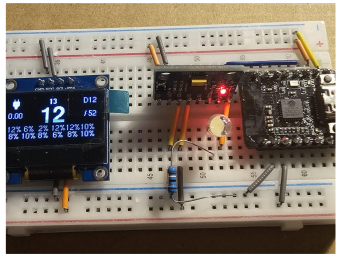
OT Presentation

Introduction (+peek around the corner).

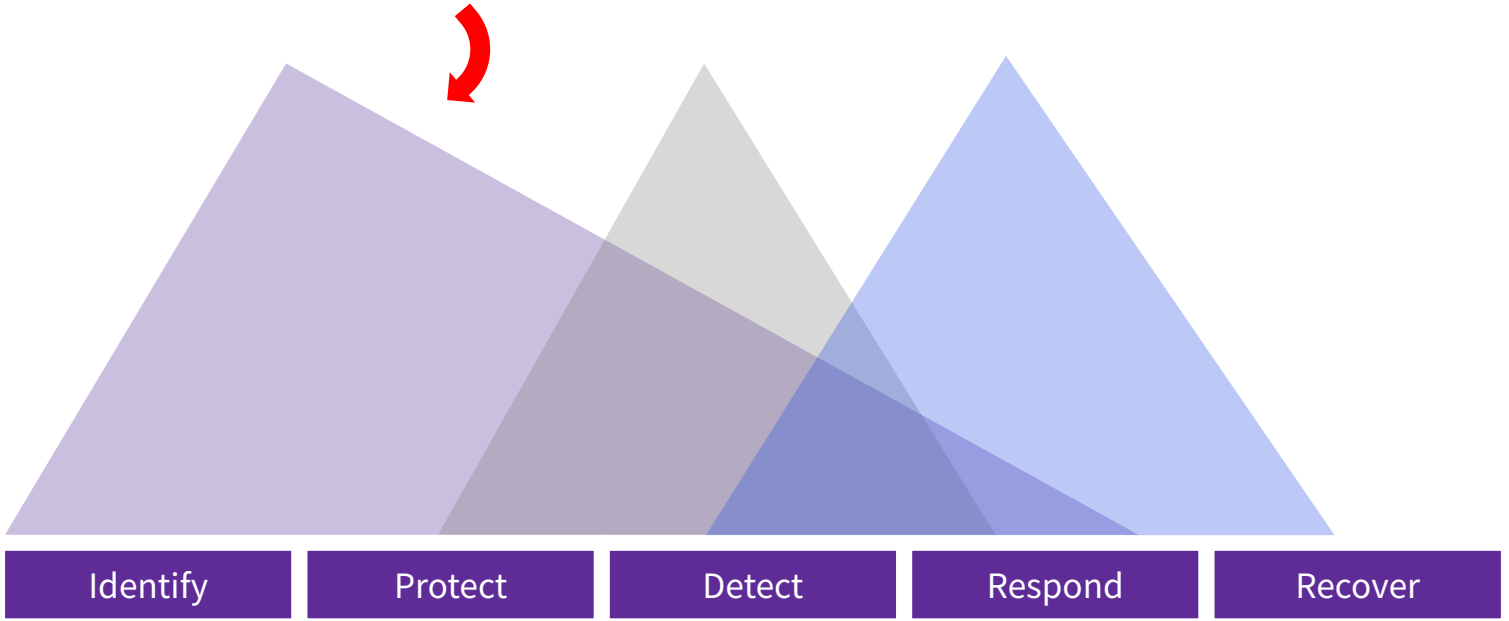
- Brief introduction & orientation to OT (+thinking).
- Introduce current key risk topics.
- Dissect (some) well known incidents.

** Any opinions are my own and from my own work/life experience. Any feedback/agreement/disagreement welcome!*



Toit

CS Careers



The NIST CSF Five Functions as described in its online learning portal.

Who wants an MVP bridge?

Tacoma Narrows bridge collapse (1940)

The Millau Viaduct In France: The World's Tallest Bridge

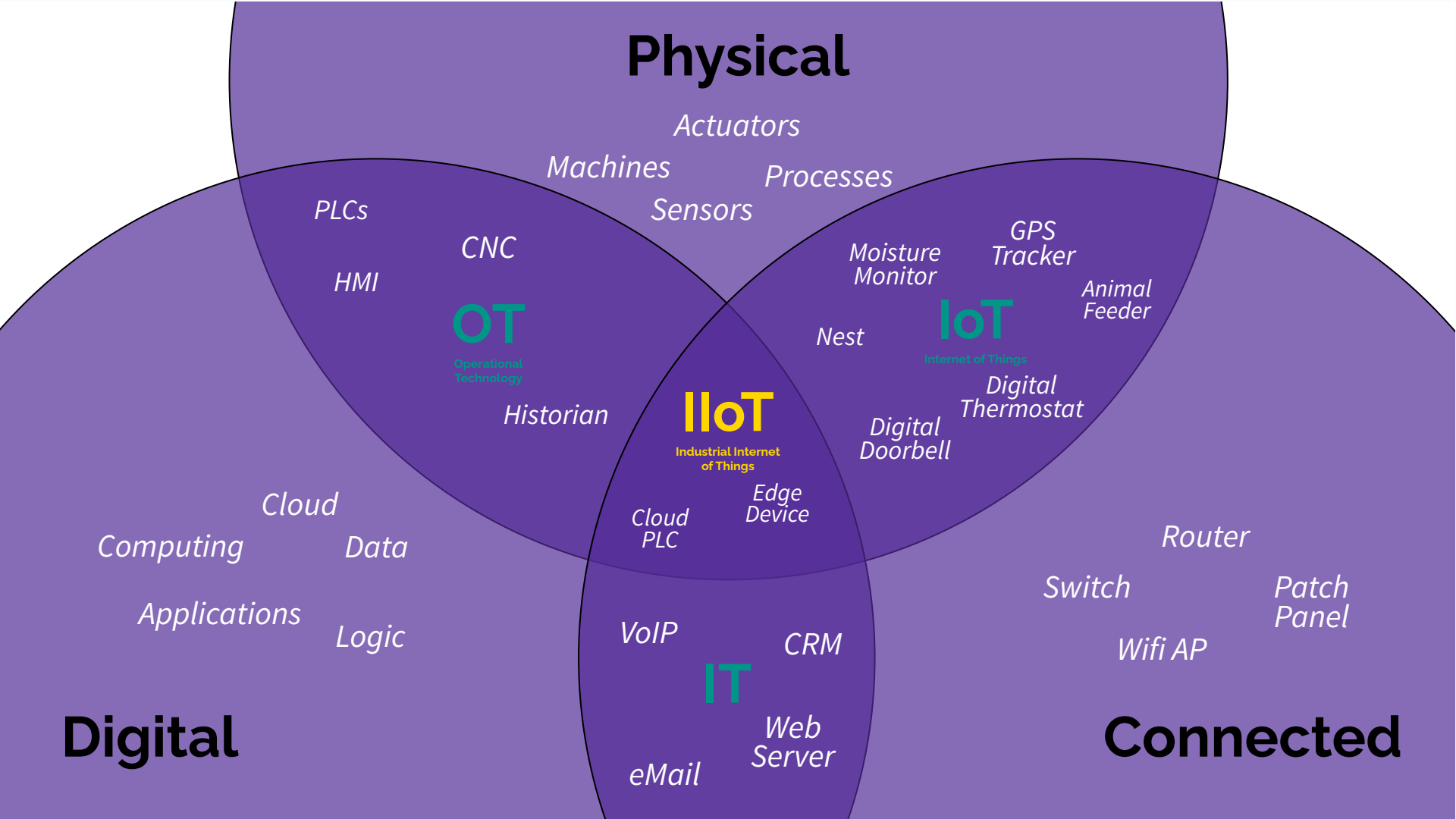
Bridges:

- Safety-critical.
- Partial functionality completely unacceptable.
- ‘Patching’ impractical or impossible.

What is OT?

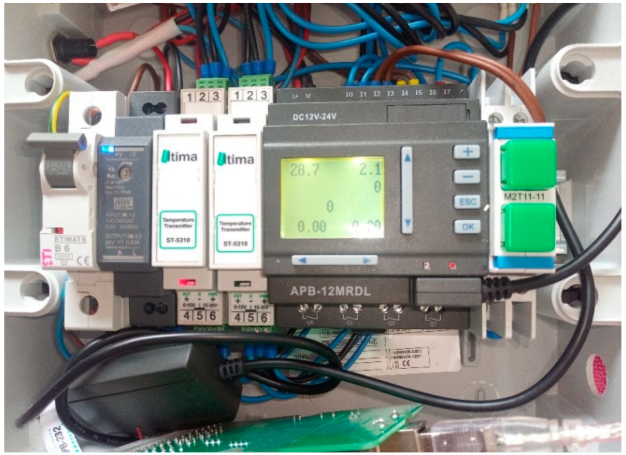
HW/SW that directly monitors and/or controls physical (industrial) processes.

- ‘Operational’ Technology
- Long lived/Slow moving
- Physical/Process Control
- Usually Realtime **
- Thinking: ‘Critical’
- Risk: Likelihood * Impact
- (SIS & IEC 61511) *


Physical
Actuators
Machines
Processes
Sensors
PLCs
CNC
HMI
OT
Operational Technology
Historian
Moisture Monitor
GPS Tracker
Animal Feeder
IoT
Internet of Things
Nest
Digital Thermostat
Digital Doorbell
IIoT
Industrial Internet of Things
Edge Device
Cloud PLC
Cloud
Computing
Data
Applications
Logic
VoIP
CRM
IT
Web Server
eMail
Router
Switch
Patch Panel
Wifi AP
Digital
Connected

OT Components

- PLCs
- Sensors/Readers
- Plant/Machinery
- Actual industrial equipment

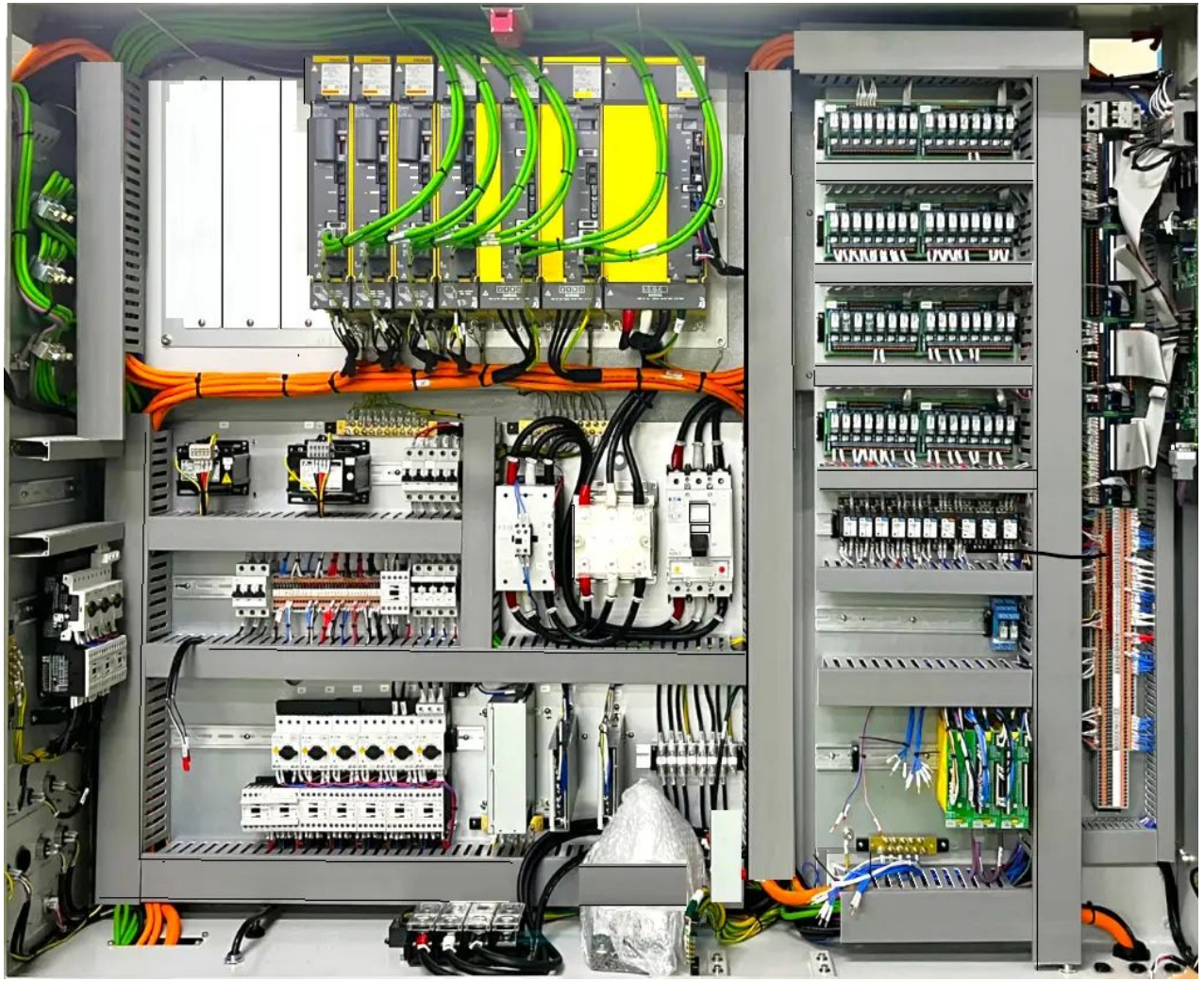


OT Components

Drive control panel featuring

- PLCs
- Circuit breakers
- Cabling and capping
- Fibre patch panel

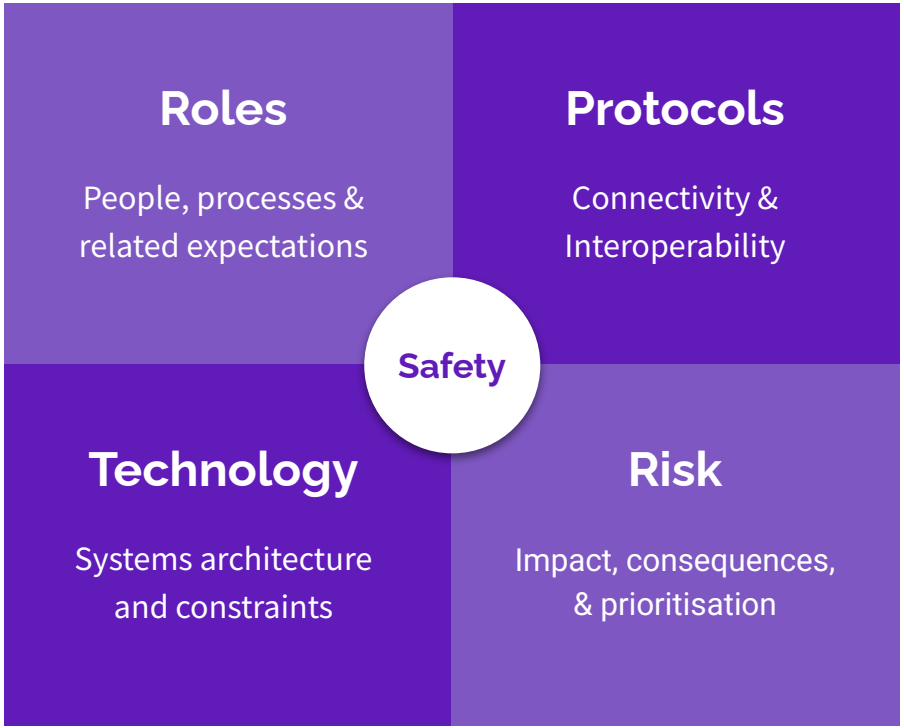
How PLC's and Drive Control Panels drive Industrial Automation



OT Components

- HMI
- Control Rooms
- SIS *

What is OT:


Roles
People, processes & related expectations
Protocols
Connectivity & Interoperability
Safety
Technology
Systems architecture and constraints
Risk
Impact, consequences, & prioritisation

Domains

Processing **Information**	**Purpose & Focus**	Managing **Processes**
CIA **Confidentiality**, Data Sec, Accessibility	**Priorities**	Safety, AIC **Availability**
Servers, Cloud, **Enterprise Apps**	**Technology**	SCADA, DCS, RTU, Sensors, Servers
Cybersecurity	**Security & Risk**	Physical & **Operational Safety**, Security
CIO, Hierarchical, **Centralized**	**Structure & Culture**	COO, Decentralized, **Field-oriented**
Computer Science, Service Management	**Expertise**	**Engineering** disciplines & maintenance

What's special about OT Devices?

(For now) let's divide into:

- Pre- and
- Post-network era.

For CS involved staff:

- 'Change cycle' still long >
- Need to live with it >
- Need to find solutions.

Engineering -centric design.

Not network capable.

Assume physical security.

Safety before security.

Long lived.

Typically appliances.

Using 3rd party NW stacks.

+Economic Pressure.

++ Attack Surface

+Vendor Pressure.

+Remote access.

+Ecosystem complexity.

Still risk averse.

+IT.. + old constraints.

Breaks things

IT tools, technologies, and thinking, can break things.

In OT, “break” might equal “catastrophe”.

OT Standards

Tailored to physical processes, ICS, or safety-critical contexts.

Common with OT:

- ISO: 27001/27002/31000
- NIST: CSF & 800-53

Specific to OT:

- ISO/IEC 62443 *
- Perdue Model *
- CISA
- Domain specific (ie IEEE 1686)

Confidentiality:

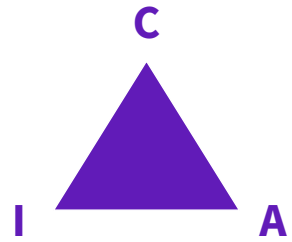
As in personal data protection.

Integrity:

As in Finance.

Availability :

As in ICS or Healthcare,
e.g: Electric power grid or water treatment OT systems.



CIA Triad:

Prioritisation contextual, not absolute.

Strip Poker

The smart player layers up before attending a game with strangers.

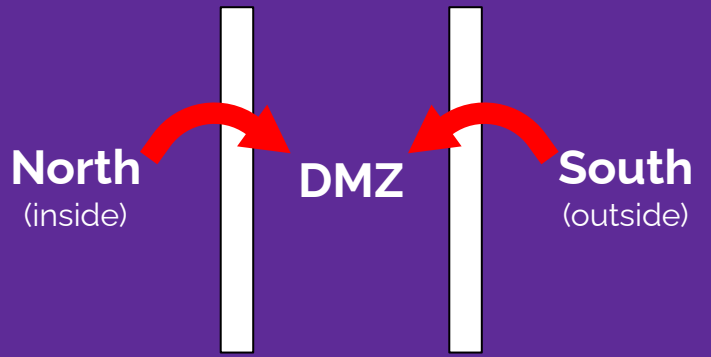
Zero Trust

*Sometimes the ‘lock’ **is** the weakness.*

- Assume Breach
- Never Trust, Always Verify
- Least Privilege

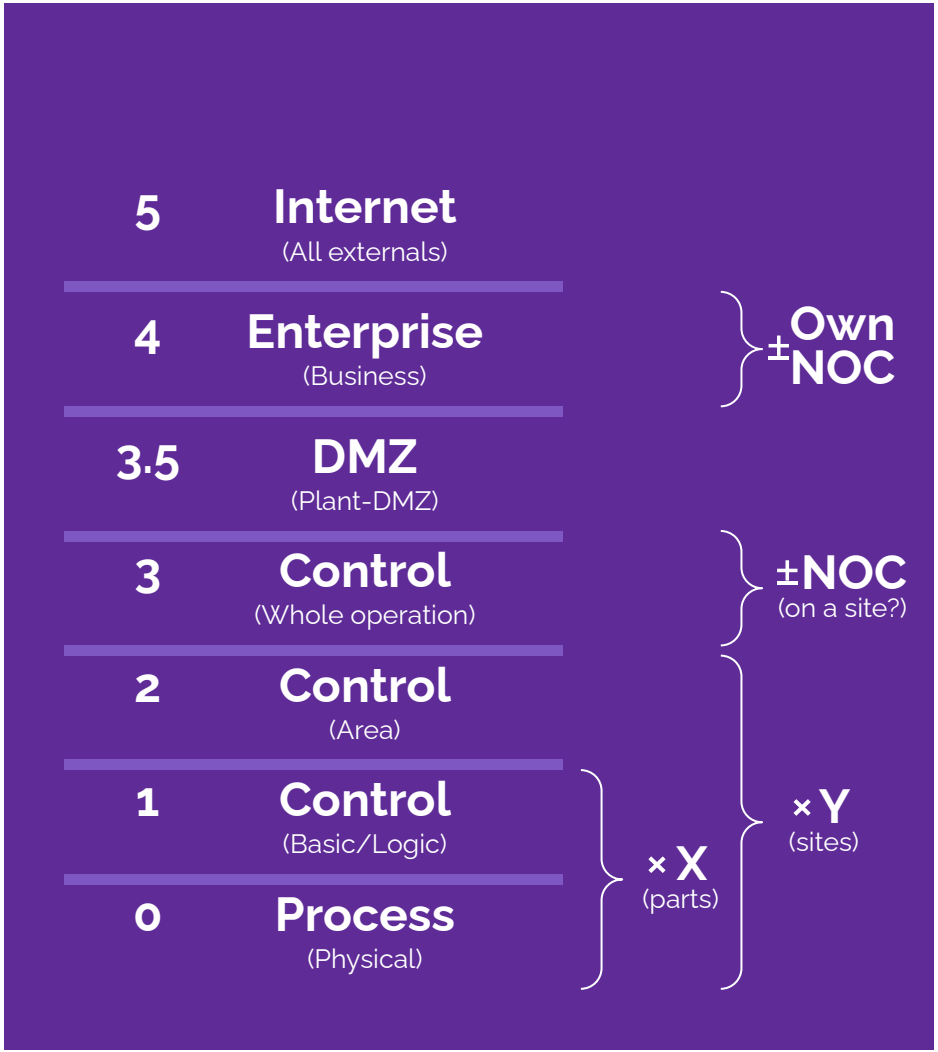
Intro to The Purdue Model

Zone/conduit architectural model.
Like a DMZ, scaled.



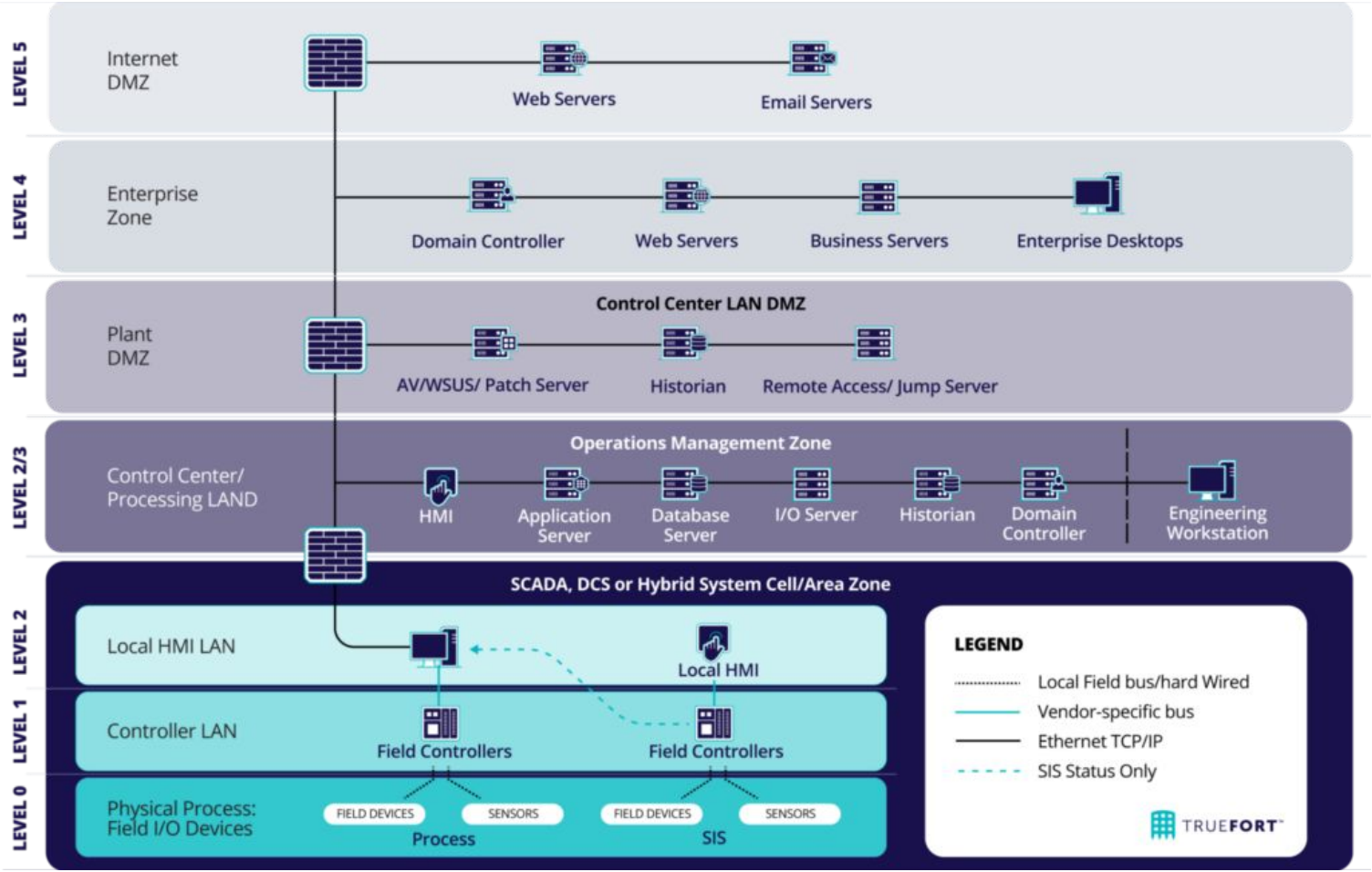
The Traditional DMZ:

Neither side can make contact directly with the other. Traffic must go via a waypoint in between.

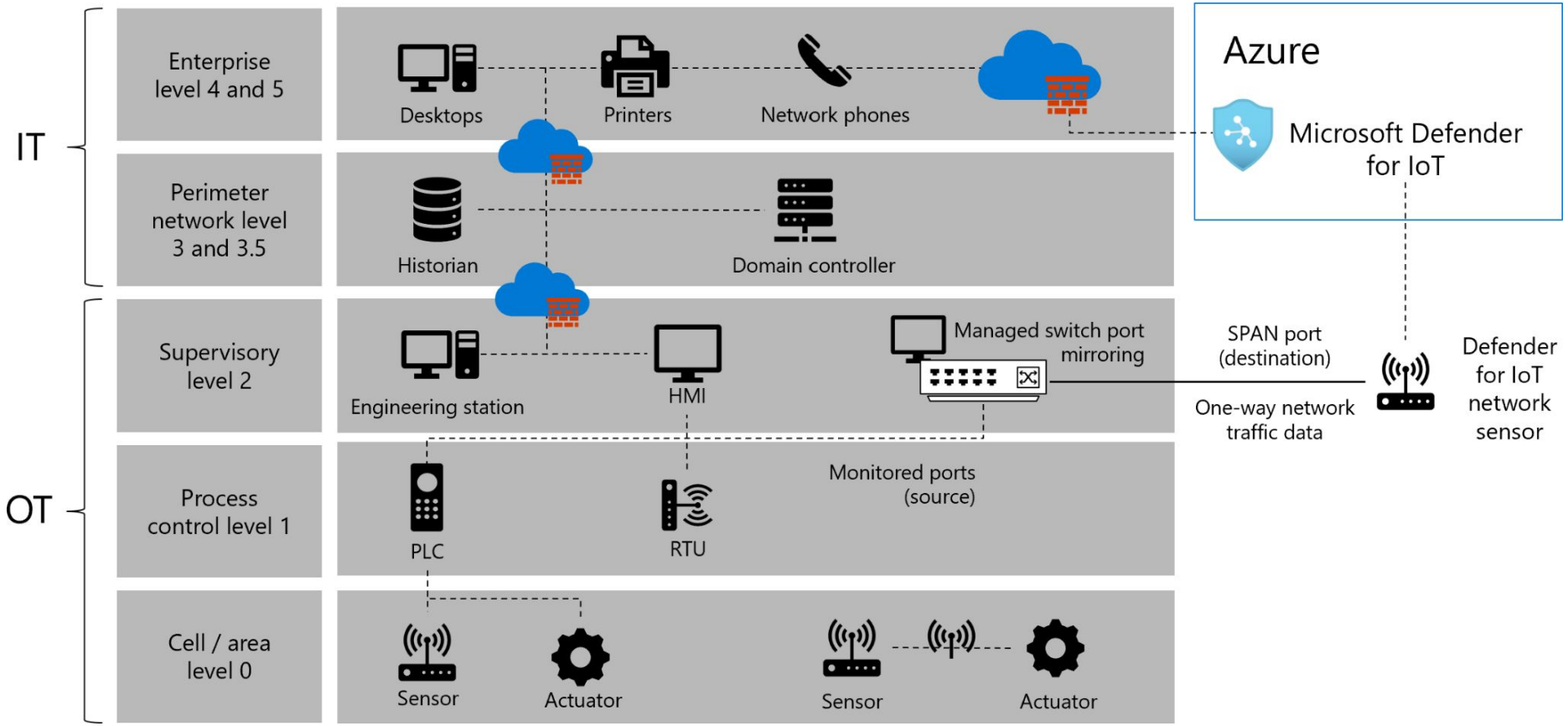


- Layered zone/conduit model.
- Many ways to skin the cat.
- More a guide than a rulebook.

- Important to understand & maintain the models **intent**...
- ...in a way that **makes sense**.



Truefort's representation of the Purdue Model as described in their TRUEFORT Purdue Model Whitepaper.



Microsoft's representation of the Purdue Model in its Defender for IoT Network Architecture Guide

Intro to ISO/IEC 62443

A set of more than a dozen comprehensive cybersecurity standards defining processes, requirements, & roles for securing ICS.

The standards:

- Are grouped into 4/5 ‘series’.
- Define *Maturity Levels.*
- Define *Roles.*
- Define *Security Levels.*
- Define *Security Requirements.*

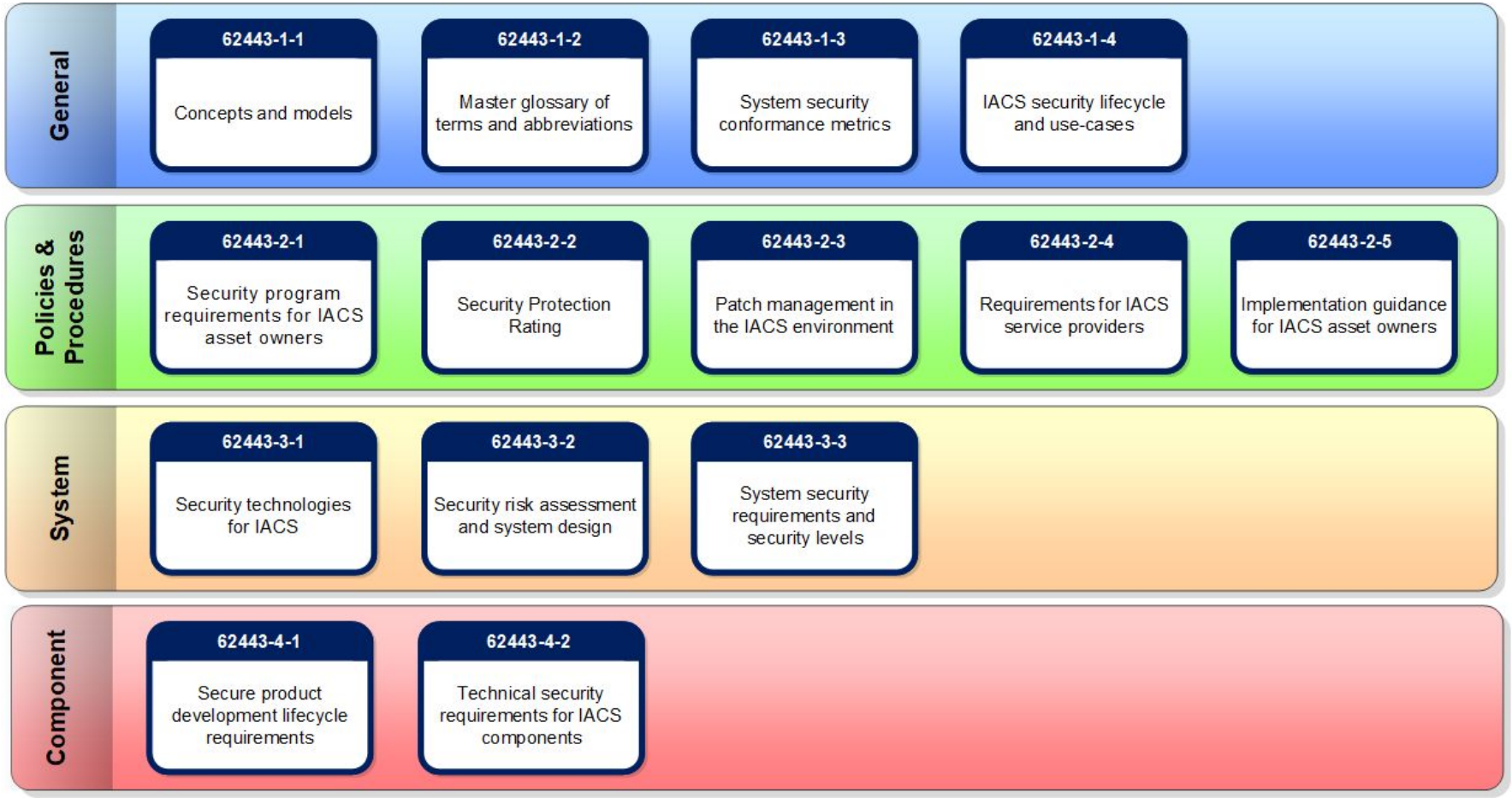


Diagram in the ISA article Structuring the ISA/IEC 62443 Standards explaining the structure and purpose of the standards.

Security Levels

Helps to understand & categorise the response (how far we go).

SL1 - Casual/Accidental Disclosure, opportunistic interference.

SL2 - Some skill, basic tools, intention.

SL3 - Good skill, specialist system knowledge, moderate resources.

SL4 - High skill, significant resources, high motivation.

Much more

ISA/IEC 62443 is produced by ISA99 committee, primarily consisting of industrial engineers.

Origin in the 90's (pre-Stuxnet era).

Still valid and being developed today.

Zones and Conduits

Foundational architecture model.

Supply-chain role definitions

Product supplier/integrator/operator responsibilities.

Secure Development Lifecycle requirements

Uplift for OT product security.

ICS-specific risk assessment method

Consistent SL assignment.

Life cycle engineering approach

Cybersecurity as part of the automation lifecycle.

NIS2

EUs baseline CS law for critical sectors - broader, stricter, and more enforceable

Breaks down into Important Entities and Essential Entities

OT explicitly in scope - no ambiguity

Stricter *minimum* requirements in OT

Mandatory incident reporting

Senior leaders personally accountable

Cybersecurity Trends

- Ransomware
- Geopolitical Conflict
- Regulatory Change
- Supply Chain
- Artificial Intelligence

Convergence

The ‘integration of (IT/OT) People Process & Technology.’

To the person with a hammer, every problem is a nail.

Especially to the person selling hammers.

Why Converge?

To improve business outcomes, e.g. cost, revenue, etc

To align or improve governance, organizational goals, or processes.

To enhance reliability, efficiency, safety, security..

Raw Data - Actionable Insights

Siloed Systems - Unified Visibility

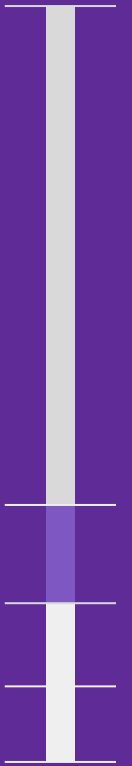
Manual Processes - Workflows

Invisible - Managed/Monitored

+ Business Opportunities

“The convergence of IT and OT is considered to be the 2nd largest cybersecurity vulnerability in 2025.”

Second behind AI/ML, as shown in the 2025 World Economic Forum Global Cybersecurity Outlook - Jan 2025.



WEF Global Cybersecurity Outlook, Jan 2025

History

Easy to see how we got here, but not a reason to stay.

1980s

Little Risk - No connection

Different platforms, isolated environments, separate buildings. Proprietary systems, minimal data sharing or connectivity.

1990s

Partial Protection by Obscurity

Networked to allow centralised operation. Most often proprietary devices with no native network capabilities. Knowledge boundaries growing wider.

2000s

OT Forgotten

OT platforms use IT protocols & systems. IT/OT boundaries start to blur. Cloud connects to IT. IT refresh cycles shortening, tech develops with pace, OT systems remain long-lived. Conflicts emerge between IT and OT.

Today

IT/Cloud Ubiquity

IT Tech ubiquitous in OT. Cloud explosion, proliferates in IT environments. ‘Anti-server-huggers’ deploy, pressure put on environments. Cloud and MVP commonly assumed as the default/the only approach.

"Convergence is just about replacing OT systems with IT systems."

"CONVERGENCE ONLY INVOLVES INTEGRATING SOFTWARE & SYSTEMS."

"Convergence is just a trend driven by marketing."

"Convergence is only relevant for large enterprises."

"Convergence is a one-time thing/project."

"Convergence [our product] solves [any/all] operational inefficiencies."

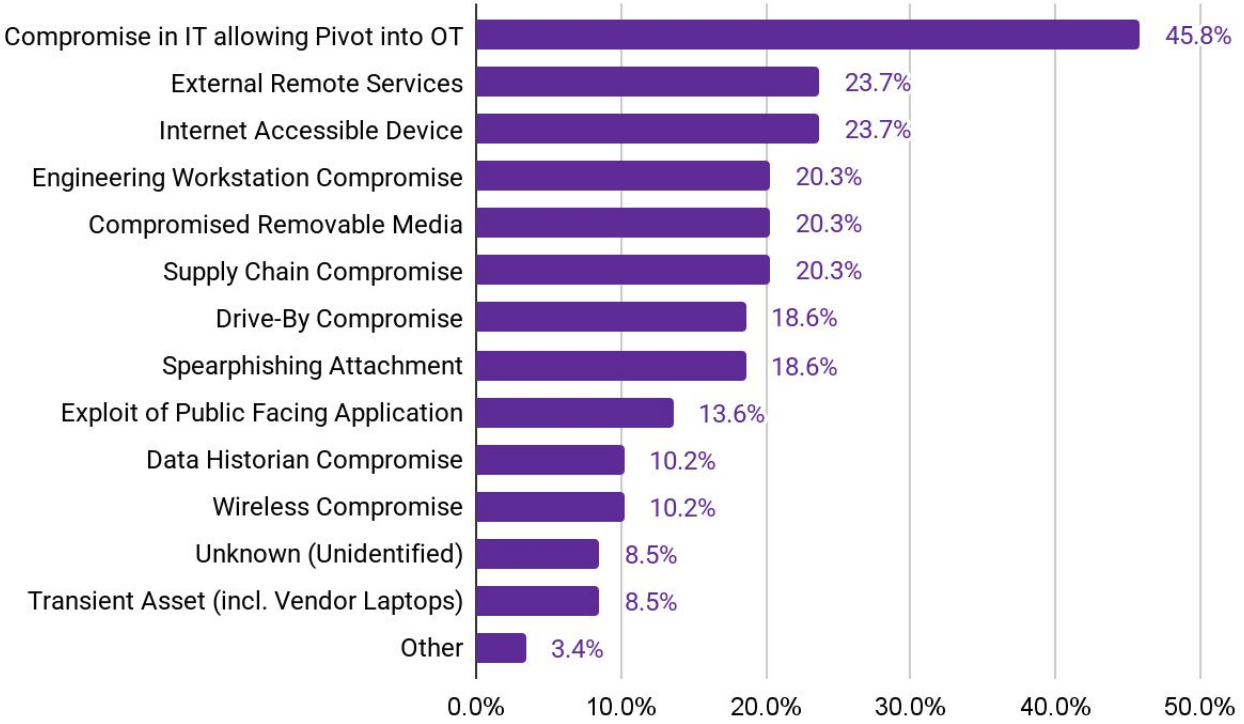
"Convergence means using the cloud." *or* ***"Maturity in OT means Convergence/Cloud"***

"Convergence is just a cost cutting measure."

"Convergence eliminates the need for specific expertise."

Initial Attack Vectors

"What were the initial attack vectors in your control systems incidents?"



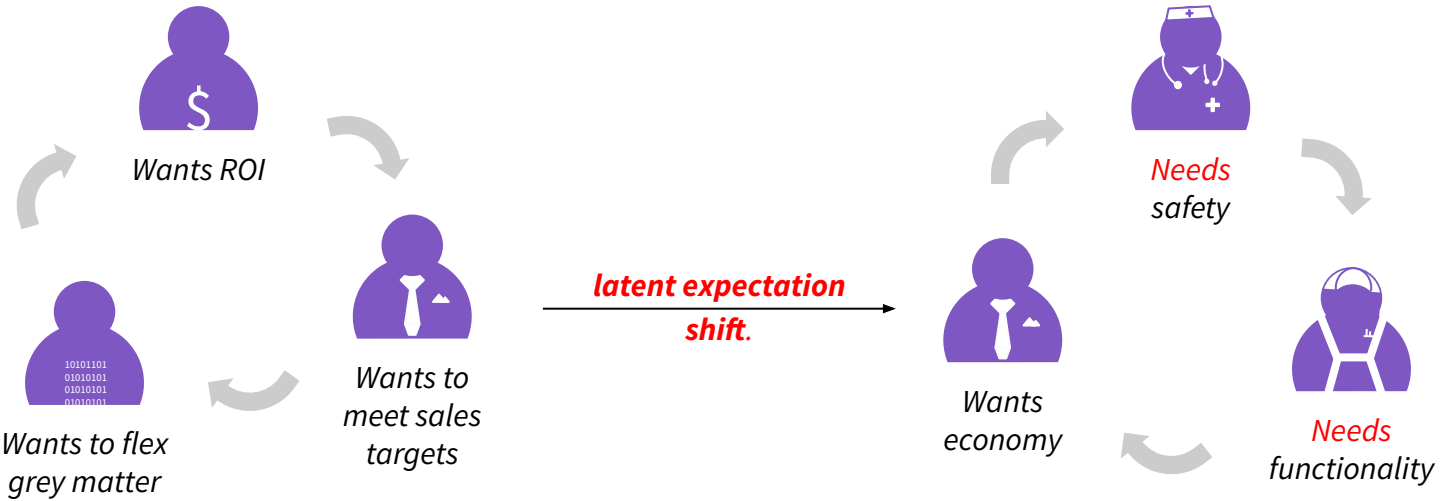
Responses from over 530 organisations responding to the SANS 2024 ICS/OT Survey: The State of ICS/OT Cybersecurity (Oct 2024)

MVP

A revolutionary idea, creeping inappropriately.

Shadow Risk

Evolution from 'POC' to 'Dependence' faster than its evolution from 'MVP' to 'mission-critical'.



IRL

Real world failures and contributing factors.

Crowdstrike

A subtle wakeup call, especially for OT and Critical Infrastructure.

Vendor Factors

- Cloud-only product.
- Liability limitations.
- Product did not want to include capabilities for on-premise/staging.
- Product includes capabilities for threat hunting teams to access clients.

Customer Factors

- Orgs implemented CS in ‘critical’ zones.
- Orgs were forced to compromise traditional models in order to use the product.
- Installation gave unchecked remote reach into critical zones.
- Orgs under-qualifying the loss of the systems in question.

Crowdstrike Incident 2004 (Wikipedia)

Cloudhopper

A warning challenging individual assumptions about 'cloud' services.

Vendor Factors

- Weak third-party access practices.
- Weak against APT.
- Supply chain dependencies.
- Missing MSP Segmentation.

Customer Factors

- High reliance/high trust of MSPs.
- Low oversight.
- Unchecked reach leading to lower protection afforded for MSP connectivity.

Operation Cloudhopper

Solarwinds

Launched ‘Supply Chain’ firmly into view. *“The most valuable by the ounce.”*

See the SUNBURST section of the Solarwinds Wikipedia article. (Robot and Frank.)

Often used in network equipment in both IT and OT environments. **Meta!**

Vendor Factors:

- Weak protection of build environment.
- Overly trusted code signing.
- Updates direct - no staggered rollout
- Huge blast radius.

Customer Factors:

- High privilege granted to monitoring systems
- Placement in IT/OT boundaries
- Limited segmentation, overconnected
- Limited analysis of trusted traffic for anomalies

Aquarium Hack

Innocuous ‘outbound-only’ IoT device was the weakest link.

Vendor Factors

- Cheap/poor security design.
- No updates.

Customer Factors

- Device connected to sensitive segment.
- Inadequate monitoring.
- Blind trust in ‘harmless’ equipment.

Smart Aquarium Hack

WWJD

Use new knowledge and wishful thinking.

Data Aggregation

An Internet Provider has new device with a large capacitor, allowing a ‘last gasp’ message. Aggregating this data could be very useful, eg, to a power company.

{practical}

Data about large scale power outages would be really useful to people like power companies.

Such data would be very useful for people with other motives too.

High Availability

Critical provider needs to participate in a nationwide scheme.

{practical}

IT approach

- Use dynamic routing/BGP.
- “Enough to run the internet!”

OT Approach

- Use static/tracked routes.
- “One less thing to go wrong.”

Cloud ZTNA

++Solution or ++Risk?

{practical}

School of Hard Knocks

The same {thing} does not necessarily apply to all circumstances

We might have impact/responsibility beyond our immediate visibility

The ones you don't see coming are the ones that catch you

Nobody thought it would happen, until it did

OT Priorities ≠ IT Priorities
Cloud ≠ Maturity
Cloud ≠ Security
Outbound only ≠ Safe

Adopt Risk Management
Context Matters

But How?

Use the resources available. (standards, etc!)

Don’t be afraid to get advice/ help/ second opinion.

Use Risk Management.

Take time & do homework.

Go back to basics:

- Zero trust principles
- BIA and Risk Management

Connectivity is one of the chief vectors of cyber incidents.

Incidents are often multifaceted and not always technical.

Links

Me:

/milkmansson
@milkmansson
milkmansson

Learning Resources:

[CISA's Virtual Learning Portal](#)
[Security Cert. Roadmap](#)