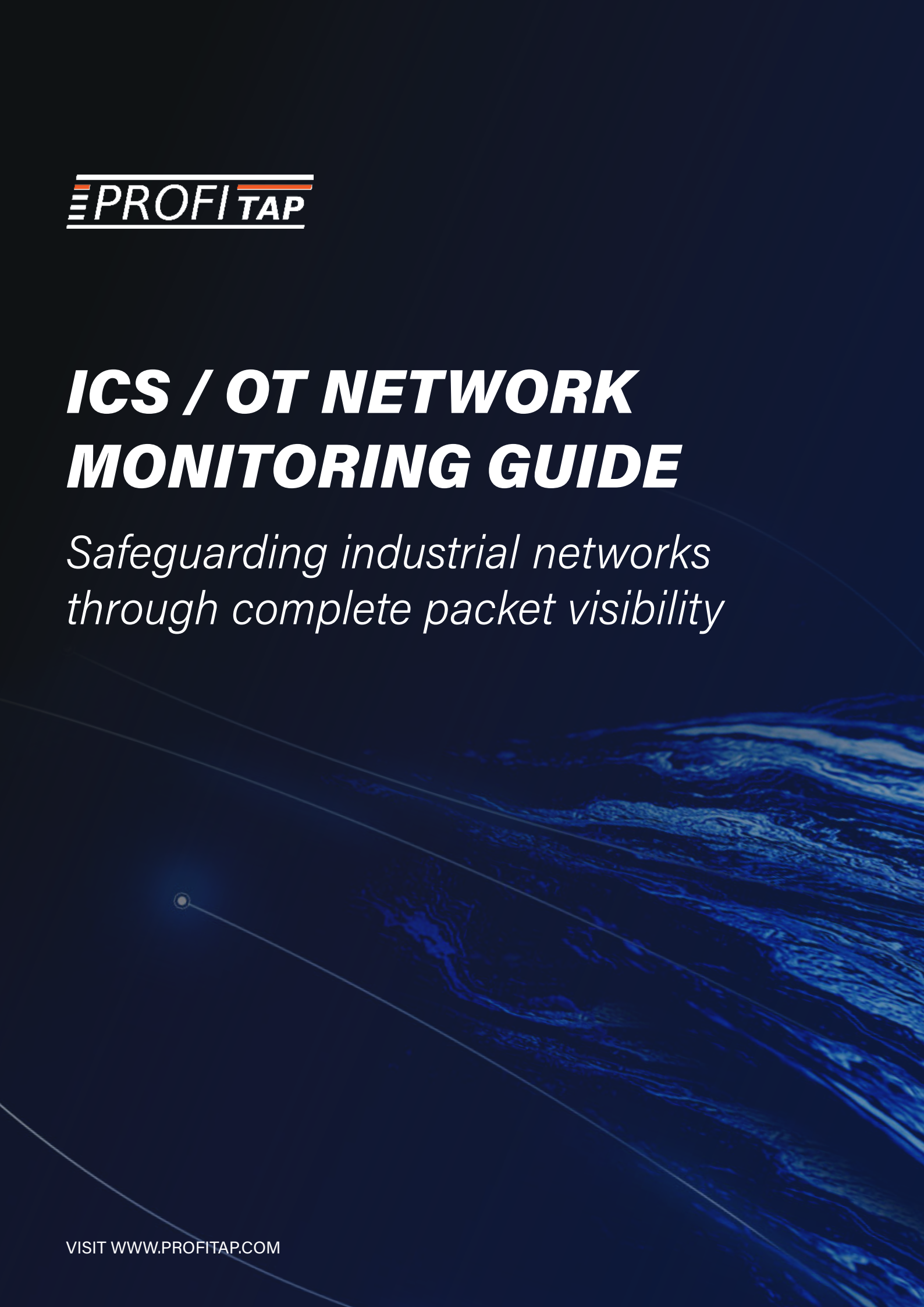
PROFITAP

ICS / OT NETWORK MONITORING GUIDE

Safeguarding industrial networks through complete packet visibility



VISIT WWW.PROFITAP.COM

Industrial Control Systems (ICS) and Operational Technology (OT) networks are critical for managing essential infrastructure and industrial operations, from power grids to manufacturing plants. However, these systems' increasing digitization and connectivity have made them more vulnerable to cyber threats and operational failures. To safeguard these environments, ICS/OT network visibility and monitoring are essential in providing real-time insight into network traffic, detecting anomalies, and identifying potential security risks.

OT monitoring solutions should deliver actionable, packet-based network insights without compromising network security or continuous machine operation. Let's explore how.

Importance of critical infrastructure

Our civilization's economy, security, and public well-being rely heavily on network infrastructure that keeps everything connected and operational. These networks are critical for the performance and security of these sectors, rightfully earning them the distinction "Critical Networks".

Any disruption to these networks can lead to widespread consequences, affecting public health, economic stability, and national security. Protecting and maintaining this infrastructure is crucial to avoid disruptions that could severely impact societal functioning.

Sectors with critical infrastructure include:

Energy:	This covers electricity production, gas distribution, and fuel supply.
Water and Wastewater Systems:	This includes water treatment facilities and wastewater disposal systems.
Transportation:	Roads, bridges, airports, rail systems, and seaports.
Communication:	Internet infrastructure, mobile networks, and broadcasting.
Healthcare:	Hospitals, emergency services, and healthcare providers.
Information Technology:	Data centers, networks, and cybersecurity.
Financial Services:	Banks, financial institutions, and payment systems.
Critical Manufacturing:	Facilities essential for the production of materials and goods.
Food and Agriculture:	Food production, distribution, and safety systems.
Government Facilities:	Buildings and services essential to government operations.
Defense and National Security:	Military installations and related services.

ICS / OT cybersecurity threats

As utility and critical infrastructures undergo digital transformation to enhance operational efficiency, they face a significant rise in cyber risks. This surge can lead to unexpected downtime, corporate reputation damage, and data security and safety concerns.

In the past, before power grids integrated Ethernet and TCP/IP-based IT communications for external connections, cybersecurity primarily revolved around communication protocols and network isolation. Today, industrial control systems (ICS) are subject to the same cyber threats as traditional IT networks, with potentially disastrous outcomes.

The need for network visibility

Visibility is key to enabling faster troubleshooting in the case of network issues or security incidents. Organizations need real-time access and insights without delay, so they incorporate low-latency monitoring, ensuring swift identification of potential threats or performance bottlenecks.

Additionally, a fault-tolerant system ensures that monitoring and analysis remain uninterrupted even in the event of unexpected failures, minimizing downtime and maintaining the reliability of critical services. This combination of low latency and failsafe mechanisms enhances security and improves efficiency in proactively handling network disruptions.

Visibility challenges

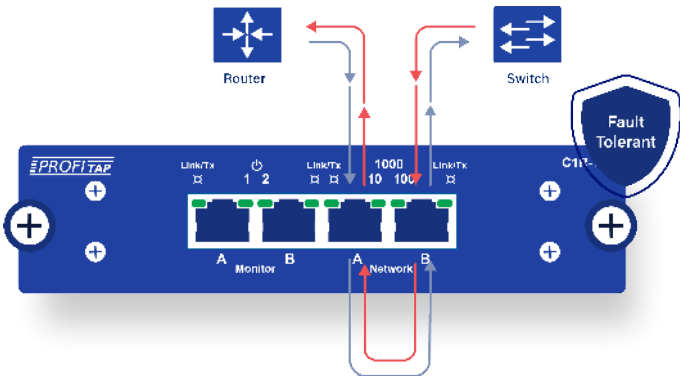
Differences in IT and OT networks

While adding new hardware to IT networks is relatively easy, this is different for OT networks because they are started simultaneously. Once the configuration or boot-up phase is complete, deploying monitoring systems is impossible without taking offline parts. Therefore, it is important to consider network monitoring in OT systems from the early stages of building network infrastructure.

The importance of data diodes

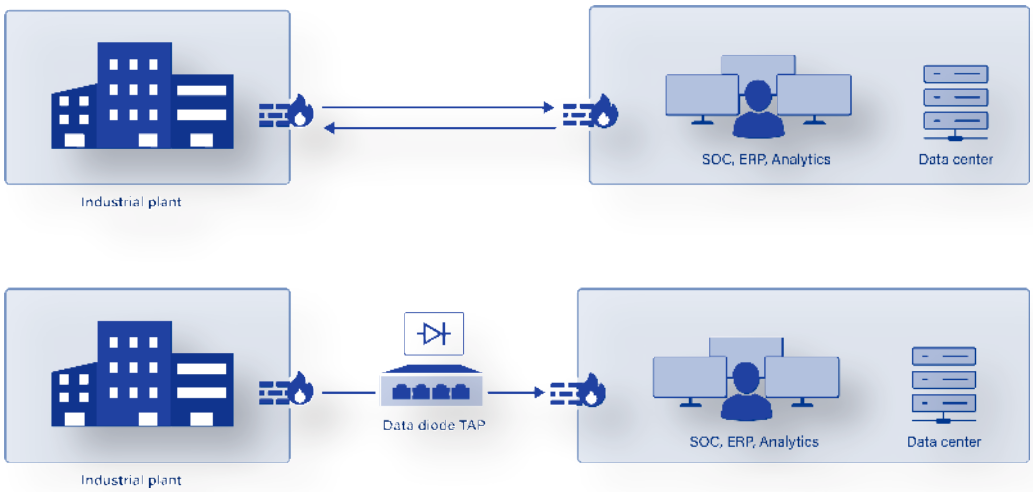
Fault-tolerant

To ensure uninterrupted network operations, the monitoring system must be deployed out-of-band, completely isolated from the operational network. This prevents interference with network traffic and maintains system integrity.



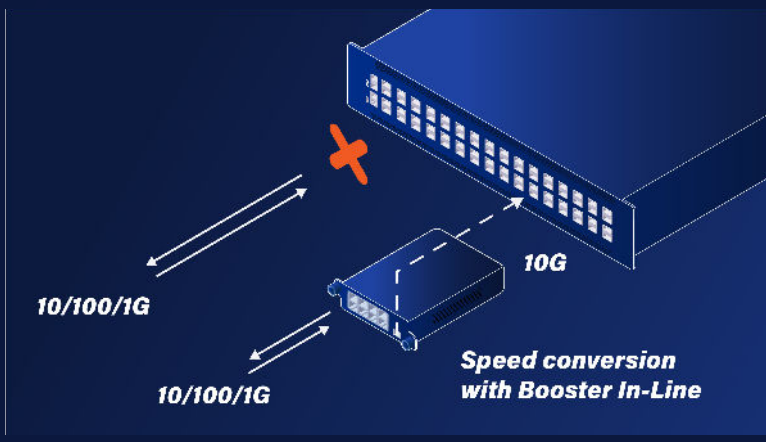
Unidirectional traffic (Data Diode)

Integrated into Profitap Diode Fiber and Copper TAPs, Data Diode technology ensures unidirectional traffic, blocking any accidental or malicious signals from re-entering the operational network through monitoring ports. This added security measure protects critical OT systems while allowing network aggregators and packet brokers to collect data and forward it to security and monitoring tools for analysis.



Media and speed conversion

Network Packet Brokers (NPBs) are useful for aggregating and filtering traffic. They typically operate at high throughput, commonly supporting 40/100 Gbps ports, and are designed to handle large volumes of network traffic. It is possible to split these high-speed connections into 10 Gbps links using breakout cables, but handling lower speeds like 10/100 Mbps is often problematic since lower-speed links cannot directly interface with the high-speed ports.



Devices like the Profitap Booster can convert 10 Mbps traffic into a 10 Gbps output. This solution allows older or slower network links to be integrated into modern toolsets, providing an efficient and cost-effective way to maintain compatibility without significant infrastructure changes.

Challenges of packet capture in OT networks

From an operations perspective, implementing network monitoring solutions in these environments can be challenging due to a number of factors, such as outdated software, specialized control systems, strict hardware approval processes, and strict communication timing requirements. These are mostly due to the downtime when deploying new hardware.

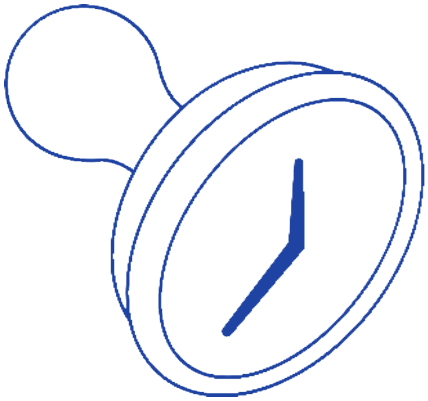
Startup/design challenge

From a machine builder perspective, the focus lies on providing pre-integrated monitoring solutions for their clients and enhancing predictive maintenance capabilities. By embedding network analysis tools during the design phase, machine builders offer seamless monitoring capabilities that do not interfere with the operational performance.

Additionally, these tools enable them to analyze communication patterns for proactive maintenance and detect potential performance issues. Tailoring network analysis solutions for machine builders involves offering hardware that easily integrates, remote diagnostics, and interfaces compatible with existing control systems.

Protocol challenge

All industrial Ethernet protocols aim to ensure packets are transmitted and received at the right time. It is easy to understand what information is transmitted, but measuring precise time intervals is much more complicated. Doing this analysis with standard PC / hardware often leads to inaccuracies because nearly all Ethernet hardware is implemented to accommodate throughput and guarantee the reception of packets instead of understanding the time at which they are received. When analyzing the network with a Windows-based PC, for instance. In that case, packets can often jitter purely through capture in a multitude of milliseconds, which renders any approach of analysis impossible.



Tailored solutions, including our non-intrusive TAPs and network packet brokers, are crucial in maintaining timing-sensitive communications while ensuring secure analysis without interrupting real-time processes. This way, the packets are timestamped as precisely and exactly as possible. Also, information about the packets (where they come from, when they are received, etc.) and additional information in the MAC layer of the packets often can only be read if the packet has been captured directly on the network.

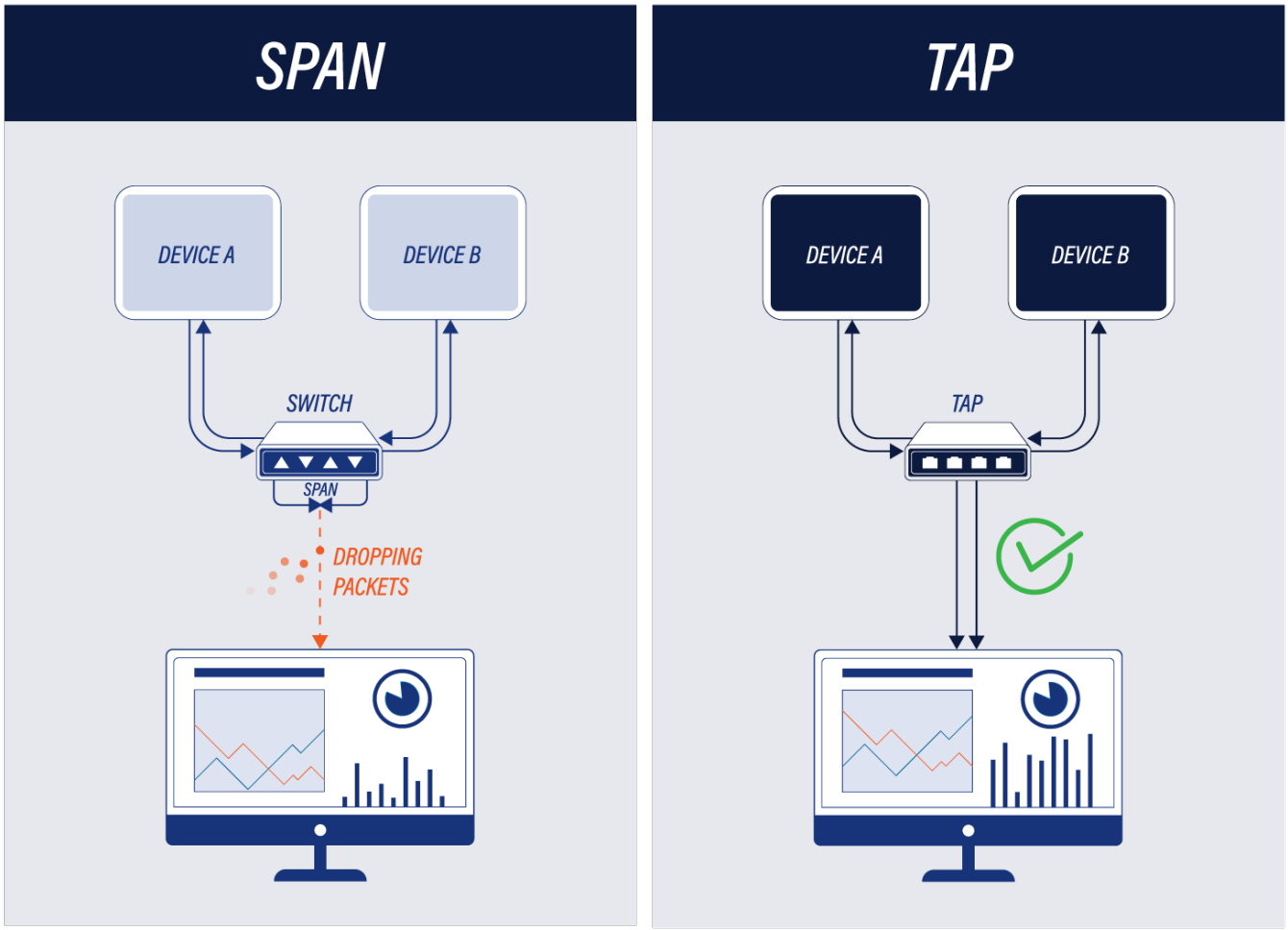
Another issue is the Ethernet preamble and suffix. Some OT protocols use those parts of the frame to transmit additional information and synchronization. Modern NICs remove these from the packets during capture, as an operating system usually does not require them.

How to monitor

TAP vs SPAN

While SPAN ports offer a simple, cost-effective method for monitoring OT networks, their limited, "interpreted view" of traffic can hinder critical insights. In high-stakes environments, where accurate and continuous monitoring is necessary to ensure operational safety and reliability, network TAPs provide a more robust solution. TAPs, on the other hand, require the network line to be broken to place the TAP in line. This may hinder ongoing network operations.

Network TAPs offer an unrestricted, real-time view of all OT traffic, capturing every packet and delivering the most accurate representation of network behavior. When paired with advanced monitoring systems, they support full-duplex traffic capture at line rate, overcoming the data aggregation and performance limitations often seen with SPAN ports.



The decision between SPAN ports and TAPs should be based on specific monitoring requirements, budget, and the importance of the monitored segment. For general OT monitoring, SPAN ports may suffice. However, for mission-critical systems, security monitoring, or performance analysis where every data packet matters, network TAPs are the superior choice to ensure complete visibility of OT operations.

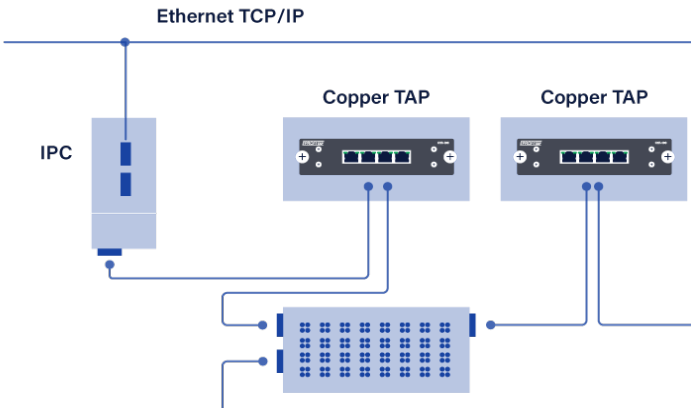
Where to capture

The effectiveness of using copper TAPs and IOTA devices depends significantly on their placement within the network.

Here are the ideal positions for placement and the monitoring benefits they provide:

1. Directly after the PLC	2. After the last configured device	3. Before and after a branch separates	4. Before and after a specific device
This placement allows for complete control over all packets sent and received. During development, an IOTA can be placed instead of a copper TAP to ensure everything sent over the network is being seen. This is the primary analysis point for configuration issues, devices configured, and general timing issues.	This placement is different from the physical placement of that device as it may differ. Positioning a TAP after the last device that will be contacted in the cycle allows for monitoring cycle times, data integration, and network consistency. Combined with the TAP behind the PLC, this point ensures visibility into cycle time correctness, propagation delays, packet completeness, and all packets transmitted.	This placement ensures that critical branches can be monitored and their timing can be tracked. It is essential to ensure that critical paths receive all correct information and required data.	A TAP should be placed before and after specific devices that need to be monitored. Only by monitoring the device can it be tracked.
◉ Control over all packets sent and received ◉ Analysis of configuration issues ◉ Monitoring of device configurations ◉ General timing issues	◉ Monitoring cycle times ◉ Integration of data ◉ Network consistency ◉ Cycle time correctness ◉ Propagation delays ◉ Packet completeness	◉ Monitoring critical branches ◉ Timing monitoring ◉ Ensuring critical paths receive correct information	◉ Monitoring specific devices ◉ Tracking direct interference by the device

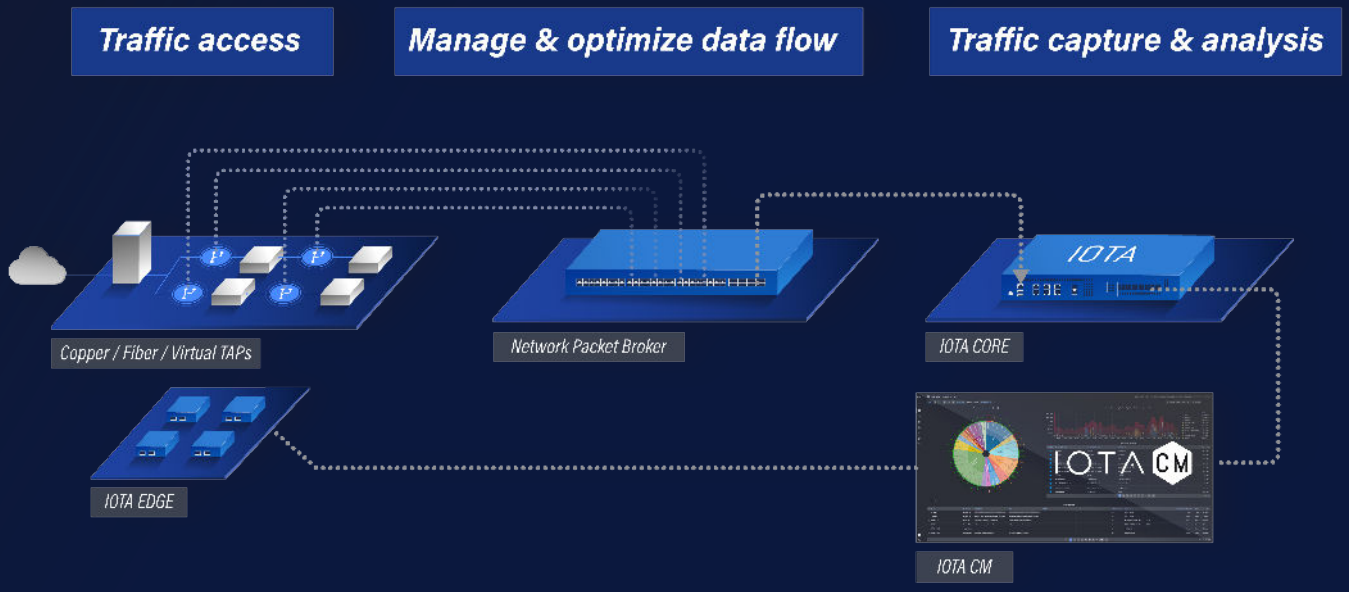
By strategically placing copper TAPs at key capture points in the network, engineers can achieve detailed insights into network performance and quickly identify and resolve issues. The combination of Profitap copper TAPs and IOTA's powerful capture and analysis capabilities provides a comprehensive monitoring solution essential for maintaining and optimizing industrial Ethernet networks.



Visibility solutions

Profitap provides comprehensive monitoring solutions for OT networks through an all-encompassing observability platform. This platform covers all critical aspects, including traffic access using TAPs, enhanced filtering, and traffic optimization through Network Packet Brokers.

The IOTA solution ensures accurate traffic capture and analysis, enabling real-time insights into network performance and cybersecurity. This holistic approach offers tailored solutions that strengthen OT networks' visibility, security, and operational efficiency in various industries.



Industrial TAPs

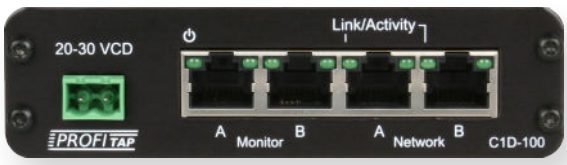
Profitap C1D-1G and C1D-100 Ethernet TAPs meet the demands of industrial network monitoring with exceptional performance and reliability. These TAPs support low latency and low jitter, ensuring seamless data transmission without compromising network efficiency. Both models feature DIN rail mounting and 24V DC powering, allowing easy integration into industrial environments.

Designed for fault tolerance, these TAPs guarantee uninterrupted network operation, even during monitoring port connections or disconnections. Built-in data diode functionality prevents any data injection from monitoring ports back into the network, providing an added layer of security. They capture a precise copy of all protocols and packet types, including low-level errors and impairment issues, offering comprehensive network visibility and diagnostics.

They monitor all seven OSI layers, mirroring all sizes and types of packets, including low-level errors and VLAN traffic. The integrated Data Diode feature enhances security by preventing data injection from the monitoring ports.

100 DIN Copper TAP

10/100M



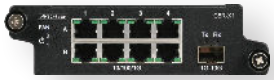
1G DIN Copper TAP

10/100/1000M

Booster Aggregation TAPs

Traffic aggregation is required to optimize the traffic flow between the capture points and the monitoring or security tools. This is where the Profitap Booster Aggregation TAP comes in. With a small form factor and the ability to achieve lossless traffic aggregation, the Booster brings multiple capture points together for monitoring purposes.

The Booster Aggregation TAPs come in different models:

Booster In-Line	Booster SPAN	Booster Dual Output
		
⦿ Aggregation of 8 x RJ45 10/100/1G ports (4 in-line links) into 1 x SFP+ 1G/10G output. ⦿ Direct link aggregation, no required management, installation, or driver. ⦿ Supports link failure propagation. ⦿ PoE passthrough ⦿ The fail-safe in-line design ensures uninterrupted network operation in case of power loss. ⦿ Network ports are galvanically separated from the monitor port for maximum security.	⦿ Aggregation of 8 x SFP 10/100/1G SPAN (out-of-band) ports into 1 x SFP+ 1G/10G output. ⦿ 100FX support. ⦿ Direct link aggregation, no required management, installation, or driver.	⦿ Dual output variants are available for both the in-line and SPAN models. ⦿ Allows two separate tools to receive the same replicated copy of all traffic aggregated by the TAP, such as an OT security system sensor and a network analysis tool. ⦿ 2 x SFP+ 1G/10G outputs. ⦿ Same features as the single output variants.
⦿ Data Diode function. ⦿ Ingress VLAN tagging (802.1Q, 802.1ad). ⦿ Low power consumption. ⦿ Non-intrusive to the network. ⦿ Redundant powering.		

Benefits of the Booster Aggregation TAPs

Booster Aggregation TAPs are essential for cost-effectively aggregating network traffic from multiple sources and preparing it for analysis by NDR (network detection and response) systems. These devices ensure that data is captured reliably from various locations and forwarded to monitoring tools without any loss, which is crucial for accurate threat detection and network analysis.

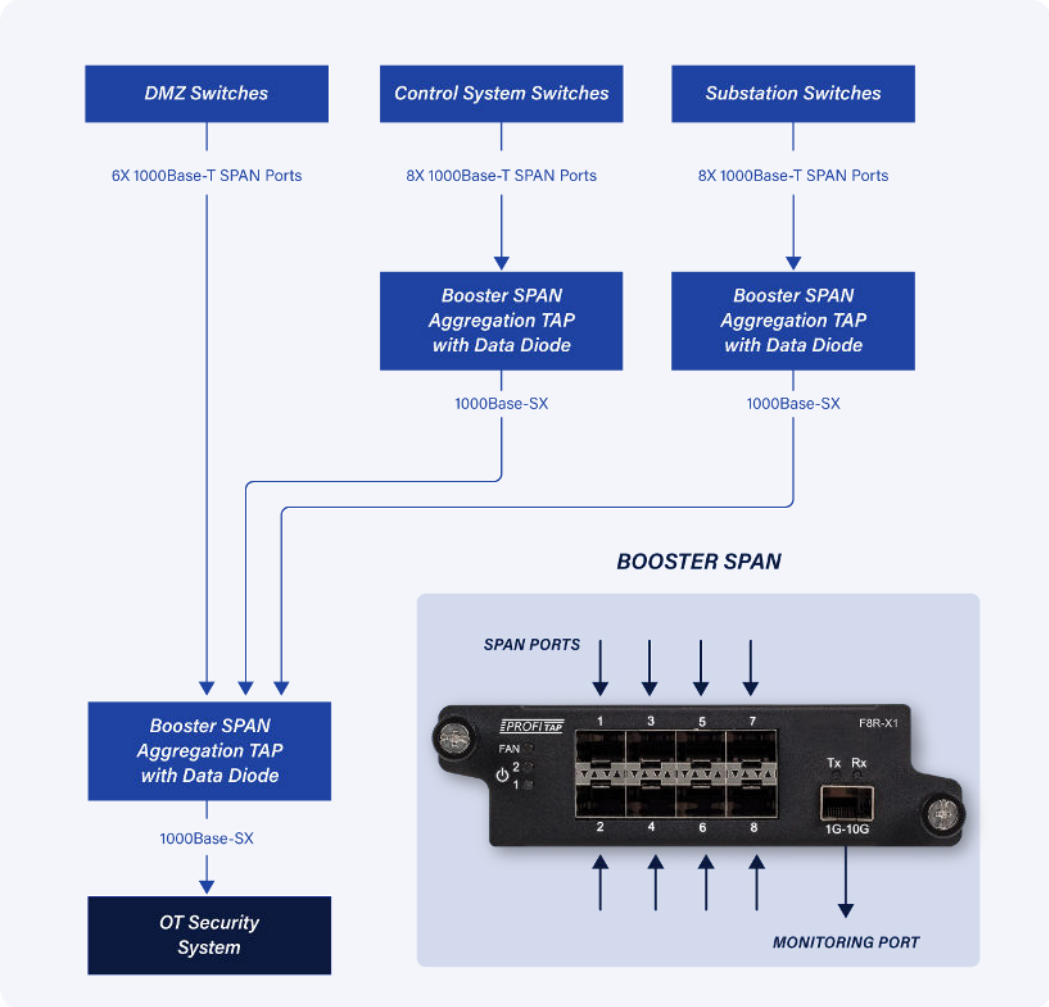
Profitap Booster Aggregation TAPs are a great asset in OT security. These TAPs aggregate traffic from multiple sources, ensuring comprehensive network visibility without impacting the network. Their Data Diode function prevents reverse data flow, enhancing security. Coupling these TAPs with NDR systems allows for continuous monitoring and threat detection.

Deployment scenarios

Booster SPAN Aggregation TAP deployment

Profitap Booster Aggregation TAPs offer great flexibility and several deployment options suited to different environments and industries.

In this deployment scenario, multiple physical locations need to be monitored. With multiple switches set up to forward traffic to the NDR tool via SPAN, the total number of incoming SPAN connections is 22. In this analysis scenario, the aggregation can be performed with just three SPAN Booster Aggregation TAPs by setting the output port to 1Gbps and daisy chaining them. This is made possible by the low data rate (sub 10Mbps) on these lines.



Aggregation to a network packet broker

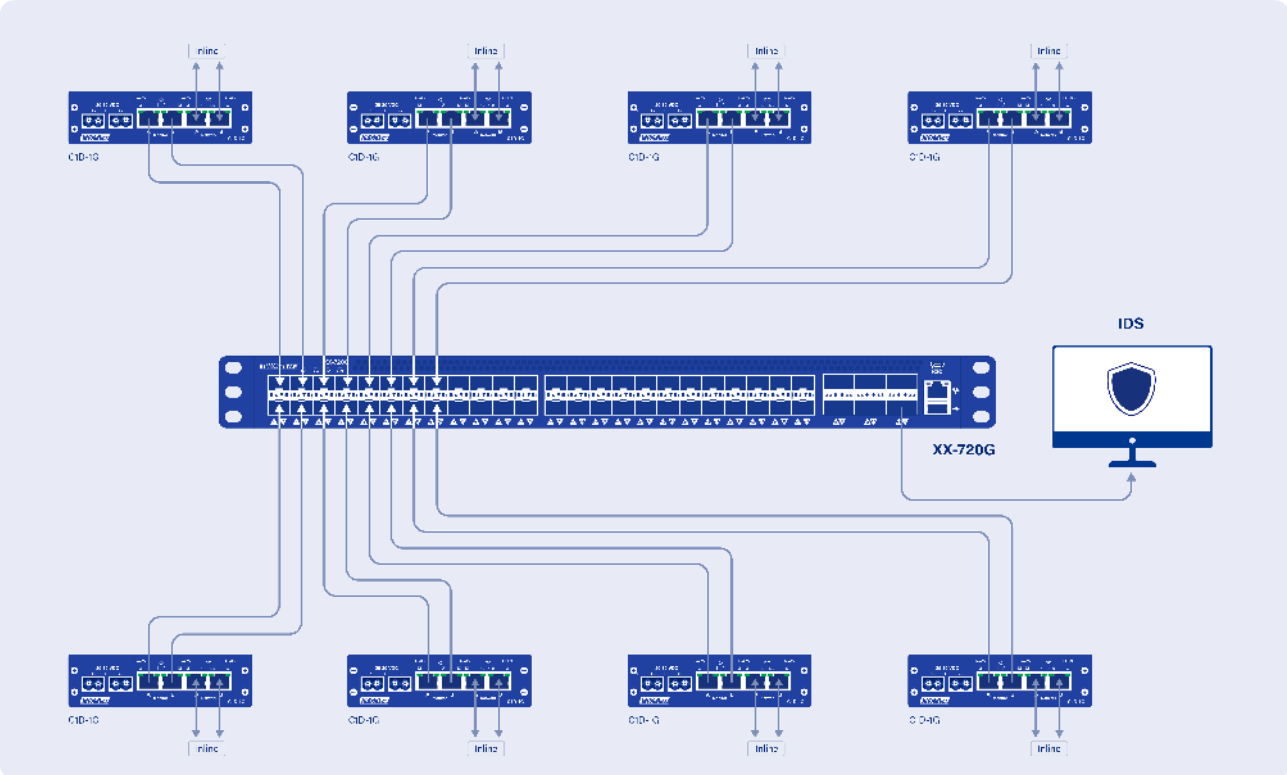
Aggregating traffic to a packet broker is essential for comprehensive monitoring and analysis without disrupting time-sensitive operations. TAPs can aggregate multiple data streams and forward them to a packet broker.

The network packet broker is a powerful tool for optimizing and managing traffic in high-bandwidth environments. Their key features include traffic aggregation, which consolidates data from multiple sources, and replication, which duplicates traffic for various analysis tools. Load balancing ensures an even distribution of network traffic across multiple monitoring tools.

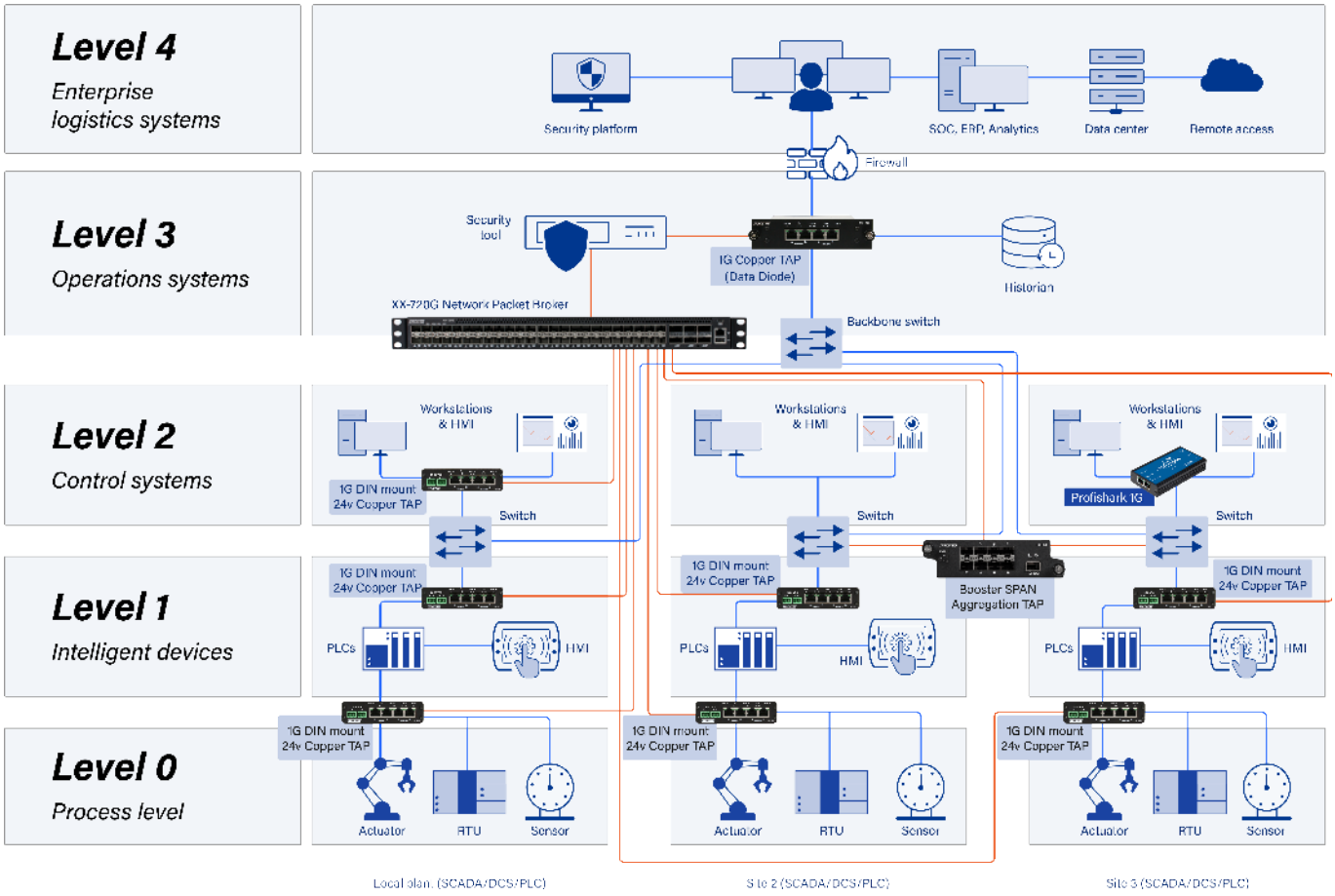
This setup monitors eight critical network connections using **C1D-1G Industrial TAPs** deployed inline. These TAPs duplicate the 1G traffic from each connection without introducing any disruption to the live network. The duplicated traffic from all eight TAPs is then forwarded to the **XX-720G Network Traffic Aggregator**.

The **XX-720G Aggregator** filters and aggregates the incoming traffic. Filtering ensures that only relevant data packets are selected based on predetermined criteria, and through aggregation, it combines the data streams from multiple TAPs into a single 40G output. This streamlined and processed traffic is then sent to an **Intrusion Detection System (IDS)** for real-time monitoring and analysis. The IDS detects and alerts potential threats or anomalies in the network.

This architecture enables efficient and centralized network visibility, ensuring enhanced security and performance for the industrial environment.

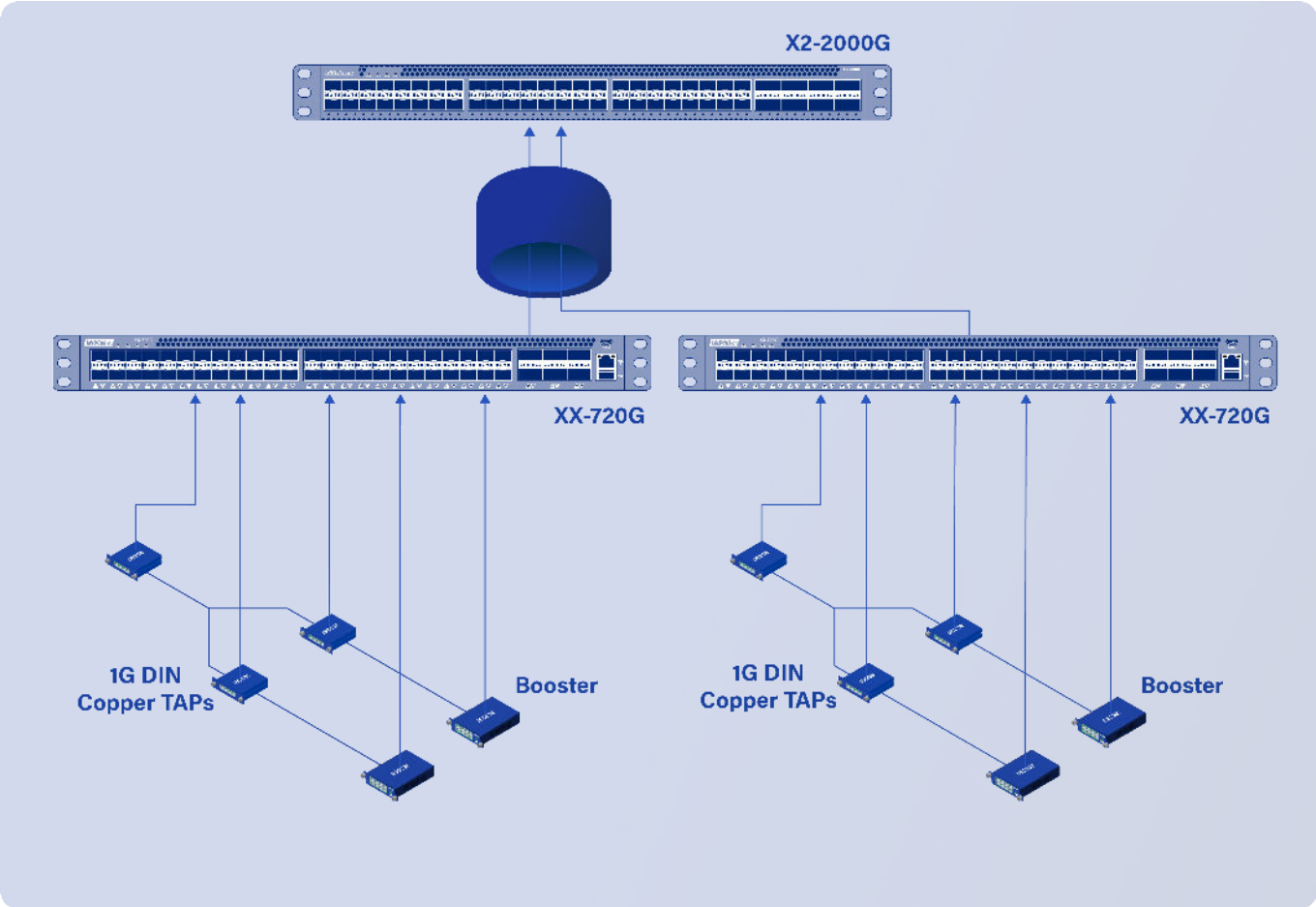


TAPs and advanced NPBs in an OT network



In larger networks, where high volumes of data flow from various sources, it becomes efficient to use traffic aggregators to consolidate the network traffic before sending it to a single network packet broker that does advanced traffic handling.

If networks are physically separated, GRE (Generic Routing Encapsulation) tunneling can be implemented to establish a direct point-to-point connection between them. This architecture allows for a scalable and streamlined approach to managing and analyzing traffic and optimizing network visibility and performance without overwhelming available resources.



Conclusion

ICS/OT network monitoring is about visibility and ensuring operational resilience and security. Profitap solutions exemplify how monitoring technologies can address the challenges of these critical environments, safeguarding infrastructure and enabling proactive threat management.

Profitap OT/ICS monitoring solutions help meet the following criteria:

Network visibility	Comprehensive visibility into network traffic is essential for identifying and addressing potential issues.
Real-time data processing	The ability to process data in real-time ensures timely detection and response to threats and performance issues.
No interruptions	Monitoring solutions should operate without causing interruptions to the network, ensuring continuous operations.
Fail-safe and secure	Solutions must be fail-safe, preventing the introduction of a point of failure in the network.
Diode/unidirectional communications	Implementing diode or unidirectional communications can prevent unauthorized access and data breaches.
No impact on security and performance	Monitoring solutions should not compromise the security and performance of the network.

PROFITAP

40	1100+	100K+	70+	0
Years of experience	Business partners	Products installed	Countries	Packets dropped

FIND OUT MORE ON WWW.PROFITAP.COM

Profitap HQ B.V.
High Tech Campus 84
5656 AG Eindhoven
The Netherlands

sales@profitap.com
www.profitap.com

Profitap
@Profitap
Profitap-international