Logicom Solutions

Cisco Partner
Gold Integrator

An Edge Architecture Approach to Securing Industrial IoT Networks

With operational environments increasingly digitalizing and connecting to the IT environment, industrial organizations are recognizing the need to protect operational technology (OT) and industrial IoT against cyberattacks. Deploying firewalls to build a demilitarized zone (DMZ) between industrial networks and the IT domain is the mandatory first step. But as organizations connect more devices, enable more remote access, and build new applications, the airgap erodes and falls short of being sufficient.

Security solutions designed for industrial networks typically monitor network traffic to gain visibility on assets, behaviors, malicious activities, and threats. The process of evaluating and testing these solutions initially tends to go well – after a successful proof of concept, industrial organizations begin to deploy at scale. That's where they begin to run into issues.

Often, it's cost-prohibitive for organizations to buy the number of security appliances they need to cover their entire operational environment. Or, the networking team doesn't have the resources to deploy, maintain, and manage a fleet of security appliances. The additional traffic created by these appliances would likely necessitate a separate network – which would also require the resources to deploy, maintain, and manage it.

Fortunately, there is a better approach to securing the OT environment. This paper introduces three architectural approaches available today, as well as an alternative that provides the visibility and security OT and IT teams need at scale, without requiring additional resources.

Challenges in securing an IIoT network

A lack of visibility:

As industrial networks can be quite old, widely dispersed, and involve many contractors, operators often don't have an accurate inventory of what's on the network. Without this, they have limited ability to build a secure communications architecture.

A lack of control:

A lack of visibility also means operators are often unaware of which devices are communicating to each other or even of communications reaching industrial devices from the outside. You cannot control what you don't know.

Understanding the operational technology environment

To thoroughly understand the scalability problem as it relates to securing the operational environment, we need to start with the OT environment itself. Industrial control networks connect many automation devices (PLC, RTU, IED, DCS, etc.) that are controlled by software in order to run a process. These OT devices have been deployed over a period of many years – sometimes even decades – back when cybersecurity wasn't a concern. As a result, they lack any strict security policies. To further complicate matters, some devices can be deployed, managed, and decommissioned by third-party contractors.

When organizations attempt to secure their industrial IoT network, they encounter two primary issues:

1. **A lack of visibility:** As industrial networks can be quite old, widely dispersed, and involve many contractors, operators often don't have an accurate inventory of what's on the network. Without this, they have limited ability to build a secure communications architecture.
2. **A lack of control:** A lack of visibility also means operators are often unaware of which devices are communicating to each other or even of communications reaching industrial devices from the outside. You cannot control what you don't know.

The first step, then, to securing an industrial IoT network is to obtain visibility. You need to understand what devices are on the network, what they are communicating, and where those communications are going.

Gaining visibility of the operational technology network

The technology to achieve network visibility is available today. Deep packet inspection (DPI) decodes all communication flows and extracts message contents and packet headers, providing the visibility to understand what devices you need to secure, and the policies required to secure them.

DPI allows you to gather device information such as the model, brand, part numbers, serial numbers, firmware and hardware versions, rack slot configurations, and more. It also allows you to understand what is being communicated over the network. For example, you can see if someone is attempting to upload new firmware into a device or trying to change the variables used to run the industrial process.

To achieve complete visibility, all network traffic must be inspected. It's important to note that in an industrial network, most traffic occurs behind a switch at the cell layer, because that's where the machine controllers are deployed. Very little traffic goes up to the central network.

What is deep packet inspection?

Deep packet inspection (DPI) is a type of data processing that decodes all communication flows to extract information from packet headers as well as the payload of the message. It requires perfect knowledge of the communication protocol to be able to decode it and understand the content of the communication. This can be quite difficult to achieve in industrial networks where many communication protocols are proprietary to control system vendors.

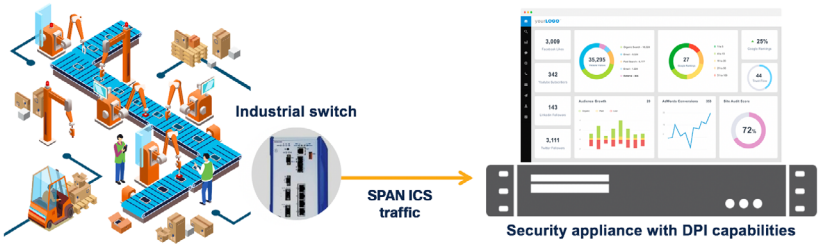
What is SPAN?

Switched port analyzer (SPAN) is a method of monitoring network traffic that forwards a copy of each packet going through a network switch to another port where the network traffic analyzer is connected.

When collecting network packets to perform DPI, security solution providers typically configure SPAN ports on network switches and employ one of three architectures:

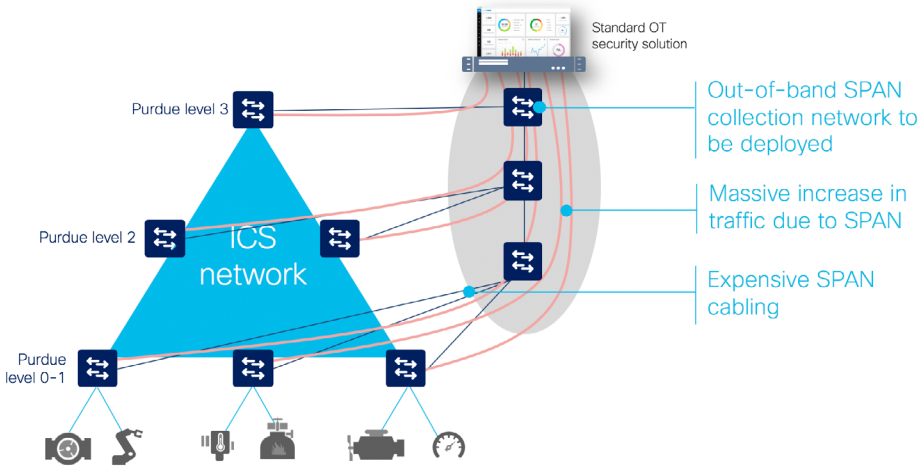
1. Send all traffic to a central server that performs DPI
2. Deploy dedicated sensor appliances on each network switch
3. Send traffic to dedicated sensor appliances deployed here and there on the network

Typical ICS detection solutions depend on SPAN



While these approaches deliver network visibility, they also create new challenges. Configuring network switches to send traffic to a central server requires duplicating network flows. A new out-of-band network will generally be needed to transport this extra traffic, which can be complex and costly. Although this can be acceptable for a very small industrial site, this cannot be seriously considered in highly automated industries generating a lot of ICS traffic (such as manufacturing), or when devices are widely spread in locations with no or poor network connectivity (oil and gas pipelines, water or power distribution, etc.).

SPAN based solutions incur huge additional hidden costs



3 common approaches to securing IIoT

1. Send all traffic to a central server that performs DPI
2. Deploy dedicated sensor appliances on each network switch
3. Send traffic to dedicated sensor appliances deployed here and there on the network

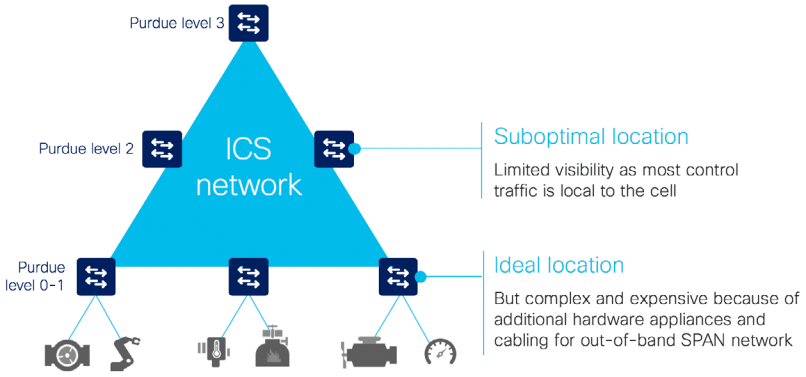
While these approaches deliver network visibility, they also create new challenges. Configuring network switches to send traffic to a central server requires duplicating network flows. A new out-of-band network will generally be needed to transport this extra traffic, which can be complex and costly.

Connecting sensor appliances to network switches addresses the issues associated with duplicating network traffic. However, installing, managing, and maintaining dedicated hardware can quickly lead to cost and scalability issues.

RSPAN reduces the number of appliances required to provide full visibility, but still increases the amount of traffic going through the industrial network, resulting in jitter.

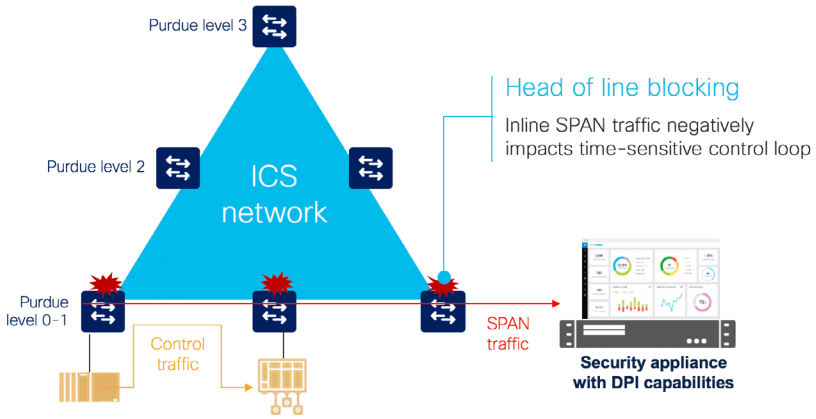
Connecting sensor appliances to network switches addresses the issues associated with duplicating network traffic. The appliance collects and analyzes network traffic locally and only sends data to a server for additional analysis. However, installing, managing, and maintaining dedicated hardware can quickly lead to cost and scalability issues. And because most industrial traffic is local, gaining full visibility requires deploying appliances on each and every switch on the network, raising cost and complexity to intolerable levels.

DPI location matters for effective ICS security



Some technology providers attempt to address this problem by leveraging remote SPAN (RSPAN). RSPAN allows you to duplicate traffic from a switch that doesn't have a sensor appliance to a switch that has one.

Remote SPAN introduces jitter



While this approach reduces the number of appliances required to provide full visibility, it still increases the amount of traffic going through the industrial network. Traffic is multiplied because you're duplicating traffic to SPAN it to a remote switch. And the more traffic on the network, the slower it becomes, resulting in jitter – often an unacceptable compromise in industrial networks where processes need to run faster and machines must be timely synchronized.

Benefits of a DPI-enabled switch

An industrial-grade switch with native DPI capability eliminates the need to duplicate network flows and deploy additional appliances. Obtaining visibility and security functionality is simply a matter of activating a feature within the network switch, router, or gateway.

Benefits include:

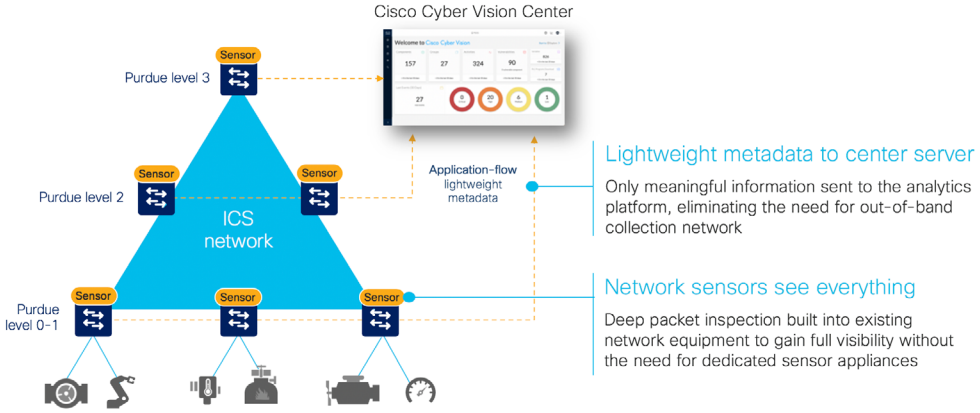
- Cost, traffic, and operational overhead are all minimized
- Traffic is analyzed locally and only lightweight metadata is sent to a central server, so no congestion is created or extra bandwidth is needed
- IT can leverage the existing network infrastructure to secure industrial operations without having to source, deploy, and manage additional hardware
- OT can obtain visibility into operations that it has never had before, with embedded sensors providing analytical insights into every component of the industrial control systems

Alternatives to SPAN

Instead of SPAN, organizations can use network TAP, port aggregators, or virtual switches, but these alternatives come with a few caveats of their own: 1) organizations must still source and deploy dedicated appliances, 2) configuration and management aren't necessarily easy, and 3) sending traffic to the OT security platform requires an out-of-band network to avoid impacting the production network.

There is a better way to achieve full network visibility: embed DPI capability into existing network hardware. An industrial-grade switch with native DPI capability eliminates the need to duplicate network flows and deploy additional appliances. Obtaining visibility and security functionality is simply a matter of activating a feature within the network switch, router, or gateway. Cost, traffic, and operational overhead are all minimized.

Visibility and detection built into your network infrastructure



A DPI-enabled switch analyzes traffic locally to extract meaningful information. It only sends lightweight metadata to a central server, which runs the analytics and anomaly detection. That metadata represents about 3-5% of general traffic. The traffic is so lightweight, it can be transferred over the industrial network without causing congestion or requiring extra bandwidth.

Embedding DPI in network equipment affords both IT and OT unique benefits. IT can leverage the existing network infrastructure to secure industrial operations without having to source, deploy, and manage additional hardware. Because these network elements see all industrial traffic, embedded sensors can provide analytical insights into every component of the industrial control systems. As a result, OT can obtain visibility into operations that it has never had before.

Monitoring traffic on legacy switches

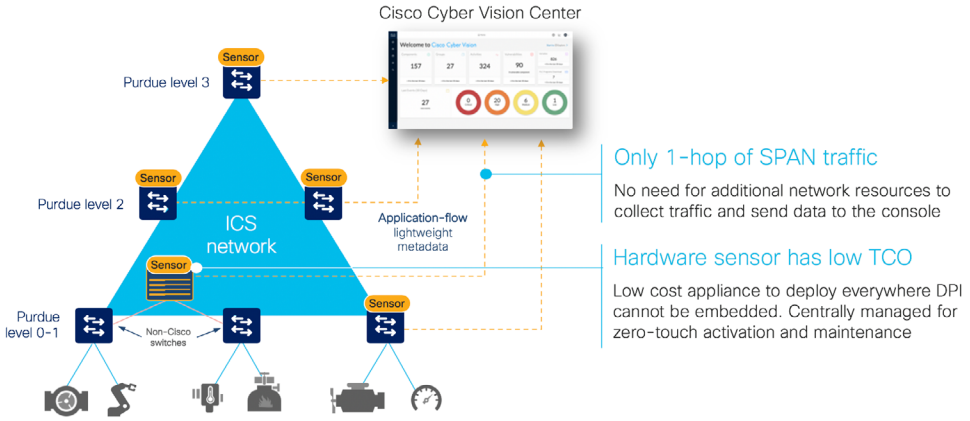
Not all network equipment can support embedded DPI capabilities. Gaining visibility on these local communications will require hardware sensor appliances, but not all appliances are created equal.

To maintain the benefits of not deploying a SPAN architecture, these appliances should:

1. Be centrally managed so they are easy to deploy and maintain
2. Have limited analytics features so they can run on low-cost hardware
3. Only send metadata to the central console so they don't need extra network resources

However, not all network equipment can support the embedded sensor feature. Gaining visibility on these local communications will require hardware sensor appliances. Beware that not all appliances are created equal – to maintain the benefits of not deploying a SPAN architecture, these appliances should 1) be centrally managed (so they are easy to deploy and maintain), 2) have limited analytics features (so they can run on low-cost hardware), and 3) only send metadata to the central console (so they don't need extra network resources).

Hardware sensors connect legacy switches to the OT security infrastructure



How Cisco can help

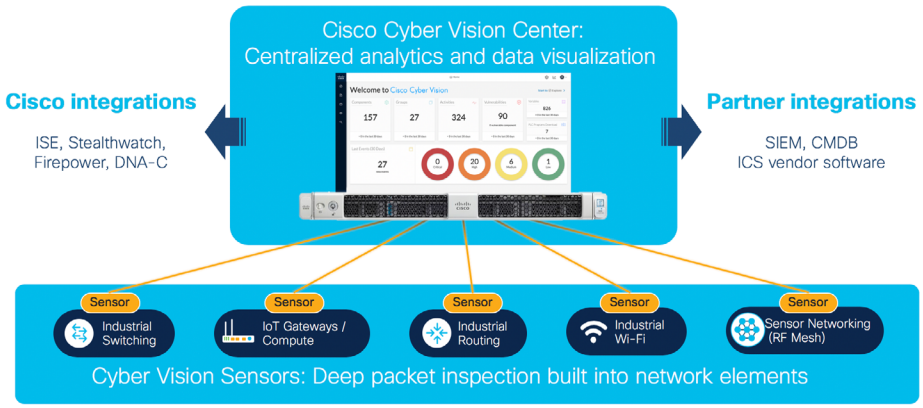
As organizations look to secure their industrial control networks, they need to be aware of the implications of the solutions they deploy. DPI location matters. Capturing traffic in the aggregation layer can be easily achieved with most solutions available today, but results in visibility of only north-south traffic. Gaining the visibility that will enable a truly effective threat detection strategy requires capturing network traffic at the cell layer, which also means deploying an expensive out-of-band SPAN network.

Cisco Cyber Vision leverages a two-tier deployment architecture and unique edge computing capabilities that offer the simplicity and cost saving benefits industrial organizations look for when deploying OT security at scale.

Cyber Vision sensors are embedded into Cisco's industrial network equipment, so that you can easily gain visibility on both east-to-west and north-to-south traffic anywhere in the network. Industrial application flows are decoded at the edge, so there is no need to mirror traffic, which can cause network congestion and jitter. Embedding DPI in the existing network hardware simplifies security deployment and makes it scalable.

Ready to secure your Industrial IoT network?

Two-tier edge monitoring architecture
Industrial cybersecurity that can be deployed at scale



The benefits of Cisco Cyber Vision aren't limited to organizations with Cisco networks. The sensor can also be offered in a SPAN architecture with Cisco IC3000 hardware sensor appliance. This provides maximum deployment flexibility to meet your needs with your existing network, while giving you time to replace older switches with DPI-enabled network equipment that's capable of seeing everything that attaches to it.

Cisco Cyber Vision provides full visibility into industrial control systems so you can build secure infrastructures and enforce security policies to control risk. Combining a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio, Cisco Cyber Vision can be easily deployed at scale so you can ensure the continuity, resilience, and safety of industrial operations.

Logicom Solutions

https://solutions.logicom.net/

Solutions@logicom.net

Cisco Partner
Gold Integrator

Greece: +30 211 1822800 | Cyprus: +357 22551010

Cisco-IoT-An-Edge-Architecture-Approach-to-Securing-Industrial-IoT-Networks-WP-08282021