Security Lancaster | Lancaster University

Pains, Gains and PLCs

Ben Green

Anhtuan Le

Rob Antrobus

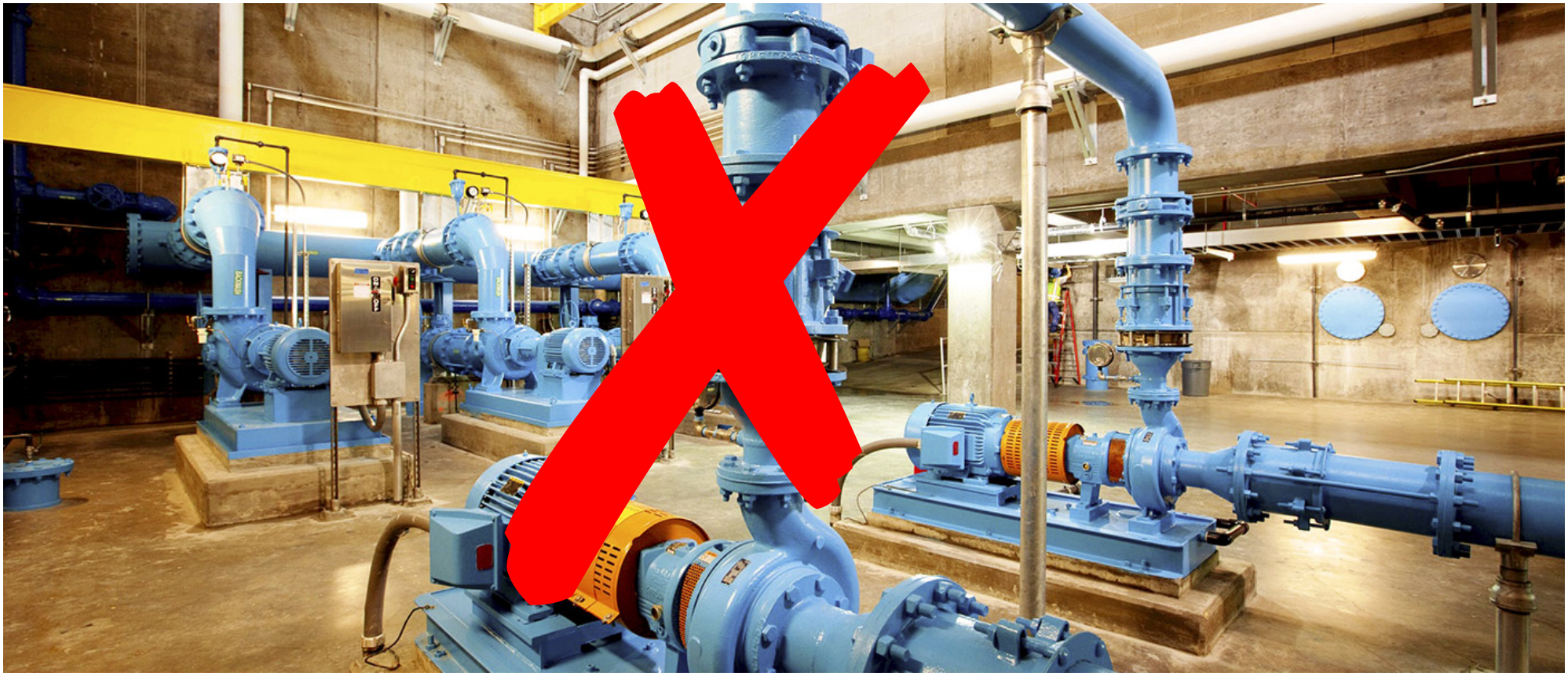
Utz Roedig

David Hutchison

Awais Rashid

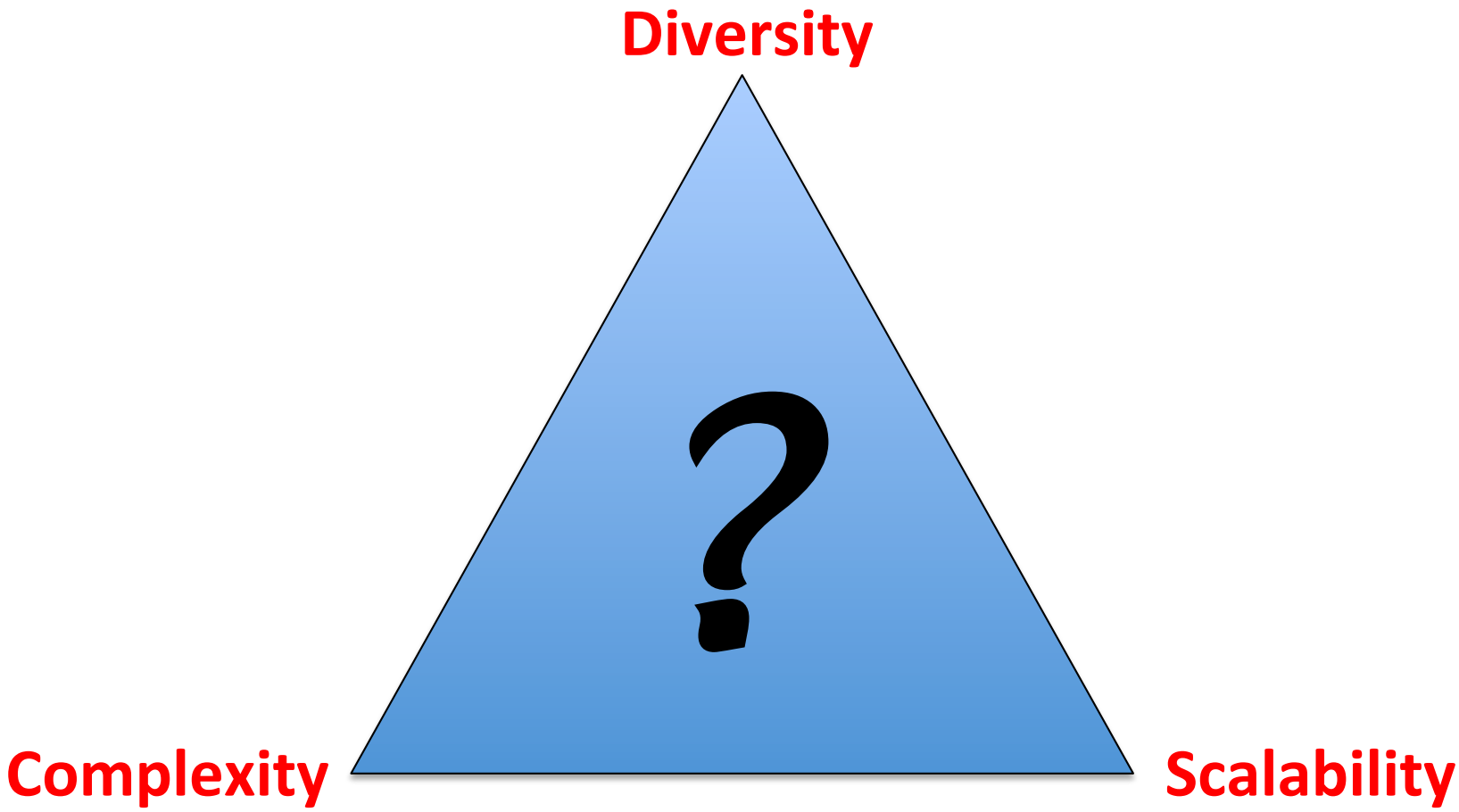
Ten Lessons from Building an Industrial Control Systems Testbed for Security Research

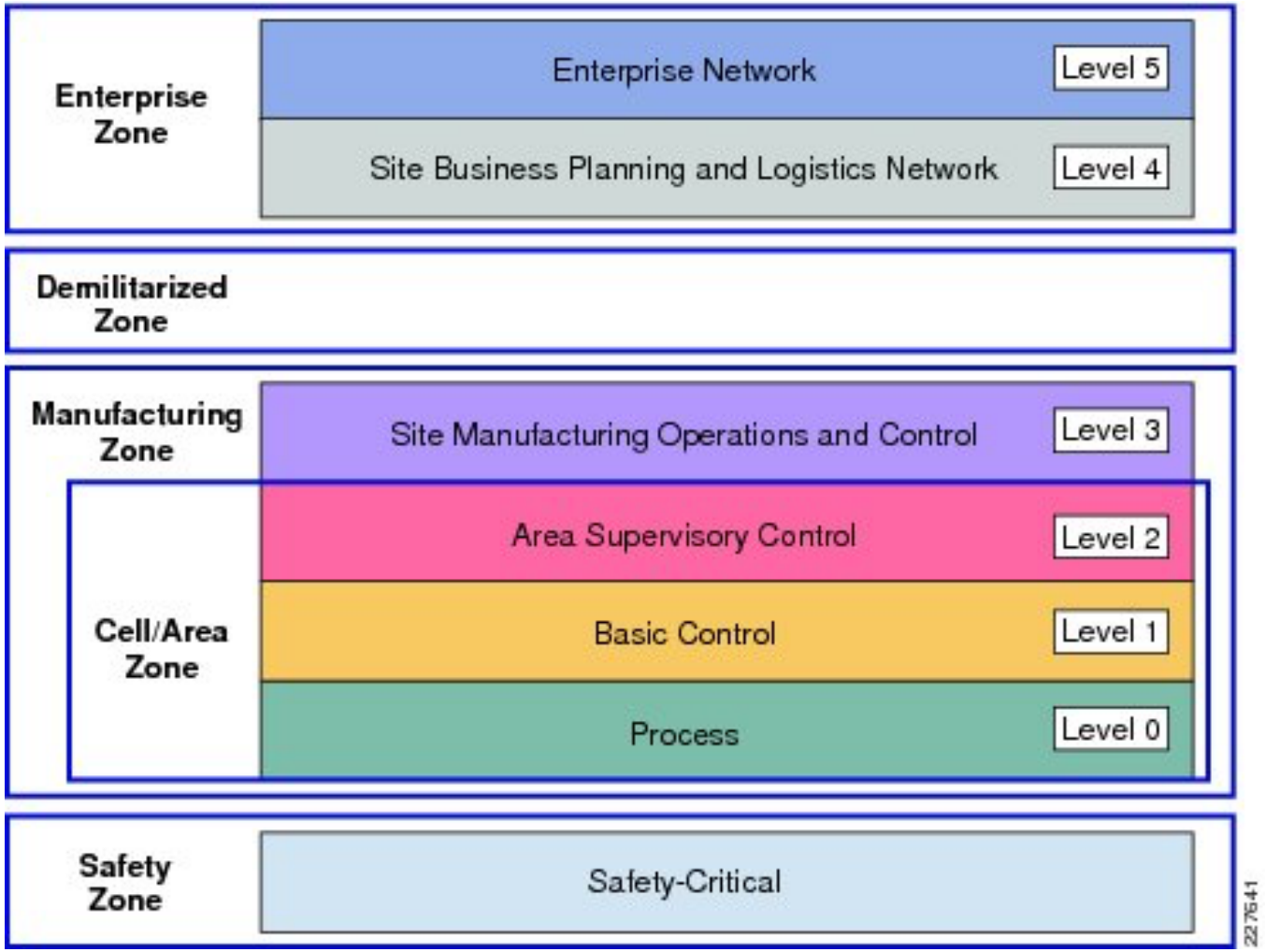

Ivano-Frankivsk

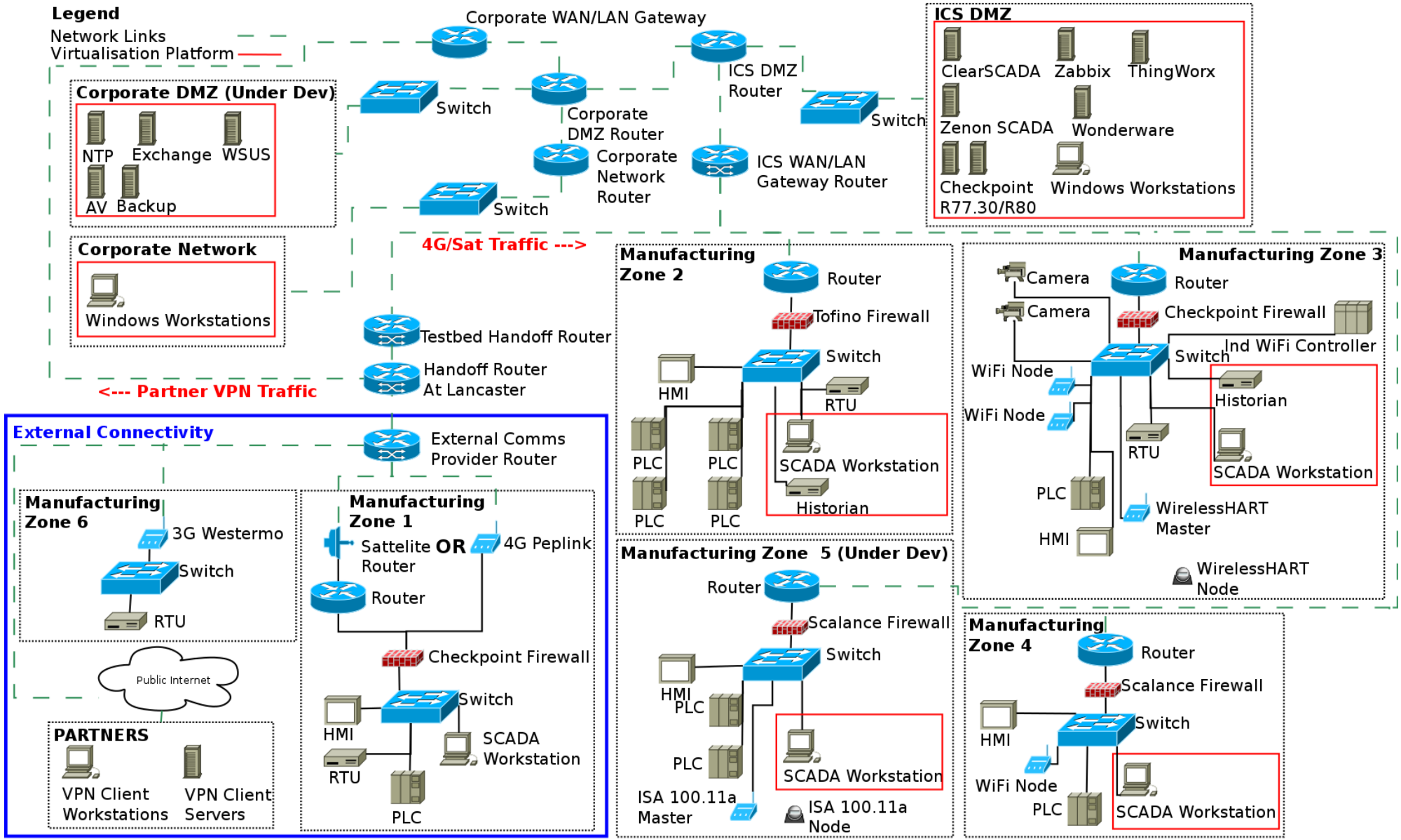


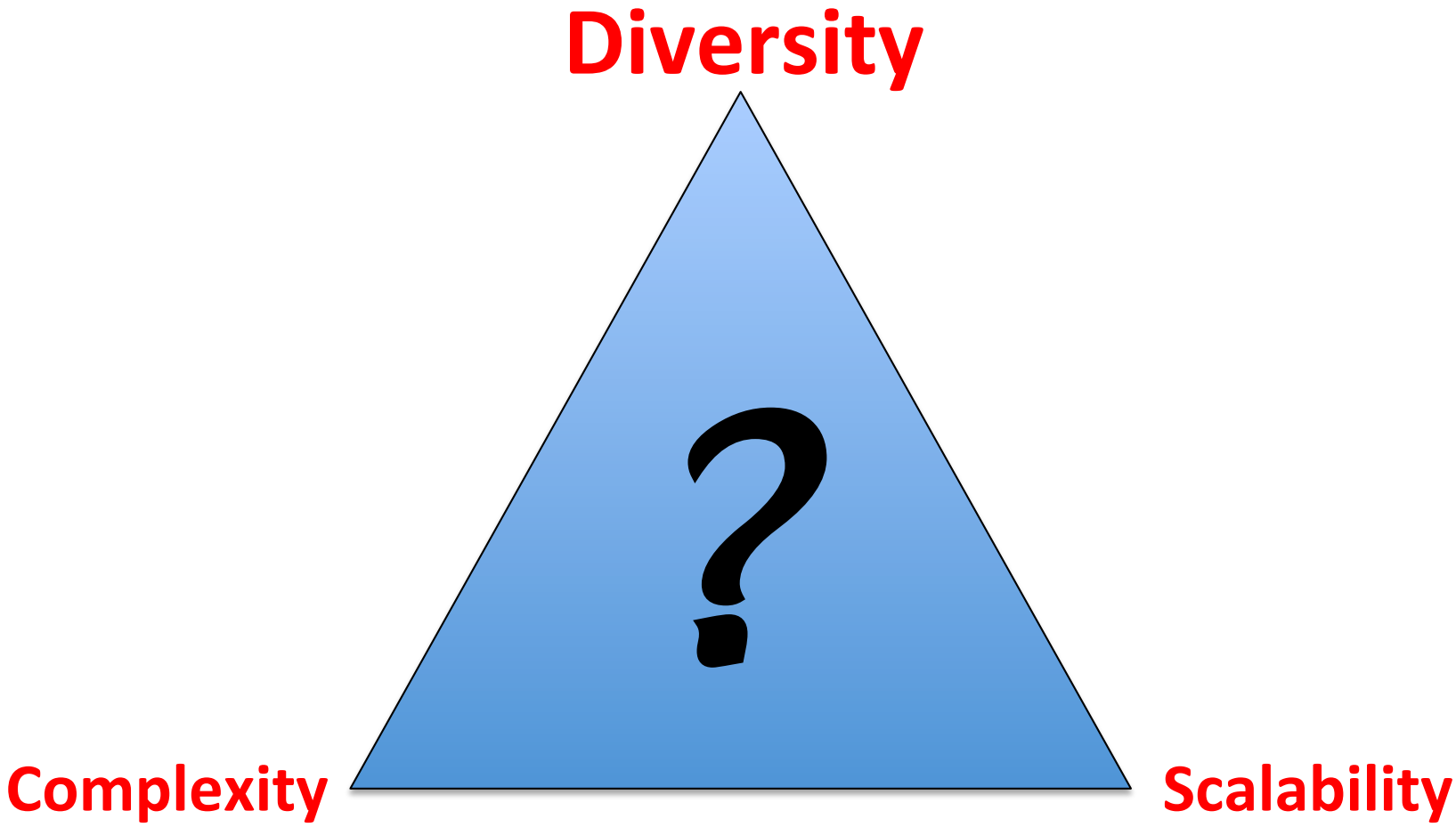

ecplc.com
Digester - Flows

Testbeds

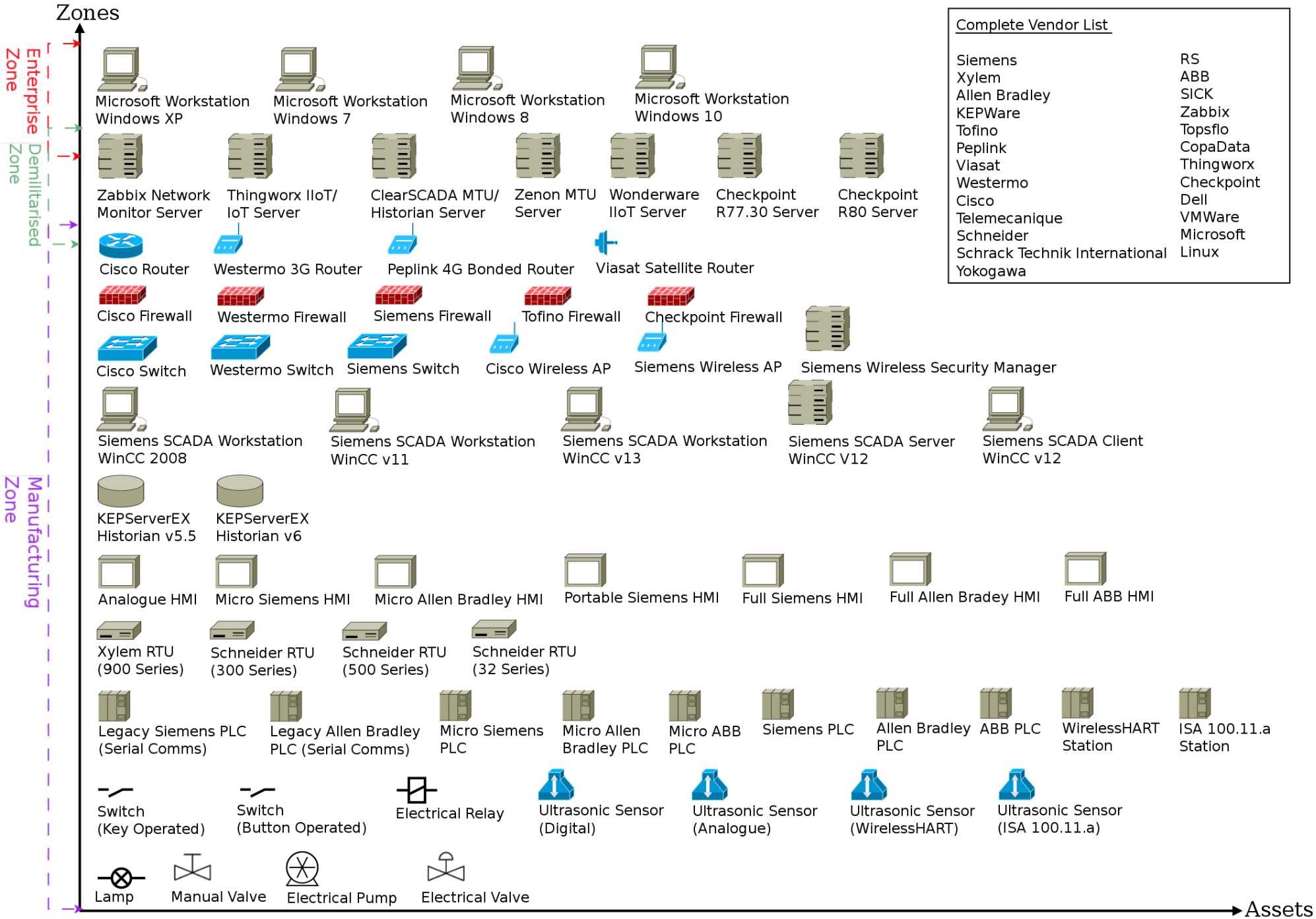

Diversity
?
Complexity
Scalability


Enterprise Zone
Enterprise Network
Level 5
Site Business Planning and Logistics Network
Level 4
Demilitarized Zone
Manufacturing Zone
Site Manufacturing Operations and Control
Level 3
Cell/Area Zone
Area Supervisory Control
Level 2
Basic Control
Level 1
Process
Level 0
Safety Zone
Safety-Critical
227641

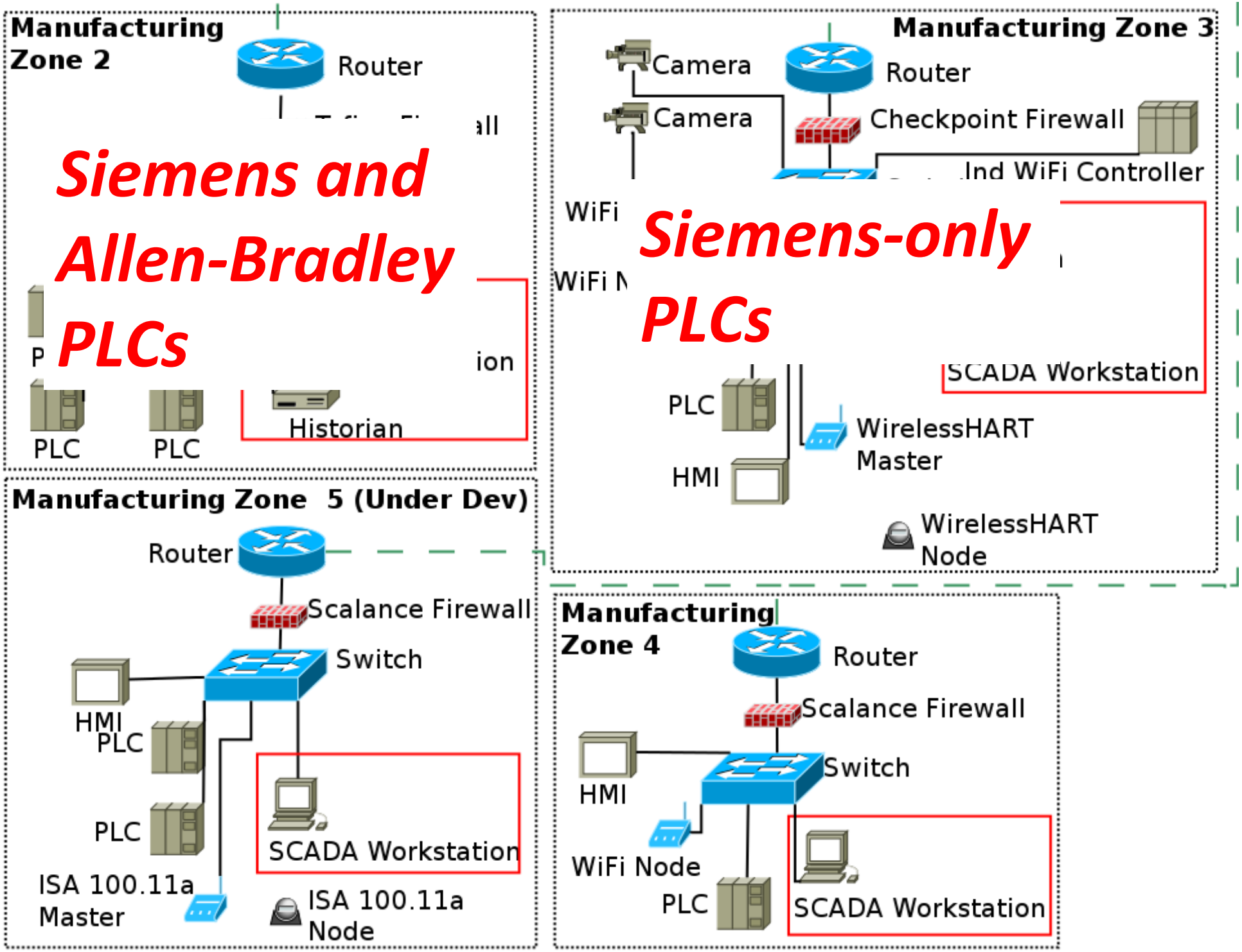

Legend
Network Links
Virtualisation Platform
Corporate WAN/LAN Gateway
ICS DMZ
ClearSCADA
Zabbix
ThingWorx
Zenon SCADA
Wonderware
Checkpoint R77.30/R80
Windows Workstations
Corporate DMZ (Under Dev)
NTP
Exchange
WSUS
AV
Backup
Switch
Corporate DMZ Router
ICS DMZ Router
Switch
Corporate Network Router
ICS WAN/LAN Gateway Router
Switch
4G/Sat Traffic --->
Corporate Network
Windows Workstations
Testbed Handoff Router
Handoff Router At Lancaster
<--- Partner VPN Traffic
Manufacturing Zone 2
Router
Tofino Firewall
Switch
HMI
RTU
PLC
PLC
SCADA Workstation
PLC
PLC
Historian
Manufacturing Zone 3
Camera
Router
Camera
Checkpoint Firewall
Ind WiFi Controller
Switch
WiFi Node
Historian
WiFi Node
RTU
SCADA Workstation
PLC
WirelessHART Master
HMI
WirelessHART Node
External Connectivity
External Comms Provider Router
Manufacturing Zone 6
3G Westermo
Switch
RTU
Public Internet
PARTNERS
VPN Client Workstations
VPN Client Servers
Manufacturing Zone 1
Sattelite OR 4G Peplink Router
Router
Checkpoint Firewall
Switch
HMI
SCADA Workstation
RTU
PLC
Manufacturing Zone 5 (Under Dev)
Router
Scalance Firewall
Switch
HMI
PLC
PLC
SCADA Workstation
ISA 100.11a Master
ISA 100.11a Node
Manufacturing Zone 4
Router
Scalance Firewall
Switch
HMI
WiFi Node
PLC
SCADA Workstation


Diversity
?
Complexity
Scalability

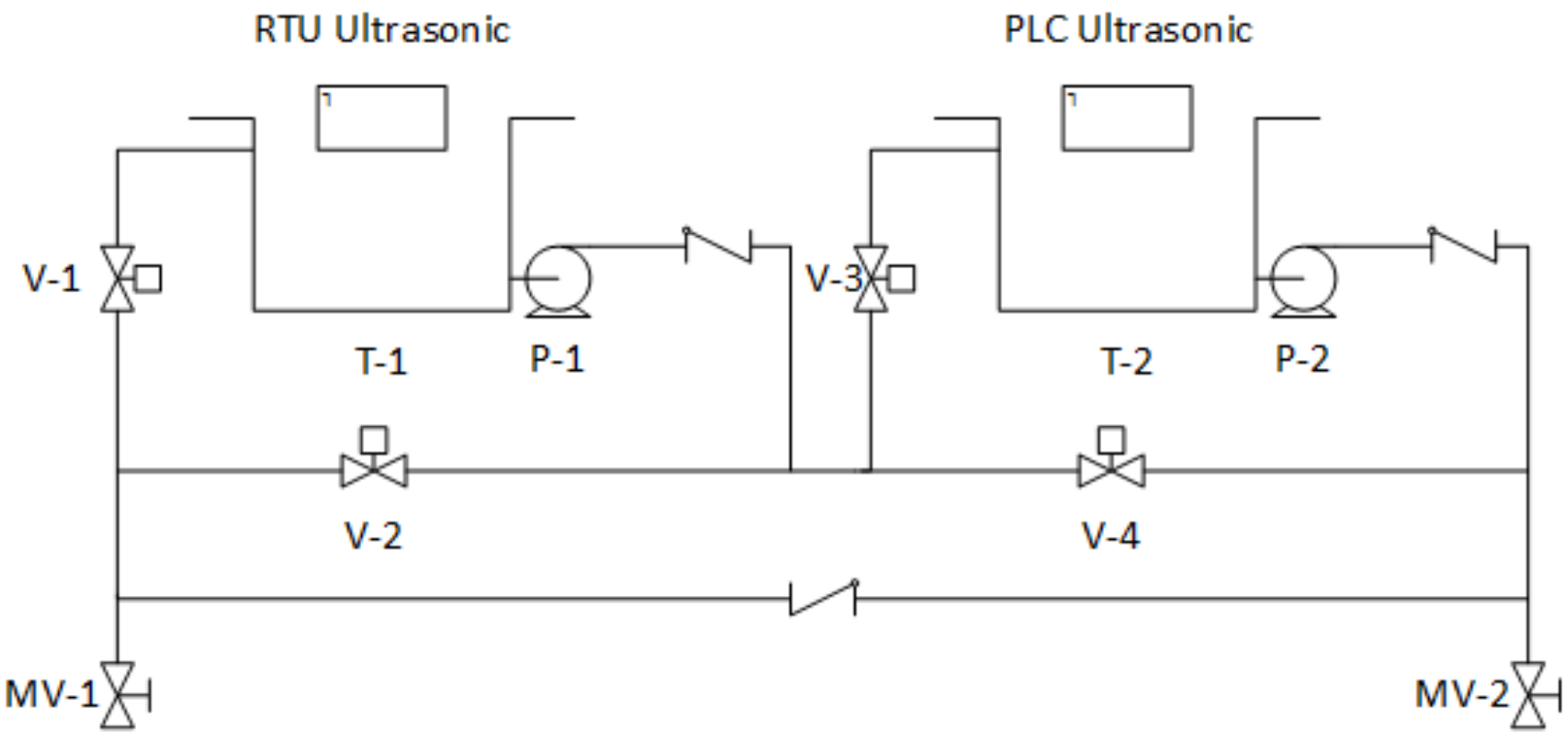
Lesson 1: Device and technology selections should be market-driven

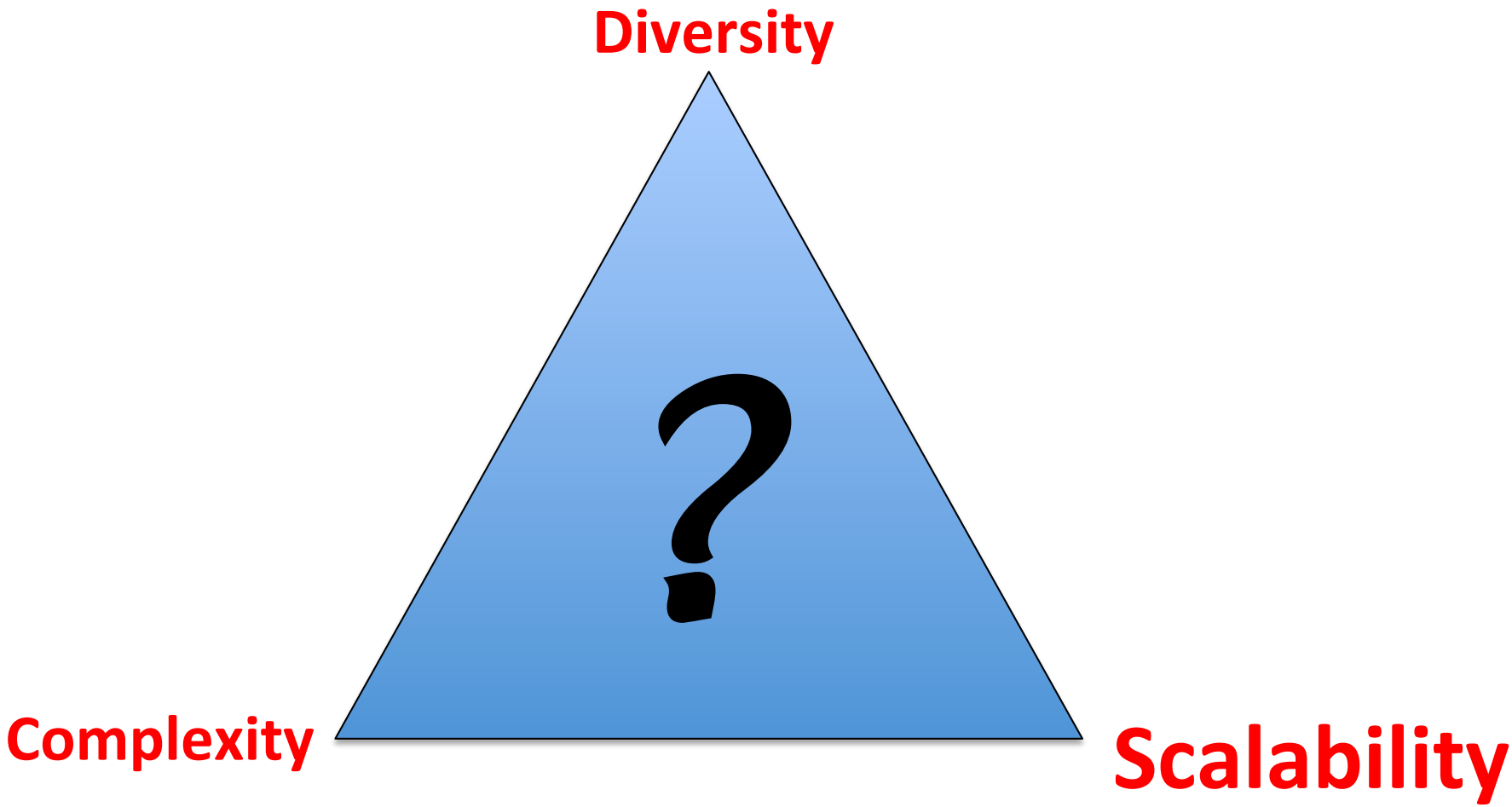

Zones
Enterprise Zone
Demilitarised Zone
Manufacturing Zone
Microsoft Workstation Windows XP
Microsoft Workstation Windows 7
Microsoft Workstation Windows 8
Microsoft Workstation Windows 10
Zabbix Network Monitor Server
Thingworx IIoT/ IoT Server
ClearSCADA MTU/ Historian Server
Zenon MTU Server
Wonderware IIoT Server
Checkpoint R77.30 Server
Checkpoint R80 Server
Cisco Router
Westermo 3G Router
Peplink 4G Bonded Router
Viasat Satellite Router
Cisco Firewall
Westermo Firewall
Siemens Firewall
Tofino Firewall
Checkpoint Firewall
Cisco Switch
Westermo Switch
Siemens Switch
Cisco Wireless AP
Siemens Wireless AP
Siemens Wireless Security Manager
Siemens SCADA Workstation WinCC 2008
Siemens SCADA Workstation WinCC v11
Siemens SCADA Workstation WinCC v13
Siemens SCADA Server WinCC V12
Siemens SCADA Client WinCC v12
KEPServerEX Historian v5.5
KEPServerEX Historian v6
Analogue HMI
Micro Siemens HMI
Micro Allen Bradley HMI
Portable Siemens HMI
Full Siemens HMI
Full Allen Bradey HMI
Full ABB HMI
Xylem RTU (900 Series)
Schneider RTU (300 Series)
Schneider RTU (500 Series)
Schneider RTU (32 Series)
Legacy Siemens PLC (Serial Comms)
Legacy Allen Bradley PLC (Serial Comms)
Micro Siemens PLC
Micro Allen Bradley PLC
Micro ABB PLC
Siemens PLC
Allen Bradley PLC
ABB PLC
WirelessHART Station
ISA 100.11.a Station
Switch (Key Operated)
Switch (Button Operated)
Electrical Relay
Ultrasonic Sensor (Digital)
Ultrasonic Sensor (Analogue)
Ultrasonic Sensor (WirelessHART)
Ultrasonic Sensor (ISA 100.11.a)
Lamp
Manual Valve
Electrical Pump
Electrical Valve
Assets
Complete Vendor List
Siemens
Xylem
Allen Bradley
KEPWare
Tofino
Peplink
Viasat
Westermo
Cisco
Telemecanique
Schneider
Schrack Technik International
Yokogawa
RS
ABB
SICK
Zabbix
Topsflo
CopaData
Thingworx
Checkpoint
Dell
VMWare
Microsoft
Linux

Lesson 2: Homogeneity and heterogeneity in field sites


Manufacturing Zone 2
Router
Siemens and Allen-Bradley PLCs
PLC
PLC
Historian
Manufacturing Zone 3
Camera
Camera
Router
Checkpoint Firewall
Ind WiFi Controller
WiFi
Siemens-only PLCs
SCADA Workstation
PLC
WirelessHART Master
HMI
WirelessHART Node
Manufacturing Zone 5 (Under Dev)
Router
Scalance Firewall
Switch
HMI
PLC
PLC
SCADA Workstation
ISA 100.11a Master
ISA 100.11a Node
Manufacturing Zone 4
Router
Scalance Firewall
Switch
HMI
WiFi Node
PLC
SCADA Workstation

Lesson 3: Process diversity is not always crucial


RTU Ultrasonic
PLC Ultrasonic
V-1
V-3
T-1
P-1
T-2
P-2
V-2
V-4
MV-1
MV-2


Diversity
?
Complexity
Scalability

Lesson 4: Hardware-in-the-Loop (HIL) is not essential in the Manufacturing Zone

Lack of exact mathematical models for
representing the behaviours of sensors and actuators
factors impacting simulation accuracy such as noise

Process diversity not a primary concern
hot-swap capability allows for a level of scalability with sensors and actuators, moving them between devices as and when required

Lesson 5: Simulations in the Manufacturing Zone are not favoured

Software does not provide simulations of many essential types of devices

from different vendors

OR

same vendor but distinctive versions

Accuracy and reliability issues in mimicking real-life operations

Despite cost, physical equipment helps experimental rigour

Lesson 6: Virtualisation and VLANs provide ease of integration and scaling

Provide an easy and cost-effective way

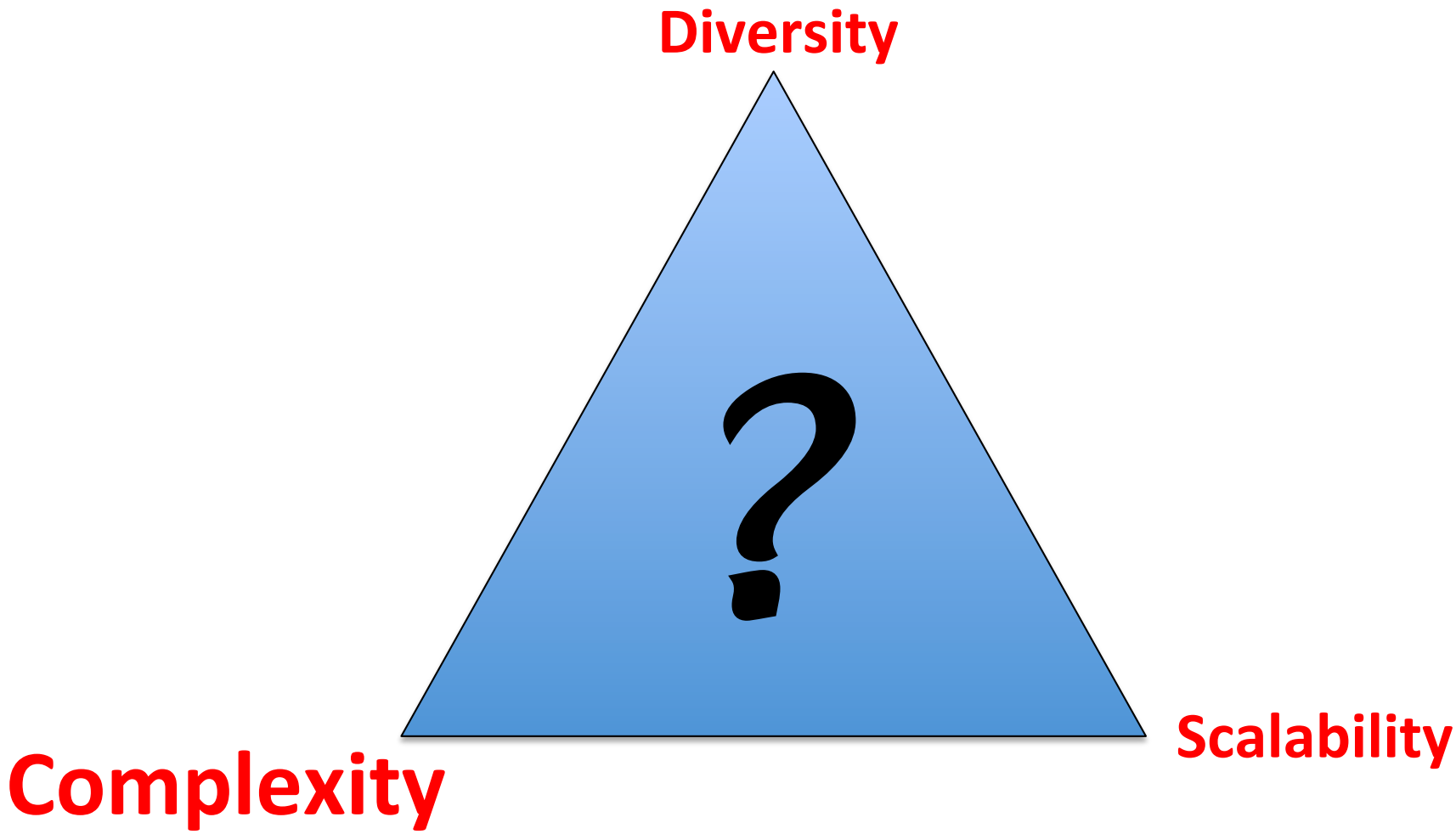
To integrate new systems

OR

Scale up existing instances

Reduces technical knowledge required during experimental set up

Clean backups **of known good systems should damage be caused during experimentation**


Diversity
?
Complexity
Scalability

Lesson 7: Employ a Management Network

Reduces the need for pre-requisite knowledge

Relies on all relevant research tools being in place

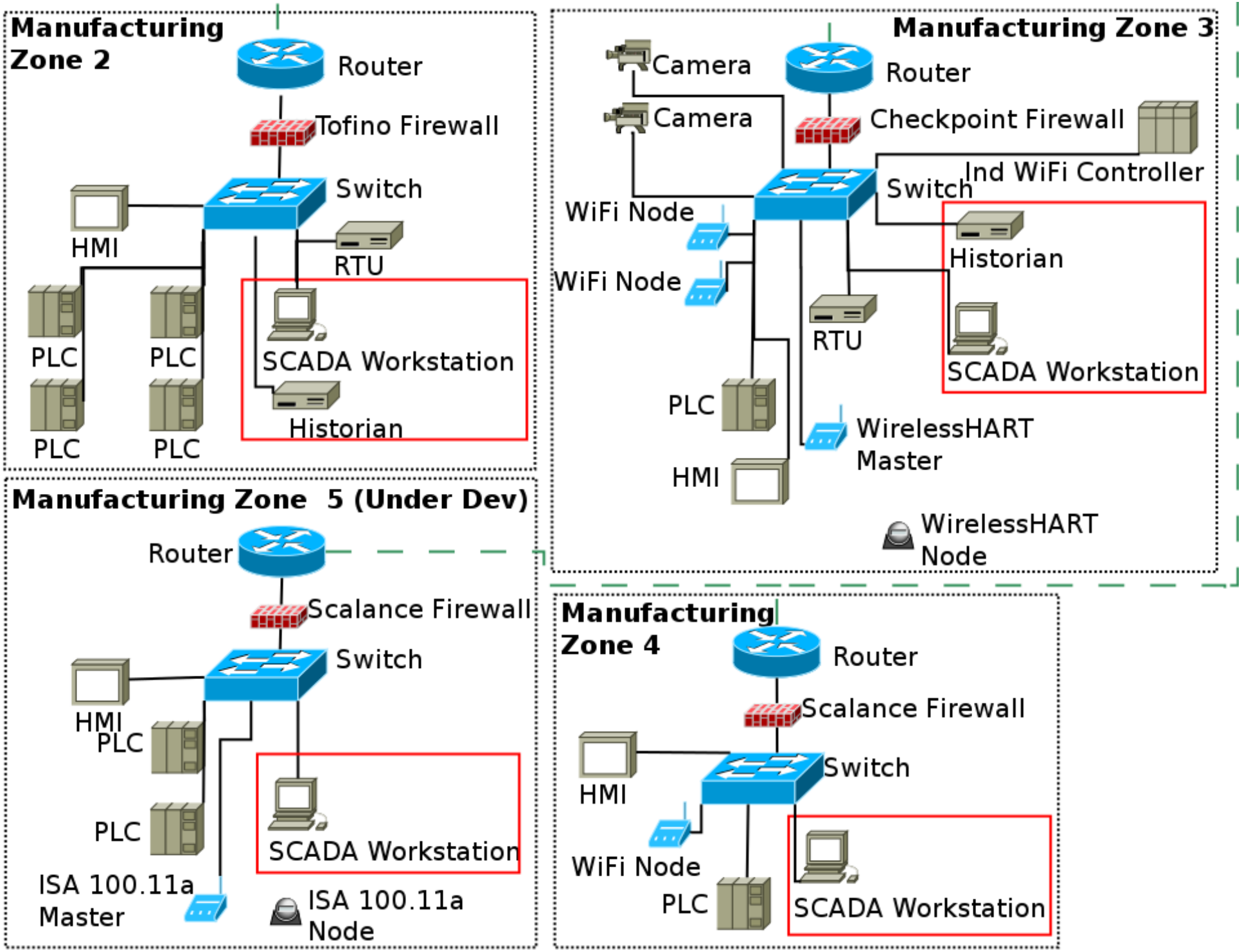
Currently being addressed

Requires appropriate data capture points

Capture traffic from all zones into a centralised location

Currently being addressed

Lesson 8: Setup Multiple Manufacturing Zones


Manufacturing Zone 2
Router
Tofino Firewall
Switch
HMI
RTU
PLC
PLC
SCADA Workstation
PLC
PLC
Historian
Manufacturing Zone 3
Camera
Router
Camera
Checkpoint Firewall
Ind WiFi Controller
Switch
WiFi Node
Historian
WiFi Node
RTU
SCADA Workstation
PLC
WirelessHART Master
HMI
WirelessHART Node
Manufacturing Zone 5 (Under Dev)
Router
Scalance Firewall
Switch
HMI
PLC
PLC
SCADA Workstation
ISA 100.11a Master
ISA 100.11a Node
Manufacturing Zone 4
Router
Scalance Firewall
Switch
HMI
WiFi Node
PLC
SCADA Workstation

Lesson 9: Comprehensively document as you build


DOH!

Document

Communication and control processes

Known vulnerabilities in devices and software

Sample attack scenarios

Keeping documentation up-to-date is significant effort!

Lesson 10: Optimise data logging for security purposes

Contributing to open ICS datasets

Collection and distribution of data is limited

Involves a manual and time consuming process

One for the future!

Experimentation using the testbed

- William Jardine, Sylvain Frey, Ben Green, and Awais Rashid. “SENAMI: Selective Non- Invasive Active Monitoring for ICS Intrusion Detection”. In: *Proceedings of the Second ACM Workshop on Cyber-Physical Systems-Security*, Vienna, Austria. ACM, 2016, pp. 23–34.
- Rob Antrobus, Sylvain Frey, Benjamin Green, and Awais Rashid. “SimaticScan: towards a specialised vulnerability scanner for industrial control systems”. In: *Proceedings 4th International Symposium for ICS and SCADA Cyber Security Research*. BCS, June 2016, pp. 11–18.
- Benjamin Green, Marina Krotofil, and David Hutchison. “Achieving ICS resilience and security through granular data flow management”. In *Proc. 2nd ACM Workshop on Cyber-Physical Systems Security & Privacy*, Vienna, Austria pages 93–101. ACM, 2016.
- Jeremy Simon Busby, Benjamin Green, and David Hutchison. “Analysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk”. *Risk Analysis*, 2017.


10 Lessons