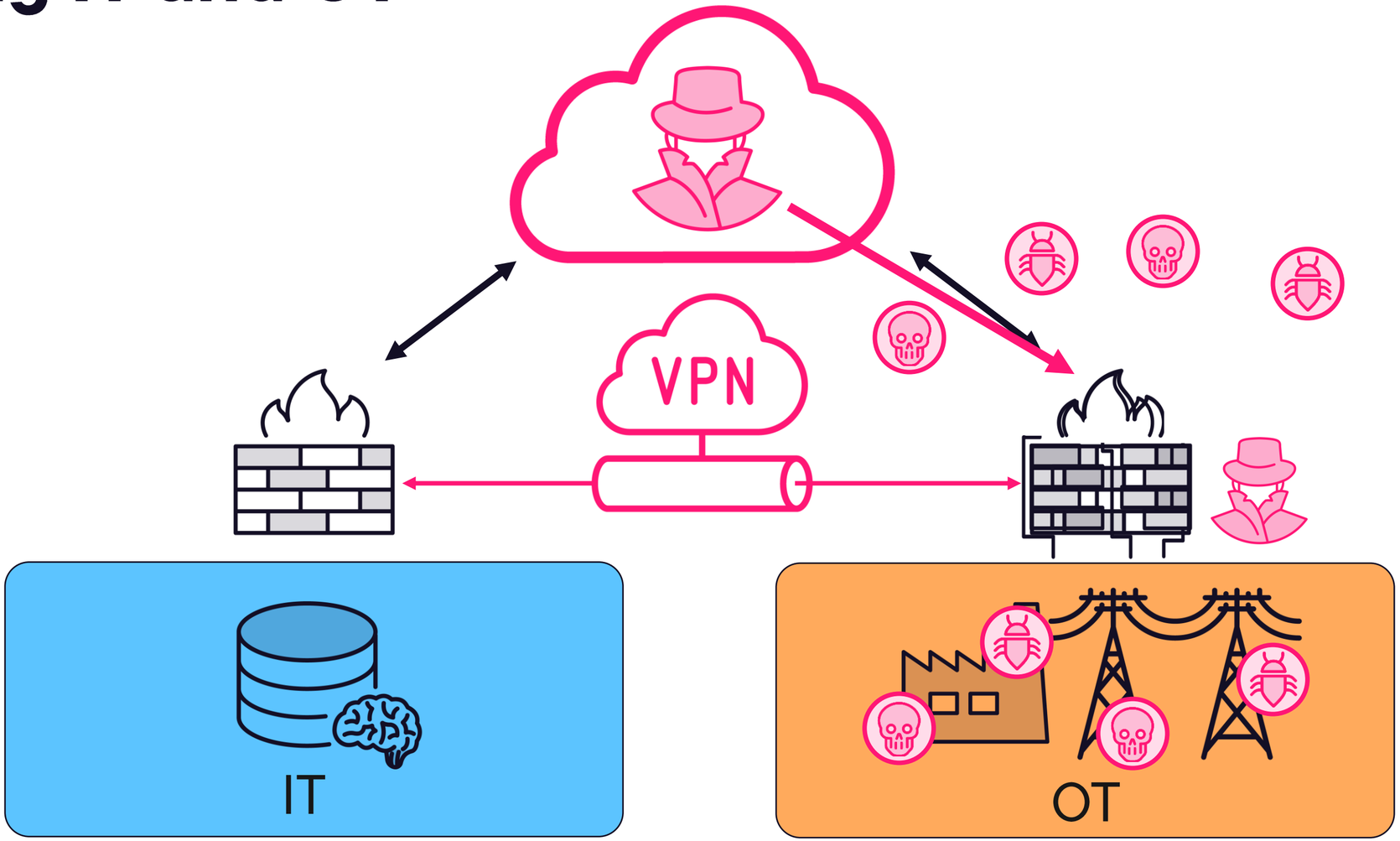
OT Network Anatomy



Davy Cavens
OT Security Architect

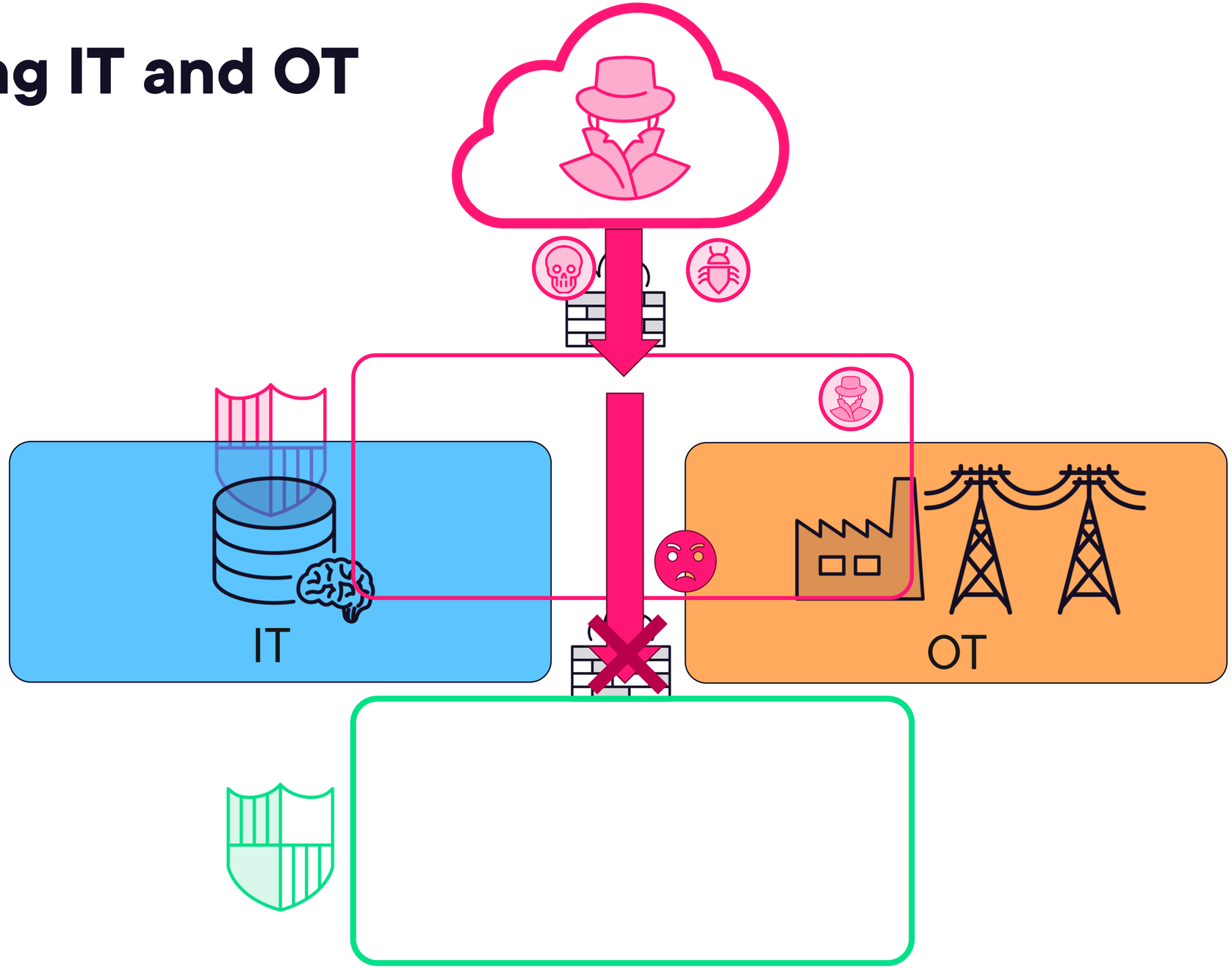
linkedin.com/in/davycavens/

Linking IT and OT



Horizontal approach

Linking IT and OT



IEC62443 Framework

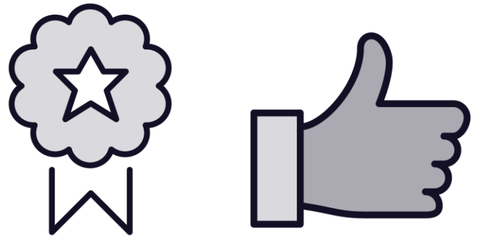
What Is a Framework?



Policies



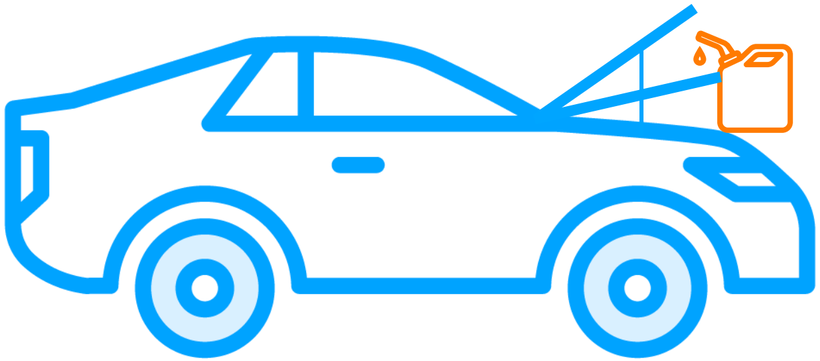
Guidelines



Best Practices

Framework Analogy

Best Practice





Quality

Maintenance



35 – 40 PSI
2.4 – 2.7 Bar

Oil Check

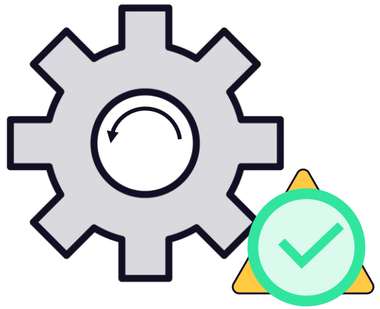


Tire Pressure

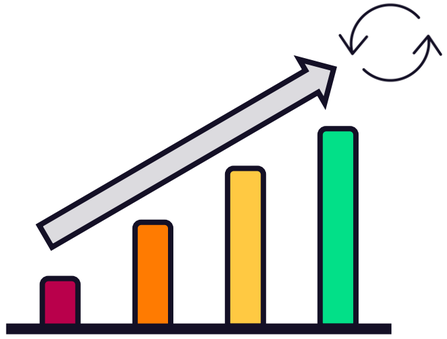
Why Use a Framework?



Compliance



Manage Risk



Continuous Improvement

Framework Structure

IEC
62443
–
2
–
3





Policies & Procedures





TR: Patch Management in the IACS environment

The IEC62443 Framework

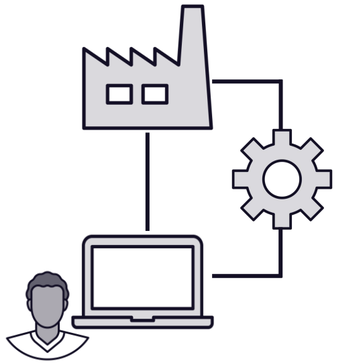
General	Policies & Procedures	System	Component
5 Documents	5 Documents	3 Documents	2 Documents
Concepts & models	CSMS	Security Levels	Secure SDLC
General Terminology	Patch Management	System Requirements	Component Requirements

IEC62443 Personas



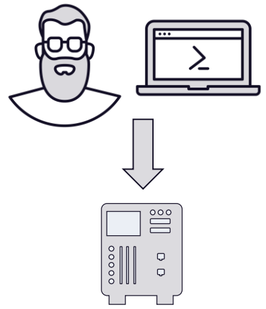
Asset owners

Policies & Procedures



System integrators

System



Product suppliers

Component

IEC62443 Key Concepts

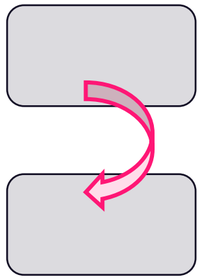
IEC62443 Key Concepts



Foundational Requirements



Security Levels



Zones & Conduits

Foundational Requirements

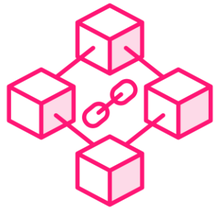
IEC 62443 – 1 - 1



Identification & access control



Use control



System integrity



Data confidentiality



Restricted data flow



Timely response



Availability





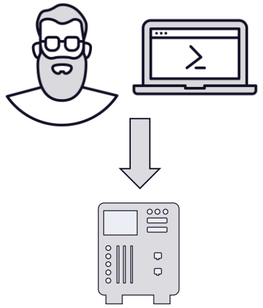


Security Level Types

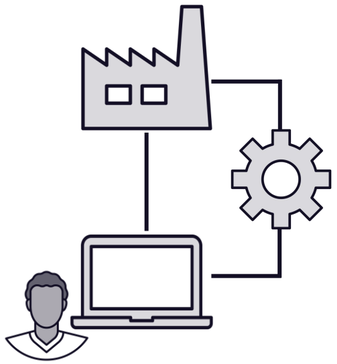
IEC 62443 – 3 - 3



Asset owners



Product suppliers



System integrators

SL-T

Target security level

3 – 2

SL-C

Capability security level

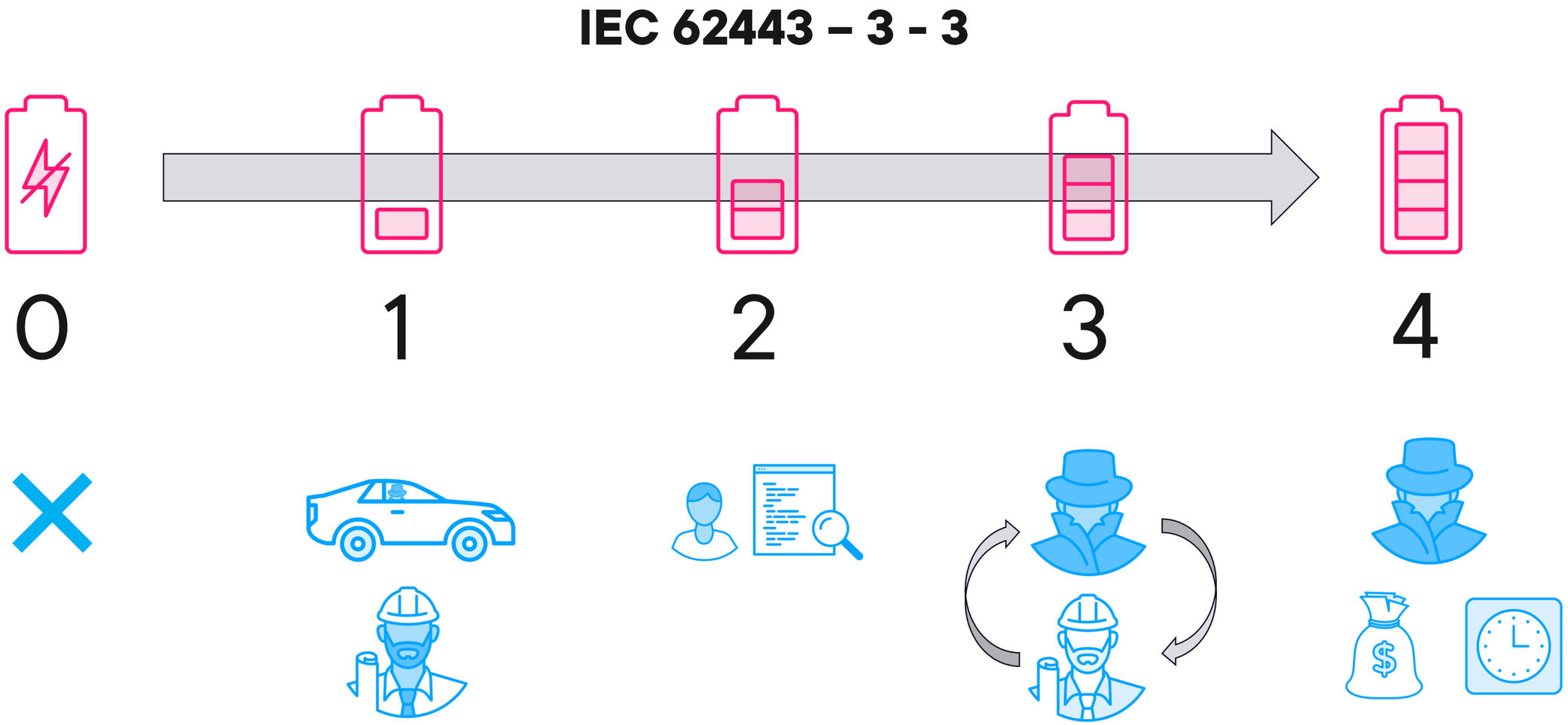
4 – 2

3 – 3

SL-A

Achieved security level

The IEC62443 Framework – Security levels



Mapping FRs to SLs

Mapping FRs to SLs

IEC 62443 – 3 - 3

FR

SL

Identification & access control	Use control	System integrity	Data confidentiality	Restricted data flow	Timely response	Availability

PLC

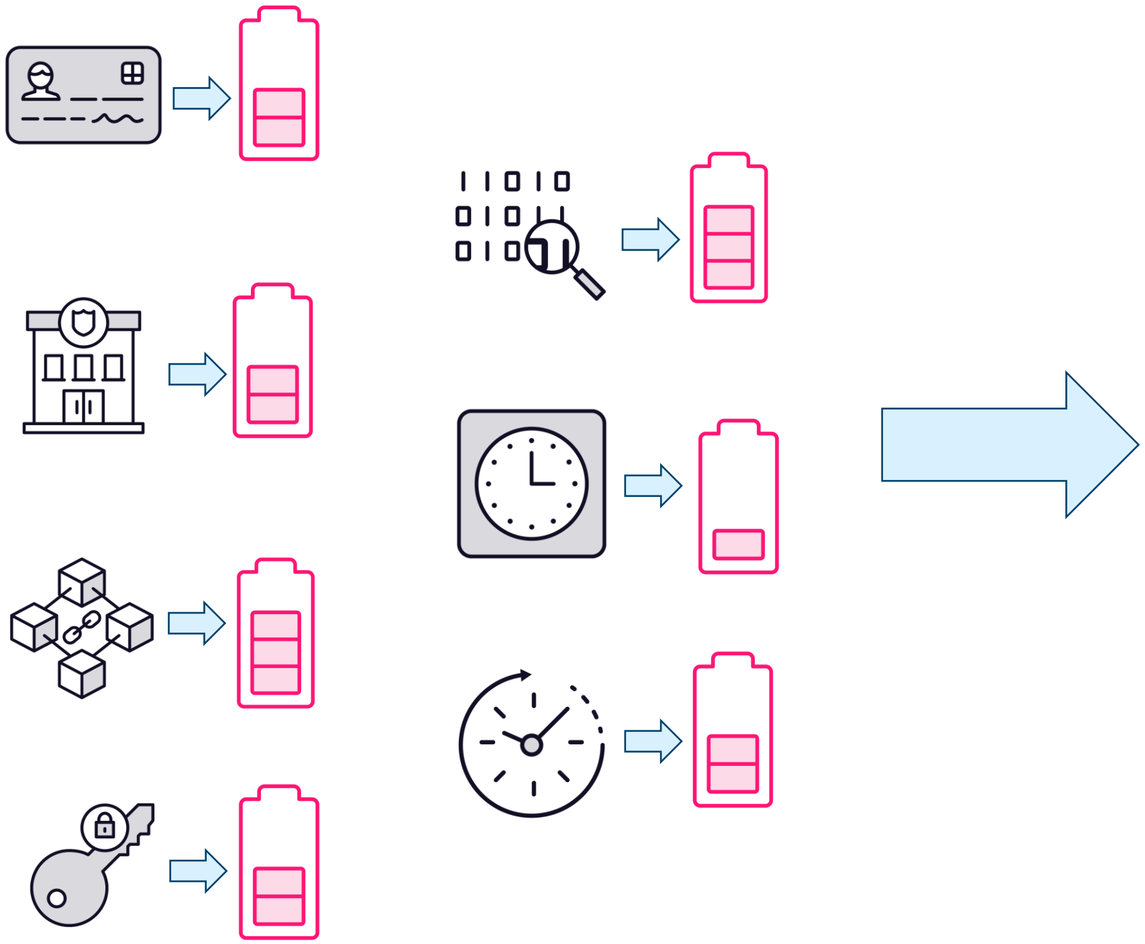
Purpose-built

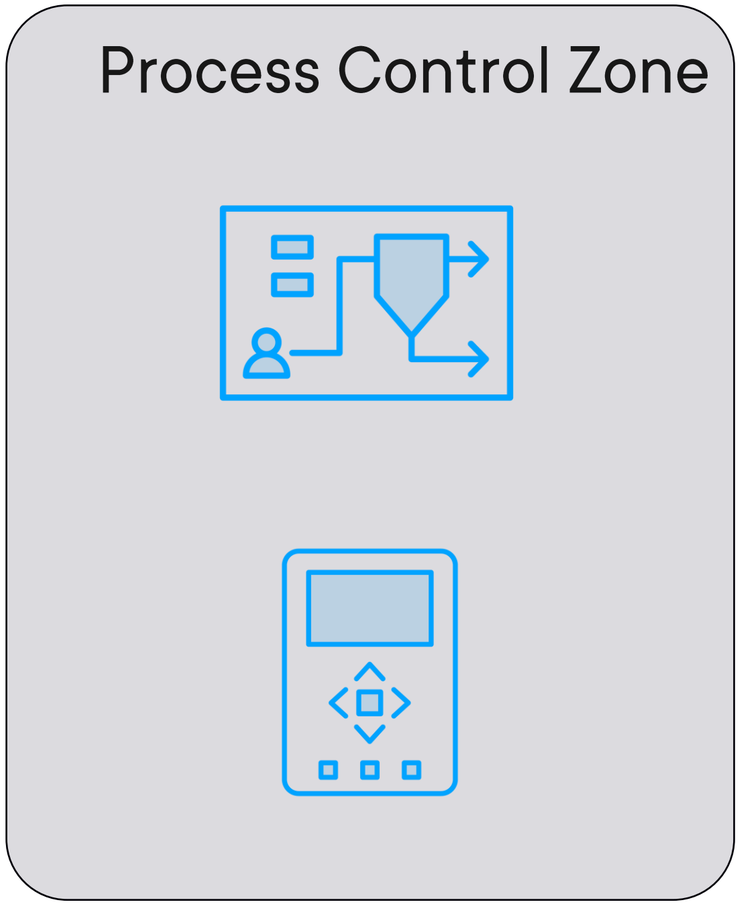
Too expensive

> !

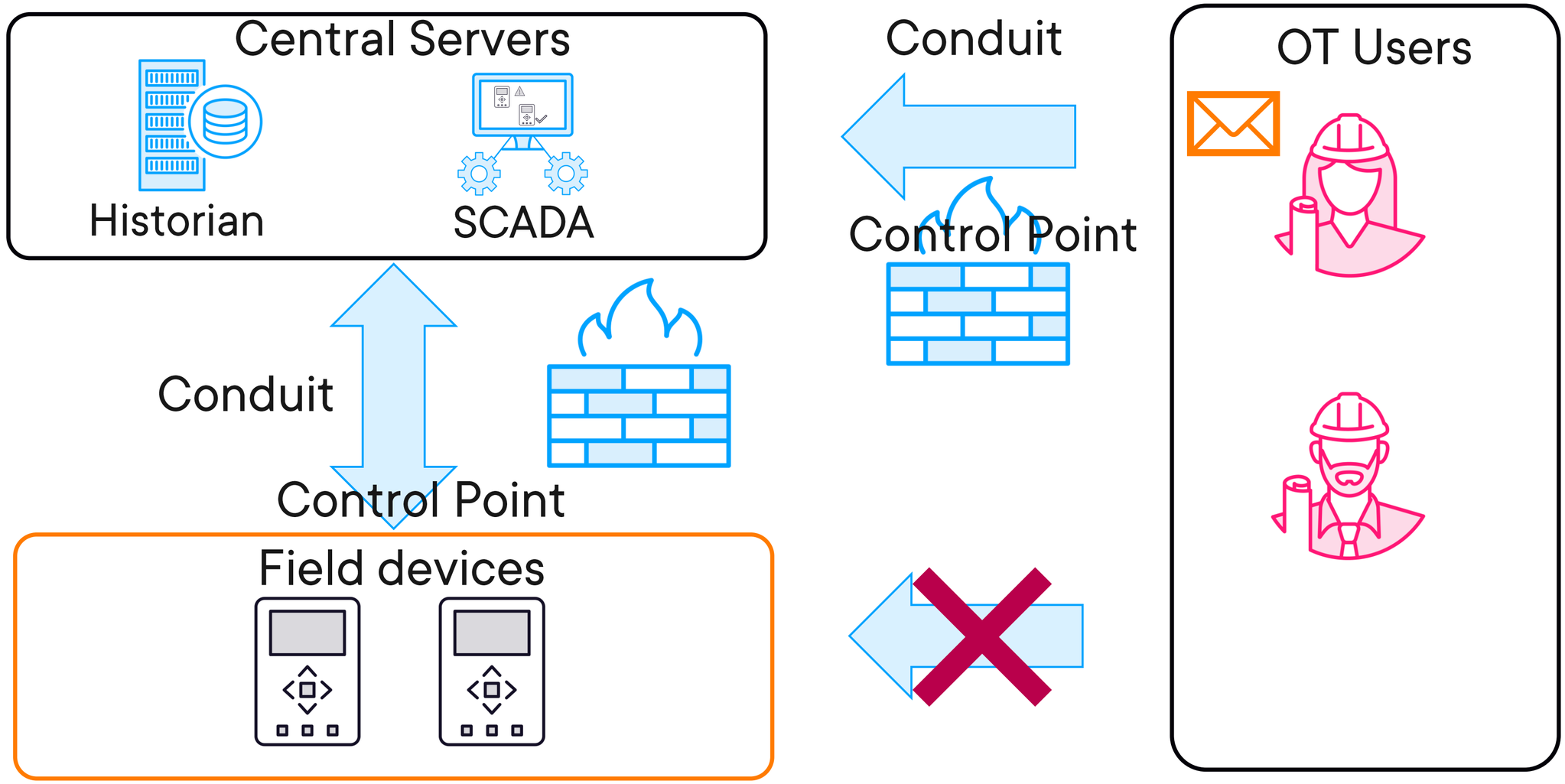
Form factor

Zones and Conduits



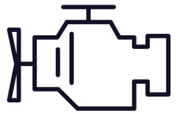


Zones and Conduits

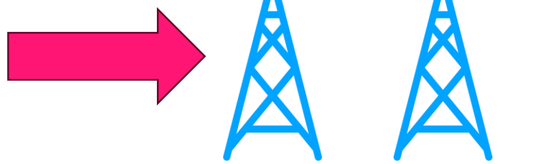


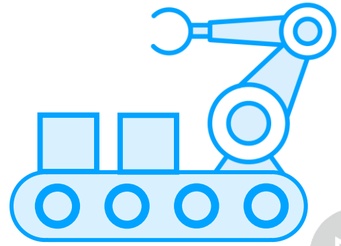
The Purdue Enterprise Reference Architecture

Industrial Process





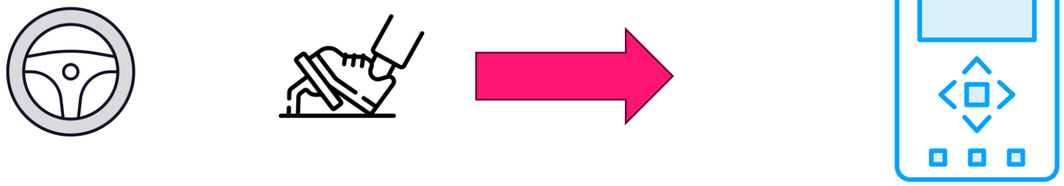




The Purdue Enterprise Reference Architecture

Basic Control

Industrial Process



The Purdue Enterprise Reference Architecture

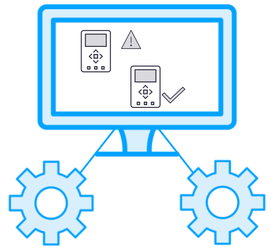
Area Supervisory Control

Basic Control

Industrial Process







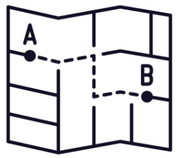
The Purdue Enterprise Reference Architecture

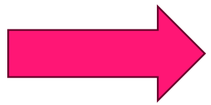
Site Operations

Area Supervisory Control

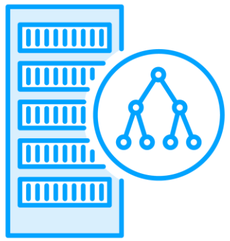
Basic Control

Industrial Process









The Purdue Enterprise Reference Architecture

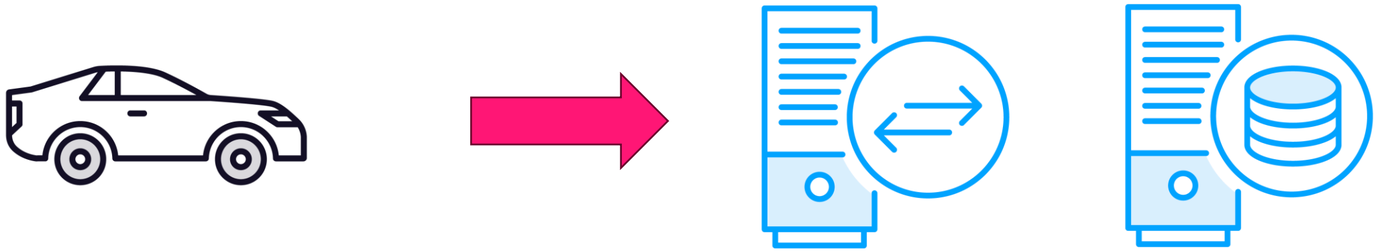
Industrial DMZ

Site Operations

Area Supervisory Control

Basic Control

Industrial Process



The Purdue Enterprise Reference Architecture

Enterprise

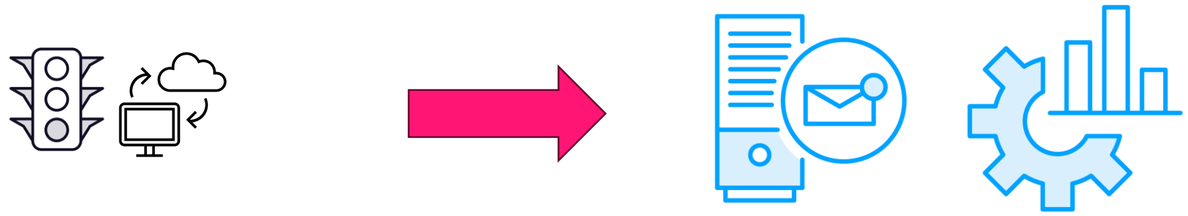
Industrial DMZ

Site Operations

Area Supervisory Control

Basic Control

Industrial Process



Summary

IT – OT Link

IEC 62443 Framework

Zones and Conduits

Purdue Model