OT/ICS Cybersecurity

Securing Critical Infrastructure in the Age of IT/OT Convergence & AI

Energy | Oil & Gas | Water | Transport | Healthcare | Utilities

Prepared by

Emad Shanab, P. Eng.

AGENDA

Talk Structure

01

OT & ICS Fundamentals

Architecture, components, Purdue model, CIA vs AIC triad

02

IT/OT Convergence Challenges

Digital transformation, legacy integration, expanding attack surface

03

Threat Landscape & Risk Vectors

Threat actors, ransomware, supply chain, case studies

04

Securing Legacy Industrial Systems

Practical strategies, compensating controls, segmentation, standards

05

Cyber Resilience: Industry 4.0 & AI

AI threats & defenses, digital twins, resilience frameworks

GLOSSARY

Key Terms & Definitions

Essential vocabulary for navigating IT/OT cybersecurity

OT (Operational Technology)

Hardware and software that monitors or controls physical industrial equipment, processes, and events in real time.

ICS (Industrial Control System)

General term for control systems used in industrial production — includes SCADA, DCS, PLCs, and related components.

SCADA

Supervisory Control and Data Acquisition — remote monitoring and control of geographically dispersed industrial processes.

DCS

Distributed Control System — continuous process control in a single plant; controllers distributed near physical processes.

RTU

Remote Terminal Unit — field devices executing real-time control logic and relaying sensor data.

HMI

Human-Machine Interface — the operator-facing screen showing process status, alarms, and controls.

SIS

Safety Instrumented System — an independent emergency shutdown system that brings processes to a safe state.

Industry 4.0

Convergence of IT, OT, IoT, AI, cloud, and analytics into smart, interconnected manufacturing and infrastructure.

PLC

Programmable Logic Controller field devices executing real-time control logic and relaying sensor data.

Air Gap

Physical or logical isolation between OT and IT — historically relied upon, increasingly broken by modern connectivity.

SECTION 01

ICS Components & Architecture

The building blocks of industrial control systems

SCADA

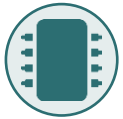
Supervisory Control & Data Acquisition

Monitors thousands of remote sites. Gathers data from RTUs/PLCs, provides operator HMI, logs historian data.

DCS

Distributed Control System

Process-level automation within a single facility. Controllers near equipment for real-time closed-loop control.



PLC

Programmable Logic Controller

Rugged field device running ladder logic. Reads sensors, executes control, drives actuators in milliseconds.

HMI

Human-Machine Interface

Operator touchscreen or workstation showing real-time graphics, alarms, and control inputs. Often Windows.

SIS

Safety Instrumented System

Independent safety layer (IEC 61511). Triggers emergency shutdown to prevent catastrophic failure.

RTU

Remote Terminal Unit

Remote field data unit. Converts sensor signals to digital, communicates over serial/IP to SCADA master.

Common OT / ICS Protocols at a Glance

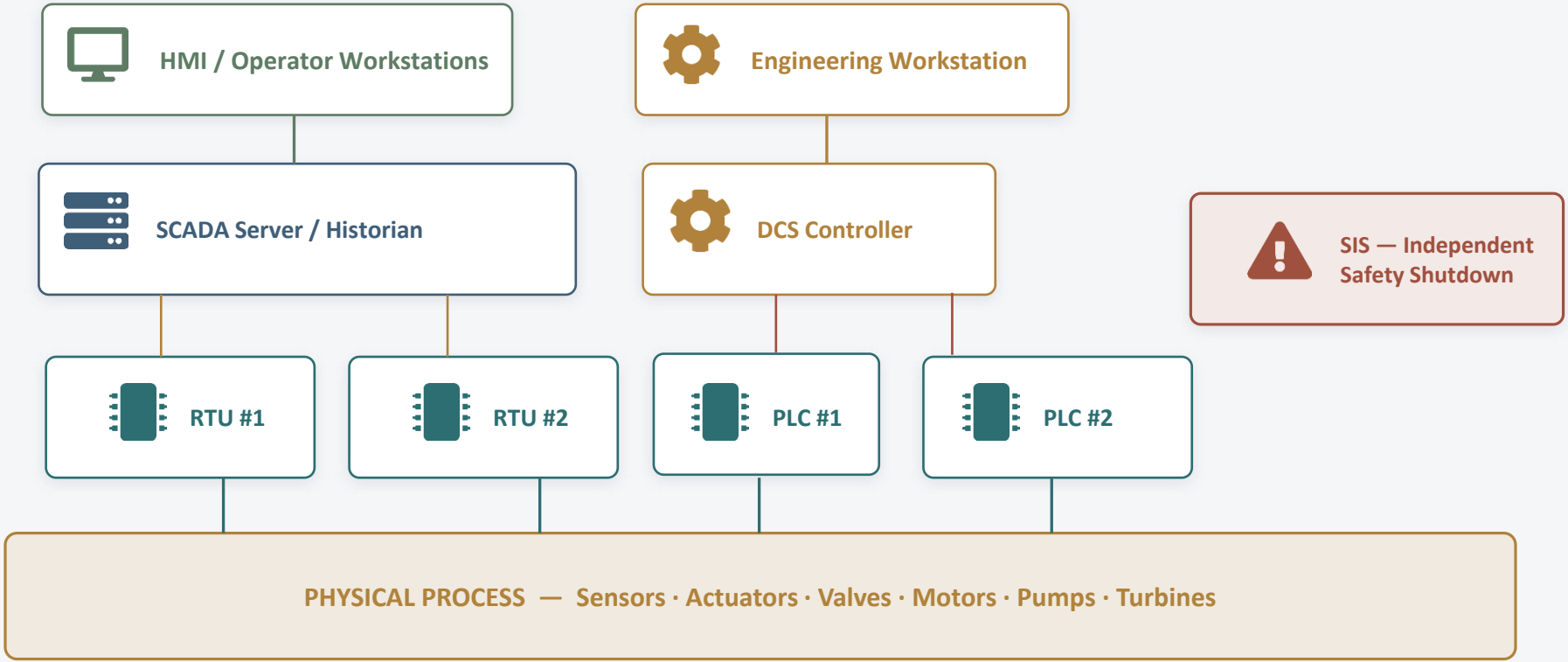
What each is for, the ports it uses, and its core security weakness

Protocol	Primary Use	Port(s)	Core Cybersecurity Weakness
Modbus TCP	SCADA ↔ PLC register read/write; the most widely used ICS protocol	**TCP 502**	No authentication or encryption — any node on the network can issue commands
DNP3	SCADA telemetry in electric & water utilities	**TCP/UDP 20000**	No native auth/encryption; Secure Auth (IEC 62351) rarely enabled; replay-prone
EtherNet/IP (CIP)	Rockwell / Allen-Bradley PLC and I/O communication	**TCP 44818 · UDP 2222**	No auth/encryption; CIP commands can stop, start, or reprogram the CPU
PROFINET	Siemens real-time device & I/O networks	**Layer 2 · UDP 34962–34964**	Layer-2, unauthenticated; DCP spoofing enables device takeover
S7comm / S7+	Siemens S7 PLC programming & control	**TCP 102**	No auth (S7comm) — abused by Stuxnet; S7comm-plus anti-replay has been broken
IEC 61850 (MMS / GOOSE)	Electrical substation automation	**TCP 102 · GOOSE/SV = L2**	GOOSE & Sampled Values unauthenticated; spoofing/replay; IEC 62351 seldom deployed
IEC 60870-5-104	European power-grid SCADA telecontrol	**TCP 2404**	Cleartext with no auth or encryption; vulnerable to spoofing and replay
OPC UA	Modern vendor-neutral IT ↔ OT data exchange	**TCP 4840**	Secure by design, but often deployed with security set to “None” (legacy OPC = DCOM/135)
BACnet/IP	Building automation & HVAC control	**UDP 47808**	No authentication; broadcast-heavy; susceptible to spoofing and denial-of-service

Takeaway: *Most OT protocols predate modern security and assume a trusted, isolated network — so segmentation, monitoring, and access control are the primary defenses, not protocol-level security.*

How ICS Components Interconnect

Data flows from physical sensors through control layers to operator screens



CIA Triad vs. AIC Triad

Why OT inverts the traditional IT security priority model

IT Security Model **OT Security Model**

The Purdue Enterprise Reference Architecture

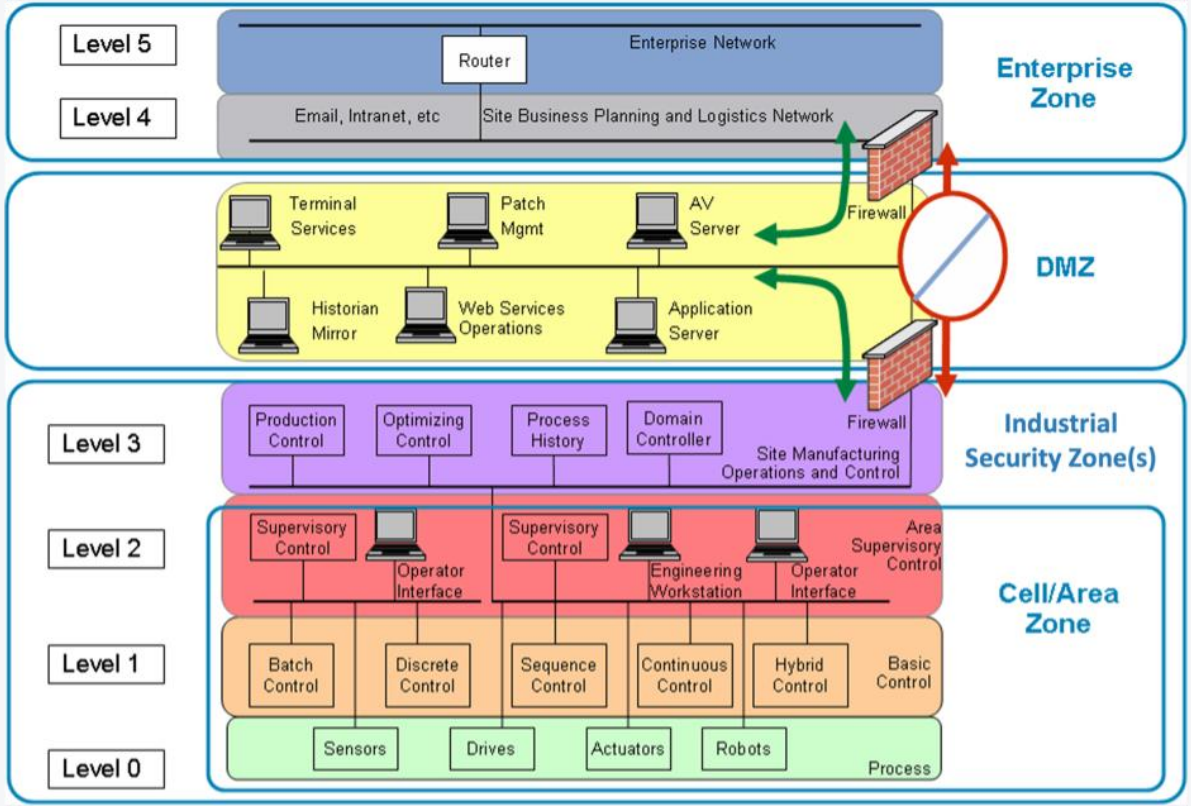
Level 5	**Enterprise Network**	ERP, email, internet	*Corporate LAN · Cloud*
Level 4	**Business Planning**	MES, plant scheduling	
DMZ Level 3.5	**Industrial DMZ**	Secure remote access, Jump servers, AV, Patch Management	**Critical security boundary**
Level 3	**Site Operations**	Historian, Alarm Management, OT Network Management	*SCADA / DCS servers*
Level 2	**Supervisory Control**	HMI, engineering stations	
Level 1	**Basic Control**	PLCs, RTUs, controllers	*Modbus / DNP3*
Level 0	**Physical Process**	Sensors, actuators, motors	*4–20mA · fieldbus*

IT ZONE

DMZ

OT ZONE

The Purdue Enterprise Reference Architecture



IT vs. OT: Fundamentally Different Worlds

Dimension	Information Technology (IT)	Operational Technology (OT)
Primary Goal	Data processing & business logic	Physical process control & safety
Security Priority	Confidentiality first (CIA)	Availability first (AIC)
System Lifecycle	3–5 years (frequent refresh)	15–30+ years (rarely replaced)
Patching	Regular, automated, tested	Infrequent; requires outage windows
Downtime Impact	Business disruption, data loss	Physical harm, environmental damage
Protocols	TCP/IP, TLS, HTTPS	Modbus, DNP3, OPC-UA, Profibus
OS Environment	Modern, supported, diverse	Legacy Windows, VxWorks, QNX
Testing	Dev/staging environments	Cannot test in production safely
Incident Response	Isolate → investigate → restore	Must maintain operations throughout

IT vs. OT: Fundamentally Different Worlds

Dimension	Information Technology (IT)	Operational Technology (OT)
Primary Goal	Data processing & business logic	Physical process control & safety
Security Priority	Confidentiality first (CIA)	Availability first (AIC)
System Lifecycle	3–5 years (frequent refresh)	15–30+ years (rarely replaced)
Patching	Regular, automated, tested	Infrequent; requires outage windows
Downtime Impact	Business disruption, data loss	Physical harm, environmental damage
Protocols	TCP/IP, TLS, HTTPS	Modbus, DNP3, OPC-UA, Profibus
OS Environment	Modern, supported, diverse	Legacy Windows, VxWorks, QNX
Testing	Dev/staging environments	Cannot test in production safely
Incident Response	Isolate → investigate → restore	Must maintain operations throughout

SECTION 02

IT/OT Convergence Challenges

Connecting OT to IT networks dramatically expands the attack surface

Expanded Attack Surface

IP-enabling legacy OT exposes protocols never designed with authentication or encryption to internet-facing threats.

Unpatched Vulnerabilities

OT averages 5-10 years unpatched. Vendors may no longer exist; patching risks operational disruption.

No Visibility / Inventory

Many sites lack a complete asset inventory. Passive monitoring is required — active scans can crash legacy PLCs.

Cloud & Remote Access

Remote access surged post-2020. VPNs and cloud historians bridge previously air-gapped networks.

IoT / IIoT Proliferation

Industrial IoT sensors and smart meters lack firmware updates and often ship with default credentials.

Organizational Silos

IT teams lack OT expertise; OT engineers lack security training. Risk falls between the cracks.

Why OT Systems Are So Hard to Secure

Constraints that make traditional IT security approaches insufficient

Cannot Reboot or Patch Freely

A furnace, pipeline, or water plant can't shut down for a patch. Maintenance windows may occur once a year.

Proprietary, Undocumented Protocols

Many ICS protocols are closed-source and undocumented. Testing needs specialized tooling and vendor knowledge.

No Encryption or Authentication

Modbus (1979), DNP3 and fieldbus protocols send commands in cleartext. Any device on the network can issue them.

Safety-Critical = Risk-Averse

Changes to safety systems require hazard analysis, change management, and regulatory review.

Vendor Lock-in & Support Gaps

Vendors control the stack; adding security tools may void warranty or breach support contracts.

Flat Network Architectures

Brownfield environments evolved without segmentation. One VLAN may connect PCs, SCADA, and PLCs.

Limited Computing Resources

Field devices have kilobytes of memory. Endpoint agents, logging, or encryption are infeasible.

Regulatory Complexity

OT spans NERC CIP, TSA, FDA, NRC, NIS2 — each with different requirements and audit frameworks.

SECTION 03

OT Threat Landscape & Risk Vectors

THREAT ACTORS

Nation-State APTs — CRITICAL

Sandworm, Volt Typhoon, XENOTIME — pre-positioning in critical infra for espionage and disruption

Ransomware Groups — CRITICAL

BlackCat, LockBit, EKANS — increasingly OT-specific. Colonial Pipeline paid $4.4M

Hacktivists — HIGH

Ideologically motivated targeting of water and energy; post-conflict activity rising

Insider Threats — HIGH

OT engineers with physical + logical access; compromised or disgruntled staff

KEY ATTACK VECTORS

- Spear phishing → IT pivot to OT
- Exploited remote access (RDP, VPN)
- USB / removable media
- Supply chain & third-party vendors
- Unpatched HMI & engineering hosts
- Default / weak / shared credentials
- Malicious firmware updates
- Rogue wireless access points
- IT/OT DMZ bypass via historians

Landmark ICS/OT Cyber Incidents

2010	**Stuxnet** *Iranian Nuclear*	First cyberweapon targeting ICS. Sabotaged centrifuges via Siemens PLCs while showing false-normal readings.	Physical destruction
2015	**BlackEnergy** *Ukraine Power Grid*	First cyberattack causing power outages. 230,000 lost power. CRASHOVERRIDE followed in 2016.	Grid blackout
2017	**TRISIS / TRITON** *Middle East Petrochemical*	Targeted Schneider SIS — designed to disable emergency shutdown. First safety-system malware.	Near-catastrophe
2021	**Colonial Pipeline** *US Fuel Pipeline*	Ransomware hit IT; OT shut preventively. 5,500-mile pipeline offline 6 days. $4.4M ransom.	National emergency
2021	**Oldsmar Water** *Florida Water Treatment*	Attacker via TeamViewer tried to raise lye to 111x safe levels. Caught by an operator in real time.	Potential mass harm

SECTION 04

Securing Legacy Industrial Systems

Practical strategies when replacement isn't an option

1. Network Segmentation

Defense-in-depth with industrial DMZs, data diodes, and zone/conduit models per IEC 62443. Limit lateral movement.

2. Passive Asset Discovery

Passive monitoring (Claroty, Dragos, Nozomi) to build inventory and baseline behavior without disrupting operations.

3. Privileged Access Mgmt

Enforce MFA, session recording, just-in-time access. Eliminate shared, default, and hardcoded credentials.

4. Compensating Controls

Virtual patching via IPS/IDS, application whitelisting, integrity monitoring, USB port controls when patching is impossible.

5. OT Incident Response

IR plans must preserve operations — no 'isolate and reimage.' Build runbooks for manual fallback and safe shutdown.

6. Vendor Risk Management

Third-party integrators are frequent vectors. Enforce secure remote access, NAC, and contractual security requirements.

Key Regulatory & Security Frameworks

IEC 62443

International

The primary global standard for industrial cybersecurity. Defines security levels (SL 1-4) and zones/conduits.

NIST SP 800-82

US NIST

Guide to ICS Security. Maps the NIST CSF functions (Identify, Protect, Detect, Respond, Recover) to OT.

NERC CIP

North America

Mandatory standards for the bulk electric system. CIP-005, CIP-010, CIP-013 are most relevant to OT.

NIST CSF 2.0

US NIST (2024)

Adds the 'Govern' function. Sector-agnostic risk management increasingly adopted for OT.

TSA Directives

US DHS/TSA

Post-Colonial Pipeline mandates: OT segmentation, access control, and incident reporting for pipelines/rail.

EU NIS2

European Union

2023 expansion covering OT in energy, transport, water, manufacturing. 24-hour incident reporting.

SECTION 05

Cyber Resilience: Industry 4.0 & AI

The double-edged sword: AI as both threat multiplier and defender

Industry 4.0 = convergence of IT, OT, IoT, AI, cloud, and analytics into smart, interconnected manufacturing and infrastructure.

AI as Threat Multiplier

- AI-generated spear phishing with convincing operational context
- LLM-assisted vulnerability discovery in ICS firmware & protocols
- Autonomous malware with adaptive, environment-tailored evasion
- Deepfake audio/video to socially engineer control-room operators
- Automated exploitation of new ICS CVEs before patches exist

AI as Defender

- Behavioral anomaly detection in OT process data, signature-free
- Digital-twin simulation for threat modeling & attack-path analysis
- Predictive maintenance + security alert fusion for correlation
- NLP-based threat-intel ingestion and IOC extraction at scale
- Graph neural networks for IT/OT lateral-movement detection

The Expanding OT Attack Surface

Each figure is sourced — with a short note on what drove the change

73%

[1]

of OT organizations had an intrusion impacting OT systems in 2024 — up from 49% in 2023

Why: IT/OT convergence widened the path; phishing & business-email compromise let IT breaches pivot into OT.

Source: Fortinet, 2024 State of OT Report

~21B

[2]

connected IoT devices in 2025 — forecast to reach ~39B by 2030

Why: Smart-manufacturing sensors, 5G rollout and predictive-maintenance devices — many ship with weak security.

Source: IoT Analytics, State of IoT 2025

$330B

[3]

potential cost of a catastrophic OT cyber event in a single year ($172B from business interruption alone)

Why: In OT, downtime — not data loss — drives cost. A halted plant or pipeline bleeds revenue and restarts slowly.

Source: Dragos & Marsh McLennan, 2025

56%

[4]

of OT organizations hit by ransomware or wiper attacks in 2024 — nearly double 2023's 32%

Why: Attackers learned OT victims pay fast. Claroty found ~2 in 3 industrial victims pay the ransom.

Source: Fortinet 2024 · Claroty 2023

REFERENCES [1] Fortinet 2024 Global State of OT & Cybersecurity Report. [2] IoT Analytics, State of IoT 2025. [3] Dragos & Marsh McLennan, OT Cyber Risk, 2025. [4] Fortinet 2024; Claroty, Global State of Industrial Cybersecurity 2023.

FOR THE RESEARCHERS

Open Research Challenges in OT Security

Rich problem spaces awaiting academic contribution

Formal Verification of ICS Security

Early

Can we formally prove IEC 62443 compliance in multi-vendor OT systems-of-systems?

ML Anomaly Detection for OT

Active

Data scarcity, explainability, adversarial robustness in process-control detection.

ICS Protocol Security Analysis

Active

Systematic analysis of Modbus, DNP3, IEC 61850 and secure upgrade paths.

Digital Twin Security

Emerging

Securing the twin-plant channel; detecting manipulation; cloud-twin data privacy.

Post-Quantum OT Cryptography

Early

PQC on resource-constrained PLCs/RTUs; migration for 30-year-lifecycle systems.

Human Factors in OT Security

Growing

Alert fatigue, cognitive load, trust calibration with AI decision-support.

OT Threat-Intel Sharing

Active

Automated ICS IOC extraction; OT attack taxonomy and ontology development.

Resilience Metrics

Open

Quantifying OT cyber resilience beyond compliance — operational readiness scoring.

SOURCES

References & Further Reading

Credible sources informing this presentation

Industry Reports & Surveys

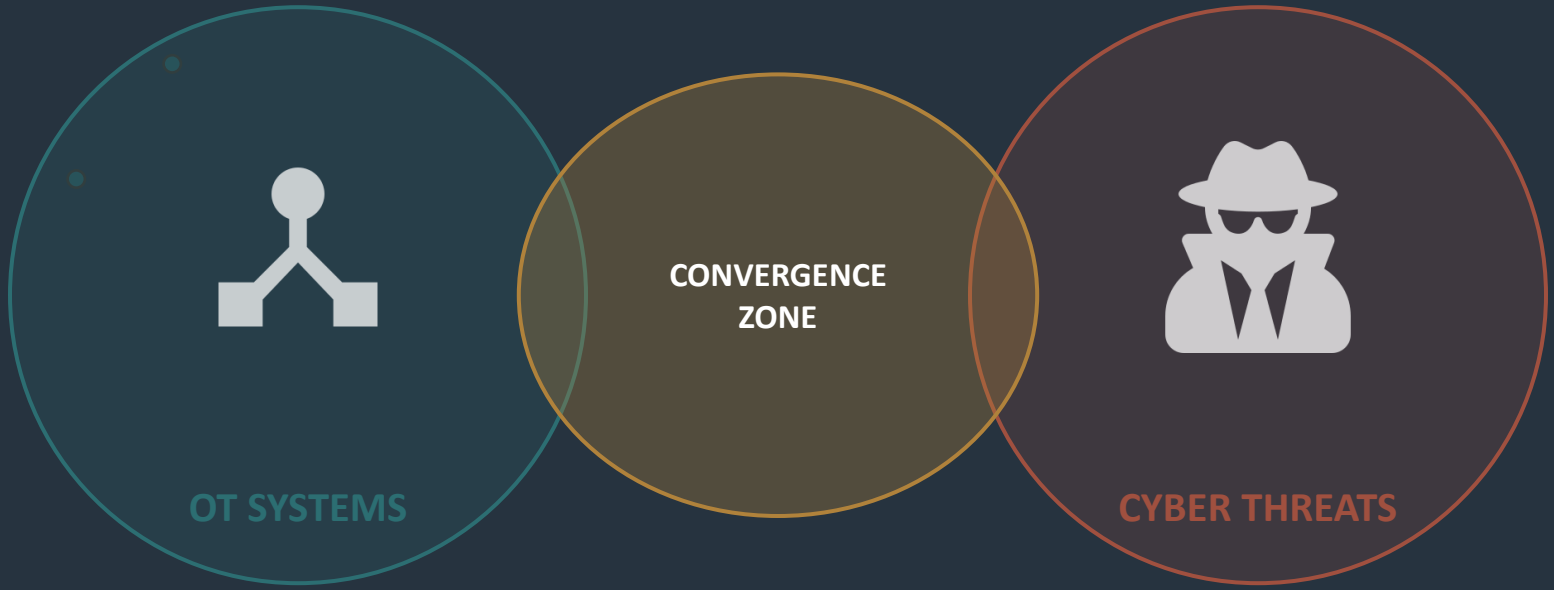
- Fortinet — Global State of OT & Cybersecurity Report (2024 & 2025)
- Claroty — Global State of Industrial Cybersecurity (2023)
- SANS Institute — ICS/OT Cybersecurity Survey (2023)
- IoT Analytics — State of IoT 2025
- Dragos & Marsh McLennan — OT Cyber Risk / loss modeling (2025)
- Palo Alto Networks — State of OT Security survey

Standards & Frameworks

- IEC 62443 — Industrial Automation & Control Systems Security
- NIST SP 800-82 Rev. 3 — Guide to OT Security
- NIST Cybersecurity Framework (CSF) 2.0 (2024)
- NERC CIP — Critical Infrastructure Protection standards
- EU NIS2 Directive (2023)
- US TSA Security Directives — Pipeline & Rail

Threat Intel & Incident Analysis

- Dragos — OT/ICS threat groups & annual Year-in-Review
- CISA — ICS Advisories & Cross-Sector Performance Goals
- MITRE ATT&CK for ICS
- Langner — Stuxnet & TRISIS technical analyses
- Mandiant / Google Cloud — APT & OT threat reporting



Questions & Discussion

"If a capable adversary had been inside your OT network for six months, would you know — and could you evict them without shutting down operations?"