ISA Ireland Section OT Cybersecurity Conference 2025

OT Resilience: Incident Prevention, Response, and Recovery

'Revisiting the Purdue Model'

Flexibility, Misconceptions, and Its Role in Modern OT Security

Barry O'Brien
Principal Architect OT
Armis

Introduction

The Purdue Model is a reference architecture for enterprise networks that incorporate industrial processes and devices.

The aim is to segregate devices on the network, i.e., “Network Segmentation”

This is useful for multiple reasons:

1. **Security** – make it harder for threats to enter and propagate within a network
2. **Risk Management** – segments individually assessed based on risk or criticality
3. **Network Management** – control of data flows
4. **Standardisation** – common architectures enables efficiencies

Introduction

Everyone surely agrees that Network Segmentation is a good thing.

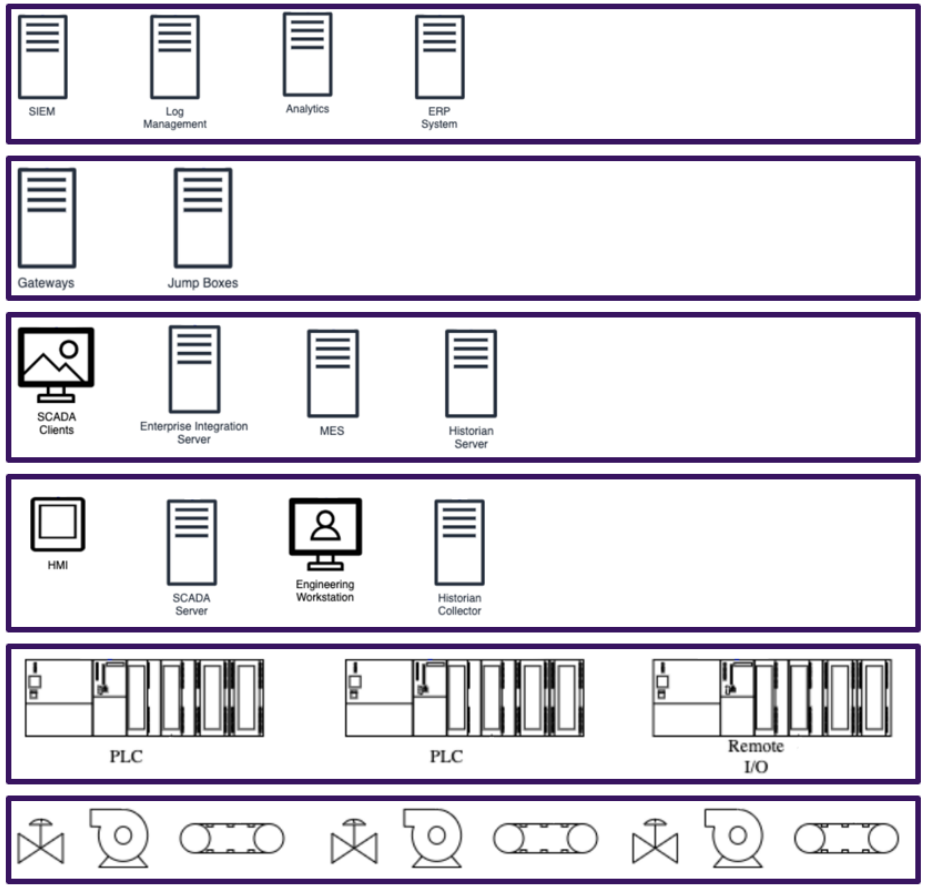
But, is the Purdue Model is the right way?

Remember that the Purdue Model is a **Reference Architecture.**

A Reference Architecture is meant to be high-level and conceptual.

The Purdue Model when combined with a Zones and Conduits methodology can be adaptable and flexible.

High Level Diagram



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

Level 1:
Process Control Level

Level 0: Field Devices

ARMIS

Notice the devices are grouped, without taking into consideration the physical or logical network design.

Each Level could be an individual zone or be made up of multiple zones.

Every network is different, hence why this is a **Reference Model**, and should not be as rigid as some practitioners assume.

Some Quick Notes

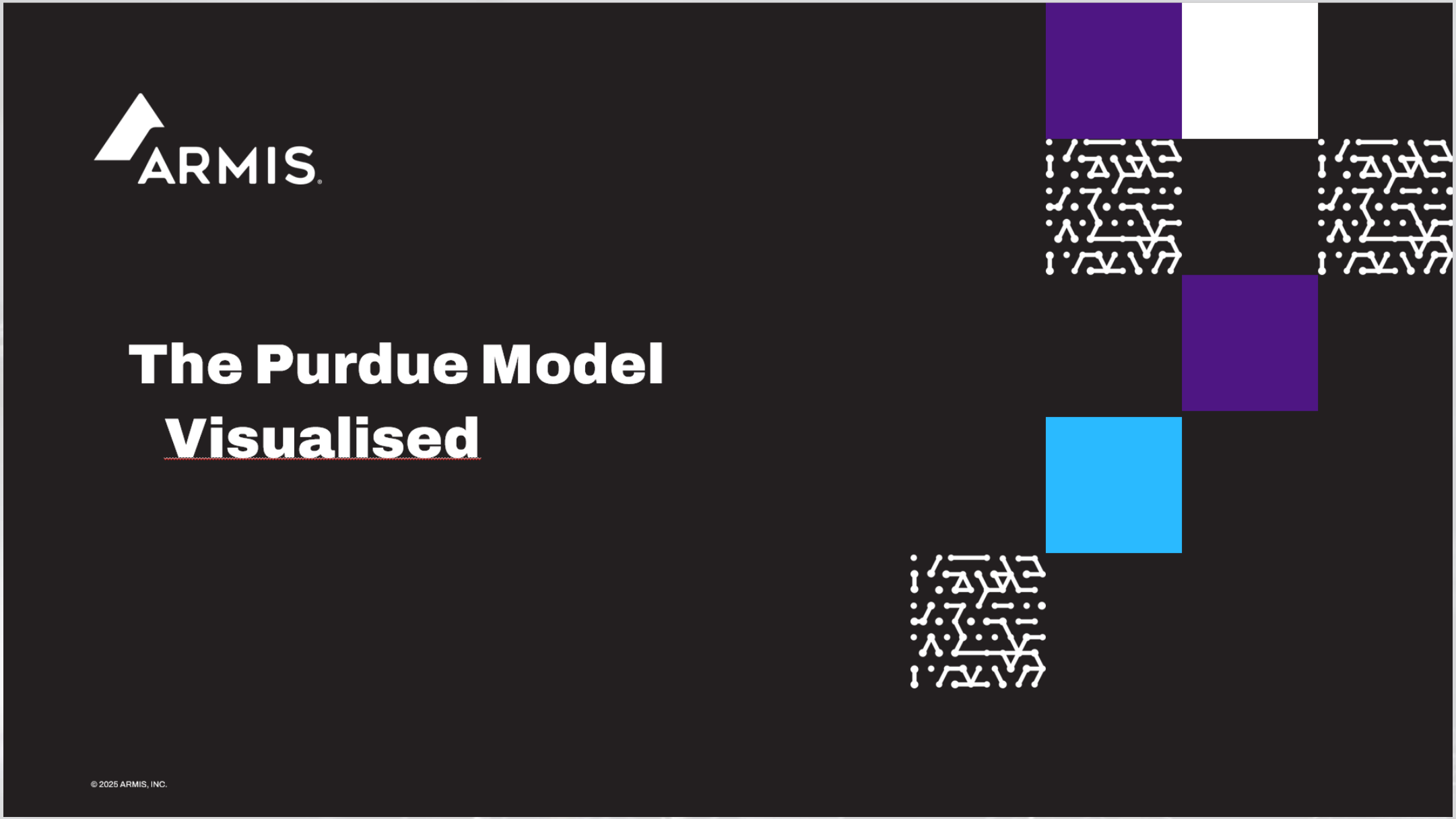
Consider all networks “north” of the OT boundary (L3 / L3.5) as External Networks, including your own IT network as an External Network.

Any point where traffic enters or leaves the OT network is considered a “Network Access Point”, e.g., IT boundary firewall, or third-party remote access.

If a threat gains entry to the OT network, it is most likely to come from the Network Access Point such as the IT network or a third-party network.

Network Segmentation is one of the most effective protection methods in OT Security. However, it is also one of the most difficult to implement effectively, especially in a cost-sensitive business.

A risk vs effort approach needs to be taken to Network Segmentation, in terms of device criticality and prioritisation of resources


ARMIS
The Purdue Model
Visualised
© 2025 ARMIS, INC.

Level 0

Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

Level 1:
Process Control Level

Level 0: Field Devices

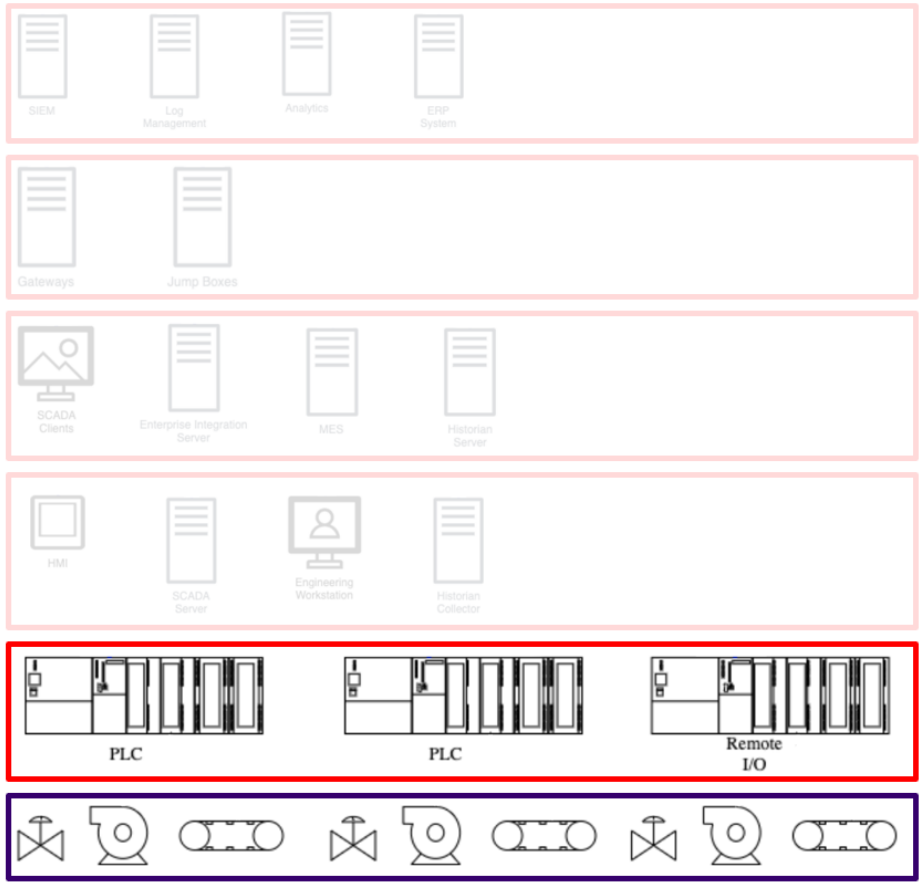
ARMIS

Level 0: Field Devices, are the sensors, actuators, etc, that interact with the physical world.

This could be a flow meter used as input in a control loop, or a motor that turns a conveyor.

These might be networked, but are commonly hardwired using analog or digital I/O.

Level 1



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

Level 1:
Process Control Level

Level 0: Field Devices

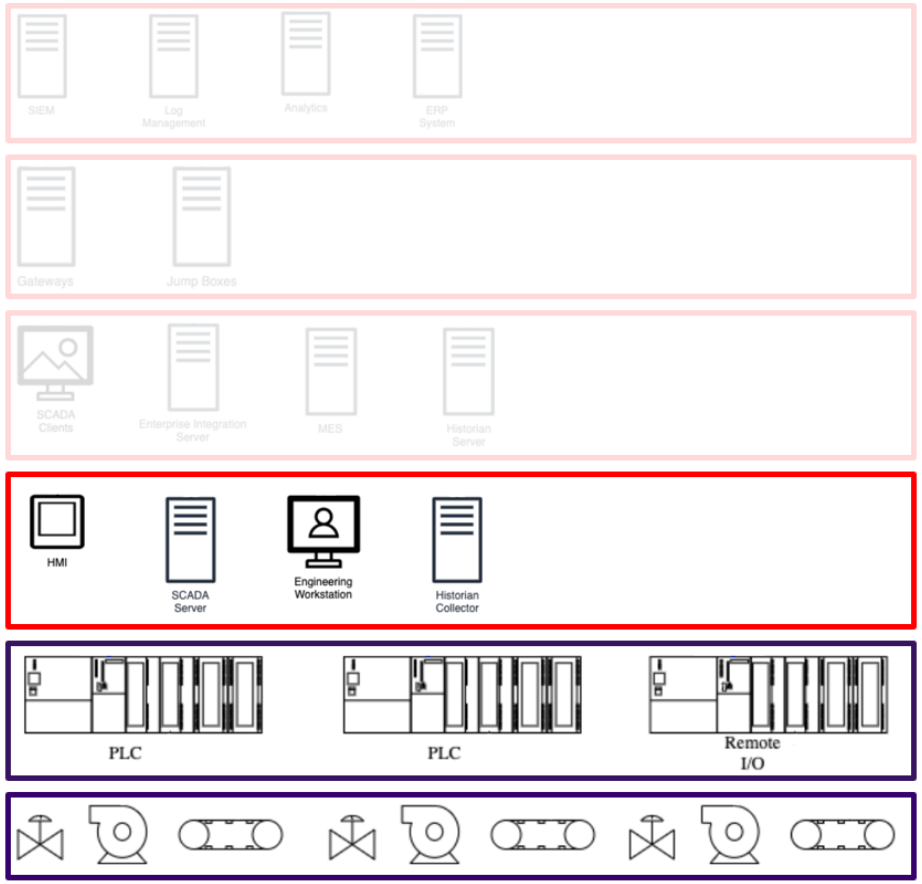
ARMIS

Level 1: The process control level, comprised of the devices that receive input signals, process them, and send output signals.

Many similar devices with different names, e.g., PLC, Controller, RTU, IED.

These devices interface directly with Level 0.

Level 2



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

Level 1:
Process Control Level

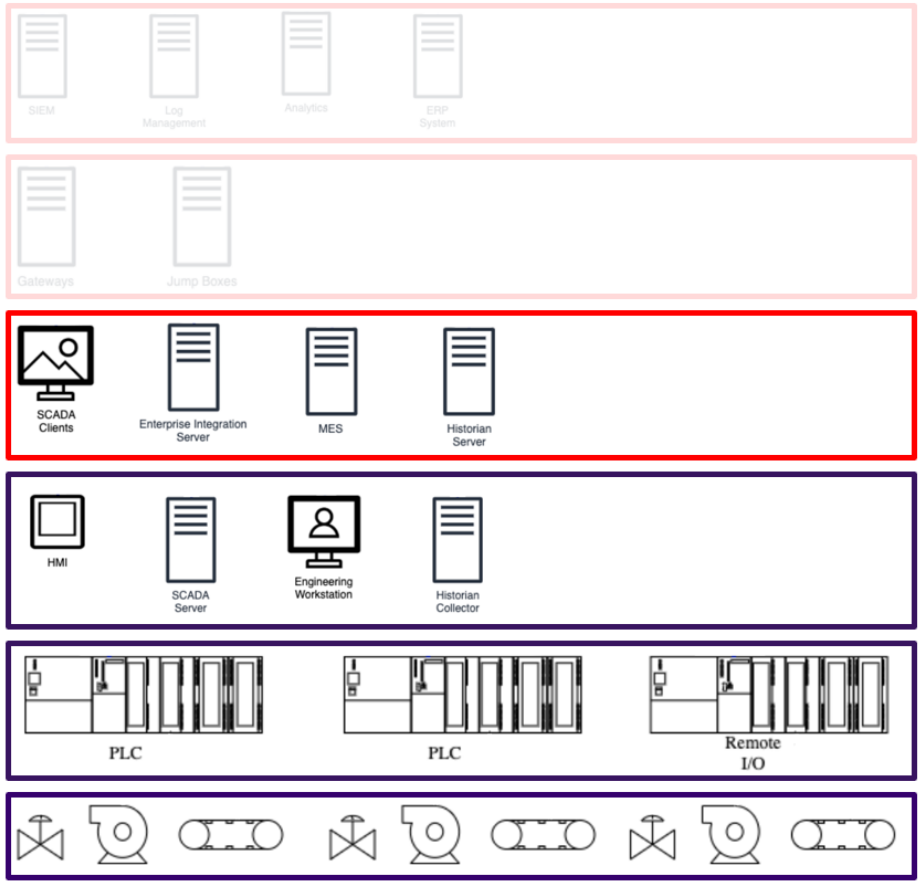
Level 0: Field Devices

ARMIS

Level 2: The Supervisory level is like the “management plane” for the Level 1.

This level interfaces with the Level 1 devices for direct control of a process by an operator, configuration changes by an engineer, and automated telemetry collection.

Level 3



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

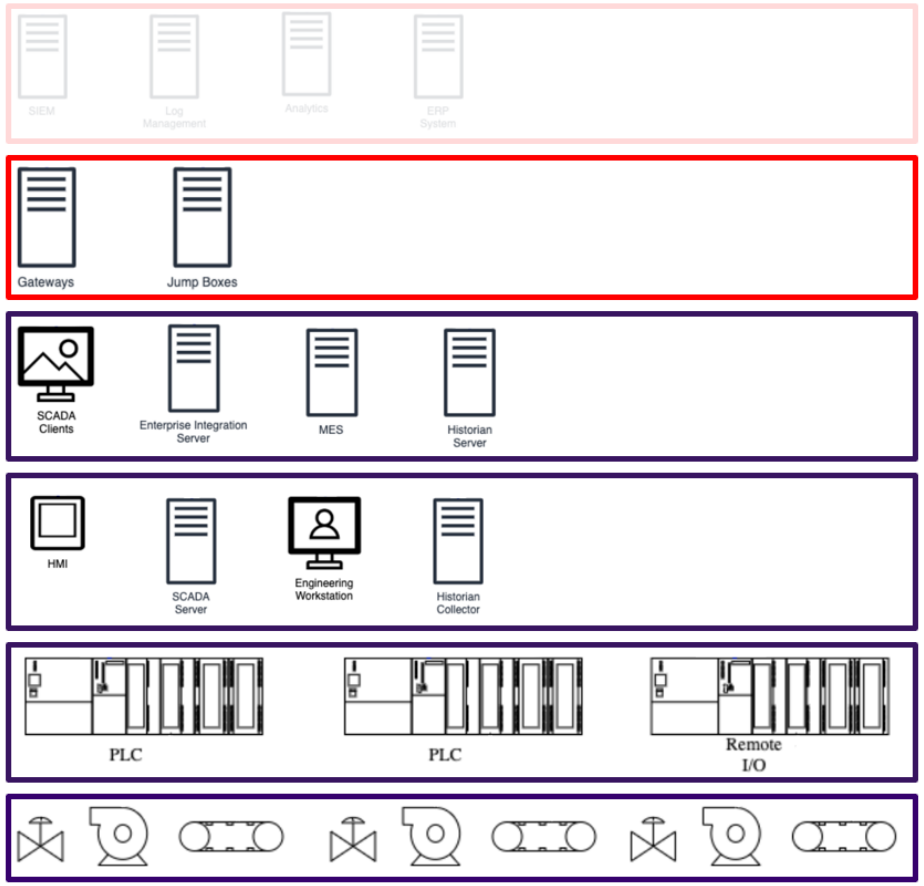
Level 1:
Process Control Level

Level 0: Field Devices

Level 3: Operations serves as the bridge between enterprise IT and plant control systems.

It hosts systems like MES and Historians that manage production data without directly controlling processes.

Level 3.5



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

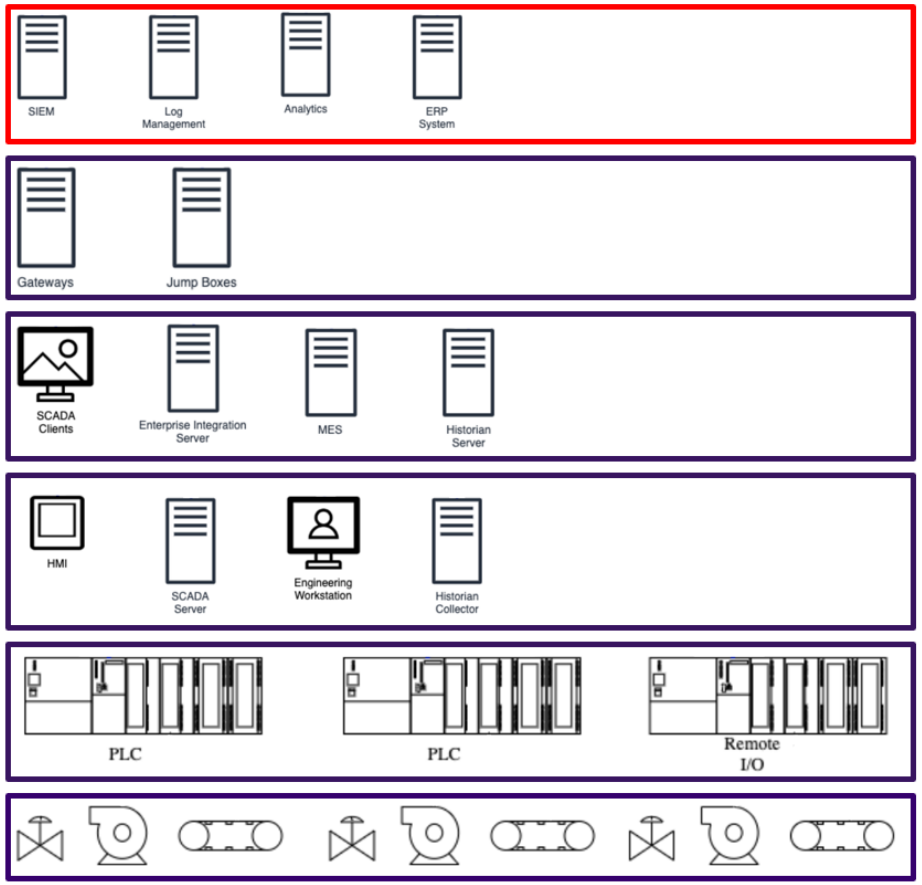
Level 1:
Process Control Level

Level 0: Field Devices

ARMIS

Level 3.5: The DMZ acts as a buffer zone where only tightly controlled communication is allowed, typically hosting systems like jump servers, patch management, and historian replication, to facilitate connectivity without exposing control systems to external networks.

Level 4



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

Level 1:
Process Control Level

Level 0: Field Devices

ARMIS

Level 4: The IT network carries a lot of risk and must be kept separate where possible from the OT network, however, data exchange must take place with the OT network in order to support functions such as production planning, logistics, and resource management.

Level 4 is considered an “external” network to the OT network and must be treated as a threat source.

Issues with The Purdue Model

Common belief is that devices shouldn't communicate across more than one level, e.g., level 1 to level 3. But, this is impractical in a lot of cases.

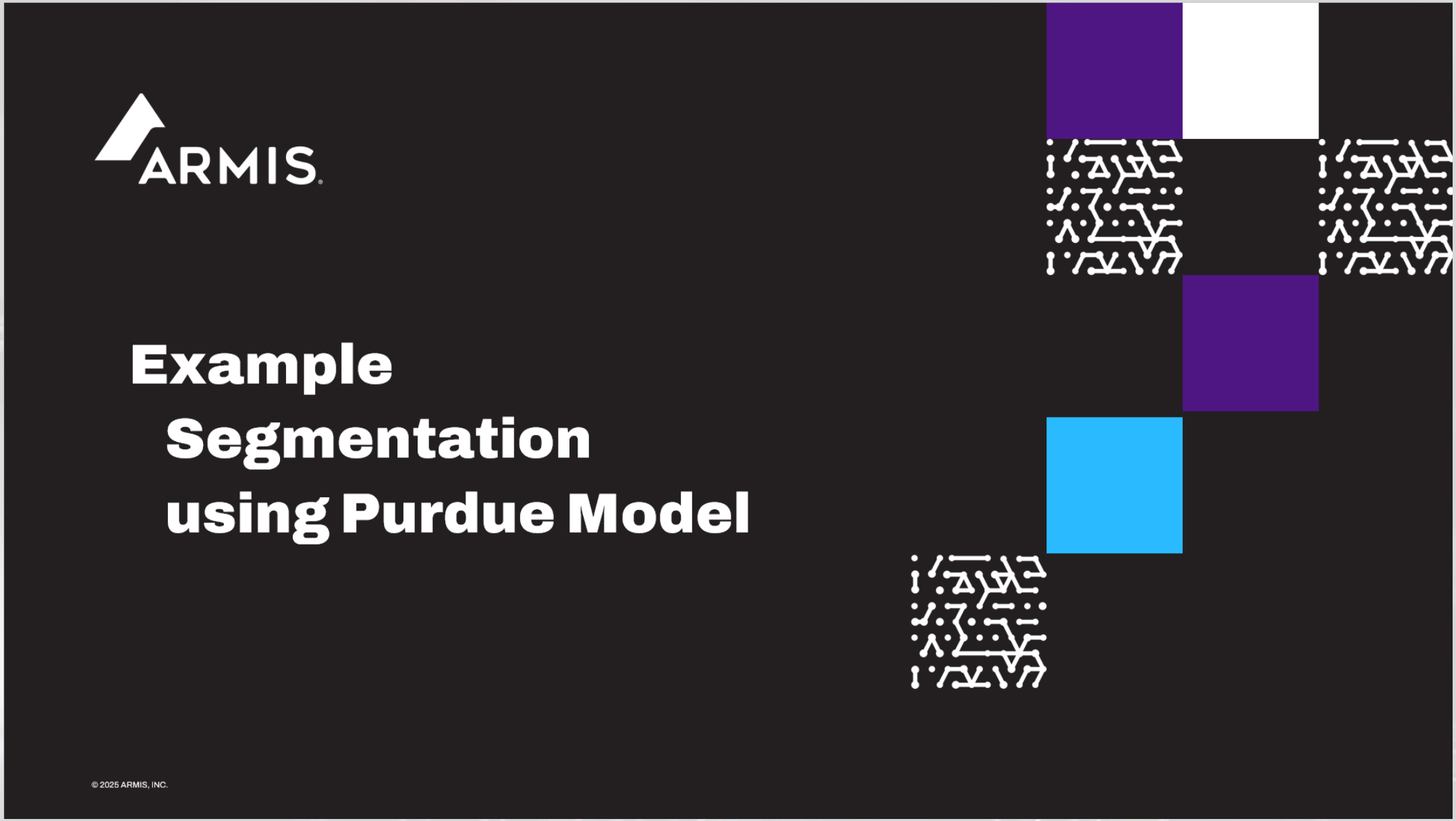
IIoT devices.

Edge networks.

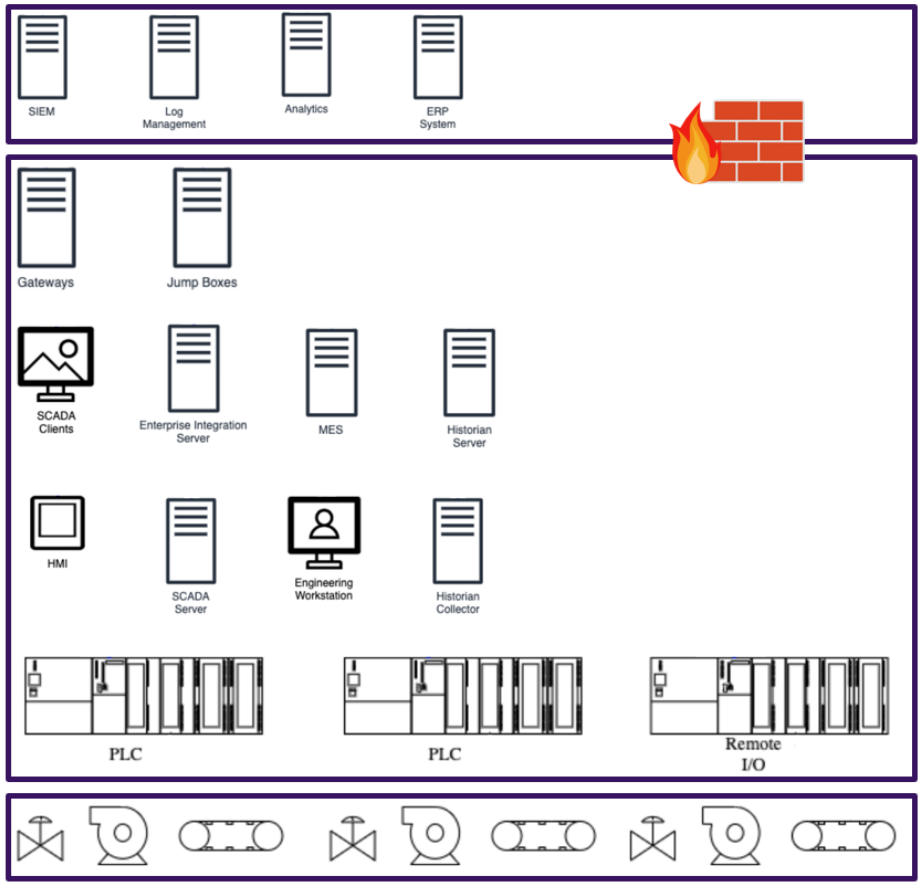
Wireless devices.

Cloud connectivity is becoming ever more common in OT.

Also, it could be implied that there should be no east-west traffic restrictions within the levels, which is not good security practice in any network.


ARMIS
Example
Segmentation
using Purdue Model
© 2025 ARMIS, INC.

Minimum Viable Segmentation



Level 4:
IT Network

OT Network

Level 0: Field Devices

ARMIS

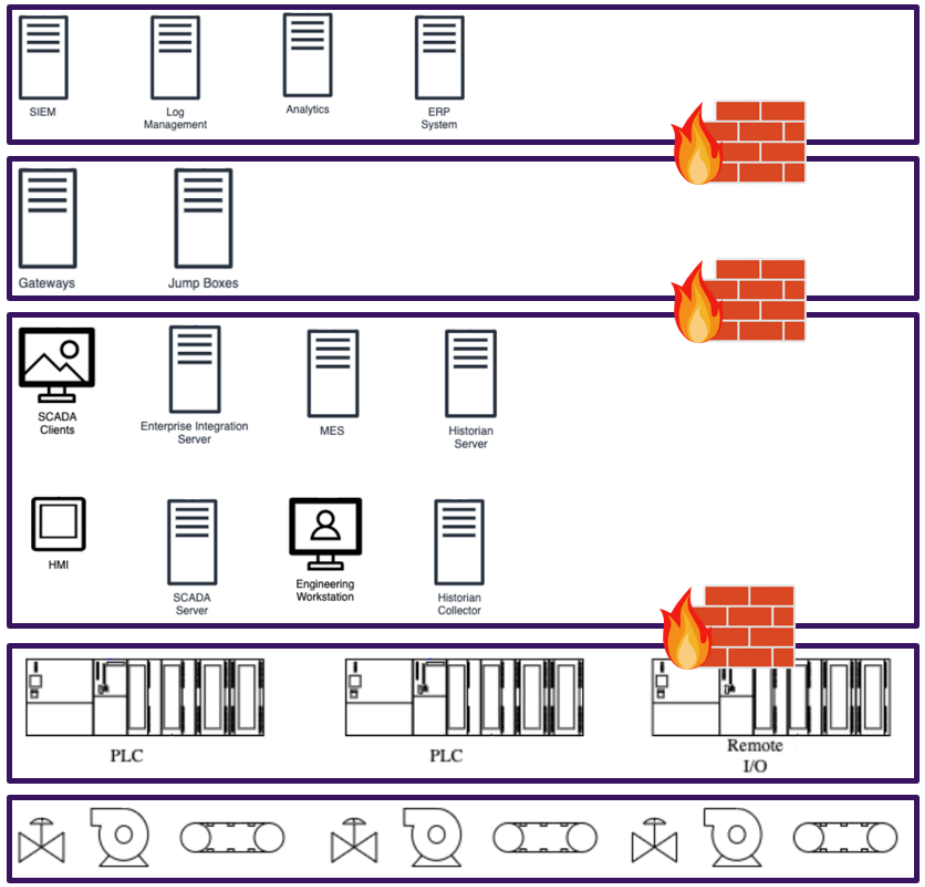
Protected boundary with IT network.

Everything else on the same network.

Cost effective for small non-critical sites/lines.

Doesn't control the blast radius if a threat gains access to the network.

Common Segmentation Design



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

Level 1:
Process Control Level

Level 0: Field Devices

ARMIS

This is a more common segmentation design that is more realistically achievable for retrofit to brownfield sites.

Still suffers issues as described earlier, e.g., east-west.


ARMIS
IEC 62443 and
Network
Segmentation
© 2025 ARMIS, INC.

IEC 62443 and Network Segmentation

IEC 62443 is a series of OT Security Standards, which has multiple sections that describe Network Segmentation.

Section 3-3 (IEC 62443-3-3) is applicable to asset owners, providing a set of controls (Security Requirements or “SR”) mapped to Foundational Requirements (“FR”).

Each SR has up to three Requirement Enhancements or “RE”.

Each RE maps to a Security Level or “SL”.

An SL is mapped to a site, level, or zone.

- SL-T is your Target level
- SL-A is your Achieved level

This is important when building a secure OT network design!

IEC 62443 and Network Segmentation

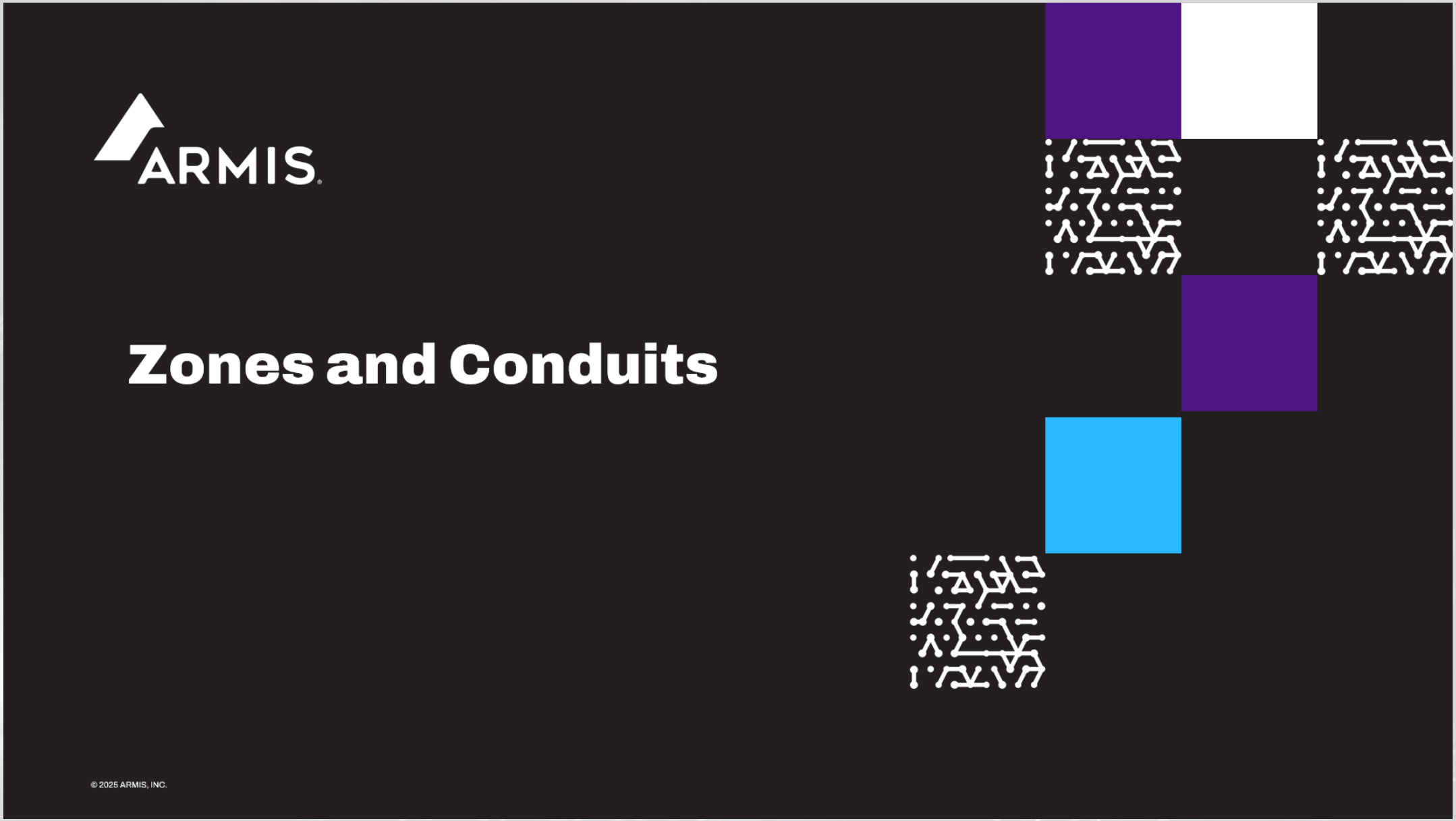
IEC 62443 FR 5 (Restricted Data Flow) focuses on controlling and limiting communications between zones and devices using Network Segmentation to reduce the risk of unauthorised access.

SR 5.1 (Network Segmentation) mandates, as a minimum, logical segmentation, i.e., the use of VLANs and Firewalls to separate OT from IT networks, allowing shared physical infrastructure such as switches.

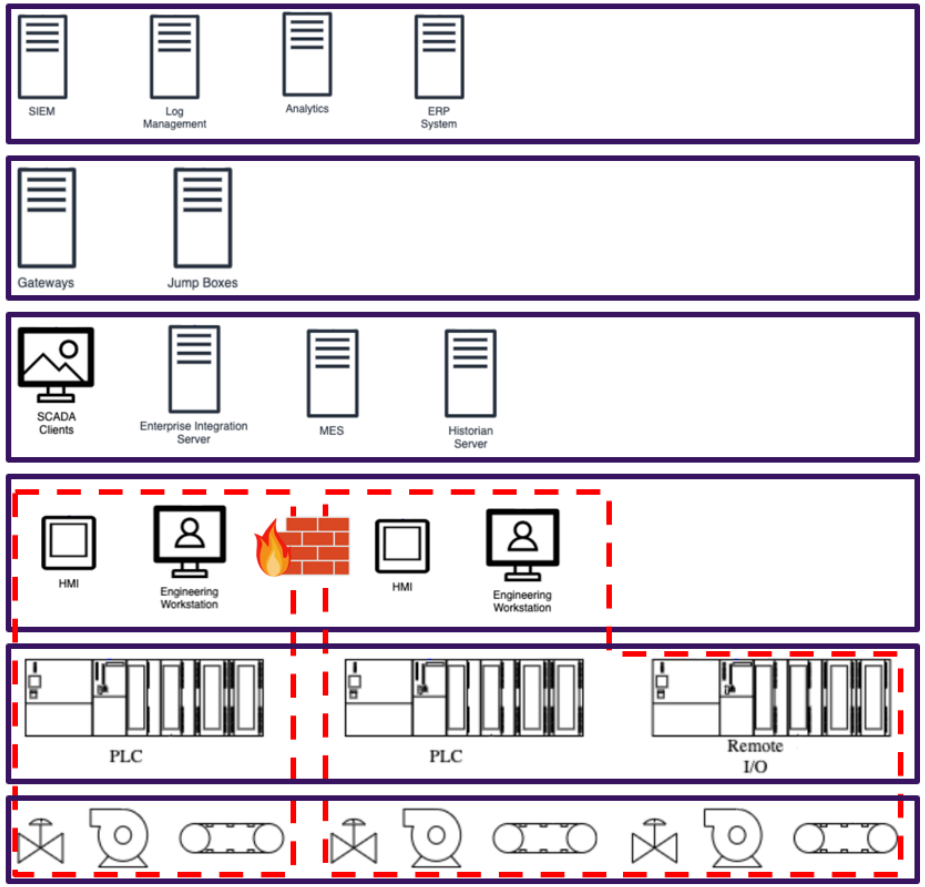
SR 5.1 RE 1 mandates physical segmentation, i.e., separate physical network infrastructure. This is not feasible for many organisations to retrofit completely across brownfield sites due to the existing network design, however is a requirement for SL2, and could possibly be retrofitted to specific critical zones depending on the criticality and risk.

SR 5.2 RE 2 mandates that a network should be able to go into “Island Mode” and operate completely independently of other networks. This is not feasible for many organisations due to the need for ERP, MES, etc, however is a requirement for SL3.

Choose your SL-T based on **zone risk** and consider the implications trying to implement that SL.


ARMIS
Zones and Conduits
© 2025 ARMIS, INC.

Zones within/across Levels



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

Level 1:
Process Control Level

Level 0: Field Devices

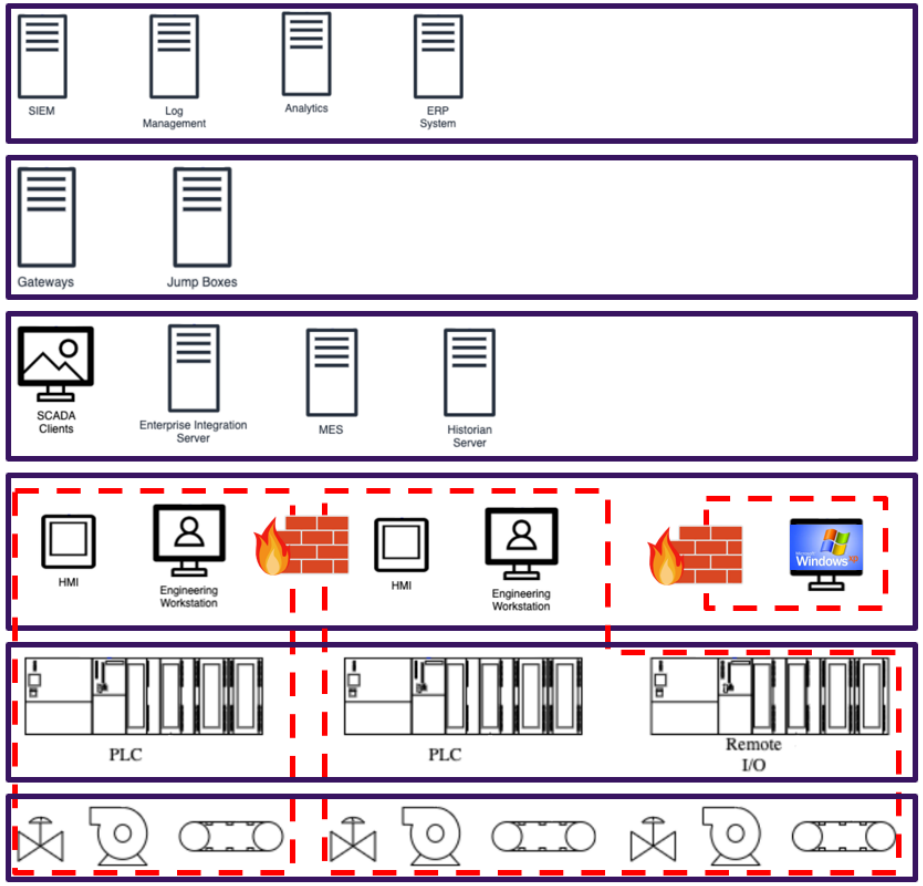
ARMIS

Levels group devices according to function.

Zones can be used to group devices according to criticality and risk.

Depending on the criticality and risk, which would define the SL-T, you could opt for physical or logical segmentation for the zones.

Zones within/across Levels



Level 4:
IT Network

Level 3.5:
OT DMZ

Level 3:
Operations Level

Level 2:
Supervisory Level

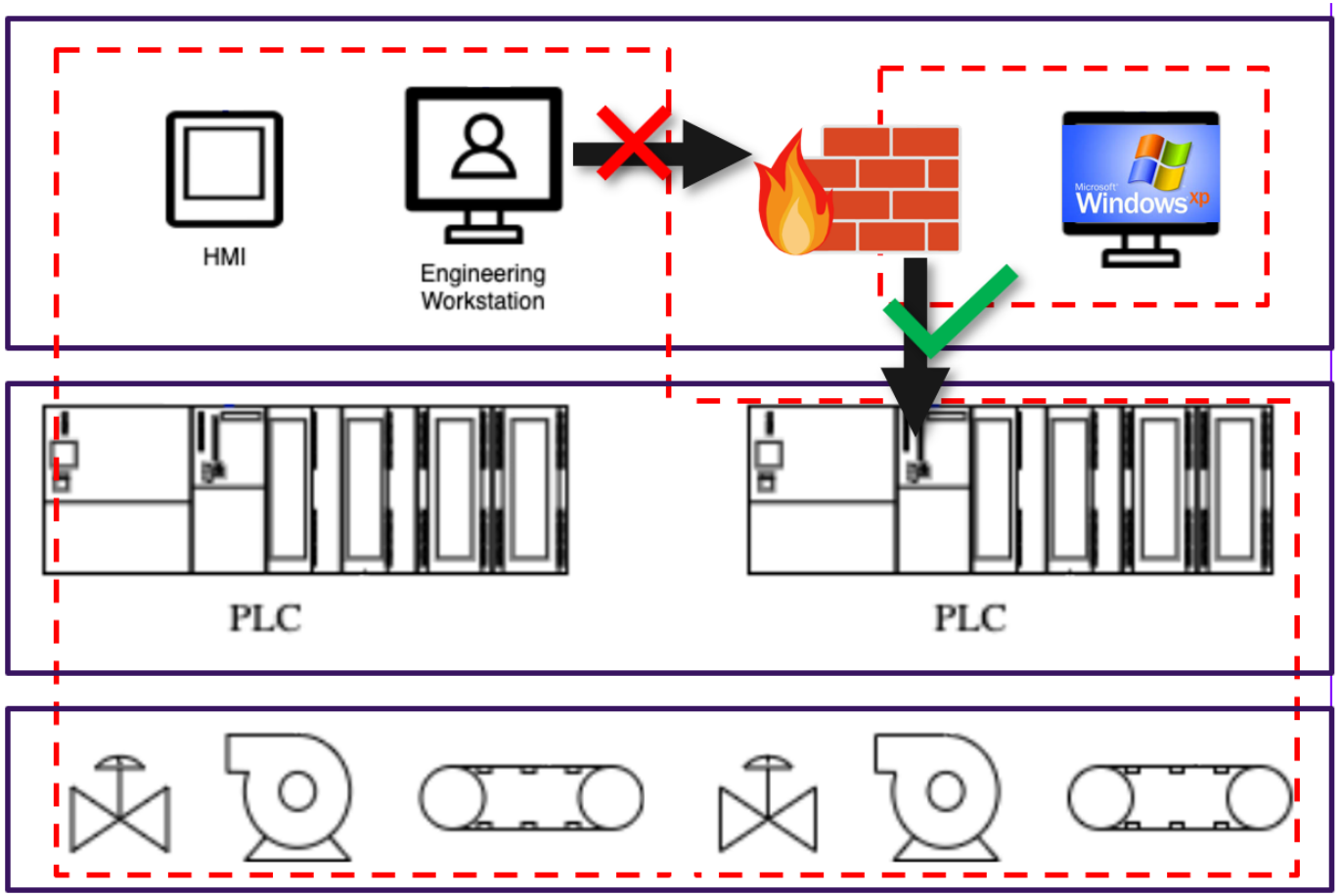
Level 1:
Process Control Level

Level 0: Field Devices

ARMIS

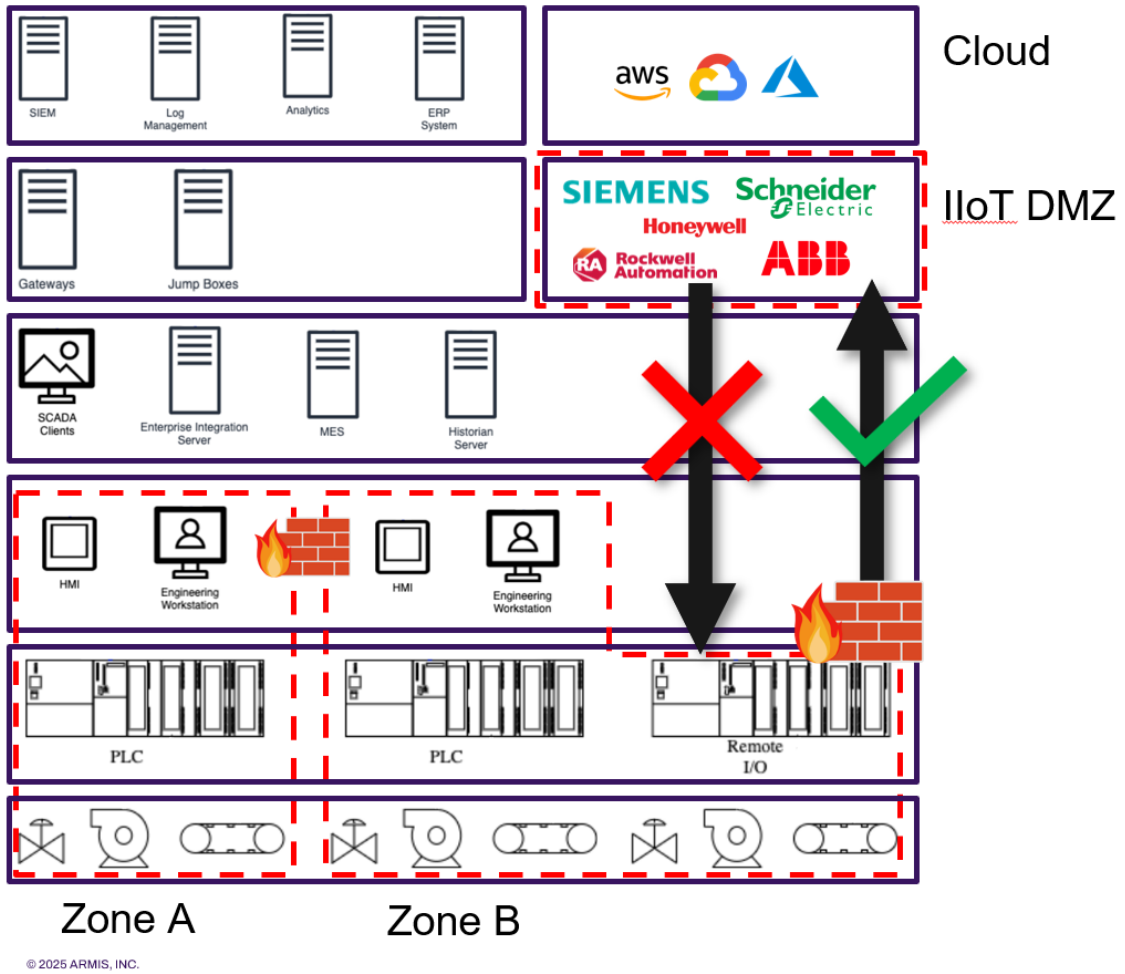
Zones can be made quite granular, depending on risk, e.g., legacy systems such as Windows XP will need more controls around isolation than other devices.

Conduits



Conduits are tightly defined and controlled communication paths that securely manage data flow between security zones, enforcing access restrictions, protocol filtering, and other protective measures.

External Connectivity for IIoT



ARMIS

Secure connectivity with IIoT and cloud can be achieved, NO VPNs!

Outbound connectivity only, no inbound, with strict IP and port rules in the firewall.

Certificate-based authentication and encryption.

Connections can be aggregated with a proxy or gateway.

IEC 62443 and The Purdue Model

The Purdue Model is still useful for classification of assets and having a conceptual understanding of the hierarchy of assets.

Segmentation using Zones and Conduits offers more benefits though.

Zones and Conduits enable a more granular segmentation with security controls applied based on risk assessment.

Zones and Conduits can be defined to take into account the IIoT, Wireless, and Cloud.

Zones and Conduits enable better protection of high-risk/vulnerable legacy systems through east-west segmentation.

Importantly, in the event of a breach the disruption can be contained by limiting the blast radius of the attack.

Thank You