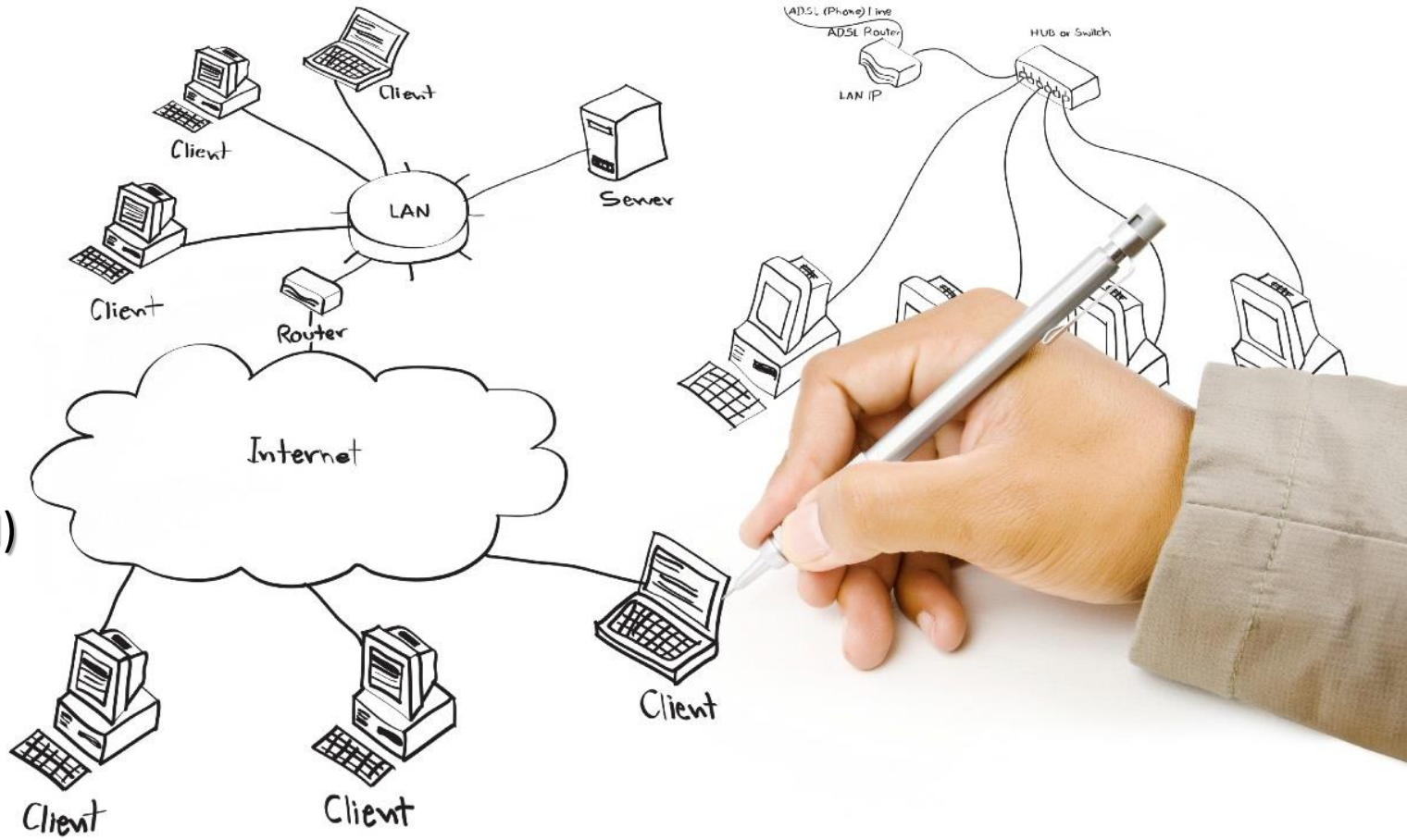
Basisconcepten voor het ontwerpen van veilig industriële netwerken

Ing. Hendrik Derre

Basisconcepten voor het ontwerpen van veilig industriële netwerken

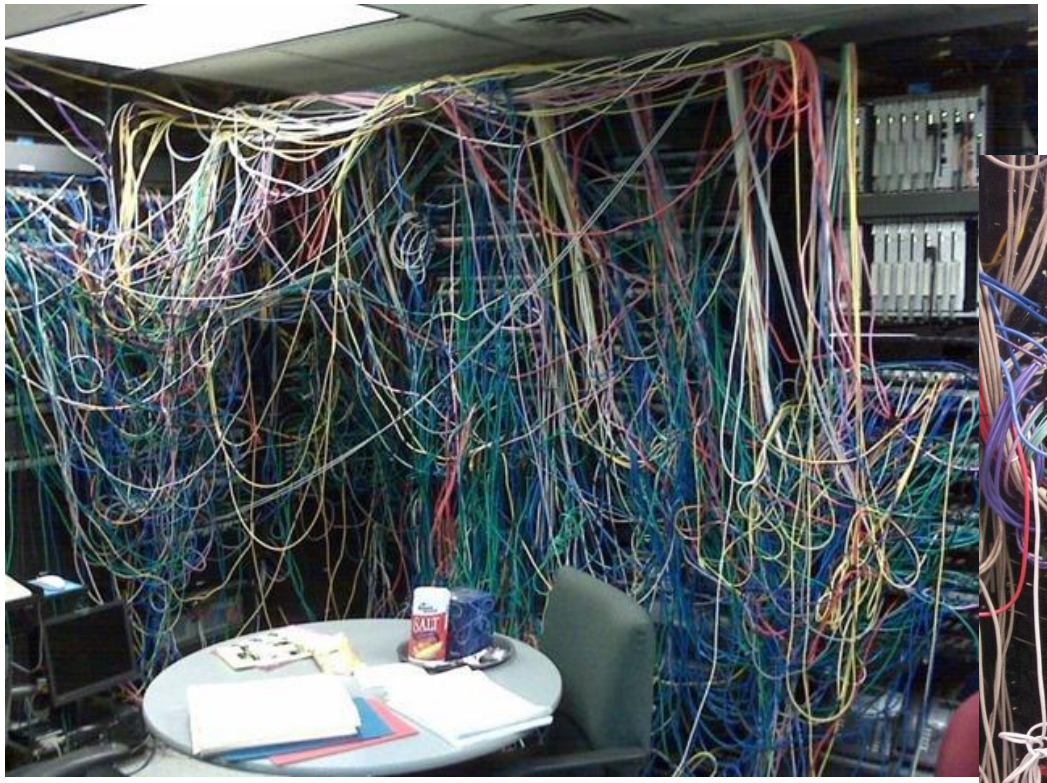
- ☑ FireWalls
- ☑ Routers
- ☑ Switches
- ☑ Virtual Private Networks (VPN)
- ☑ Virtual local area networks (VLAN)
- ☑ .....

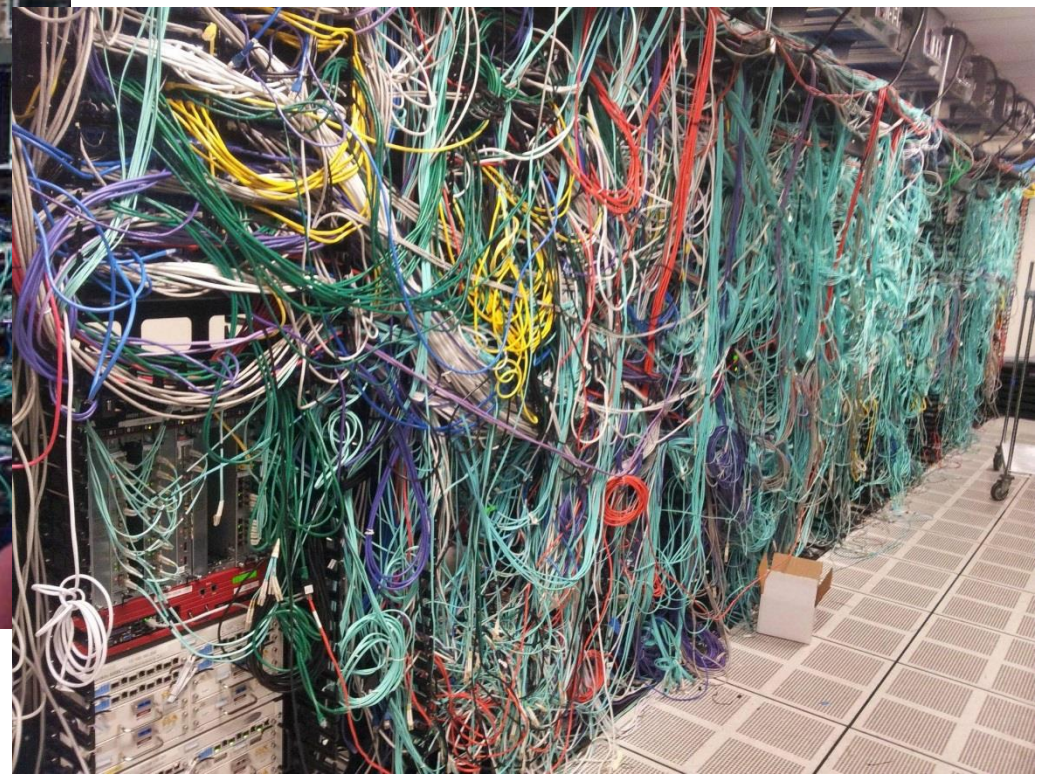


Basisconcepten voor het ontwerpen van veilig industriële netwerken

Basisconcepten voor het ontwerpen van veilig industriële netwerken

Basisconcepten voor het ontwerpen van veilig industriële netwerken





Basisconcepten voor het ontwerpen van veilig industriële netwerken

- ☑ FireWalls
- ☑ Routers
- ☑ Switches
- ☑ Virtual Private Networks (VPN)
- ☑ Virtual local area networks (VLAN)
- ☑ .....

Basisconcepten voor het ontwerpen van veilig industriële netwerken

- Zones & Conduits model
- Network Segmentation & Segregation
- Defense in Depth

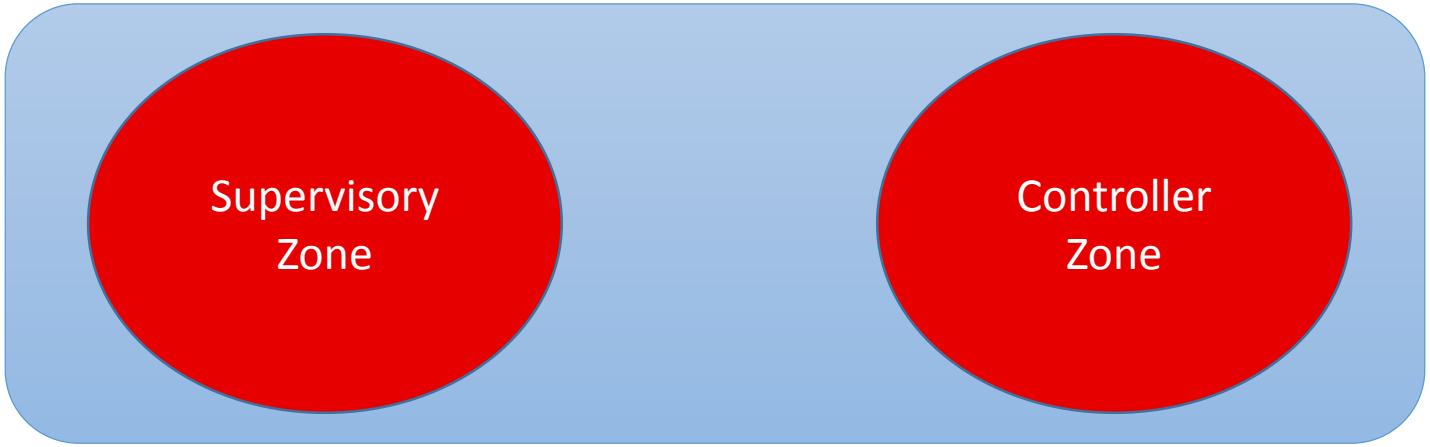
Basisconcepten voor het ontwerpen van veilig industriële netwerken

- **Zones & Conduits model**
- Network Segmentation & Segregation
- Defense in Depth

Zones & Conduits

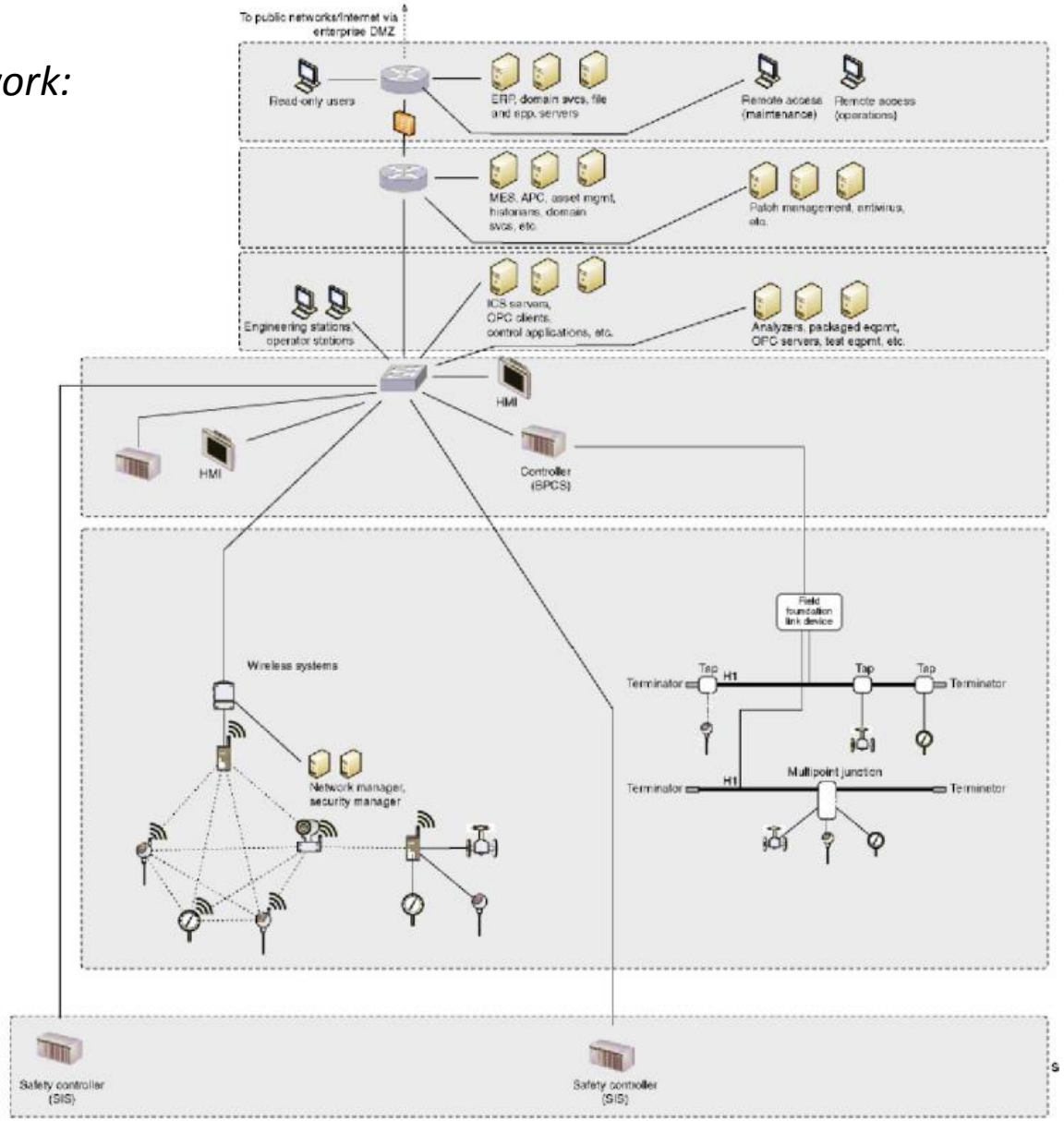
"**Security Zone**": grouping of logical or physical assets that share common security requirements. [ANSI/ISA99][IEC-62443]

A zone has a clearly defined border (either logical or phyiscal), which is the boundary between included and excluded elements



Zones & Conduits

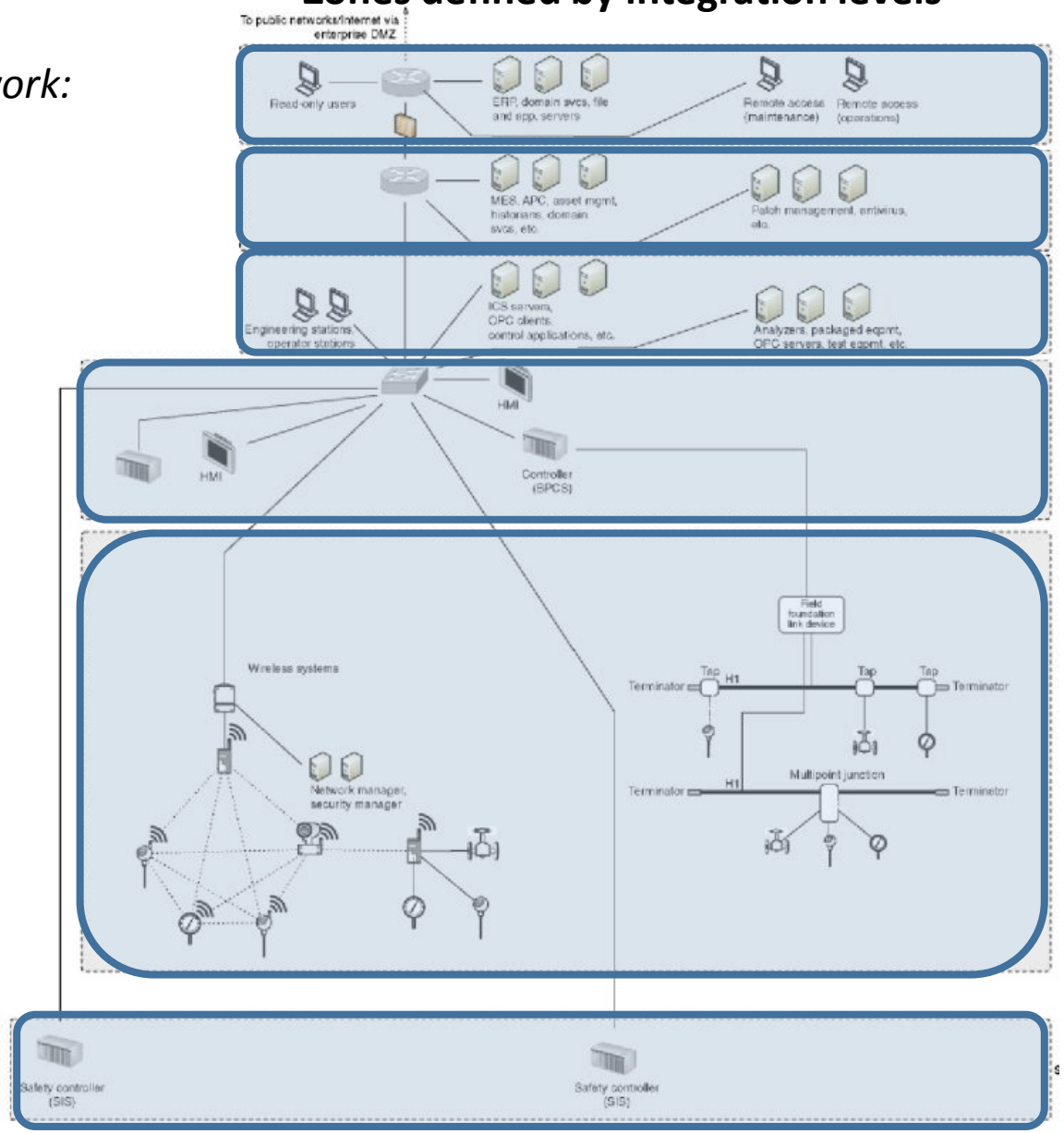
Example network:



Zones & Conduits

Example network:

Zones defined by integration levels



Business Zones

Operational control zones

Supervisory control zones

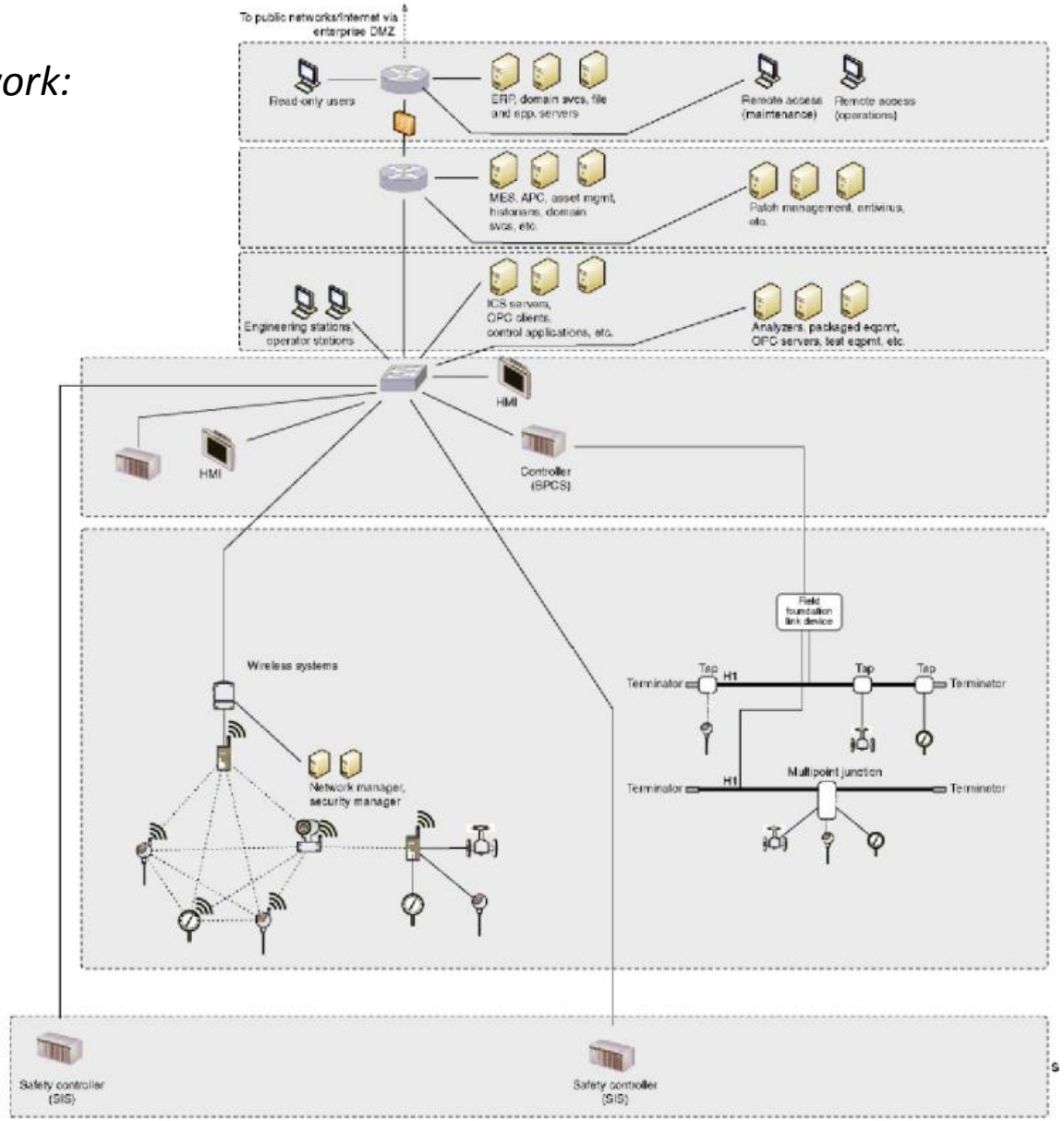
Local control zones

Process zones

Safety Zones

Zones & Conduits

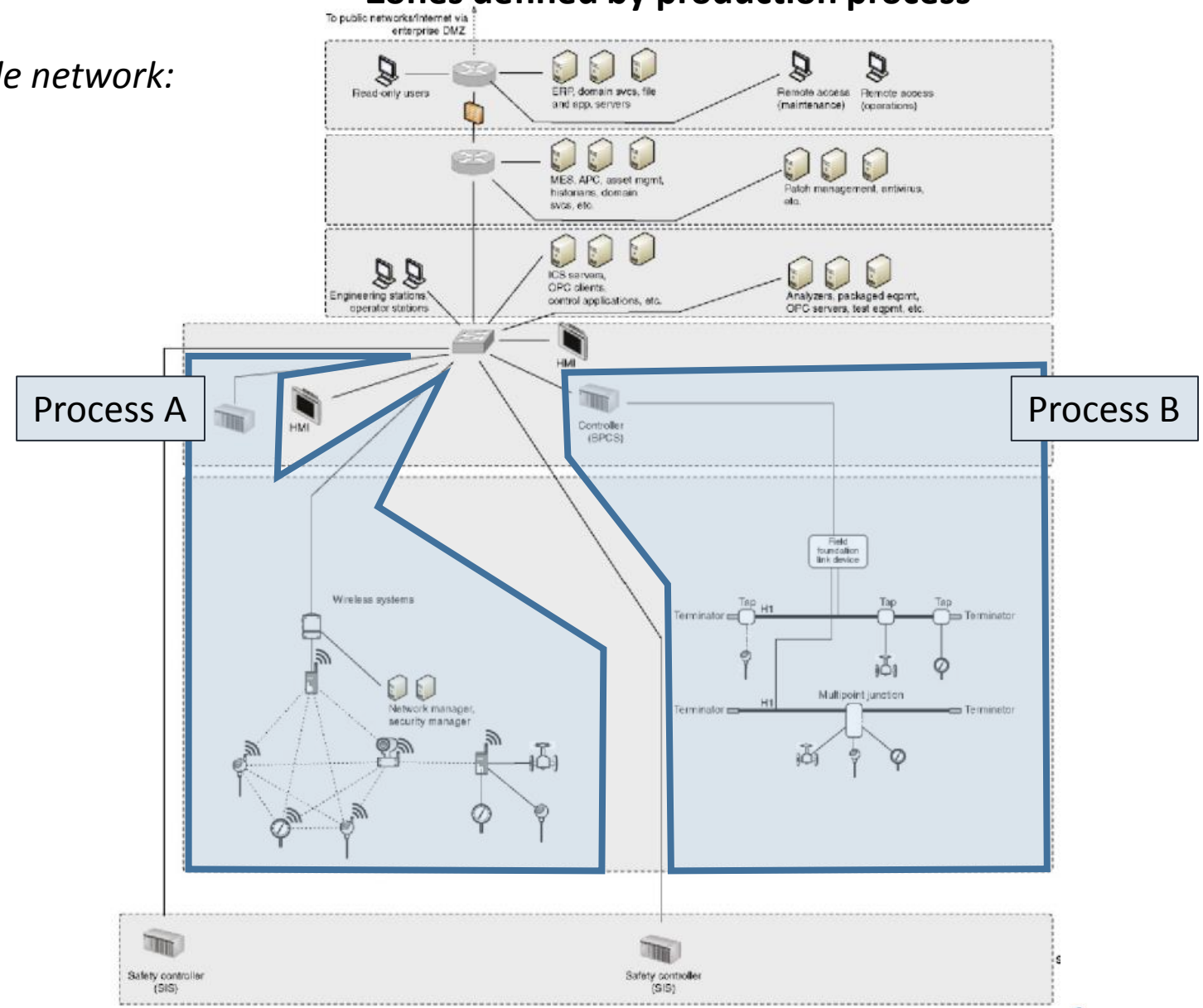
Example network:



Zones & Conduits

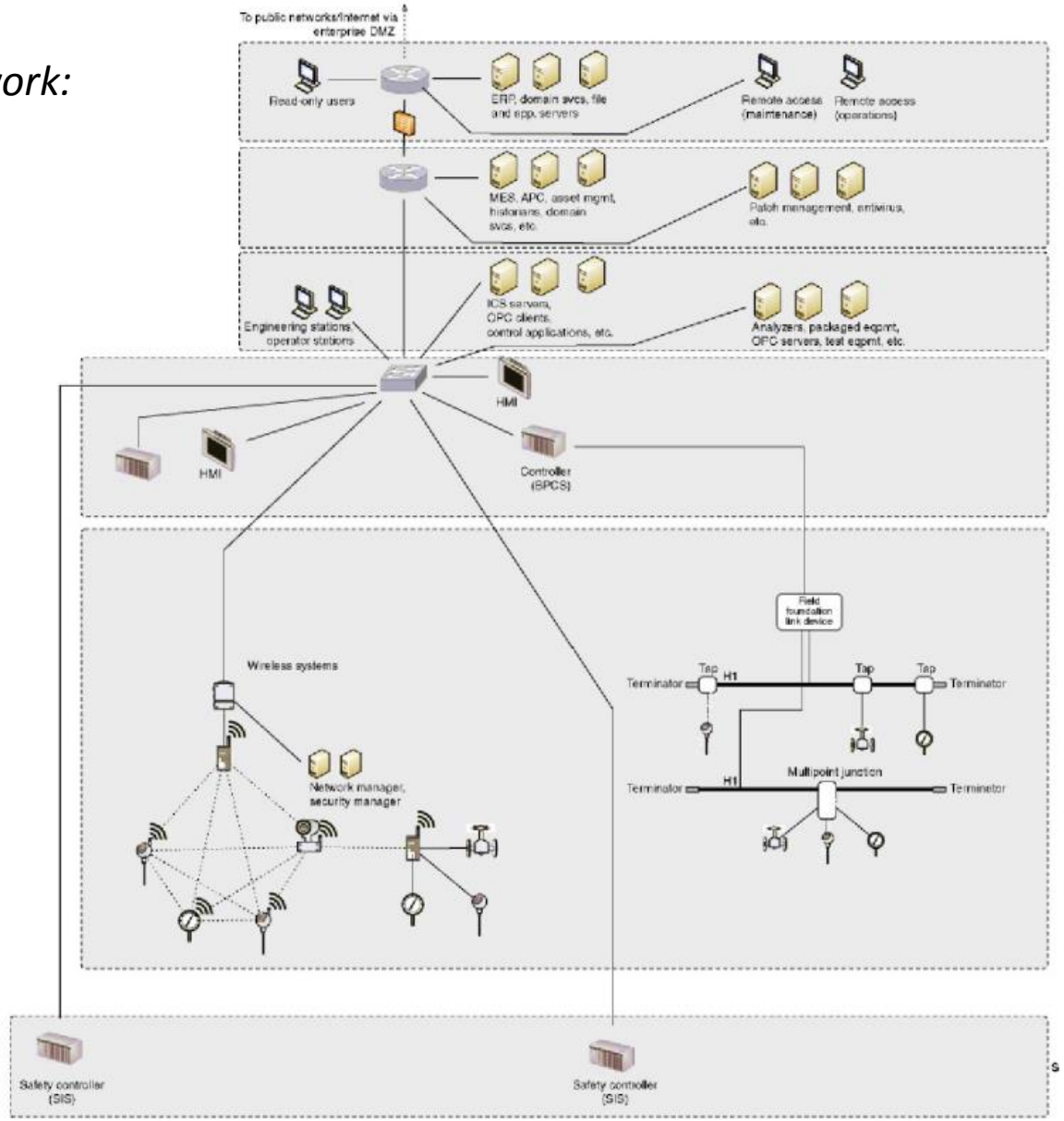
Example network:

Zones defined by production process



Zones & Conduits

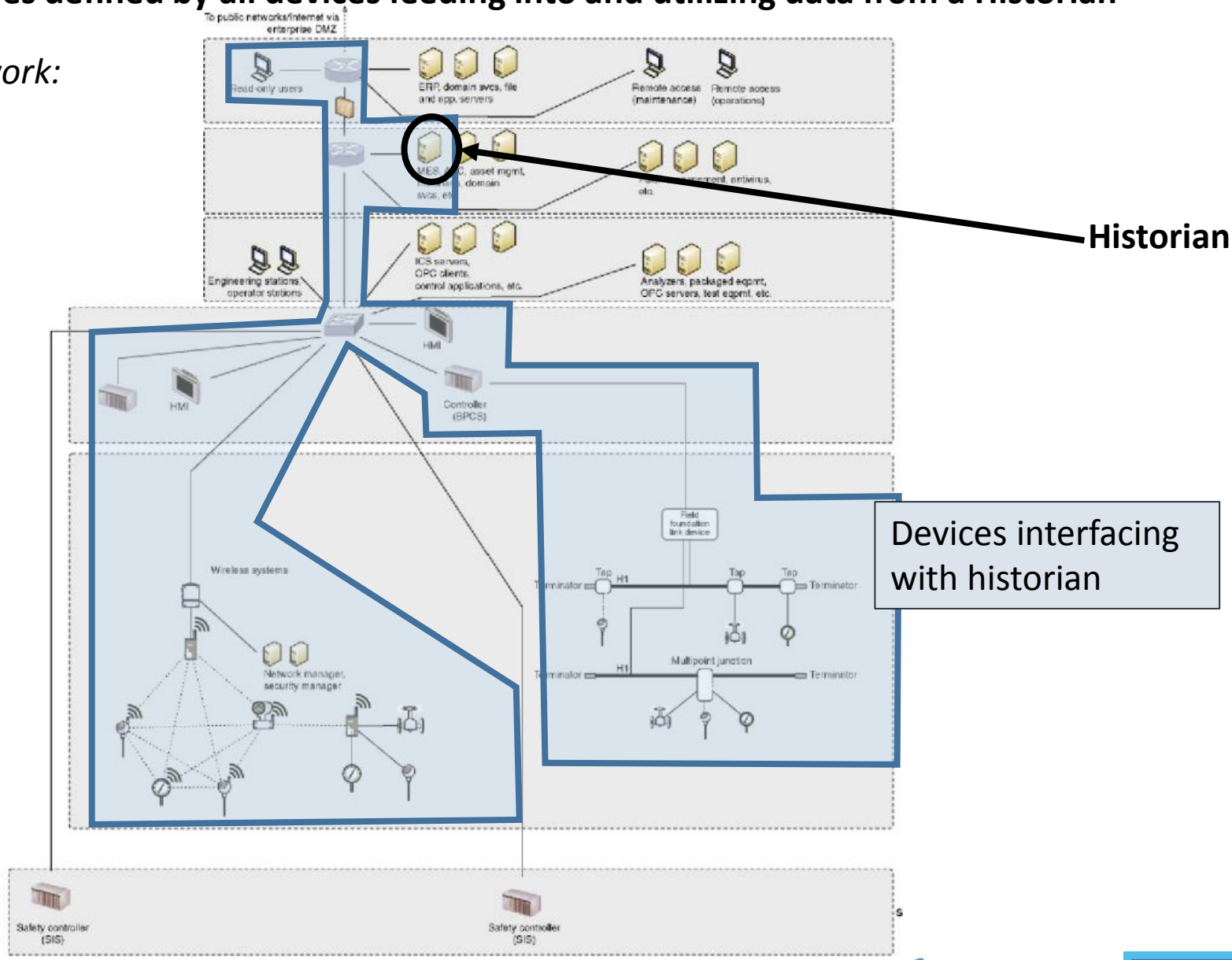
Example network:



Zones & Conduits

Zones defined by all devices feeding into and utilizing data from a Historian

Example network:

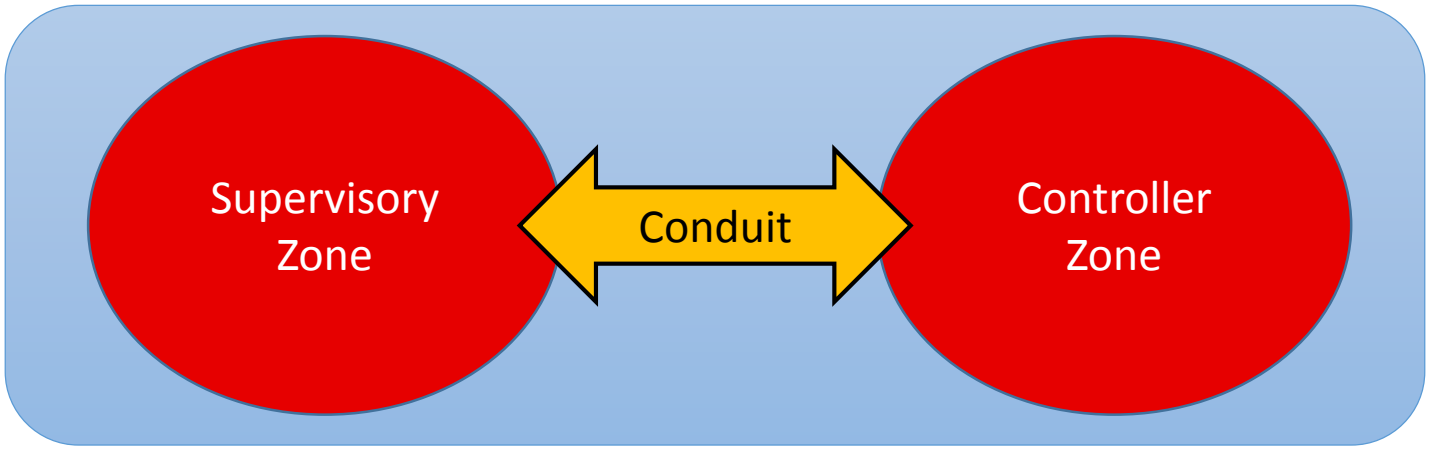


Devices interfacing with historian

Zones & Conduits

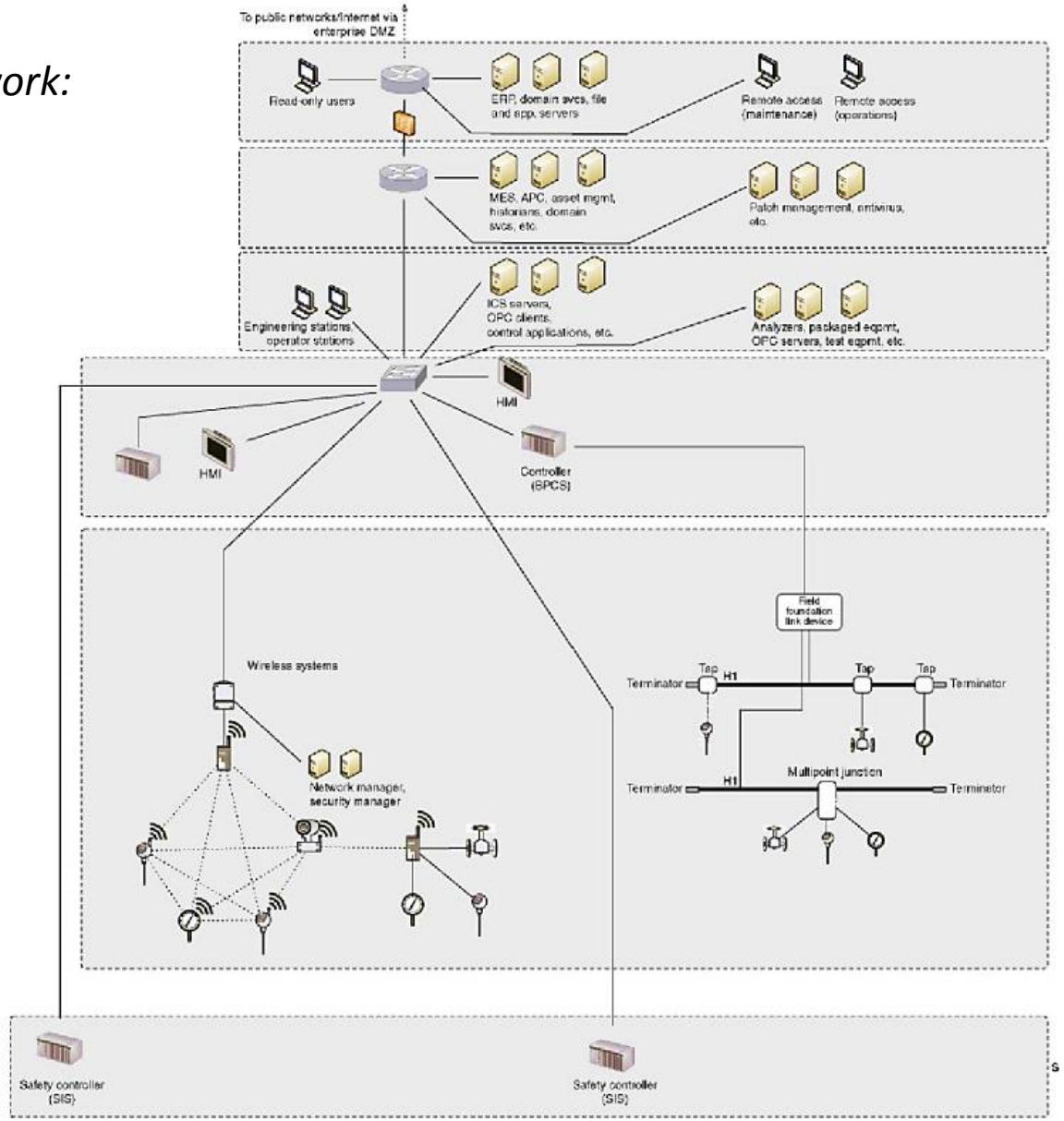
"**Conduit**": is a path for the flow of information between two zones.

- It can provide the security functions that allow different zones to communicate securely
- Any transfer of electronic data between zones must have a conduit



Zones & Conduits

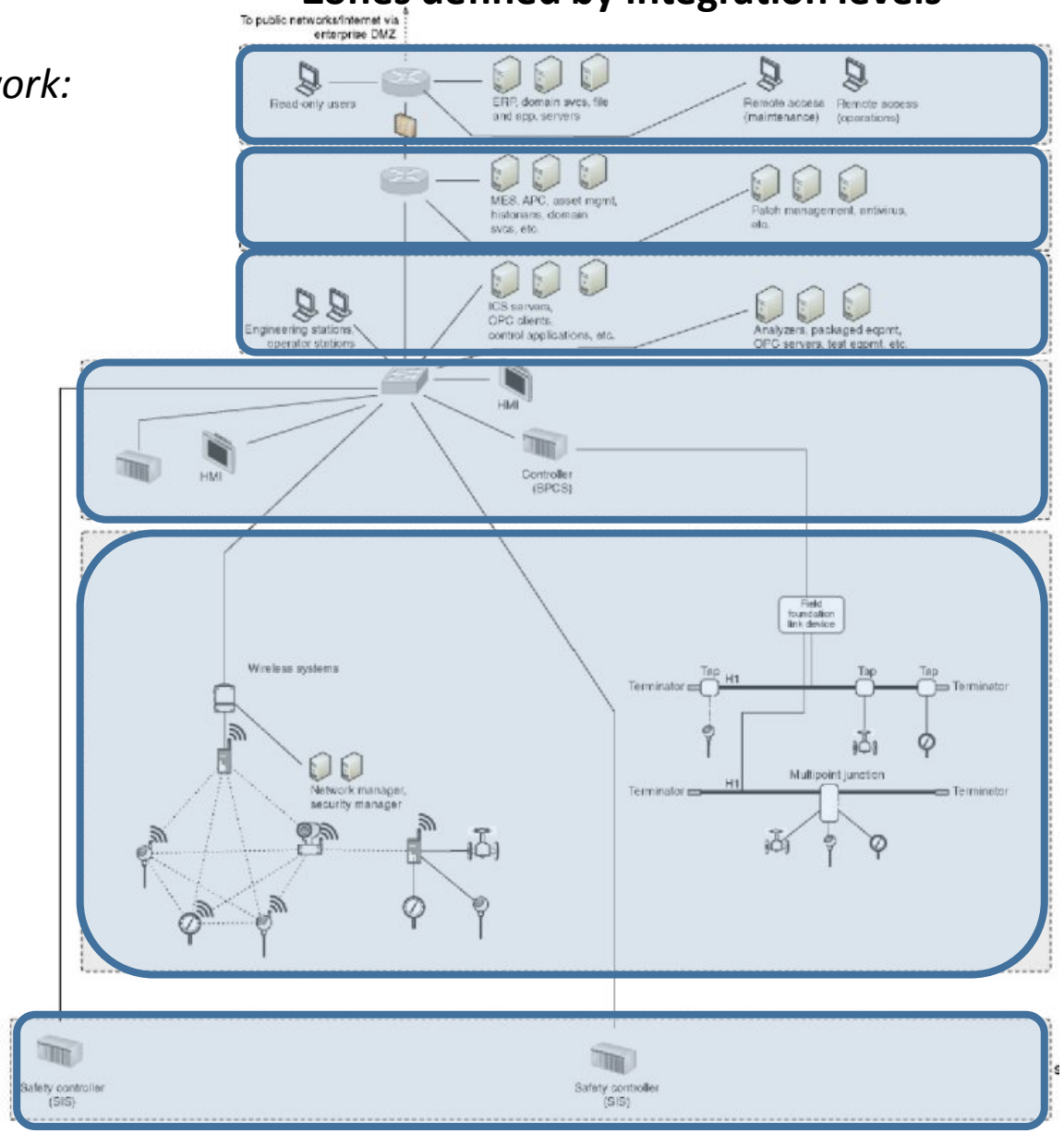
Example network:



Zones & Conduits

Example network:

Zones defined by integration levels



Business Zones

Operational control zones

Supervisory control zones

Local control zones

Process zones

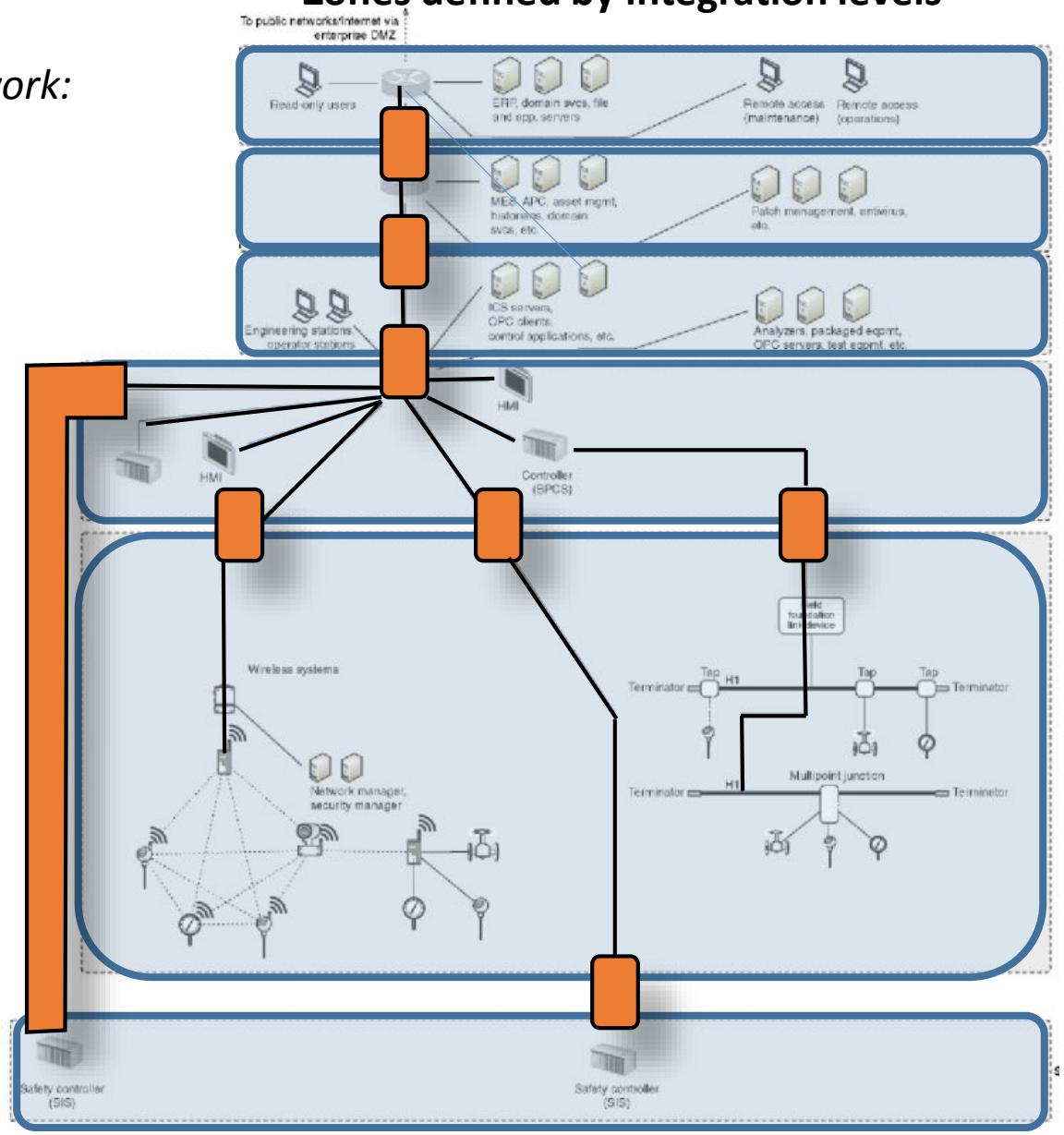
Safety Zones

Zones & Conduits

Example network:

Conduits

Zones defined by integration levels



Business Zones

Operational control zones

Supervisory control zones

Local control zones

Process zones

Safety Zones

Zones & Conduits

The zone and conduit model, when properly implemented,

- will **limit digital communications** in such a way that each zone will be inherently more secure
- provides a very **strong and stable foundation** upon which to build and maintain a cyber security policy
- supports other wellknown security principles;
  - **the Principle of Least Privilege**
    (where user can only access systems to which they are authorized)
  - **the Principle of Least route**
    (where a network node is only given the connectivity necessary to perform its function)

Basisconcepten voor het ontwerpen van veilig industriële netwerken

- Zones & Conduits model
- Network Segmentation & Segregation
- Defense in Depth

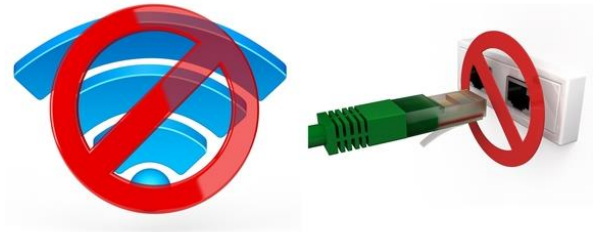
Basisconcepten voor het ontwerpen van veilig industriële netwerken

- Zones & Conduits model
- **Network Segmentation & Segregation**
- Defense in Depth

Network Segmentation & Segregation

"**Segregation**" pertains to the elimination of communication or data flow either within or between the networks and/or zones, in orde to fully isolate systems.

=> *Examples include the "air gap"*

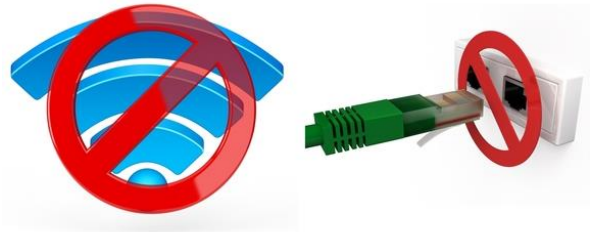


Segregation (like segmentation) can occur at any layer of the OSI model, provided that the segregated environments do not share hardware or protocol implementations.

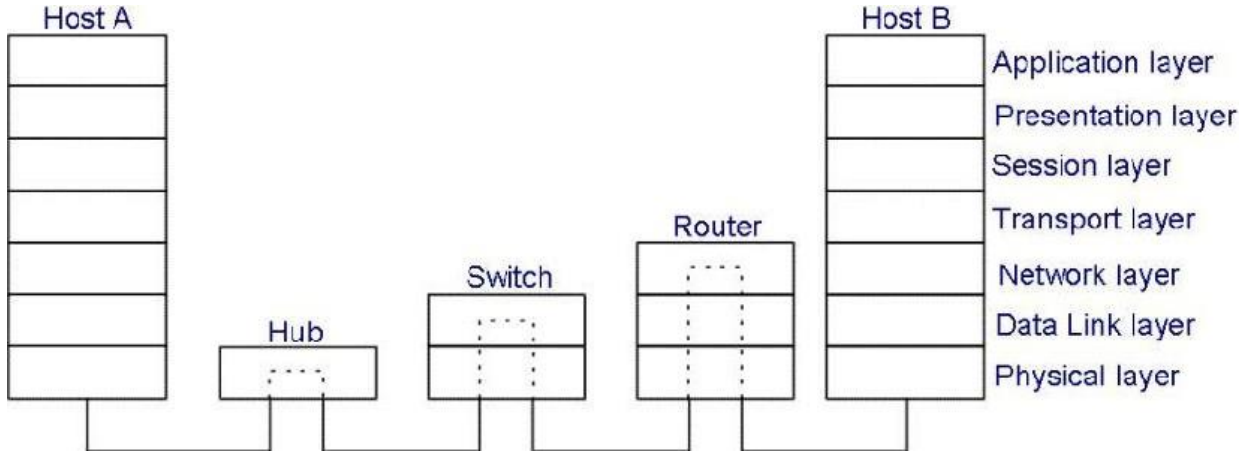
Network Segmentation & Segregation

"**Segregation**" pertains to the elimination of communication or data flow either within or between the networks and/or zones, in orde to fully isolate systems.

=> *Examples include the "air gap"*



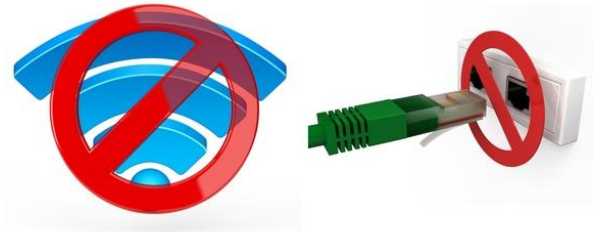
Segregation (like segmentation) can occur at any layer of the OSI model, provided that the segregated environments do not share hardware or protocol implementations.



Network Segmentation & Segregation

"**Segregation**" pertains to the elimination of communication or data flow either within or between the networks and/or zones, in orde to fully isolate systems.

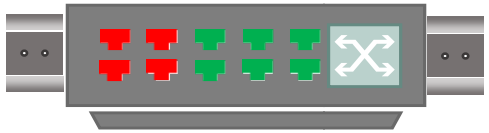
=> *Examples include the "air gap"*



Segregation (like segmentation) can occur at any layer of the OSI model, provided that the segregated environments do not share hardware or protocol implementations.

=> *Example: VLANS*

Vlan 1
Vlan 2

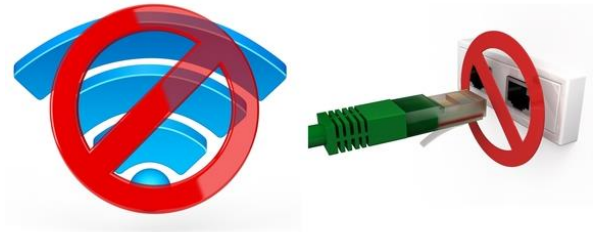


2 VLANS on one switch

Network Segmentation & Segregation

"**Segregation**" pertains to the elimination of communication or data flow either within or between the networks and/or zones, in orde to fully isolate systems.

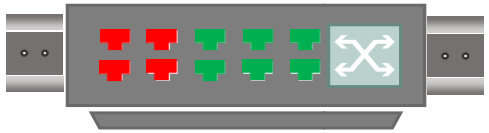
=> *Examples include the "air gap"*



Segregation (like segmentation) can occur at any layer of the OSI model, provided that the segregated environments do not share hardware or protocol implementations.

=> *Example: VLANS*

Vlan 1
Vlan 2



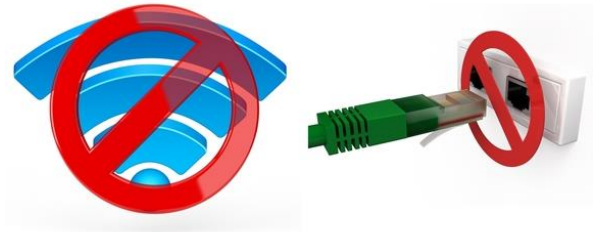
2 VLANS on one switch => shared hardware

~~**Segregation**~~

Network Segmentation & Segregation

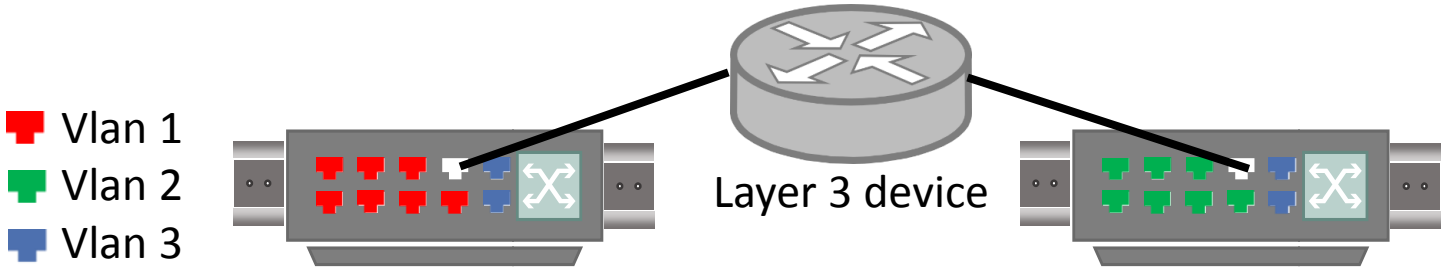
"**Segregation**" pertains to the elimination of communication or data flow either within or between the networks and/or zones, in orde to fully isolate systems.

=> *Examples include the "air gap"*



Segregation (like segmentation) can occur at any layer of the OSI model, provided that the segregated environments do not share hardware or protocol implementations.

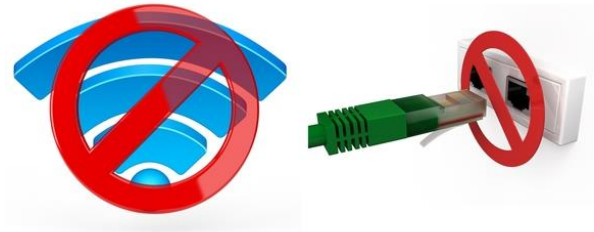
=> *Example: VLANS*



Network Segmentation & Segregation

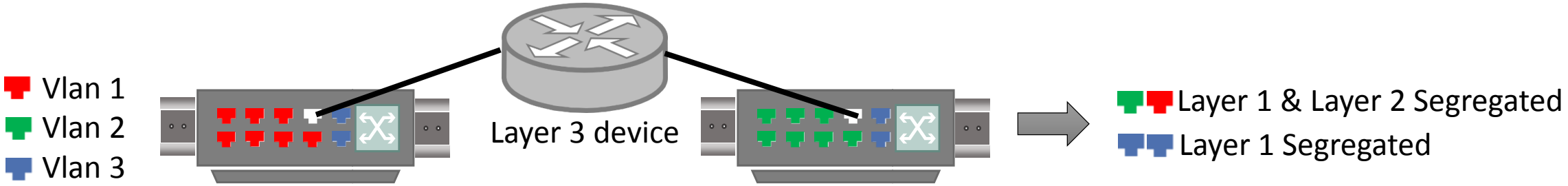
"**Segregation**" pertains to the elimination of communication or data flow either within or between the networks and/or zones, in orde to fully isolate systems.

=> *Examples include the "air gap"*



Segregation (like segmentation) can occur at any layer of the OSI model, provided that the segregated environments do not share hardware or protocol implementations.

=> *Example: VLANS*



Network Segmentation & Segregation

"**Segmentation**" pertains to the division of networks (network segmentation) or zones (zone segmentation) into smaller units. Segmented networks still must intercommunicate over common infrastructure.

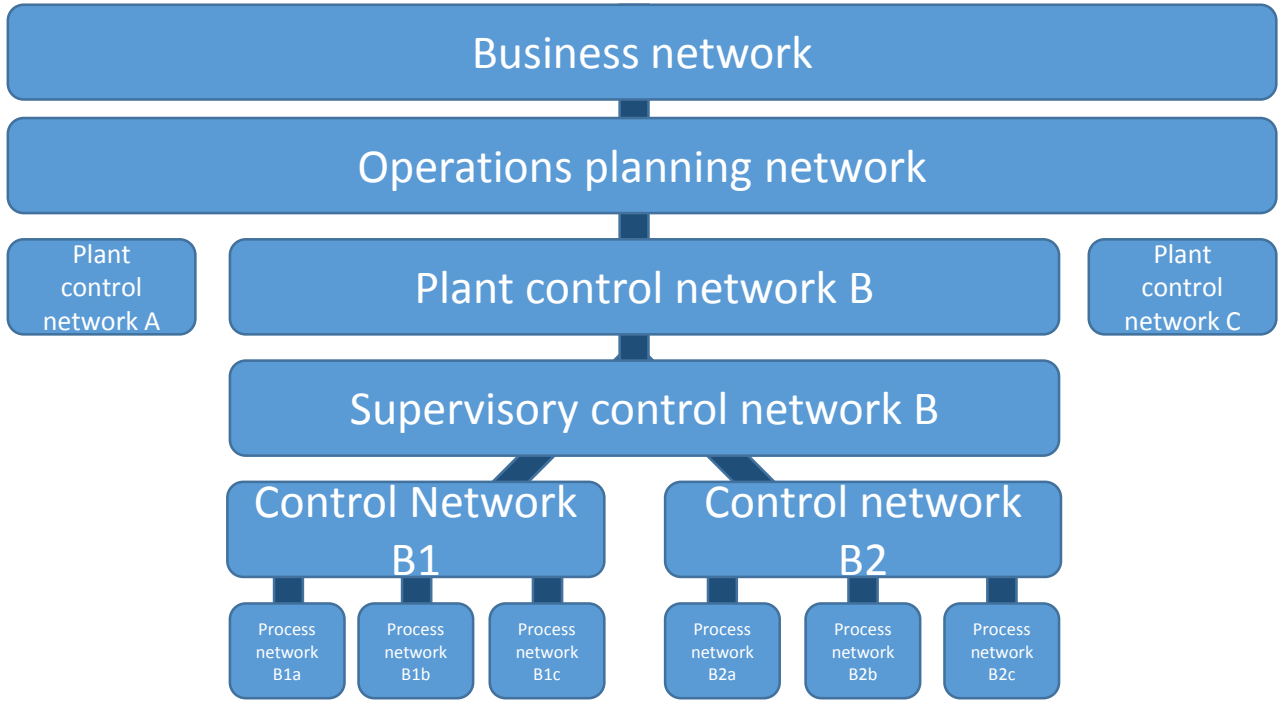
Segmentation (like segregation) can occur on every level of the OSI model:

Segmentation	Provided by	Management	Perfomance	Network security	ICS protocol support	OT applicability
Phyical layer	*Data Diode	None	Good	Absolute	N/A	High
Data Link Layer	*VLAN	Moderate	Good	Very Broad *	High	High
Network layer	*Layer 3 switch *Router	Low	Moderate	Broad	High	High
Session Layer	*Firewall *IPS *Protocol anomaly detection	Moderate	Low	Specific	Moderate	Moderate
Application Layer	*Application Proxy/IPS *application Firewall	High	Poor	Very Specific	Low	Low

** VLANS are susceptible to a variety of Layer 2 attacks (Flood attacks, Spanning Tree attacks, ARP poisening,...)*

Network Segmentation & Segregation

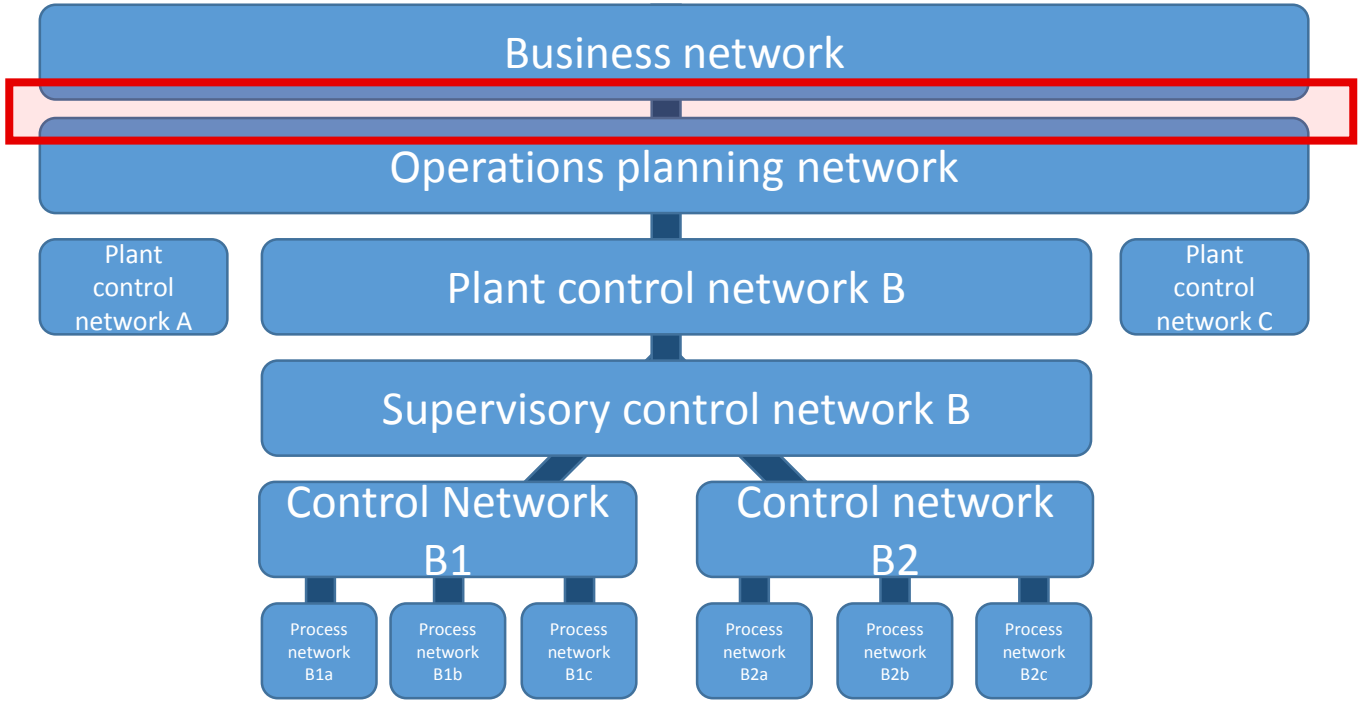
"**Segmentation**" pertains to the division of networks (network segmentation) or zones (zone segmentation) into smaller units. Segmented networks still must intercommunicate over common infrastructure.



A conceptual representation of network segmentation in industrial systems

Network Segmentation & Segregation

"**Segmentation**" pertains to the division of networks (network segmentation) or zones (zone segmentation) into smaller units. Segmented networks still must intercommunicate over common infrastructure.

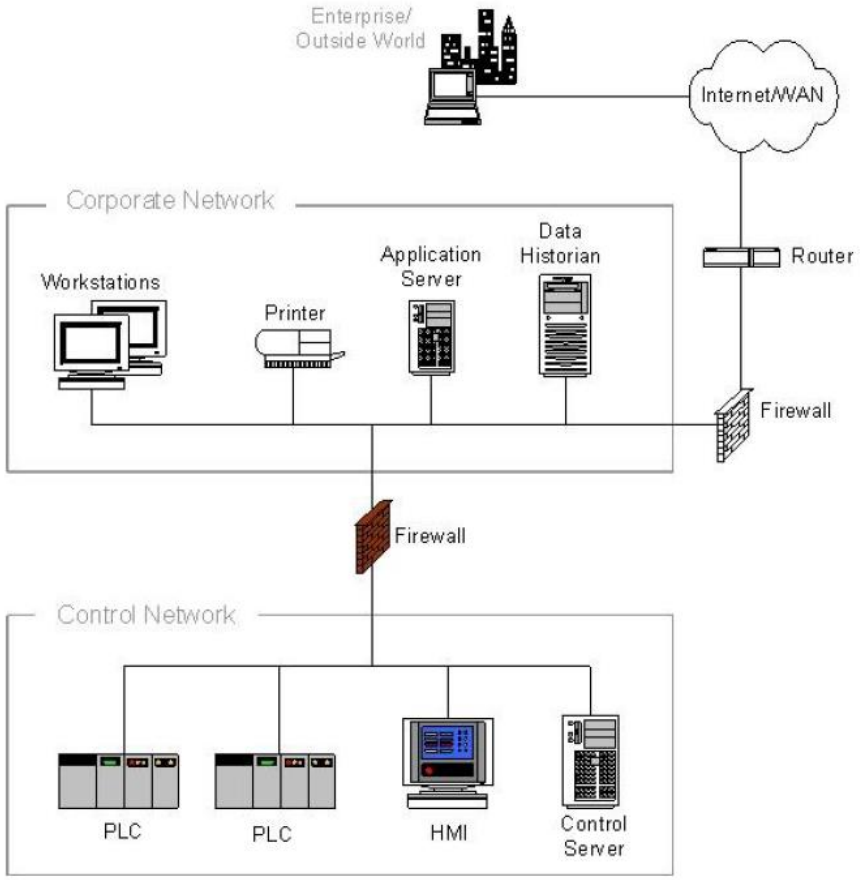


A conceptual representation of network segmentation in industrial systems

Network Segmentation & Segregation

ICS networks and corporate networks can be segmentated to enhance cybersecurity using different architectures:

Architecture 1: Firewall between corporate Network and Control Network

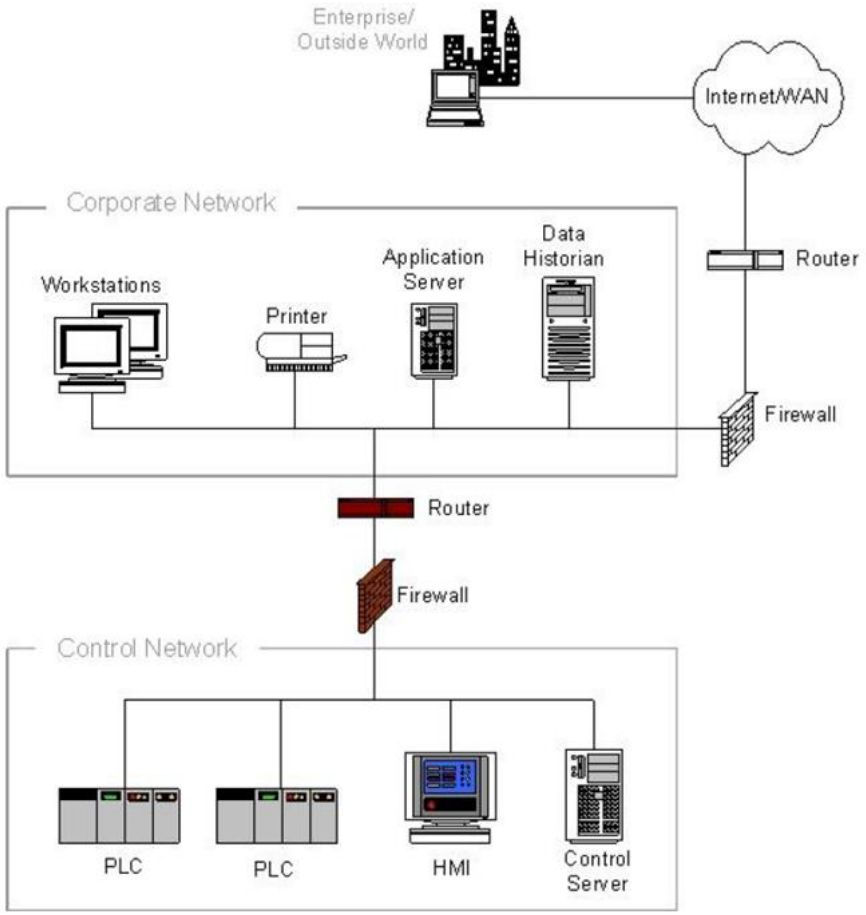


- ✚ Significant improvement over non-segmentated networks
- ▬ Requires the use of firewall rules that allow direct communications between corporate and control network

Network Segmentation & Segregation

ICS networks and corporate networks can be segmentated to enhance cybersecurity using different architectures:

Architecture 2: Firewall and router between corporate Network and Control Network

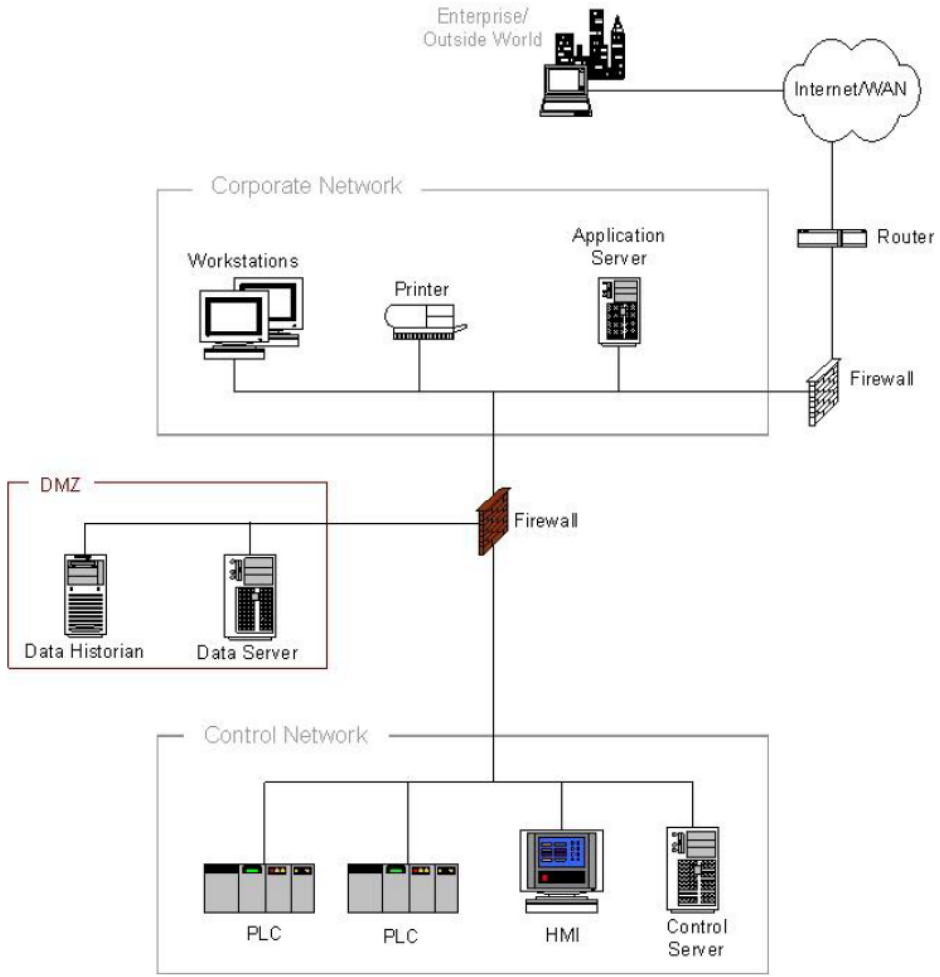


- ✚ Router offers basic packet filtering services and reduces load on firewall
- ✚ two devices must be bypassed (Improved defense in depth)
- ➖ Direct communication between office and Control network

Network Segmentation & Segregation

ICS networks and corporate networks can be segmentated to enhance cybersecurity using different architectures:

Architecture 3: Firewall with DMZ between corporate Network and Control Network

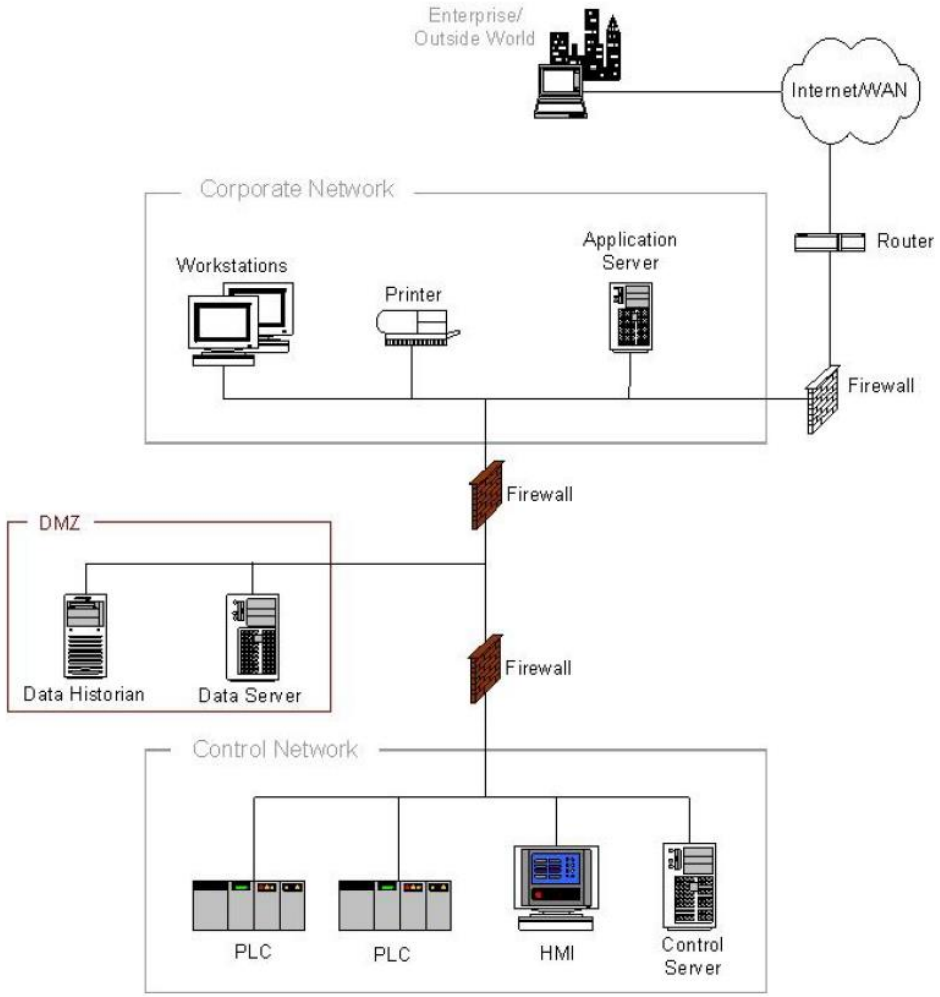


- \+ Significant improvement by creating DMZ
- \+ No direct communication paths between office and control network
- – Only one device must be bypassed
- – If server in DMZ is compromised it can launch attack on Control network (efforts must be made to harden and actively patch servers in DMZ)

Network Segmentation & Segregation

ICS networks and corporate networks can be segmentated to enhance cybersecurity using different architectures:

Architecture 4: Paired Firewalls with DMZ between corporate Network and Control Network



- ✚ Second firewall can prevent unwanted traffic from compromised server in DMZ
- ✚ Two devices can be managed seperatly (one for office needs, one for Control needs)
- ✚ two devices must be bypassed (Improved defense in depth)
- ▬ Increased cost and management complexity

Network Segmentation & Segregation

Segmentation is important for many reasons, including **network performance** considerations and **cyber security**.

Segregation is often byproduct of segmentation, but not all segments are segregated.

Segmentation and segregation are useful security controls in that they are vital in **mitigating the propagation or lateral movement** (i.e. Pivoting) of an attack once a network intrusion has occurred.

Basisconcepten voor het ontwerpen van veilig industriële netwerken

- Zones & Conduits model
- Network Segmentation & Segregation
- Defense in Depth

Basisconcepten voor het ontwerpen van veilig industriële netwerken

- Zones & Conduits model
- Network Segmentation & Segregation
- **Defense in Depth**

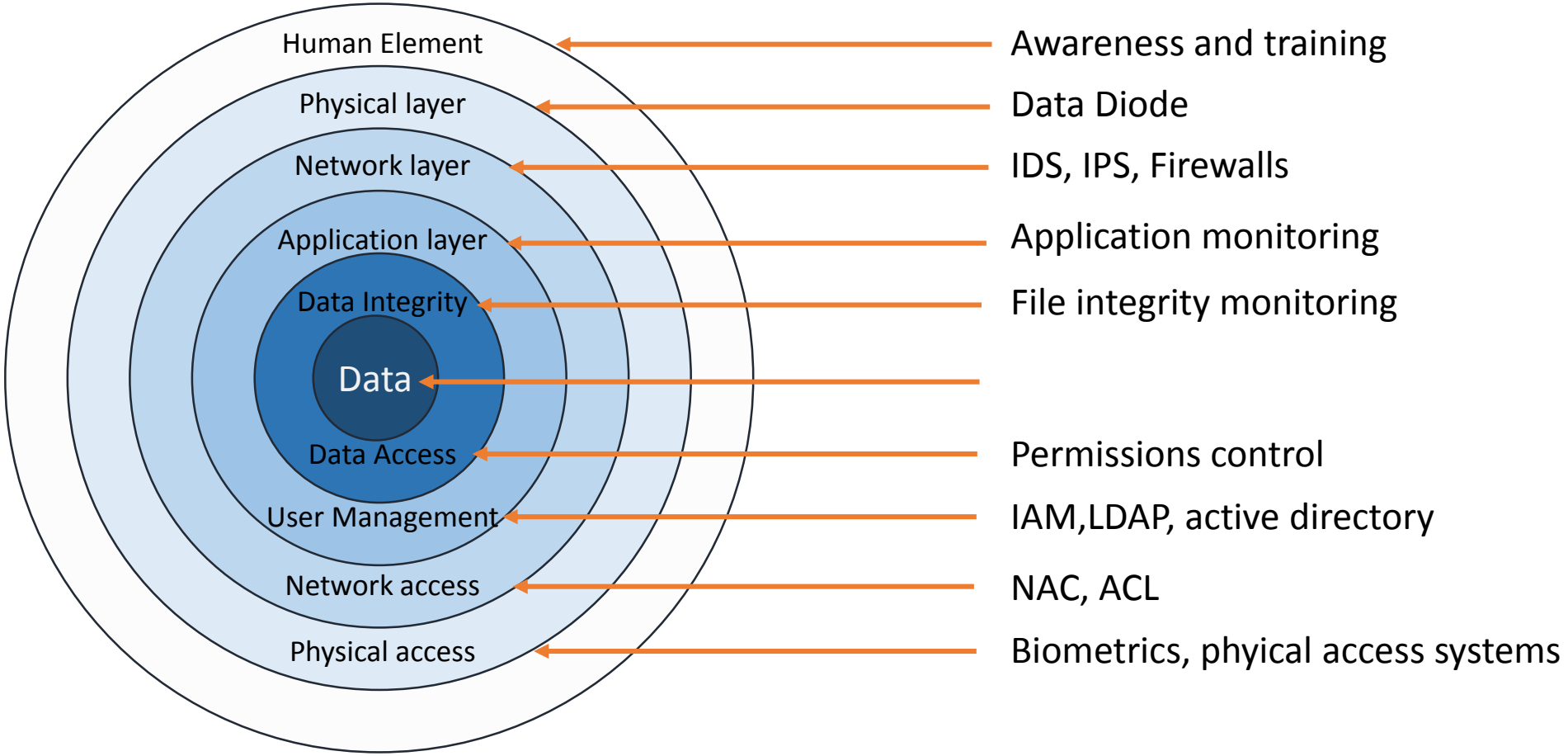
Defense in depth

The philosophy of a layered or tiered defensive strategy, also known as ***Castle Approach***

Defense in depth

Defense in depth

Layered Security approach



Defense in depth

A single security product, technology or solution cannot adequately protect an ICS by itself.

If a hacker gains access to a system, defense in depth minimizes the adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent recurrence

Basisconcepten voor het ontwerpen van veilig industriële netwerken

- Network Segmentation & Segregation
- Zones & Conduits model
- Defense in Depth


ANY
QUESTIONS
?