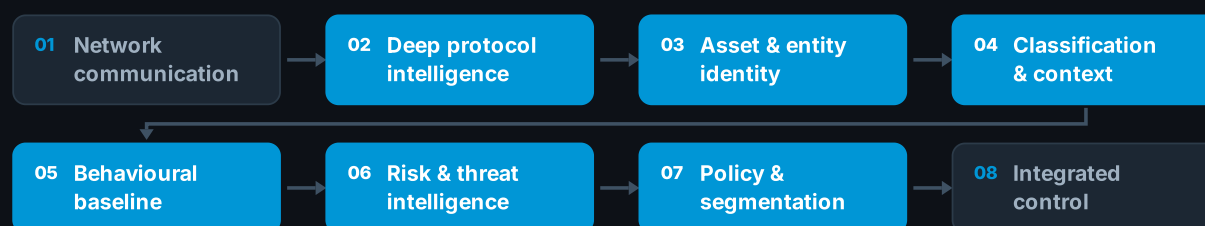


INDUSTRY SOLUTION

OT Security

Know every controller and field device, see what is being asked of them, and evidence your segmentation, from the industrial protocols your plant already speaks and without touching the process.



For: OT security, plant and control engineering, utilities, manufacturing, oil and gas

Industrial networks run the processes that matter most and tolerate intervention least. Most security tooling was built for the opposite conditions. WireTrace works from what control systems already say to each other: **it reads the industrial protocols on the wire, identifies each controller and field device from its own identity record, and watches the commands that change the process.**

01 The OT reality

Scanning is a risk

Controllers and protection devices were not built to answer unexpected traffic, so scanning is usually restricted.

No room for agents

PLCs, RTUs, relays and drives cannot run endpoint software.

Devices outlive plans

Equipment runs for decades, firmware is rarely updated and records drift.

Flat networks

Traffic can reach controllers from business networks through paths nobody intended.

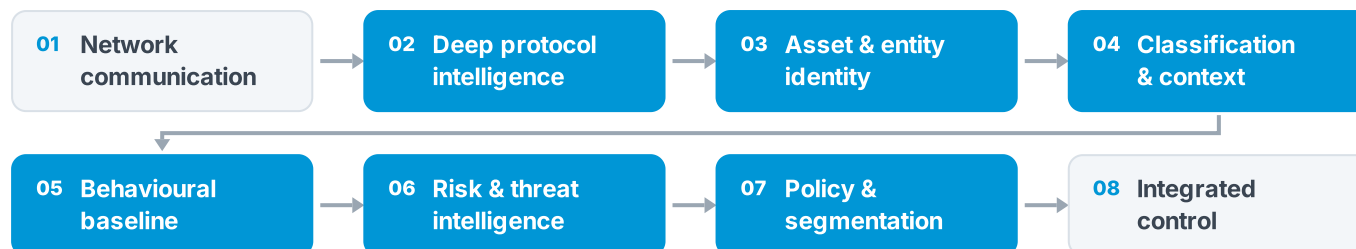
Engineering access

Workstations and vendor laptops can write to controllers; dangerous operations look like maintenance.

Evidence is demanded

OT frameworks expect inventory, segmentation and monitoring to be shown, not asserted.

WireTrace is a **Deep Protocol & Asset Intelligence (DPAI)** platform. It is passive by default: sensors take a copy of traffic from a SPAN port, TAP or ERSPAN session, and the capture interface only receives, never transmitting onto the monitored network. Nothing is installed on the devices being observed.



The WireTrace platform flow. Highlighted layers are the subject of this document.

02 What WireTrace reads from industrial protocols

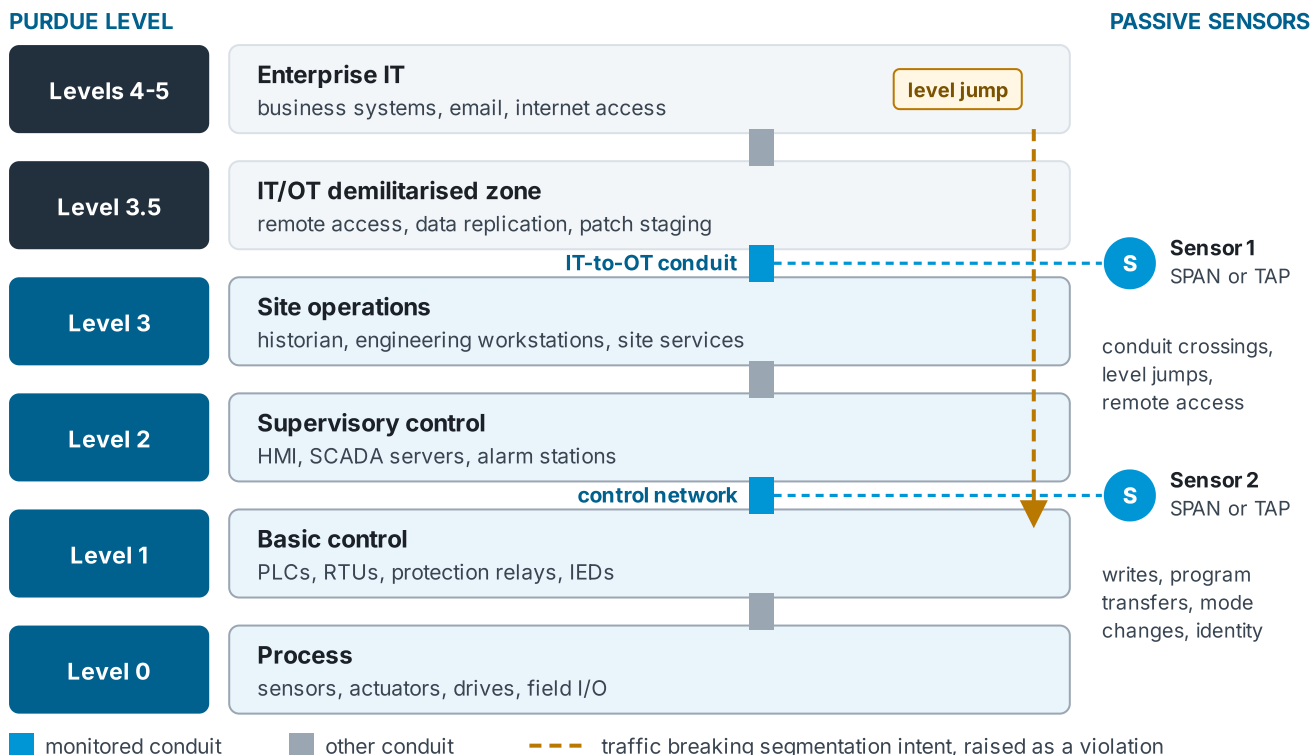
WireTrace decodes protocol payloads, not just headers, and understands what an industrial conversation does: reads, writes, program transfers, mode changes and exceptions, not just that two devices talked. Many industrial protocols carry the device's own identity record, and WireTrace uses it as primary evidence.

Protocols	What WireTrace reads	Command monitoring
Modbus, S7comm, DNP3, IEC 60870-5-101/104, IEC 61850 MMS, Omron FINS, Mitsubishi SLMP/MELSEC, SEL Fast Message	Device identity where stated, operations and function codes, the points and values written, controller mode and program transfers	Yes
EtherNet/IP and CIP, PROFINET, OPC UA, S7CommPlus (session level), CODESYS, HART-IP, EtherCAT, IEC 60870-5-103	Identity records such as the CIP identity object, PROFINET station name and identification data and OPC UA application certificates; device discovery and communication	Identity and discovery
IEC 61850 GOOSE and Sampled Values, IEEE C37.118 synchrophasor, PRP/HSR, PTP	Substation and grid devices, publishing devices, timing and redundancy	Identity and discovery
BACnet, KNXnet/IP, Niagara Fox, MQTT	Building controllers and IoT gateways that share the plant network, including the BACnet device object	Identity and discovery

03 Controller and field-device identity

When an engineering workstation reads a controller's identity, the reply carries the manufacturer, order number, firmware and often the serial number. Where a device states these, as many industrial controllers do, WireTrace records each value with its source. The manufacturer is normalised to one name. The device keeps **one durable identity** across address changes, redundant interfaces and several sensors, joined only on values it states uniquely. Cloned or default values are not used to merge devices.

Each device is classified by type, such as PLC, RTU, protection relay, HMI or engineering workstation, and placed on a **Purdue level with a stated confidence and a one-line reason**. Devices the evidence cannot place stay unknown rather than guessed, and for each device WireTrace states which kinds of evidence are present, missing or stale.



A Purdue-level view with two passive sensors. One watches the IT-to-OT conduit for crossings, level jumps and remote access; one watches the control network for commands to controllers and their identity records. Placement follows your architecture.

04 Watching what the process is told to do

OT command monitoring

On Modbus, S7comm, DNP3, IEC 60870-5-101/104, IEC 61850 MMS, Omron FINS, Mitsubishi SLMP/MELSEC and SEL Fast Message, WireTrace detects unauthorised writes, parameter changes, controller mode changes and stops, program download and upload, forced I/O, firmware transfers, new or rogue masters and illegal function codes. Detections are mapped to MITRE ATT&CK for ICS and name the devices involved by their durable identity.

Protocol behaviour baseline

For industrial protocols, WireTrace learns which fields and values each protocol normally carries. Once you approve the baseline, a new field or value, such as a previously unseen function code, raises a deviation. Nothing is treated as normal until an engineer has approved it.

Conduits and Purdue-level jumps

Declare which zones and devices may communicate, in which direction and over which services, and declare IEC 62443 zones, conduits and target security levels. WireTrace then continuously detects traffic that breaks that intent, including IT-to-OT conduit crossings and large Purdue-level jumps, such as a business-network host talking directly to a controller.

WireTrace observes

- A DNP3 outstation that has only ever been polled by one master
- A second host begins issuing control operations to it
- The approved protocol baseline has never seen that function code on this link

WireTrace produces

- A new or rogue master detection, mapped to ATT&CK for ICS
- A protocol behaviour deviation, with the new value as evidence
- Both devices identified, classified and placed on their Purdue levels

05 Vulnerabilities, end of life and risk

WireTrace matches each device's identified firmware and OT product to OT vendor advisories and the NVD, prioritised with CISA KEV and FIRST EPSS. Every finding states how it was matched, how strong the match is, and whether the vulnerable version is confirmed on that device. This depends on version evidence: a controller that states its firmware can be matched precisely; one that states only its product family yields a weaker match, labelled as such. Operating systems and products past vendor end of life are flagged, using lifecycle data that also works offline; OT firmware lifecycle coverage is not complete. Each device carries a 0-100 Asset Risk Score in which impact reflects its Purdue level and its safety or control role, and the remediation workspace includes a containment view for devices that cannot be patched.

06 Segmentation and compliance evidence

WireTrace provides the intelligence, policy intent and continuous validation layer for segmentation; your existing firewalls, NAC and switches enforce it. Proposed rules can be tested against observed traffic and exported as text for your firewall team; the Policy Automation & Micro-Segmentation brief describes this in full.

WireTrace maps network observations to controls in IEC 62443-3-3, NERC CIP and NCA OTCC, among the seven frameworks it supports. Every control is rated observable, partial, manual assessment or not assessable from the network, and auditors close the rest in the platform's assessment workflow. For IEC 62443, WireTrace shows observed security-level gaps per zone against your targets where they are observable; levels that cannot be observed are marked as requiring declaration. Evidence can be exported as a signed evidence bundle.

07 Safe deployment

Passive monitoring is the default, and it is how industrial devices are observed. Optional, administrator-governed active enrichment can add deeper inventory for IT and network devices, such as read-only switch polling and credentialed collection from IT hosts at Level 3 and above. It needs defined scopes and read-only credentials, runs from the management interface, and an OT-safe profile keeps probes away from industrial devices unless explicitly allowed. The platform runs on your infrastructure, without internet access if required.

08 By sector

Manufacturing

Controller identity from S7comm, EtherNet/IP and PROFINET; detection of program downloads, mode changes and forced I/O; Purdue mapping of lines and cells.

Energy and utilities

Substation visibility from IEC 61850 MMS, GOOSE and Sampled Values; command monitoring on DNP3 and IEC 60870-5-104; evidence for NERC CIP and NCA OTCC.

Oil and gas

Sensors at remote sites reporting to one platform; Modbus and DNP3 command monitoring for pipeline and terminal control; operation without internet access.

Limits, stated plainly

- WireTrace sees what reaches its sensors. Level 0 devices are visible only where their traffic, or a controller's, reaches a monitored segment.
- Command monitoring covers the protocols listed above. EtherNet/IP, PROFINET, OPC UA, BACnet and S7CommPlus are used for identity and discovery, and encrypted OT payloads are not analysed.
- Model and firmware are recorded where devices state them; advisory matches are only as precise as that version evidence.
- WireTrace detects segmentation violations and hands proposed rules to your teams. Your firewalls, NAC and switches enforce them.
- Compliance mapping provides evidence for audits. It does not certify a security level or replace the assessor.

Start passively, on one mirrored port

A WireTrace evaluation starts on a SPAN or TAP at a single conduit, with nothing sent to the control network. Controllers, the firmware they state and the commands they receive appear as soon as their traffic is observed.

Book a demo at wiretrace.io/request-demo or email sales@wiretrace.io