TELESOFT

STOUR OT PROBE

CYBER SECURITY FOR OPERATIONAL TECHNOLOGY

STOUR OT PROBE

SEE MORE, RISK LESS: MASTERING OT SECURITY VISIBILITY

THE CHALLENGE

Due to their nature, Operational Technology (OT) environments face a number of specific cybersecurity risks.

LEGACY SYSTEMS AND LONG LIFECYCLES

OT systems often run on outdated hardware and software that were designed decades ago without security in mind. These systems frequently have lifecycles of 15-20 years or more, making regular updates or replacements impractical. Many still run older operating systems that no longer receive security patches.

SUPPLY CHAIN VULNERABILITIES

OT environments rely on complex supply chains with many third-party vendors and contractors needing access. Each connection point and vendor represents a potential security risk, as demonstrated by attacks like NotPetya that spread through software supply chains.

PROTOCOL VULNERABILITIES

Many industrial protocols were designed for reliability rather than security. They often lack basic security features and can't be easily replaced due to their deep integration into industrial processes.

IT/OT CONVERGENCE RISKS

As traditionally isolated OT networks become connected to IT networks and the internet for efficiency and remote monitoring, they become exposed to threats they weren't designed to handle. This convergence creates new attack vectors while many OT protocols lack basic security features like authentication or encryption.

Monitoring Operational Technology for these potential vulnerabilities and attacks presents a number of challenges:

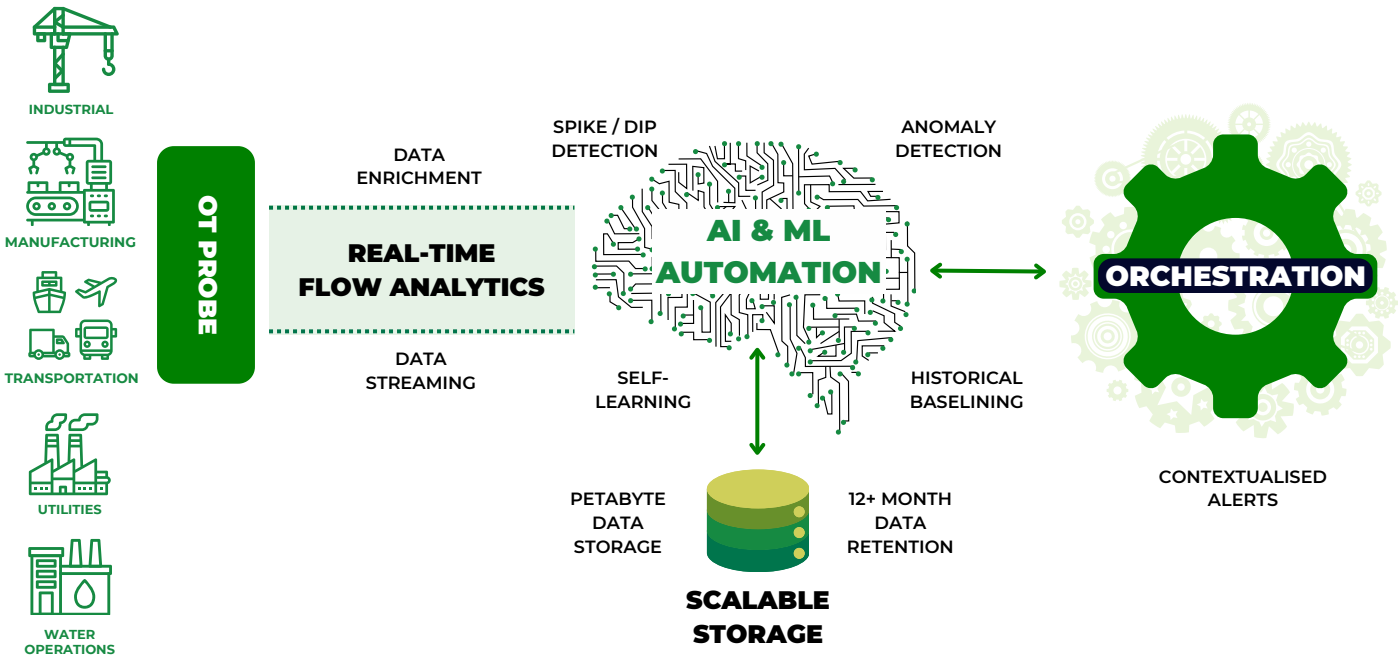
- Network monitoring tools designed for IT environments often **misinterpret** or completely miss OT protocol traffic, as these tools are built to understand common IT protocols and can either **generate false positives** or **fail to detect** actual threats hidden in OT protocol traffic.
- Traditional antivirus and endpoint detection solutions can cause **significant performance issues** when installed on OT endpoints, interfering with the real-time processing requirements of industrial control systems. In many cases, the use of proprietary or custom firmware on OT devices **prevents the installation** of security monitoring agents altogether.
- Log collection and analysis is particularly challenging in OT environments because many legacy devices either don't generate logs at all or produce them in **proprietary formats** that standard Security Information and Event Management (SIEM) systems **can't process** effectively.

THE SOLUTION

The key to successful security monitoring Critical National Infrastructure (CNI) in OT environments is finding the right balance between security visibility and operational stability.

Telesoft provides a non-intrusive, non-service affecting solution to monitoring the network traffic in the OT environment through the deployment of the Stour OT Probe.

Available for deployment within the central network switching infrastructure, or distributed across multiple physical locations within end point machinery, eg cranes, or localised cabinetry, the OT Probe captures all network packets, performs deep packet inspection and generates metadata for analysis. Flow records generated can be forwarded from the probe in IPFIX format to follow on systems.



Coupled with the TDAC (Telesoft Data Analytics Capability) Platform, Telesoft can provide a complete cyber security offering with the following capabilities:

- **Deep Packet Inspection (DPI)** capabilities for industrial protocols like Modbus, DNP3, BACnet, and PROFINET
- **Baseline profiling** of normal OT network traffic patterns
- **Real-time alerting** for anomalous behavior or unauthorized commands
- **Protocol validation** to detect malformed packets or potential attacks
- **Custom parsers** for industrial protocol logs
- **Correlation rules** specific to industrial attacks
- **Custom dashboards** for OT-specific metrics and KPIs
- **Long-term storage** of security events for compliance and forensics

TECHNICAL SPECIFICATION

Available in three form-factors, the Stour OT Probe can be deployed rack-mounted for passive tapping of multiple OT devices from the core switching infrastructure, or in smaller ruggedised forms, for deployment into more hostile environments where space, temperature or air quality may be problematic.

VARIANT	PHYSICAL	INTERFACES
Rack Mounted	1RU 19-inch rack mount- 1.7" x 17.2" x 30.6"	2 x 10GbE
Ruggerdised	Size: 7.68" x 1.73" x 5.94"	1 x 1GbE Serial
DIN Mounted	Size: 5.4" x 3.2" x 1.75"	1 x 1GbE Serial

SUPPORTED PROTOCOLS

- BACnet
- Bristol Babcock BSAP
- DNP3
- ENIP
- CIP
- Ethercat
- GE SRTP
- Genisys
- HART-IP
- Modbus
- OPCUA
- PROFINET/PROFISAFE
- S7COMM
- Synchrophasor
- IEC 60870-5-104
- IEC 61850
- Telnet
- MQTT

Note - Additional Protocol decodes are available on request

HEADQUARTERS
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford,
DT11 9LQ, UK
sales@telesoft-technologies.com

LONDON
Telesoft Technologies Ltd
Octagon Point, Office 501,
5 Cheapside, St. Paul's,
London EC2V 6AA
sales@telesoft-technologies.com

ASIA
Telesoft Technologies Ltd
Unit No B 409-410
Floor 4, Plot 8, Sector 62
Noida, 201309
salesindia@telesoft-technologies.com

SAUDI ARABIA
ATCO-Telesoft
ATCO Building
P.O. Box 718 - Dammam 31421
Kingdom of Saudi Arabia
salesindia@telesoft-technologies.com