

OT & ICS SECURITY.



Operational technology runs the physical world — valves, turbines, breakers, pumps — so a compromise isn't just a data-loss event. **Safety and availability outrank confidentiality here, and the controls that work in IT can crash the equipment they're meant to protect.**

- SCADA & ICS
- NETWORK SEGMENTATION
- LEGACY PROTOCOLS
- SAFETY INSTRUMENTED SYSTEMS

01 THE MECHANISM

Physical Process Control

PLCs, RTUs, and DCS controllers directly operate physical equipment. **An attacker who reaches this layer causes physical consequences**, not just a data breach — a distinction IT security models don't capture.

Purdue Model Segmentation

Industrial networks are conventionally divided into numbered levels, field devices through enterprise IT, with a DMZ at the IT/OT boundary. **Segmentation only protects where those boundaries are actually enforced**, not just diagrammed.

Legacy Protocols, No Security Built In

Modbus, DNP3, and similar protocols were designed decades ago for reliable delivery on isolated serial links. Most **lack native authentication or encryption**, so anyone who reaches the segment can often issue commands.

02 THE FLOW

The Segmented, Monitored Environment

CONTAINED

1

IT and OT are separated by an enforced DMZ; remote access runs through jump hosts with **MFA and time-limited, logged sessions**, not a direct VPN drop onto the control network.

2

Engineering workstations used to program PLCs are dedicated and **never dual-homed** onto the business network.

3

An IT-side intrusion is contained at the DMZ — the compromised segment is isolated while **OT operations continue safely**.

The Flat / Converged Network

EXPOSED

1

IT and OT share a flat network, or a dual-homed engineering laptop bridges both, so a **phishing-based IT compromise reaches the control network directly**.

2

Legacy protocols accept unauthenticated commands from any host on the segment, letting an attacker **issue write commands straight to a PLC**.

3

Even without a direct pivot, ransomware on the IT side can force a **precautionary OT shutdown** — real-world physical disruption either way.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Network Segmentation & Zoning	Enforced boundaries between IT, DMZ, and OT levels (IEC 62443 zones and conduits) so a compromise on one side can't reach the physical process directly.
Asset Inventory & Visibility	A verified inventory of every PLC, RTU, HMI, and engineering workstation — environments can't secure equipment that was never fully cataloged.
Secure Remote Access	Vendor and engineer access brokered through jump hosts, MFA, and session recording rather than direct VPN drops onto the control network.
Safety Instrumented System (SIS) Isolation	Independent safety systems kept isolated from what they monitor, so a control-system compromise can't also disable the layer meant to catch it.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Air-Gapping Alone, Assumed Not Verified	No	USB media, dual-homed laptops, and undocumented vendor remote-access links routinely bridge networks assumed to be isolated.
IT Security Tools Applied Directly to OT	No	Active vulnerability scanning or agent-based EDR can crash legacy PLCs and RTUs never built to absorb unexpected traffic or load.
Patching on the Same Cadence as IT	No	Many ICS components need vendor recertification before an update, and can't be rebooted without halting a physical process.
Perimeter Firewall at the IT/OT Boundary Only	No	A single boundary control does nothing once an attacker, or a compromised vendor connection, is already inside the OT segment.
IEC 62443 Zones/Conduits + Asset Inventory + Passive Monitoring + Isolated SIS	Yes	Layers segmentation, visibility, and OT-safe monitoring instead of relying on IT tooling or a single boundary.

OT & ICS SECURITY.

SEGMENT · MONITOR · ISOLATE

05 PROGRAM OPERATIONS

Safety and availability outrank confidentiality in OT, the reverse of the typical IT priority — a control action that's a second late can matter more than data that briefly leaks.

Passive, out-of-band monitoring is the OT default, precisely because active scanning can crash equipment that was never built to absorb it.

The Purdue Model is a reference architecture, not automatic protection. Segmentation only works where the zones and conduits it describes are actually enforced.

Engineering workstations carry disproportionate risk. A single compromised laptop with programming software installed can push malicious logic directly to a PLC.

06 CONTROL MAPPING

IEC 62443

The primary ICS/OT security standard, defining security levels (SL 0–4) and the zones-and-conduits model for segmenting industrial networks.

NIST SP 800-82

Guide to Industrial Control Systems Security, covering ICS-specific risk management, network architecture, and controls.

MERC CIP

Mandatory, enforceable standards for the North American bulk electric system, from asset identification to incident reporting.

CISA / ICS-CERT

Ongoing vulnerability and threat advisories specific to industrial control system products and critical infrastructure sectors.

07 WHAT THIS DOES NOT SOLVE

IT Security Debt

OT segmentation doesn't fix weak identity, unpatched servers, or phishing exposure on the IT side that still gives an attacker an **initial foothold**.

Vendor & Supply Chain Trust

A compromised vendor update or remote-support connection can **bypass network segmentation entirely**, since it's trusted by design.

Physical Security

Segmenting the network does nothing if a facility badge or an exposed control cabinet gives an attacker **direct physical access** to a PLC.

Legacy Equipment Lifespan

Some ICS hardware runs 15–20+ years. Architecture has to work around equipment that **will never be replaced or patched** on a review cycle.

08 MYTHS VS. REALITY

MYTH "Our OT network is air-gapped, so it isn't reachable."	REALITY Most claimed air gaps have undocumented bridges — USB media, dual-homed laptops, or a vendor's remote-support link — never inventoried.
MYTH "Standard IT vulnerability scanners are safe to run on OT."	REALITY Active scanning has crashed legacy PLCs and RTUs never built to handle unexpected traffic; passive monitoring is the OT-safe default.
MYTH "An attack on IT systems can't affect physical operations."	REALITY Colonial Pipeline shut its pipeline down as a precaution after ransomware hit only its IT systems, since OT integrity couldn't be confirmed.
MYTH "The safety system will catch it even if control is compromised."	REALITY TRITON/TRISIS specifically targeted a plant's safety instrumented system — an attacker can go after the safety layer directly.
MYTH "OT security just means applying IT controls to industrial gear."	REALITY OT prioritizes safety and availability over confidentiality and runs on legacy protocols IT tools weren't built for — it needs its own risk model.

09 SPEAK THE PROGRAM — KEY TERMS

SCADA

Supervisory Control and Data Acquisition — software and hardware that **monitors and controls industrial processes** across often distributed sites.

PURDUE MODEL

A reference architecture dividing industrial networks into numbered levels, field devices through enterprise IT, used to **design segmentation boundaries**.

PLC (PROGRAMMABLE LOGIC CONTROLLER)

An industrial computer that **directly controls physical equipment** — valves, motors, breakers — based on programmed logic.

SAFETY INSTRUMENTED SYSTEM (SIS)

An independent system designed to **bring a process to a safe state** if the primary control system fails or is compromised.

ZONES & CONDUITS

The IEC 62443 model for grouping assets into security zones and **explicitly controlling the conduits** between them.

IT/OT CONVERGENCE

Growing connectivity between operational technology and IT/business networks for remote monitoring, which **expands OT's attack surface**.