**
- Control all communication between zones through **conduits**
- Assign Security Levels (SL) to each zone based on risk
- Apply appropriate controls at conduit boundaries

2 Core Concepts

2.1 Zones

Security Zone

A grouping of logical or physical assets that share common security requirements. All assets within a zone have the same Security Level (SL) target.

Zone characteristics:

- **Clear boundary** – Defined perimeter with controlled entry/exit
- **Common SL** – All assets share the same target Security Level
- **Trust relationship** – Assets within a zone trust each other
- **Managed independently** – Each zone has defined ownership

2.2 Conduits

Conduit

A logical grouping of communication channels that share common security requirements, connecting two or more zones.

Conduit characteristics:

- **Controlled path** – All traffic between zones flows through conduits
- **Security controls** – Firewalls, data diodes, or other mechanisms

- **Defined protocols** – Only approved communication is permitted
- **Monitored** – Traffic is logged and inspected

3 Zone Architecture

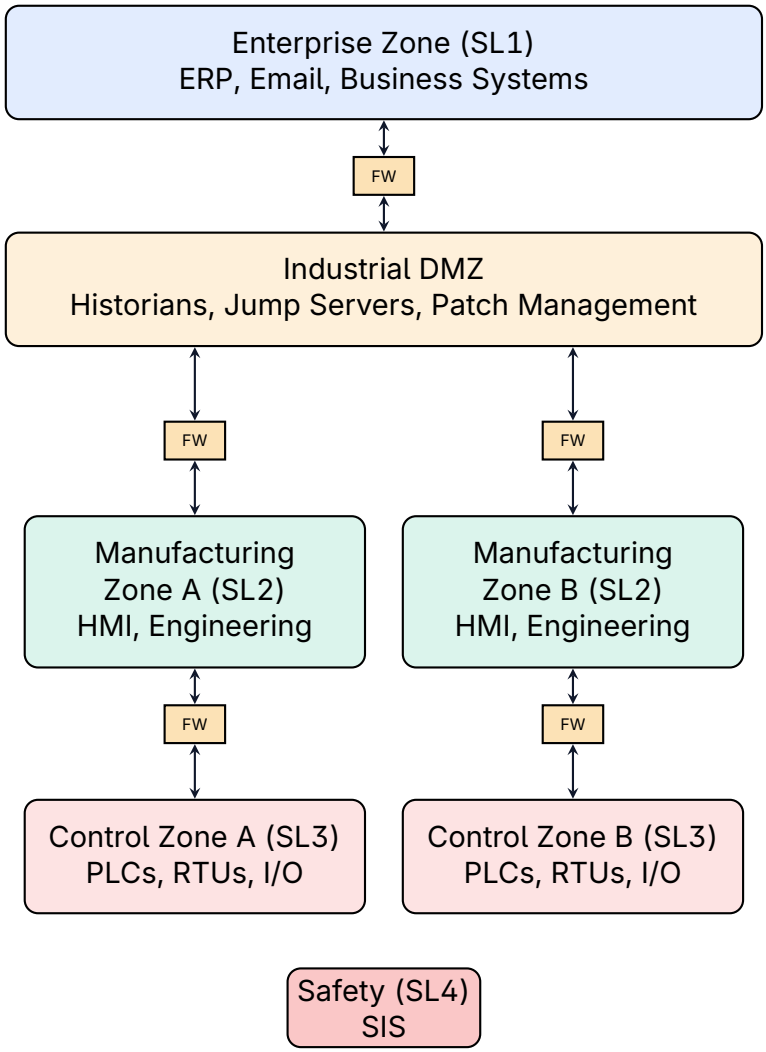

Figure 1: Zone and Conduit Architecture Example

4 Zone Types

4.1 Common Zone Classifications

Zone Type	Typical SL	Contents
Enterprise	SL1	Corporate IT, ERP, email, internet access
Industrial DMZ	SL2	Historians, patch servers, jump hosts
Manufacturing	SL2	HMI, engineering workstations, SCADA
Control	SL2–SL3	PLCs, RTUs, DCS controllers
Safety	SL3–SL4	SIS, emergency shutdown systems
Field	SL1–SL2	Sensors, actuators, field devices

Table 1: Common Zone Types and Security Levels

4.2 Zone Sizing Considerations

- **Too large** – Difficult to manage, broad attack surface
- **Too small** – Excessive complexity, operational burden
- **Right size** – Based on function, criticality, and connectivity

Warning

Avoid creating zones purely based on vendor or equipment type. Zone boundaries should reflect security requirements and operational dependencies.

5 Conduit Design

5.1 Conduit Security Controls

Control Type	Description
Firewall	Stateful packet filtering, application awareness
Data Diode	Hardware-enforced unidirectional flow
Jump Server	Controlled access point for administration
Protocol Proxy	Protocol break, inspection, and translation
VPN Gateway	Encrypted tunnel for remote connectivity
IDS/IPS	Traffic inspection and threat detection

Table 2: Conduit Security Control Options

5.2 Conduit Rules

Key Point

Every conduit should have explicitly defined rules specifying:

- Permitted protocols and ports
- Allowed source and destination addresses
- Direction of data flow
- Authentication requirements

5.3 Conduit SL Requirements

The conduit must meet the **higher** SL of the two zones it connects:

Zone A SL	Zone B SL	Conduit SL
SL1	SL2	SL2
SL2	SL2	SL2
SL2	SL3	SL3
SL3	SL4	SL4

Table 3: Conduit Security Level Determination

6 Implementation Steps

1. **Asset Inventory** – Identify all assets in the IACS
2. **Group by Function** – Cluster assets by operational role
3. **Identify Dependencies** – Map communication requirements
4. **Define Zone Boundaries** – Draw logical/physical perimeters
5. **Assign Security Levels** – Based on risk assessment
6. **Design Conduits** – Define allowed flows between zones
7. **Implement Controls** – Deploy firewalls, monitoring
8. **Validate** – Test that zones are properly isolated
9. **Document** – Maintain zone/conduit diagrams and rules

7 Common Mistakes

Critical

Anti-patterns to avoid:

- Flat networks with no segmentation
- Single firewall between IT and all of OT
- Zones based on physical location only
- Conduits with “allow all” rules
- Undocumented or forgotten connections
- Mixing different SL requirements in one zone

8 Summary

Key Takeaways

- **Zones** – Group assets with same security requirements
- **Conduits** – Controlled paths between zones
- **Security Levels** – Drive control requirements per zone
- **Defense in depth** – Multiple zone layers increase security
- **Documentation** – Maintain accurate zone/conduit diagrams
- **IEC 62443-3-2** – Standard for zone/conduit design

9 Further Reading

Standards

- **IEC 62443-3-2** – Security risk assessment and zone design
  https://webstore.iec.ch/publication/7032
- **IEC 62443-3-3** – System security requirements
  https://webstore.iec.ch/publication/7033

Resources

- **CISA – Network Segmentation**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series