INDUSTRIAL
CONTROL
SYSTEMS
Community of Interest

Architectural Considerations for Cyber Security Tooling in Industrial Control System/Operational Technology Environments

Aims of this guidance

This new guidance is designed to help organisations with architectural considerations for the deployment of cyber security tooling within Industrial Control Systems (ICS)/Operational Technology (OT) environments and ultimately gain assurance on the cyber security maturity of their environments. It focuses on practical 'HOW-TO' architectural element guidance for implementing cyber security tooling.

It has been designed to complement a range of NCSC generic architectural guidance, while focusing on the specific and unique aspects relating to ICS/OT, to support other ICS/OT focused guidance developed by the ICS COI.

Important Note: *While the ICS COI is supported by the NCSC, and NCSC staff are involved in a range of its activities, no formal review of this guidance article has been undertaken by the NCSC. The ICS COI and its members strive to produce relevant ICS/OT specific cyber security guidance to supplement principle based cyber security guidance published by NCSC and have taken care to reference this guidance where applicable. This guidance article will be reviewed every 18 months to ensure that it has not been superseded by guidance published by NCSC, relevance and that any references are still accurate. The ICS COI and its activities are purely voluntary, with guidance articles produced that are deemed needed by UK Operators and their supportive industry partners. The fact that this guidance article has been published by the ICS COI has no relevance to the priority and focus of guidance published by NCSC.*

Who is this guidance for?

If you are responsible for the cyber security of ICS/OT environments this article is designed to provide you with architectural understanding for the successful deployment of ICS/OT cyber security tooling, to enhance the cyber security maturity of your environment.

Structure of this guidance

This article provides guidance with respect to the following aspects of ICS/OT cyber security tooling architecture.

- High Level Architectures
  - On Premise
  - Pure Cloud
  - Hybrid Cloud
- Passive vs Active Approaches
- Traffic Capture
- Network Infrastructure

Introduction

In the context of this article, ICS/OT cyber security tooling refers to systems designed to provide one or more of the following functions:

- **Asset Discovery** – identifying devices connected to the monitored OT network including metrics such as IP address, MAC address, OS or firmware version, make model etc. This may be undertaken passively by listening to network traffic, actively by interrogating devices or a combination or both active and passive.
- **Vulnerability Management** – identifying known vulnerabilities of devices and/or software discovered within the monitored OT network, together with measures of criticality and likelihood.
- **Detection of Suspicious or Potentially Dangerous Operations** – identifying use of default passwords, weak encryption, malformed communication packets, program uploads, firmware changes etc.
- **Anomaly-Based Intruder Detection** – whereby a baseline of existing devices and communication patterns is developed during an initial learning period such that deviations from the baseline which may indicate suspicious behaviour can be enunciated.

Examples of vendors providing such ICS/OT cyber security tooling are provided here.

High Level Architectures

On-Premises

Pure on-premises refers to solutions comprising ICS/OT cyber security tooling sensors deployed on ICS/OT sites, typically with one or more central aggregators to provide single ‘pane-of-glass’ coverage of multiple ICS/OT sites and/or multiple ICS/OT cyber security tooling sensors on single sites.

Island Mode

Depending on the capabilities of ICS/OT cyber security tooling sensors and associated aggregators, architectures can be deployed supporting island-mode fallback, whereby visibility and security monitoring continues if connections to other parts of the OT Security Tooling solution are interrupted accidently, maliciously, or even deliberately as part of security incident response.

High Availability

ICS/OT cyber security tooling sensor and aggregators may support high availability deployments to mitigate ICS/OT cyber security tooling sensor/aggregator device failure. Typically, customers restrict high availability deployment to aggregators only, as the loss of these devices is likely to impact visibility and security monitoring across multiple ICS/OT sites.

ICS/OT Cyber Security Tooling Appliances

Depending on the particular ICS/OT cyber security tooling solution, on-Premises appliances may be deployed on vendor-specific hardware, 3rd-party hardware, virtualised appliances, or containerised appliances running on network hardware.

Restricted Hybrid Cloud Model for On-Premises

Some Hybrid Cloud OT cyber security tooling support a restricted hybrid model with the ability to limit internet connectivity to pulling down vulnerability information, exploit signatures and sensor application updates. Importantly, no actual customer ICS/OT data is shared with the cloud, other than the number of assets monitored (in the case of pay-per-asset licensing). In situations where continuous internet access is restricted, certain ICS/OT cyber security tools can accommodate intermittent cloud connections and/or facilitate manual downloads. Offline updates are also typically supported.

ICS/OT cyber security tooling sensors can be deployed in one or more ways depending on the specific vendor. The following table considers the pros and cons of each deployment approach.

Deployment Type	Description	Pros/Cons
ICS/OT cyber security tooling vendor- Specific Hardware	Typically provided as a range of commercial grade and ruggedized devices in various sizes and form factors to support maximum number of ICS/OT devices to be monitored. Appliance are deployed as combined software/hardware stack.	Pro: Single point of contact for support. Support arrangements should be scrutinised as some vendors white label 3rd party hardware and leave support to that 3rd party. Pro: Hardware tends to be optimised for ICS/OT cyber security tooling. Con: Not supported by all vendors as it complicates their service offering Con: can lead to vendor lock-in.
Generic 3rd Party Hardware	Appliance deployed on commercial grade or ruggedised hardware from 3rd-party vendors e.g., Dell, HP, Siemens, Schweitzer etc. Hardware typically needs to be sized to support expected maximum number of ICS/OT devices.	Con: No single point of support when ICS/OT Security Device fails. Possible finger pointing between vendors. Pro: Preferred by some vendors as it simplifies their service offering.
Virtualised Appliance	Appliance deployed on hypervisors such as VMWare ESXi, MS Hyper-V, Linux KVM, etc., depending on chosen ICS/OT cyber security tooling solution.	Pro: Scalability - Additional compute and storage resources can be added to increase the number of ICS/OT devices supported. Pro: Can use hypervisor supported failover mechanisms where available (e.g., VMWare vMotion) to provide high availability. Pro: May be able to leverage existing customer hardware. Con: Requires additional support for virtualised environments.

Containerised Appliance	Appliance deployed as Docker container on a range of 3rd party hardware such as network switches and routers.	Pro: Obviates the need for additional sensor device. Pro: Portability Pro: Scalability Con: Tend to be limited in resources affectively constraining sensor capabilities.

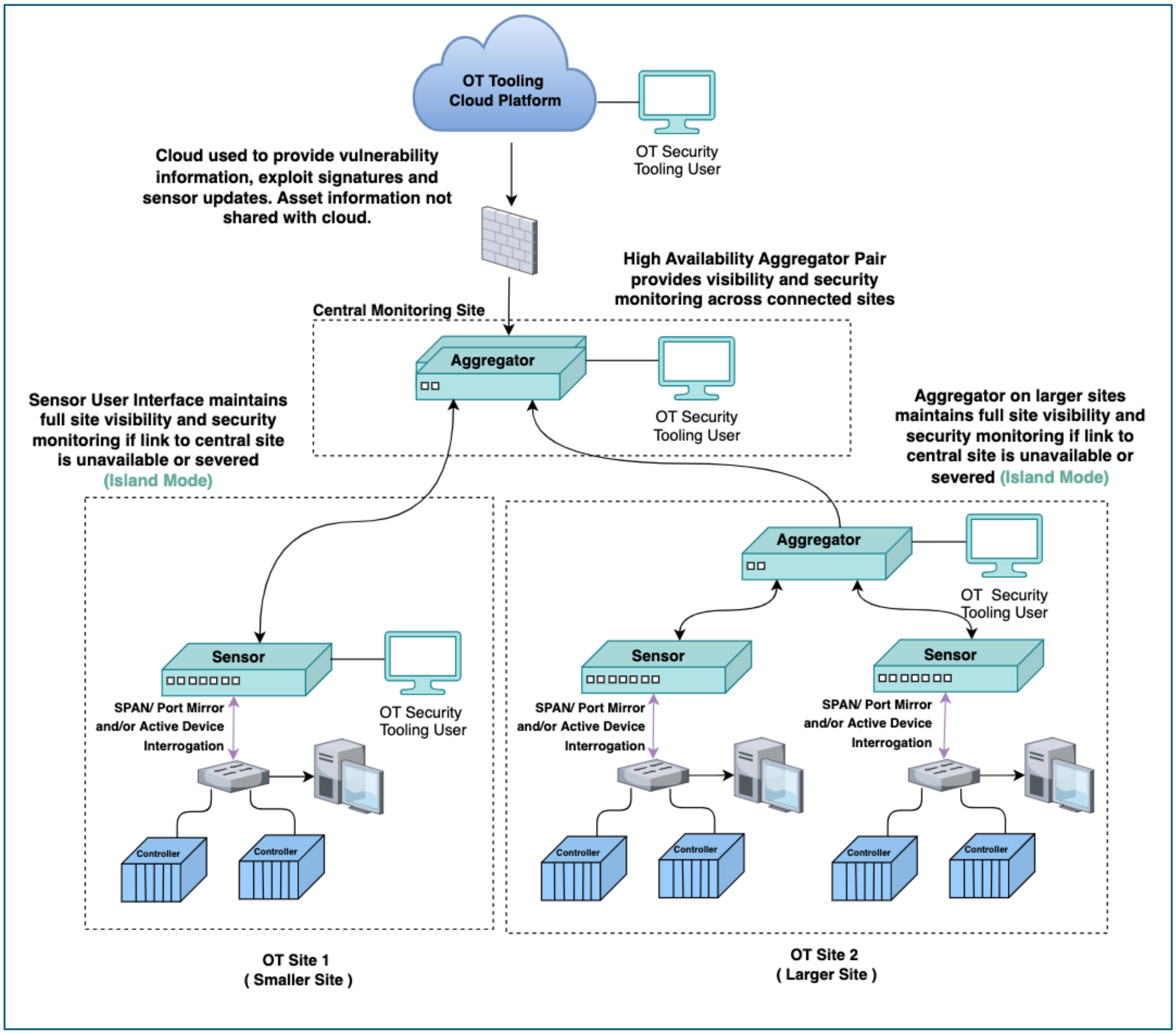
OT Tooling Cloud Platform
OT Security Tooling User
Cloud used to provide vulnerability information, exploit signatures and sensor updates. Asset information not shared with cloud.
High Availability Aggregator Pair provides visibility and security monitoring across connected sites
Central Monitoring Site
Aggregator
OT Security Tooling User
Sensor User Interface maintains full site visibility and security monitoring if link to central site is unavailable or severed (Island Mode)
Aggregator on larger sites maintains full site visibility and security monitoring if link to central site is unavailable or severed (Island Mode)
Aggregator
OT Security Tooling User
Sensor
OT Security Tooling User
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
OT Site 1 (Smaller Site)
OT Site 2 (Larger Site)

Figure 1- On-Premises Architecture with Restricted Cloud and Supporting Island Mode

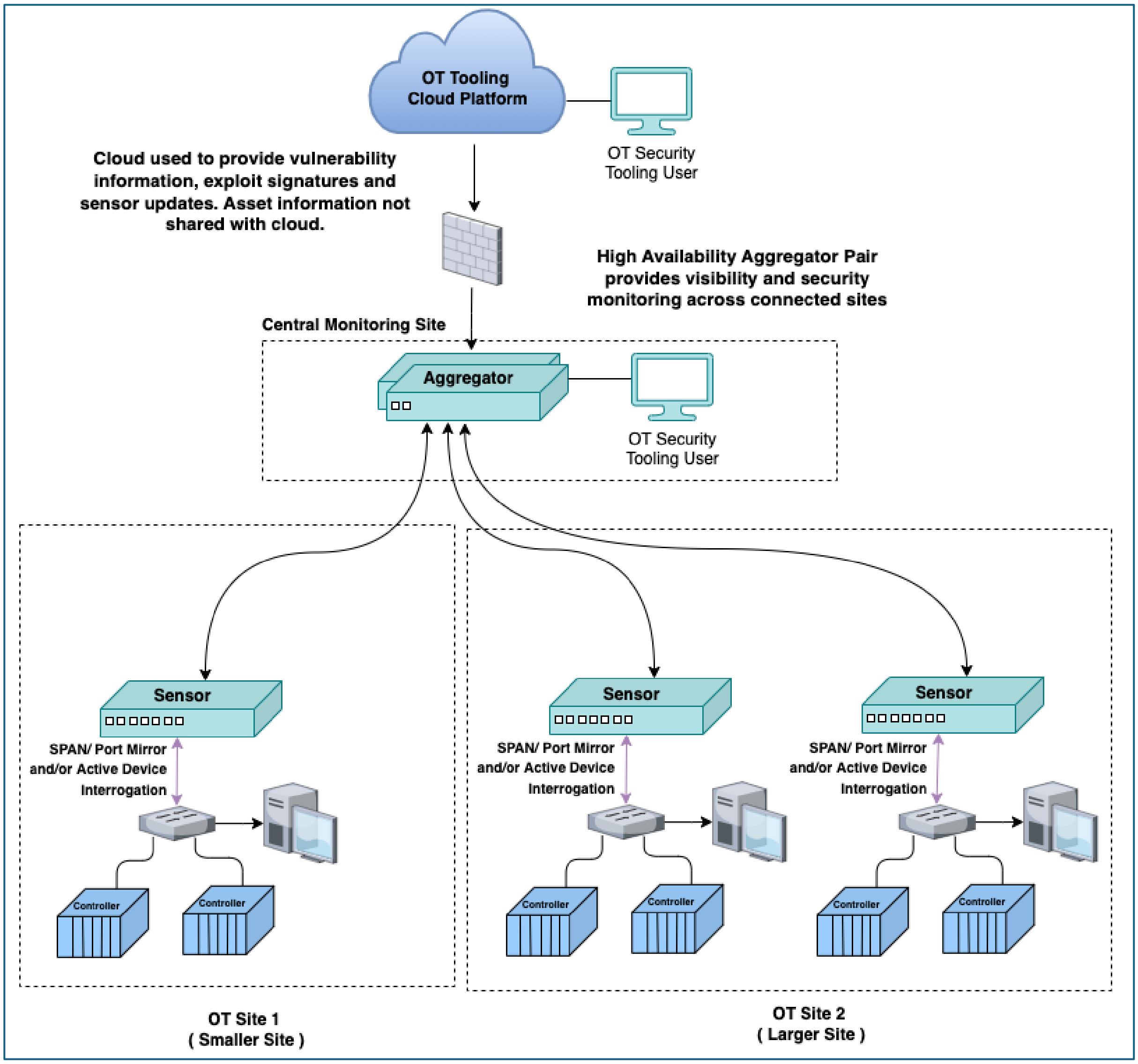
OT Tooling Cloud Platform
OT Security Tooling User
Cloud used to provide vulnerability information, exploit signatures and sensor updates. Asset information not shared with cloud.
High Availability Aggregator Pair provides visibility and security monitoring across connected sites
Central Monitoring Site
Aggregator
OT Security Tooling User
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
OT Site 1 (Smaller Site)
OT Site 2 (Larger Site)

Figure 2- On-Premises Architecture with Restricted Cloud Not Supporting Island Mode

Pure and Hybrid Cloud

Pure cloud-only ICS/OT cyber security tooling refers to solutions that handle asset discovery and security monitoring centrally in the cloud, with no processing undertaken at ICS/OT sites apart from maybe some compression and encryption prior to sending ICS/OT network traffic to the cloud for processing.

Hybrid Cloud solutions offer numerous advantages similar to those of pure cloud-based ICS/OT cyber security tooling including seamless scalability, secure access via the internet, and artificial intelligence/machine learning. Additionally, they allow for a transition to pure on-premises island mode when internet connectivity is lost and/or deliberately severed as part of a security incident response.

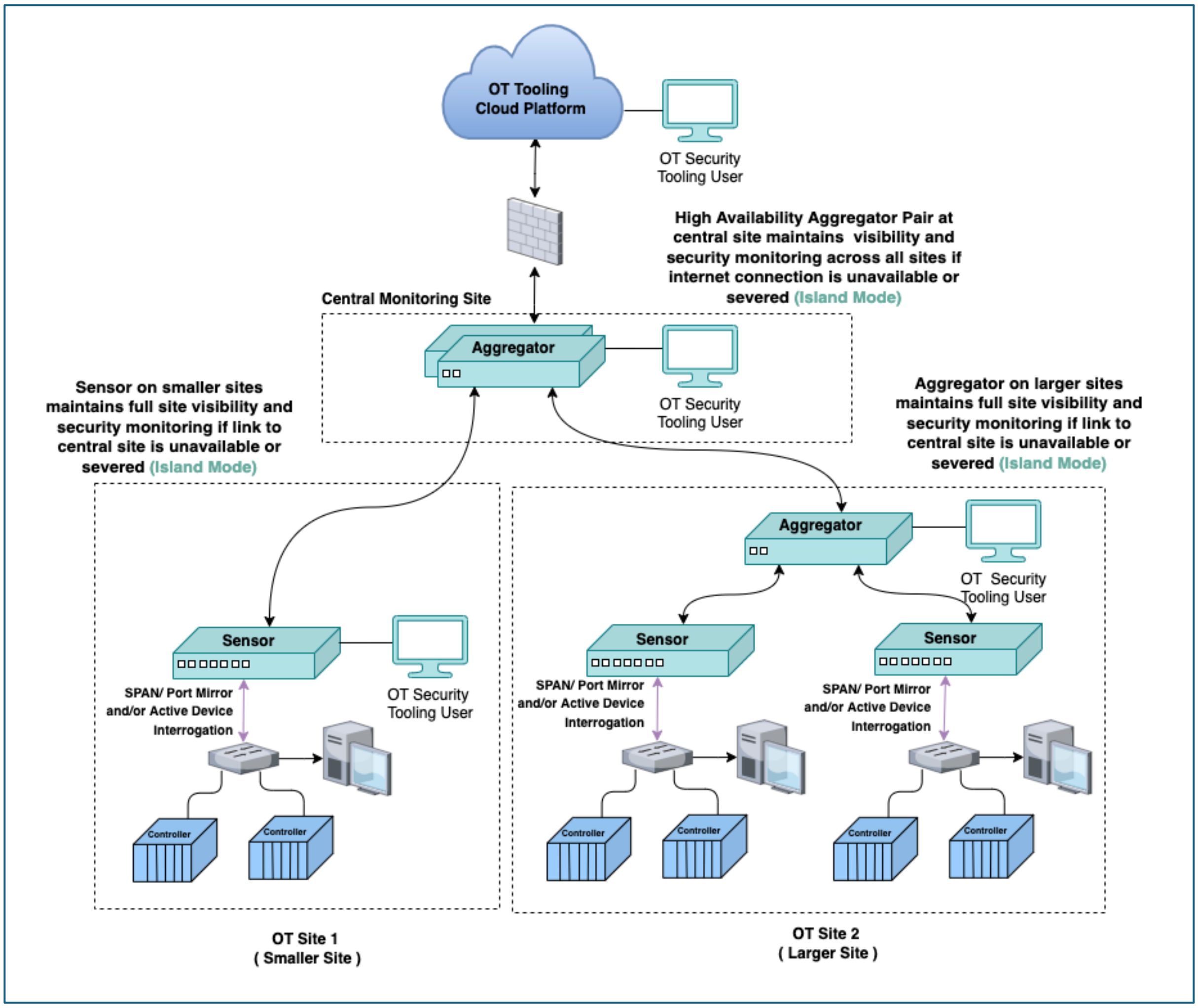
OT Tooling Cloud Platform
OT Security Tooling User
High Availability Aggregator Pair at central site maintains visibility and security monitoring across all sites if internet connection is unavailable or severed (Island Mode)
Central Monitoring Site
Aggregator
OT Security Tooling User
Sensor on smaller sites maintains full site visibility and security monitoring if link to central site is unavailable or severed (Island Mode)
Aggregator on larger sites maintains full site visibility and security monitoring if link to central site is unavailable or severed (Island Mode)
Aggregator
OT Security Tooling User
Sensor
OT Security Tooling User
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
Sensor
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
Controller
Controller
OT Site 1 (Smaller Site)
OT Site 2 (Larger Site)

Figure 3 -Hybrid Cloud Architecture Supporting Island Mode

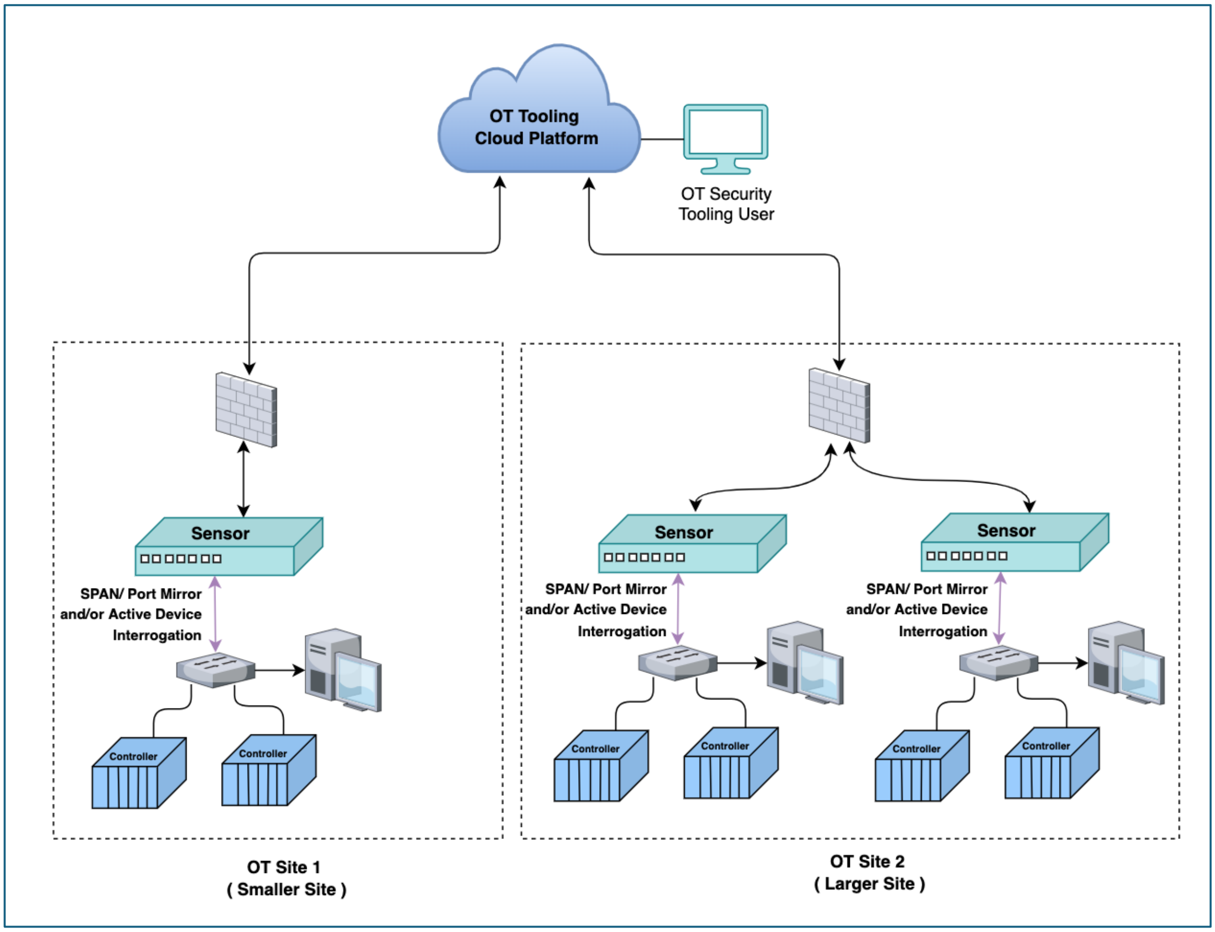
OT Tooling Cloud Platform
OT Security Tooling User
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
OT Site 1 (Smaller Site)
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
Sensor
SPAN/ Port Mirror and/or Active Device Interrogation
Controller
Controller
OT Site 2 (Larger Site)

Figure 4 - Hybrid Cloud Architecture without Island Mode

The idea of employing cloud-based ICS/OT cyber security Tools remains a contentious issue within the ICS/OT community for various reasons. A significant concern among some members is the perception that any link to the cloud inherently exposes vital ICS/OT environments to potential threats from malicious actors.

However, given the reliance of organisations on cloud platforms for virtually every other aspect of their business, it would seem logical that there must be tangible advantages such platforms can offer ICS/OT cyber security tooling, and there are.

With few exceptions, most organisations deploying ICS/OT cyber security tooling these days do so with the acceptance that cloud connections are necessary – if only to provide real-time updates of threat intelligence, vulnerability information, exploit signatures, etc., to on-prem sensors.

Advantages of cloud-based ICS/OT cyber security tooling:

Artificial Intelligence (AI) / Machine Learning (ML) - Early detection of suspicious behaviour within ICS/OT systems is key to providing appropriate and timely security incident responses.

AI/ML within some ICS/OT cyber security tooling can already assist security response personnel by identifying patterns, correlations and context of attacks that may not be immediately obvious.

Further AI/ML models can increasingly provide recommendations regarding which security alerts and incidents to prioritise based on vulnerability-linked attack paths, device criticality, trending traffic rates etc.

The reason cloud-platforms are particularly suited for AI/ML is that they can dynamically allocate the significant compute and storage resources needed by AI/ML models as and when required, something that on-prem solutions struggle to achieve economically. Furthermore, ICS/OT cyber security tooling based on multi-tenanted cloud platforms, have access to increasing amounts of security incident data from many organisations across multiple industrial verticals with which to train underlying AI/ML models.

Even if on-premises solutions can achieve similar levels of detection today, it's extremely likely that only ICS/OT cyber security tooling leveraging AI/ML will keep pace with the evolving sophistication of ICS/OT cyber-attack tactics and techniques, especially as bad actors turn to AI tools themselves.

Feedback Telemetry - As well as enhancing security detection capabilities, cloud-based ICS/OT cyber security tooling has major advantages for basic ICS/OT device visibility. For example, an unknown device type found within one organisation's ICS/OT system can be flagged within the cloud's back end, allowing the ICS/OT cyber security tooling vendor to manually add relevant device details. This will then make the device a known type for all monitored systems connected to the vendor's cloud. This is an example of feedback telemetry.

Development of ICS/OT cyber security tooling also benefits from feedback telemetry by allowing ICS/OT cyber security tooling vendors to gauge whether new capabilities are providing value as expected.

Cross Customer Correlation - ICS/OT cyber security tooling leveraging multi-tenanted cloud will have the possibility of using anonymised customer security incident data to identify global attack trends and provide advance warning of potential attacks. For example, if ICS/OT cyber security tooling identifies multiple attacks on electrical utilities involving a particular vendor's substation control system, warnings can be issued to other utilities around the world using the same control system, or even to non-utility users of the same systems, such as rail and even data centre operators.

Development Velocity - Unlike on-premises solutions that typically see software releases measured in months, cloud-based solutions typically use a Continuous Integration, Continuous Delivery (CI/CD) approach where software releases are measured in days.

Faster software development provides greater opportunity to keep up with evolving security attack techniques as well as addressing specific customer requirements in a timelier fashion.

Resilience/Disaster Recovery - Cloud based solutions typically leverage highly resilient architectures based on multiple geographically separated data centres with dynamic load balancing. Workloads in any one data centre are seamlessly transferred another in response to an infrastructure failure. Often a third data centre is employed to provide data recovery in response to a disaster affecting the primary online data centres.

Security and the Cloud

The need to scrutinise security provisions of cloud-based ICS/OT cyber security tooling is vital give such system may involve the transmission and storage of ICS/OT system information outside of physical and/or logical ICS/OT site boundaries, for example complete lists of ICS/OT assets deployed together with their known exploitable vulnerabilities. Extremely useful for any potential bad actor to get hold of.

Security considerations when choosing Hybrid Cloud and Pure Cloud ICS/OT cyber security tooling:

- How is data at rest and in motion secured?
- Is access to customer data held in multi-tenanted clouds suitably segregated and secured (e.g., unique tenant encryption keys)?
- Are all communications initiated outbound to the cloud, even for sensor updates?
- Is security by design methodologies used for cloud development?
- Is Role Based Access Control supported, and if so, how granular is this?
- Is multi-factor user authentication supported?
- What level of access does OT Security Tooling vendors have to undecrypted customer data?
- Do cloud platform users have the ability to change OT Security Tooling sensor configurations on site? It is important to understand whether this can be leveraged to affect a cyber-attack from the vendor’s cloud platform.
- Is there independent 3rd party (e.g., DNV) testing and certification backing up answers to the above questions.
- Are there data sovereignty issues that will restrict where data is held geographically.

Pure On-Premises vs Hybrid Cloud vs Pure Cloud Summary

	Pure On-Prem	**Hybrid Cloud**	**Pure Cloud**
Tooling Sensors deployed on ICS/OT Sites perform asset discovery and security monitoring	Yes	Yes	No
Internet Connection Required	Typically for pulling down latest vulnerability information, exploit signatures, OT Tooling updates. Manual downloads are normally supported.	Yes for pulling down latest vulnerability information, exploit signatures, ICS/OT cyber security tooling updates	Yes
Scalability	Not as good as cloud-based solutions	Extensive	Extensive
Simple secure remote user access to assets inventory and security alerts	No access often requires the use of jump servers and or remote desktop services (e.g., Citrix)	Yes	Yes
Raw OT traffic sent to cloud	No	No	Yes
Bandwidth requirements between ICS/OT site and cloud	Typically for updates only	Low can be less than 500kbps per sensor	High can be multiple Gbps per sensor
Supports Island-Mode in case internet connection is unavailable or purposely severed.	Yes	Yes	No

	Pure On-Prem	**Hybrid Cloud**	**Pure Cloud**
Comprehensive filtering of unwanted or less critical traffic prior to sending to cloud	Not Applicable	Yes	No
Software Updates	Typically measured in months	Often measured in days for cloud-based elements Typically measured in months for on-prem elements	Often measured in days

Passive vs Active Approaches

Whether passive or active approaches are leveraged to provide the required ICS/OT cyber security tooling capabilities has a significant architectural impact. This section covers the most popular approaches used by current ICS/OT cyber security tooling, including:

- Passive Network Monitoring
- Active Discovery/Intelligent Device Interrogation
- Active Host-Based Agents

Note not all these approaches are supported by all ICS/OT cyber security tooling, and not all approaches are appropriate for all organisations. The pros and cons associated with these approaches are discussed, including the potential risks such approaches introduce into ICS/OT systems.

More detailed information can be found in the following ICS COI guidance articles:

- Visibility for ICS/OT environment asset management
- Active Discovery/Intelligent Device Interrogation in an ICS/OT Environment - Meet Admin Corp

Passive Network Monitoring

Passive ICS/OT cyber security tooling, also referred to as network-based security tooling, perform asset discovery and security monitoring by listening to communications occurring between ICS/OT system devices. In theory, these systems don't introduce new traffic into monitored systems and consequentially should never lead to process disruption.

Simple data diodes located between ICS/OT systems and ICS/OT cyber security tooling sensors can be used if there are any doubts about how SPAN/Port Mirror ports might deal with received data. Such data diodes can also be used as a point of demarcation when ICS/OT cyber security tooling is not managed by ICS/OT staff.

Pure passive solutions can also result in process issues if not deployed carefully. Network switch port mirroring, often used to provide ICS/OT traffic flows to ICS/OT cyber security tooling sensors, can result in switches being overwhelmed and unable to provide normal switch functions, especially with older, less capable switches. Also, remote traffic capture techniques, used to deliverICS/OT traffic flows across multiple switches to ICS/OT cyber security tooling sensors, can potentially impact ICS/OT system performance by significantly increasing traffic volumes.

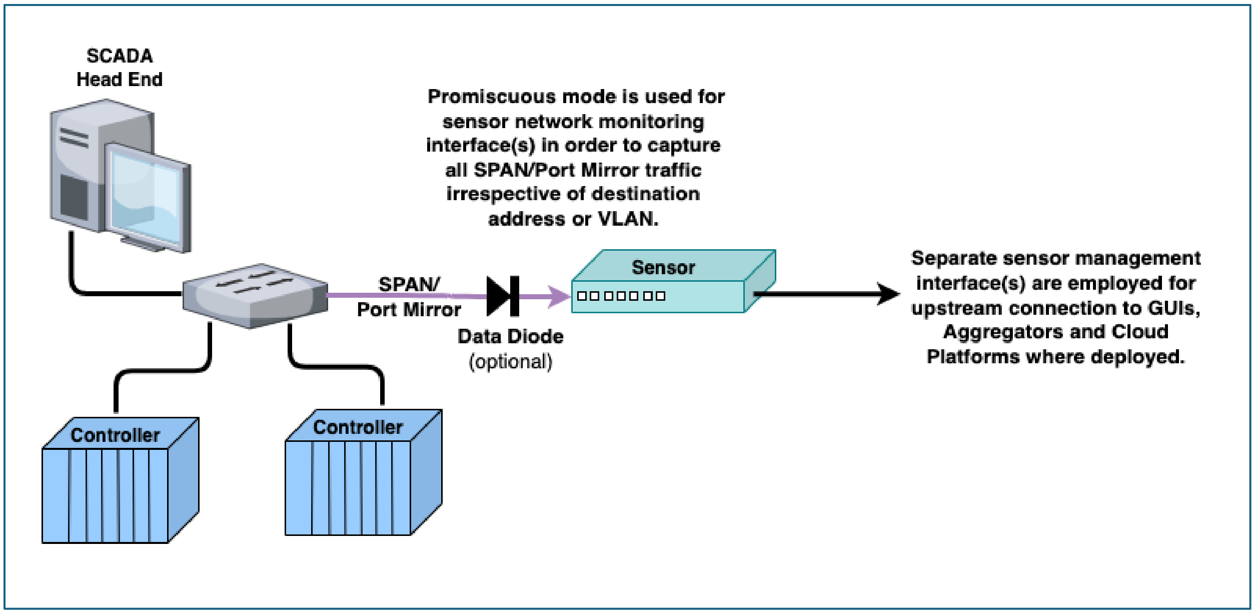
SCADA
Head End
Promiscuous mode is used for sensor network monitoring interface(s) in order to capture all SPAN/Port Mirror traffic irrespective of destination address or VLAN.
SPAN/
Port Mirror
Sensor
Data Diode
(optional)
Separate sensor management interface(s) are employed for upstream connection to GUIs, Aggregators and Cloud Platforms where deployed.
Controller
Controller

Figure 5- Passive Network Monitoring

Active Discovery/Intelligent Device Interrogation

Many ICS/OT cyber security tooling solutions can actively communicate with ICS/OT devices to provide asset information, or to augment existing asset information collected passively. Typically, this will involve querying devices using their native protocols e.g., Ethernet/IP for Rockwell Automation industrial controllers, WinRM for hosts running Windows, SNMP for any devices that respond to SNMP queries.

The amount and accuracy of device information afforded through active querying will almost always be more extensive than is possible through passive mean alone. Passive techniques can't for example identify open ports on industrial controllers, or software installed on Windows systems, as such information is not available within the monitored communications. Even correctly identifying basic information such as device MAC address is not always possible passively.

The threat of malicious actors targeting ICS/OT systems via the very ICS/OT cyber security tooling used to protect them is likely to increase as deployment of such tooling become ubiquitous, and market consolidation results in a much smaller pool of ICS/OT cyber security tooling products for malicious actors to focus on. Customers need to be sure that processes adopted by ICS/OT cyber security tooling vendors in order to mitigate such threats are sufficient.

OT cyber security tooling using only active querying have the advantage of requiring little if any network infrastructure configuration, thus making deployment quicker and less prone to the potential pitfalls associated with such configuration. However, because pure active querying does not examine network communications, it has little ability to provide security monitoring or provide device communication maps.

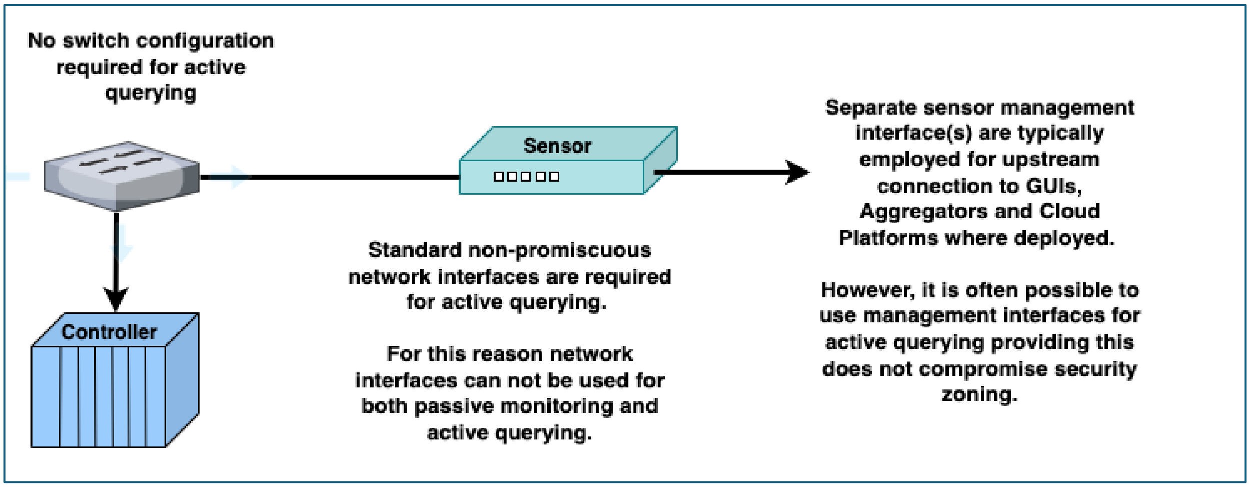
No switch configuration required for active querying
Sensor
Controller
Standard non-promiscuous network interfaces are required for active querying.
For this reason network interfaces can not be used for both passive monitoring and active querying.
Separate sensor management interface(s) are typically employed for upstream connection to GUIs, Aggregators and Cloud Platforms where deployed.
However, it is often possible to use management interfaces for active querying providing this does not compromise security zoning.

Figure 6 - Active Device Querying

Active Host Based Agents

A number of ICS/OT cyber security tooling solutions support agents to continuously monitoring host computers on which they are installed. Depending on the specific ICS/OT cyber security tooling product, these agents can report operating system versions, installed patches, installed software, running processes, logged in users, USB insertion, and in at least one case, act as a sensor to provide visibility of connected devices, either passively or actively.

Whilst historically, these agents have been restricted to general-purpose compute platforms such as Windows and Linux hosts, variants now exist that support specialised ICS/OT devices such as Programmable Logic Controllers (PLCs).

Given agents are intended to run on host devices within live ICS/OT systems, careful consideration of how they may affect host operations should be assessed to ensure host primary functions are not compromised. Ideally agents should by qualified by associated automation product vendors.

As with Active Discovery/Intelligent Device Interrogation, the threat of malicious actors targeting ICS/OT systems via host-based ICS/OT cyber security tooling agents need to be considered. Customers need to be sure that assurance processes adopted by ICS/OT cyber security tooling vendors to mitigate these threats are sufficient.

Passive vs Active Discovery/Intelligent Device Interrogation vs Host Agent Summary

	Passive Monitoring via SPAN/Port Mirroring	Passive Monitoring via TAP (see section on TAPs)	Active Discovery/Intelligent Device Interrogation	Host Agent
Network based asset discovery	Yes	Yes	No	If agent supports passive monitoring of connected devices
Network based security monitoring	Yes	yes	No	If agent supports passive monitoring of network
Querying devices for enhanced information	No	No	Yes	If agent supports active querying of connected devices
Network switch configuration required	Yes	No	No	No
Can impact monitored devices	No Assumes appropriate switch configuration	No	Yes	Yes
Sensor can act as attack vector	Possible but unlikely Can be mitigated by using simple data diode	No	Yes	Yes

	Passive Monitoring via SPAN/Port Mirroring	Passive Monitoring via TAP (see section on TAPs)	Active Discovery/Intelligent Device Interrogation	Host Agent
Capability considerations	Which protocols are supported passively? Can new protocol support be developed and how long?	Which protocols are supported passively? Can new protocol support be developed and how long?	Which protocols are supported for active querying? Can new protocol support be developed and how long?	Supported hosts? Windows (what versions), 'NIX (what versions), Controllers?

Traffic Capture

Capture Location

When considering the deployment of ICS/OT cyber security tooling, it is important to understand the need to capture device-to-device communication traffic for good visibility and security monitoring. Simply connecting an ICS/OT cyber security tooling sensor to a core switch may not be sufficient.

Consider the situation depicted below where an ICS/OT cyber security tooling sensor is capturing SPAN/Port mirror traffic from a Core Switch. The sensor has full visibility of communication packets flowing between the Primary Automation Server and both Controllers, as these packets flow through the monitored Core Switch. However, this is not the case for communication packets flowing between the Secondary Automation Server and Controller #2, which do not flow through the monitored core switch. Broadcast and Multicast communication packets will still be detected in the case of Secondary Automation server communications; however, these provide minimal visibility.

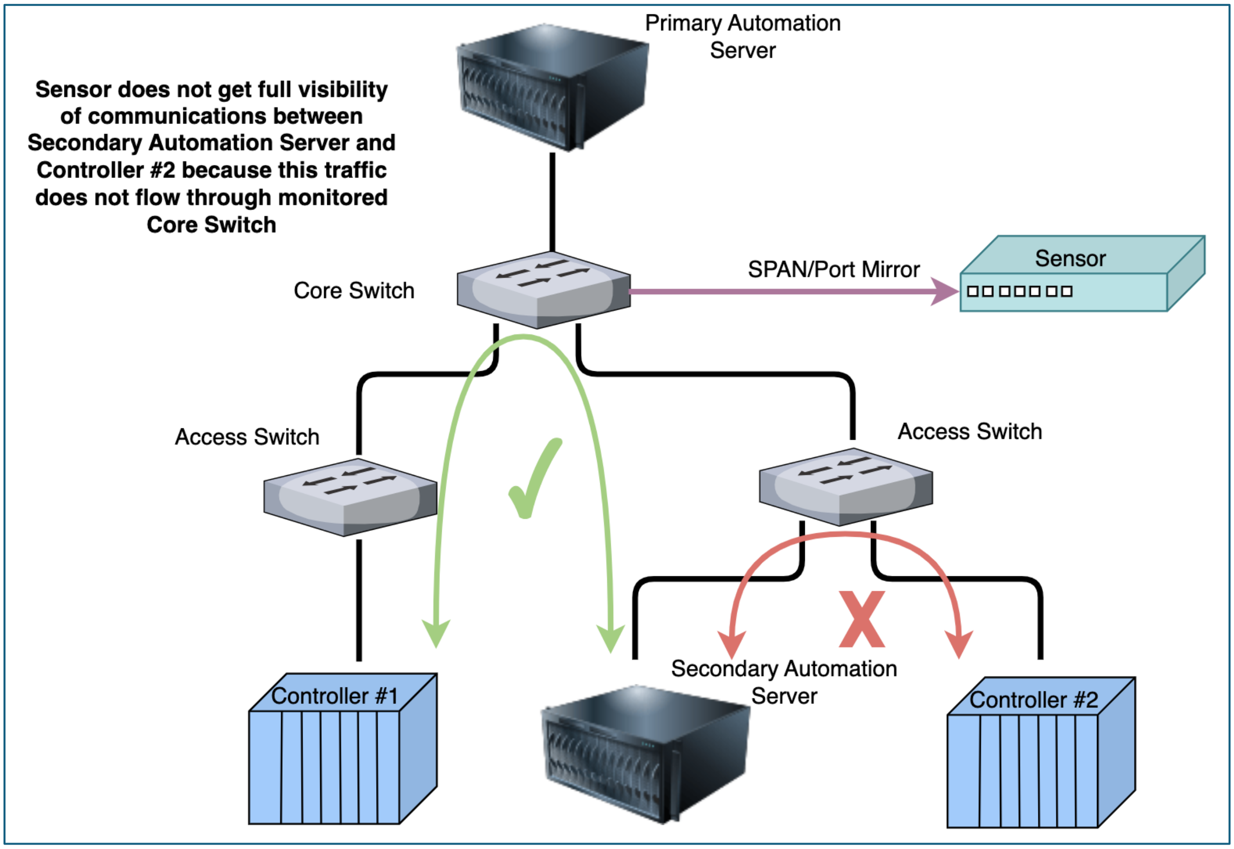
Primary Automation Server
Sensor does not get full visibility of communications between Secondary Automation Server and Controller #2 because this traffic does not flow through monitored Core Switch
Core Switch
SPAN/Port Mirror
Sensor
Access Switch
Access Switch
✓
X
Secondary Automation Server
Controller #1
Controller #2

Figure 7 - Capture Location Considerations

Minimal Capture Approach (Passive)

In theory it should be possible for ICS/OT cyber security tooling to provide 100% coverage by monitoring every single network switch. Indeed, given unlimited budgets, sufficient time, an acceptance of the potential disruption, and agreement with any third-party maintainers, such an approach is indeed possible, at least for devices that communicate over IP / Ethernet.

However, if the primary objective is passive asset discovery and/or vulnerability management then a more pragmatic approach is possible by recognising that the majority of ICS/OT systems are server-client based. This means that most if not all communications flow between central automation servers and connected controllers, with little or no traffic between controllers.

Comprehensive asset discovery and/or vulnerability management and detection of suspicious operations can be achieved by concentrating traffic capture only on those switches used to connect automation servers and engineering workstations. This is likely to be significantly cheaper, quicker and less invasive than attempting to monitor all switches.

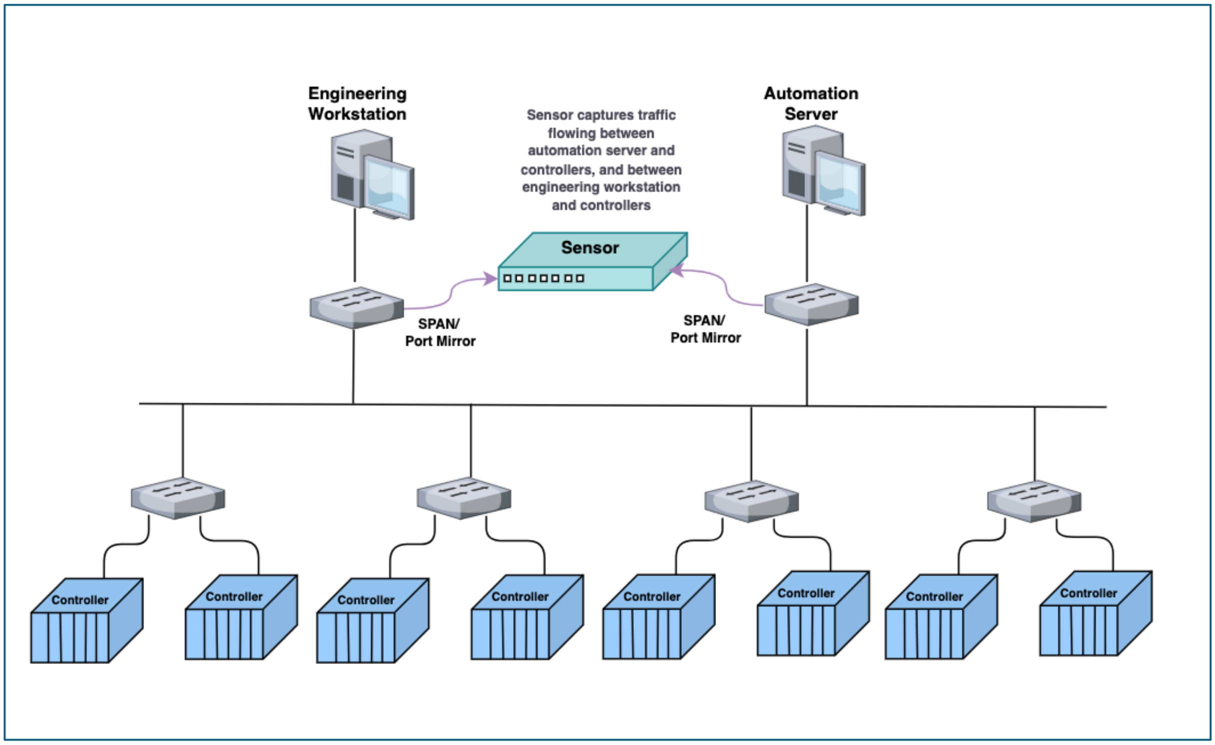

Figure 8 - Minimal Capture Approach (Passive)

A potential downside of this minimal capture approach is that an attacker could in theory plug a laptop or other device into an unmonitored switch. However, the attacked would first need to be on site. Also, any broadcast traffic generated by the new device would still be detected. This downside could also be minimised where active querying of network switches is supported by the ICS/OT cyber security tooling.

Phased Capture Approach

Organisations looking to deploy ICS/OT cyber security tooling may like to consider a phased approach whereby the Minimal Traffic Capture approach described above is deployed in the first instance, with later expansion to monitor other switches if further coverage is deemed necessary.

Input /Output (IO) Device Traffic Capture

Some ICS/OT cyber security tooling can monitor communications between controllers and smart input/output devices, however the additional visibility and security monitoring gained by doing this is often minimal as these communications typically comprise little more than bundled digital and analogue values with little or no meta data to provide context. Also, communications between controllers and smart IO devices are usually private to the controllers, with no direct access from higher levels in the control system (Purdue level 2 and above).

Some ICS/OT cyber security tooling can import automation project files to provide additional context for smart IO devices, but whether or not this level of monitoring is worth the additional expenses and effort needs to be considered based on the likely risk.

Traffic Capture and Purdue

Because most ICS/OT cyber security tooling sensors have several monitoring ports with which to passively monitor multiple network segments simultaneously, a single sensor can often monitor an entire ICS/OT system or sub-system. Unless there are constraints with respect to the capabilities of existing switches, or other factors such as network topology, cabling infrastructure, or physical site arrangements, the aim should typically be to keep ICS/OT cyber security tooling deployments as simple as possible. Customers need to confirm ICS/OT cyber security tooling sensors cannot bridge network segments, either inadvertently or maliciously.

Reference to Purdue should not be used to restrict ICS/OT cyber security tooling sensors to monitoring only Purdue levels in which they are deployed. This is because Purdue is not a risk-based security model. On the other hand, IEC62443 risk-based principles should always be considered.

The following diagram shows how simple data diodes can be used to control risk between an ICS/OT cyber security tooling sensor in one zone, and network segments associated with two other zones.

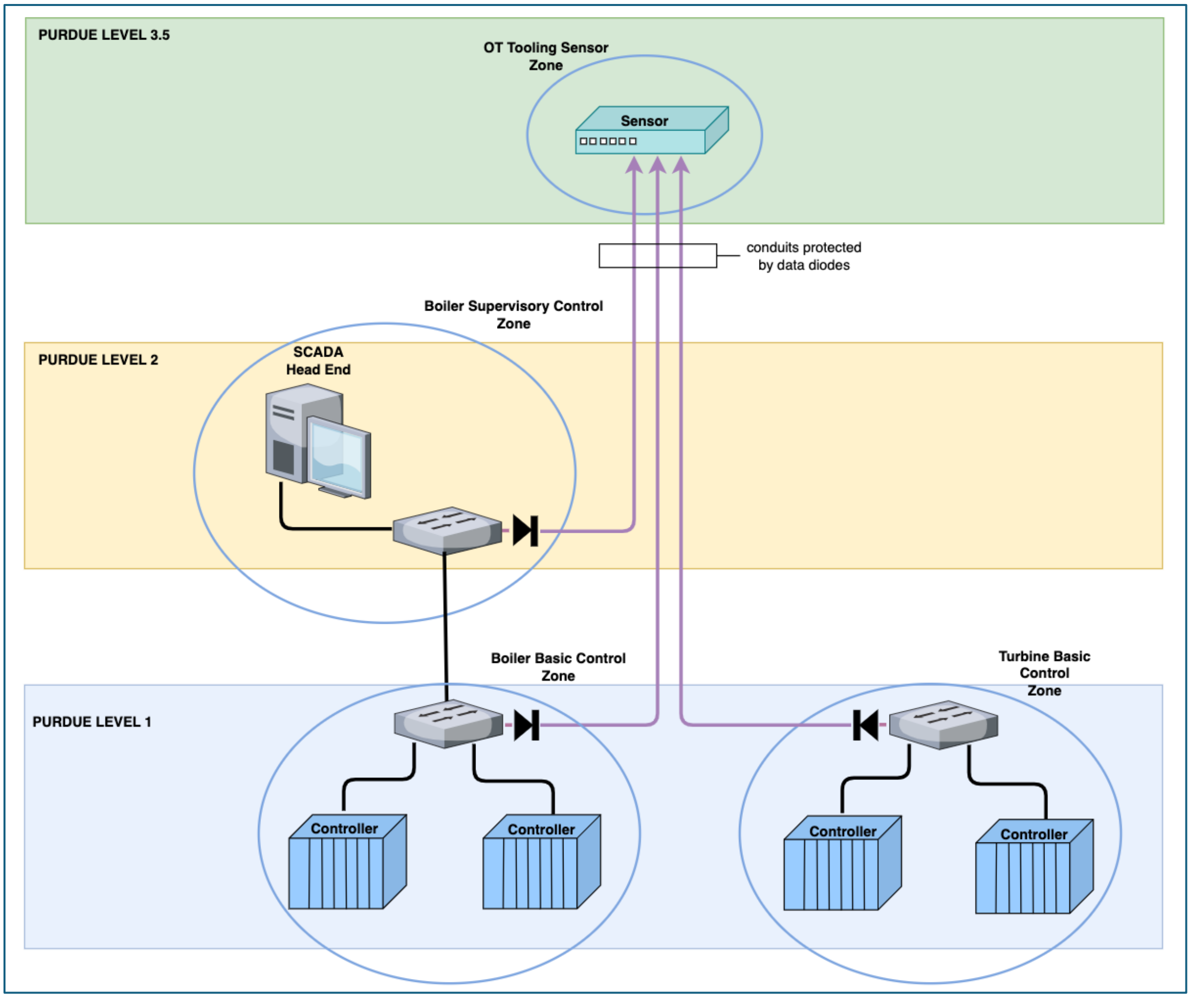

Figure 9 - ICS/OT Security Tooling and IEC62443 (Not Purdue)

Network Infrastructure

Once identifying the optimal traffic capture locations for effective passive monitoring, it is essential to consider the methods for acquiring the necessary network traffic at these sites for the ICS/OT cyber security tooling sensors. The integration of OT cyber security tooling into existing ICS/OT networks is likely the most complex element of its deployment. In contrast, networking for active monitoring is comparatively straightforward, as long as valid network paths are available between the ICS/OT cyber security tooling sensors and the devices that require monitoring.

SPAN/Port Mirroring

The first question is whether or not existing network switches support SPAN (Switch Port Analyser) or port mirroring. Both can provide a copy of traffic flowing from selected source switch ports to at least one destination port on the same switch. However, not all switches are equal in this regard, and the following should be considered:

- Can SPAN/Port mirroring impact normal switch operation be affecting performance of the ICS/OT system being monitored? Ideally SPAN/Port mirroring should have lower priority than normal switch functions such that SPAN/Port mirroring degrades (drop packets) before normal switch operation is affected.
- Can all switch ports required for data capture be used as source ports concurrently? Many switches support mirroring only on a subset of available ports which may impact the ability to capture all traffic of interest.
- Can source VLANs be selected as sources rather than individual ports? This can be useful for filtering out unwanted traffic, for example pure IT traffic.
- Do switches support SPAN/Port Mirroring of input traffic in preference to switch output traffic? Ideally switch input traffic is selected so traffic is captured prior to any processing undertaken by the switch (e.g., copied with VLAN encapsulation intact etc.)
- Do switches definitely support SPAN/Port mirroring? These capabilities can vary with firmware version, and even hardware revisions and should be checked.

SPAN/Port mirror traffic collection is restricted to local / direct connections between switch and ICS/OT cyber security tooling sensor. In the case of copper connections, this generally means distances less than 90m (allowing 10m for tails) should be used, although fibre connections where supported can be much greater.

SPAN/Port Mirroring should act as a data diode between switches and connected ICS/OT cyber security tooling sensors, preventing interference with ICS/OT systems being monitored. A separate data diode can be provided if there are any doubts about how a SPAN/Port Mirror port might deal with received data.

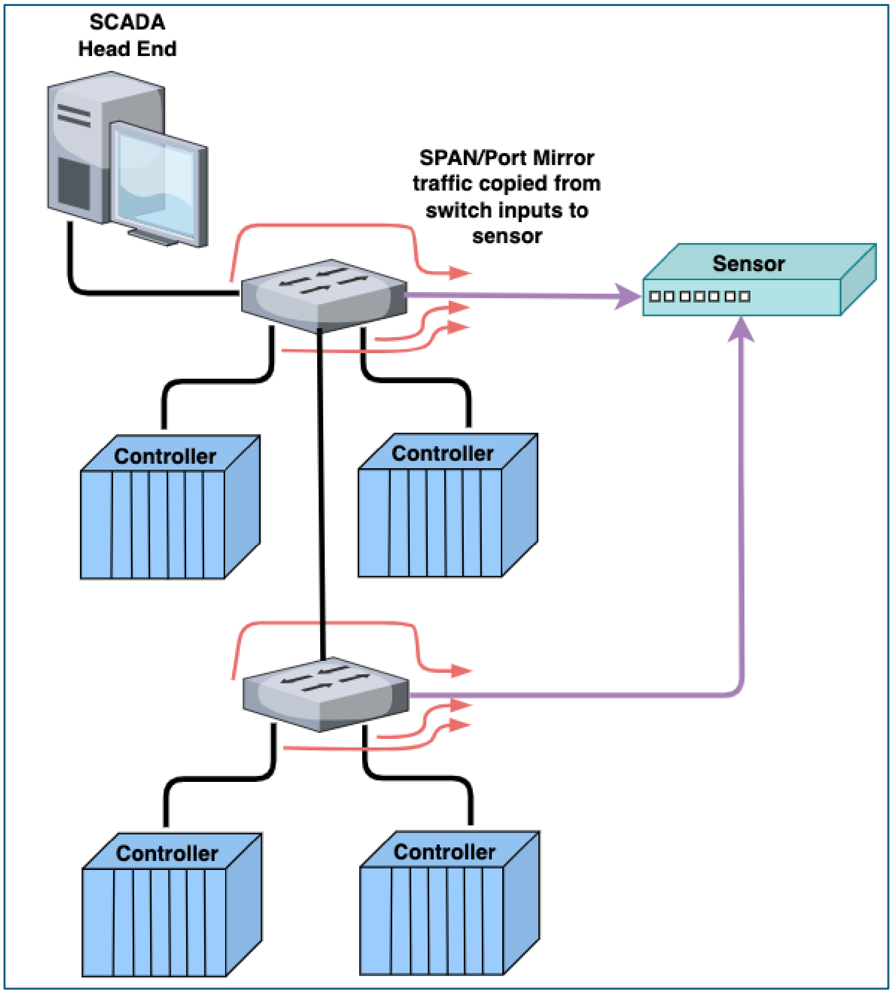

Figure 10 - SPAN/Port Mirror directly connects to Sensor.

TAPs

TAP (Test Access Point) devices obviate the need to configure managed switches for SPAN/Port mirroring and can be used with unmanaged switch infrastructure. They also have the advantage of never missing (dropping) network traffic packets, which can be an issue for SPAN/Port Mirroring when switches become heavily loaded. However, switch configuration will typically be undertaken where possible rather than introducing additional devices.

TAP devices provide a copy of traffic flowing through them. As a minimum they comprise three ports: two network ports and a monitoring port. TAPs are deployed in-line on network connections of interest using two network ports with a monitoring port connected to the ICS/OT cyber security tooling sensors. There are a number of different network TAP types. For ICS/OT cyber security tooling, aggregating TAPs are typically used, whereby traffic flowing between the two network ports in both directions is copied to the monitoring port. Because no traffic can flow from the monitoring port back into the monitored network connections, TAP devices act as simple data-diodes.

Multi-way Aggregating TAPs are available providing single aggregated output from multiple TAPs e.g., 4-way, 8-way.

Considerations when deploying TAP devices:

- Copper vs Fibre
- Active Querying vs Passive Monitoring
- Supported line speed.
- Combined throughput of aggregating TAPs.
- Failover time for active TAPs
- Cost of TAP vs cost and disruption of replacing existing unmanaged switch with managed switch

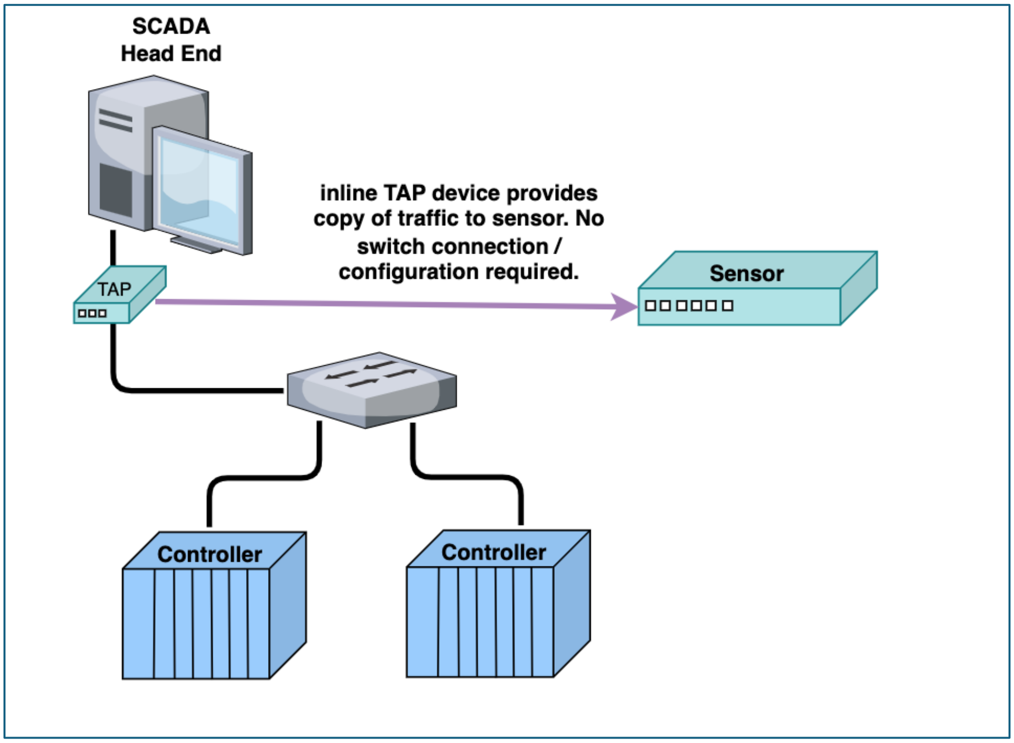
SCADA Head End
inline TAP device provides copy of traffic to sensor. No switch connection / configuration required.
TAP
Sensor
Controller
Controller

Figure 11- TAP Devices Alternative to SPAN/Port mirroring.

RSPAN

Switches supporting RSPAN (Remote SPAN) facilitate the collection of traffic from switches not local to ICS/OT cyber security tooling sensors by copying switch port traffic into RSPAN Virtual Local Area Networks (VLANs) that are then trunked across the network to destination switches. Destination switches de-encapsulate RSPAN VLANs trunks to provide individual SPAN connections to adjacent ICS/OT cyber security tooling. Considerations for use include:

· All switches involved in the RSPAN session must support RSPAN. While it's possible to use switches from different vendors, using switches from different vendors can cause compatibility issues, as they may implement RSPAN features differently, potentially affecting the session's proper functioning.

- RSPAN operates across Layer 2 segments only, so cannot traverse firewalls and routers.
- Multiple source switches and multiple destination switches can take part in a single RSPAN session.
- Uplink utilisation should be considered to ensure selection of source ports and source VLANs will not exceed available uplink bandwidth. Uplink bandwidth can increase by over 100%.
- Because all RSPAN VLAN packets are flooded (sent to all switches associated with the RSPAN VLAN), the number of source switches needs to be considered taking into account monitored traffic volumes.
- VLAN Identifiers (IDs) may not be preserved within RSPAN traffic depending on the make and model of switch.
- Capabilities of switches purporting to support RSPAN should be checked. These capabilities can vary with firmware version, and even hardware revisions.

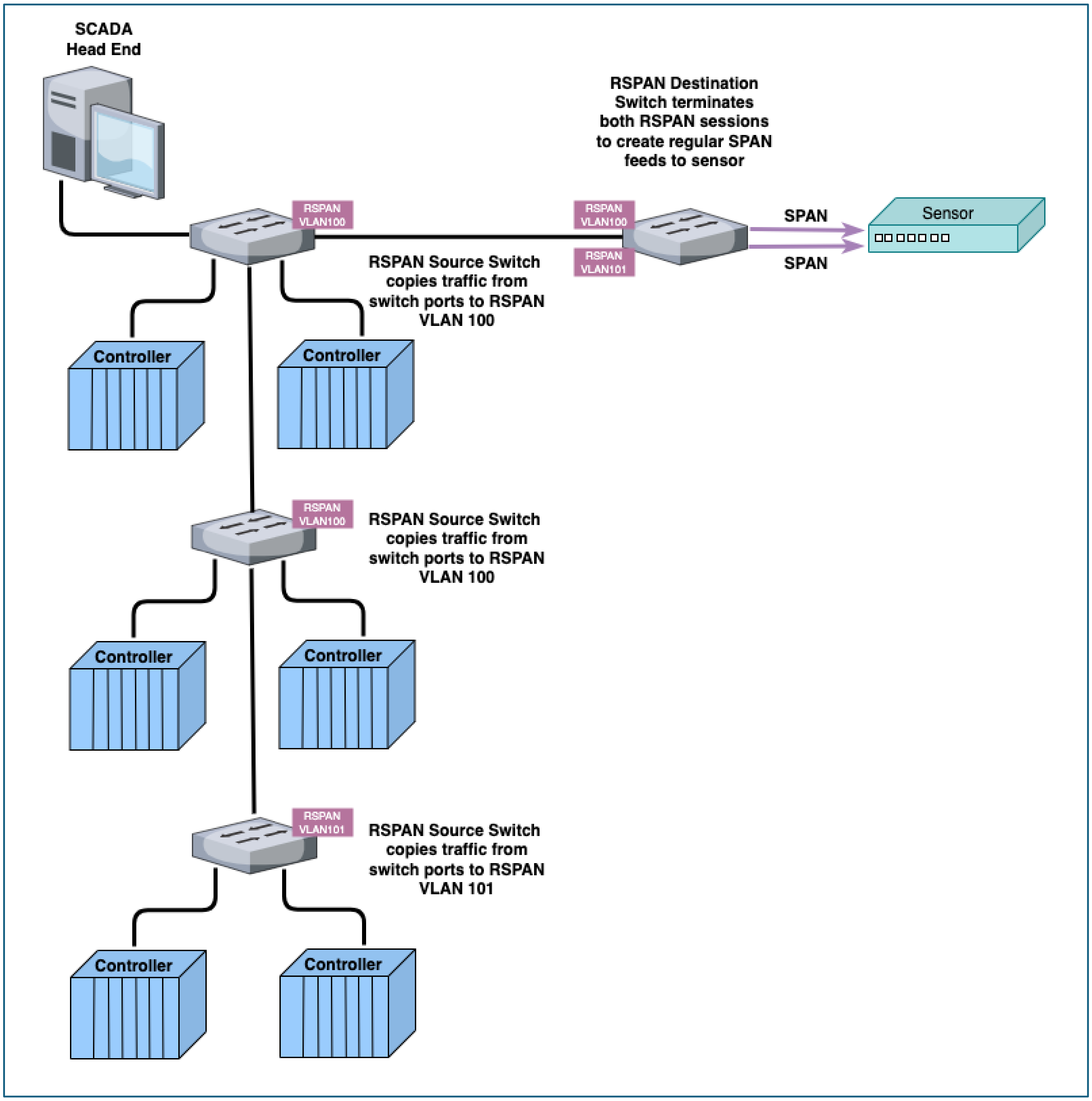

Figure 12 - Remote SPAN for Remote Traffic Capture over Layer 2 Network

ERSPAN

Like RSPAN, ERSPAN (Encapsulated Remote SPAN) also facilitate collection of traffic from remote switches to ICS/OT cyber security tooling sensors. However, ERSPAN sends traffic of interest from source switches to destination switches at Layer 3 using point-to-point Generic Routing Protocol GRE) tunnels. Providing suitable Internet Protocol (IP) network routes exist, there is no real limitation on the distance that can exist between source and destination switches, including between sites. Considerations for their use include:

- ERSPAN does not use VLANs for carrying captured traffic and is not subject to VLAN flooding.
- ERSPAN preserve VLAN IDs.
- ERSPAN sessions can traverse layer-3 devices such as firewalls and routers (policies will need to allow GRE tunnelling)
- ERSPAN can be used with VMWare Distributed Switches (dvSwitches).

ERSPAN, where supported, should be the first choice for collecting remote switch traffic on site however, support for ERSPAN is generally limited to more capable, high-end switches.

Some ICS/OT cyber security tooling sensors can act as an ERSPAN destination, obviating the need for an ERSPAN destination switch.

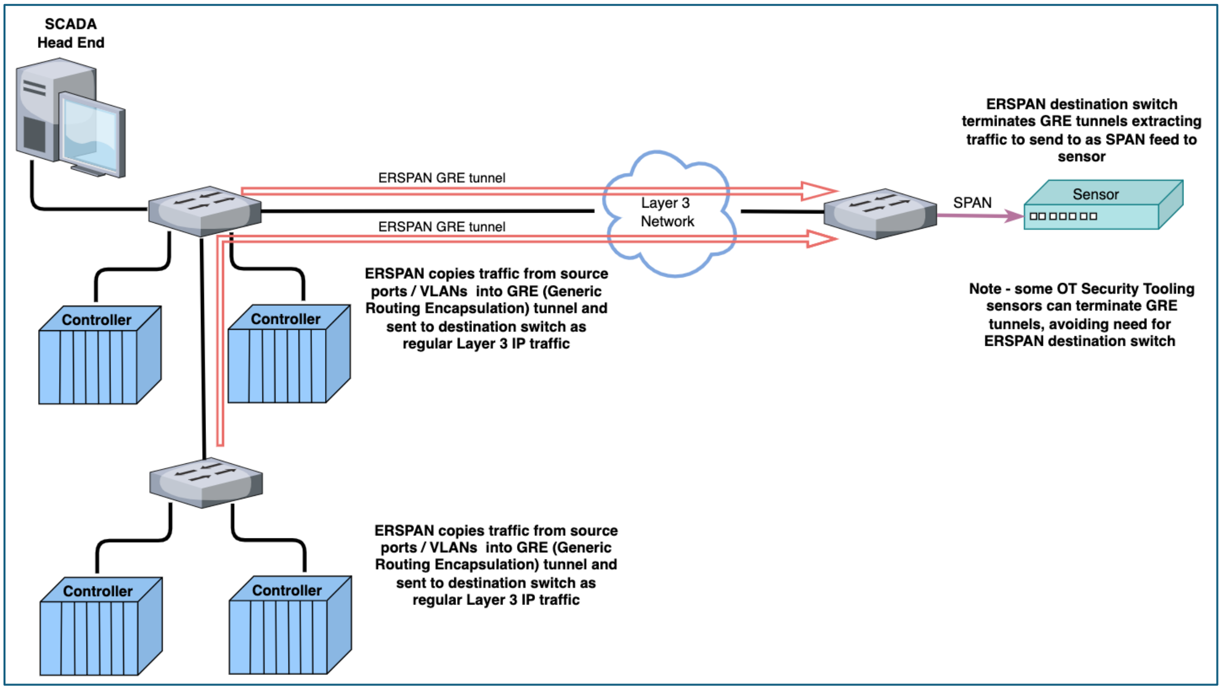
SCADA Head End
ERSPAN GRE tunnel
ERSPAN GRE tunnel
Layer 3 Network
ERSPAN destination switch terminates GRE tunnels extracting traffic to send to as SPAN feed to sensor
SPAN
Sensor
ERSPAN copies traffic from source ports / VLANs into GRE (Generic Routing Encapsulation) tunnel and sent to destination switch as regular Layer 3 IP traffic
Note - some OT Security Tooling sensors can terminate GRE tunnels, avoiding need for ERSPAN destination switch
Controller
Controller
Controller
Controller
ERSPAN copies traffic from source ports / VLANs into GRE (Generic Routing Encapsulation) tunnel and sent to destination switch as regular Layer 3 IP traffic

Figure 13 - ERSPAN for Remote Traffic Capture over Layer 3 Network

Encapsulating Devices

Some ICS/OT cyber security tooling solutions support encapsulating devices that effectively bundle SPAN/Port mirror traffic into IP based communications, providing similar benefits to ERSPAN, even where ERSPAN is unsupported by existing switch infrastructure.

Additionally, encapsulating devices can perform deduplication and compression of the aggregated traffic, thereby minimizing the network bandwidth requirements.

Packet brokers from specialized third-party vendors can also be utilised to direct switch SPAN/Port mirror traffic to ICS/OT cyber security Tooling, frequently featuring similar deduplication and compression functionalities. Packet Brokers can additionally distribute captured traffic between multiple monitoring platforms.

Moreover, encapsulating devices from ICS/OT cyber security tooling vendors may also provide support for overlapping IP addresses by integrating the IP addresses of the encapsulating devices IP with those of each monitored device. Overlapping IP addresses are relatively common within manufacturing environments, where manufacturing cells or lines operates with the same IP address range.

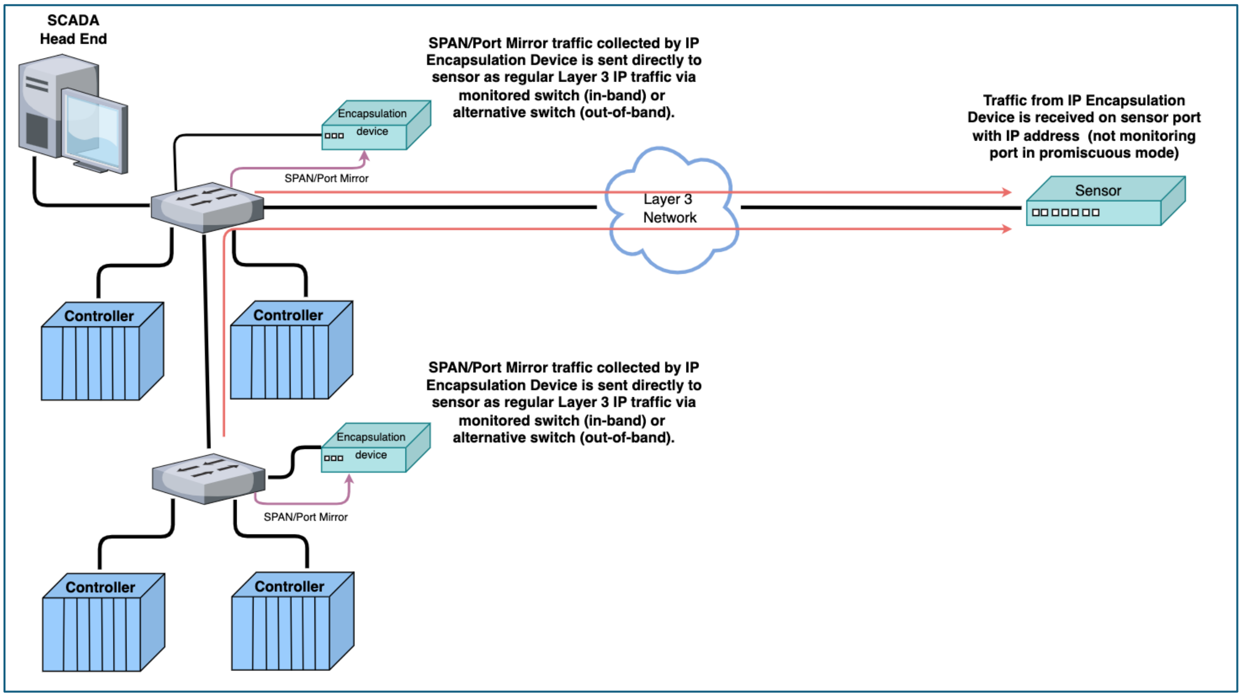
SCADA
Head End
SPAN/Port Mirror traffic collected by IP Encapsulation Device is sent directly to sensor as regular Layer 3 IP traffic via monitored switch (in-band) or alternative switch (out-of-band).
Encapsulation device
SPAN/Port Mirror
Traffic from IP Encapsulation Device is received on sensor port with IP address (not monitoring port in promiscuous mode)
Layer 3 Network
Sensor
Controller
Controller
SPAN/Port Mirror traffic collected by IP Encapsulation Device is sent directly to sensor as regular Layer 3 IP traffic via monitored switch (in-band) or alternative switch (out-of-band).
Encapsulation device
SPAN/Port Mirror
Controller
Controller

Figure 14 - Encapsulating Device for Remote Traffic Capture over Layer 3 Network

CAF Indicators of Good Practice Summary

This case study discusses measures that contribute to the following CAF Indicators of Good Practice:

- A2.a Risk Management - Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) and communicating associated activities.
- A3.a Asset Management - Determining and understanding all systems and/or services required to maintain or support essential functions.
- B4.a Secure by Design -You design security into the network and information systems that support the operation of the essential function(s). You minimise their attack surface and ensure that the operation of the essential function(s) should not be impacted by the exploitation of any single vulnerability.

- B4.b Secure Configuration -You securely configure the network and information systems that support the operation of essential function(s).
- B4.d. Vulnerability Management - You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function(s).
- B5.b Design for Resilience -You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated.
- C1.a Monitoring Coverage -The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).

Statement of support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

This document is provided on an information basis only, and whilst ICS-COI members have exercised reasonable care in compiling the guidance, they provide no warranty as to its accuracy, completeness, or suitability for any particular purpose.

To the fullest extent permitted by law, neither the ICS-COI or its members accept any liability for any loss, damage, cost, or expense arising directly or indirectly from the use of and / or reliance on, this document. Users of this guidance are advised to exercise their own judgement and consider taking independent professional advice.

Any reference to commercial products, services, or entities by name or otherwise, does not constitute or imply endorsement, recommendation or preference by the ICS-COI. The views and opinions expressed in this document shall not be used for advertising or product endorsement purposes.

Document Details

This document is version 1.0 and was published on 23/09/2025. It will be reviewed every 18 months.