MASTER OF SCIENCE IN ENGINEERING

TSM_SecIndOpT

Securing OT-relevant aspects of SCADA, DCS & ICS (I) Version: 1.1

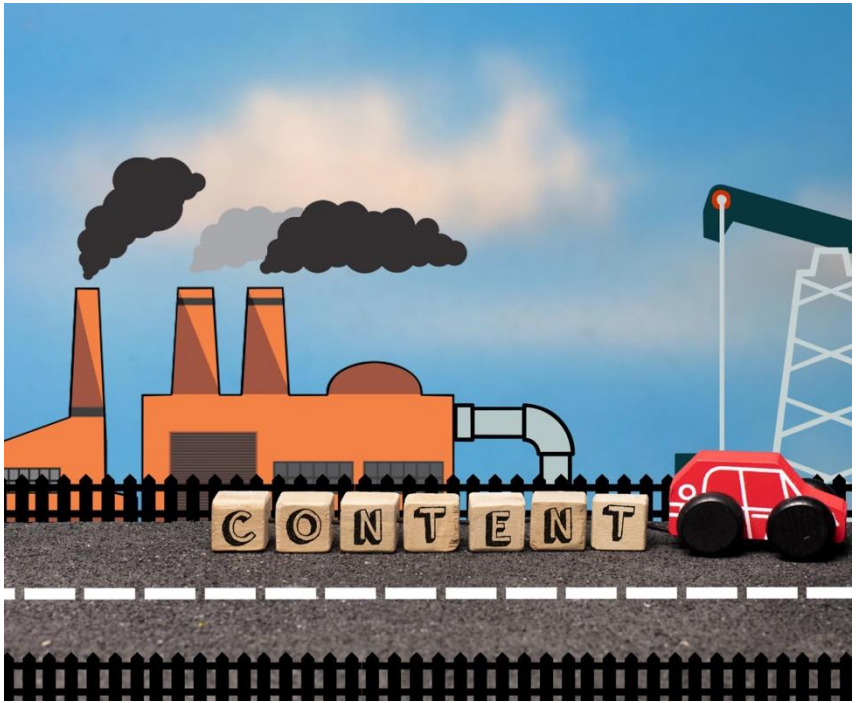
Luca Haab | 24.02.2025 | Cours MSE

Take away from the last time

Understanding Differences Between IT & OT

- IT focuses on data management, while OT focuses on physical processes
- IT systems prioritize confidentiality; OT systems prioritize availability and safety
- OT environments have stricter uptime requirements due to real-time operations

Key OT Threats



Differing Operational Priorities

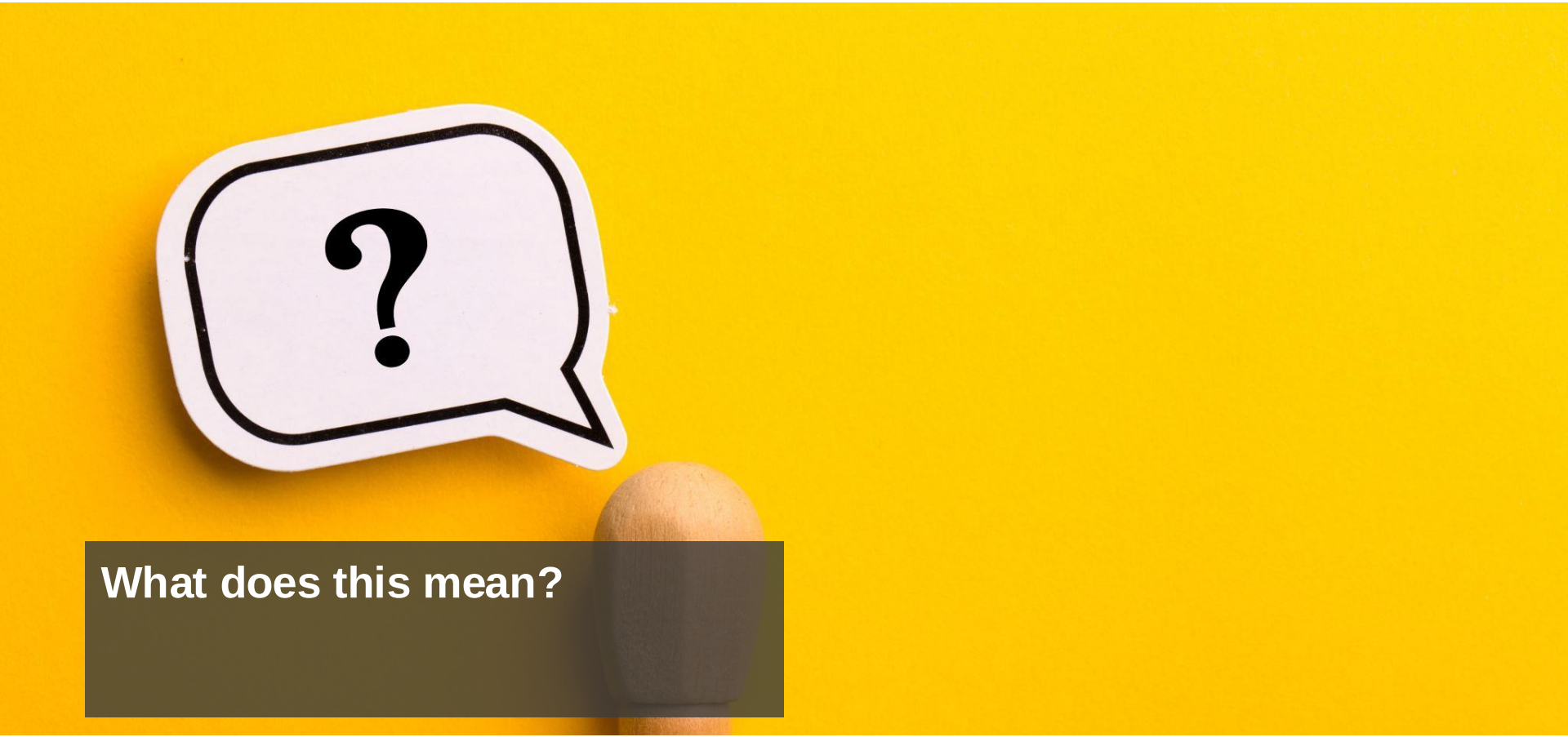
Operational Technology (OT) has unique priorities that differ significantly from Information Technology (IT), necessitating specialized security approaches.

Unique Risk Profiles

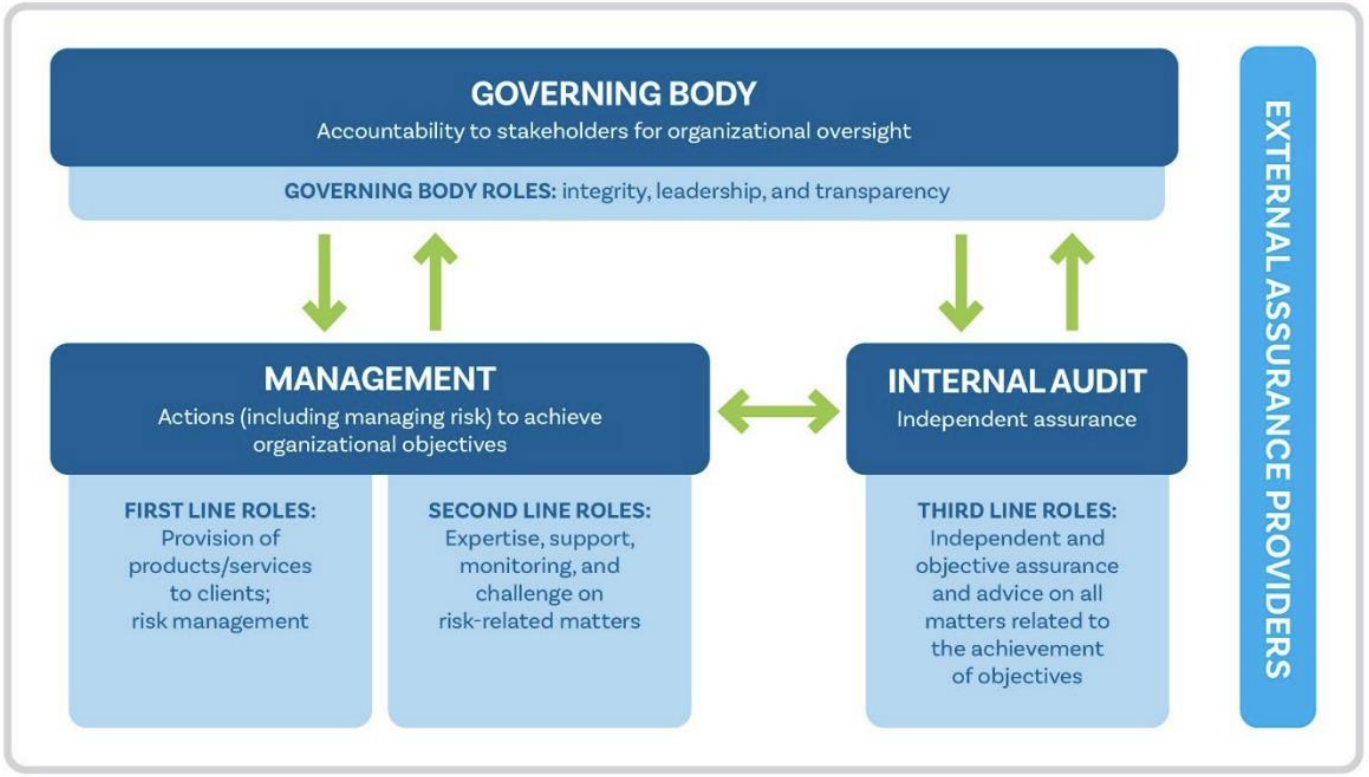
OT risk profiles are distinct, often involving critical infrastructure where security breaches can have severe consequences.

Consequences of Breaches

Security breaches in OT systems can lead to significant operational disruptions and safety hazards in critical infrastructure sectors.


What does this mean?

The overall organization is similar



Source: The Institute of Internal Auditors' Three Lines Model

Risk Management (should be known already ;-))

Risk definition

"The effect of uncertainty on your objective"*

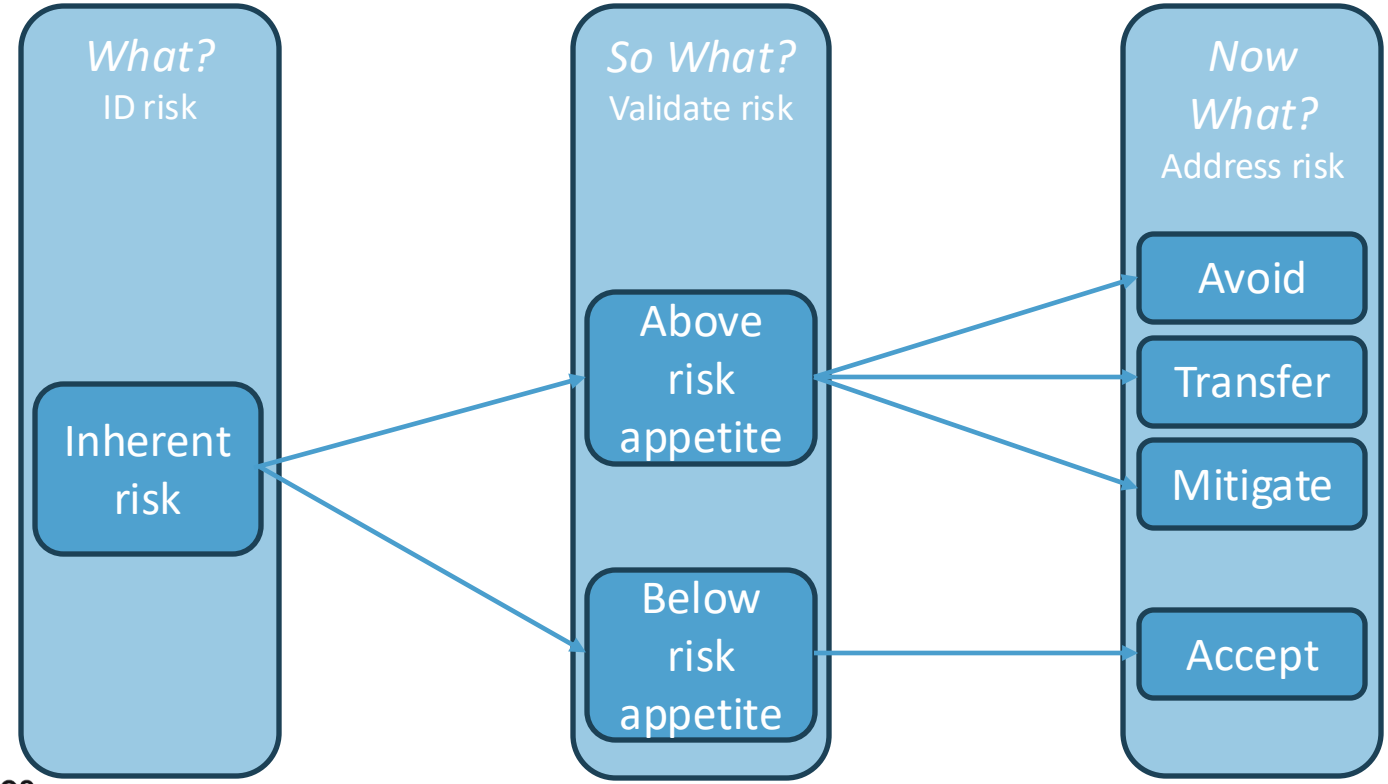
Repeatable

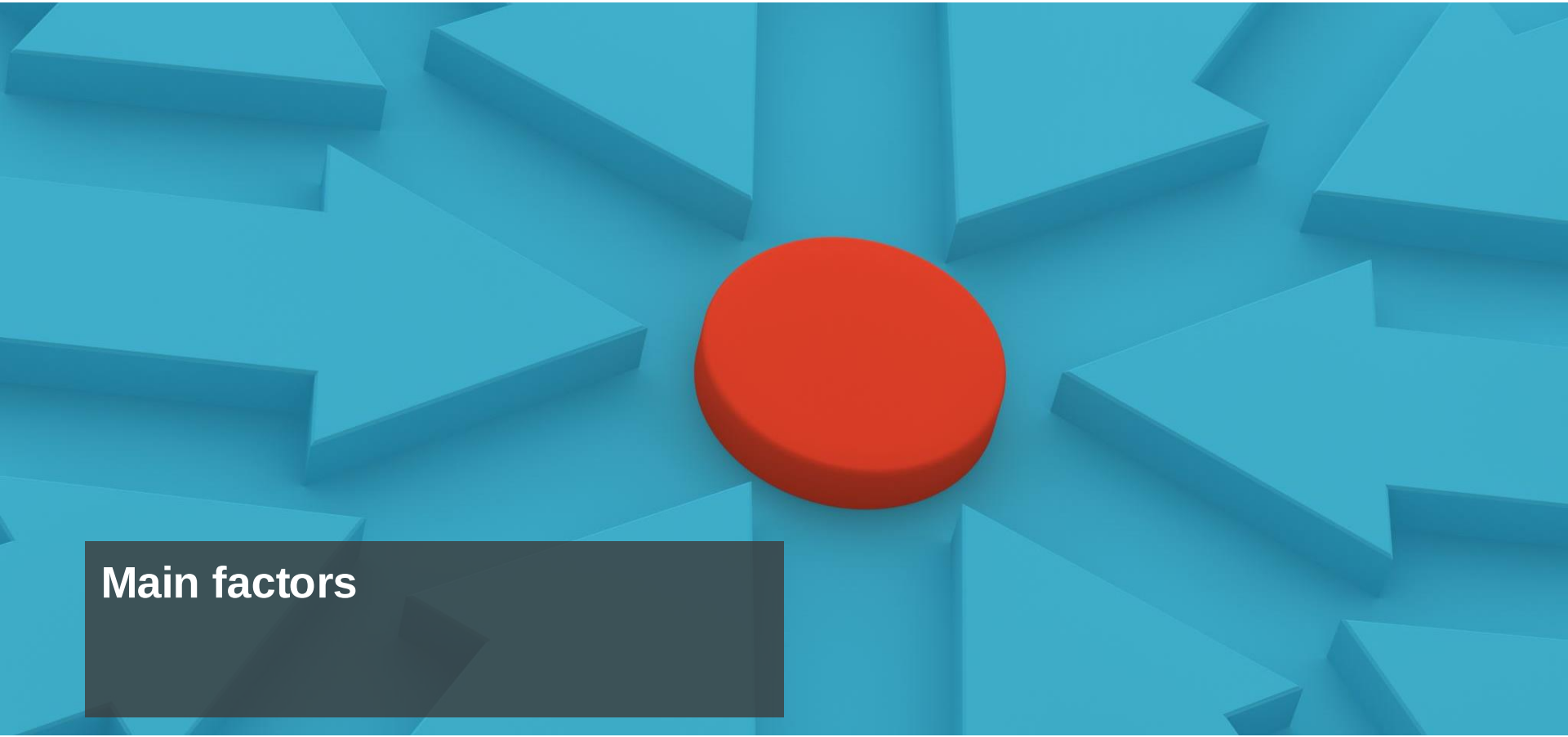
Scalable

Transferability

* : Source: ISO 31000

Risk Management: “What? So what? Now what?”





Main factors

Focus on operation

Results in systems that

- Have a long-lifecycle (10-20+ years)
- Deliver real-time and deterministic behaviour
- Are ruggedized and capable of running 24/7 in harsch conditions * and **
- Have strict SLA requirements (e.g. 99.99% vs 99.9999% availability – *“4 vs 6-nines”*)

* : industrial operational range is often specified as -40°C to 85°C (acc. IEC 60068-1)
** : while still respecting IEC product safety requirements

Cybersystems

- Generate injuries/casualties
- Cause physical damages

Other factors

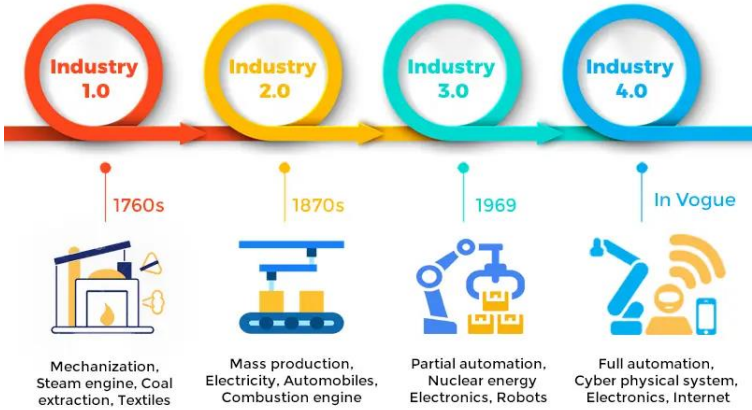
IT

"Change is essential for progress."

OT

"Never change a running system."

Source: https://i-flow.io/wp-content/uploads/2024/10/Infografiken-9.svg



Source: https://img.bevywise.com/images/help1.webp

Skill gaps (in IT/Cybersecurity)

Source: https://www.linkedin.com/pulse/miscommunication-breeds-misalignment-derailing-even-wager-psy-d--7sv6c

How to secure such systems

Security Architecture in OT Systems

Network Segmentation

Network segmentation is crucial for minimizing the attack surface in OT environments and isolating critical assets.

Defense-in-Depth Strategies

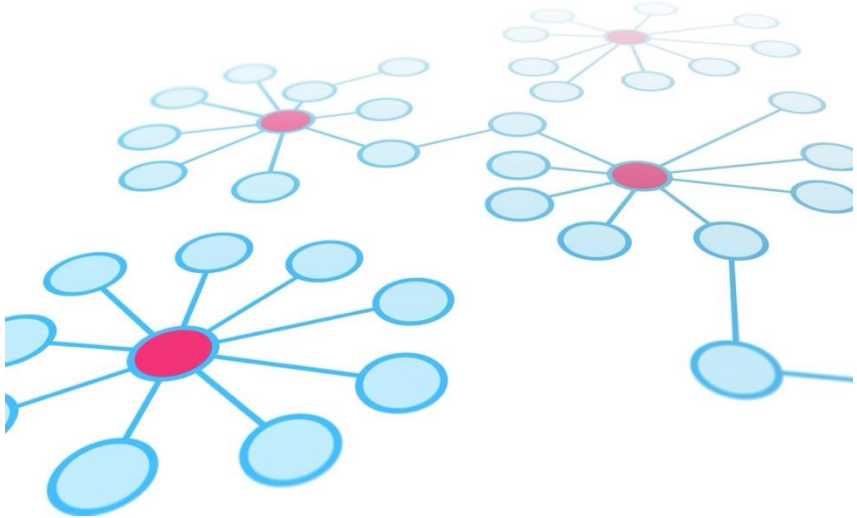
Implementing defense-in-depth strategies ensures multiple layers of security are in place, enhancing overall protection against threats.

Access Control Mechanisms

Access control mechanisms are vital for regulating who can access critical systems and data within an OT environment.

Secure Communication Protocols

Secure communication protocols are necessary to protect data integrity and confidentiality in OT communications.



Network Segmentation

Separation of OT and IT

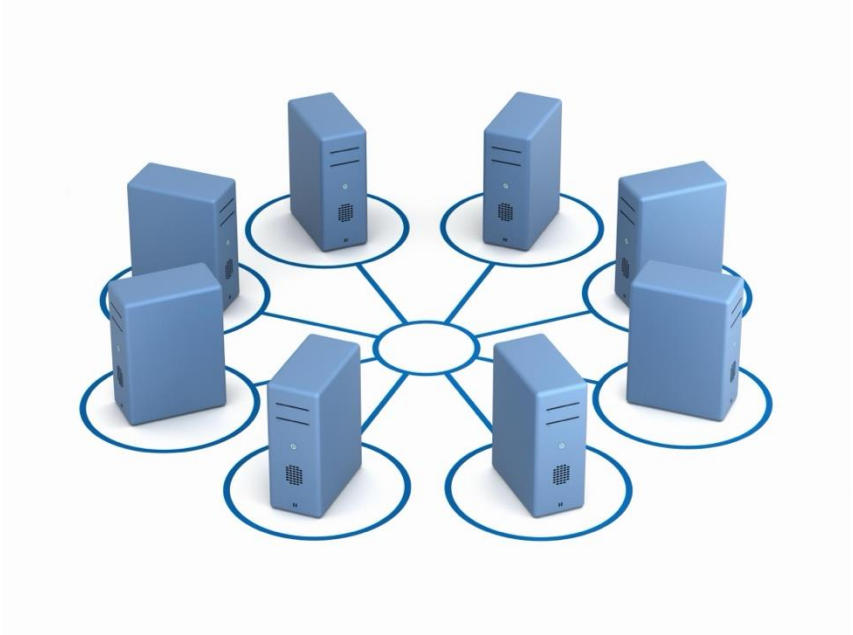
Separating Operational Technology (OT) from Information Technology (IT) networks enhances security and operational efficiency.

Limiting Lateral Movement

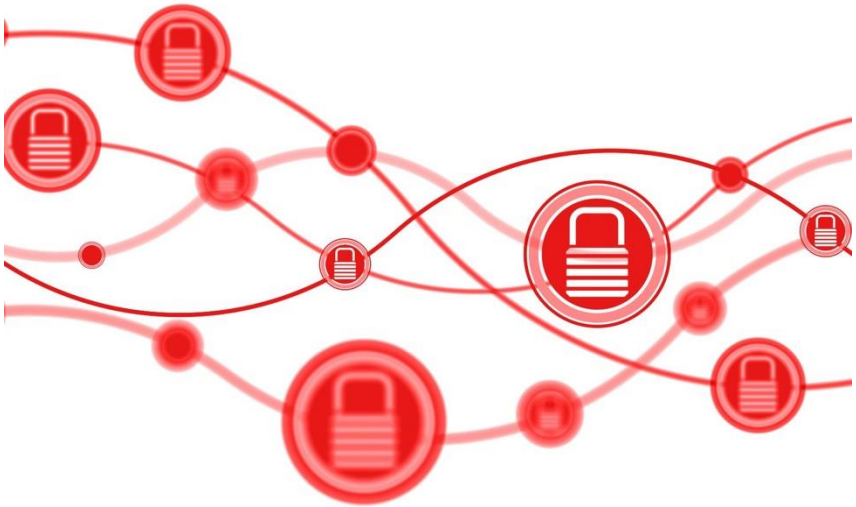
Effective network segmentation limits lateral movement of threats, safeguarding critical operational systems from potential attacks.

Reducing Unauthorized Access

By implementing network segmentation, organizations can significantly reduce the risk of unauthorized access to sensitive systems.



Defense-in-Depth



Multiple Security Layers

A defense-in-depth strategy utilizes various security measures to create a robust protection framework.

Firewalls

Firewalls act as a barrier between trusted and untrusted networks, preventing unauthorized access.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) monitor network traffic for suspicious activities, providing alerts for potential threats.

Data Encryption

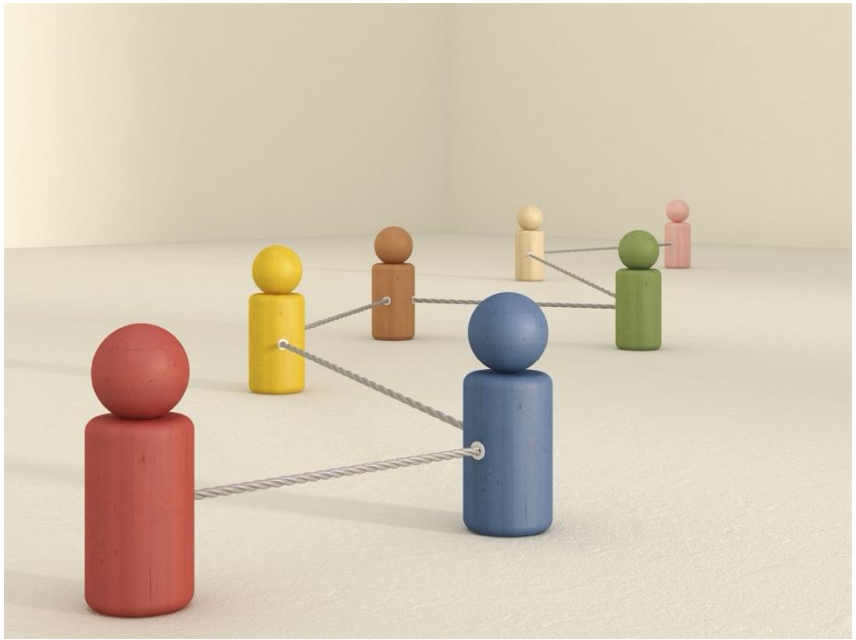
Encryption secures sensitive data, ensuring that it remains confidential even if intercepted.

Introduction to the Purdue Model (PERA)

- The Purdue Model* provides a framework for securing industrial control systems.
- It outlines the interaction between IT and OT environments.
- Understanding the model is essential for effective cybersecurity strategies.
- Facilitates better communication between IT and OT teams.
- It aims to reduce the risk of cyber threats to critical infrastructure.

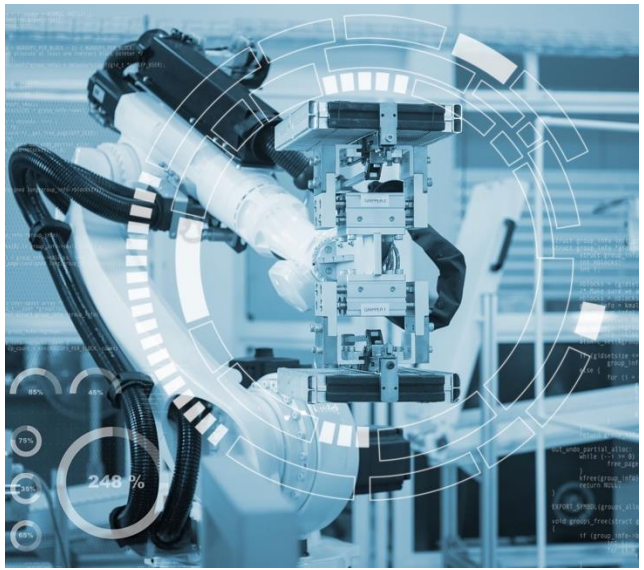
*: by Prof. Theodore J. Williams (see copy of the paper on the course website)

Overview of the Purdue Model Levels



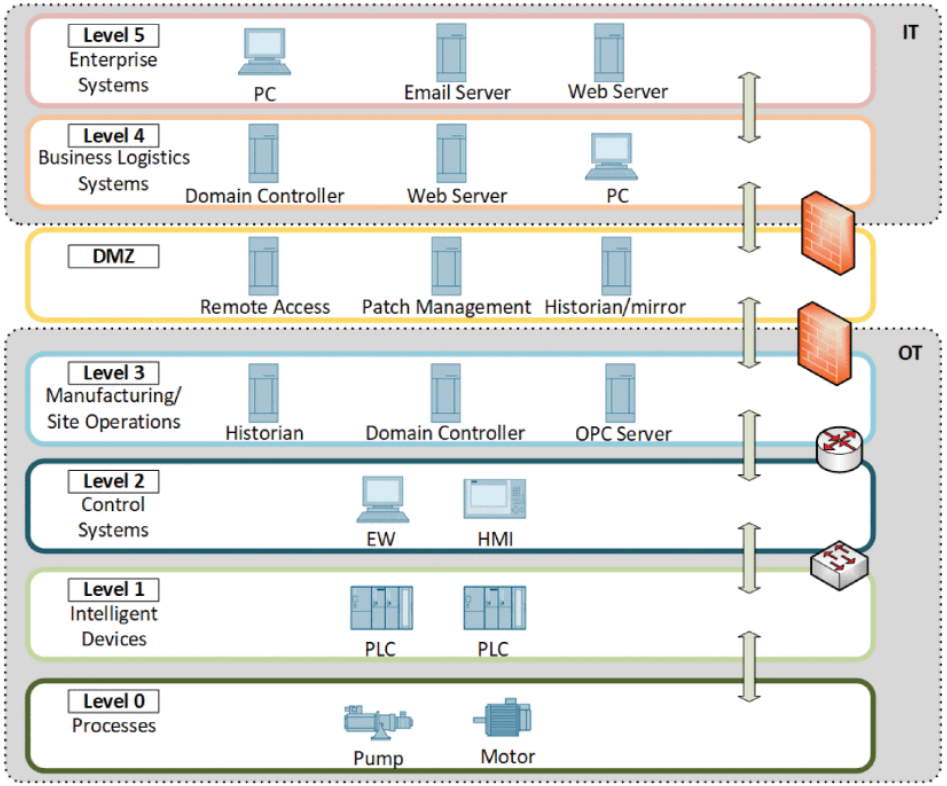
- The model consists of five distinct levels, each with specific functions.
- Levels range from enterprise systems to field devices.
- Each level has unique security requirements and risks.

In-Depth Look at the Purdue Model Levels



- Level 0: sensors, motors, pumps and valves. That is, instruments whose purpose is to provide sensing or actuating capabilities.
- Level 1: Intelligent devices that sense, monitor, and control the physical processes. It comprises control devices such as PLCs and Safety Instrumented System (SIS) controllers.
- Level 2: Control systems used for supervising and monitoring the physical processes. Among others, this level includes HMIs and SCADA.
- Level 3 manufacturing/site operations systems used to manage the production workflow for plant-wide control. Devices typically found in this level are the Data Historians, Microsoft Active Directory Domain Controllers and file servers.
- DMZ : acts as a secure buffer between the ICS network and external networks, housing security devices like firewalls and IDS/IPS. Proxy servers, database replication servers, and remote access servers are typical entities at this extra level.
- Level 4: enterprise network used for production and resource data exchange for business-to-business, and business-to-customer purpose services.

Purdue Model – an example



Source: https://ieeexplore.ieee.org/document/9638617

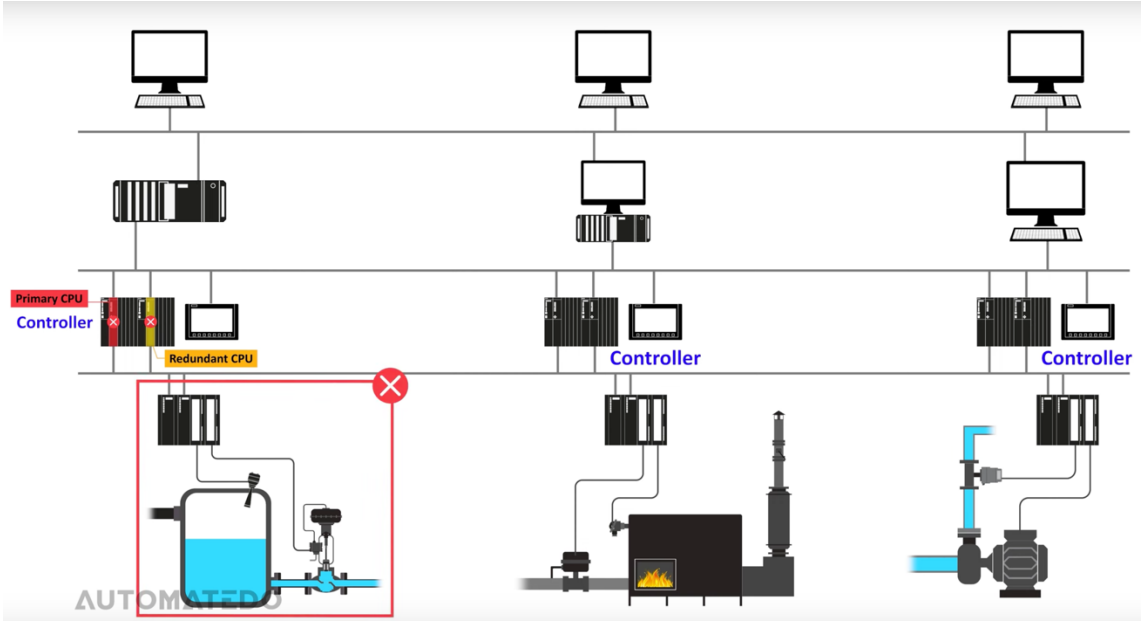
Terms – Information Control System

"An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes."

What is shown in the Purdue Model

Term – Distributed Control System

" In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit."



Purdue Level 3

Source: https://www.youtube.com/watch?v=WyIRpfBQif4

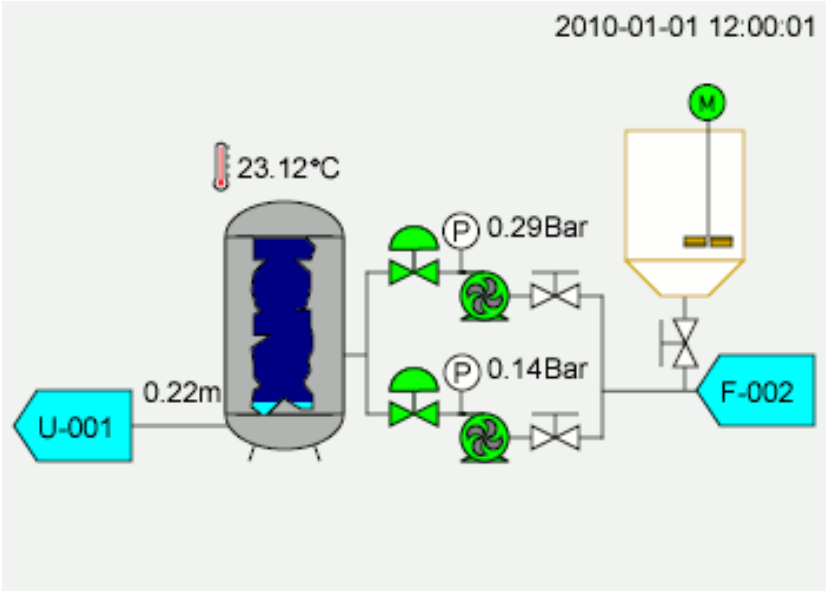
Source: https://csrc.nist.gov/glossary/term/dcs

- Note: Distributed is sometimes replaced by Decentralized

Terms – Supervisory Control and Data Acquisition

"A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave and satellite."

Source: https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition



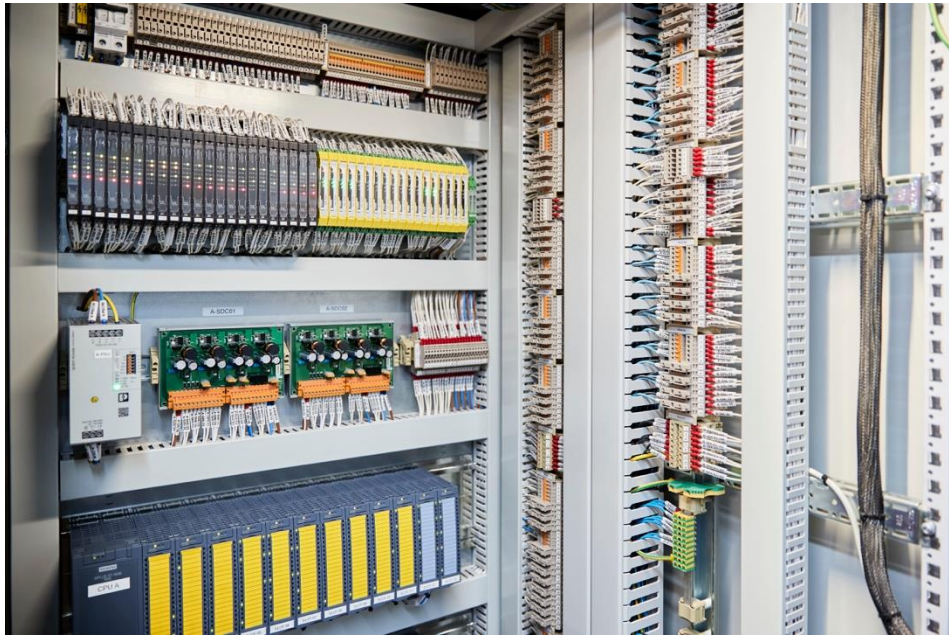
Source: https://en.wikipedia.org/wiki/SCADA

Purdue Level 2

Terms – Programmable Logic Controller

"A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing."

Source: https://csrc.nist.gov/glossary/term/programmable_logic_controller



Source: https://www.semcomaritime.com/hubfs/PLC_20210421_Semco_102.jpg

Purdue Level 1

Terms – Remote Terminal Unit

"A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs."

Source: https://csrc.nist.gov/glossary/term/remote_terminal_unit

Source: https://www.hitachienergy.com/br/pt/products-and-solutions/substation-automation-protection-and-control/products/remote-terminal-units/rtu500-series-function-and-software

Purdue Level 1

Terms - Intelligent Electronic Device

In the electric power industry, an intelligent electronic device (IED) is an integrated microprocessor-based controller of power system equipment, such as circuit breakers, transformers and capacitor banks.

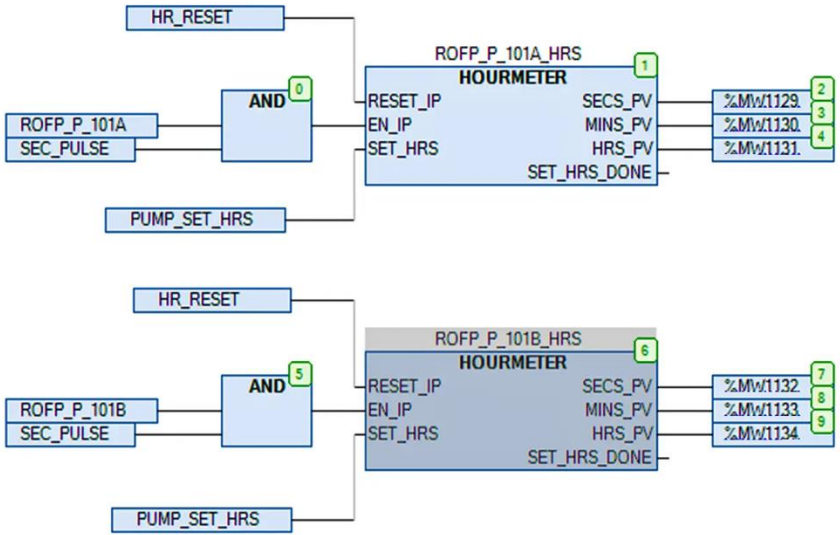
Source: https://en.wikipedia.org/wiki/Intelligent_electronic_device

Source: https://www.hitachienergy.com/products-and-solutions/substation-automation-protection-and-control/products/protection-and-control/relion-product-family/relion-670-series

Purdue Level 1

Terms – Function Block Programming

Part of IEC 61131-3



Source : https://instrumentationtools.com/user-defined-function-blocks-in-plc/

"The function block diagram (FBD) is a graphical language for programmable logic controller design that can describe the function between input variables and output variables. A function is described as a set of elementary blocks. Input and output variables are connected to blocks by connection lines."

Source: https://en.wikipedia.org/wiki/Function_block_diagram

A few considerations

Devices in Level-0 and 1 are ruggedized, low-power, fanless devices operating 24/7 in harsch conditions that have a very long-lifecycle (10-20+ years) and deliver real-time and deterministic behaviour…

Do you see any challenges?

Source: https://wordclouds.ethz.ch/

An example

gehealthcare.de/security

Investoren Karriere

GE HealthCare Produkte Service Weiterbildung Fachbereiche News & Stories Über uns Kontakt

D

Product: VxWorks | Product Version: VxWorks 6.9 | Status: All | ID: Enter Vulnerability ID

Year: 2025 | Keyword: Enter keyword... | Search | Reset

GE Healthcare Coordinated Vulnerability

dium vulnerabilities within the TCP/IP stack

on-critical vulnerabilities, CVE-2019-12255

depth assessments by internal GE Healthcare
cluding validated patches and patch

Healthcare Product Security Portal

Showing 50 of **6673** entries | Login to export | 1 2 3 4 5 ... 133 ›

ID	Description	Priority	Modified date	Fixed Release
CVE-2025-27218	Sitecore Experience Manager (XM) and Experience Platform (XP) 10.4 before KB1002844 allow remote code execution through insecure deserialization.	--	Feb 20, 2025	n/a
CVE-2025-27113	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a NULL pointer dereference in xmlPatMatch in pattern.c.	--	Feb 18, 2025	n/a
CVE-2025-27100	lakeFS is an open-source tool that transforms your object storage into a Git-like repository. In affected versions an authenticated user can crash lakeFS by	--	Feb 21, 2025	n/a

Digital Radiographic System powered by Helix™

Sources: GE Healthcare Discovery XR656HD Product Datasheet, https://www.gehealthcare.com/services/lifecycle-management/product-security-portal/security, https://www.gehealthcare.de/security, https://support2.windriver.com/index.php?page=cve&on=list&show=50&product_id=14&product_version%5B%5D=16&cve_id_filter=&s=&submit=#list

Common ICS security challenges

Legacy Protocols and Systems

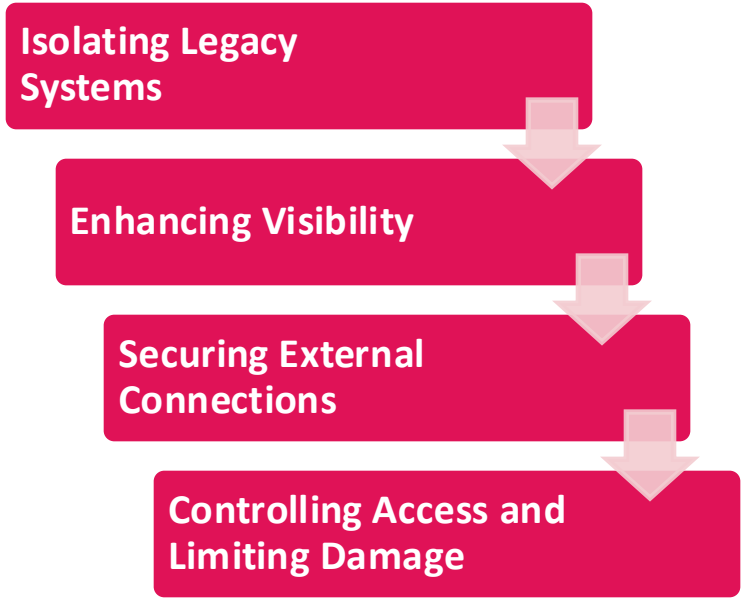
Limited Visibility and Patch Management

Convergence of IT and OT

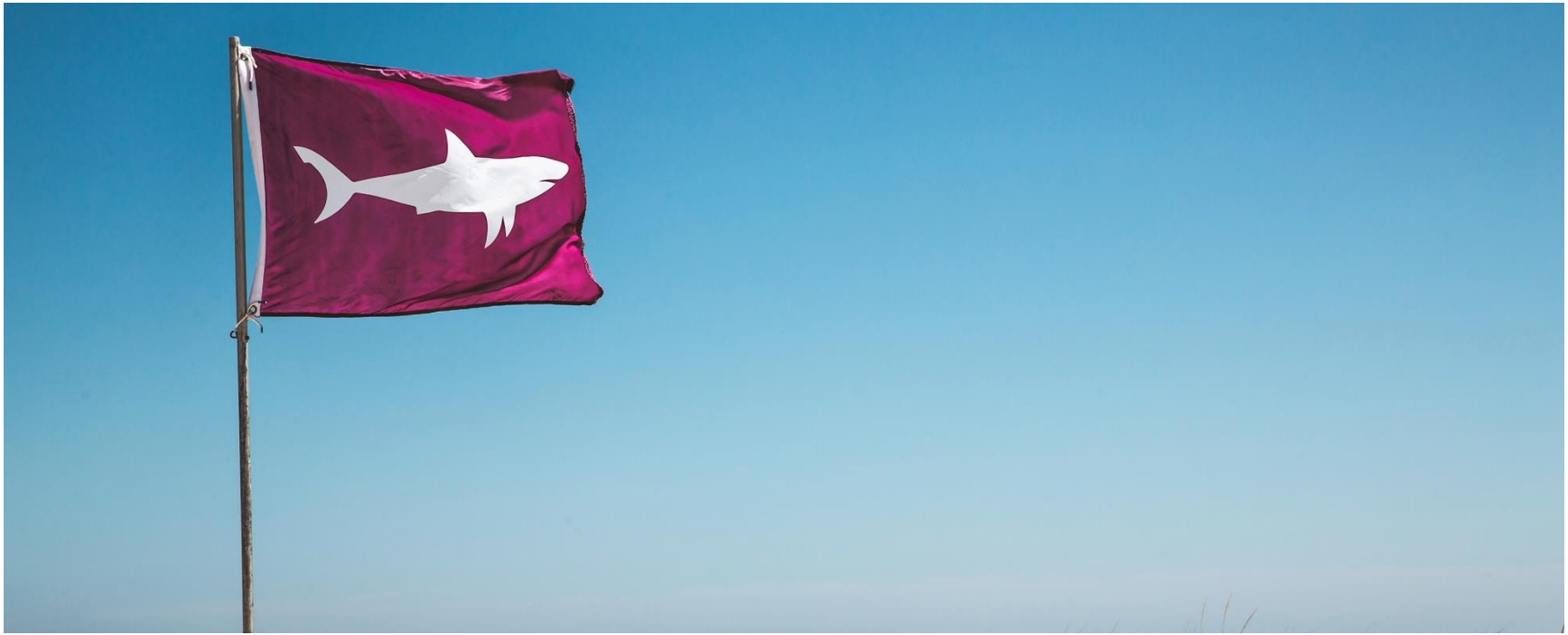
Supply Chain Risks

Human Error

Purdue's positioning:



Cyberattacks



Cyberattacks (I)

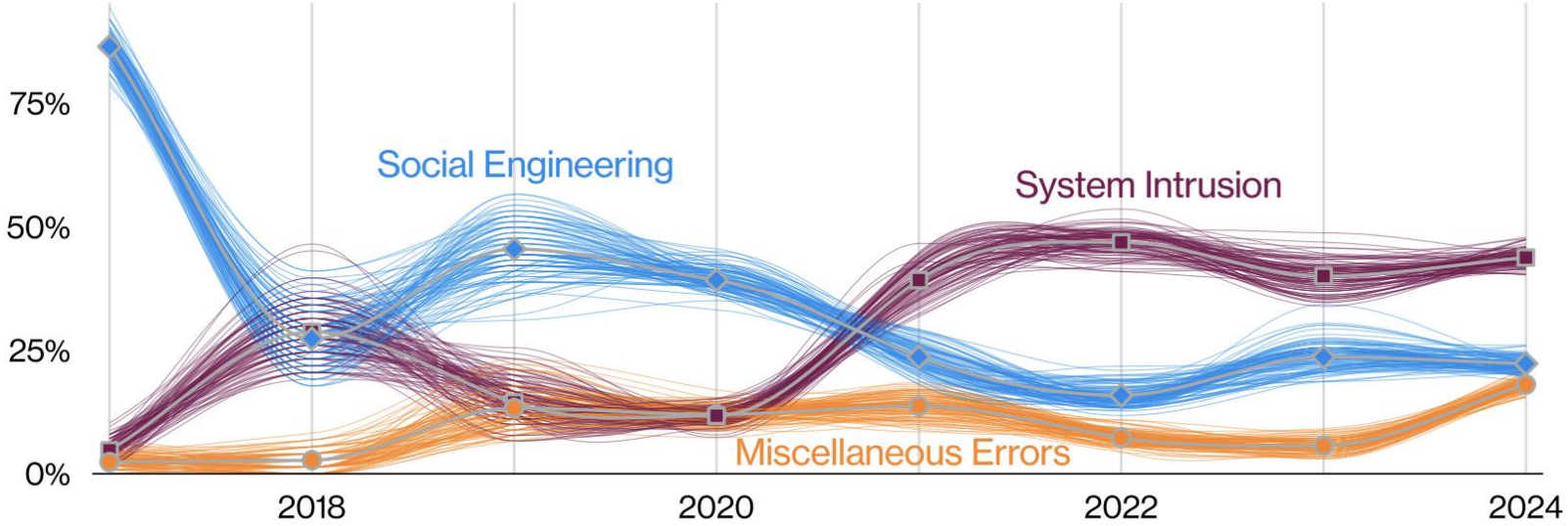
IBM's X-Force Threat Intelligence Index 2024

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

Source: https://www.ibm.com/downloads/documents/us-en/107a02e952c8fe80

Cyberattacks (II)



System Intrusion

These are complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying ransomware.

Social Engineering

This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.

Miscellaneous Errors

Incidents where unintentional actions directly compromised a security attribute of an information asset fall into this pattern. This does not include lost devices, which are grouped with theft instead.

Source: 2024 Data Breach Investigations Report, Manufacturing Snapshot, Verizon Business

Source: https://img.itch.zone/aW1nLzIzNTkyMDEucG5n/original/HXrjt2.png