Purdue Model: the Good, Bad and Ugly

Purdue Model - Agenda

- Introduction
- Basic’s
- Differences of Model’s and interpretations
- Rabbit Holes and Mistake’s
- Use Case’s

- Key Take Away’s
- Q&A

Purdue Model - Disclaimer

- Opinions expressed are solely my own and do not express the views or opinions of my employer.

- Additionally, I will be leading you astray, when it comes to zones and conduits

Purdue Model – Whoami? Gavin Dilworth

BACKGROUND

Operator, Control System Engineer / Industrial Automation Engineer, Managing Consultant

PAST EXPERIENCE

Companies: Various system integrators, consultancy firms and end users
Industries: Manufacturing, Water and Waste, Oil and Gas and Energy

Roles: Engineer, ICS/OT Cybersecurity Lead, Managing Consultant
ICS/OT Security architecture, auditing, risk assessment and training

Qualifications:

- Master of Professional Practice in ICS Cyber Security
- Advanced Diploma in Industrial Automation
- SANS GICSP and GRID
- Offensive Security: OSCP

CURRENT ROLE

Nozomi Networks: Solution's Delivery Engineer

Activities:

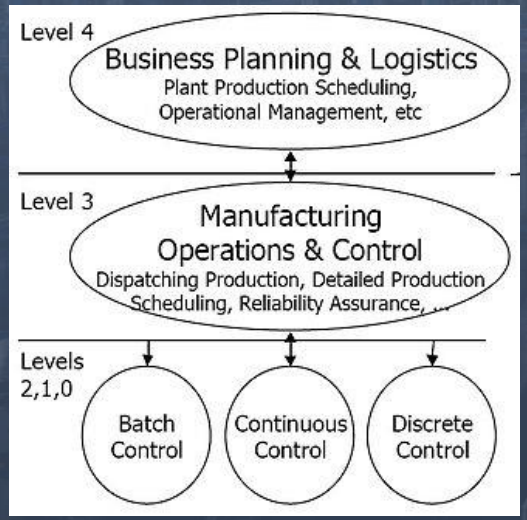
- Solutions Design, Delivery and Deployment
- Training Instructor
- Systems Integration
- PoCs

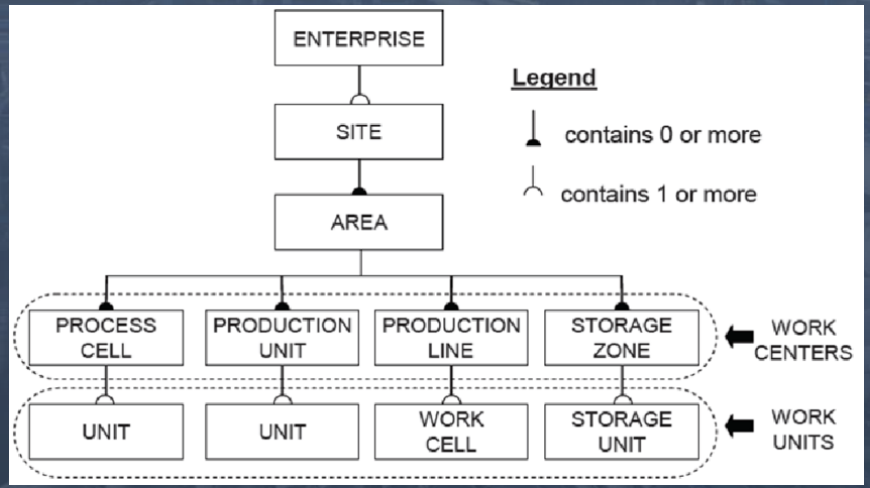
Purdue Model – Basic's

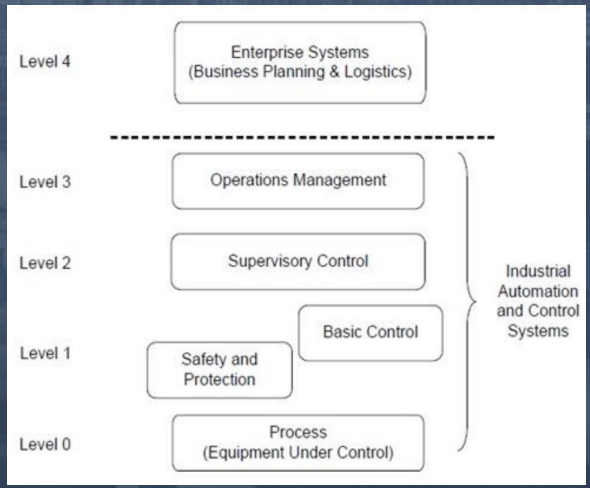
Purdue University != ISA-95 != IEC 62443

Model's are not gospel, they can change. Remember the saying
"all models are wrong, but some are useful"

Purdue Models can be done Logically or Physically







Purdue Model – Basic's

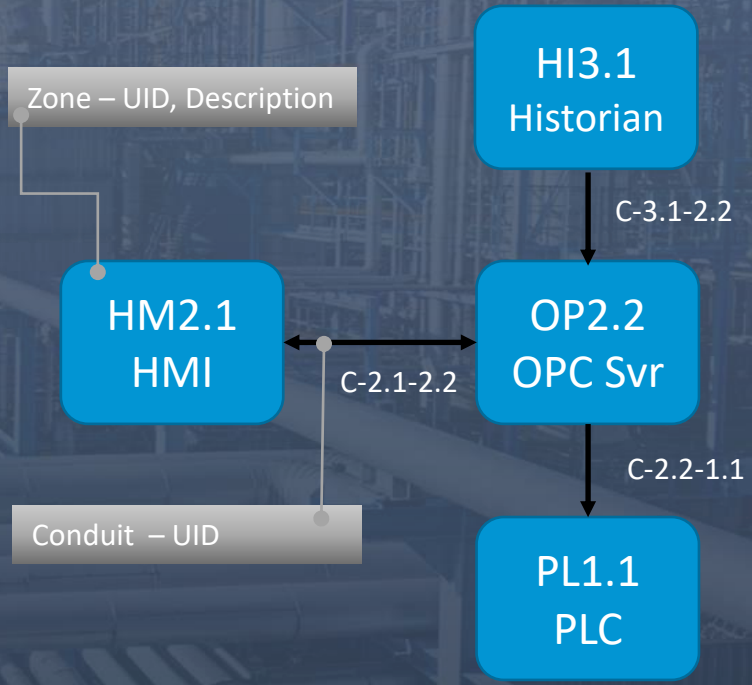
What do we need to know?

Levels, Zones and Conduits

Levels could look like this:

Level 5: Enterprise Networks
Level 4: Business Networks
Level 3: Site-Wide Supervisory
Level 2: Local Supervisory
Level 1: Local Controllers
Level 0: Field Devices

Why? "Could look like"
Well there's different interpretations, more on that later...

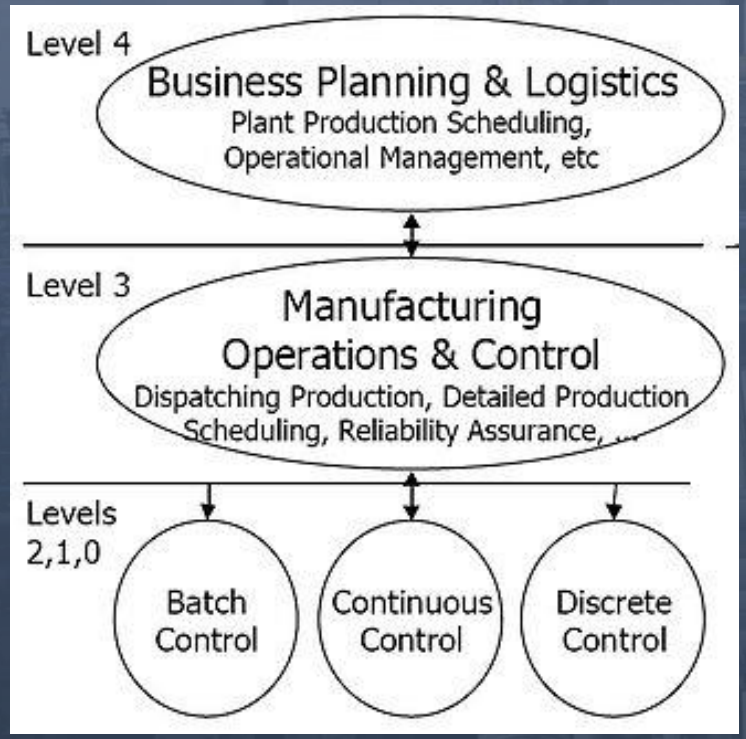


Purdue Model – Difference's

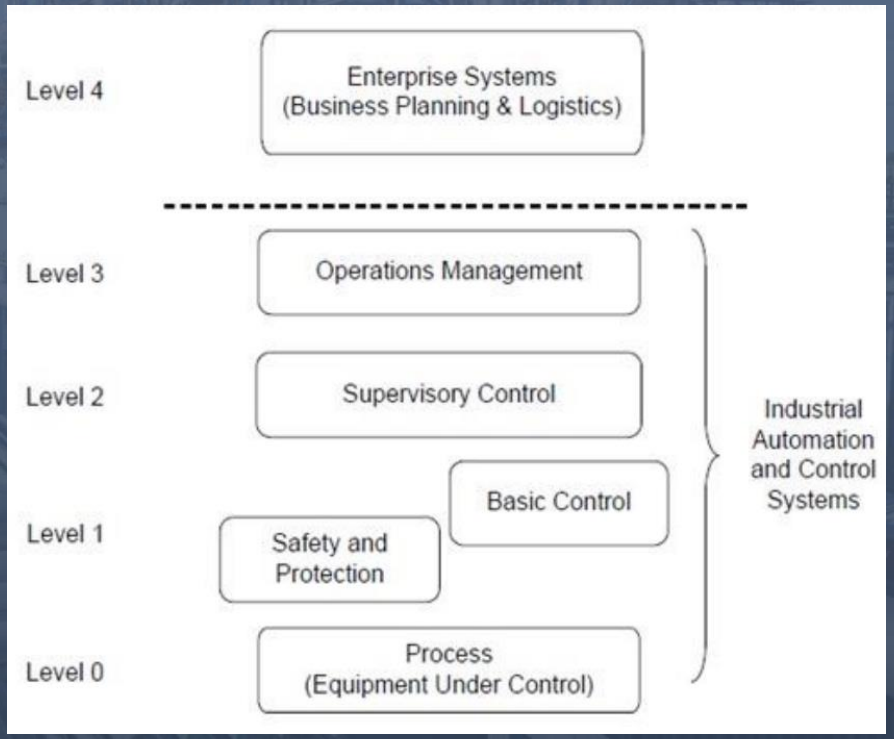
What's really the difference?

Data Model vs Security

ISA-95

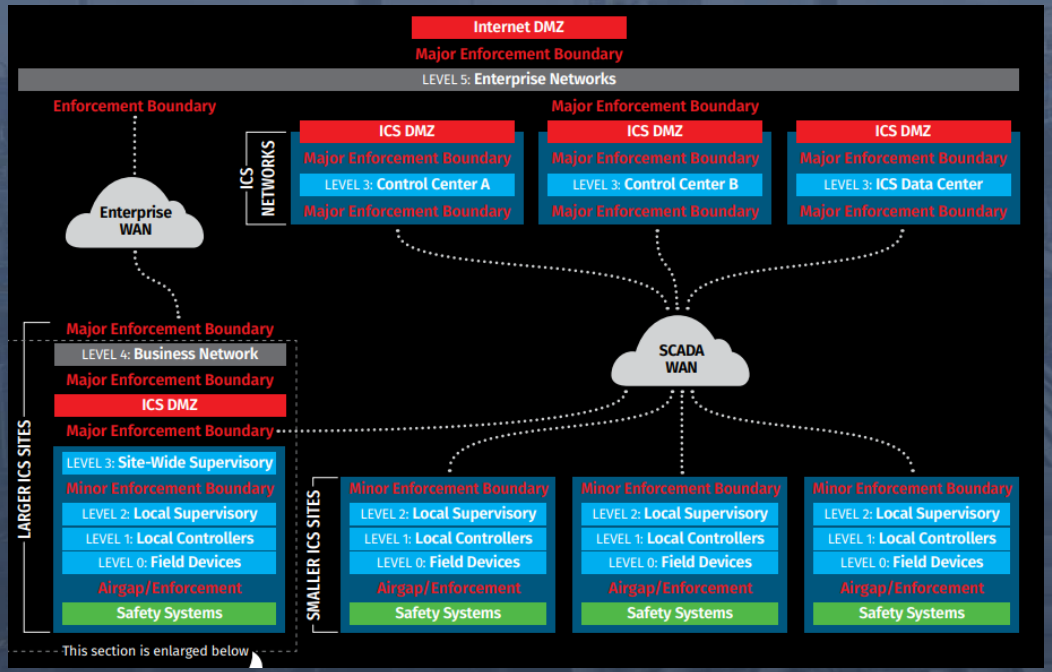


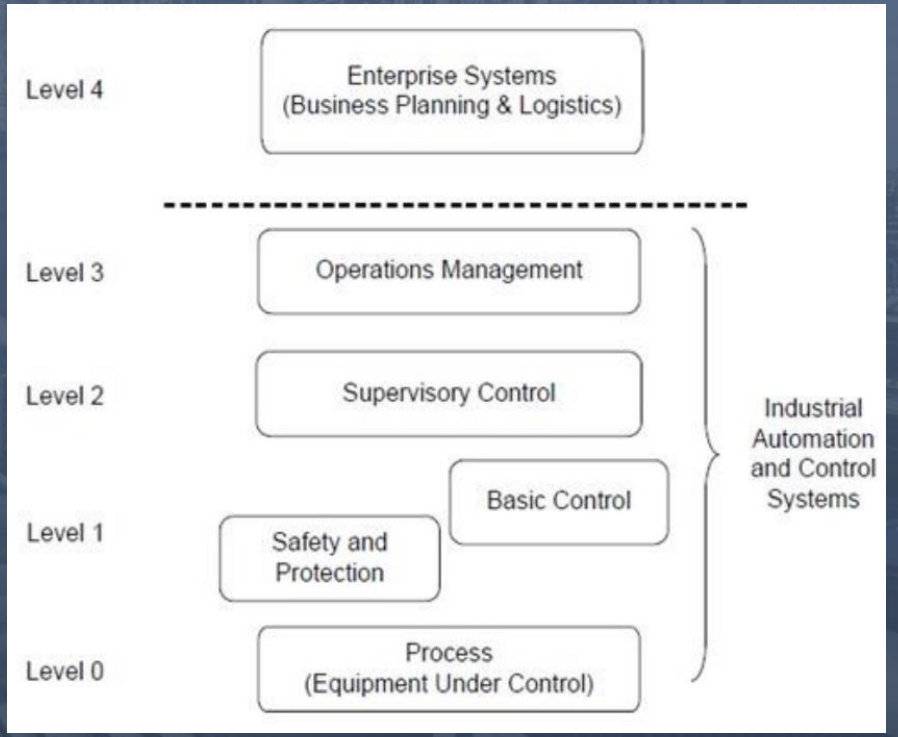
ISA-99 / IEC-62443



Purdue Model – Difference's

What's really the difference?

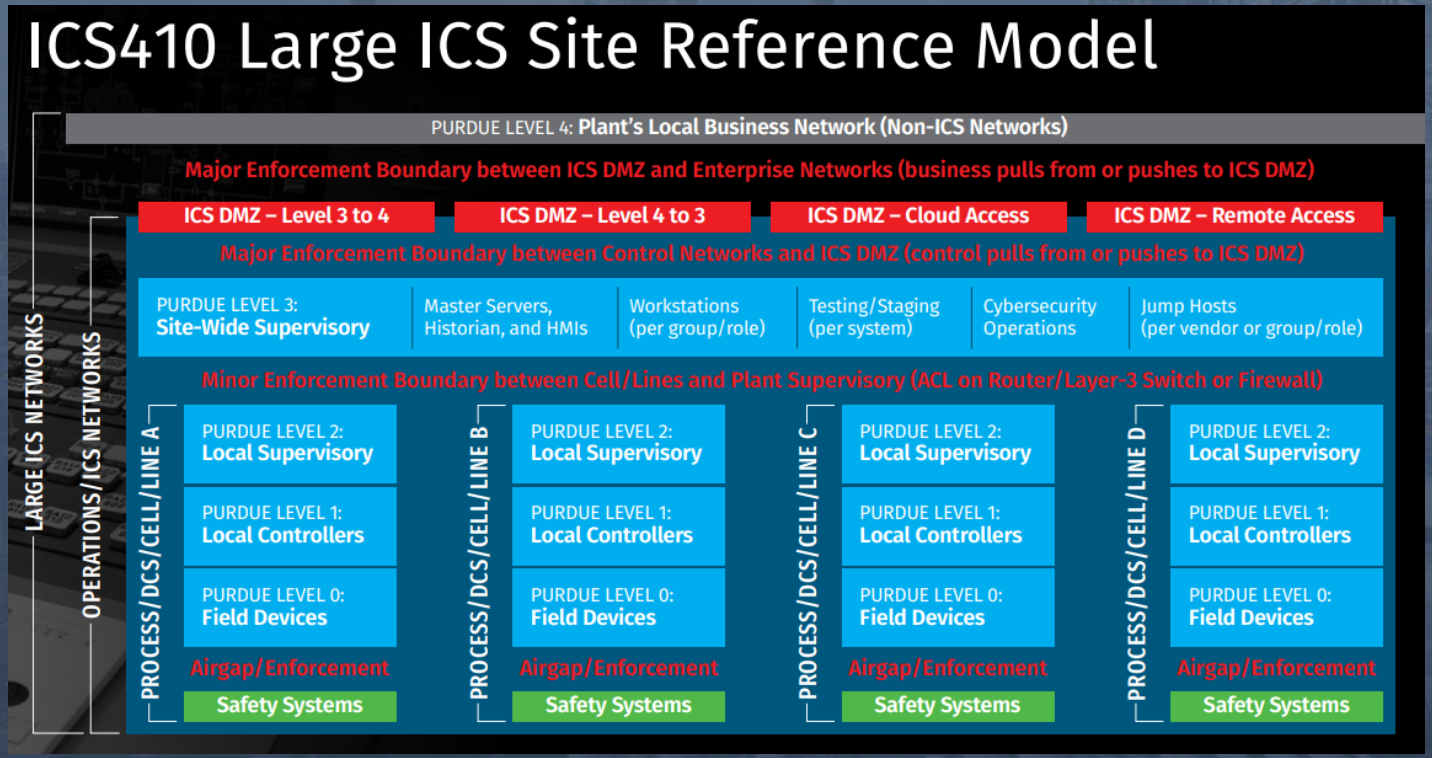


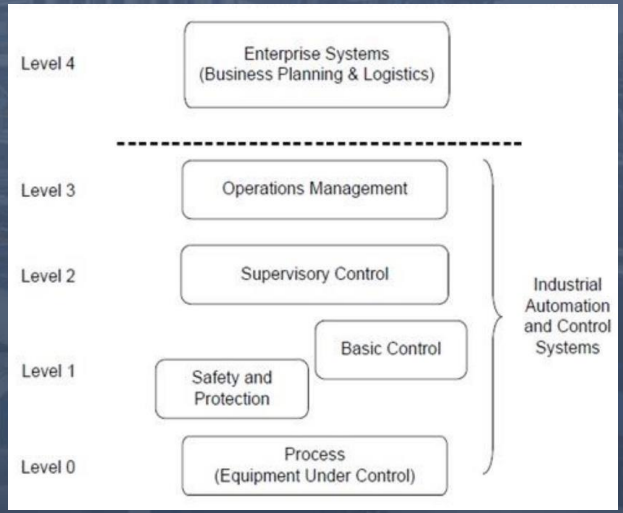


Source: SANS ICS Security – Control Systems Are a Target
https://sansorg.egnyte.com/dl/eQu4hT5fCW

Purdue Model – Difference's

What's really the difference?

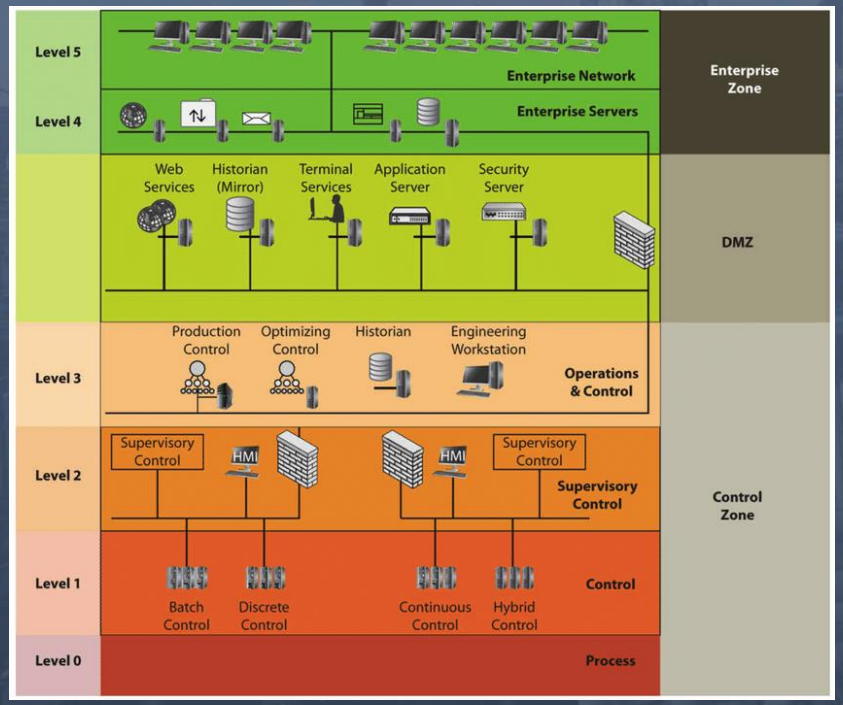


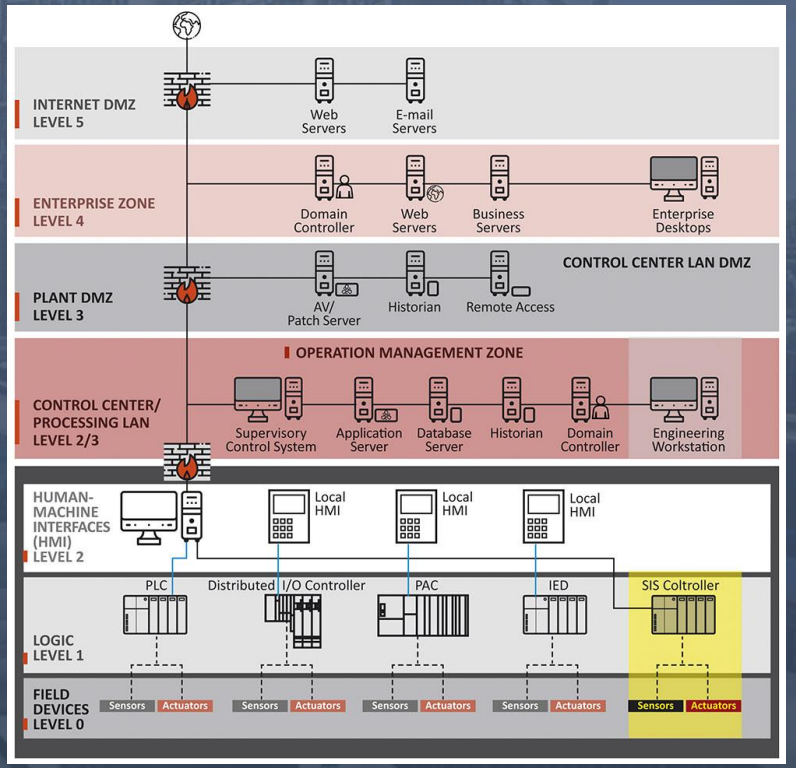


Source: SANS ICS Security – Control Systems Are a Target
https://sansorg.egnyte.com/dl/eQu4hT5fCW

Purdue Model – Difference's

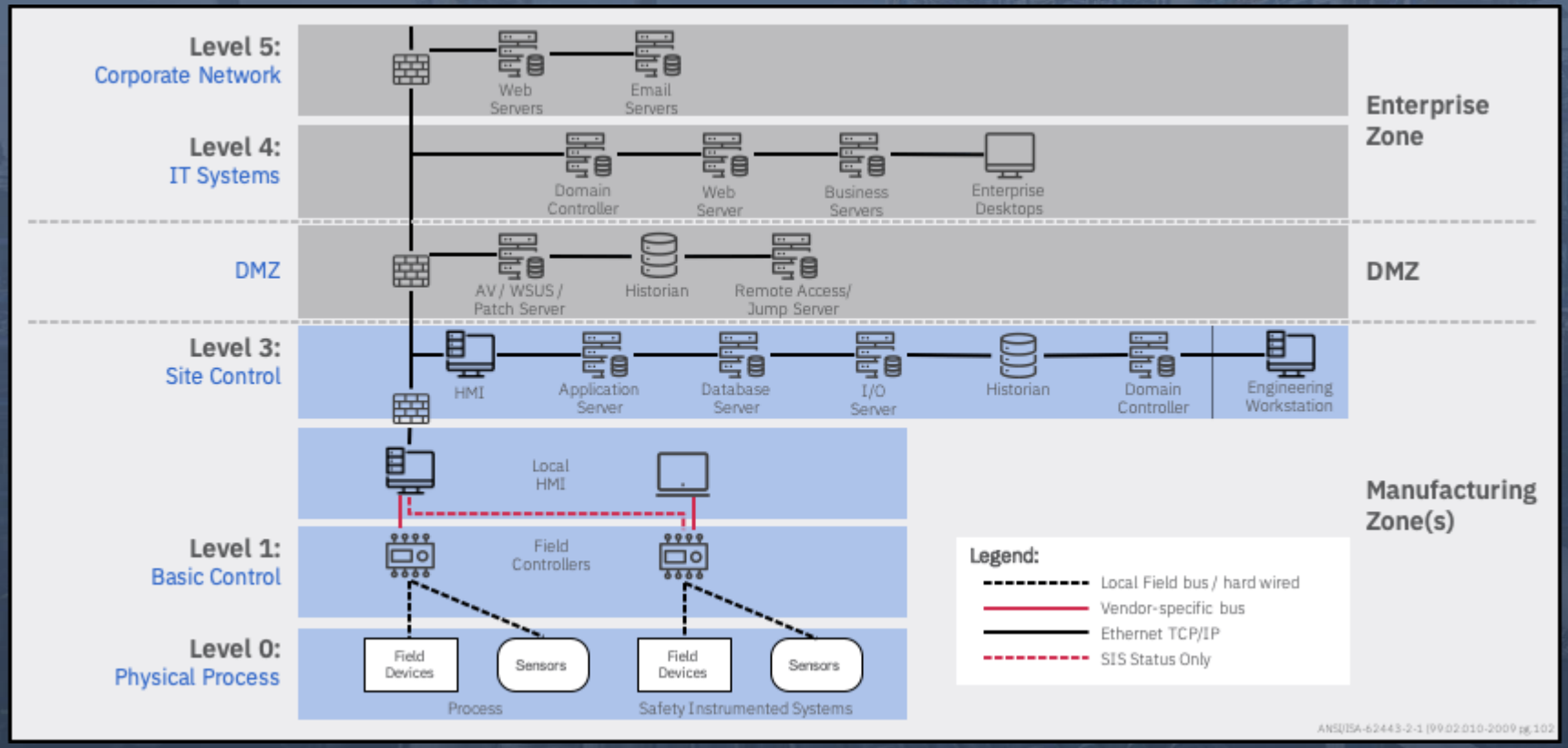
What's really the difference?





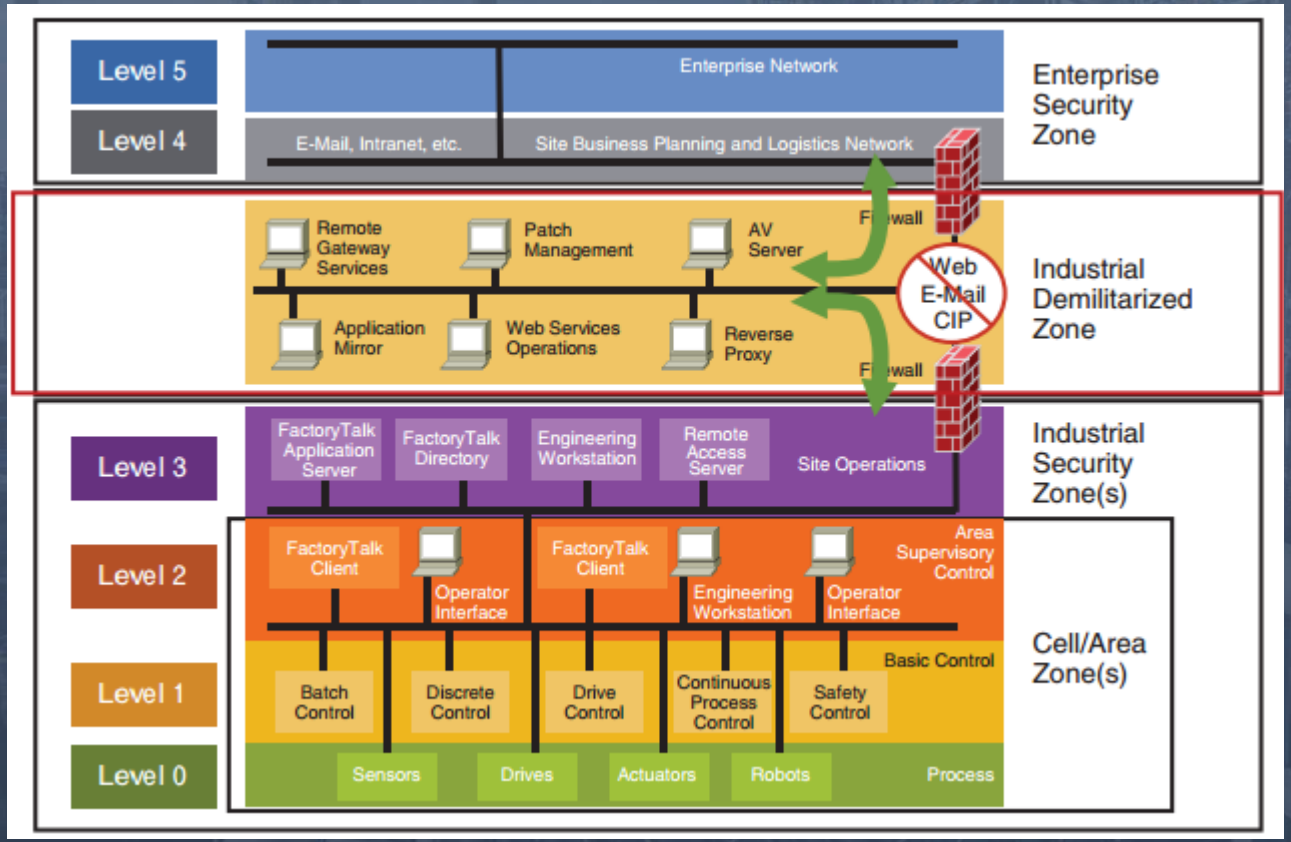
Purdue Model – Difference's

What's really the difference?



Purdue Model – Difference's

What's really the difference?



Purdue Model – Difference's

Back to the basics….

IEC 62443 Purdue Model – based on function

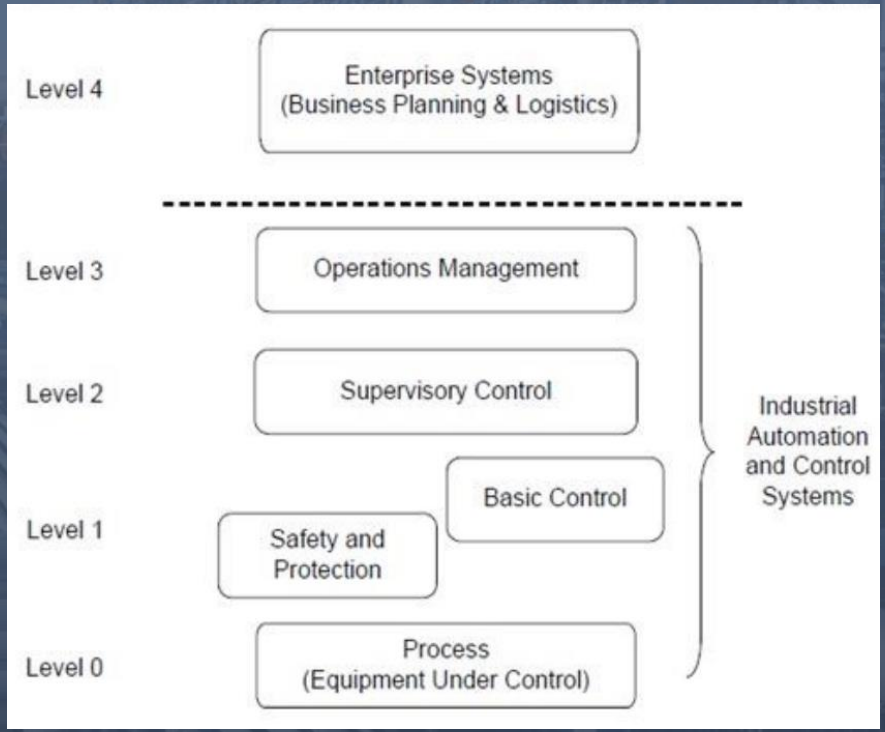
Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

Level 3: Operations Management
Historians, Domain Controllers, Jump Hosts, File Servers

Level 2: Supervisory Control
Local Visulisation

Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators



Purdue Model – Difference's

IEC 62443 Purdue Model – based on function

Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

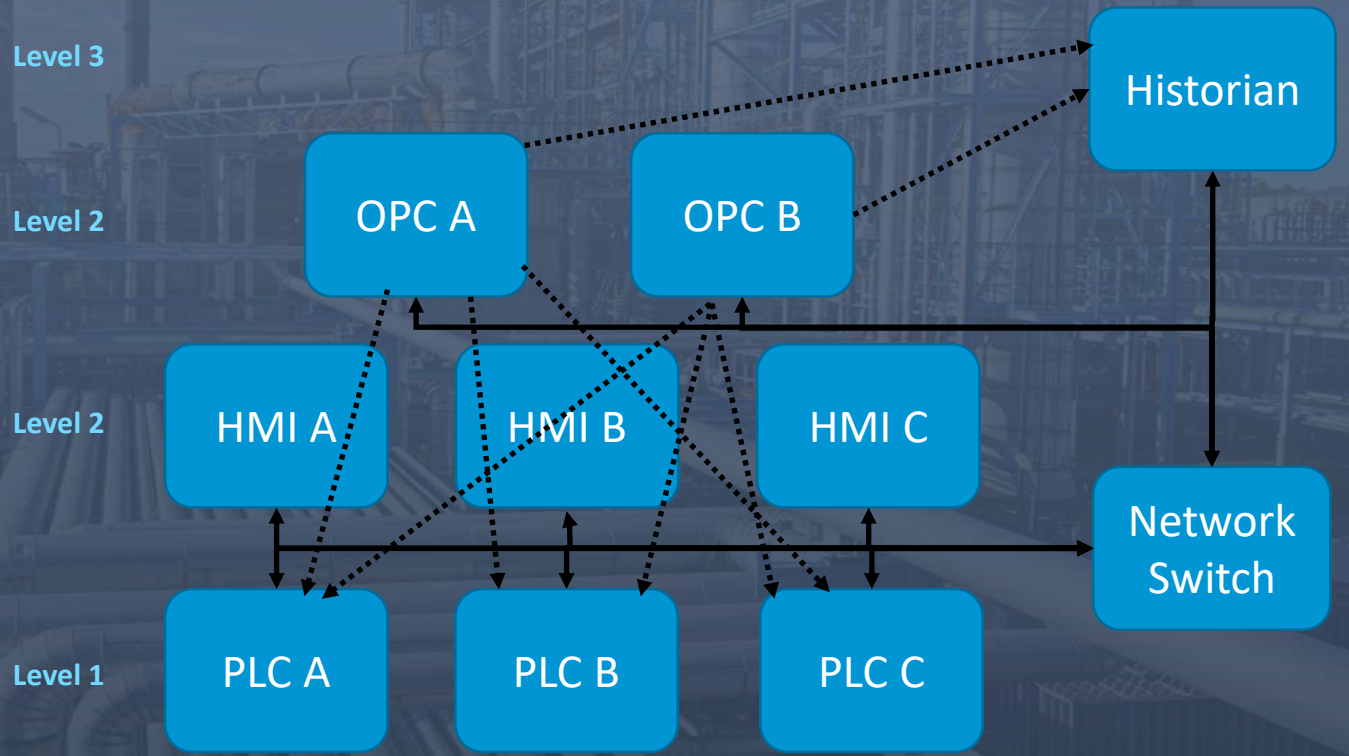
Level 3: Operations Management
Historians, Domain Controllers, Jump Hosts, File Servers

Level 2: Supervisory Control
Local Visulisation

Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators

One Site (Small Systems - Physical)



Purdue Model – Difference's

One Site (Small Systems - Logical)

IEC 62443 Purdue Model – based on function

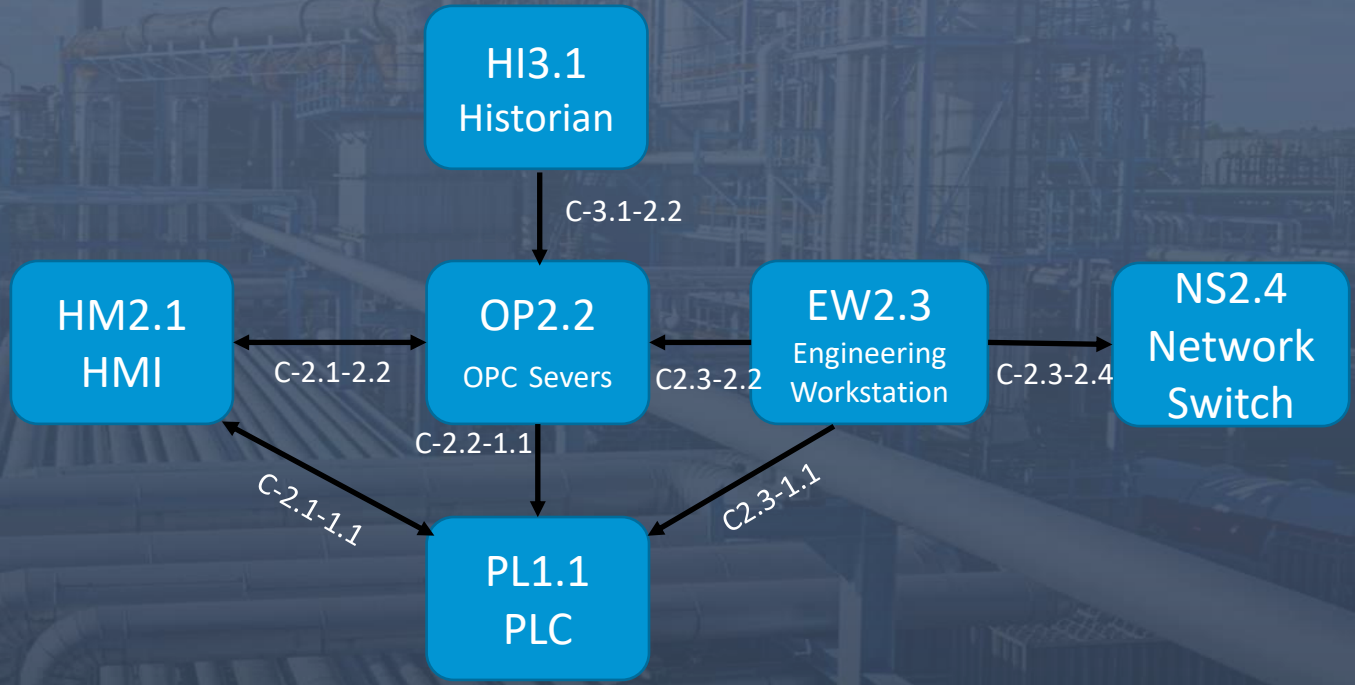
Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

Level 3: Operations Management
Historians, Domain Controllers, Jump Hosts, File Servers

Level 2: Supervisory Control
Local Visulisation

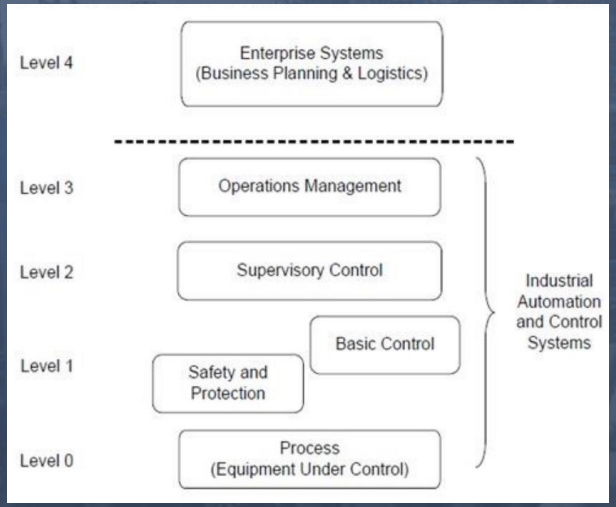
Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators



Purdue Model – Difference's

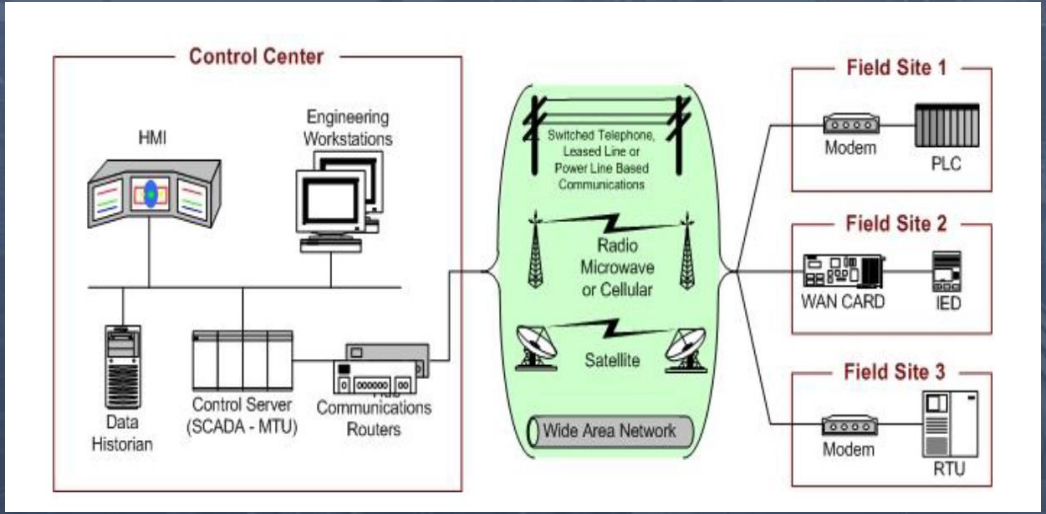
One Site (Large Systems - Logical)



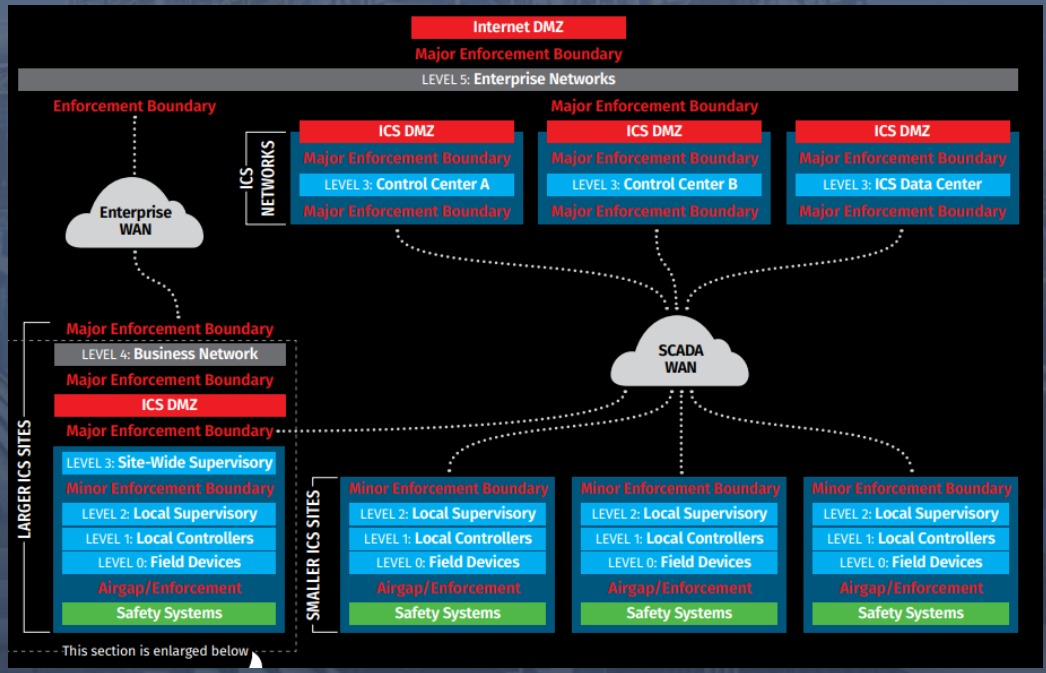
It's the same, just more zones and more conduits

Purdue Model – Difference's

Multiple Site's (Logical)



Source: NIST SP 800-82 Rev. Guide to Operational Technology (OT) Security
https://doi.org/10.6028/NIST.SP.800-82r2



Source: SANS ICS Security – Control Systems Are a Target
https://sansorg.egnyte.com/dl/eQu4hT5fCW

Purdue Model – Difference's

IEC 62443 Purdue Model – based on function

Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

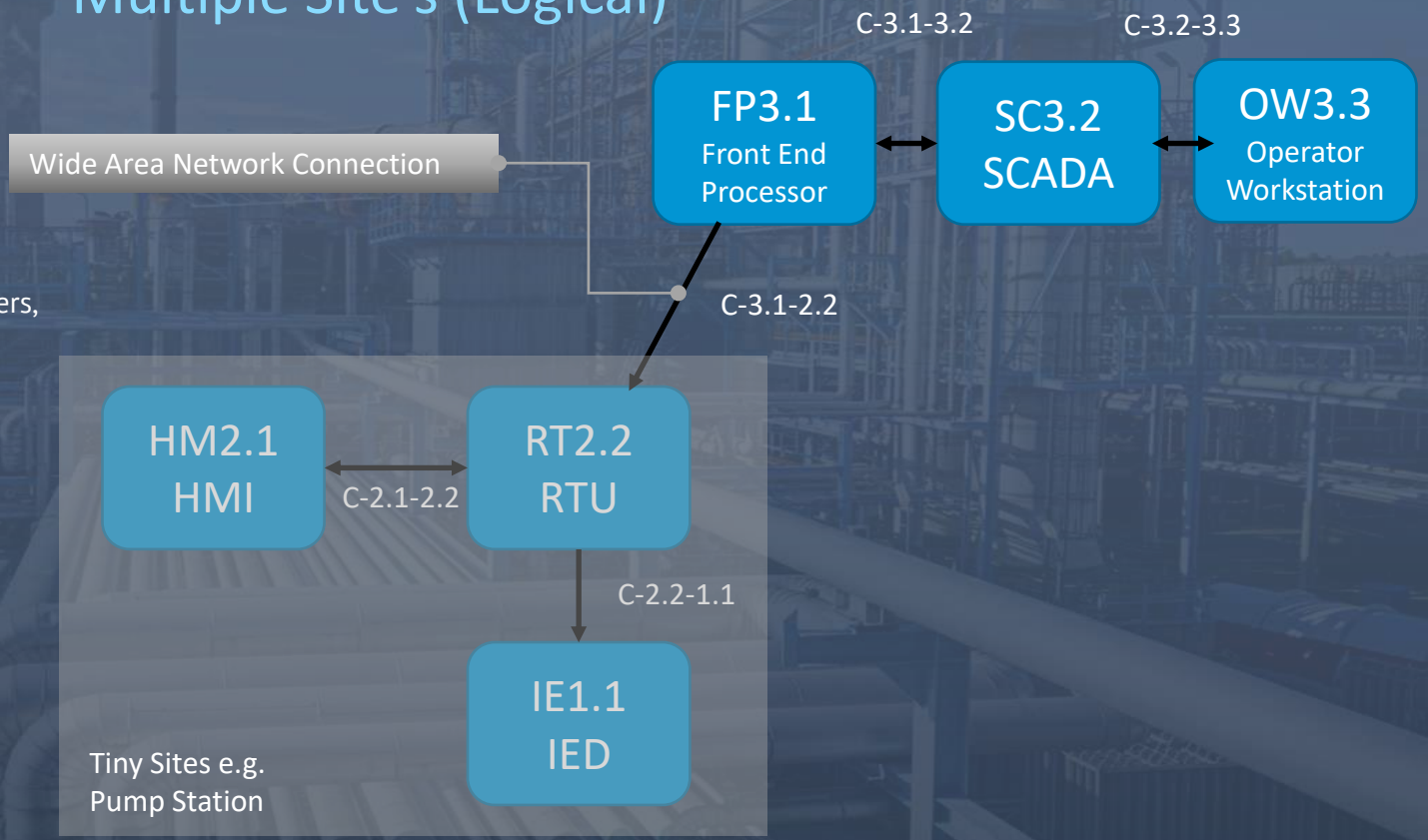
Level 3: Operations Management / Site-Wide Supervisory
Historians, Domain Controllers, Jump Hosts, File Servers, Wide Are Network SCADA (Supervisory Control)

Level 2: Supervisory Control
Local Visulisation

Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators

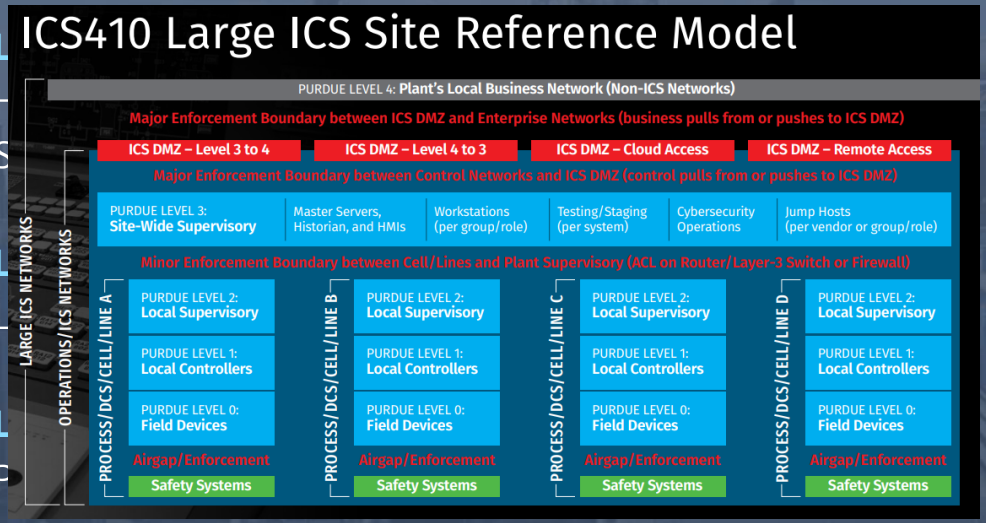
Multiple Site's (Logical)



Purdue Model – Rabbit Hole's – SCADA Plant A/B/C

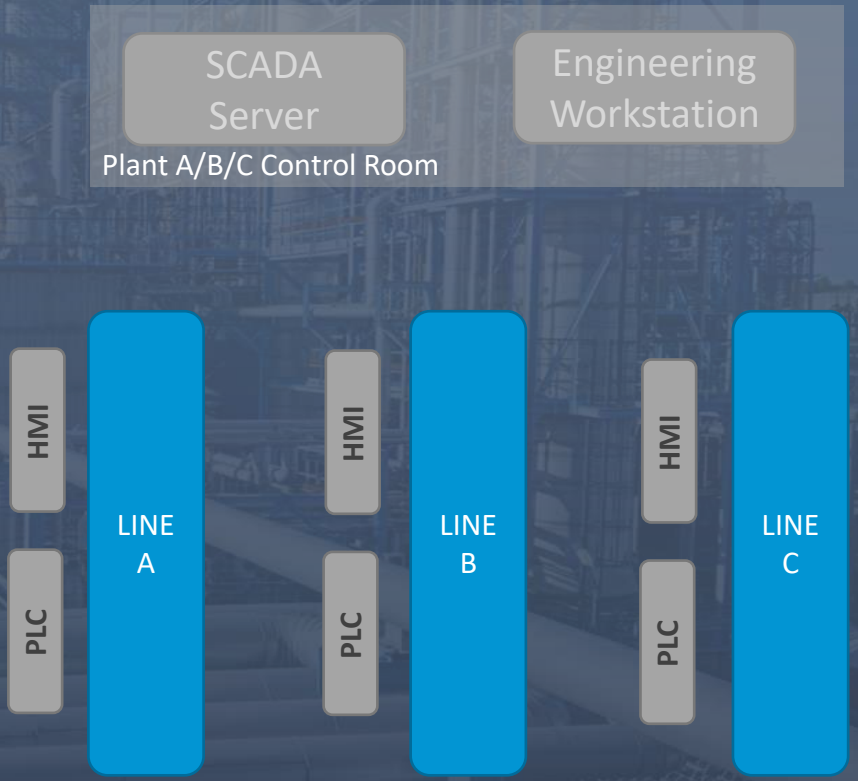
Level 4: Enterprise Systems

General IT Systems (Servers, Workstations)



Level 0: Process

Instruments, Sensors and Actuators



Purdue Model – Rabbit Hole's - RIO

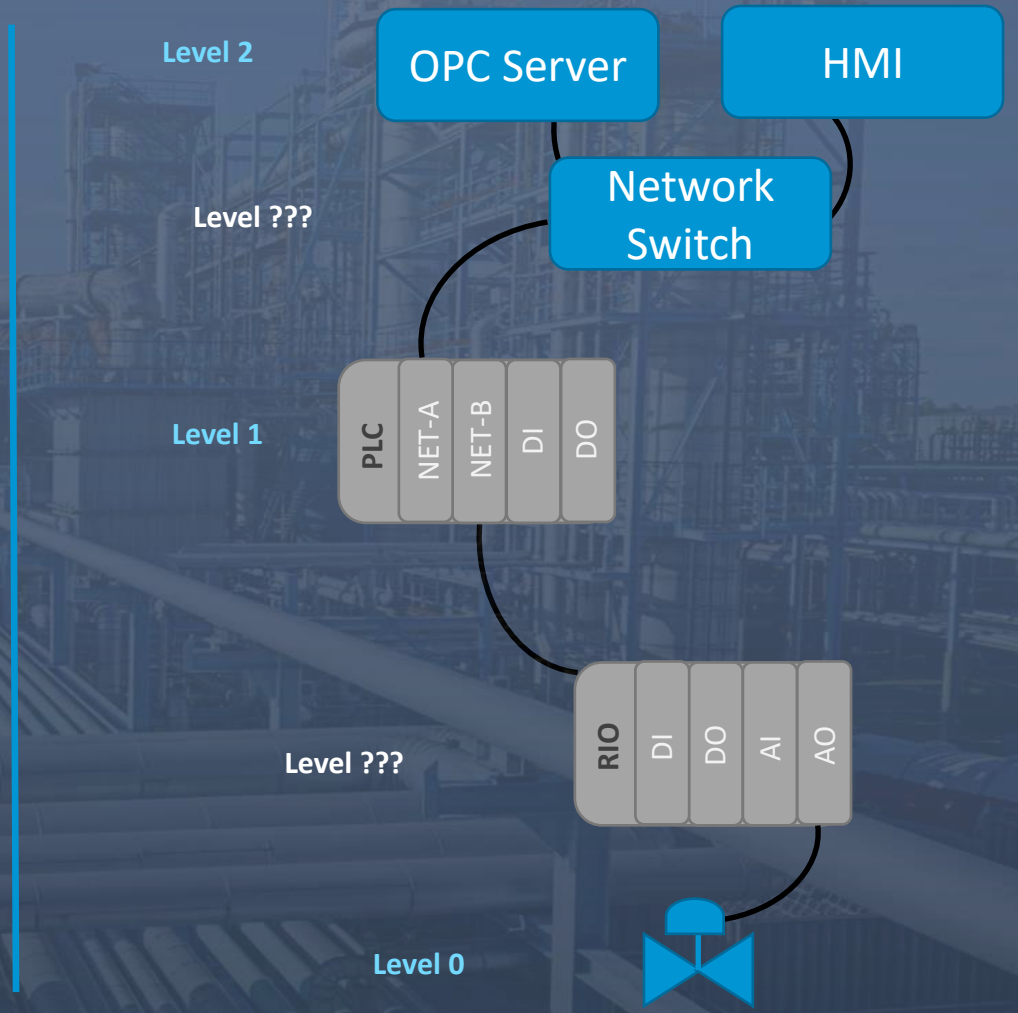
Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

Level 3: Operations Management
Historians, Domain Controllers, Jump Hosts, File Servers

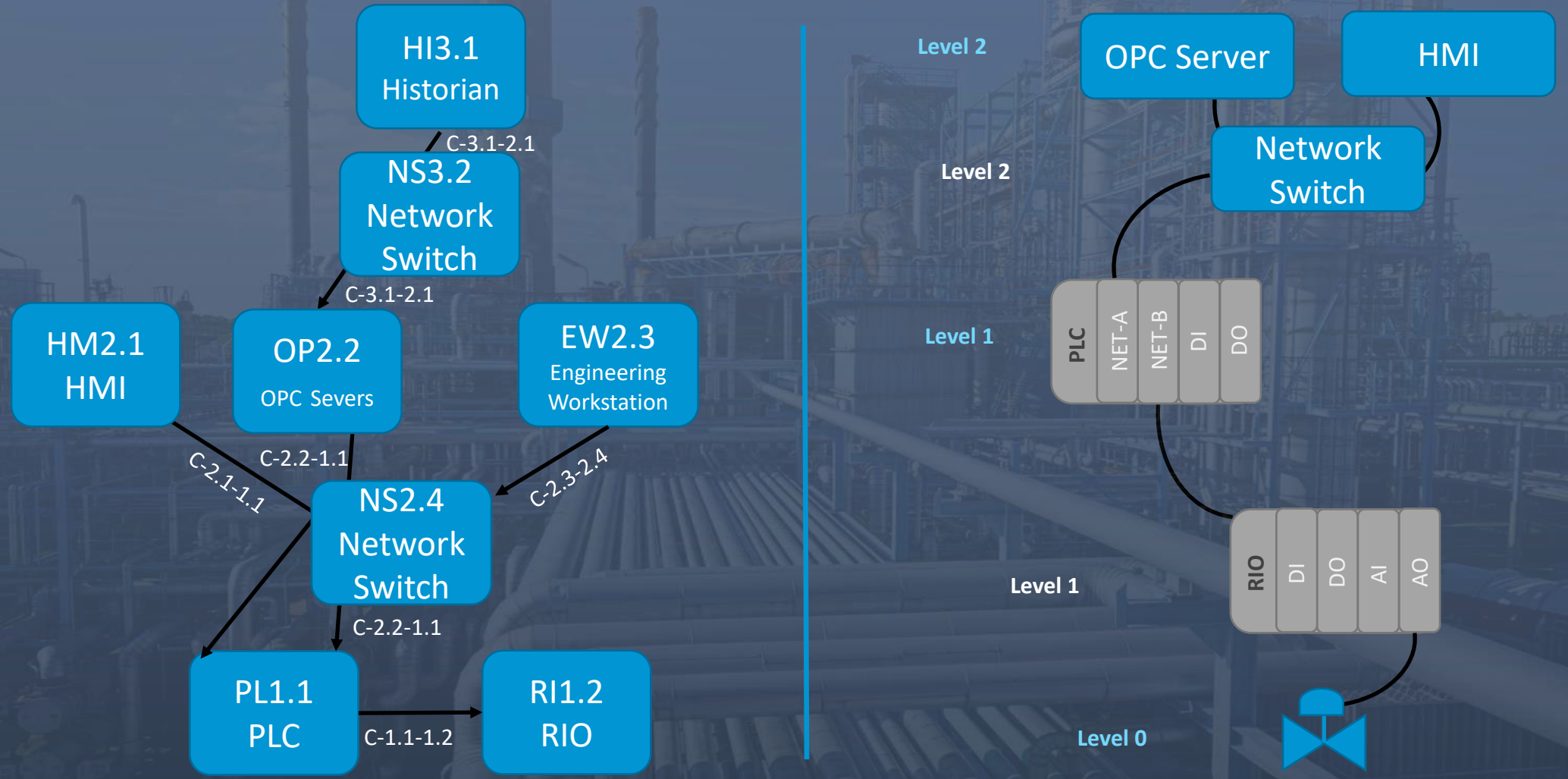
Level 2: Supervisory Control
Local Visulisation

Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's and potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators



Purdue Model – Rabbit Hole's - RIO



Purdue Model – Rabbit Hole's – RTU's

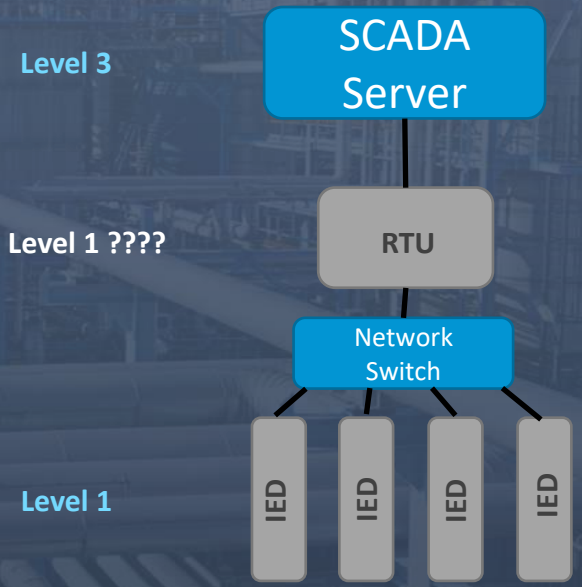
Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

Level 3: Operations Management
Historians, Domain Controllers, Jump Hosts, File Servers

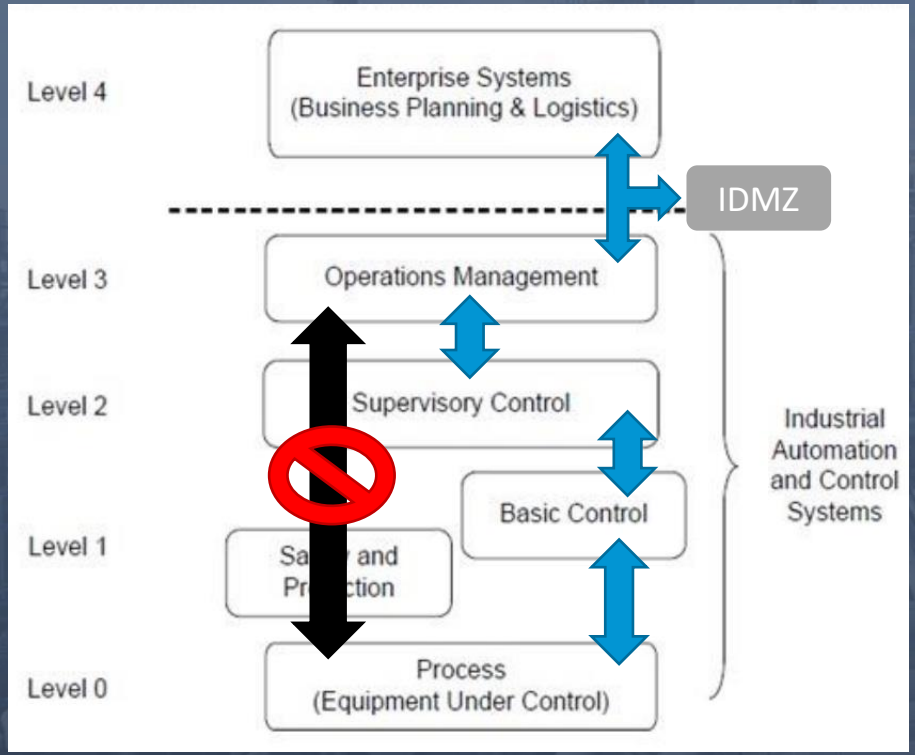
Level 2: Supervisory Control
Local Visulisation

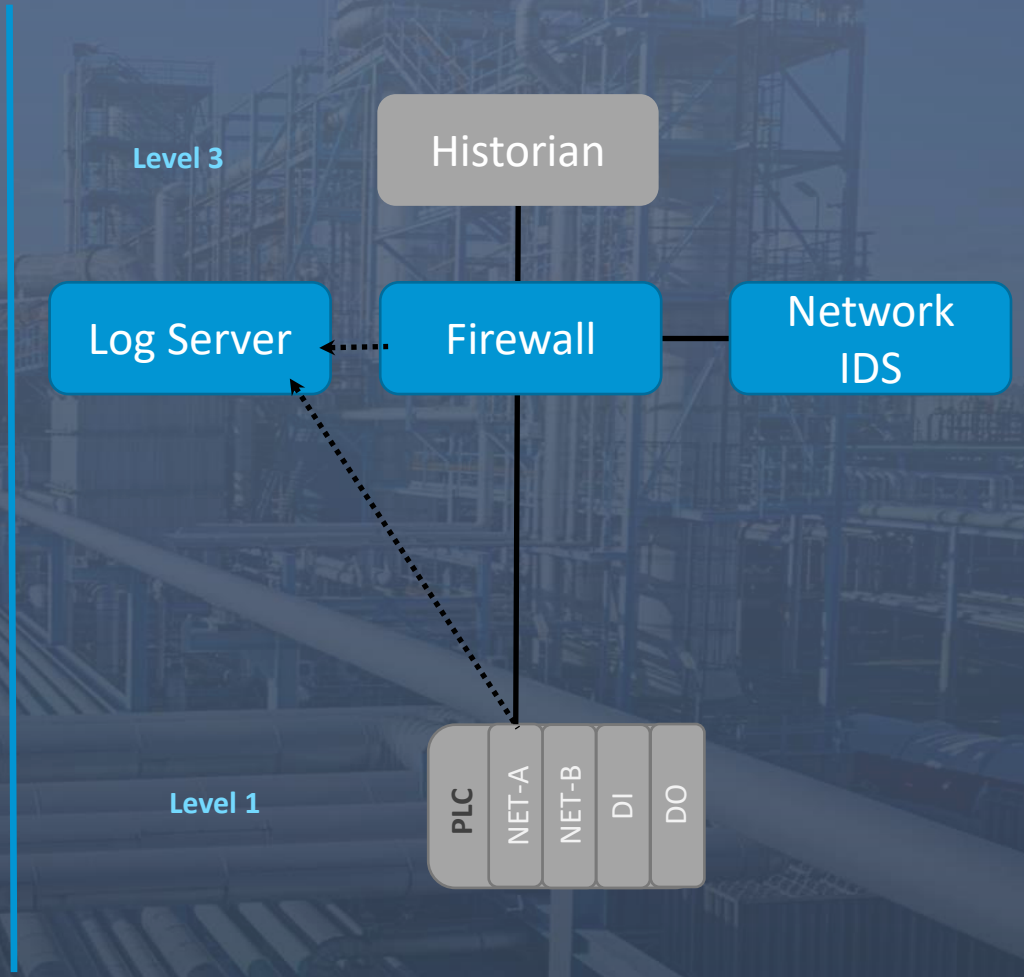
Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's and potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators



Purdue Model – Rabbit Hole's – Level Termination





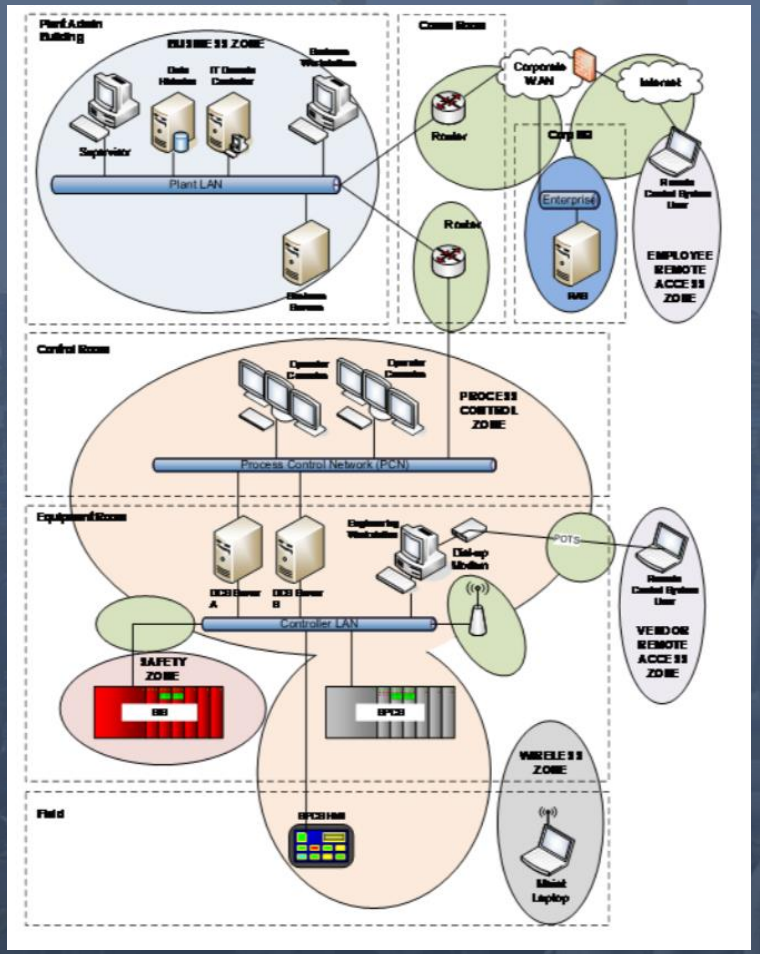
Purdue Model – Rabbit Hole's – Chasing Perfect

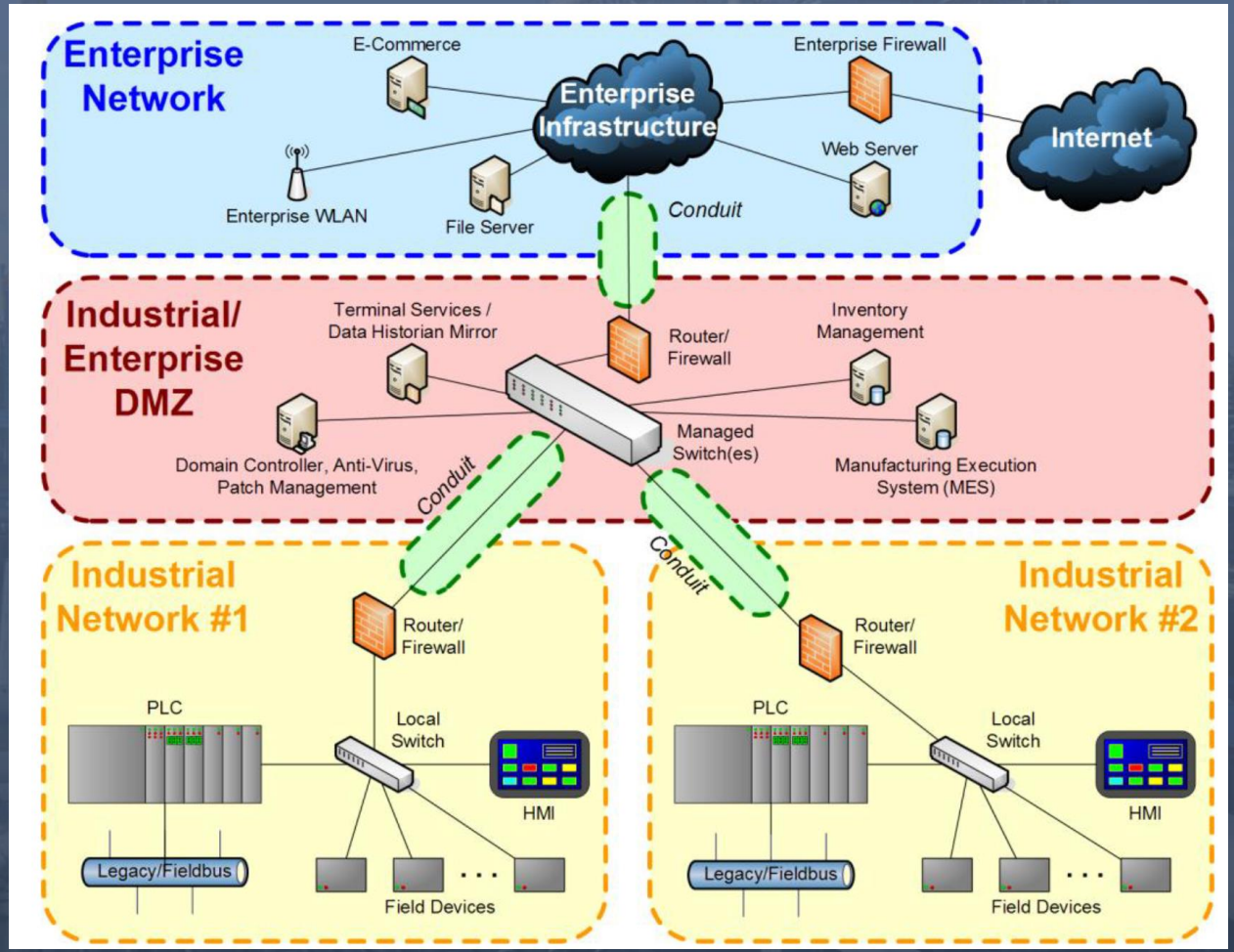
You will get it wrong

Remember I said I would lead you astray

When it came to Zones and Conduits ?

Purdue Model – Rabbit Hole's – Chasing Perfect





Purdue Model

Alright lets do this …. One last time, back… to the basics….

Source: Some random google image search of spiderman into the spider verse

Purdue Model – Use Cases

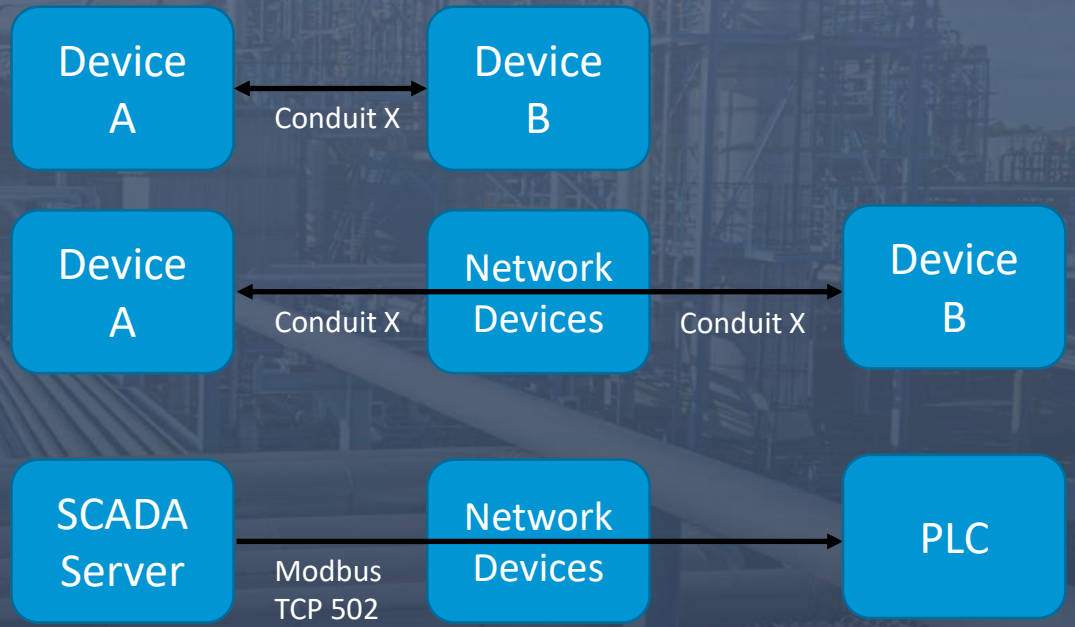
Break it down to simple steps

Prime Questions:

- How do they connect (protocols and physical)
- What is their function? To assign levels
- How do we restore their config, should the worse happen
- How do we monitoring them for abnormal behaviour

Once Assessed:

- Add Zone and Conduit labels as required.



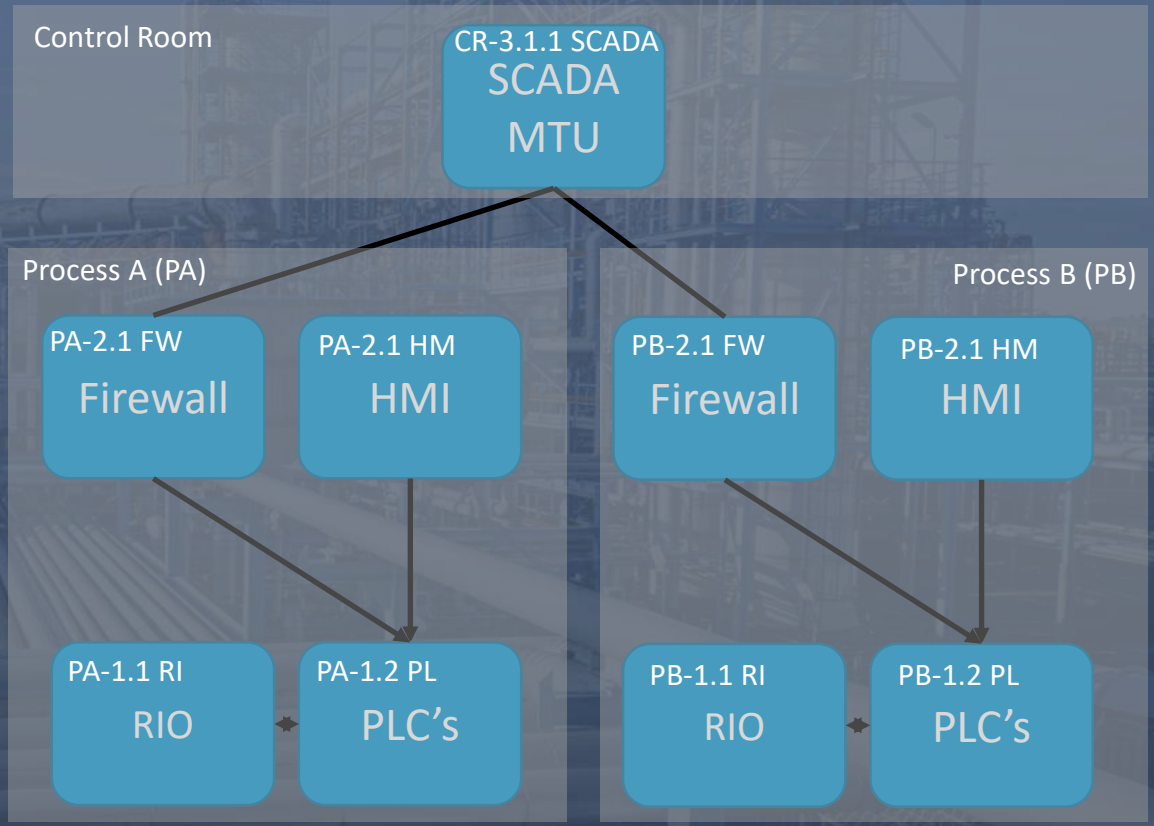
Purdue Model – Use Cases

Break it down to simple steps

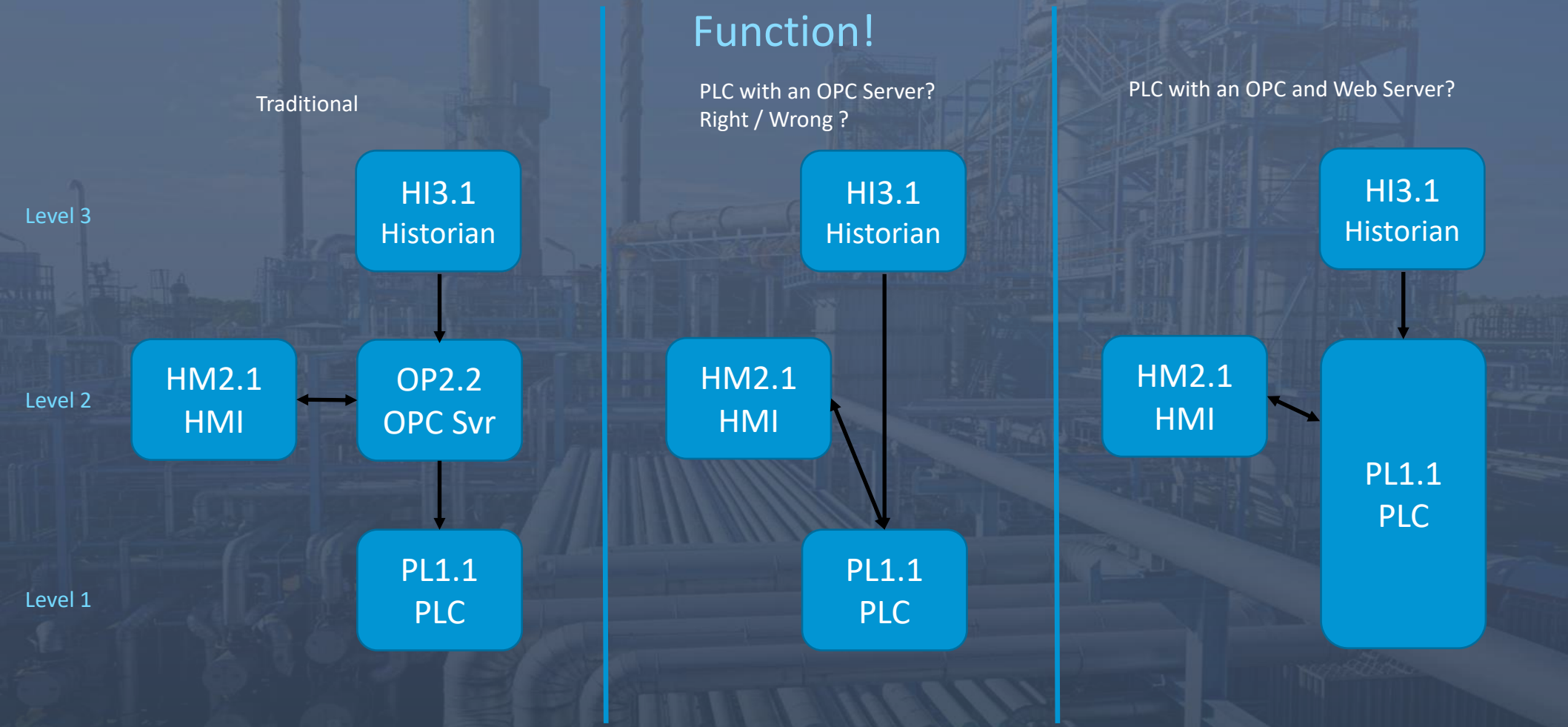
Zone's and Sub Zone's

- Zone's are simple, group common assets together into a security zone, this can be done plant by plant or process by process

- Sub-Zone's are not part of IEC-62443, however identifying exact communication between asset groups can be key after an incident.
- You've probably had to identify that information anyways to get just the Zone categorised.



Purdue Model – Use Cases



Purdue Model – Use Cases

Is the Purdue model dead?

IEC 62443 Purdue Model – based on function

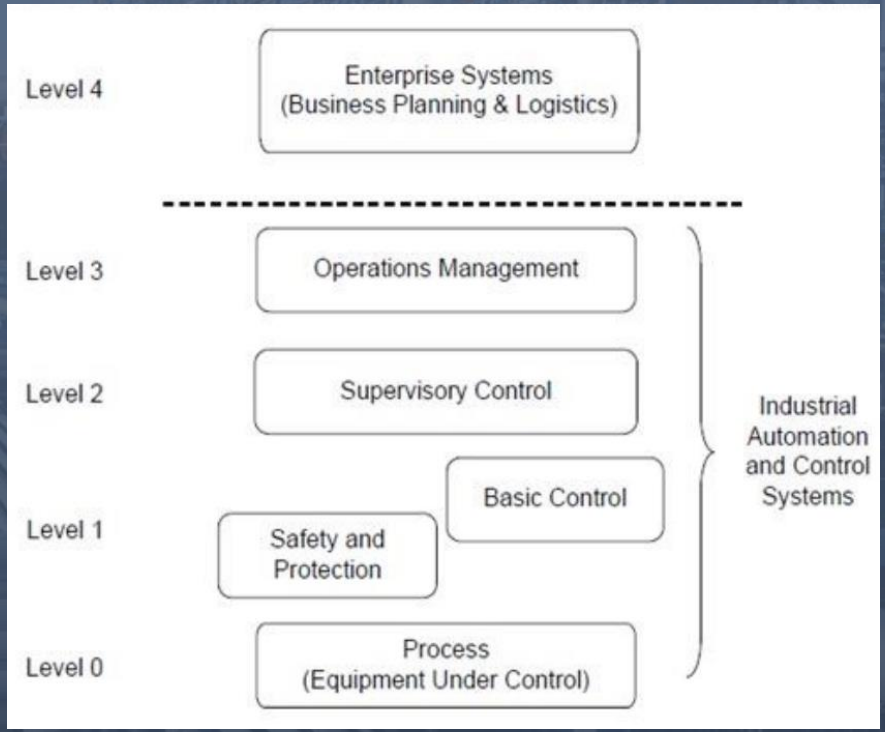
Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

Level 3: Operations Management
Historians, Domain Controllers, Jump Hosts, File Servers

Level 2: Supervisory Control
Local Visulisation

Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators



Purdue Model – Use Cases

IoT or IIoT Connected to the Cloud (SCADA)

This tiny site contains three pumps, two level transmitters, a Micro PLC with IIoT Capabilities has been selected. We will now classify assets and zone it

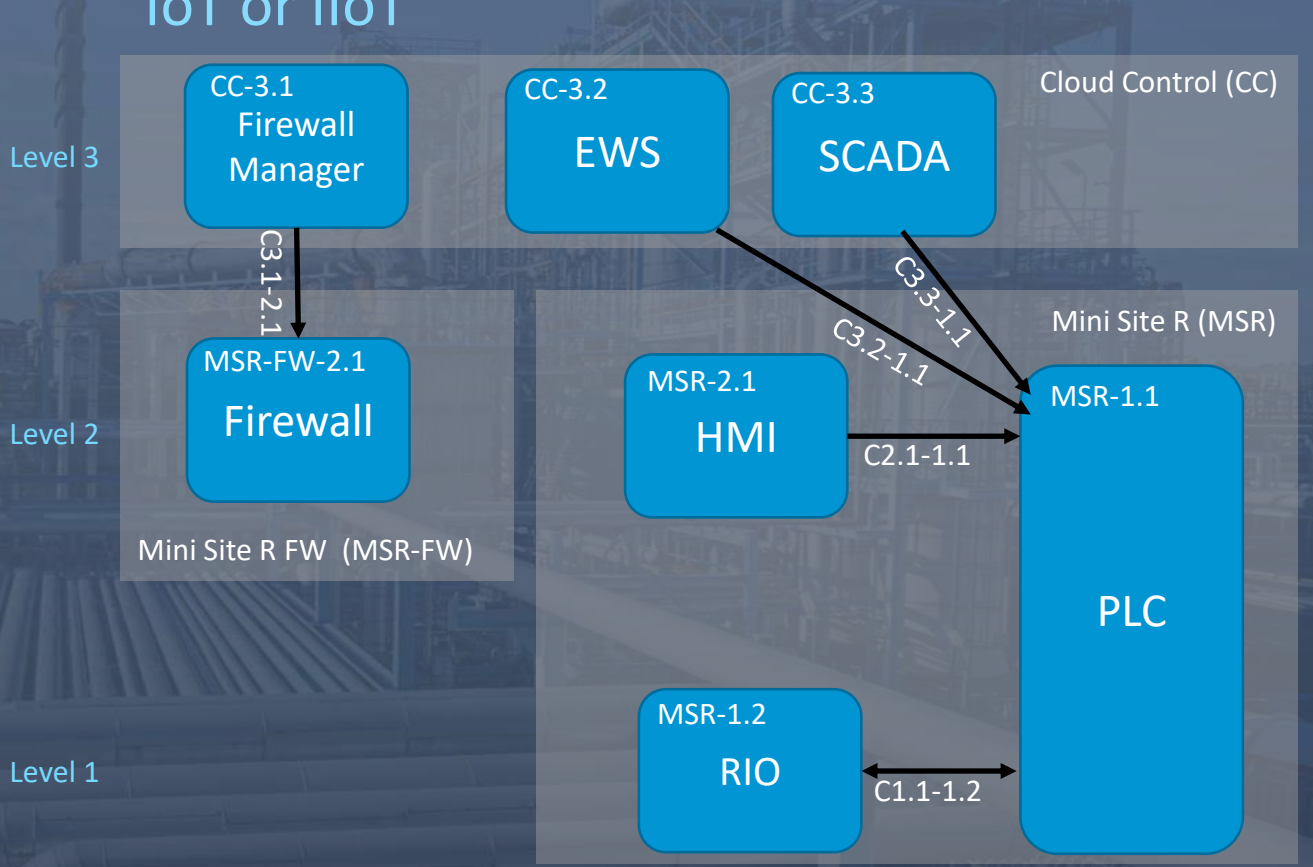
Prime Questions:

How do they connect (protocols and physical)

What is their function? (assign levels)

How do we restore their config, should the worse happen

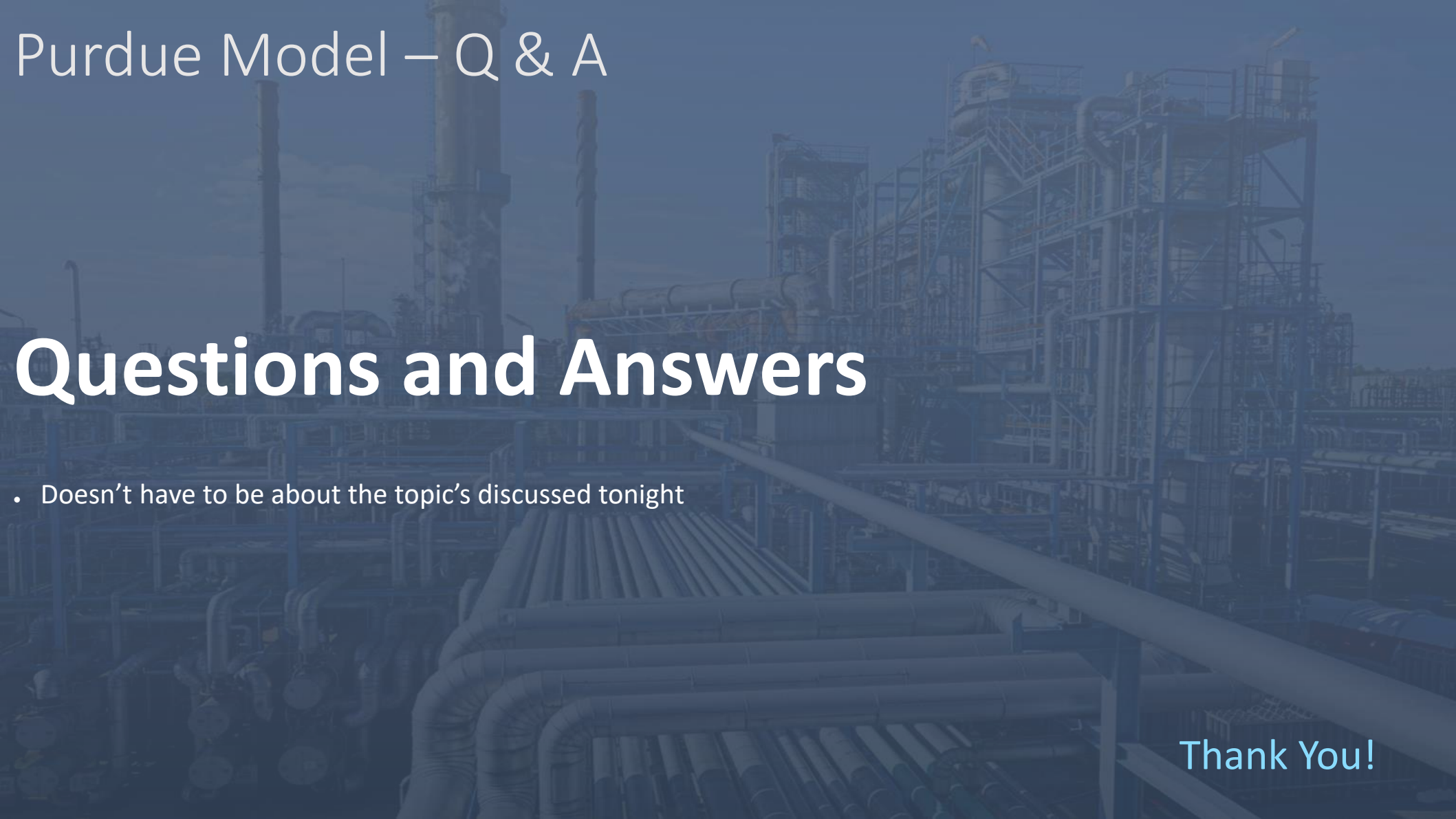
How do we monitoring them for abnormal behaviour



Purdue Model – Key Take Away's

- Keep it simple, break it down to the basics, identify devices and how they communicate.
- Zone items accordingly (Sub-Zoning is advanced and may not be needed)
- When confused what level or asset type , look at the function, What is it doing? Don't make it complicated.
- Levels, Zone's and Conduits are there to help you identify risk and implement controls/counter measures

Purdue Model – Q & A



Questions and Answers

- Doesn’t have to be about the topic’s discussed tonight

Thank You!