Nebras

CyberSecurityExpert

OT Cybersecurity

Fundamentals

Nebras
CyberSecurityExpert

Introduction to Operational Technology CyberSecurity

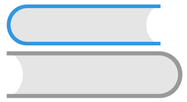
OT Cybersecurity Fundamentals

Contents

IT/OT Gap

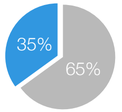
OT Terminology

OT Network



Purdue Reference Model

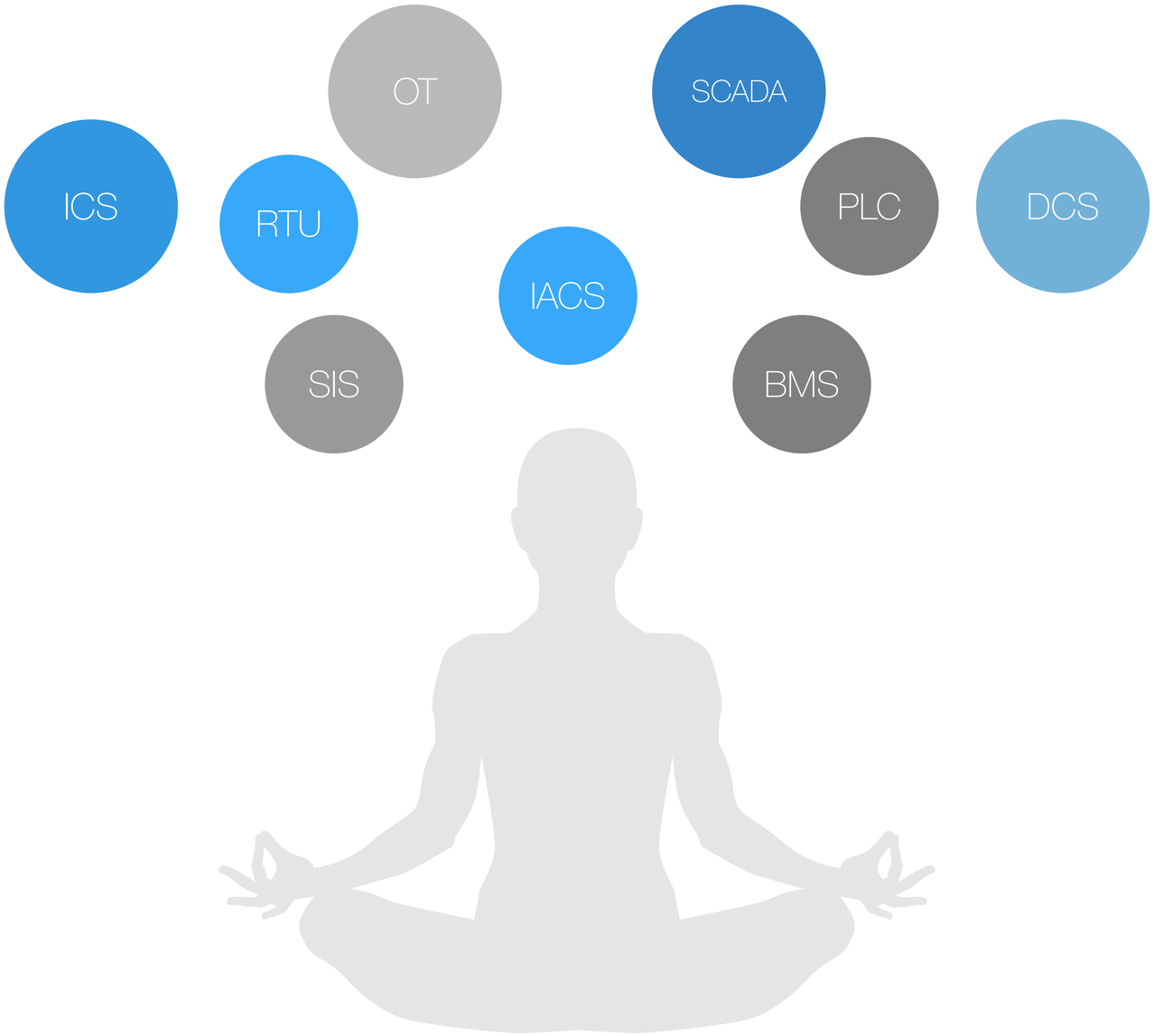
IT within OT



IT vs OT

Nebras
CyberSecurityExpert

OT Terminology



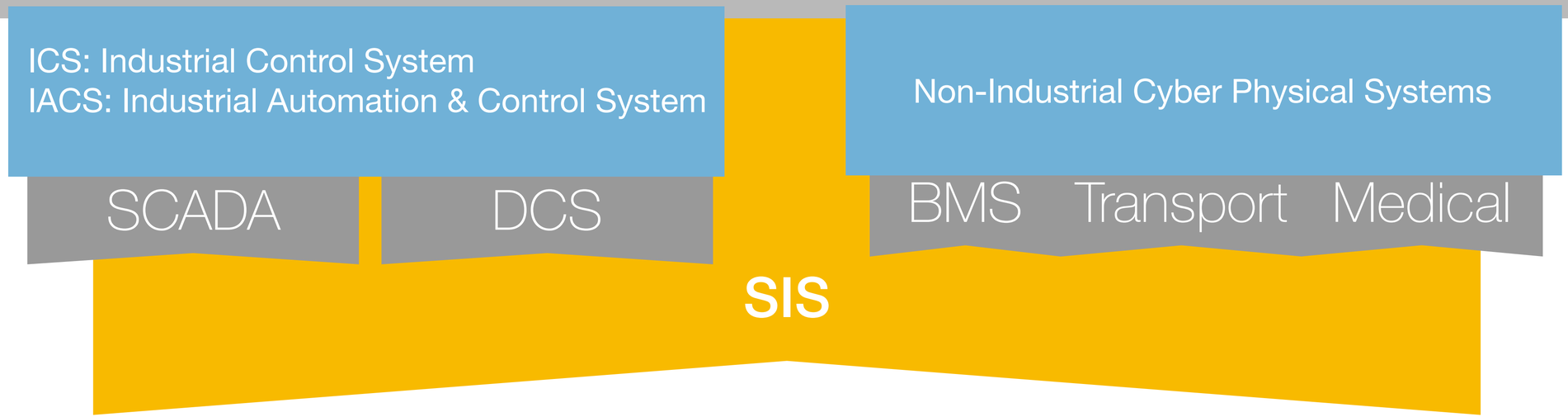
Nebras
CyberSecurityExpert

OT Terminology

Operational Technology OT:

Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

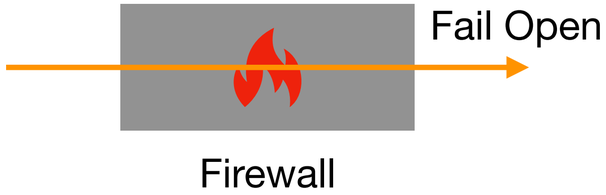
Industrial Control Systems (ICS) and other “cyber physical systems” – but is also used to describe automation systems that aren’t industrial in nature but use similar technology.



Nebras
CyberSecurityExpert

IT / OT Gap

Confidentiality

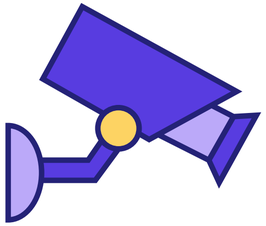


Firewall

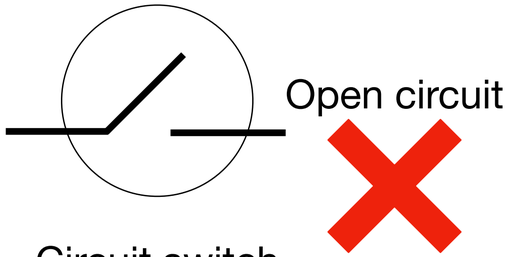
IT

Priority **Different meanings**

OT



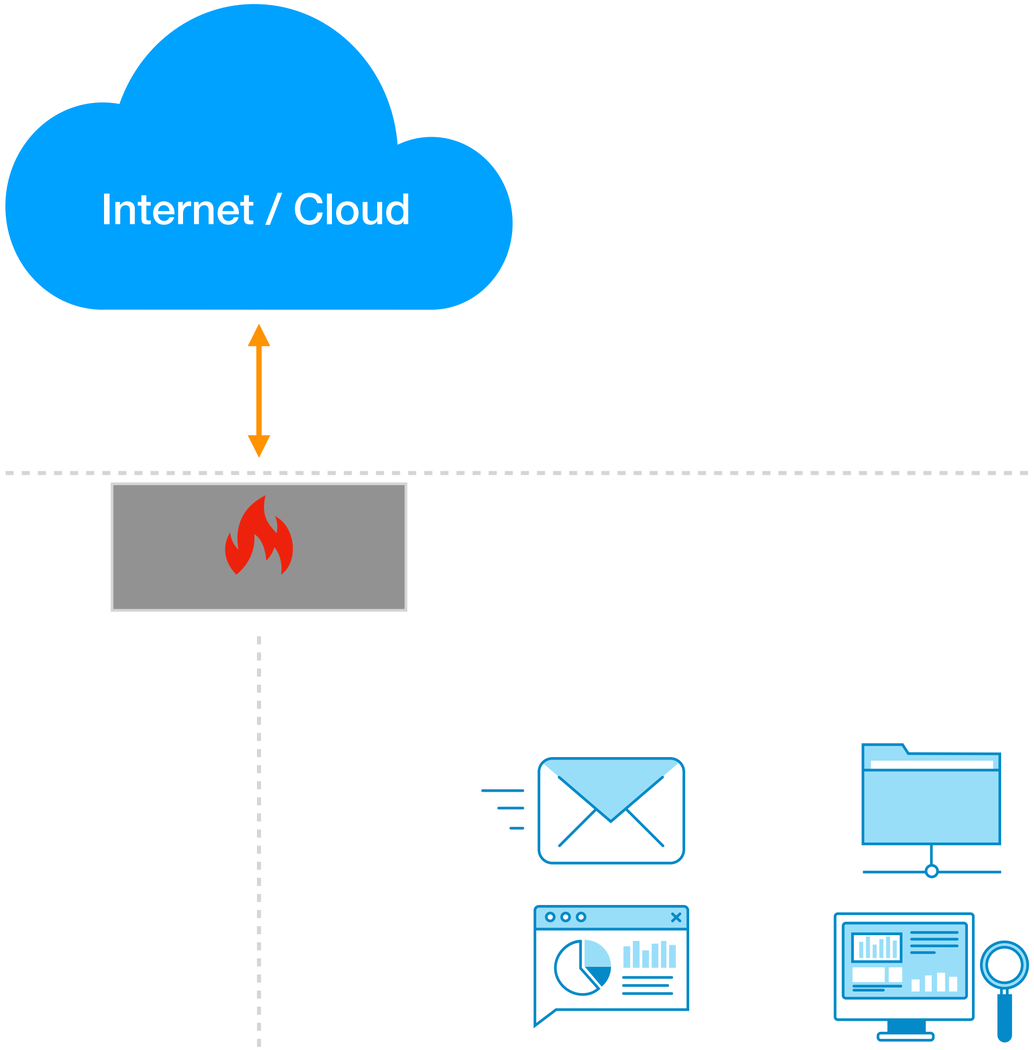
Safety



Circuit switch

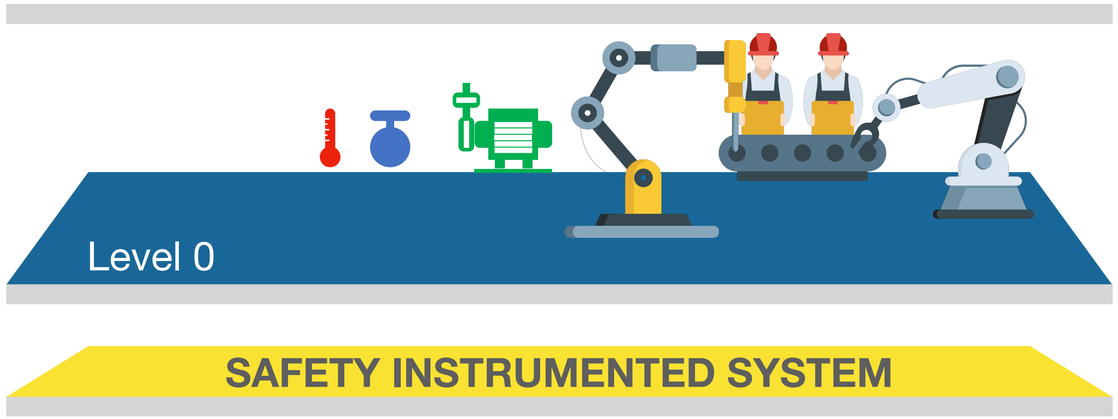
Nebras
CyberSecurityExpert

IT Network Design



Nebras
CyberSecurityExpert

OT Network Design

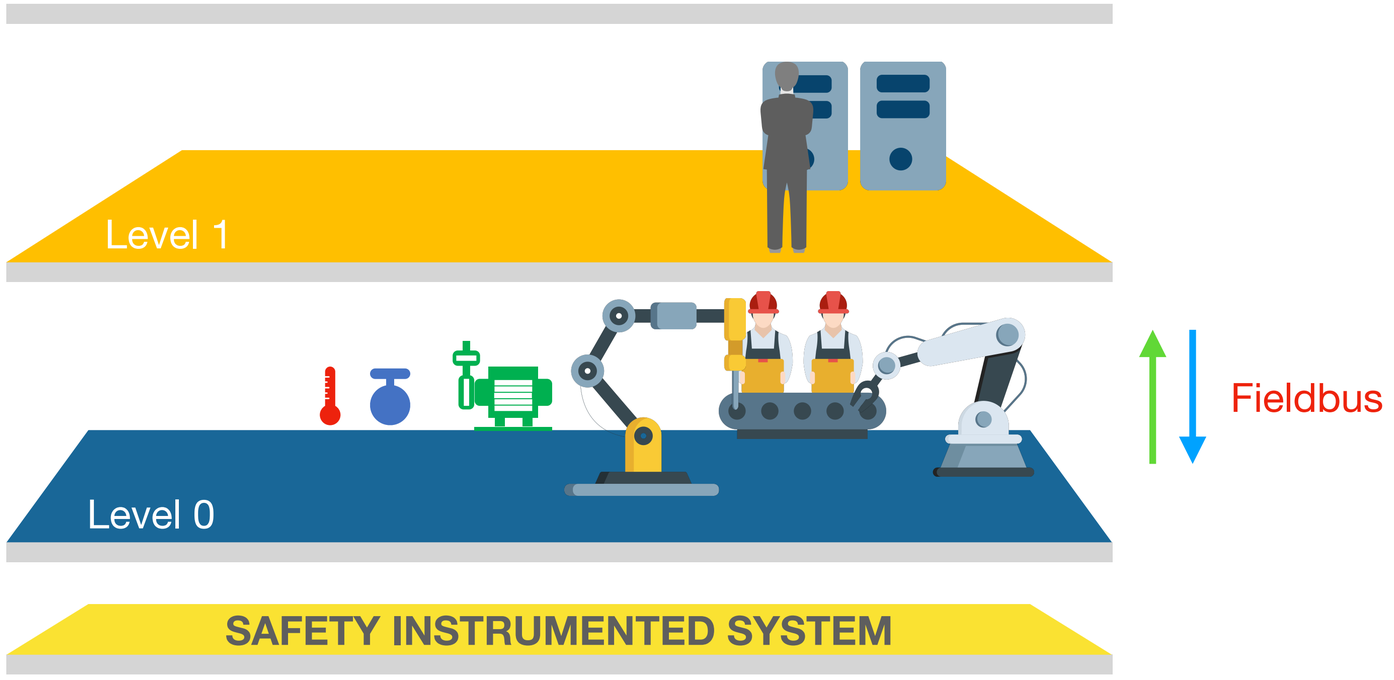


Process: Field Devices

Nebras
CyberSecurityExpert

OT Network Design

Control: PLC / RTU / PAC / IED



Process: Field Devices

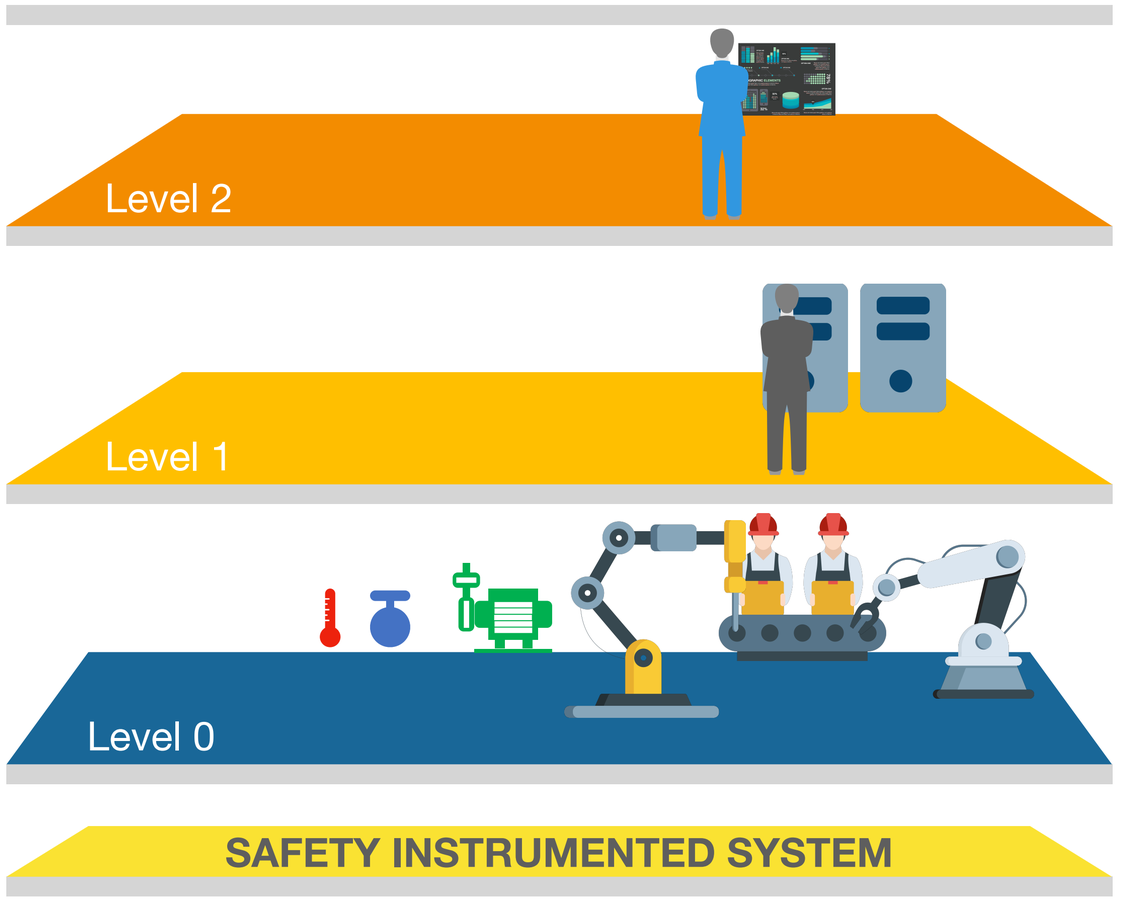
Nebras
CyberSecurityExpert

OT Network Design

Supervisory:
HMI / ENG / SCADA / HISTORIAN

Automation: PLC / RTU

Process: Field Devices



Ethernet / Serial

Fieldbus

Nebras
CyberSecurityExpert

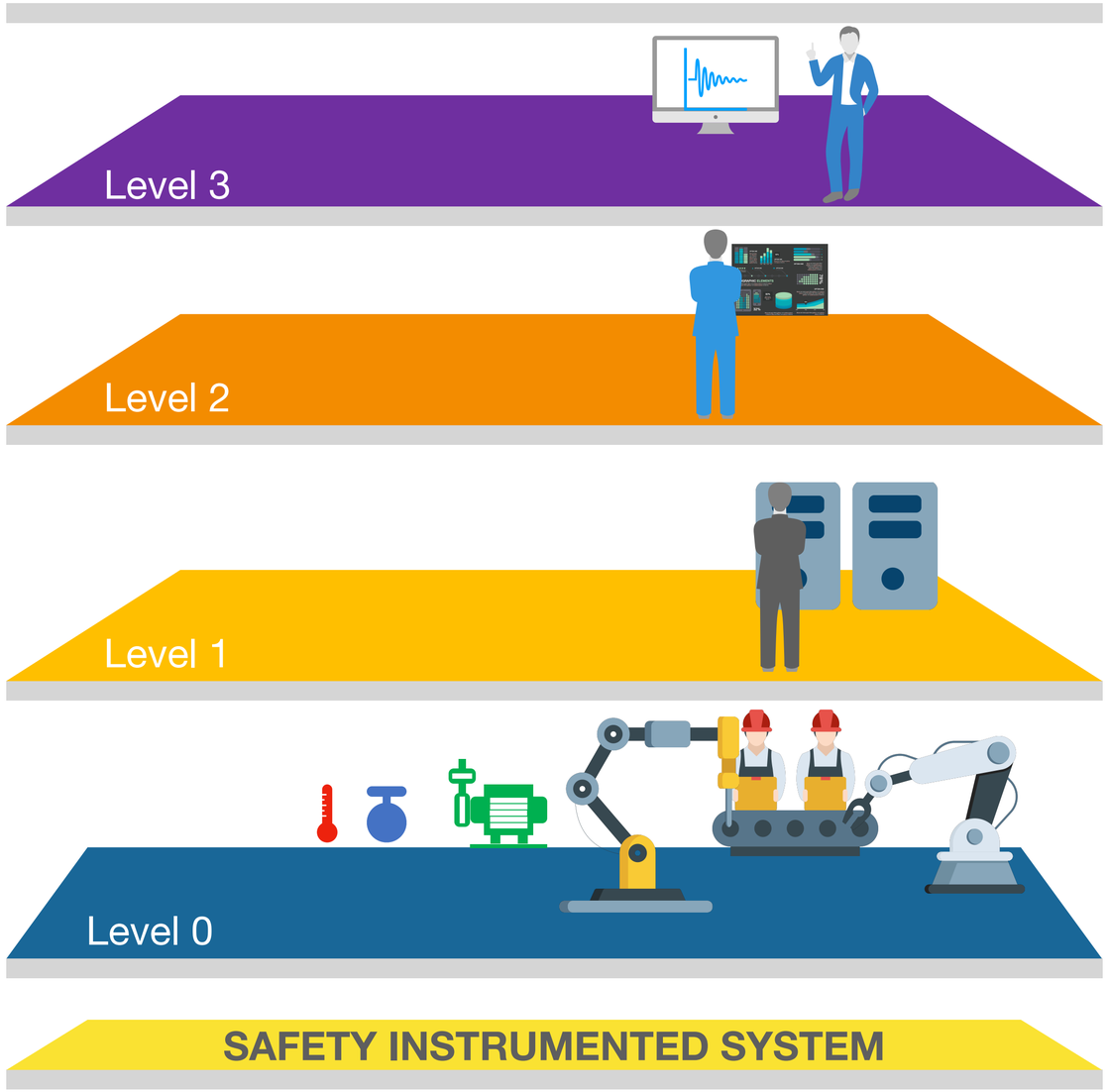
OT Network Design

Planning: MES
(Manufacturing Execution System)

Supervisory:
HMI / ENG / SCADA / HISTORIAN

Automation: PLC / RTU

Process: Field Devices



MES provides full visibility to management over the operation processes, from start to end. Helps in optimizing production and other decisions (Quality / Quantity)

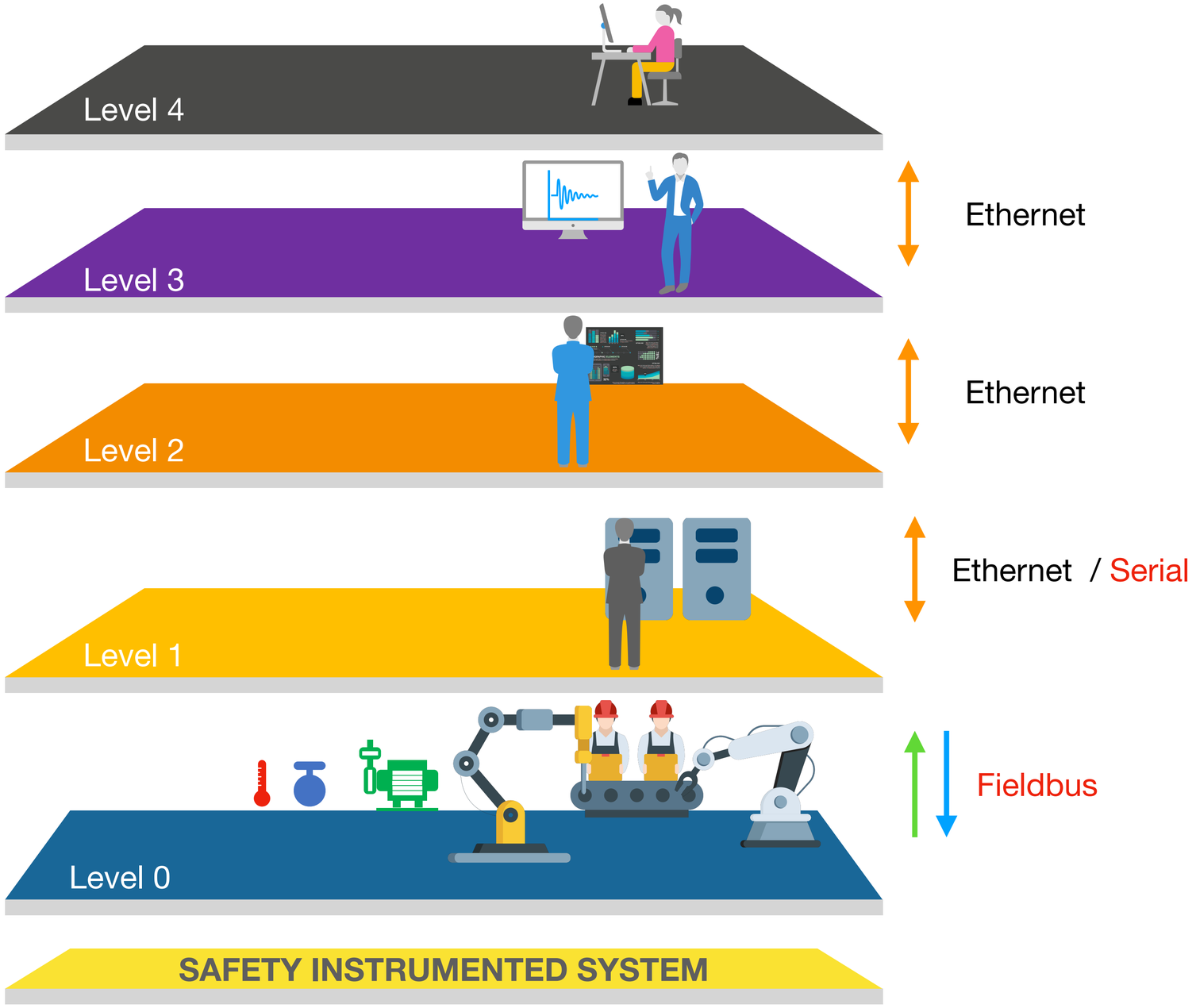
Ethernet

Ethernet / Serial

Fieldbus

Nebras
CyberSecurityExpert

OT Network Design



Management: ERP

Planning: MES

Supervisory:
HMI / ENG / SCADA / HISTORIAN

Automation: PLC / RTU

Process: Field Devices

Ethernet

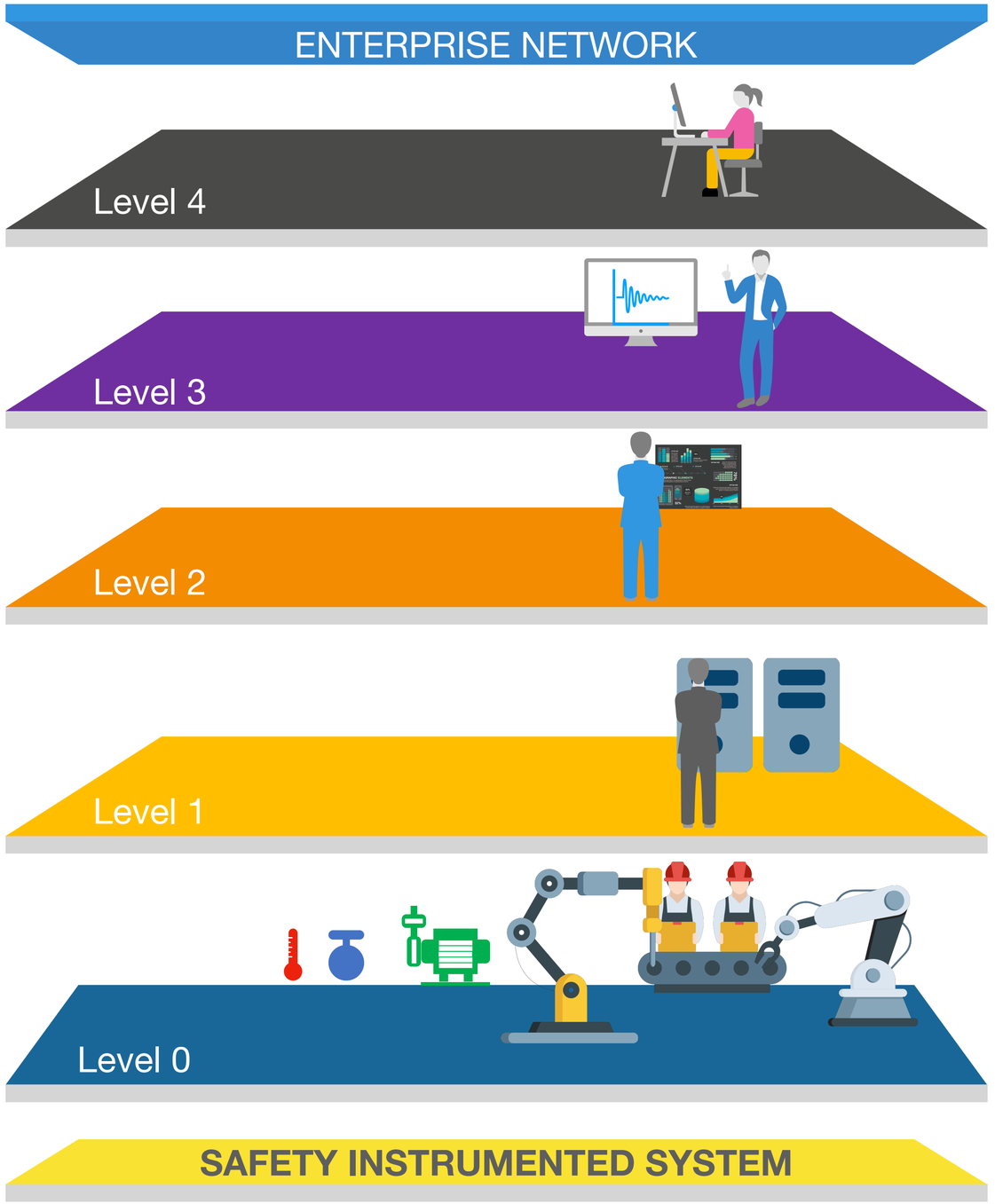
Ethernet

Ethernet / Serial

Fieldbus

Nebras
CyberSecurityExpert

OT Network Design



Management: ERP

Planning: MES

Supervisory:
HMI / ENG / SCADA / HISTORIAN

Control: PLC / RTU

Process: Field Devices

Ethernet

Ethernet

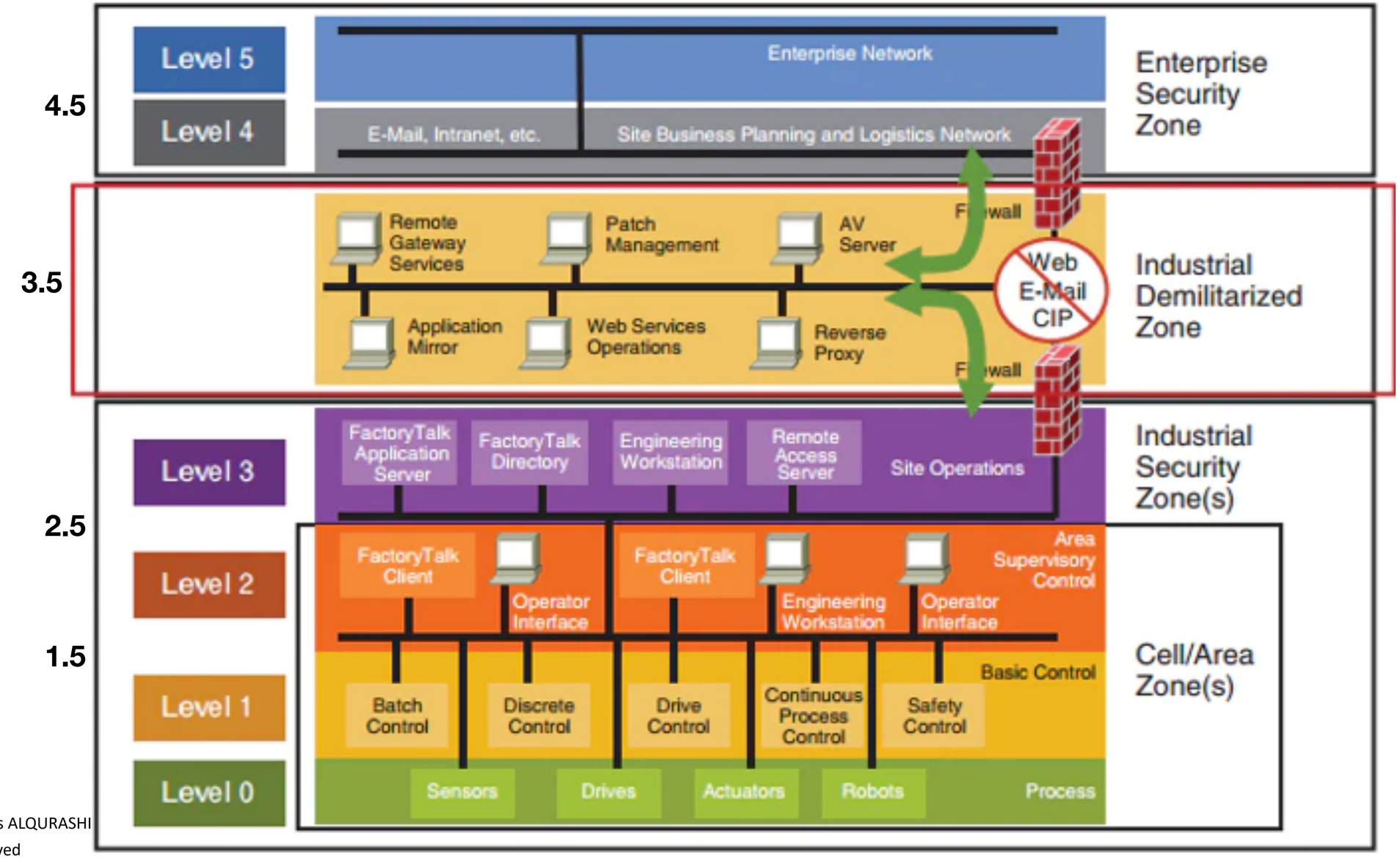
Ethernet

Ethernet / Serial

Fieldbus / Wireless

Purdue Reference Model

IT/OT Convergence vs Segmentation vs Micro Segmentation



Nebras CyberSecurityExpert

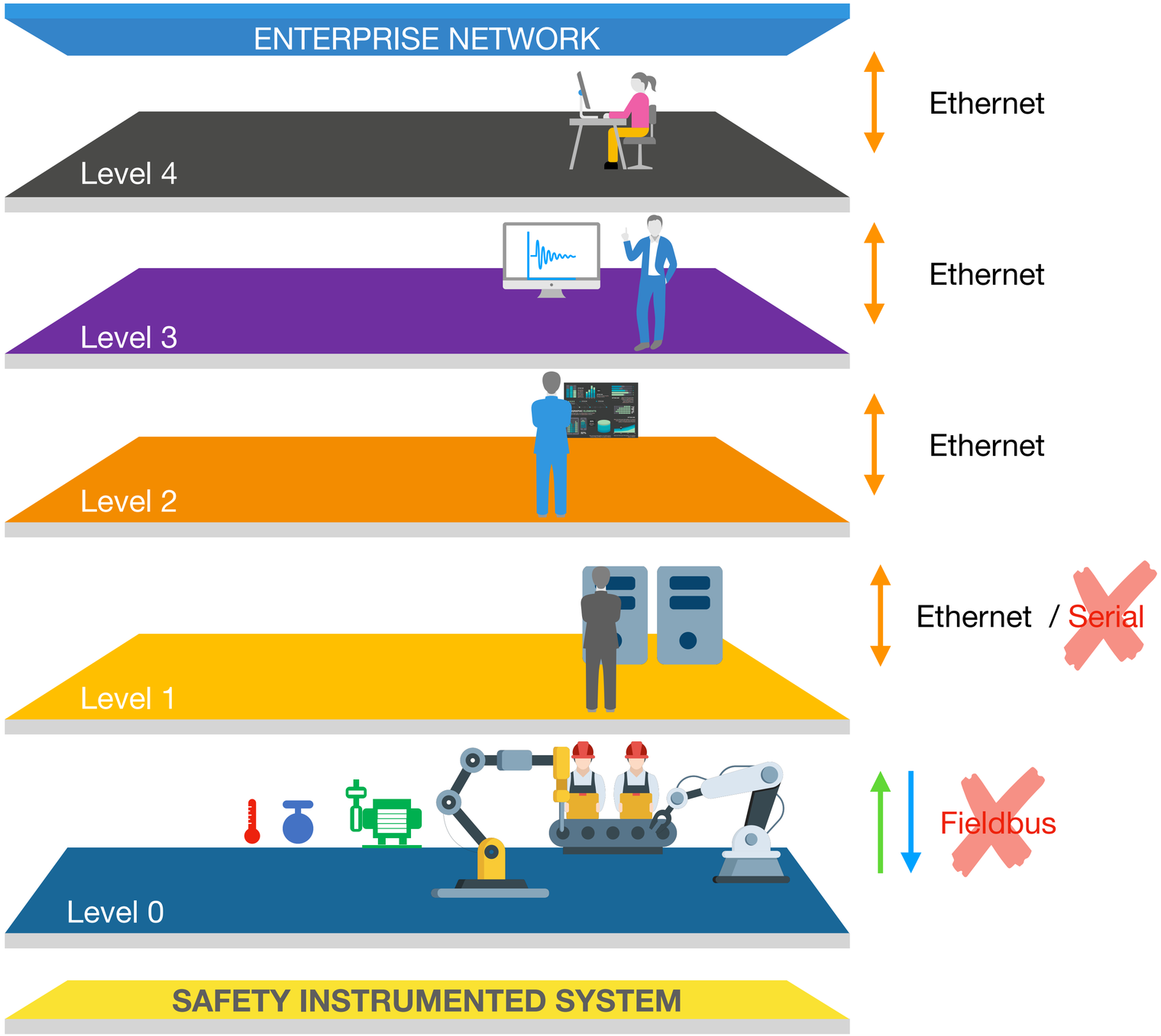
OT Cybersecurity

IT components

Servers
Workstations
Routers
Switches
Firewalls
OS
Software
Antivirus
IT Protocols

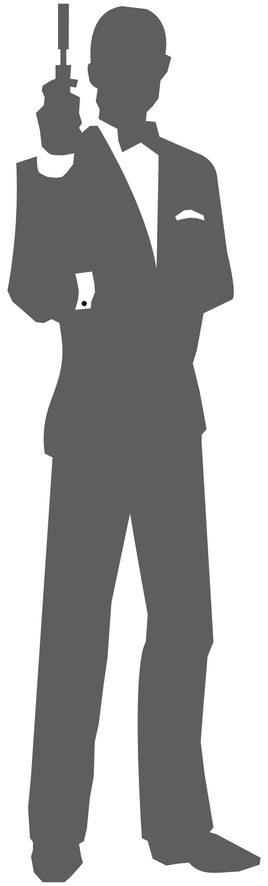
None-IT components

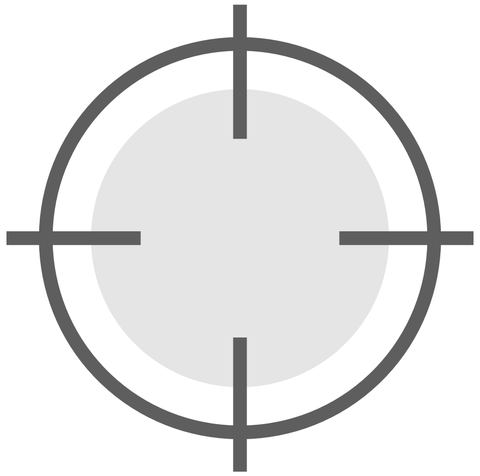
PLC / RTU
Industrial Protocols



Nebras
CyberSecurityExpert

IT vs OT Question?





Nebras
CyberSecurityExpert

IT vs OT Cybersecurity strength

Higher exposure to Internet

Security comes first

IT systems are equipped with security

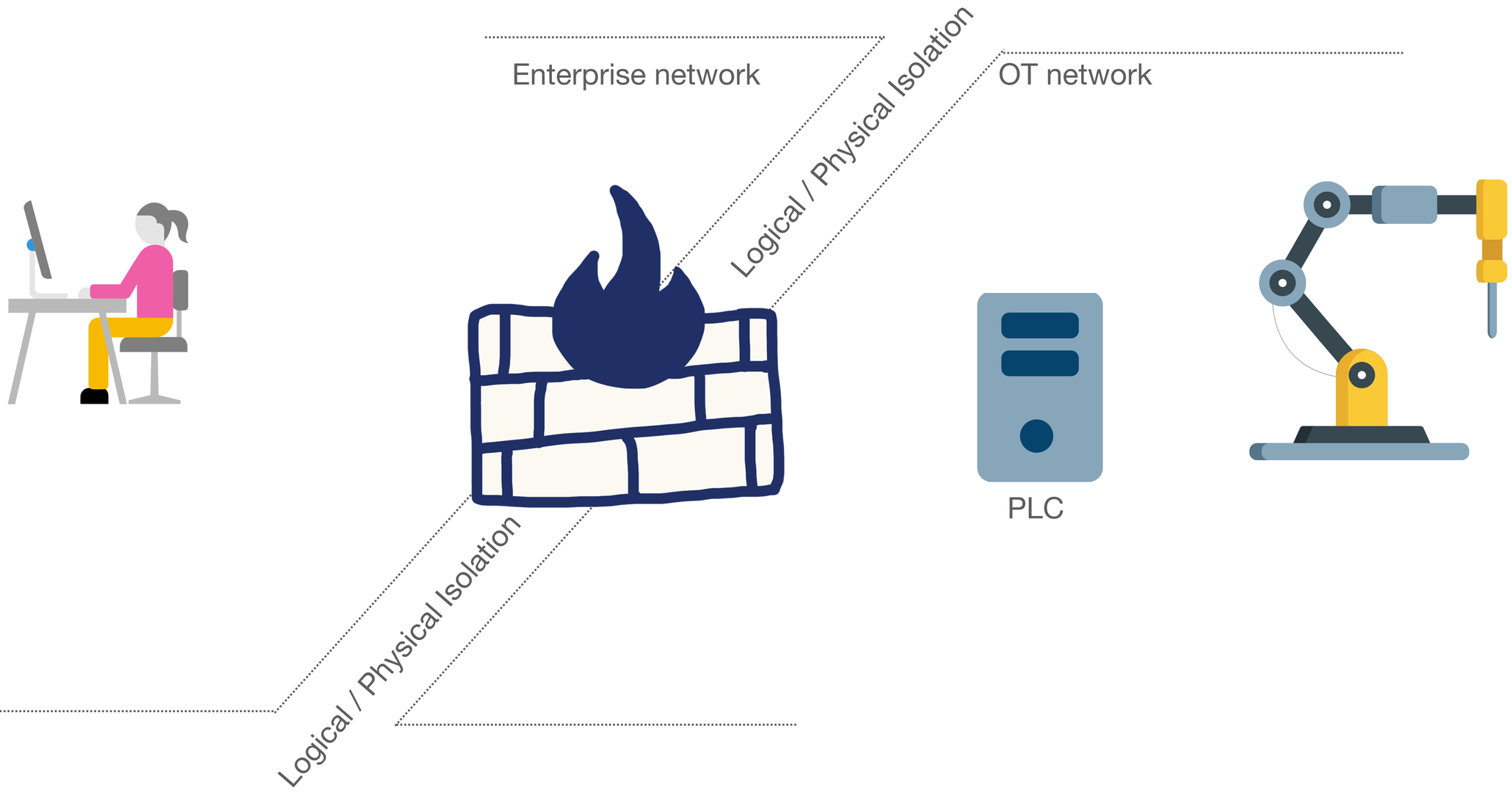
Mostly Isolated

Safety comes first

OT systems are insecure by design

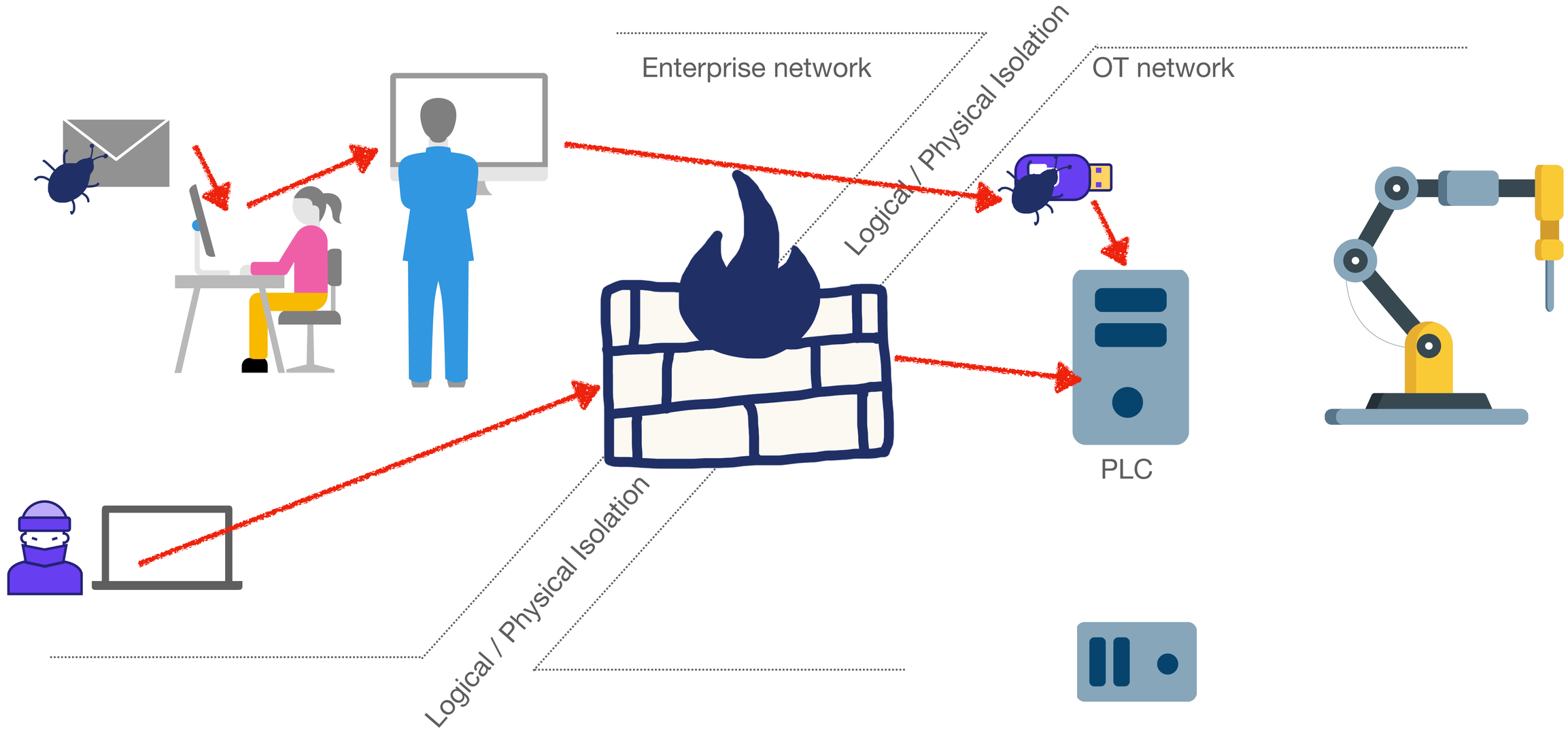
Nebras
CyberSecurityExpert

OT is air gapped (offline) networks, is this true?



Nebras
CyberSecurityExpert

OT is air gapped (offline) networks, is this true?



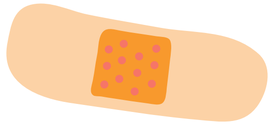
Nebras
CyberSecurityExpert

IT vs OT (Cybersecurity)

Encryption: used sometimes or not at all, delays caused by encryption/decryption may impact the operation.

Encryption: Advanced encryption is often used.

Patch Management: Not frequently, Vendors must be involved, impact must be tested offline.

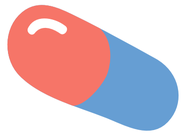


Patch Management: Performed routinely under standard procedures.

Pen-test: Dangerous and performed with cautious in specific timing.

Pen-test: Widely used by ethical hackers to identify vulnerabilities.

Upgrade: Many legacy systems still in use with few changes over years.



Upgrade: Continuously.

Nebras
CyberSecurityExpert

IT vs OT (Cybersecurity)

Cybersecurity Awareness: Low.

Cybersecurity Awareness: Medium-High.

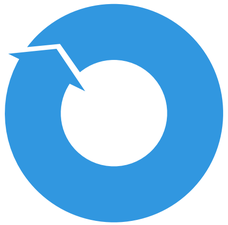
OT

IT

Data Loss: Loss of product and disturb plant process.

Data Loss: Restored from Backups.

Availability: Systems are designed with resilience, as it will have huge impact on plant processes and lives.



Availability: Critical.

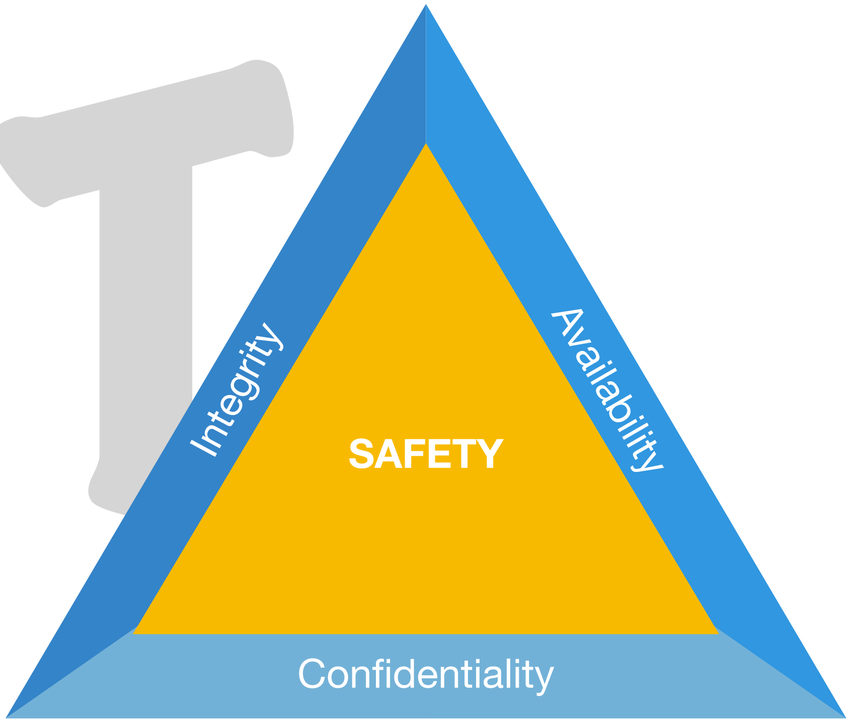
Performance: Critical.

Performance: Minor-Major.

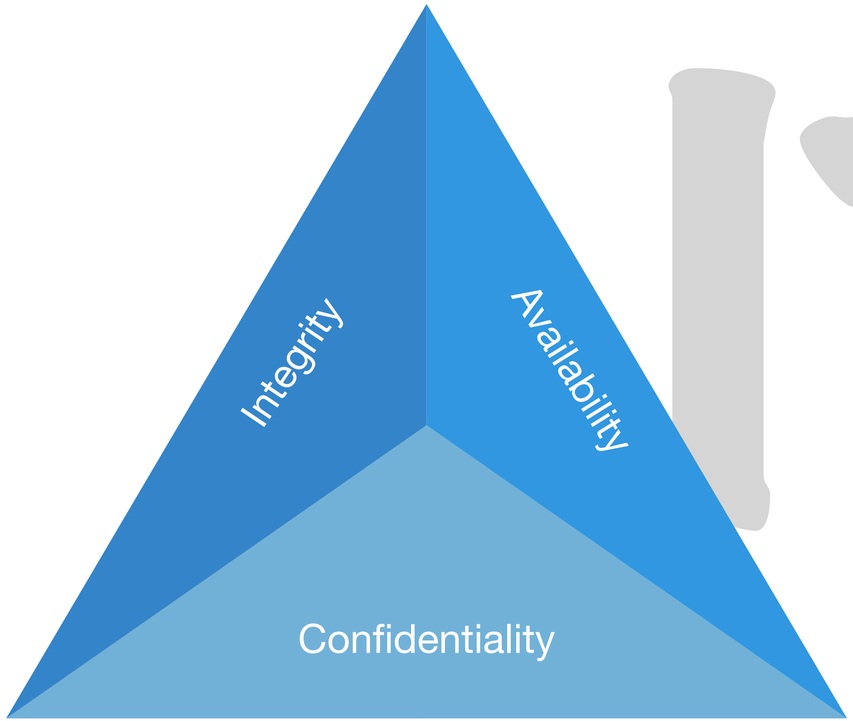
Nebras
CyberSecurityExpert

IT vs OT (Cybersecurity)

OT



IT



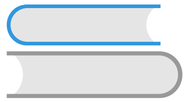
Nebras
CyberSecurityExpert

Quick Summary

IT/OT Gap

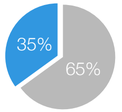
OT Terminology

OT Network



Purdue Reference Model

IT within OT



IT vs OT

Nebras
CyberSecurityExpert