tripwire®

TRIPWIRE®
INDUSTRIAL
VISIBILITY

TRIPWIRE INDUSTRIAL VISIBILITY 4.x
ARCHITECTURAL GUIDE

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Contents

1 Introduction

1.1 About this Document

Tripwire Industrial Visibility (TIV) provides real-time visibility over assets and networks. To do this, it uses Continuous Threat Detection (CTD) technology, an agentless and passive security solution for Operational Technology (OT) networks. It provides real time visibility over assets and networks, and uses both anomaly-based and behavior-based profiling to identify operational and security threats, including network failures, malicious attacks, and operator errors.

This guide is intended for Tripwire customers to prepare their environment for a TIV installation. This guide provides a range of common installation scenarios but cannot cover every possible scenario. Tripwire will work with individual customers to determine cost effective designs for deploying the monitoring solution. Installation of software is handled by Tripwire support representatives.

1.2 Terms and Definitions

The following table summarizes terms and abbreviations used in this document.

Term	Definition
Alert	User notification that requires user interaction. A single alert is often comprised of multiple related *events* with a common cause.
Asset	Any machine, computer, or controller used at the operational level.
Baseline	The Passive Platform's collection of valid network behaviors.
CTD	Continuous Threat Detection
DPI	Deep Packet Inspection.
Event	A single network action that deviates from normal ICS operation or security standards.
ICS	Industrial Control System.
Incident	An instance of invalid network activity (network failure / malicious attack / user error and so on).
IT	Information Technology.
Operator	A person in charge of operating the ICS.
OT	Operational Technology.
Patch	A software update.
User	A person using the Platform's web interface.

2 System Overview

2.1 Functional Overview

2.1.1 The Approach

Operational Technology (OT) is changing. The machines that manage industrial production are increasingly interconnected and are gaining remote accessibility. Despite the benefits of increased connectivity, increased access opens the door to operational disruptions to production via system faults, network failures, operator errors, and malicious attacks.

IT solutions applicable to the threat of increased access are not applicable to OT networks for several reasons. One of which is the fact that OT assets have the requirement of constant operation. IT solutions require upgrades, restarts, and replacements, which are too disruptive for OT and therefore cannot be implemented.

Additionally, IT assets communicate over IP-based protocols, while OT assets communicate over a wide range of IP-based, fieldbus and serial protocols. Furthermore, the IP-based protocols used in the OT environment are often proprietary in nature, making typical IT solutions irrelevant to OT networks.

Tripwire Industrial Visibility (TIV) application monitors an ICS network by reading all communication and alerting users of possible operational and security incidents.

By passively examining network communication, the TIV software constructs a comprehensive set of valid network behaviors (a "baseline") and differentiates between valid communication and operational events / security threats that may disrupt availability. By leveraging Deep Packet Inspection (DPI), the software identifies the specific assets on the network, the lines of asset communication, communication timing, protocols between particular assets, the type of commands and registers used, and even the values of valid responses.

This OT anomaly detection is more stringent than IT anomaly detection due to the machine-focused nature of operation. The majority of OT processes involve identical, repetitive communication between machines, so contextual anomalies can be detected immediately as possible threats. IT involves activity between humans and machines, which is inconstant and not repetitive, so anomaly detection does not work as reliably.

A single threat to network operation often includes many deviation events from the normal baseline, and may potentially include security attack events as well. The Platform's algorithm closely inspects and analyzes every network communication, collecting all events and event relationships to identify a possible threat to network availability. The algorithm condenses all related events into a single alert that notifies the user of a possible threat to availability (which could be an operational anomaly or a security attack). Triggering one alert per threat,

rather than one alert per event, avoids alert-overload and makes working with alerts manageable. The user can then assign, address, and process the threat alert.

The baseline is dynamic, allowing users the option to change what is acceptable as the ICS evolves over time.

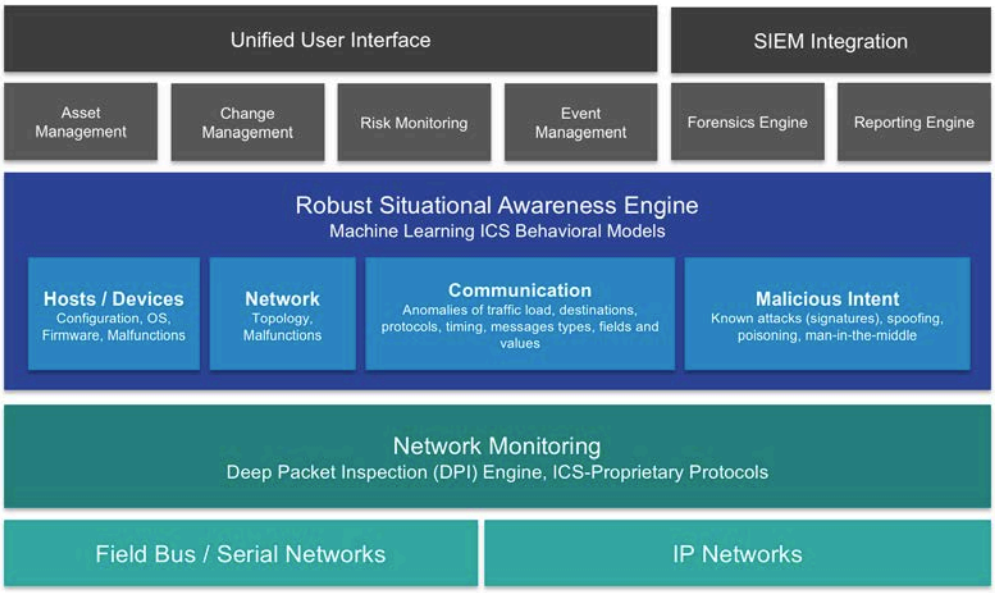

Figure 1: Application System Flow

The input to TIV is a copy of all network communication, taken passively by connecting to the SPAN port (or "mirror port") on a network or, in the case of segmented networks, from IP and fieldbus sensors. In this manner, the software can monitor the entire network without disrupting network operations or undermining the availability of the underlying industrial process.

TIV's interface is a web application that can be reached from a browser provided access rights. From this interface, users can access and inspect all assets and network architecture, process and examine notifications of potential threats, and create reports for further analysis.

All users are additionally categorized into specific groups, used to assign alerts for clear workflow management, increasing company production.

2.2 System Architecture

2.2.1 Architecture Overview

The application performs DPI on all network activity passively using port mirror, SPAN, RSPAN, or ERSPAN configured on a managed switch or network hardware TAPs which send data to the Site installation (located at site) for analysis. The Site installation sends only metadata to the EMC component for aggregation and consolidation.

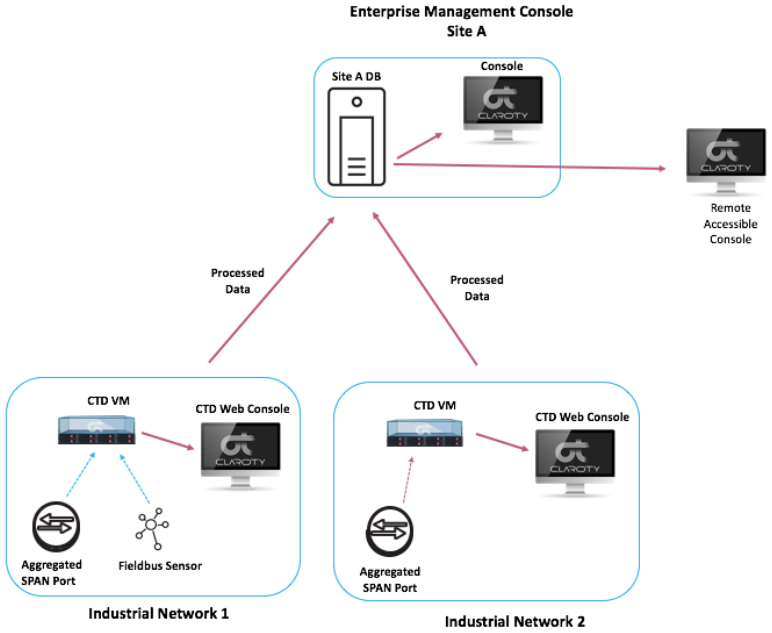

Figure 2: Site/EMC Architecture

In large distributed implementations, that required installations over different regions, a distributed EMCs architecture can be used

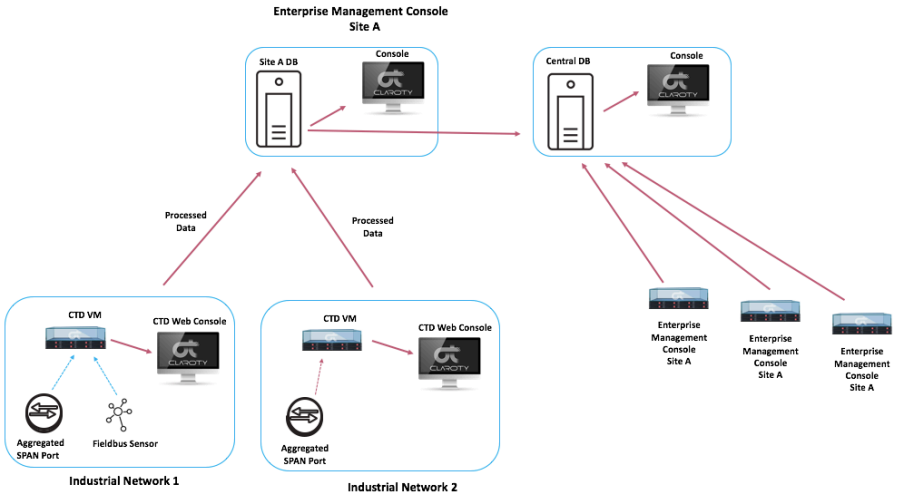

Figure 3: Distributed EMCs Architecture

2.2.2 Site Installation

The software web interface and all site alerts are generated from the Site installation, as the local processor of network activity. The component that is installed in the Site is called the TIV Server. If the solution is being installed across several sites, a Site installation at each site presents a local network monitoring web interface, and sends metadata (asset list, processed data, statistics, and alerts) to the EMC.

2.2.3 Enterprise Management Console (EMC) Installation

An EMC installation is only necessary if the OT network spans several sites. The EMC installation will typically be installed into a Network Operations Center (NOC), Security Operations Center (SOC), or corporate data center. This installation is named the EMC component, displaying information aggregated from all other sites on its web interface.

The EMC web interface displays a network diagram and alerts for each site. Site statistics, as well as overall statistics, are displayed on tabs representing site locations on the EMC dashboard.

2.2.4 Distributed EMCs Installation

The platform is designed to scale based on a Site to EMC architecture that allows the software to aggregate information to a central point. For very distributed sites, over different regions and geography a Distributed EMC architecture is used. With this architecture you can configure a Site installation to send data to multiple EMC components, each can be placed in different locations. Thus, you

can have a Site installation that is sending information to a regional EMC and in addition to a central EMC located in the headquarter which aggregate the information from all the various Sites.

When considering a Distributed EMC architecture, factors such as the number of sites and geographical distance are taken into consideration.

2.2.5 Sensors

2.2.5.1 Single distributed architecture

Sensors should be used when there is a single site, but the network is distributed geographically over different location, yet it constructs one site with one network. In order to TAP such network there is a need in placing sensors in strategic locations on the network.

2.2.5.2 IP Networks without SPAN

If network communication cannot be relayed through a SPAN port due to hardware limitations it may be necessary to place hardware TAPs in strategic locations on the network. This should be done only after other options such as remote SPAN or ERSPAN have been explored.

3 Hardware Specifications

3.1 Overview

The general hardware requirements are listed in the following sections. Because not all networks are the same, it's important to point out the hardware requirements below are Tripwire recommendation based on tests and experience in the field. The dynamic nature of ICS networks should be taken into account when determining hardware requirements. Factors such as the amount of traffic on the network (represented as Expected Traffic), the number of assets (represented as #SCADA assets) and assets that produce heavy traffic (represented as #DCS Assets) can help to determine the minimum hardware requirements.

The software is designed to operate in a virtual or physical environment. The nature of virtual environments is share hardware resources. The specs that are provided in this document make the assumption that resources for the application are available.

The recommended hard drive sizing, described in the sections below, is tuned for the average deployment for storing the data for 1 year. If it's required to store the data for longer period, a bigger hard drive size should be used

3.2 EMC

Information such as Assets, Alerts, Baselines and some other metadata from all connected TIV Servers are stored in the EMC (by default PCAPs are not stored in the EMC).

The minimum specifications for the EMC are:

	Small Deployment	Mid-range deployment	Large Deployment
#TIV Server	<10	<25	<120
Processor	6 cores	12 cores	24 (2x12) cores
RAM	16Gb	32Gb	64Gb
Hard Drive	80Gb SSD in RAID (+20 GB per site)		
Network Cards	At least one network card for mgmt. and one network card for connected TIV Servers.		
OS	ClarotyOS		
Accessing the web portal	The web portal has been optimized for use with the Google Chrome browser latest version from the past 6 months		

3.3 TIV Server

The minimum specifications for the TIV Server are:

	Small Deployment	Mid-range deployment	Large Deployment	Very large deployment
# Assets*	<300	300-1500	1500-5000	5000-12000
Expected Traffic	100Mbps	200Mbps	500Mbps	1Gbps
Processor	6 cores	12 cores	16 (2x8) cores	24 (2x12) cores
RAM	16Gb	32Gb	32Gb	64Gb
Hard Drive	80Gb RAID or SSD	240Gb RAID or SSD	240Gb RAID or SSD	480Gb+ RAID or SSD
Network Cards	At least one network card for mgmt. and one network card for connected TIV Servers.			
OS	ClarotyOS			
Accessing the web portal	The web portal has been optimized for use with the Google Chrome browser latest version from the past 6 months			

For complex and intensive networks a multi-layers architecture of TIV Sensors and TIV Server is recommended.

3.4 TIV Sensor

The minimum specifications for the TIV Sensor are:

	Small Deployment	Mid-range deployment
Expected Traffic	40Mbps	200Mbps
Processor	2 cores	6 cores
RAM	4Gb	16Gb
Hard Drive	40Gb	40Gb
Network Cards	At least one network card for mgmt. and one network card for connected TIV Servers.	
OS	ClarotyOS	

*** The sensor requires a bandwidth of ~1 Megabit between the Sensor box and TIV.

4 Network Requirements

4.1 Overview

General network requirements are listed in the following sections. Because not all networks are the same, its important to point out these requirements are a generalization. Factors such as the amount of traffic on the network, network redundancy, environmental conditions of the site, and physical constraints of the site must be taken into account when determining network requirements.

4.2 Obtaining Network Traffic

4.2.1 IP Networks

4.2.1.1 Switched Networks – Out-of-Band

The most common scenario for monitoring data on the ICS network is to connect to the SPAN port (or "mirror port") on existing network switches. The input to the application is a copy of all network communication, taken passively by connecting to the SPAN port (or "mirror port") on a network switch. In this manner, the Site installation can monitor the entire network without disrupting network operations or undermining the availability of the underlying industrial process. SPAN ports are the preferred setup for monitoring the network since these ports only transmit data and do not require the monitoring solution to become part of the ICS network. This out-of-band traffic is then connected to the Site installation. An aggregation switch should be used when the number of out-of-band network cables exceeds the number of physical ports on the Site installation.

4.2.1.2 Switched Networks – In-Band

There may be instances when deploying an out-of-band network is not desirable. For these instances, we have two recommended options.

Option 1

For networks that have available bandwidth and contain switches that are capable of RSPAN (Remote SPAN), network switches are configured with RSPAN to send data to the local Site installation. RSPAN allows traffic monitoring from source ports distributed over multiple switches, which allows traffic to be sent back to a centralize Site installation.

- A copy of all SPAN traffic is sent to the Site installation.
- No additional switch ports are needed on the network switches running RSPAN.

Option 2

For networks that have available bandwidth and contain switches that are capable of ERSPAN (Encapsulated Remote SPAN), network switches are configured with ERSPAN to send through a routed network to an IP configured on the installation. The SPAN traffic is passed through the network and is routed back to the site installation.

- A copy of all ERSPAN traffic is sent to the Site installation.
- No additional switch ports are needed on the network switches running RSPAN.
- An IP is configured on the Site installation.

In cases of high bandwidth utilization, Option 2 should be used with ACLs that filter out unnecessary traffic to help reduce bandwidth usage.

4.2.1.3 Switches Incapable of SPAN

When a switch doesn't support SPAN port (or "mirror port"), the preferred method for resolving the issue is to replace the switch with a managed switch that supports SPAN.

If replacing the switch is not an option, hardware network TAPs (Fiber or Copper) can be used in strategic places such as switch uplinks to capture pertinent data on the ICS network.

4.2.2 Non-IP Networks

If it is determined there is a threat vector that includes non-IP based communication, sensors can be attached to the serial links to relay non-IP communication through the network to the Site installation, without disrupting the normal communication of the asset.

4.3 Deployment Examples

4.3.1 Overview

The following sections provide typical deployment examples in different industrial environments.

For ISA-99 Zone and Conduit analysis of the system, the out of band network cable used for the SPAN port traffic would have to be part of a conduit that connects these two zones. Since it is out of band, it will likely be a new conduit, where the security associated with the new conduit is information flow is occurring through a SPAN port, and is effectively one-way. A detailed review of network diagrams, and the sites existing Zone and Conduit analysis should always be performed when planning for the installation of the software.

4.3.2 PCN Network

Placing of the Site installation should take into consideration the existing site zones and conduits as well as which individuals will be monitoring the Site installation console. For example, with the network shown in Figure 4 below (ISA-99 Part 3, Figure 4), if the Site installation is going to be monitored by the Control Center then the Site installation should be positioned within the Control Center.

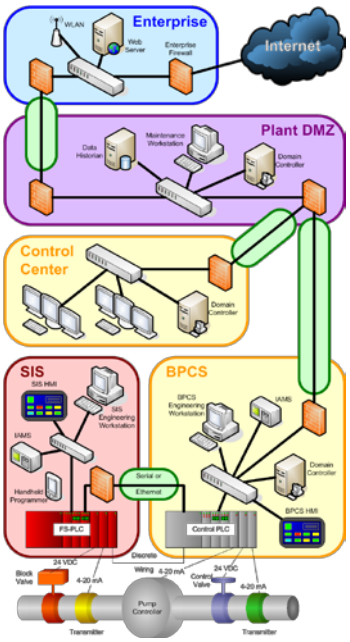

Figure 4 – High-Level Process-Industry Example Showing Zones and Conduits.

The EMC installation would then be positioned in the Plant DMZ to display information aggregated from multiple Site installations.

4.3.3 Manufacturing Network

For the example network shown in Figure 5 below (ISA-99 Part 3, Figure 5), depending on the size of the Industrial Networks, the Secure Site might reside in the Industrial/Enterprise DMZ while the EMC installation will reside in the Enterprise Infrastructure.

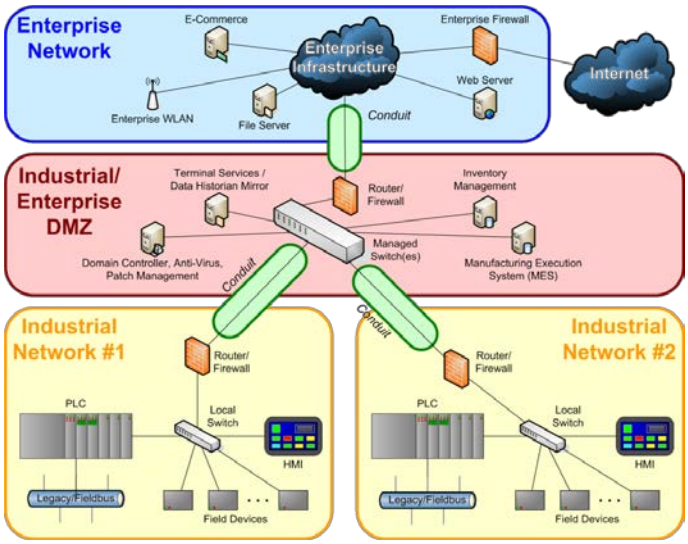

Figure 5 – High-level Manufacturing Example Showing Zones and Conduits

4.3.4 Distributed EMC Installation

From Figure 6 below, a typical installation of a Distributed EMC installation can be seen. Data is processed at various Site installations and sent to local EMC installations as well as to additional regional EMC installation. Typically, the distributed central installation resides at a corporate data center.

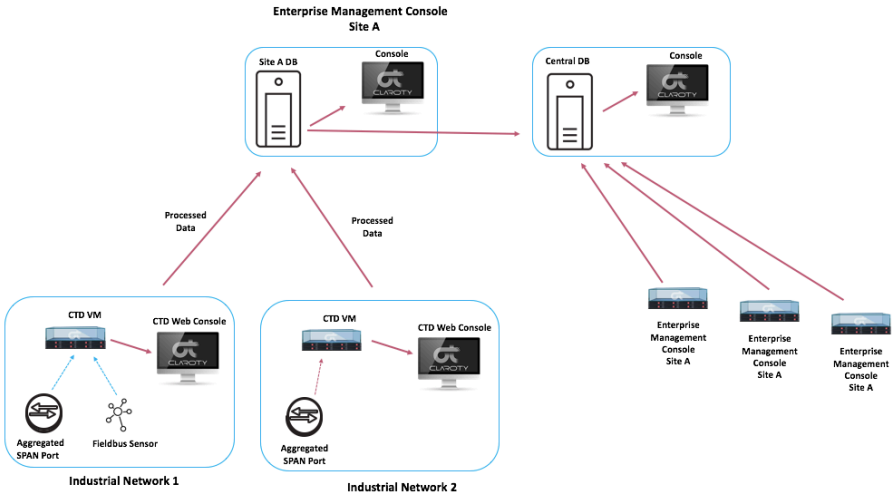

Figure 6 – High-level Distributed EMC Installation Example

4.3.5 Data Diodes

From Figure 7 below, a typical installation of the platform utilizing a data diode between a Site installation and an EMC installation can be seen. The Site installation resides on the protected side of the data diode. The Site installation sends processed data using SFTP to the EMC installation that resides on the unprotected side of the data diode.

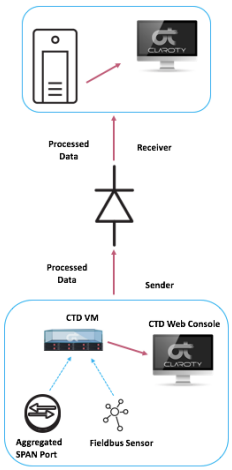

Figure 7 – High-Level Data Diode Deployment Example