WIRETRACE

WIRETRACE

SOLUTION BRIEF - OT/ICS SECURITY

Passive Protocol Intelligence for Industrial Networks

WireTrace reads the actual commands flowing between PLCs, RTUs, HMIs, and SCADA systems - not just traffic metadata. Security and operations teams gain continuous visibility into what industrial controllers are doing, who is communicating with them, and whether that activity is authorized. Deployed passively with zero impact on safety-critical operations.

The Challenge

- **Industrial Assets Operating in the Dark** - Legacy PLCs and RTUs were never designed to be inventoried by IT tools. Many have been running for years without appearing in any asset register. Shadow connections between Purdue levels go unnoticed until an incident exposes them.
- **Port-Level Tools Cannot Read Industrial Commands** - Generic security tools see "traffic on port 502" but cannot distinguish a routine register read from an unauthorized write to a safety-critical setpoint. Without protocol-level context, real OT threats are invisible.
- **Active Scanning Disrupts Industrial Operations** - Active network discovery tools have caused PLC faults, safety system trips, and production outages. In OT environments where uptime is measured in years, active interrogation is an unacceptable risk.

How WireTrace Solves It

Command-Level Protocol Dissection	WireTrace decodes Modbus function codes and register values, S7Comm PLC parameters, DNP3 control commands, EtherNet/IP CIP messages, and IEC 104 telecontrol sequences. Security teams see the actual operations being performed on controllers.
Passive Industrial Asset Discovery	Every PLC, RTU, HMI, engineering workstation, and protocol gateway is identified from observed traffic alone. Vendor, model, firmware version, and network role assigned automatically - without sending a single packet into the OT network.
Operational Behavioral Baselines	WireTrace learns normal command patterns per device and per protocol. Deviations - an unexpected Write command, a new communication peer, a change in polling frequency - are detected with full protocol context.
Cross-Zone Communication Detection	Real-time visibility into which Level 1 field devices communicate with Level 3 systems. Unauthorized lateral movement and zone boundary violations identified automatically to help enforce segmentation policies.

Industrial Protocol Intelligence

Modbus TCP/RTU · S7Comm · EtherNet/IP CIP · PROFINET · BACnet · DNP3 · IEC 60870-5-104 · OPC-UA · GOOSE · Sampled Values · EtherCAT · HART-IP · FINS · MELSEC · SLMP · CODESYS · KNXnet/IP · LonTalk · Synchrophasor · FF-HSE · DLMS/COSEM · MMS · and more+

Representative examples. WireTrace supports proprietary and vendor-specific industrial protocols beyond this list, with continuous expansion.

Protocol Depth (Examples)

Modbus	Unit ID, function codes, register addresses and values, Read vs. Write discrimination, request/response correlation.
S7Comm	PLC model identification (S7-300/400/1200/1500), programming activity detection, diagnostic access, vendor and firmware extraction.
DNP3	Master/outstation role identification, control relay commands, analog and binary monitoring data, unsolicited responses, outstation addressing.

Industry Applications

Energy & Utilities	Continuous SCADA visibility across substations, distribution networks, and generation facilities. DNP3, IEC 104, and GOOSE/SV protocol intelligence. Detect unauthorized control commands and generate IEC 62443 and NERC CIP evidence.
Manufacturing	Monitor PLC communications across production lines and robotic cells. Detect unauthorized programming activity, firmware changes, and lateral movement between OT zones. Identify unsafe configuration changes before they cause failures.
Oil & Gas	Pipeline SCADA, refinery DCS, and offshore platform monitoring with Modbus, HART-IP, and FF-HSE protocol visibility. Identify unauthorized access to safety instrumented systems across distributed sites.
Water & Wastewater	Treatment plant and distribution network visibility with DNP3 and Modbus command-level inspection. Detect unauthorized setpoint changes to pumps, valves, and chemical dosing systems.

Compliance & Audit Evidence

WireTrace generates continuous compliance evidence from observed OT network traffic. Asset inventories, zone boundary communications, access control validation, and protocol usage documentation are always current - replacing periodic manual assessments that go stale between audits.

Supported frameworks: IEC 62443 · NCA OTCC · ISO 27001 · NERC CIP · Custom frameworks

Deployment

A single WireTrace sensor on a SPAN port or network TAP captures all OT traffic in a zone. The sensor is 100% passive - it never transmits on the monitored network. Multiple sensors cover multiple segments and report to a centralized server. Fully air-gap deployable. First industrial assets classified in under 30 seconds.

See What Your Controllers Are Actually Doing

Request a proof-of-value deployment.
wiretrace.io | sales@wiretrace.io