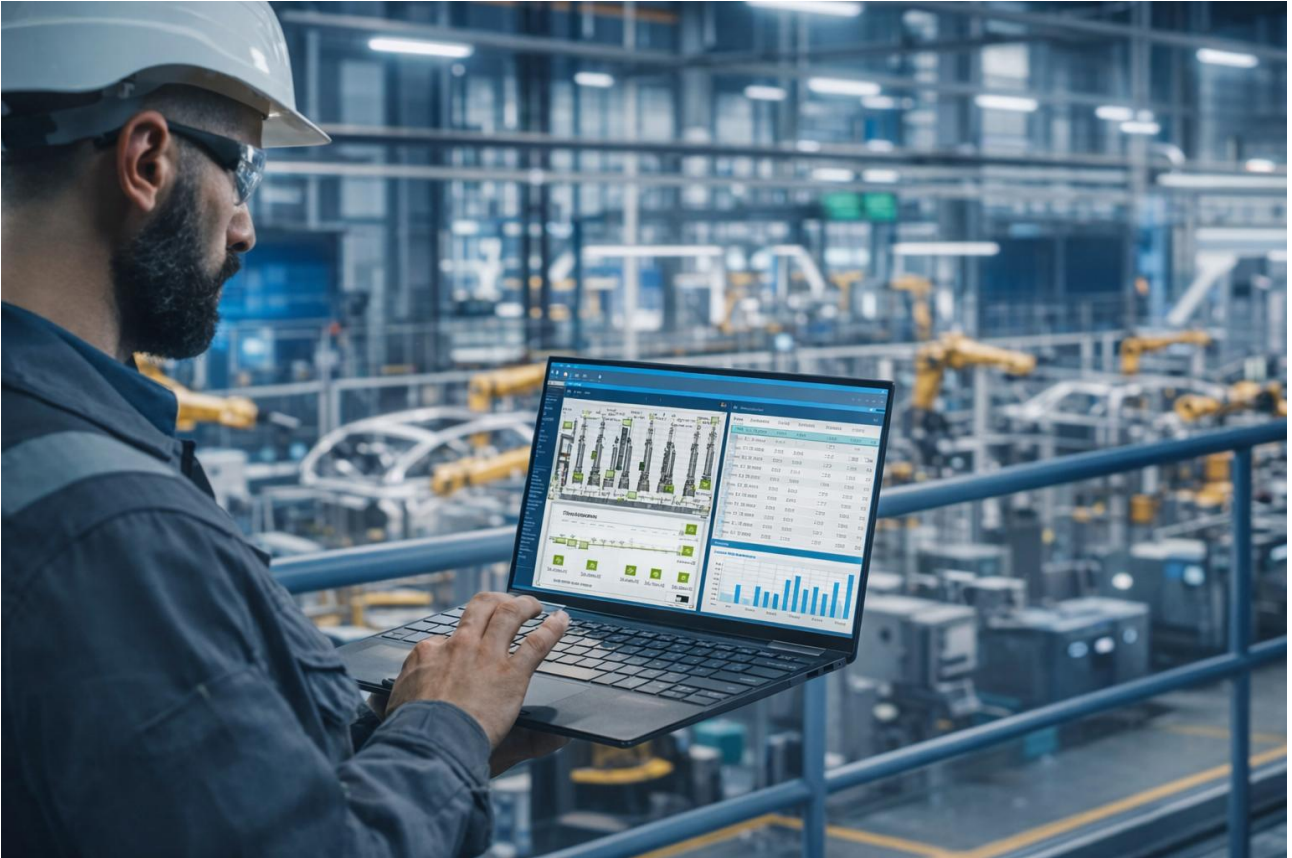




Monitoring OT

Bridging IT and OT with i-Vertix

Data: 16.03.2026

Version: 1.0

Author: Jochen Platzgummer CEO & founder i-Vertix

Summary

Introduction: Navigating IT & OT Convergence.....	4
Monitoring OT Equipments.....	5
Monitoring OT devices.....	6
Leveraging Standard IT Protocols and Open Source Flexibility.....	8
The Benefits of Extending Monitoring Beyond IT.....	9
Increasing Operational Efficiency	10
Defining Key Performance Indicators (KPIs).....	10
Creating and Sharing SLA Reports	11
i-Vertix NeDi: Discovery & Monitoring for IT/OT Networks	12
How Discovery Works.....	12
Comprehensive MAC & IP Inventory (Including SCADA/PLC).....	13
Classification & Shadow IT Governance.....	13
Visualizations & Operational Use	13
Why This Matters for OT.....	14
Monitoring OT Devices with i-Vertix	15
Native Support for MQTT Brokers.....	15
Native Support for Modbus	15
Native Support for Cameras and Environmental Sensors.....	16
Native Support for Industrial Network Devices.....	16
Native Support for HMS Netbiter Argos (Cloud-Based).....	17
Summary	17
Visualizing and Managing OT Monitoring with i-Vertix.....	18
Visualizing Monitored Devices with Maps.....	18
Creating Dashboards for the Big Picture	19
Role-Based Access Control (ACL) for Targeted Visibility	20
Integrating OT Monitoring with Security Platforms: Forwarding Events to SIEM.....	21
How It Works.....	21

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

Why This Is Important.....	22
Summary	22

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

INTRODUCTION: NAVIGATING IT & OT CONVERGENCE

As digital transformation accelerates, organizations are increasingly blending Information Technology (IT), Internet of Things (IoT), and Operational Technology (OT). This integration is essential but brings new challenges—especially when equipment is distributed across multiple locations.

A top-tier IT Infrastructure Monitoring platform excels at tracking your IT assets. But what about the OT systems connected to this infrastructure? These are vital for your business operations, customer service, and employee productivity. Are they running smoothly? Can they communicate with your cloud-based or data center applications?

This guide explores the hurdles and solutions for achieving comprehensive visibility and monitoring across IT and OT. We'll break down the five essential building blocks of a robust monitoring system—designed to maximize uptime, boost efficiency, and drive business value.

Key questions arise: Are your systems secure from threats? Are your operations running efficiently? Can you anticipate maintenance needs? Addressing these challenges requires a monitoring solution that goes beyond traditional IT, empowering you to confidently tackle IT and OT convergence projects.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

MONITORING OT EQUIPMENTS

Network Connectivity and Security

When extending monitoring to IoT and OT environments, the first priority is ensuring reliable network connectivity and robust security at every location where operational equipment is deployed. Whether your sites are connected via traditional MPLS, modern SD-WAN, or a mix of both, it's essential to monitor each network access point for both connectivity and security risks.

In industrial and distributed branch scenarios, unique challenges arise—such as remote locations, harsh environments, and limited IT presence. Here, deploying dedicated hardware pollers can make a significant difference. For example, the **i-Vertix Poller Pro S3** is specifically designed for industrial use. This hardware poller is ruggedized for demanding environments and supports 4G out-of-band communication, ensuring continuous monitoring even if the primary network connection fails. With 4G connectivity, remote sites remain accessible for monitoring and troubleshooting, providing an extra layer of resilience and operational continuity.



Key considerations:

- Ensure all network connections to OT and IoT equipment are monitored for both uptime and security.
- For distributed branches or industrial sites, consider deploying hardware pollers like the i-Vertix Poller Pro S3, which offers industrial-grade reliability and 4G out-of-band access for remote management.
- Always implement strong authentication, encryption, and network segmentation to safeguard sensitive operational data.

PGUM S.r.l

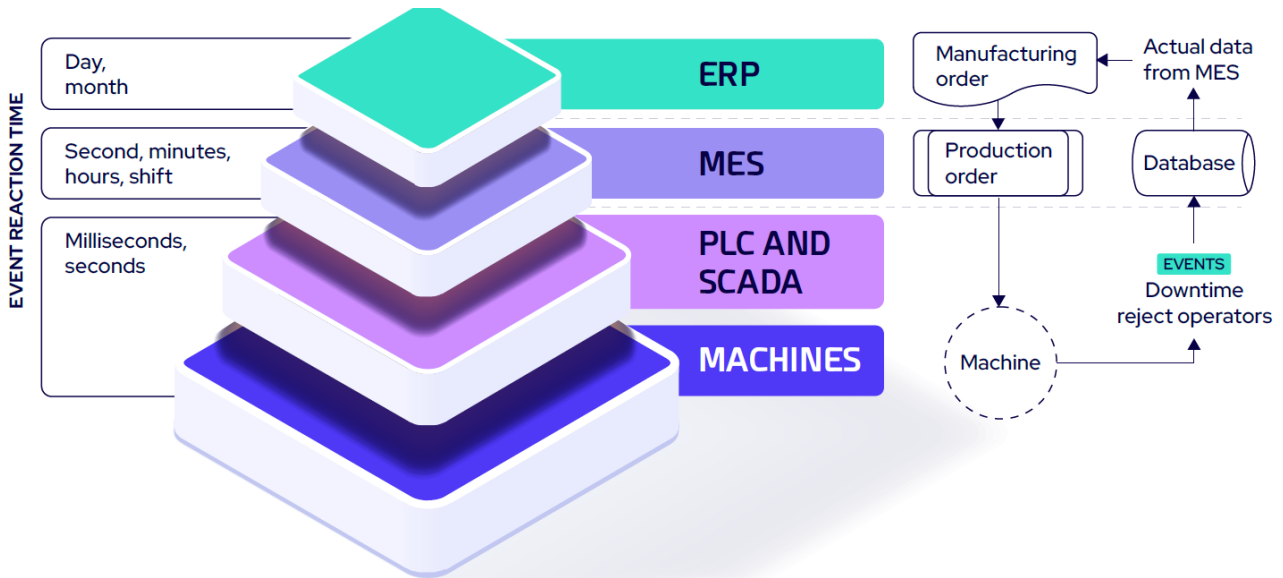
NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

Monitoring OT devices

Modern agentless monitoring solutions are designed to handle the wide variety of technologies found in today's operational environments. Beyond basic network connectivity, it's essential to monitor several critical layers:



1. Industrial Control Systems (ICS):

These include SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems), PLCs (Programmable Logic Controllers), and RTUs (Remote Terminal Units). Monitoring these systems ensures that physical processes and equipment in OT environments remain available and reliable.

2. Controllers and Human-Machine Interfaces (HMIs):

Controllers and HMIs are the bridge between operators and industrial systems. Monitoring their status and responsiveness is crucial for maintaining safe and efficient operations.

3. Sensors and Actuators:

Sensors collect data and measure physical parameters, while actuators control equipment and processes. Any malfunction can impact both performance and safety, so continuous monitoring is vital.

4. Sensor Data:

It's not enough to monitor the devices themselves—environmental data such as temperature, humidity, or pressure (e.g., in a cold storage room) should also be tracked to ensure optimal conditions and early detection of anomalies.

Operational Technology (OT) environments rely on specialized communication protocols to connect and monitor devices. Understanding these protocols is essential for effective monitoring:

- **MQTT (Message Queuing Telemetry Transport):**
A lightweight, publish-subscribe protocol ideal for environments with limited bandwidth or unreliable networks. Widely used in industrial IoT for efficient, scalable remote monitoring.
- **Modbus:**
A simple and reliable serial communication protocol, common in industrial automation. Available in Modbus RTU (Serial) and Modbus TCP/IP variants, it's used across manufacturing, energy, and utilities.
- **OPC UA (Open Platform Communications Unified Architecture):**
Extensively adopted in manufacturing, energy, utilities, and transportation. OPC UA integrates PLCs, SCADA systems, MES, and other automation devices for seamless data exchange and monitoring.
- **DNP3 (Distributed Network Protocol):**
Primarily used in utilities and energy sectors for remote monitoring and control in SCADA systems—such as electric grids, water treatment, and pipelines.
- **PROFIBUS:**
An older master-slave protocol for industrial automation, enabling communication between controllers and multiple field devices.
- **Other Protocols:**
You may encounter EtherNet/IP, BACnet (building automation), CANopen (robotics/automotive), PROFINET, IEC 60870-5, LoRaWAN, and more—each suited to specific industrial needs.

Leveraging Standard IT Protocols and Open Source Flexibility

Many OT devices can be monitored using standard IT management protocols, especially if they have an IP address. If a direct connector isn't available, consider retrieving data from the server or controller managing the device.

Open Source Monitoring Advantages:

- Open source solutions offer flexibility for unique or bespoke environments. Communities can adapt or develop connectors for specialized devices.
- Modern OT devices often provide REST APIs, enabling external systems to interact and collect monitoring data.
- SNMP (Simple Network Management Protocol), traditionally used in IT, is increasingly adopted in OT for environmental monitoring (e.g., temperature, humidity).
- Standard server monitoring techniques apply to devices running common operating systems (Linux, Windows).
- For simple devices, ICMP (ping) can be used to check basic availability.

Security Considerations for Monitoring Distributed OT Environments

Integrating IoT and OT devices into your operational environment often means managing assets that are widely distributed—sometimes across hundreds of remote sites. This distributed nature introduces unique security and connectivity challenges.

- **Remote Data Collection:**
For geographically dispersed locations, deploy remote servers (pollers) that locally gather monitoring data and securely transmit it to your central monitoring platform. This approach ensures continuous visibility, even in areas with unreliable connectivity.
- **Prioritize Security:**
When monitoring OT devices remotely, security must be a top priority. Always implement strong authentication, authorization, and encryption to protect sensitive data and prevent unauthorized access or tampering. For example, use HTTPS for REST APIs and SNMP v3 for encrypted communication.
- **Network Segmentation:**
Separate OT networks from IT networks using firewalls and access control lists (ACLs). This limits the spread of threats and helps contain potential security incidents.
- **Resilient Pollers:**
Pollers can buffer monitoring data during network outages and forward it once connectivity is restored. They can also be deployed on compact, industrial-grade hardware (such as Raspberry Pi

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

or dedicated appliances) for installation in challenging environments without edge computing facilities.

- **Out-of-Band Access:**

For critical or remote sites, consider pollers with out-of-band communication capabilities (e.g., 4G/LTE) to maintain monitoring and management access even if the primary network is down.

The Benefits of Extending Monitoring Beyond IT

When your organization relies on IoT and OT systems to deliver services and support operations, expanding your monitoring strategy beyond traditional IT brings significant advantages:

- **Scalability:**

Deploying remote pollers—such as hardware appliances or virtual instances—enables horizontal scalability. You can easily add new devices and sites without impacting the performance of your central monitoring platform. This approach is especially valuable as your infrastructure grows in size and complexity.

- **Optimized Network Bandwidth:**

Selecting the right monitoring protocol and adjusting data collection frequency helps manage network usage efficiently. For most OT environments, a five-minute interval between data collections is sufficient, minimizing bandwidth consumption while maintaining timely visibility.

- **Cloud-to-Edge Visibility:**

Comprehensive monitoring provides end-to-end visibility, from cloud-based business applications and data centers all the way to the physical edge—where manufacturing, logistics, and customer interactions occur. This ensures that every part of your organization is covered.

- **Real-Time Alerts and Notifications:**

Proactive monitoring means you're notified of issues before they impact operations. Instead of waiting for users to report problems, your team can respond quickly to early warnings, reducing downtime and improving service reliability.

- **Enhanced Security:**

Monitoring OT environments is a critical component of your cybersecurity strategy. It delivers essential visibility, detection, and response capabilities to protect your most valuable infrastructure assets.

By embracing these benefits, organizations can achieve greater operational resilience, efficiency, and security—laying the foundation for successful IT and OT convergence.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

Creating and Sharing SLA Reports

For the most critical KPIs, formal Service Level Agreements (SLAs) are established between IT and business operations. Achieving SLAs often involves setting internal Service Level Objectives (SLOs) focused on specific performance aspects such as availability, latency, or error rates.

SLA reports are typically shared in monthly meetings with senior management, enabling data-driven decisions about investments or organizational changes. Modern monitoring platforms can automatically generate SLA, MTTR, and MTBF reports for any segment of your infrastructure.

Examples of SLA Metrics:

- Monthly network connection availability per site
- Monthly business application availability per application
- Monthly end-to-end business process availability per site
- Monthly average MTTR

Balancing Performance and Resource Usage

Sustainability requires IT operations to balance performance with resource consumption. Sometimes, reducing resource usage is more valuable than maximizing performance. Evaluate the cost-effectiveness of IT and OT investments by comparing maintenance costs before and after implementing predictive maintenance and monitoring improvements.

Best Practices:

- Directly monitor electricity consumption of equipment
- Use analytics to identify unused resources for decommissioning
- Apply capacity planning to manage energy and right-size infrastructure
- Share insights with stakeholders for collaborative decision-making

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

I-VERTIX NeDi: DISCOVERY & MONITORING FOR IT/OT NETWORKS

Overview

i-Vertix NeDi extends automated network discovery and monitoring to both IT and OT, building a complete, continuously updated topology from your core switches down to edge devices. By leveraging multi-protocol Layer-2 discovery (SNMP, LLDP/CDP/FDP), NeDi walks the network graph, enumerates neighbors, and persists relationships so you can visualize how everything connects—servers, workstations, and industrial devices such as **Hirschmann** switches and **Cisco Industrial Ethernet (IE)** platforms.

How Discovery Works

Seed & Walk

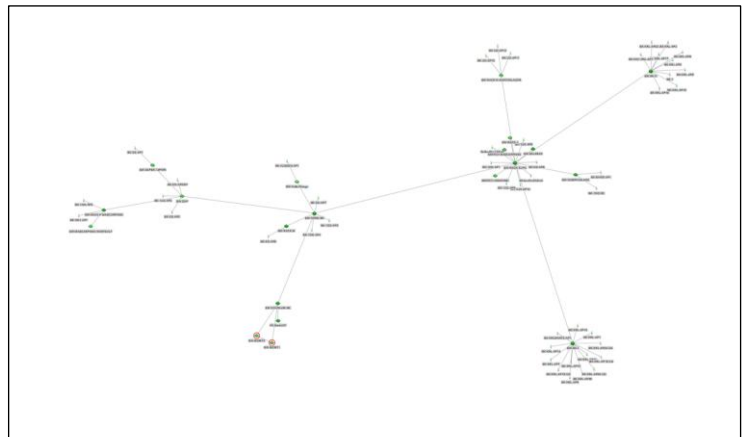
- Start from one or more seed devices (typically core/aggregation switches).
- Use SNMP to read neighbor tables (LLDP/CDP), bridge-MIBs, ARP tables, VLAN membership, and port states.
- Traverse links to discover downstream devices iteratively, storing *device ↔ interface ↔ VLAN* relations and link attributes (e.g., throughput/duplex).

Industrial/OT Awareness

- NeDi's discovery logic and device definition library recognize common OT vendors (e.g., Hirschmann, Cisco IE), exposing what the device publishes via standard MIBs and LLDP/CDP—so topology mapping remains consistent across ruggedized switches and controllers used in plants, utilities, and transport.

Auto-updated Topology

- Scheduled scans reconcile additions, moves, or cabling changes; topology views are refreshed automatically



PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

Comprehensive MAC & IP Inventory (Including SCADA/PLC)

NeDi builds an end-system inventory by correlating Layer-2 data across discovered infrastructure:

- **MAC Address Inventory:** Every MAC seen on the network is captured and indexed.
- **Port & VLAN Mapping:** For each MAC, NeDi records the exact network device, interface, and VLAN where it is attached.
- **IP Correlation:** When Layer-3 data is available (ARP, DHCP, routing), the associated IP address is linked to the MAC entry.
- **Vendor Identification:** OUI lookup classifies the vendor/manufacturer of each MAC (e.g., OT controllers, HMIs, cameras).
- **OT Device Types:** Because MAC/IP inventory is protocol-agnostic, SCADA servers, PLCs, HMIs, sensors, and rugged switches are inventoried alongside IT assets—giving a single source of truth for converged environments.

Top Node Vendors		
Vendor		Nodes
 Siemens AG		110
 WAGO Kontakttechnik GmbH		76
 VMware		61
 ?		45
 Intel Corporate		30
 SIEMENS AG		27
 Zhejiang Dahua Technology Co		22
 Hewlett Packard		20
 SOCOMEC		15

Result: You know **what** is connected, **where** it is connected, **on which VLAN**, and **who manufactured it**—for both IT and OT endpoints.

Classification & Shadow IT Governance

To keep large estates under control, NeDi includes device classification and governance features:

- **Device Status Classification:** Mark discovered endpoints as *authorized*, *under review*, or *unauthorized* to manage Shadow IT and OT-side additions systematically.
- **Node & Vendor Summaries:** Roll-up views aggregate by location, vendor, and device type for quick audits and compliance reviews.

Visualizations & Operational Use

- **Automated Topology Map:** Autogenerates a map with device-to-device relations; optional throughput indicators help spot oversubscribed links.
- **Manual Map (Custom Background):** Place discovered nodes on plant/site schematics (e.g., Visio/draw.io) to mirror physical layout for field technicians.

Why This Matters for OT

In converged IT/OT networks, change is constant: new PLC lines, HMI replacements, maintenance laptops, and smart sensors appear daily. NeDi turns these dynamics into controlled, visible, and auditable events:

- **Security & Compliance:** Detect unauthorized endpoints and unapproved OT changes rapidly.
- **Operational Resilience:** Faster root-cause analysis when issues are tied to specific ports/VLANs or link saturations.
- **Documentation at Scale:** Keep plant and branch diagrams current without manual rewrites; export artifacts to change records.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

MONITORING OT DEVICES WITH I-VERTEX

Modern OT environments are highly diverse, featuring a mix of protocols, device types, and connectivity requirements. i-Vertex is designed to natively support this diversity, providing robust, scalable, and flexible monitoring for industrial and operational networks.

Native Support for MQTT Brokers

i-Vertex offers out-of-the-box integration with leading MQTT brokers, including Eclipse Mosquitto, RabbitMQ, ActiveMQ, and others. MQTT is a lightweight, publish-subscribe protocol widely adopted in industrial IoT for its efficiency and scalability.

How it works:

- OT devices (such as PLCs, sensors, and controllers) publish telemetry data (e.g., temperature, status, alarms) to topics on an MQTT broker.
- i-Vertex connects as a subscriber to these brokers, collecting messages in real time.
- Data from hundreds or thousands of devices can be ingested, visualized, and used to trigger alerts or automation.

Example:

A factory floor with 200 temperature sensors and 50 PLCs, all publishing data to an Eclipse Mosquitto broker. i-Vertex subscribes to relevant topics, aggregates the data, and provides dashboards and alarms for abnormal readings or device failures.

Native Support for Modbus

i-Vertex natively supports Modbus, one of the most common protocols in industrial automation.

How it works:

- i-Vertex polls Modbus-enabled devices (PLCs, RTUs, energy meters) to read registers and coils.
- Data such as process values, equipment status, and alarms are collected and monitored.
- Custom polling intervals and register maps can be configured for each device type.

Example:

Monitoring a set of Modbus-connected energy meters in a power substation, i-Vertex collects real-time consumption, voltage, and fault status, alerting operators to anomalies.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertex.com
PEC: pgumgmbh@pec.it
Web: i-vertex.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

Native Support for Cameras and Environmental Sensors

i-Vertex provides native integrations for a wide range of cameras and environmental/security sensors, including brands such as AKCP, Hikvision, Hanwha, and Mobotix.

How it works:

- i-Vertex communicates with these devices using SNMP, HTTP APIs, or vendor-specific protocols.
- It can monitor camera status, storage health, motion detection events, and environmental parameters (temperature, humidity, door status, etc.).
- Alarms can be set for offline devices, tampering, or threshold breaches.

Example:

A logistics center uses AKCP sensors for temperature and door monitoring, and Hikvision cameras for security. i-Vertex provides unified dashboards and sends alerts if a cold room exceeds temperature limits or a camera goes offline.

Native Support for Industrial Network Devices

i-Vertex is built to monitor industrial-grade network equipment from vendors such as Hirschmann, Cisco (including Industrial Ethernet series), Huawei, and others.

How it works:

- Uses SNMP, LLDP/CDP, and vendor-specific MIBs to discover, inventory, and monitor switches, routers, and firewalls.
- Tracks device health, port status, VLANs, link utilization, and topology.
- Supports ruggedized and OT-specific devices, ensuring visibility across harsh environments.

Example:

A manufacturing plant with Hirschmann and Cisco IE switches: i-Vertex maps the network topology, monitors link status, and alerts on port errors or device failures, ensuring reliable plant connectivity.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertex.com
PEC: pgumgmbh@pec.it
Web: i-vertex.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

Native Support for HMS Netbiter Argos (Cloud-Based)

i-Vertex integrates with HMS Netbiter Argos, a cloud-based platform for remote monitoring of industrial assets.

How it works:

- i-Vertex connects to the Argos cloud API, automatically discovering connected devices and sensors.
- Supports monitoring of hundreds of technologies—such as generators, pumps, HVAC, and more—regardless of the underlying protocol (Modbus, SNMP, proprietary).
- Enables centralized monitoring and alerting for geographically distributed assets.

Example:

A utility company uses HMS Netbiter Argos to connect remote water pumps and generators. i-Vertex pulls operational data from Argos, providing a single-pane-of-glass view and alerting on equipment faults or maintenance needs.

Summary

i-Vertex delivers a unified, scalable solution for monitoring the full spectrum of OT devices and protocols. With native support for MQTT, Modbus, leading camera and sensor brands, industrial network equipment, and cloud-based platforms like HMS Netbiter Argos, i-Vertex empowers organizations to achieve comprehensive visibility, rapid incident response, and operational excellence across IT and OT environments.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertex.com
PEC: pgumgmbh@pec.it
Web: i-vertex.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

VISUALIZING AND MANAGING OT MONITORING WITH I-VERTEX

Visualizing Monitored Devices with Maps

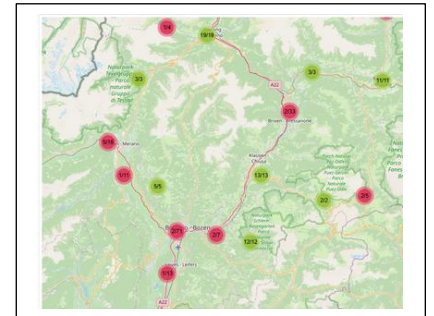
i-Vertex provides multiple ways to visualize your monitored assets, making it easy to understand both the physical and logical layout of your infrastructure:

- **Geo Maps:**

Display all monitored sites on an interactive world or country map. Each site is color-coded by status (e.g., green for healthy, red for critical alarms). Clicking a site zooms in to show local devices and their health.

Example:

A multinational company can see all its plants across Europe at a glance. If a plant in Milan has a network issue, it turns red on the map, allowing instant identification and drill-down.

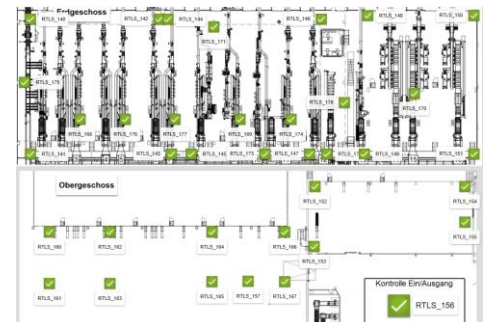


- **Plant Maps:**

Overlay device icons on a floor plan or plant schematic. Devices are positioned according to their real-world location (e.g., production lines, control rooms, cold storage). Status indicators show live health.

Example:

In a food processing plant, temperature sensors, PLCs, and cameras are placed on the digital plant map. If a cold room sensor fails, its icon turns yellow, and the maintenance team can immediately locate it.



- **Topology Maps:**

Automatically generated network diagrams show how switches, routers, OT devices, and endpoints are interconnected. Links are color-coded by status or bandwidth utilization.

Example:

A plant network manager can view the full topology, quickly spotting bottlenecks.

Creating Dashboards for the Big Picture

i-Vertix dashboards are highly customizable, allowing users to build views tailored to their needs:

- **Global Operations Dashboard:**

Shows total devices, active alarms, network health, and recent incidents across all sites. Useful for NOC teams and executives.

- **Plant Manager Dashboard:**

Focuses on a single plant or production area. Displays key metrics such as uptime, environmental sensor status, production line health, and security alerts. Includes widgets for energy consumption, maintenance schedules, and compliance status.

Example:

The plant manager at a beverage factory sees a dashboard with:

- Real-time temperature and humidity readings for storage areas
- Status of all PLCs and critical sensors
- Alerts for any unauthorized device detected on the network
- Energy usage trends and predictive maintenance reminders

- **Custom Role-Based Dashboards:**

Maintenance teams can have dashboards showing only devices they are responsible for (e.g., HVAC, pumps), while security teams see only cameras and access sensors.

Role-Based Access Control (ACL) for Targeted Visibility

With i-Vertix's granular ACL system, every team member sees exactly what matters to them—no more, no less:

- **Single Plant Access:**
A technician assigned to the Bolzano plant only sees devices, alarms, and maps for that location.
- **Multi-Plant or Regional Overview:**
Area managers can access dashboards and maps for all plants in their region, comparing performance and responding to cross-site issues.
- **Geographic Overview:**
Executives or NOC staff can view the entire organization's health on a global map, drilling down as needed.

Example Scenarios:

- A security officer is granted access only to camera and door sensor data for the Milan site.
- An OT engineer responsible for all Italian plants can view and compare network topologies and alarms across those sites.
- The CEO has a high-level dashboard summarizing uptime, critical incidents, and compliance across all locations.

INTEGRATING OT MONITORING WITH SECURITY PLATFORMS: FORWARDING EVENTS TO SIEM

Modern organizations face increasingly complex security challenges, especially as IT and OT environments converge. i-Vertex addresses this by enabling seamless forwarding of monitored events, statuses, and metrics from both IT and OT devices to security platforms—such as SIEM (Security Information and Event Management) systems—using HTTP stream connectors.

How It Works

- **HTTP Stream Connectors:**
i-Vertex can be configured to send real-time monitoring data—including device statuses, alarms, performance metrics, and event logs—directly to SIEM solutions via HTTP stream connectors.
- **Supported Security Platforms:**
This integration is compatible with leading SIEM products (e.g., i-Vertex SIEM, Splunk or others) and other security analytics platforms.

Data Types Forwarded:

- Events: device health and status changes
- Metrics: all metrics regarding the monitored devices
- Environmental and process anomalies from OT sensors

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertex.com
PEC: pgumgmbh@pec.it
Web: i-vertex.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

Why This Is Important

- **Centralized Security Monitoring:**
By forwarding all relevant events to a SIEM, organizations gain a unified view of security across IT and OT domains, enabling faster detection and response to threats.
- **Advanced Analytics & Correlation:**
SIEM platforms can correlate i-Vertex data with logs from firewalls, endpoints, and other sources, helping identify complex attack patterns or insider threats.
- **Compliance & Forensics:**
Storing monitoring data in a SIEM supports regulatory compliance (e.g., NIS2, IEC 62443) and provides a forensic trail for incident investigations.

Summary

By integrating i-Vertex with SIEM and other security platforms via HTTP stream connectors, organizations can achieve real-time, centralized security monitoring and analytics for both IT and OT environments. This not only strengthens cyber resilience but also supports compliance, incident response, and operational transparency.