

PT ISIM 5.12. Architecture

■ positive education

In this course, you will learn about the components of PT ISIM, its architecture and licensing policy, as well as how to install and adapt it to your infrastructure.



Introduction



PT ISIM overview



Licensing policy



Using the product and adapting it to the infrastructure



Deploying the product



Test



Summary

Time to complete:

~60 minutes



Course expert

Dmitriy Darensky

Head of Industrial Cybersecurity Practice



Course expert

Alexandr Sadunin

ICS Product Practice Lead

Topics covered in this course

- PT ISIM overview
- Licensing policy
- Using the product and adapting it to the infrastructure
- Deploying the product

BEGIN



PT ISIM overview

Industrial infrastructures have long been the primary targets of cyberattacks. Vulnerabilities of these infrastructures are often related to both technical aspects and industry-specific factors, such as:

- The use of workstations that don't meet project requirements, including those with internet access
- Uncontrolled access to the OT network, including via remote connections
- The use of default passwords and shared accounts
- The lack of network segmentation
- The use of infected and unauthorized USB devices
- The lack of regular updates for software and threat detection rules

Detecting sophisticated targeted attacks requires analysis of anomalies and suspicious activities in the network and for security events to be identified at the level of the operating system and automation system. **It is important to identify dangerous process control commands in industrial control system software and establish logical connections between all these actions.** To address the tasks above, a unified system is required that can simultaneously monitor OT traffic and track activity on nodes.



What is PT ISIM?

PT ISIM is a comprehensive cybersecurity system for OT infrastructures* with a wide range of tools and extensive industrial expertise designed to analyze traffic, collect events, and safeguard OT networks, industrial enterprises, and engineering infrastructure facilities.

* Operational technology (OT) refers to the use of IT in hardware and software systems that monitor and control physical processes, devices, equipment, and engineering infrastructure in industrial environments. Unlike information technology (IT), which centers on data processing and information flows, OT is about direct control and automation of industrial processes and production operations.

PT ISIM includes a mandatory component and optional components.

Mandatory component

PT ISIM View Sensor

View Sensor analyzes and stores network traffic, scans the network, receives and manages security events and inventory data transmitted by host agents, and calculates vulnerabilities.
It is installed at the access or aggregation level of the OT network or ICS.

Optional components

PT ISIM Endpoint Agent

Collector is deployed on SCADA servers and workstations and is responsible for antivirus protection, event collection, inventory maintenance, vulnerability detection, and response.

PT ISIM Overview Center

Overview Center is a management server for groups of companies that collects events from sensors and centralizes the management of

PT ISIM Collector

Collector collects traffic and scans and manages host agents in remote and isolated OT networks segments.

PT ISIM is an XDR (extended detection and response) product. It is one of the key components of security operations centers (SOCs) which respond to cybersecurity incidents in OT networks.

Application area

- Industrial control systems (ICS)
- Engineering infrastructure control systems of public utilities
- Railway traffic control systems
- Automated control systems of critical infrastructure facilities
- Engineering infrastructure control systems of data centers, business centers, and retail centers
- Industrial plants and facilities with distributed infrastructure
- Industrial Internet of Things (IIoT)

Application area

- Automatized industrial control systems (ICS)
- Engineering infrastructure control systems of public utilities
- Railway traffic control systems
- Automated control systems of critical infrastructure facilities
- Engineering infrastructure control systems of data centers, business centers, and malls

Purpose

- Intrusion detection
- Continuous cybersecurity assessment of OT networks
- Protection of endpoints from cyberthreats
- Monitoring of staff and contractor actions
- Detection of security breaches and attacks on ICSs

- Industrial plants and facilities with distributed infrastructure
- Industrial Internet of Things (IIoT)
- DICOM-compatible systems and networks of healthcare institutions

- Timely detection of incidents and informing of individuals in charge of cybersecurity
- Creation of a trusted data source for efficient investigation of cybersecurity incidents
- Incident analysis, cause identification, and consequence assessment
- Recommendations for mitigation and prevention of incidents
- Ensuring compliance with regulatory guidelines (including FSTEC orders 31 and 239, 187-FZ, and coordination with GosSOPKA centers)

- Response to detected cybersecurity threats
- Simple integration with existing security processes
- Support for cybersecurity incident response and investigation
- OT infrastructure inventory and monitoring of network integrity
- Visualization of infrastructure, events, and security incidents
- Tailored approach
- Fit for industrial settings
- Setting asset importance

- Continuously updated database with thousands of out-of-the-box rules for detecting security violations
- Building of incident chains
- Customized tools for network event analysis
- Storage and export of copies of traffic, events, and network incidents for investigation
- Monitoring of critical process settings
- Extraction of files to be checked from traffic

PT ISIM components

PT ISIM is a hardware and software suite with a choice of several hardware platforms (typically 1U and 2U rack servers) and special software. All PT ISIM components run on Debian: Debian 10.X or 12.X. PT ISIM components are divided into four functional groups.

1. Data collection

1.1. Data sources

The system collects and processes data from the following sources:

- Network traffic copies captured via SPAN or RSPAN ports or TAPs
- Endpoints, such as operator workstations, engineer workstations, and servers running Windows or Linux
- Specialized industrial devices, such as programmable logic controllers (PLCs), remote input/output modules, and communication equipment

1.2. Components

Data collection components deliver data and manage edge nodes.

PT ISIM Endpoint agents (host agents)

- Purpose: monitoring the state of endpoints and extracting data from the operating system and applications.
- Location: SCADA servers, engineer workstations, and workstations.
- Features:
 - Collect data and security events from application and operating system logs.
 - Collect data about installed software, software versions, and hardware.
 - Ensure antivirus protection.
- Connections: host agents deliver data to local sensors or collectors.

Servers and agents communicate over TCP or HTTPS (HTTP is the backup protocol).

PT ISIM Collector

- Purpose: collecting events and configuration data from network nodes, managing endpoint agents, and aggregating traffic from remote segments to optimize communication channels.
- Location: remote sites or network segments with unidirectional transmission channels.
- Features:
 - Collects events and configuration data and manages endpoint agents.
 - Polls or scans OT network devices.
 - Tunnels traffic copies.

- Connections: Collector transmits data to View sensors.

Collector interacts with other components over TCP and UDP.

PT ISIM View Sensor (microView, netView, or proView).

- Purpose: collecting events and configuration data from network nodes and managing endpoint agents when there is no need to use PT ISIM Collector.
- Location: local sites or isolated network segments.
- Features:
 - Collects events and configuration data and manages endpoint agents.
 - Polls or scans OT network devices.
 - Tunnels traffic copies.
- Connections: View Sensor transmits aggregated security event data to PT ISIM Overview Center.

Management interfaces use SSH and HTTPS (HTTP is the backup protocol) for system component connections and interactions.

2. Processing, analysis, and presentation of data —

2.1. Functionality

At this stage, the system transforms data flows into analytical reports and alerts:

- Inventory: automatic discovery of assets, asset configurations, installed software, and software versions.
- Process monitoring: monitoring of critical process signals and detection of dangerous commands or abnormal telemetry.
- Detection of security events, incidents, and threats: detection of attacks on industrial control systems, vulnerability exploitation, and illegitimate activity in OT networks.
- Investigation: tracking and recreating the chronology of events and incidents using accumulated events and traffic history.

2.2. Components

Data is processed, analyzed, and displayed by PT ISIM View Sensor components. Specific editions are selected based on the volume of data to be collected and processed:

- microView Sensor: processes up to 10 Mbps of a copy of incoming traffic, as well as events and configuration data from no more than 10 agents.
- netView Sensor or proView Sensor: processes 100–500 Mbps+ of traffic, as well as events and configuration data from 100 or more agents.

3. Centralized management of system components and users

At this level of system hierarchy, you can control the entire corporate infrastructure.

PT ISIM Overview Center

- Purpose: centralized monitoring and management of all system sensors.
- Location: cybersecurity situation center (SOC) or headquarters.
- Features:
 - Collects and consolidates data from all subordinate sensors.
 - Provides unified configuration and update of components.
 - Connections: interacts with global update servers, expert knowledge bases, and external enterprise cybersecurity systems.

Overview Center interacts with other components over TCP.

PT Management and Configuration

- Purpose: centralized management of system users.
- Location: PT ISIM View Sensor or PT ISIM Collector server.
- Features:
 - Manages accounts.
 - Enables authentication and synchronizes user access rights via Microsoft Active Directory.
 - Provides single sign-on to allow users to switch between web interfaces of products without re-authentication.

PT MC interacts with other components over TCP.

4. Users and integration —

User roles:

- ICS specialists: monitor commands and deviations in critical process signals to prevent accidents.
- IT administrators: monitor software configurations, software versions, and hardware.
- Information security specialists: analyze events, OS logs, and application logs and detect and investigate attacks.

Integration into a SOC:

The system transmits data to related products for comprehensive protection:

- MaxPatrol SIEM manages events and incidents.
- PT Sandbox checks suspicious files in traffic and from host agents.

Hardware platform specification

PT ISIM can be supplied as a trusted hardware and software suite. PT ISIM View Sensor, ISIM Endpoint Server, and ISIM Endpoint Management can be deployed together on any product version. PT MC can be installed on its own or together with PT ISIM Overview Center.

Advantages of this specification:

1

Ready for industrial environments. The hardware is adapted to industrial settings by being resistant to temperature, vibration, and electromagnetic interference.

2

High performance. Optimized hardware ensures fast event processing (analytics, incident response) even in real-time.

3

Reliability and fault tolerance. Built-in redundancy mechanisms (disk mirroring and redundant power supplies) minimize downtime of critical infrastructure.

4

Security. An isolated environment reduces the risks of unauthorized access.

5

Ease of implementation. Preinstalled software configured for the OT environment.

6

Compliance with industry standards. Certified for use in ICS systems.



NS-1050

An entry-level model suitable only for PT ISIM microView Sensor (it does not store events and can be used to view only incidents (not original events))

Up to 10 Mbps, up to 10 agents
ISIM Endpoint

NS-2010

A higher-end model for PT ISIM netView Sensor or PT ISIM proView Sensor (proView supports uploading SCD (substation configuration description) files according to IEC 61850)

Up to 500 Mbps, up to 100 ISIM Endpoint
Agents

Supported network protocols

ABB SPA BUS	IEC 60870-5-101 (IEC101)
ABB ACP	IEC 60870-5-104 (IEC104)
ABB DEBUG PORTS	IEC 61850 GOOSE
ABB FREELANCE	IEC 61850 MMS
ABB ODBC	INA2
ADS (AMS)	INA2000
ALPHA.SERVER CONFIGURATOR	ISACOM
ANSL	LLDP
ARP	LLMNR
BACHMANN RPC TCP	MELSOFT
BACNET/IP	MODBUS
CDP	MQTT
CE_A	NETBIOS NAME SERVICE (NBNS)
CIP (ETHERNET/IP)	NTP
CODESYS 2	OPC DA
CODESYS 3	OPC UA
COS	PHOENIX
DCE/RPC	PROFINET DCP
DELTA V COMMISIONER	PRP
DELTA V FIRMWARE UPGRADE	PUSH EVENTS
DHCP	R200 (ИТК «КВИНТ»)
DIAG GW (ИТК «КВИНТ»)	SIEMENS DIGSI 4
DICOM	SIEMENS SPPA
DNS	SIEMENS S7COMM (STEP7)
ETHERCAT	SIEMENS S7COMM-PLUS, OMS+ (TIA PORTAL)
FINS (OMRON)	SLMP
FTP	SMB
HiDISCOVERY	SNMP
HONEYWELL EPICMO	SSH
HONEYWELL CDA	TELNET
HONEYWELL CDA	TFTP
HTTP	UMAS
ICMP	VNET/IP
	ДК «КУРС-2»

Analyzed protocols

These protocols are analyzed in sufficient detail to retrieve message attributes and their values from traffic and use them for correlation. Each protocol is usually associated with several types of incidents and specific or unique detection rules.

Recognized Protocols

For these protocols, the traffic collection and analysis component includes only rules for detecting unauthorized connections. The key difference when compared to other protocols is that there are no specific or unique rules for application-level incident detection.

PT Industrial Security Threat Indicators (PT ISTI)

PT ISIM detects cybersecurity violations using PT Industrial Security Threat Indicators (PT ISTI), a proprietary database of industrial cyberthreats. It helps you to do the following:

- Detect attacks on ICS software or hardware (node scanning, vulnerability exploitation) while the attacks are still at an early stage.
- Identify system configuration errors (weak passwords or deactivated encryption).
- Detect potentially unsafe network practices, such as outdated protocols, and undocumented and unsafe commands used for controlling hardware (including PLCs, industrial switchboards, and terminals).

Industrial expertise



Operating systems

Windows 7–10

Windows Server 2012–2019

Linux: Debian, Ubuntu, CentOS,
Red Hat,

Industrial automation software

AVEVA

B&R

Schneider Electric

ABB

Siemens

Emerson

General Electric

Honeywell

Rockwell Automation

Bachmann

Mitsubishi Electric

Omron

Yokogawa

Beckhoff

18 000

rules and industrial security threat
indicators out of the box

130+

industrial
and general-purpose network
protocols supported

PT ISIM experts regularly update PT ISTI with new signatures and rules for detecting attacks on industrial equipment and software.

NEXT



Licensing policy

License life cycle

Initial license purchase

The purchase of any PT ISIM component (View Sensor, Overview Server, or Endpoint) comes with the need to buy a basic license for this component, depending on the required functionality and specific usage environment.

Licenses can be granted for a limited period of time (term licenses) or for the entire duration of exclusive rights. The default license term is one (1) year, but a different term may be agreed upon, provided it is no less than one year.

Licenses for PT ISIM software, supplied as part of PT ISIM hardware and software suites, are granted for the entire duration of the exclusive rights.

Renewal of a term license

Term licenses must be renewed before they expire.

To renew a term license, the customer needs to buy a renewal license. By default, the renewal license is valid for one year, but a different term is also possible on request.

License (update provision period) expiration

When a term license expires (that is, when it reaches the expiry date indicated in the license certificate), it becomes invalid; updates and technical support for PT ISIM are no longer provided. If the license is not renewed, PT ISIM must be uninstalled after license expiration.

Licenses granted for the entire exclusive rights period (perpetual licenses) do not require renewal. However, from the date the update period specified in the license

require renewal. However, from the date the update period specified in the license certificate expires, access to Technical Support, software updates, and the PT ISTI expert rules database is terminated until the end user obtains the appropriate update license.

PT ISIM components and their functions

PT ISIM is a software solution or a hardware and software suite that includes network traffic analysis servers (sensors), a server, endpoint protection agents, and SOC-level analysis and control servers.

The system includes the following components:

1

View Sensor is a server that collects and analyzes network traffic. This sensor receives a traffic copy from the ICS network and performs the main processing steps. It also provides a management interface. This is a mandatory component of the system.

Three versions of sensors are available, with different features and scopes (traffic volumes and the number of ICS nodes):

- microView Sensor is a lightweight PT ISIM version for smaller sites (such as water treatment facilities, heating substations, and engineering systems of buildings and industrial plants). It contains a complete PT ISIM knowledge base with protocols and rules (same as other versions) and registers security incidents, but does not log all events. It requires significantly less hardware resources and has been successfully tested on fanless industrial PCs. It is supplied as part of the PT ISIM NS-1050 suite.

- netView Sensor has the most requested features, which include logging and storage of the entire event flow. It can process up to 10,000 network nodes and up to 500 Mbps of traffic.

- proView Sensor provides more extensive configuration options than netView Sensor. It supports extended control over digital communications under IEC 61850 and can scan the network to capture inventory data from Windows and Linux systems.

2

Overview Center is a server for centralized sensor management. It aggregates registered incidents and enables centralized configuration and updates on connected sensors. This component is optional. It is supplied as part of the PT ISIM NS-2010 suite.

3

Endpoint is a protection agent for workstations and SCADA servers within Industrial Control Systems (ICS). Agents are

installed on servers and workstations that are running a compatible OS and are used by operators and/or engineers. These agents connect to Endpoint Server for centralized management and for transmitting cybersecurity events to View Sensor. The license is not tied to the type of node (server or workstation). Agents cannot be installed on network devices or PLCs.

The initial license is acquired during the first purchase of PT ISIM and includes the following:

- A basic license for one or multiple network traffic analysis sensors of the required type
- A basic license for one or multiple sensor control servers (if such components are required)
- A basic license for one or more ICS endpoint protection agents (if such components are required)

Renewal license

When the term licenses expire, the customer needs to purchase renewal licenses for their View Sensors, Overview Centers, and Endpoint Agents (if any) to continue using PT ISIM.

The type and quantity of renewal licenses must fully match the type and quantity of the previously purchased initial licenses.

Product IDs of renewal licenses include the product ID of the basic license followed by the EXT suffix. For example, PT-ISIM-NV-SNR-B2-EXT is a renewal license for 10–19 PT ISIM netView Sensors.

Licenses granted for the entire exclusive rights period do not require renewal. Update licenses (with the -UPD suffix) for 1 year or more must be purchased for such licenses.

License extension

Acquisition of new licenses or license extension may be required in the following cases:

Issue	Solution
The number of geographically distributed traffic capture points has grown or the network traffic speed has significantly increased	The customer may need to purchase: Additional basic licenses (with installation of additional View Sensors) to accommodate the changes in the customer's network architecture Additional licenses for Overview Centers (control servers) if the customer needs the servers to manage a distributed sensor system
Infrastructure has changed	
There is a need to monitor cybersecurity events on ICS workstations and servers	It may be necessary to purchase basic Endpoint licenses agents for the number of servers and workstations where agents need to be installed. Backup or non-production workstations should also be taken into account
System requirements have changed	The specification needs to be revised together with the Positive Technologies team.

NEXT



Using the product and adapting it to the infrastructure

Industrial sectors

To adapt enterprise information security solutions, you have to understand and take into account the key risks and effects of cyberattacks on production and processes. Each industrial sector has its own risks, but they will inevitably lead to financial losses, interruption of production or business, and may even pose a threat to public health. PT ISIM can be used in the following sectors and facilities:

- Electric power
- Fuel industry
- Ferrous and non-ferrous metallurgy
- Chemical and petrochemical industry
- Mechanical engineering and metalworking
- Consumer goods industry
- Facilities that use automated control systems

- Transportation infrastructure facilities
- Engineering systems of civilian, commercial, and production buildings and facilities
- Data centers

An enterprise's IT infrastructure is a comprehensive framework that brings together all information technologies and resources, taking into account the specifics of server and network equipment, software, and network topology.

One of the main tasks of information security is strict segmentation of the network, access control, perimeter protection, and prevention of cyberthreats.

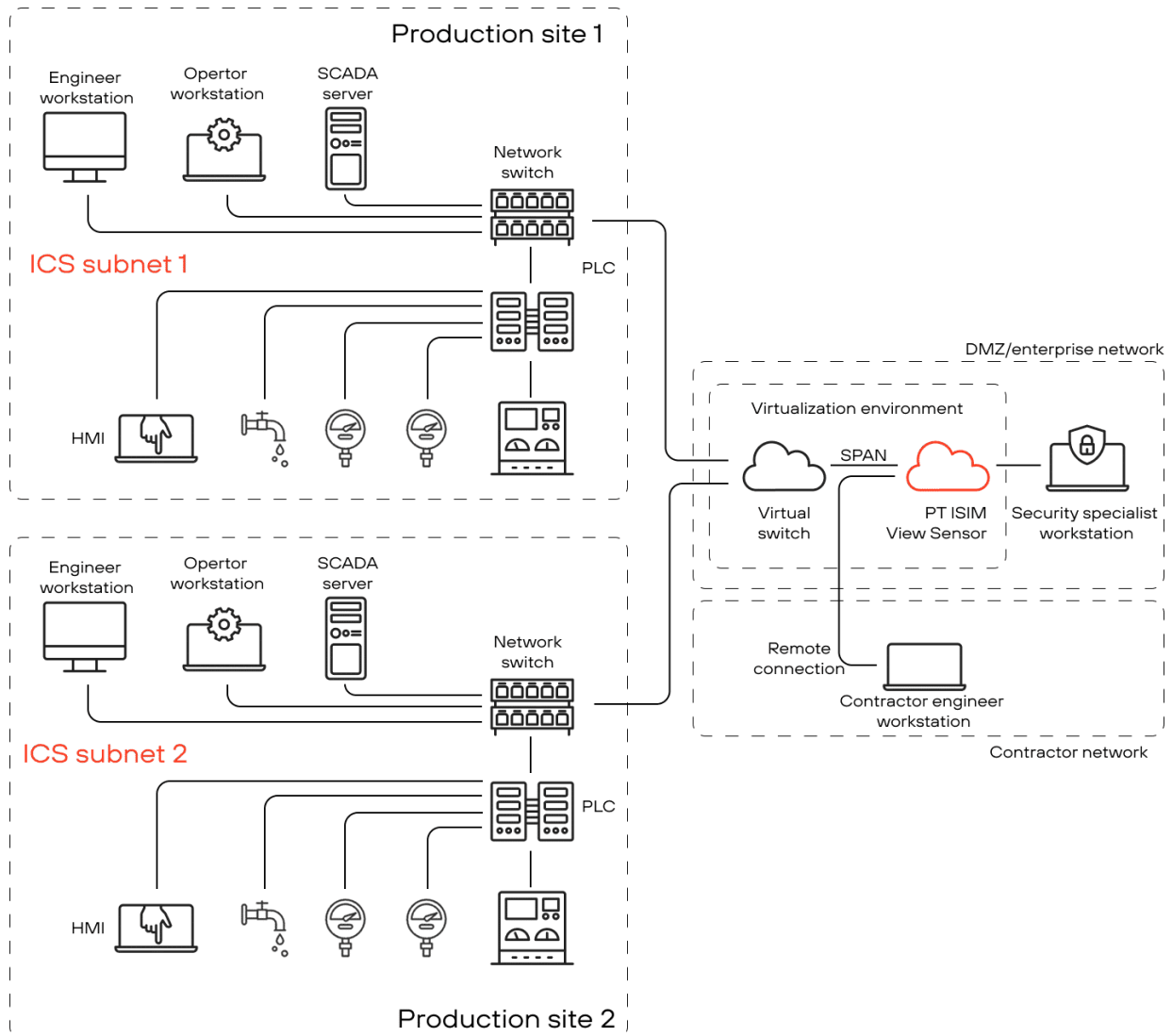
Today, ICSs and OT networks are a blind spot for IT specialists and cybersecurity experts

- | | |
|---|---|
| 1 | Server and network equipment |
| 2 | Software |
| 3 | General system services and  |
| 4 | Programmable logic controllers |
| 5 | Intelligent electronic devices (IED) |

Adapting to the infrastructure

When choosing where to install PT ISIM View Sensor in the customer's infrastructure, take into account all its features, such as whether it is possible to install a software

and hardware suite, or whether a virtual appliance image must be installed on the customer's hypervisor. PT ISIM can work with virtualization environments that support AVX.

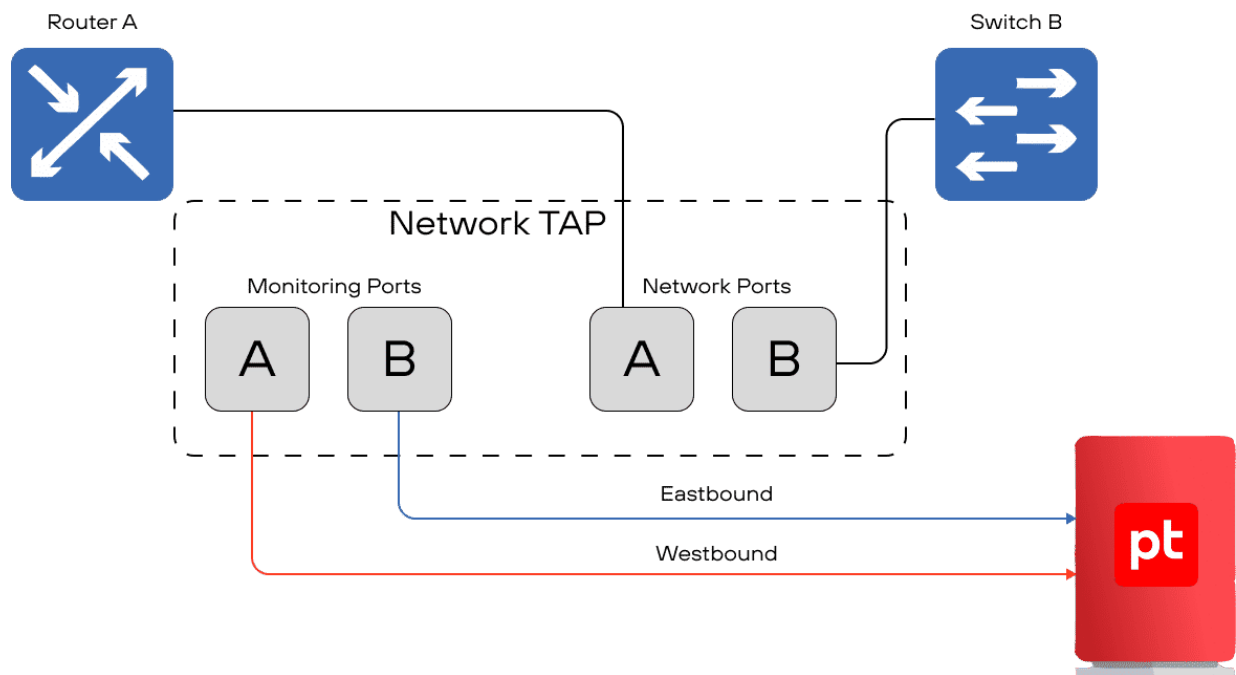


Supported hypervisors:

- VMware Workstation
- VMware vSphere
- Oracle VM VirtualBox

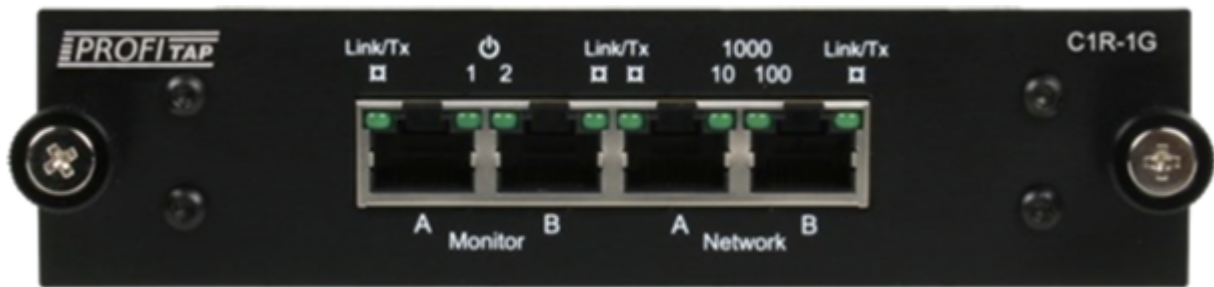
Is it possible to configure port mirroring on necessary switches or must additional network devices be used? These devices are called TAPs, or test access points.

TAP connects the gap in the communication link



Network devices do not support SPAN or port mirroring.

Network TAP



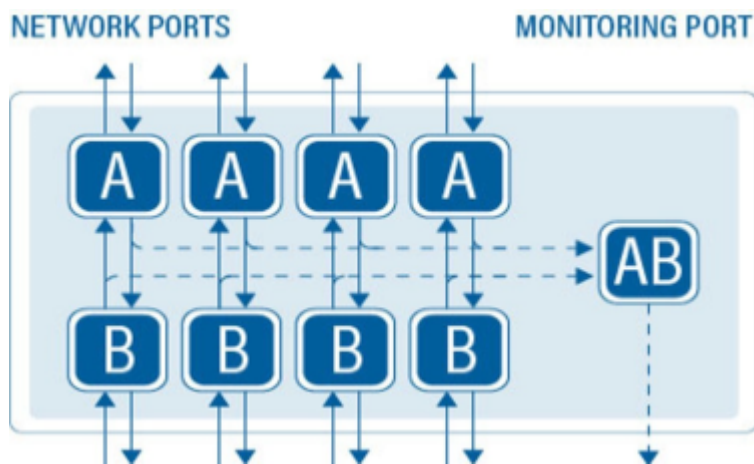
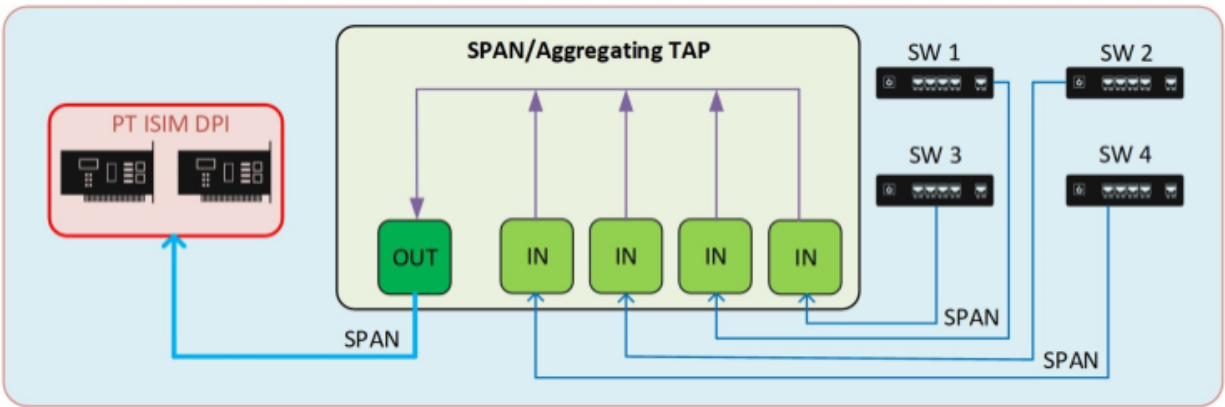
Traffic flow with a network TAP



We could also capture traffic from several SPAN ports and then send a copy of it to several ports to be connected to the analyzing interface of PT ISIM Sensor.

SPAN TAPs (matrix switches) allow you to choose only the necessary data flows to be routed to the sensor.

Multiple SPAN ports



Industrial network standards

Industrial Ethernet (IE) is mainly used for data exchange between PLCs and human-machine interfaces (HMI).

Popular real-time protocols

- Profinet
- EtherCAT
- Ethernet Powerlink

Other: Modbus

Popular IE protocols

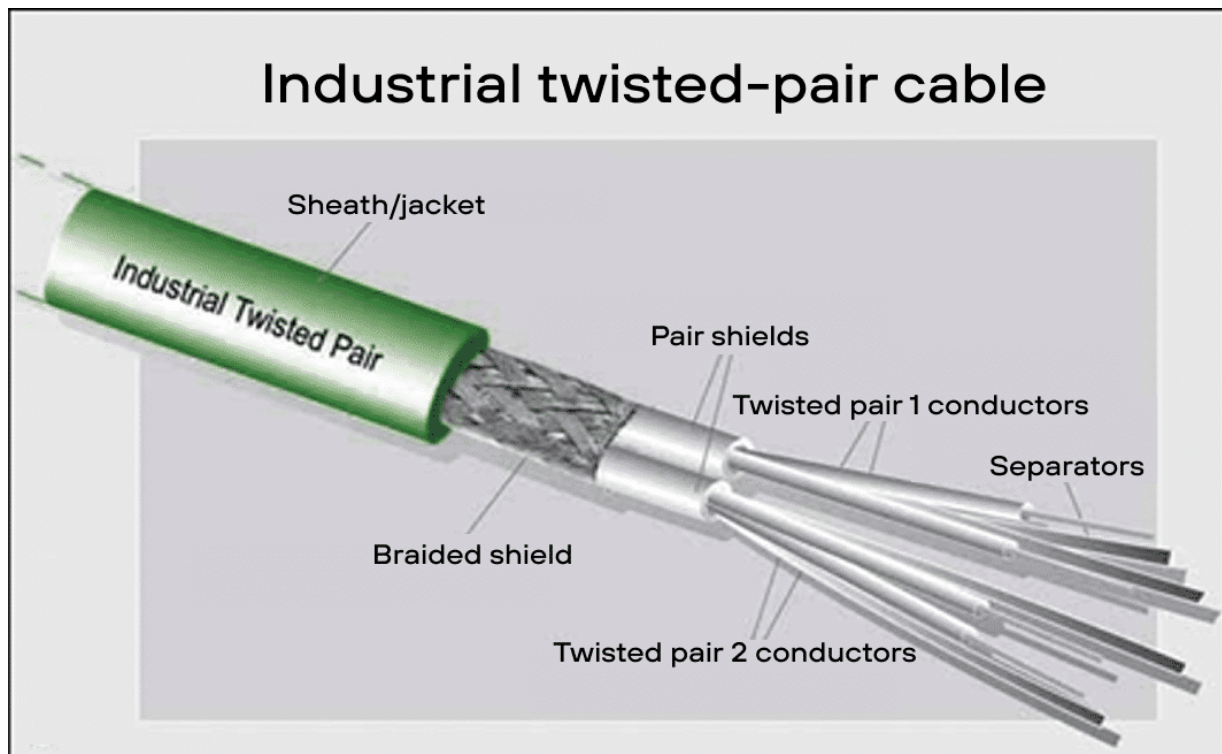
- Siemens S7comm
- S7comm+
- Common Industrial Protocol (CIP)

Other: EtherCAT, EtherNet/IP

- EtherNet/IP
- SERCOS III
- LAN eXtensions for Instrumentation
- Schneider Electric UMIAS
- Yokogawa Vnet/IP
- Modbus TCP

Industrial equipment is usually designed to withstand a wide range of operating temperatures, strong electromagnetic fields, and various humidity, wind speed, and dust levels.

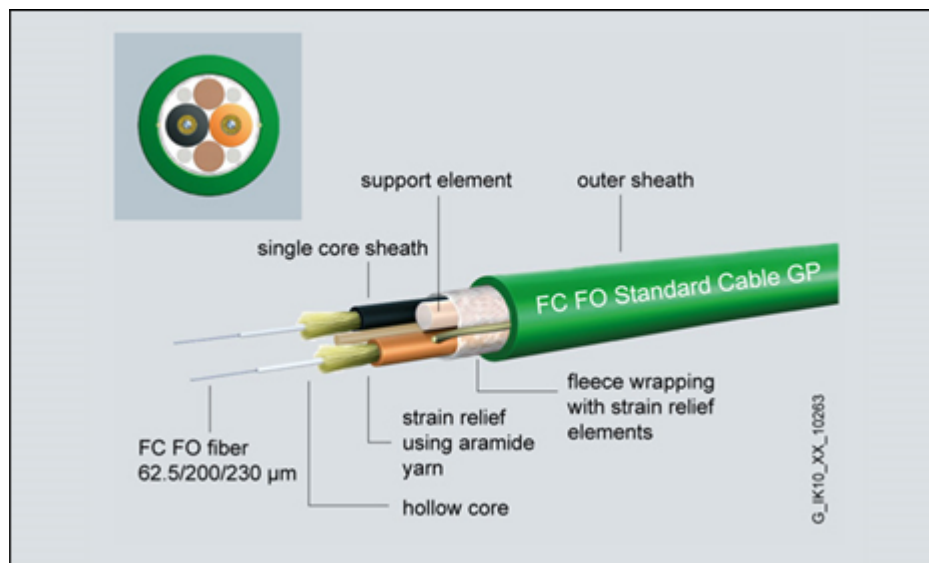
This means increased requirements for the reliability of network cables and connectors.



Industrial twisted pair



Standard IE FC TP GP cable and connectors





AS-Interface (Actuator Sensor Interface)

Ethernet standards

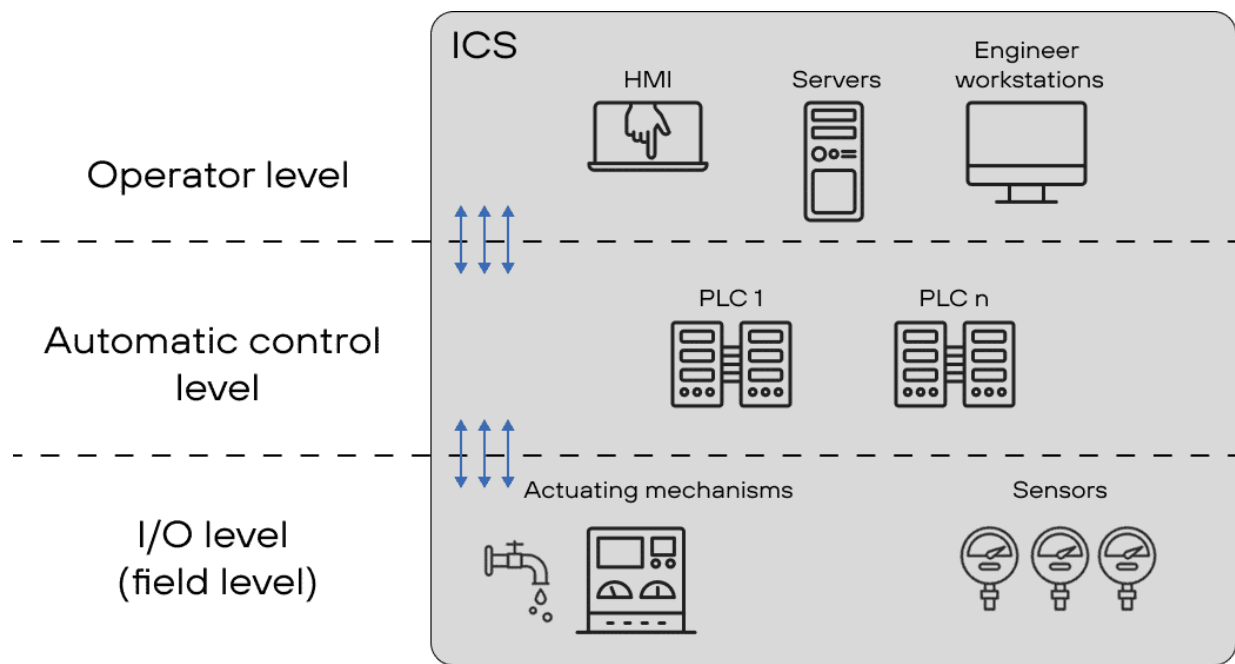
The most popular Ethernet implementations are 10Base-T, 10Base2, 10Base5, 100Base-TX, and 1000 Base-T. If a network uses any of these standards, it likely supports PT ISIM.

Standard	Year of adoption	Description
IEEE 802.3e	1987	1Base5 (StarLAN): 1 Mbps over twisted pair
IEEE 802.3u	1995	100Base-TX, 100Base-T4, 100Base-FX, Fast Ethernet: 100 Mbps (12.5 Mbps) with autonegotiation (compatible with IEEE 802.3i)

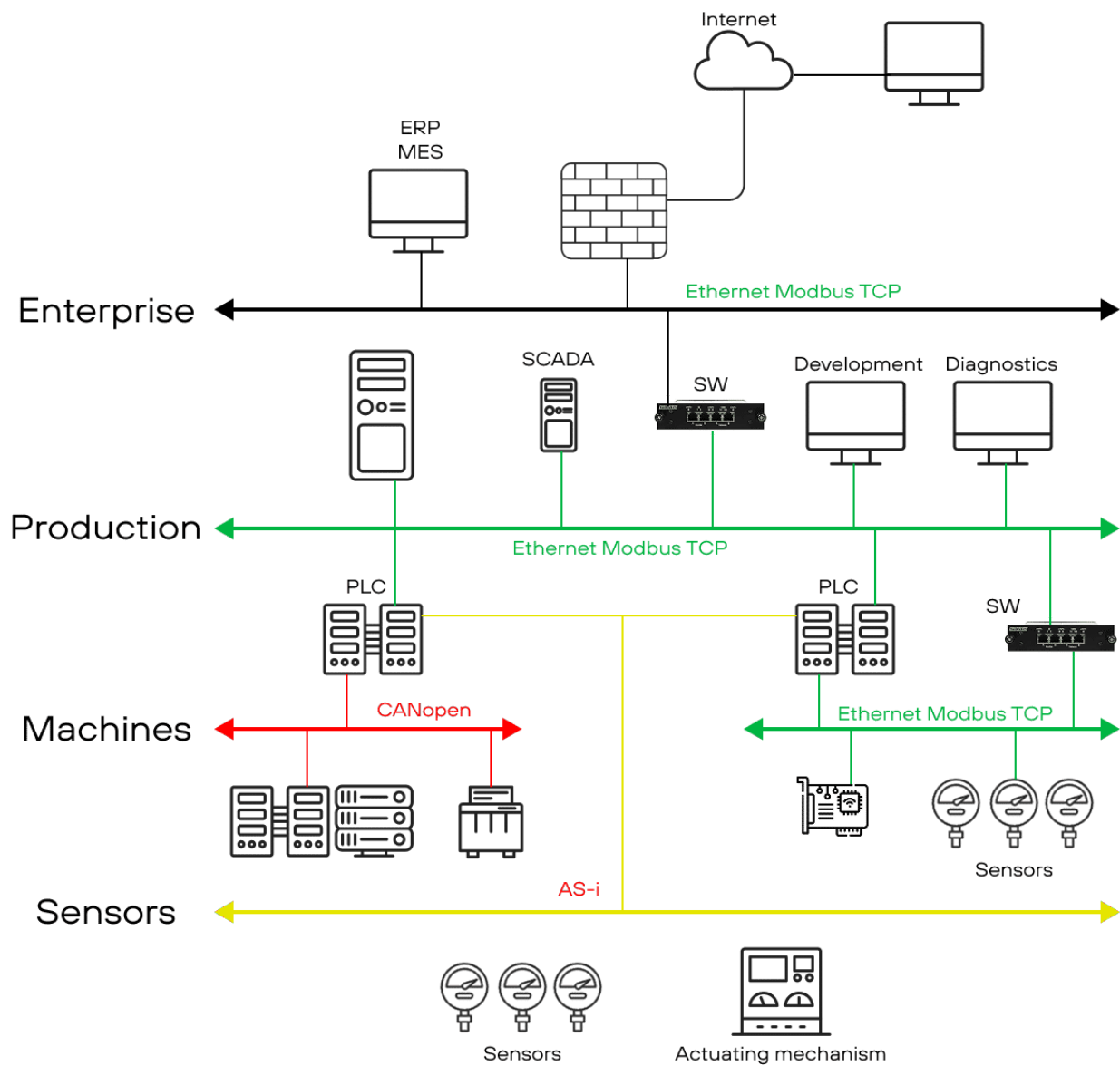
IEEE 802.3x	1997	Full duplex, compatible with DIX
IEEE 802.3z	1998	1000Base-X, Gigabit Ethernet: 1 Gbps (125 MB/s) over optical fiber

Control system levels

In general, all control systems consist of three levels.



Standard topology of a Schneider Electric network

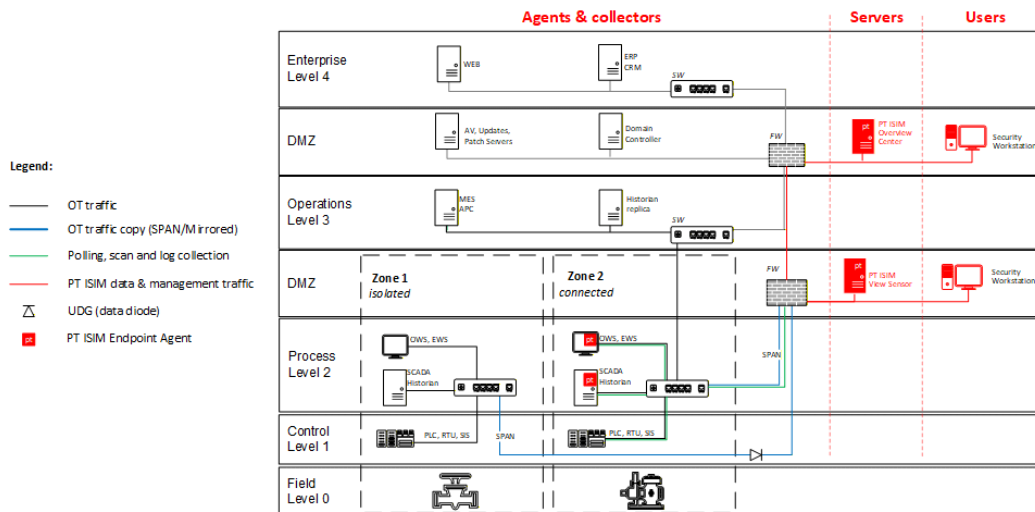


Automated control systems often use several network standards and various types of interfaces and protocols at once. But you need to understand that PT ISIM can be installed only in Industrial Ethernet environments:

- Ethernet Modbus TCP
- CANopen
- AS-Interface

Local industrial control systems (ICS)

PT ISIM. Connectivity diagrams



Example solution for local production sites with several local ICSs

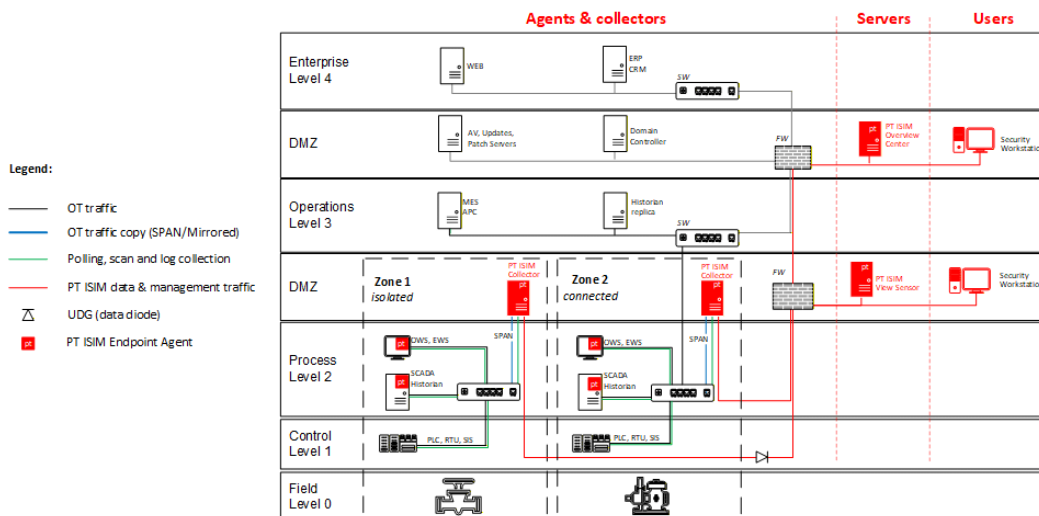
When designing a PT ISIM-based system for local industrial automation systems, you must take into account the architecture of industrial control systems:

- In an enterprise or industrial site, an ICS or an emergency shutdown (ESD) system may be the only system that supports the operation of one process unit.
- These systems can use several controllers combined into a single network, but can have no SCADA servers or operator or engineer workstations.
- In cases like these, service maintenance and updates to controller configurations can be performed locally using an HMI panel or connected mobile workstation.

- A single site can have several process units and therefore several ICSs and ESD systems, both local and connected by a single OT network.

Distributed industrial control system (DCS)

PT ISIM. Connectivity diagrams



Example solution for a distributed production infrastructure with sensors located on each site

When designing PT ISIM-based systems for distributed control systems, you must take into account the architecture of industrial control systems:

- Industrial sites of enterprises with distributed production are usually connected by a single OT network.

- Each site usually has its own SCADA system, and industrial processes are managed locally on-site.
- Centralized production management is generally carried out using dispatch control systems.
- Certain industrial sectors may not have SCADA systems on-site, meaning their functions are performed by dispatch control systems.
- Service maintenance and configuration of ESD systems can only be performed locally.
- A single site can have several process units and therefore several ICSs and ESD systems, both local and connected by a single OT network.

Where to capture traffic from

Let's determine the optimal points for capturing traffic based on the characteristics of local and distributed control systems. Segmenting your network and restricting access to those segments lengthens a hacker's path to target assets but also complicates getting a copy of traffic data. Depending on the size of the network, the number of segments will vary. A small network may have only a few services and therefore few segments. In a large network, conversely, the number of services and network segments will be higher. PT ISIM is primarily designed to capture traffic copies on access switches, which are a perfect point for data collection. However, there may be too many such devices in the network, and installing PT ISIM View Sensor on each one can be expensive and time-consuming.

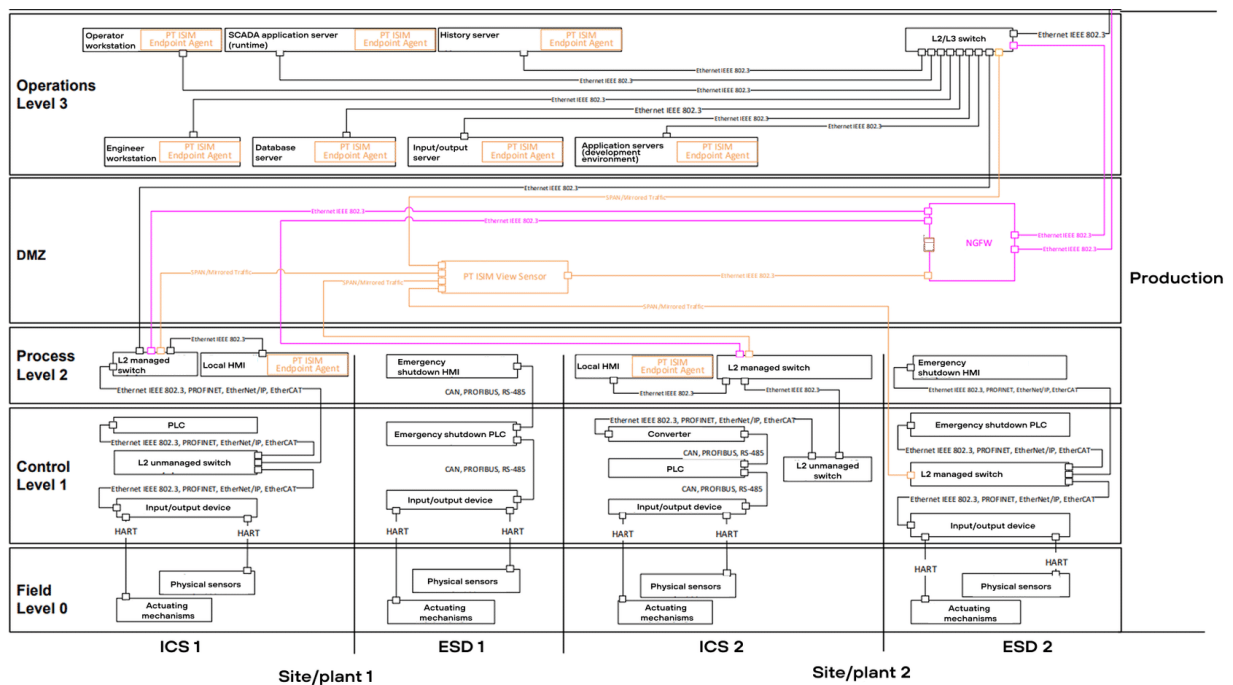
Despite the variety of traffic capture options, TAPs are the best choice. They allow interception of electromagnetic signals and binary data that are transmitted through cables and used by network cards to create frames. With this capture method, frames

are not lost, and their order remains intact. Together with network packet brokers, TAPs help an organization build a monitoring network that operates separately from the data transmission network, does not affect it in any way, and is completely hidden from users and administrators. A well-developed separate monitoring network allows quickly connecting any existing segments to network traffic analysis systems without the need for physical reconfiguration: you simply specify the interfaces to capture traffic from in the network packet broker. There is no need to look for free interfaces in switches, understand their configuration, or solve arising issues. However, there is a downside to these devices: they are quite expensive.

What can be done? Earlier, we mentioned other traffic mirroring technologies. For example, Remote SPAN (RSPAN), which allows traffic monitoring on physically remote ports through a network of switches. In an RSPAN configuration, traffic comes from source ports (SRC), which are part of a special RSPAN VLAN, specified for each RSPAN session individually. Additionally, there is the ERSPAN protocol that allows for traffic mirroring by encapsulating it inside IP packets using **GRE (Generic Routing Encapsulation)**. This means that a copy of the packet is transmitted as "regular IP traffic" with an ERSPAN header. These technologies also have drawbacks. The main one is that not all ICS products support them.

These collection methods are the best option. But if you cannot use them, you can mirror traffic from aggregation switches, provided there are no horizontal connections between network segments.

The optimal location of the sensor for capturing a traffic copy



The diagram above shows how to collect a traffic copy from aggregation switches without losing information from upstream segments.

Compliance with legal requirements

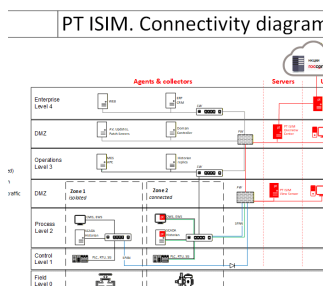
One of the principles for selecting a solution to ensure the cybersecurity of industrial control systems is the significance category of the critical information infrastructure object, assigned to the industrial control system or emergency shutdown system based on the significance criteria indicators in accordance with the provisions of Federal Law № 187-FZ 'On the Security of Critical Information Infrastructure of the Russian Federation.'

When adapting a PT ISIM-based solution for automated control systems (ACS) classified as critical information infrastructure (CII) objects, it is necessary to consider the significance category and the list of required protective measures to be implemented in accordance with the requirements of FSTEC of Russia Order № 239 dated December 25, 2017.

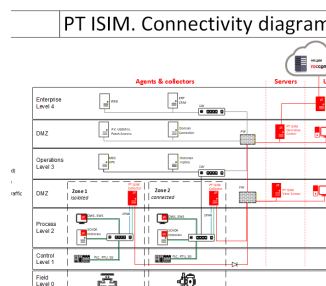
Features of solutions for such objects

- Protective measures must ensure the technical implementation of security measures in accordance with the assigned significance category of the CII object.
- Protective measures must be included in the unified registry of domestic software and databases.
- Protection measures must be certified by FSTEC.
- The cybersecurity system of a critical information infrastructure (CII) object must have the technical capability to interact with the State System for Detection, Prevention, and Elimination of Computer Attacks (GosSOPKA) of the National Coordination Center for Computer Incidents (NCCCI).

Standard solutions



Solution option based on PT ISIM and MaxPatrol SIEM with MaxPatrol 360 for organizing the interaction of the local production site's automated control system



Solution based on PT ISIM and MaxPatrol SIEM with Max Patrol 360 for organizing the interaction of the distributed production infrastructure's

with the State SOPKA.
Click on the image to view
it in more detail.

automated control system
with GosSOPKA.
Click on the image to view
it in detail.

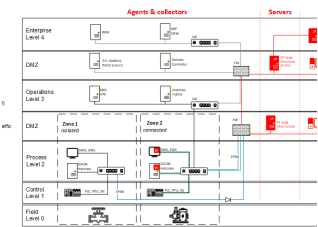
Integration with existing cybersecurity subsystems

When deploying new security tools, they usually need to be connected to centralized security incident monitoring and management systems of the enterprise, such as SIEM or IRP.

PT ISIM-based solutions can be integrated into these systems.

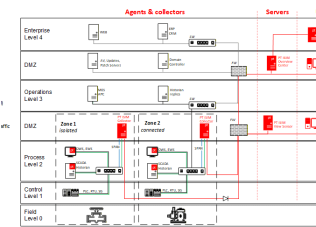
Standard solutions

PT ISIM. Connectivity diagram



PT ISIM-based solution
for interaction with third-
party SIEM or IRP systems
on a local production site.
Click the figure to enlarge
it.

PT ISIM. Connectivity diagram



PT ISIM-based solution
for interaction with third-
party SIEM or IRP systems
in a distributed
production infrastructure.
Click the figure to enlarge
it.

Deploying the product

Installing Debian for PT ISIM

05:29



Timestamps:

0:00—Starting Debian installation

1:14—Configuring system users

4:02—Installing system components

Deploying PT ISIM

You can find hardware requirements for the installation and operation of PT ISIM components [here](#).

"Verifying install success" checklist

#	Check	Result
1	PT ISIM View Sensor was installed without errors	☐
2	PT MC was installed without errors	☐
3	ISIM Endpoint Server was installed without errors	☐
4	Login to the PT ISIM View Sensor web interface is successful	☐
5	Login to the PT MC web interface is successful	☐
6	Login to the ISIM Endpoint Server web interface is successful	☐
7	A PT ISIM View Sensor license is activated	☐
8	A PT MC license is activated	☐
9	An ISIM Endpoint Server license is activated	☐
10	All PT ISIM services are running correctly	☐
11	All connected sites (View Sensor, ISIM Endpoint) are shown in the PT MC web interface	☐
12	All connected ISIM Endpoint agents are authorized in the ISIM Endpoint Server web interface	☐
13	Traffic is received on the analyzing interface	☐
14	Events are created based on analyzed traffic	☐
15	Events are created from endpoints	☐
16	Groups of network nodes are created	☐
17	Connections are created between network nodes	☐
18	Process signals are created	☐
19	Incidents are created based on analyzed traffic	☐
20	ISIM Endpoint incidents are created	☐

[Download the checklist](#)

Deploying View Sensor, Endpoint, and MC on a single server

09:06



Timestamps:

- 0:00—Preparing the system for installation
- 1:03—Installing the Management Console
- 2:22—Configuring the SqlStorage role
- 3:29—Installing LogConnector and Observability
- 5:10—Configuring Management and Configuration
- 6:22—Installing ISIM View Sensor
- 7:22—Installing ISIM Endpoint
- 8:28—Configuring services and testing connection

Deploying Overview

06:14



Timestamps:

0:00—Installing PT ISIM Overview Center

1:12—Configuring the system

Connecting to Overview

02:15



Timestamps:

0:00—Authorizing in the web interface

1:11—Connecting ISIM nodes

Connecting a subordinate Overview

02:04



Timestamps:

0:00—Authorizing in the web interface

1:15—Activating a registration package

Deploying an EDR agent and connecting it to the server.

Windows agent

01:20



Timestamps:

0:00—Installing ISIM Endpoint

"Getting ready to deploy" checklist

#	Check	Result
1	SPAN ports are configured and connected	☐
2	System learning is completed	☐
3	The list of detected nodes is verified	☐
4	Network node names agree with ICS documentation	☐
5	Network node interfaces are merged and/or split	☐
6	OT network nodes are grouped based on installation or device type	☐
7	Lists of network connection permissions are created	☐
8	Additional user profiles are created	☐
9	System data is filled out	☐
10	A connection to PT MC is set up	☐
11	Collection of cybersecurity events is set up on OT network endpoints	☐
12	Scanning in audit mode is set up on an endpoint	☐
13	File analysis is set up in PT Sandbox (if PT sandbox is installed)	☐
14	PT ISTI expert database update is tested	☐

What you have learned in this course



PT ISIM is a comprehensive cybersecurity system for OT infrastructures with a wide range of tools and extensive industrial expertise to analyze traffic, collect events, and safeguard OT networks, industrial enterprises, and engineering infrastructure facilities.



PT ISIM is an XDR (extended detection and response) product. It is one of the key components of security operations centers (SOCs) which respond to cybersecurity incidents in OT networks.



PT ISIM is a hardware and software suite with a choice of several hardware platforms (typically 1U and 2U rack servers) and special software. All PT ISIM components run on Debian: Debian 10.X or 12.X. PT ISIM components are divided into four functional groups.



PT ISIM can be supplied as a trusted hardware and software suite. PT ISIM View Sensor, ISIM Endpoint Server, and ISIM Endpoint Management can be deployed together on any product version. PT MC can be installed on its own or together with PT ISIM Overview Center.



PT ISIM detects cybersecurity violations using PT Industrial Security Threat Indicators (PT ISTI), a proprietary database of industrial cyberthreats.



When choosing where to install PT ISIM View Sensor in the customer's infrastructure, take into account all its features, such as whether it is possible to install a software and hardware suite,

or whether a virtual appliance image must be installed on the customer's hypervisor. PT ISIM can work with virtualization environments that support AVX.

Useful links

Positive Technologies

Official website

VISIT

Positive Education

All educational programs

LEARN MORE

Help Portal

Product documentation

GO

