Rail Communications-Based Train Control (CBTC) and Safety

Design Guide

March 2024

Cisco Systems, Inc. www.cisco.com

Contents

Rail CBTC and Safety Design Guide

Scope of Rail CBTC and Safety Solution

According to the UITP World Metro Figures 2021 report, approximately 3,300 km of new rail infrastructure was put in service between the start of 2018 and the end of 2020. During this timeframe, operational fleets worldwide increased by 28,000 vehicles to a total of 140,000 vehicles. In 2019, an average of 190 million passengers per day were taking the metro globally. Rail operators are constantly striving to keep their trains moving safely, providing superior and reliable services to the riders, and lowering their operational cost. A modern railway signaling system called "Communications-based train control (CBTC)" was introduced in the mid-1980s with the objective to achieve maximum capacity while maintaining the safety requirements.

On October 23, 2023, the Transportation Security Administration (TSA) renewed cybersecurity security directive – Enhancing Rail Cybersecurity -SD 1580/82-2022-01 to regulate passenger and freight railroad carriers through the implementation of layered cybersecurity measures, with the goal to reduce the risk that cybersecurity threats pose to critical railroad operations and infrastructures.

This guide provides comprehensive design guidance for the Cisco Rail CBTC and Safety solution. It includes an overview of this solution, solution architecture, solution components, solution design considerations, and conclusions. The objectives of this rail CBTC and safety CVD include:

- Design and validation of end-to-end architecture that meets CBTC Data communication system (DCS) specifications: latency, redundancy, high availability, performance, and network management.
- Validation of Catalyst IW9167/IW9165 performance per CBTC traffic profile
- Next Gen Converged trackside infrastructure with integration of MPLS and Segment Routing.
- Apply Industry Automation (IA) security CVD to support vital and non-vital application on common DCS and MSN (multi-service network) architecture.
- Introduction of Catalyst IR8340, IR1835, and IR1101 multiservice router into rail infrastructure for connectivity to various trackside and station devices
- Validation of rail safety related use cases: Rail safety with axle counter integration and enhance level crossing safety with vehicle and people detection.

The intended audience for this document is Cisco account teams, Cisco CX teams, A&E consultants, rolling stock manufacturer, CBTC technology suppliers, operations, and maintenance companies.

References

This solution is based on and integrated with other Cisco solutions. The relevant documents related to this solution include:

- IoT Industrial Router Design Guide Extension to SD-WAN Small Branch Design Case Study: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/m-sd-wan-iiot-case-study.pdf.
- Industrial Automation Security Design Guide 2.0: https://www.cisco.com/c/en/us/td/docs/Technology/industrial-automation-security-design-guide.html.

- Secure Remote Access for Industrial Networks Design Guide: https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Networking/Secure-Remote-for-IA-Networks/Secure-Remote-Access-for-Industrial-Networks-design-guide.pdf?ccid=cc002176&dtid=odicdc000509.
- Segment Routing Configuration Guide for Cisco NCS 540 Series Routers: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/segment-routing/74x/b-segment-routing-cg-74x-ncs540.html.
- Cisco Cities and Communities Infrastructure – Roadways Solution: www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/Roadways/cci-dg_roadways/cci-dg_roadways.html
- Renewable Energy – Offshore Wind Farm Design Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-industry-solutions/wind-farm-design-guide.pdf
- Renewable Energy – Offshore Wind Farm Implementation Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-industry-solutions/wind-farm-implementation-guide.pdf
- Industrial Automation Network Design Guide: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG/Industrial-AutomationDG.html
- Cisco IoT Solutions Design Guides: https://www.cisco.com/go/iotcvd.

The following industrial directives, whitepapers, and publications are also referenced in this guide.

- Zoning and conduits for railways | ENISA: https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways/@@download/fullReport.
- Rail cybersecurity mitigation actions and testing: https://www.tsa.gov/sites/default/files/sd-1580_1582-2022-01a-rail-cybersecurity-mitigation-actions-and-testing.pdf
- Securing control and communications systems in rail transit environments: https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf

Customers and partners with an appropriate Cisco Account (CCO account) can access additional IoT solutions sales collaterals and technical presentations via IoT Solution hub: https://salesconnect.cisco.com/IoT/s/solutions.

Solution Overview

Benefits of CBTC

Some key benefits that CBTC brings to the rail operators include:

- **Improved safety**: With implementation of CBTC, the location of the train can be determined with a high degree of accuracy, independent of track circuits. The speed of a train can be regulated to protect trains against collision, excessive speed, and maintain the safe braking distance and train separation. With additional functions such as programmed stopping, door control, route interlocking, work zone protection, and highway grade-crossing warning, accidents and hazardous conditions can be significantly reduced.
- **Maximize capacity**: The key objective of deploying CBTC is to allow rail operators to better utilize their railway infrastructure, maximize the capacity by keeping the headway between operating trains at minimum while maintaining the safety requirements.
- **Enhanced passenger experience**: CBTC enables trains to run closer together at higher speed, meaning faster services to the riders. With increased precision of train location information, the accuracy of real-time arrival information can be improved significantly. And thanks to CBTC, riders can enjoy smoother rides because acceleration and braking are controlled by the system so passengers can expect more consistency in terms of train operation.

- **Reduced Capex and OpEx**: As CBTC technology evolves, the system becomes more compact, and the architecture gets simpler. This means less equipment at wayside that is easier to implement and maintain. Moreover, these systems allow rail operators to monitor trains and adjust the performance level of individual trains to maintain schedule. The CBTC system provides flexibility to the rail operators to respond to schedule changes and emergencies more efficiently.
- **Improved sustainability:** CBTC enables different levels of Grades of Automation (GoA) and has proven to be more energy efficient than traditional manual operation. With automatic speed regulation provided by the system, unnecessary acceleration and braking are not required, which leads to big energy saving. With reduced power consumption and less air pollution, environmental sustainability is improved.

CBTC Deployment Network Challenges

Although CBTC brings tremendous benefits to the rail operator, there are some key networking challenges the rail operator needs to consider when deploying this solution. These are discussed below.

Ultra-reliable train to wayside wireless connectivity

Successful operation of CBTC relies on a ultra-reliable bi-directional train to wayside wireless communication technologies when trains operate at high speed. This wireless technology must support high-speed train mobility, full coverage of long sections of track, seamless handoffs without data loss as a train moves along the track, tightly controlled network latency, and extremely low data packet loss.

Reliable and highly available infrastructure

The network infrastructure for CBTC operations is highly distributed among many locations, including rail cars and locomotives, maintenance vehicles, wayside, yards, terminals, and stations. A scalable and resilient network is needed to connect all the locations, sites, and operations centers throughout a rail operator's geographic region. Due to the criticality of the system, network redundancy and high availability must be taken into consideration. It needs proven end-to-end security, high reliability, and scalability to many geographically distributed locations. Managing all the network policies and assuring that they are properly implemented can be overly burdensome if done manually for each network node, so good tools for automation and provisioning, centralized network management, service assurance, analytics and assurance, service assurance, policy and security are needed.

Due to the mission critical nature of CBTC operation and regional compliance requirements, rail operators mostly deploy CBTC within a dedicated Data Communication Systems (DCS) whose sole responsibility is to deliver a highly redundance, reliable and secure network that supports CBTC operation only. With proper technologies and design in place, CBTC providers and rail operators start instrumenting converged multi-service network architecture to support both mission critical application like CBTC and other non-mission critical applications like passenger Wi-Fi, video surveillance, and ticketing etc. Network segmentation, zoning, and conduits are some of the key considerations for operating CBTC on a converged network infrastructure.

Cybersecurity

Cybersecurity attacks on rail systems can disrupt the flow of goods on freight lines, completely stop train operations, and degrade passenger services, disappointing the customers that rail operators are seeking to delight. Attacks on vital rail systems can cause shutdowns or, even worse, harm to human safety. Given the digitization of operations that rail providers must achieve to remain viable and competitive, the need for strong cybersecurity is only increasing. Experience has shown that a strategy of trying to simply "air-gap" and isolate operational networks does not prevent attacks.

A comprehensive, systematic, coordinated approach is needed, with consideration for issues such as ensuring that only authorized users and devices are connecting to the network, users and systems can access only data and services for which they are authorized, users are not connecting to malicious sites, malware is not brought into systems, and only legitimate traffic is transiting the network. Robust tools are needed to manage profiles and policies at scale and monitor that users and devices on the network comply

with those policies, and all this must be done in a way that enables a quick response to new threats and intrusions as they emerge.

Challenging environment

Equipment installed onboard trains and on the trackside must meet industry standards set out for protection against temperature variations, vibration, ingress of metallic dust and other particles, moisture, fire, electrical surges, and other challenges associated with rail operations. Equipment that doesn't meet the required specifications can result in costly system disruptions and repairs, shortened equipment lifespans, lost revenue with assets being taken out of service, lapses in passenger services, and even liability and fines. CBTC operation relies on train to wayside wireless technology, which is susceptible to signal interference and range restrictions that are caused by unpredictable and dynamic radio frequency environment.

Vertical Use Cases

As listed in Table 1, rail operators and Cisco solution partners use Connected Rail as a secure foundation on which to build their solutions to support use cases including passenger Wi-Fi, infotainment, video surveillance and analytics, operations management, maintenance, signaling, and control.

Table 1. Cisco Rail CBTC and Safety Use Cases

Use case	Type of Services	Description
Vital Application	• Communications-based train control (CBTC) • Data Communication System (DCS)	• Core network that supports data center applications for CBTC • Next gen backbone network that supports both vital and non-vital applications • Wayside network to support wired connection to various trackside assets for CBTC applications such as local ATS server, wayside zone controller, diagnostic data collector, ATS workstations • Wayside network to support wireless trackside radio connectivity for train-to-wayside wireless communication • Onboard network to support connectivity to onboard CBTC component including train-bone controllers, operator display and onboard radios
Non-vital Application	• Video surveillance • Passenger Information System	• Video surveillance at station, trackside and onboard • Passenger Information Systems for onboard and at station
Rail Safety	• Train Detection • Secondary detection for CBTC • Level crossing and traffic light preemption • Axle counter diagnostic • Trackside asset connectivity • Passenger and vehicle detection at level crossing	• Integration with Axle counter for train detection • Integration with Axle counter for CBTC interlocking • Traffic light control at level crossing • Provide network to axle counter diagnostic data collection • Provide connectivity to the trackside assets with IR8340 multiservice routers. • Detect vehicle and people at level crossing with Meraki and MV object detection analytics

Solution Architecture

CBTC Major Subsystems, Communication Flow, and Traffic Profile

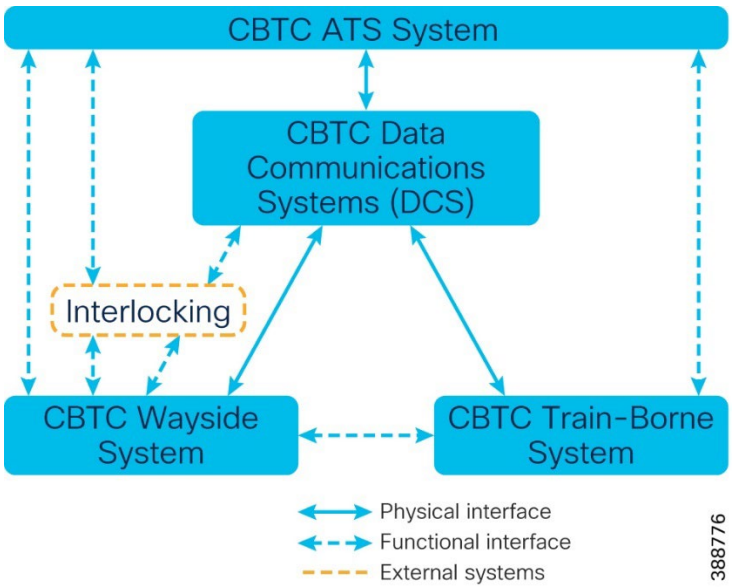
The primary function of the CBTC system is to provide high precision determination of the train location independent of track circuits, high throughput bidirectional communication from the train to the wayside, and processors on the train and wayside performing vital functions. The primary goal is to eliminate collisions and prevent speeding. The systems commonly associated with CBTC are Automatic Train Protection (ATP), Automatic Train Operation (ATO), and Automatic Train Supervision (ATS). ATP ensures that the speed of the train conforms to the permitted speed given by signaling and applies the brakes if necessary. ATO manages how automated a train can operate. This can be a minimal automation where the driver does the work of driving and operating doors while the ATO system looks for issues caused by human error. There can also be a full automation where there is no driver present and all aspects of the train operation including driving, safety detection, and door operation is run by the ATO system. The ATS system ensures that the train schedule is maintained and can change speeds or zone permissions as needed.

At a minimum, ATP can be deployed to ensure that the train operates in a safe manner and can be stopped in an emergency. Adding more subsystems will ultimately increase the overall safety, efficiency, and capacity of the train network.

Other secondary systems can be added to increase visibility for train positioning as well as provide a backup in case CBTC is unavailable. These secondary systems include track circuits or axle counters. They can be beneficial if the track network must support non-CBTC vehicles such as older trains or track maintenance vehicles.

A summary of these different systems work together is shown in the following figure.

Figure 1 *CBTC major subsystems*



The DCS interconnects all system together and enables the end-to-end communication. The train-borne system is the equipment installed on the train that communicates directly with the wayside and functionally with the systems in the Operational Control Center (OCC). Interlocking includes all the signaling devices used to prevent conflicting movements on a set of tracks.

An example communication flow is that the train constantly communicates its position and speed over the wireless signal and the ATS system determines the train is getting ahead of schedule. It then tells the driver to slow down which he performs manually. In a more automated system, the ATO will control the throttle and brake to achieve the same results. In a system with only ATP, if the speed is not reduced enough, the ATP can automatically apply the brakes to prevent an accident.

The traffic profile is typically low throughput, up to 1 or 2 Mbps per train. However, because this traffic is vital to the operation of the train, it must be sent with the highest priority value with multiple network redundancies, including duplicating each CBTC packet, to ensure there is no loss.

CBTC Overall Reference Architecture

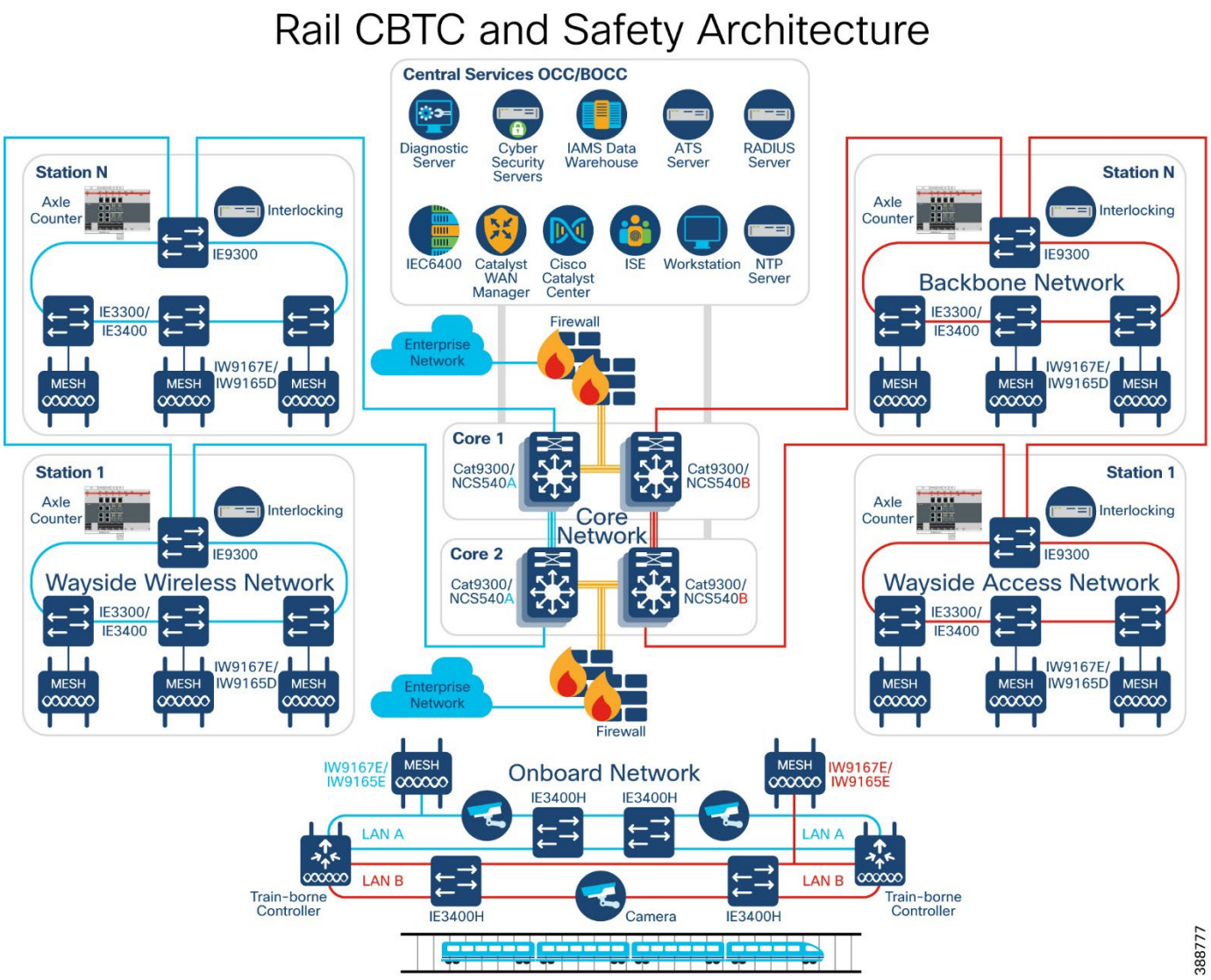
The Rail CBTC and safety solution architecture is built on the premise that vital traffic must have redundancy built-in at every level. For this reason, the Operations Center, core, distribution, wayside, and even the train-to-wayside wireless network are duplicated. Any vital traffic used for the operation and maintenance of the train must have two distinct paths in the event that a network failure causes one path to fail. Each network path has the same basic functional blocks.

- Operational Control Center (OCC): This hosts the services vital for the train operation including the central networking devices (e.g. zone controllers, NTP server, NMS), central signaling equipment, ATS, and controllers for the wayside wireless network like the IEC-6400.
- Core network: This connects the OCC to the backbone network and the enterprise network. It can be a traditional L3 enterprise network, a private MPLS network, or leased lines from a service provider.
- Backbone network: This network connects the core to the wayside access networks. It is formed between the station switches and the core switches.
- Wayside access network: This network provides connectivity to wayside devices such as Interlocking systems, axle counters, wireless access devices, and other vital safety equipment.
- Wayside wireless network: This network provides wireless connectivity from the wayside to the train.
- Onboard train network: This ethernet network connects to the CBTC systems, the onboard wireless network devices, as well as non-vital passenger systems.

Another functional block that is not duplicated is the datacenter which includes systems for NMS and other types of management. This includes Cisco Catalyst Center, Integrated Services Engine (ISE), and systems for cyber security and SD-WAN.

See the figure that follows for the end-to-end system architecture.

Figure 2 *Rail CBTC and Safety Architecture*



When discussing these architectures, a common topology is discussed, a ring. When discussing a switched ring in the context of the Rail CBTC and Safety Solution, the technology used is Resilient Ethernet Protocol (REP).

REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) for controlling network loops, handling link failures, and improving convergence time. REP controls a group of ports that are connected in a segment, ensures that the segment does not create bridging loops, and responds to link failures within the segment. REP provides a basis for constructing complex networks and supports VLAN load balancing. It is the preferred resiliency protocol for IoT applications.

A REP segment is a chain of ports that are connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. The preferred alternate port selected by REP is blocked during normal operation of the ring. If a REP segment fails, the preferred alternate port is automatically enabled by REP, which provides an alternate path for the failed segment. When the failed REP segment recovers, the recovered segment is made the preferred alternate port and blocked by REP. In this way, recovery happens with minimal convergence time.

CBTC Onboard Network

The train onboard network provides connectivity to all the train systems whether vital or non-vital and forms the backbone of all train communication. A rail certified switch must be used aboard the train that complies with the required certifications.

The switch used in this solution is the Cisco Catalyst IE3400 Heavy Duty, which is rail certified and provides up to 24 M12 ports of 10/100 Mbps (D-code) or 10/100/1000 Mbps (X-code). It is powered by the next generation IOS-XE with built-in security features and management capabilities through Cisco Catalyst Center. It also offers edge compute capabilities to run IOx applications specifically for the OT environment. Cisco Cyber Vision is supported to improve visibility into industrial assets as well as Secure Equipment Access to provide secure access to those industrial assets.

More details can be found here: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie3400-heavy-duty-series/datasheet-c78-742313.html

Figure 3 *Cisco Catalyst IE3400 Heavy Duty models*

Other onboard devices include the various controllers needed to monitor the train which is vital traffic as well as non-vital traffic such as CCTV or Passenger Information Systems. The train to ground wireless radios are also connected to the onboard network and connect the train to the wayside.

CBTC Train to Wayside Wireless

The train to wayside wireless network provides connectivity from the train systems to the wayside network and allows all systems to be centrally monitored from the OCC. The Cisco Catalyst IW9167E and IW9165E access points are rail-certified, ruggedized wireless radios installed on the wayside and train to provide high throughput connectivity with high-speed roaming and zero loss handovers. The IW9167E is IP67 rated with three 4x4 radios (2.4GHz, 5GHz, and 5/6GHz) and ports for external antennas. The 5GHz and 5/6GHz radios can be used in this context which enables flexible deployment options on the train or on the wayside.

More information can be found here: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-iw9167-series/cat-iw9167e-heavy-duty-ap-ds.html

Figure 4 *Cisco Catalyst IW9167E Heavy Duty Access Point*

The IW9165D and IW9165E are IP67 and IP30 rated respectively with two 2x2 radios (5GHz and 5/6GHz). The IW9165E has external antenna ports and is rail certified while the IW9165D has a built-in patch antenna as well as external antenna ports but is not rail certified. The IW9165E can be used on the train while taking up a smaller footprint than the IW9167E and the IW9165D can be deployed wayside provided that all certification restrictions are satisfied.

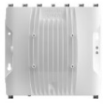
More information can be found here:
https://www.cisco.com/c/en/us/products/collateral/networking/industrial-wireless/catalyst-iw9165-series-ds.html

Figure 5 *Cisco Catalyst IW9165E Rugged Access Point*

Figure 6 *Cisco Catalyst IW9165D Heavy Duty Access Point*

The high-level differences between the different radios are shown in the figure that follows.

Figure 7 *Cisco Catalyst 6E Industrial Wireless Portfolio*

	 IW9165E	 IW9165D	 IW9167
Application	Wireless client for mobile assets	Wireless backhaul for fixed and mobile assets	Wireless backhaul for fixed and mobile assets
Radio	2 x 802.11ax radios (5GHz, 5/6GHz)	2 x 802.11ax radios (5GHz, 5/6GHz)	3 x 802.11ax radios (2.4GHz, 5GHz, 5/6GHz)
Antenna	4 x RP-SMA	Built-in 15dBi directional plus 2 x N-Type (f)	8 x N-Type (f)
Modulation	2x2 MIMO	2x2 MIMO	4x4 MIMO
Wireless Mode	WGB or URWB	URWB	WiFi, WGB, URWB
Ethernet	1 x 2.5Gbps + 1 x 1Gbps RJ45 Optional M12 adapter	1 x 2.5Gbps + 1 x 1Gbps RJ45 Optional M12 adapters	1 x 5Gbps RJ45 + 1 x SFP+ Optional M12 adapters
Expendability	BLE, GNSS, GPIO	BLE, GNSS	BLE, GNSS
Certifications	IP30, EN50155 -40C to +70C	IP67 -50C to +75C	IP67, EN50155 -50C to +75C

388782

For large L3 deployments, the IEC6400 is deployed as a Global Gateway to enable seamless roaming between separate mesh networks. It is installed at the OCC and BOCC as a dedicated appliance in conditioned space. All IW916x access points can function as the Global Gateway for L3 deployments, but the IEC6400 is the recommended platform because of the high throughput and power protection due to dual redundant power supplies. The IEC6400 can also be deployed in large L2 deployments as a Mesh End if the aggregate throughput will exceed 2Gbps.

More details can be found here: https://www.cisco.com/c/en/us/products/collateral/networking/industrial-wireless/iec6400-edge-compute-appliance/iec6400-edge-compute-appliance-ds.html

Figure 8 *Cisco IEC6400 Edge Compute Appliance*

CBTC Wayside Wired Network

The wayside wired network is deployed near the track and provides connectivity to wayside devices such as Interlocking systems, axle counters, video cameras, and other systems needed to monitor and maintain the safety of the train. The switches are typically installed in wayside bungalows which may or may not be airconditioned. The switches are then backhauled directly to a station backbone switch or through a ring connecting the other wayside switches. The recommended switch for this network is the Cisco Catalyst IE3400 or IE3300 Rugged Series switch.

CBTC Backbone Network

The backbone network connects the wayside network to the core network and is logically divided up by stations. Each station is a node on the backbone network and is a L3 demarcation for the wayside network. If the backbone switch can satisfy the wayside connectivity requirements, then the wayside network can be collapsed into the backbone switch. If the space is conditioned, the Cisco Catalyst 9300 Series switch can be positioned while in unconditioned space, the Cisco Catalyst IE9300 Rugged Series switch should be positioned.

Like the wayside wired network, the backbone switches are connected to the core switches directly or as part of a ring with the other backbone switches.

CBTC Core Network

The core network connects the backbone network, comprised of the stations, to the OCC and Backup OCC (BOCC). Because this connects all the stations together and to the operations center, it must be highly resilient and high performance. In this solution, two different types of cores are described, an L3 core which may be used in an enterprise setting, or an MPLS core which is typical in a service provider context. The Cisco Catalyst 9300 Series switch is used for the L3 core while the Cisco NCS 540 series switch is used for the MPLS core.

The core network also connects to the datacenter which contains services not strictly related to train operation such as NMS and cyber security. These services, while not considered vital to the train operation, are vital to a well-managed, secure, and scalable network architecture.

Solution Components

This section describes the components of a CBTC and safety network. Several device models can be used at each layer of the network. The device models that are suitable for each role in the network and the corresponding CVD software versions are described in Solution Hardware and Software Compatibility. The device model should be chosen based on specific deployment requirements such as network size, cabling and power options, and access requirements. Table 2 describes device models that are used in this solution.

Table 2 *Components and Device Models in Rail CBTC and Safety Architecture*

Component Role	Component	Description
Wayside access switch	Cisco Catalyst Industrial Ethernet (IE) 3400 Series Switch and/or Cisco Catalyst Industrial Ethernet (IE) 3300 Series Switch	1Gig REP access ring – IE3400 10Gig REP access ring – IE3300
Station Backbone switch	Cisco Catalyst 9300 Series switch or Cisco Catalyst IE9300 Series switch	Connects to wayside REP access ring and core network.
Core network switch – L3	Cisco Catalyst 9300 Series switch	Connects to backbone switch and OCC
Core network switch – MPLS	Cisco NCS540	Connects to backbone switch and OCC
Firewall	Firepower 2100 or 4100 Series	Network firewall.
OT network sensor	Cisco Cyber Vision network sensor on IE3400 Series Switches	CV network sensors on all IE switches in the ring and FAN.
OT security dashboard	Cisco Cyber Vision Center global and local virtual appliances	CVC deployed globally and locally in control center and OSS network infrastructures, respectively.
Ultra Reliable Wireless Backhaul (URWB) gateway	IEC6400 Edge Compute Appliance	URWB wireless network mesh end.
Network management	Cisco Catalyst Center	Network management application in datacenter.
Authentication, authorization, and accounting (AAA)	Cisco ISE	AAA and network policy administration.
IT and OT security management	Cisco Secure Network Analytics (Stealthwatch) Manager and Flow Collector Virtual Edition	Network flow analytics and security dashboard in control center.
Train to wayside wireless (high performance)	IW9167E	URWB Mesh radio on train and wayside
Train to wayside wireless (lower cost)	IW9165E/D (IW9165D on wayside only)	URWB Mesh radio on train and wayside
Onboard network	Cisco Catalyst IE3400 Heavy Duty	Ruggedized network access switch

Solution Hardware and Software Compatibility

Table 3 lists the Cisco products and software versions that are validated in this CVD.

Table 3 *Cisco Hardware and Software Versions Validated in this CVD*

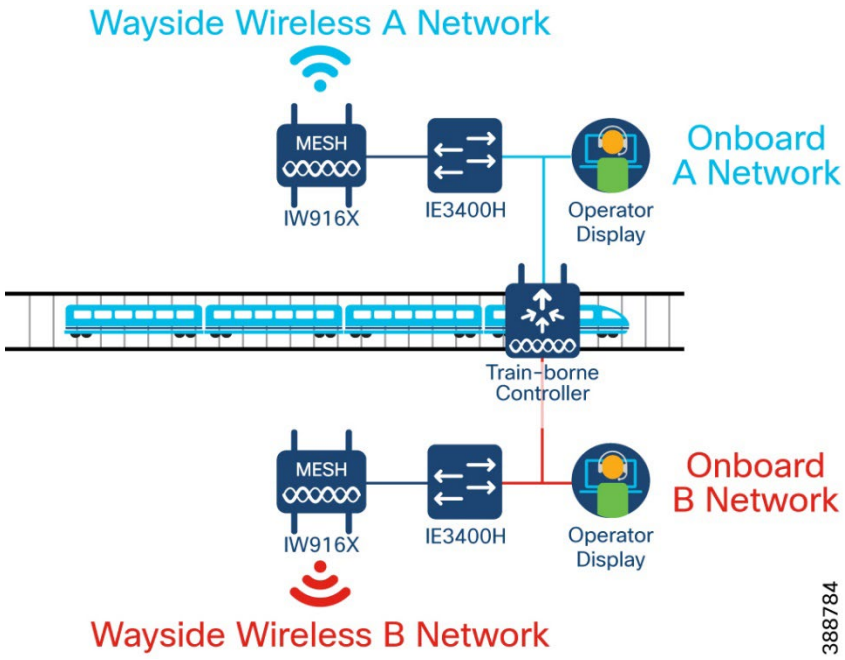
Component Role	Hardware Model	Version
Wayside network	IE3400-8P2S	17.13.1
Core network – L3	C9300-24UX	17.13.1
Core network – MPLS	N540X-6Z18G-SYS-A	7.9.2
Station backbone switch	IE-9320-22S2C4X	17.13.1
Network management application	Cisco DNA Center Appliance DN2-HW-APL	2.3.7.0
Authentication, authorization, and accounting (AAA) server	Cisco ISE Virtual Appliance	3.2
URWB mesh point	IW9167E, IW9165E, IW9165D	17.13.1
URWB mesh gateway	IEC6400	1.0
URWB IW Monitor	IW Monitor VM	v2.0

Design Considerations

Onboard Network Design

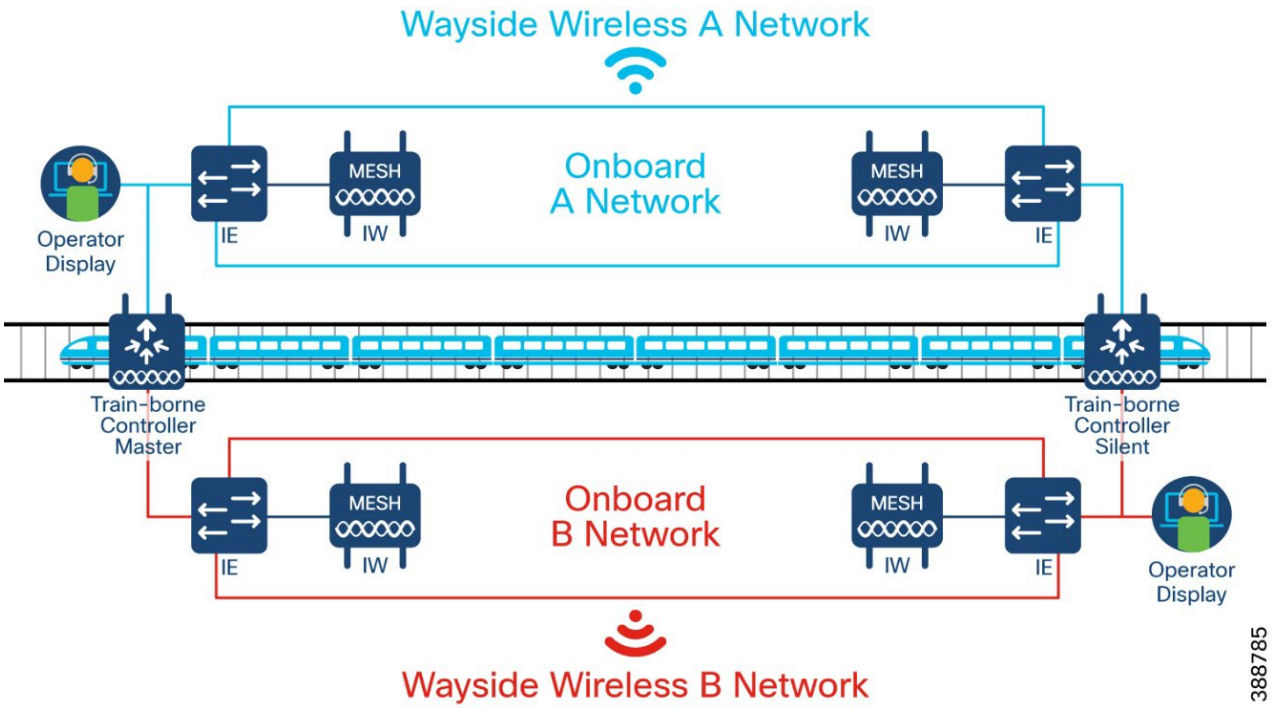
In the onboard network, a rail certified switch provides connectivity to all the train devices. In this solution, the Cisco Catalyst IE3400 Heavy Duty is used due to its EN50155 certification and IP67 construction. Because all vital systems must have fully independent network paths, the switching network is also duplicated throughout the train consist. In the most basic case, all train systems could be confined to a single car connected to a single switch for each LAN path. The example that follows shows a single switch for each path with the train controller and wireless train to wayside radio.

Figure 9 *Onboard Network Single Switch*



If the switched network must extend beyond one car to multiple cars, each car must have connectivity to the next within the coupling or some other means. Connecting the first switch to the last switch in the path creates a ring and is the most resilient design in the event of a failure. If redundant train control systems are used within the consist, this type of network design provides the most resiliency in the event of a system failure. It also enables future services to be offered in different parts of the train such as CCTV or passenger infotainment. An example of this design follows.

Figure 10 *Onboard Network Multiple Switches*



Train to Wayside Wireless Design

The train to wayside wireless network is built using the Cisco IW916x series of access points using Cisco Ultra-Reliable Wireless Backhaul (URWB) Fluidity technology. More details about this technology can be read here, https://www.cisco.com/c/dam/en/us/td/docs/wireless/ultra-reliable-wireless-backhaul/device-software/cisco-urwb-fluidity-specs-usermanual.pdf

The IW916x access point can be configured in different Cisco URWB modes depending on which function it serves. The functions are described below. It should be noted that when describing MPLS in the context of Fluidity, it is used internally for the Cisco URWB functionality and not related to MPLS configured in the core network.

Mesh End: In the Fluidity network, the Mesh End is the demarcation point between the wireless mesh network and the wired switched network. Packets destined for the wired network will have the MPLS label popped off while packets coming into the wireless mesh network will have the MPLS label imposed. In terms of MPLS, the Mesh End is a Label Edge Router (LER).

Mesh Point: The Mesh Point swaps MPLS labels on the received traffic when it is destined for another device in the mesh network. They serve as the primary RF path between the train and the wayside. The vehicle radio is a special kind of Mesh Point that imposes an MPLS label on the incoming data from the train network and also removes the label before putting it onto the onboard network.

A wireless mesh comprises a Mesh End and one or more Mesh Points. The wireless mesh is kept separate from other wireless meshes by having a unique passphrase on the Mesh End and associated Mesh Points.

Global Gateway: A Global Gateway is a special Mesh End for a L3 mesh network. A wireless mesh network cannot span a L3 domain and mesh networks in different L3 domains do not support seamless roaming. The Global Gateway allows different mesh networks with the same passphrase to support seamless roaming between them. Each Mesh End in the mesh network forms an L2TP tunnel to the Global Gateway which allows this seamless communication. In the Rail CBTC and Safety solution, the Global Gateway role is performed by the IEC6400 appliance.

RF Design

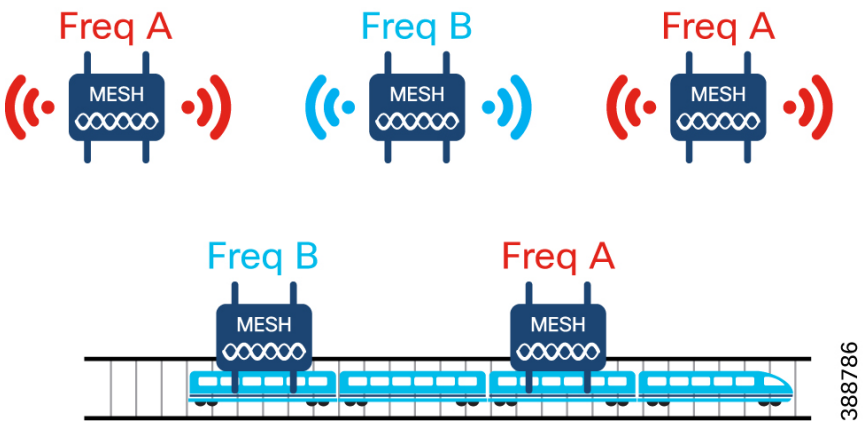
The RF design will largely be dictated by the traffic requirements and site survey of the train path. High throughput requires high signal strength and less RF noise. If the system only needs to support CBTC or other low bandwidth services, the wireless network will have less stringent requirements.

Because the RF network is duplicated to serve both LAN paths off the train, care must be taken to lay out the frequencies to minimize interference. Wayside radio placement will also affect the wireless design depending on where they can be installed. The track may have installation options on both sides of the track or just one. The IW9167E and IW9165E access points both have two radios inside that can be used to support the mesh network. Additionally, two access points can be configured on the same switched onboard train network acting as a single unit to increase the RF coverage and improve the overall signal quality from train to wayside.

Regardless of the deployment chosen, the access points on separate LAN paths must use different frequencies to prevent interference between the two paths. The access point antennas must also be installed far enough away from the other access point antennas to also prevent interference.

In the example that follows, the poles are shown on one side of the track. The radios for each LAN path are alternated and given a different frequency.

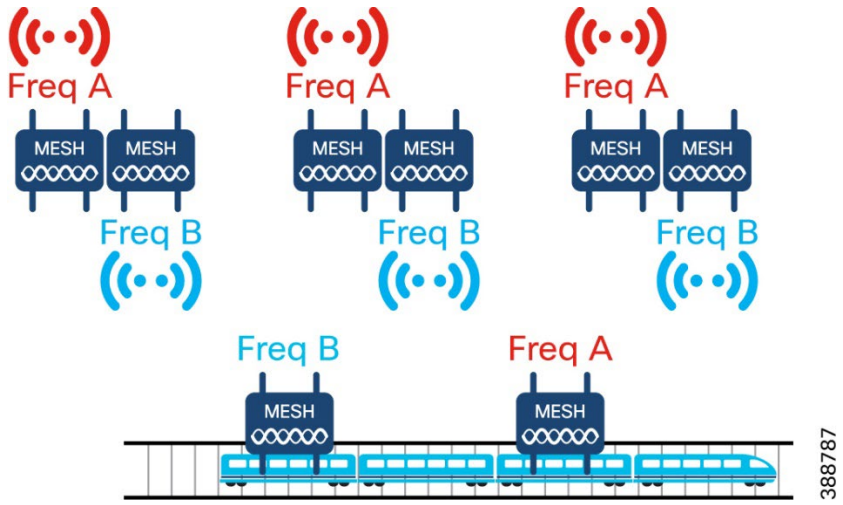
Figure 11 *Poles single side, single radio*



In this design, the wayside access points must have antennas pointed up and down the track to provide full coverage. The train radio antennas must also be pointed up and down the track to ensure full coverage while also positioned away from the other radio to minimize interference. Note that depending on the distance between poles, the signal at the halfway point between radios of the same LAN path could be too low to support the highest throughput rates.

In the example that follows, access points for both LAN paths are installed on every pole.

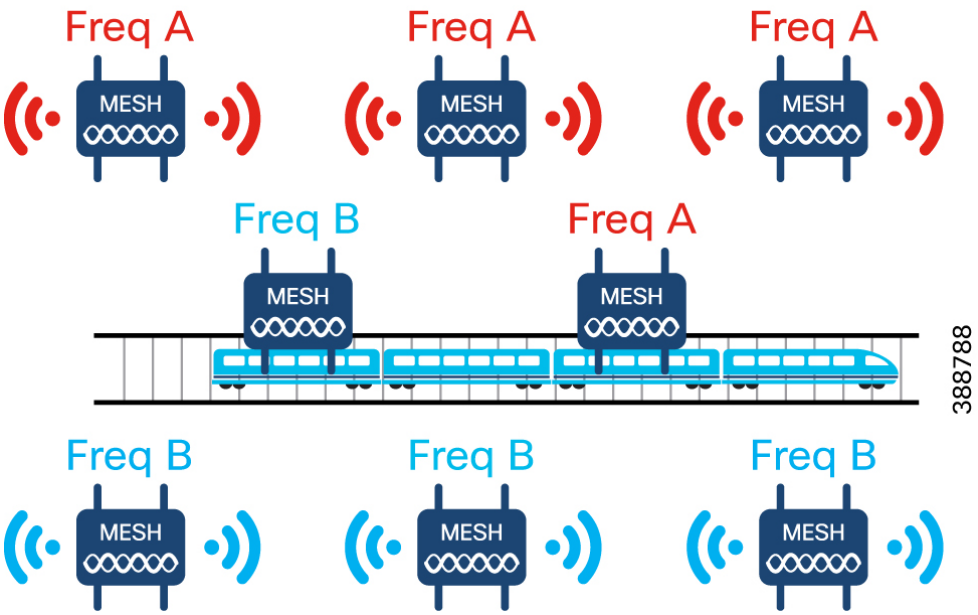
Figure 12 *Poles single side, dual radios*



With antennas pointing up and down the track, the RF coverage is denser at the risk of interference between the collocated access points. The antennas must be installed at least 6ft apart to minimize this interference. The train access point antennas must also be installed to account for this difference in height.

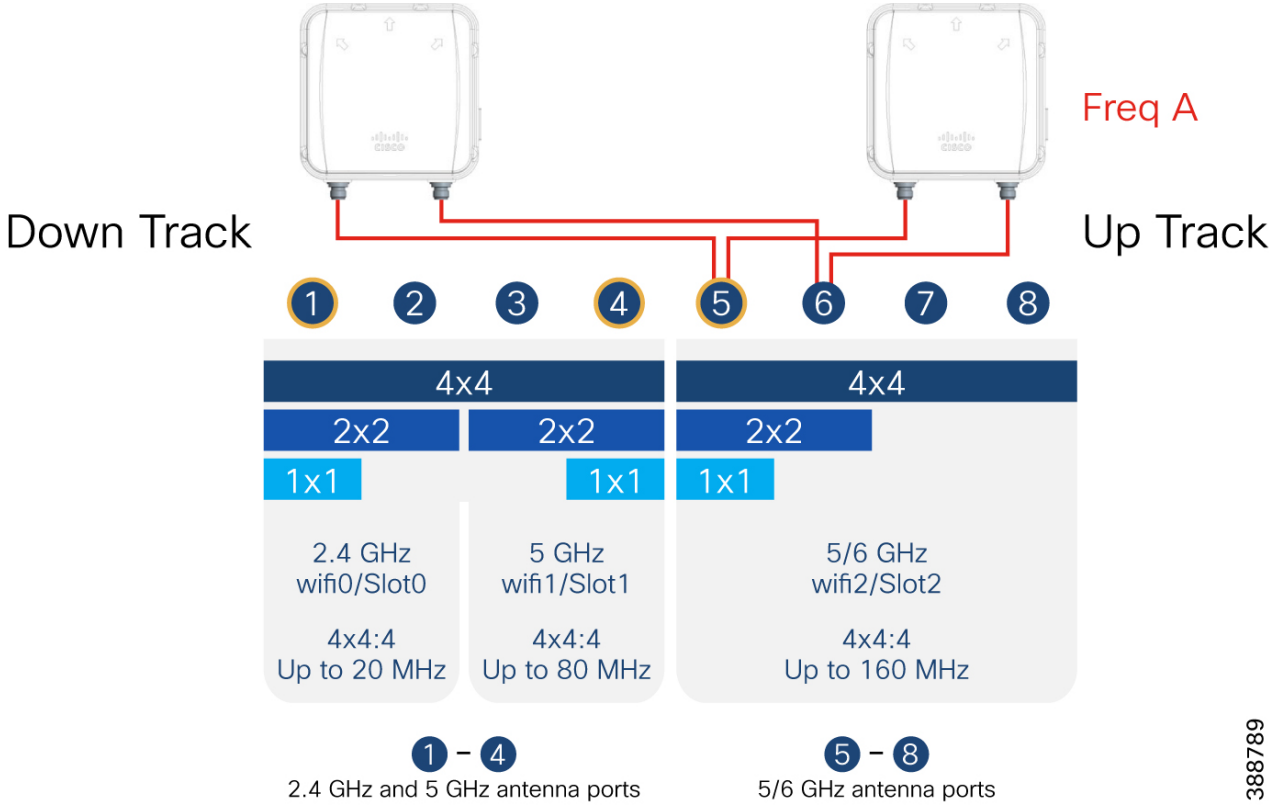
If poles are deployed on both sides of the track, each LAN path could be dedicated to one side of the track which could increase density as well as minimize interference. In this scenario, antennas would be positioned to face up track and down track. This requires the use of splitters to ensure the antenna ports see all the signals from all the antennas. In cases where splitters cannot be used due to compliance, another wayside radio must be installed with antennas facing the other direction. In the case of a single radio used onboard the train, the RF signal at the pole will be weaker as the train passes by. This can be mitigated with dual radios which is explained in the High Availability Design section. The single radio deployment is shown below.

Figure 13 *Poles on both sides of track*



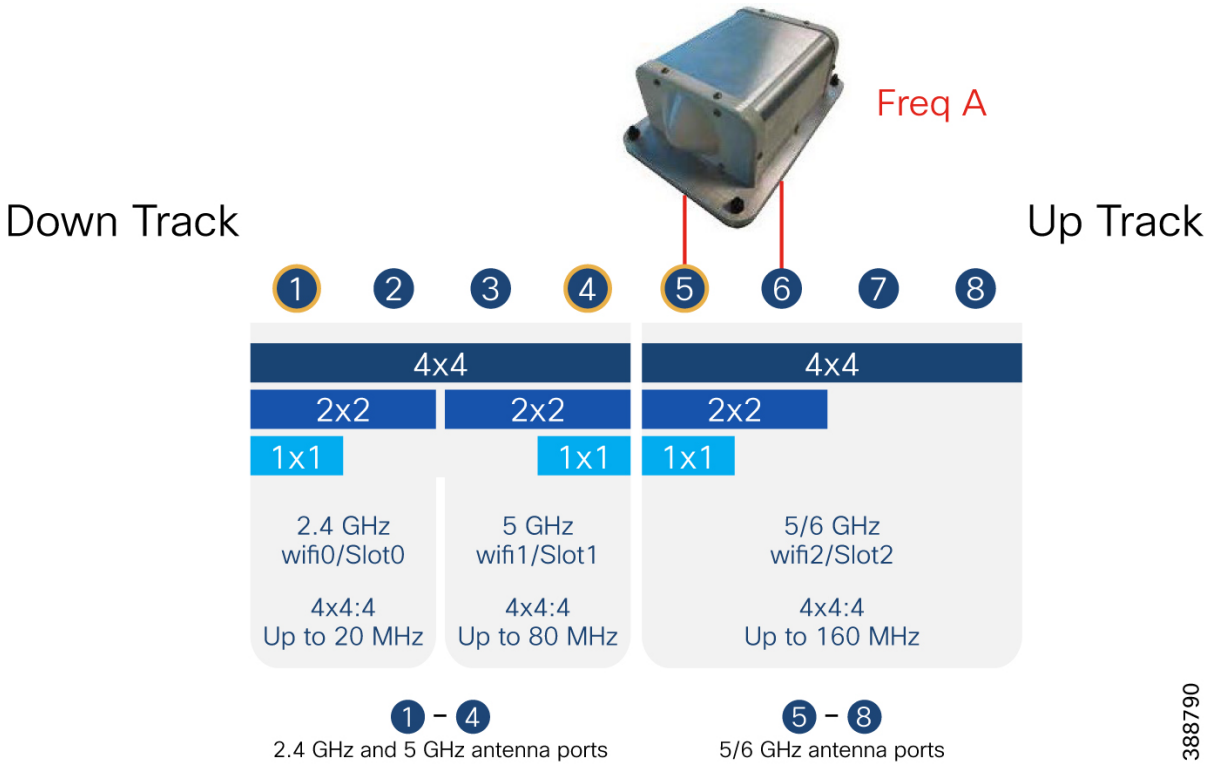
An example of the physical cabling for the wayside radio to antenna is below. For simplicity, a 2x2 MIMO setup is shown with the up track and down track antenna connected to the same physical ports using a splitter. A 4x4 MIMO setup could also be used with extra antennas and cabling.

Figure 14 *Wayside single frequency antenna connections*



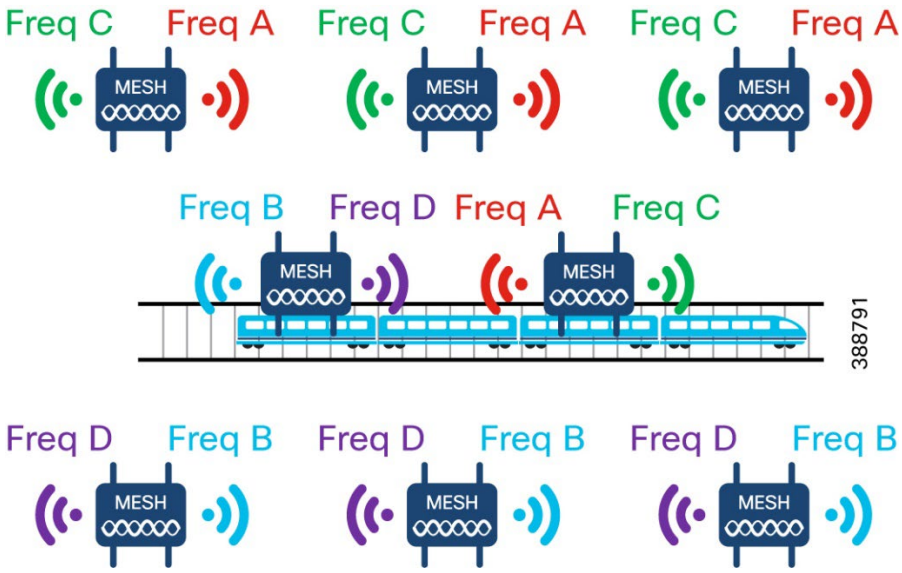
The onboard train antenna connections are shown in the figure that follows. A single bidirectional antenna with 2x2 MIMO is used in the example but can be expanded to 4x4 MIMO with extra antennas and cabling.

Figure 15 *Onboard train single frequency antenna connections*



In cases where there are numerous frequencies available, the multi-radio functionality of the IW916x can be used to improve throughput and coverage. Each radio on the IW916x corresponds to a separate set of antenna ports that work together as one logical system. This means one radio can be pointed up track with a dedicated antenna and frequency while the other radio is connected to a different antenna pointed down track on a different frequency. This eliminates splitting the overall signal at the expense of extra RF spectrum. In an area with significant RF and WIFI usage, this option may not be feasible.

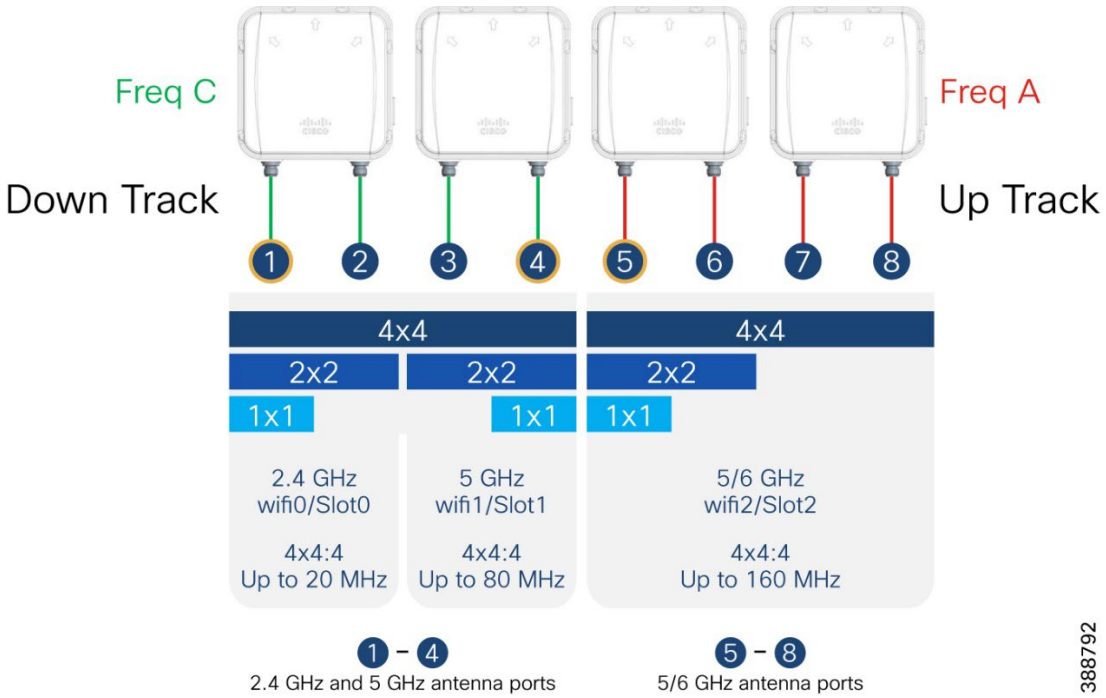
Figure 16 *Dual frequency with Dual Radio*



On the train, the extra frequencies can be collocated on the same IW916x using the two radio interfaces or split between two radios using fast failover See the High Availability Design section for more details about this option.

The wayside antenna cabling design is shown below for a single LAN path. This example depicts two antennas per radio for 4x4 MIMO but the antenna gain must be balanced against the radio power output to not exceed EIRP limits.

Figure 17 *Wayside dual frequency antenna connections*



The onboard train antenna design can use a single IW916x radio because of the multiple built-in radios or expanded to multiple IW916x radios to use the benefits of fast failover. Both examples are shown below.

Figure 18 *Onboard train dual frequency antenna connections*

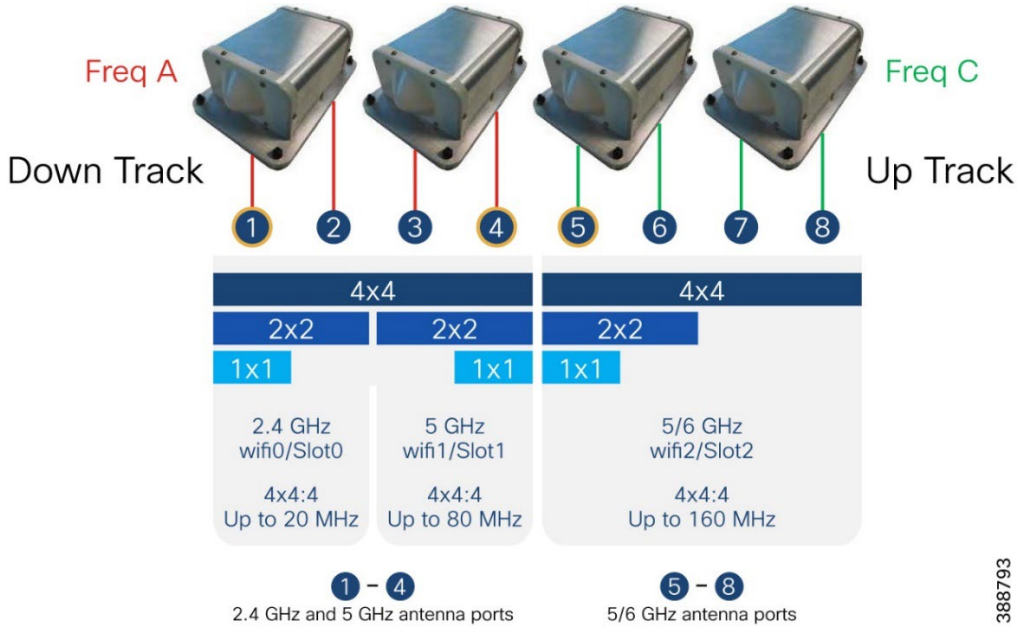


Figure 19 *Onboard train dual frequency dual radio antenna connections*

Antennas

Wayside

The wayside antennas are responsible for covering the largest amount of track to provide the best signal coverage for the passing trains. Each radio is responsible for coverage in two directions, up track and down track while minimizing overlap with the radio coverage for the secondary LAN path. The recommended antenna is the Cisco IW 2-port High Gain Panel Antenna (IW-ANT-PNL-515-N). This antenna supports 2x2 MIMO and can be combined with a second antenna if 4x4 MIMO is desired. While adding a second antenna means increased costs, it allows a higher overall signal strength due to increased radio paths and diversity between the signals.

They have dual slant antenna elements to support a variety of orientations for the train radio antennas. To support up track and down track connectivity using a single radio inside the IW radio, it is recommended to use splitters for the antennas so the radio ports see all the signals from the different directions.

More details about this antenna can be found here:
https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/b-cisco-industrial-routers-and-industrial-wireless-access-points-antenna-guide/m-iw-ant-pnl-515-n.html .

Figure 20 *IW-ANT-PNL-515-N*

Train

The train antenna must be rugged and low profile to prevent damage to itself and the infrastructure. Like the wayside antenna, it must be positioned on the train to give the best coverage alongside the track. Poor placement could mean minimal or weak coverage and poor roaming to the next wayside radio. There are two suitable options for the train in this solution depending on how many radios are installed on the train and their spacing from each other. Both are shark type antennas with dual-slant 45 deg antenna elements. One is the Cisco Directional Train Top Antenna (IW-ANT-SKS-514-Q) and the other is the Cisco Bi-Directional Train Top Antenna (IW-ANT-SKD-513-Q).

With two radios in fast failover mode on the same LAN path, one can be facing forward on the train and the other backward with both using the directional antenna. This way there is no RF interference between them and the full energy of the antenna can be directed in two directions. If the radios are much farther apart or if there is only one radio on a LAN path, the bidirectional antenna can be used to ensure complete coverage as the train moves down the track and roams between wayside radios.

More details about the bidirectional antenna can be found here:
https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/b-cisco-industrial-routers-and-industrial-wireless-access-points-antenna-guide/m-iw-ant-skd-513-q.html

Figure 21 *Bidirectional Train Antenna*

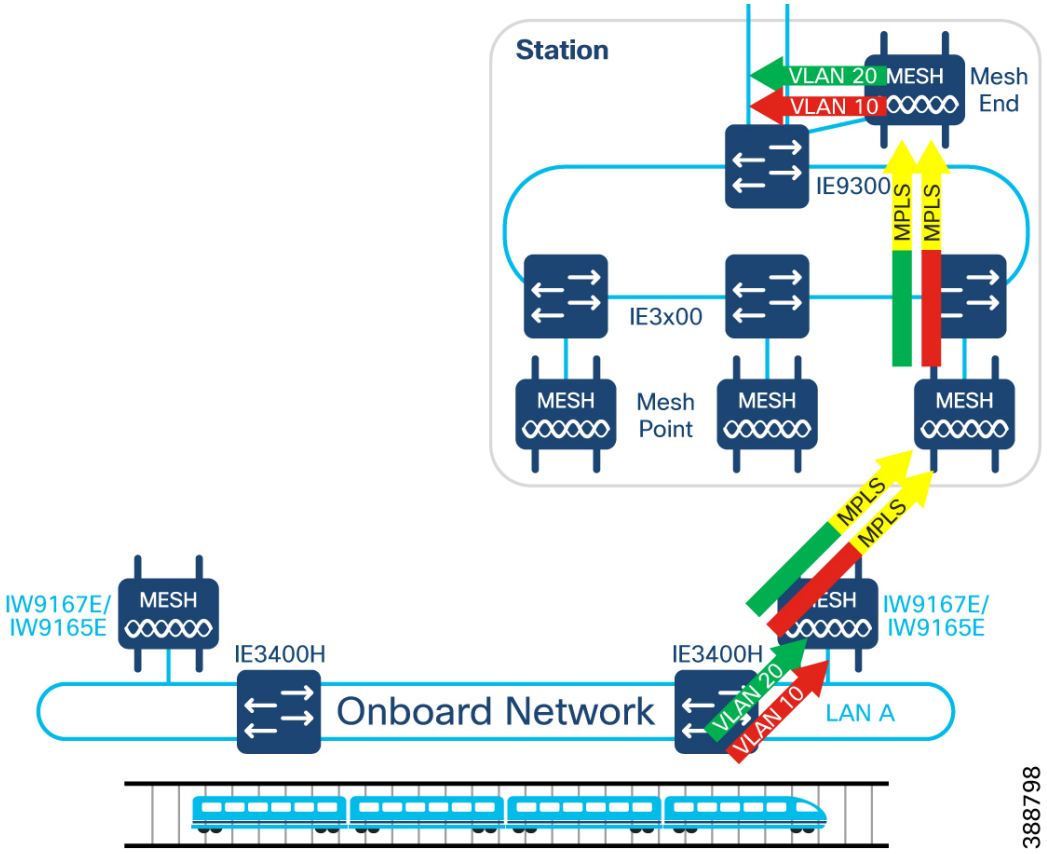
More details about the directional antenna can be found here:
https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/b-cisco-industrial-routers-and-industrial-wireless-access-points-antenna-guide/m-iw-ant-sks-514-q.html

Figure 22 *Directional Train Antenna*

Layer 2 Wireless Design

When using Fluidity with a L2 design, there is one Mesh End and enough Mesh Points to provide RF coverage for the service area. All radios in the mesh network are in the same broadcast domain and the data VLANs on the train are trunked end to end. An example of this is shown below.

Figure 23 *L2 Fluidity*

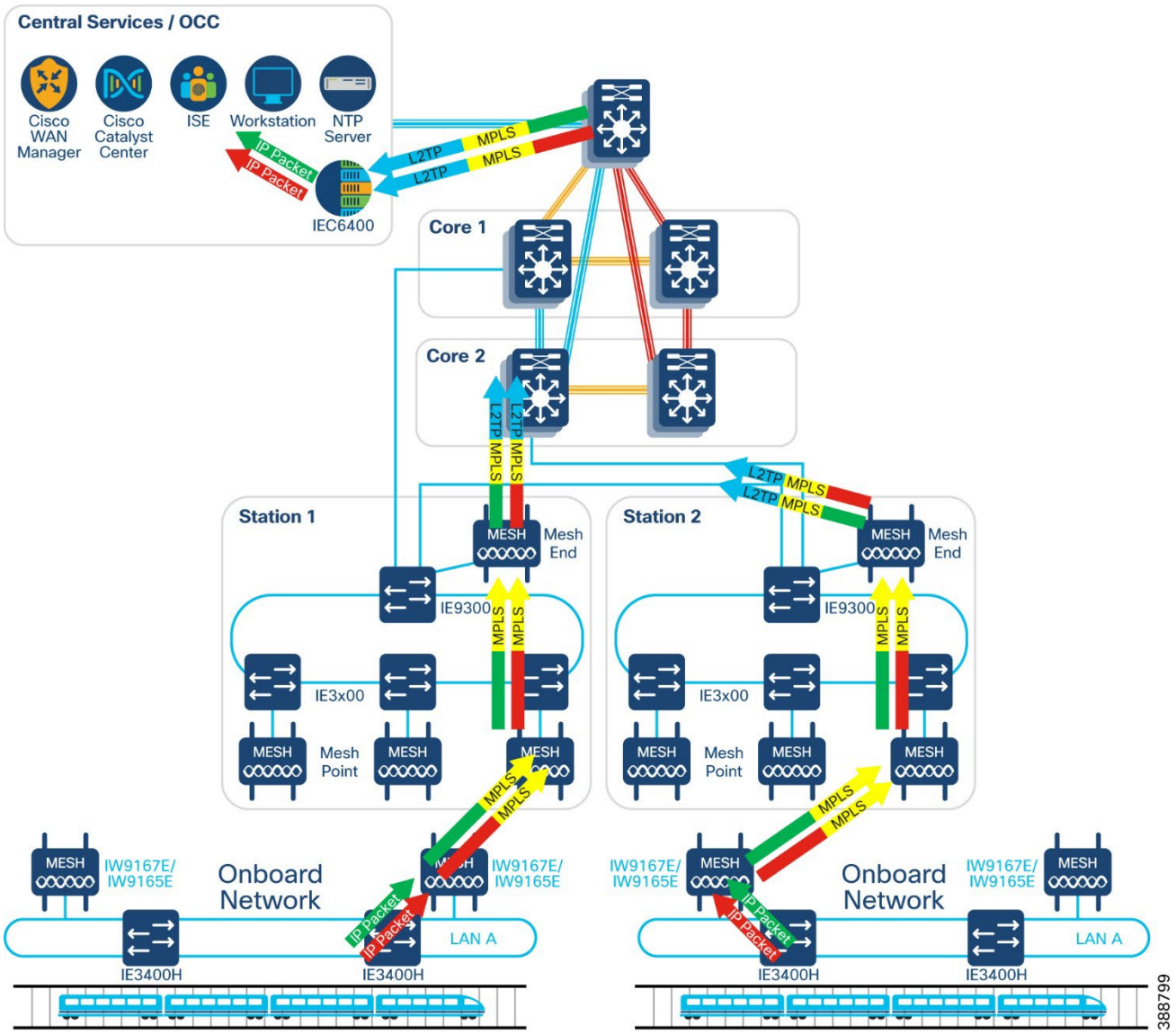


This is simpler to deploy than a L3 design but does not scale to the same level and is recommended for a smaller deployment where a Mesh End can be centrally deployed and the Mesh Points can support all the expected traffic. If the Mesh Points or Mesh End must cross a L3 domain, L3 Fluidity must be used.

Layer 3 Wireless Design

L3 Fluidity is required when a train must roam between L3 boundaries such as multiple stations with their own L3 domains. In this deployment, a Mesh End is still used with several Mesh Points to support the RF coverage area. When the train roams into another station's coverage area, there will be another mesh network with Mesh Ends and Mesh Points. Seamless roaming is enabled between the mesh networks by using a Global Gateway. This Global Gateway forms L2TP tunnels to all the Mesh Ends and provides seamless roaming. Each mesh network has its own IP subnet which is different from the other mesh networks and the train access point is on a shared subnet with a L3 gateway installed on the train. In this deployment, VLANs on the train are not trunked end-to-end, but rather the data is tunneled to the Global Gateway and then routed to the destination.

Figure 24 *L3 Fluidity*



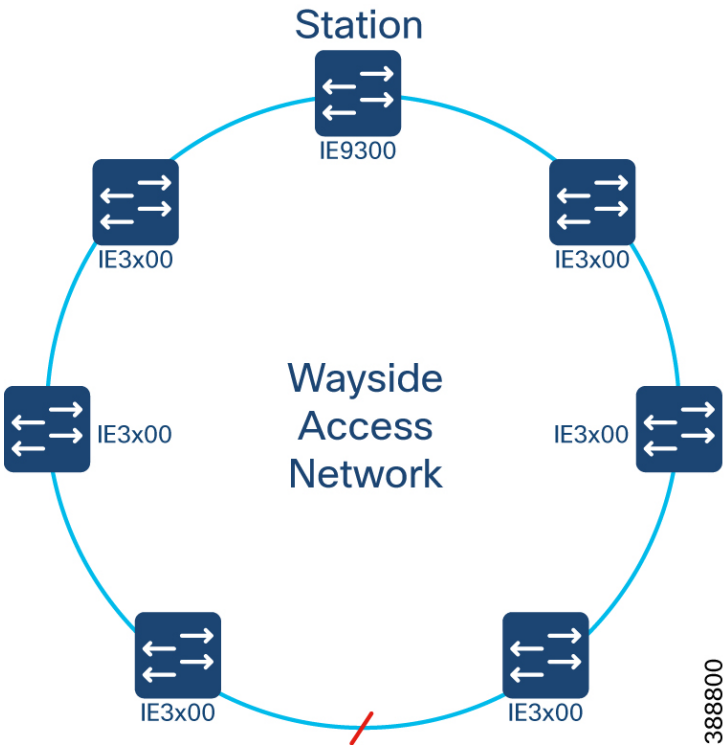
Wayside Wired Access Design

The wayside wired access network provides connectivity to the wayside devices situated along the track or within bungalows near the track. Depending on the bungalow construction, the wayside switches may be in unconditioned space or in a dusty environment subject to vibration from the passing trains. The Cisco IE3x00 Rugged series switch is the recommended option because of its fanless and rugged design. When determining the model, it is important to size the switch for current and future expansion. While the vital traffic may be low bandwidth, supporting CCTV and passenger traffic may be a future business need requiring much more bandwidth. In this solution, the IE-3400 or IE-3300 is recommended for bandwidth up to 1Gbps and the IE-3300-8U2X (or IE-3300-8T2X for non-POE) for bandwidth up to 10Gbps.

The wayside access network also provides connectivity to the backbone switch which is usually installed in a station or other centralized location. Depending on the physical fiber layout, this could be done as a ring or hub and spoke. A ring topology most closely follows the layout of the track where the fiber can be installed in the same direction as the track and connect the adjacent wayside switches. The disadvantages of this network are increased bandwidth requirements for the switches closest to the station and longer latency for the switches furthest away from the station. The advantages of this network are reduced fiber installation

costs and more efficient use of land during construction since all fiber runs can use the same conduit. It also reduces the number of ports needed on the backbone switch and allows the backbone switch to support more wayside access switches. In this solution, a REP ring is deployed which minimizes convergence during a failure. Since REP blocks a segment port to prevent loops, it is recommended to manually set the blocked port in the middle of the ring to minimize the end-to-end latency of any switch in the ring. This setup depiction follows.

Figure 25 *REP ring with blocking port*



A hub and spoke design connects each wayside switch directly to the backbone switch and reduces the overall bandwidth on links while also minimizing latency. The disadvantages of this network are increased installation and fiber costs as well as decreased port density on the backbone switch.

The wayside network is duplicated to provide two redundant paths and must therefore be laid out to maximize the investment. It is recommended to install the fiber on opposite sides of the tracks or sufficiently far apart from each other to prevent an accidental fiber cut from affecting both fiber runs.

To minimize unnecessary traffic in the access network and to increase security through segmentation, it is recommended to put each distinct service into a separate VLAN.

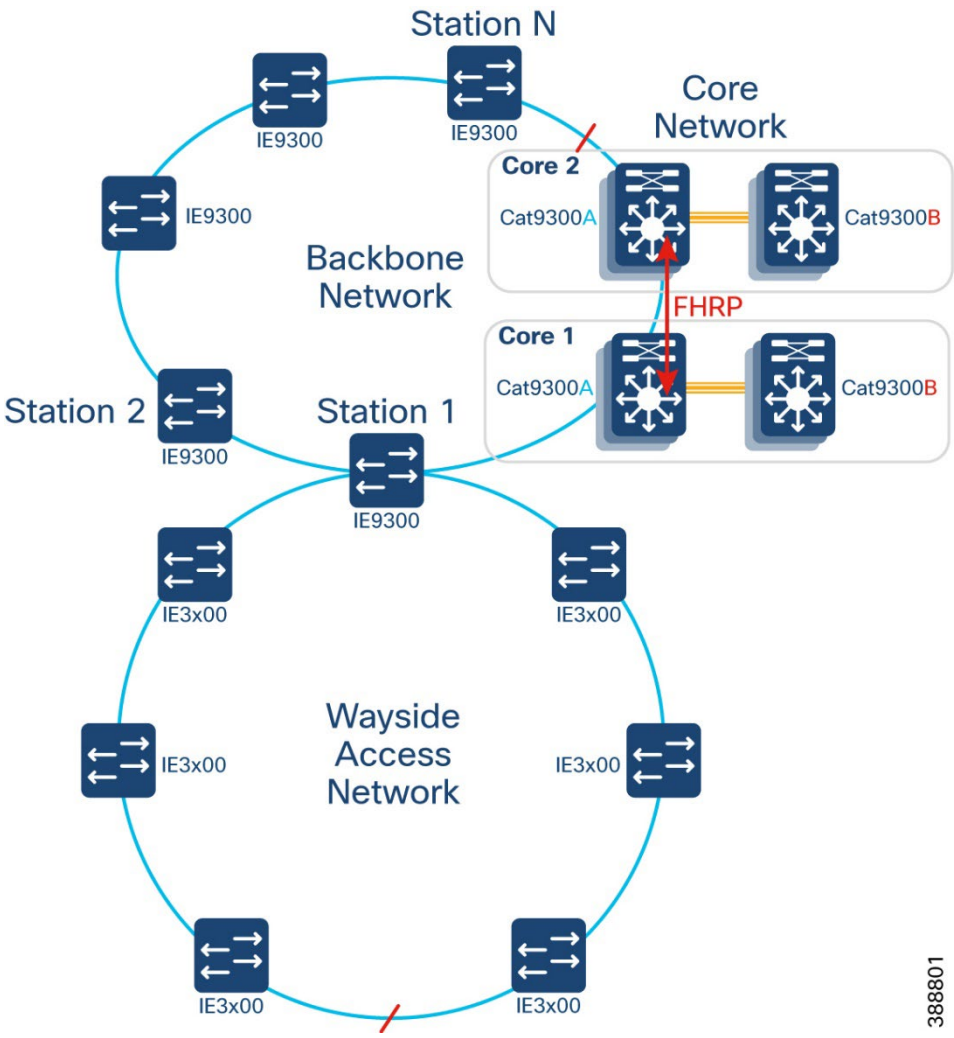
Wayside Backbone Design

The wayside backbone connects the wayside access network to the core network. The backbone switch network is duplicated to have two separate paths and also connects to two different core networks. Depending on the environmental conditions of the installation location, the Cisco Catalyst IE9300 Rugged series switch or the Cisco Catalyst 9300 series switch can be used to connect the wayside to the core network. In this solution, the backbone switch is connected to the wayside access switches with a REP ring topology and to the other backbone switches with another REP ring topology. Because a number of wayside access rings can connect to the backbone switch to support the entire coverage area, it is important to size

the switch appropriately given that two ports are needed for every wayside ring and 2 or more ports are needed to connect to the backbone ring.

The backbone switch is the L3 gateway for all the wayside networks and needs L3 reachability to the OCC/BOCC. Because the backbone network is in a ring with two different core network devices, the backbone switches can potentially have multiple paths to the OCC. It is recommended to use a First Hop Redundancy Protocol (FHRP) between the core nodes to provide a default gateway to the backbone switches. An example follows.

Figure 26 *Backbone Network*



Because the backbone switches have a default route to the core, it is recommended to choose an IP scheme for the wayside devices that can be efficiently summarized. The core switches will have static routes to these summarized networks which will make troubleshooting and management easier.

Core Network Design

Layer 3 Routing

A L3 routed core is most like a standard enterprise core network that is high performance and highly resilient. In this solution, each core node is a Cisco Catalyst C9300 that supports greater than 10Gbps links and two separate core networks for both LAN paths. The backbone network is connected to a core node in each path to ensure that a failure in one node or network segment does not cause a complete outage. Each core node also has full route reachability with the other core nodes to ensure the best path is chosen through the core.

Each core node should be connected to each other using multiple links configured as a port channel for increased throughput and resiliency against link failures.

As mentioned in the previous section, it is recommended to use a FHRP between the two core switches with a single virtual address on a Switched Virtual Interface (SVI). Each backbone switch in that REP ring will then use the virtual address as the default gateway. If there are multiple backbone rings connected to the same core switches, they can use a different virtual IP for each ring and then load balance them between the core switches. In this way, one core switch can be the primary node for half the rings and the backup for the other half. The REP alternate port should be chosen such that the link between the core nodes in the ring does not block traffic. If this link blocks traffic, the FHRP traffic will traverse the rest of the ring which would result in suboptimal forwarding.

MPLS with Segment Routing

An MPLS core is typically deployed in a service provider or large multitenant datacenter due to its support for VPNs and frequent usage with BGP. Alternatively, a legacy optical network may have been deployed and then migrated to MPLS-TP to have some of the same advantages as the optical network. MPLS has several advantages over a traditional routed network in terms of convergence and the ability to create different topologies using VPNs or Traffic Engineering (TE). MPLS with Segment Routing (MPLS-SR) further improves on these advantages while reducing operational complexity.

MPLS relies on switching packets based on labels rather than performing a routing table lookup for every packet. It creates a Label Switch Path (LSP) for every next hop based on the routing table and all packets that match a certain Forwarding Equivalence Class (FEC) are put on that same LSP. This way packets do not have to be checked against the routing table at every hop, the ingress MPLS router, called a Label Edge Router (LER), looks up the destination for a packet and then imposes a label. Afterward, each next hop switch in the path is called a Label Switch Router (LSR) and simply swaps labels until reaching the destination. MPLS can be further enhanced using Traffic Engineering (MPLS-TE) that predetermines a specific path through the MPLS network by reserving bandwidth using Resource Reservation Protocol (RSVP). This can be operationally challenging because it requires signaling across the network to reserve a path based on network constraints like bandwidth or latency.

Segment routing is the next evolution of MPLS that simplifies the operation and increases scalability. With MPLS currently, the labels must be distributed through some protocol. It can be LDP which relies on the routing table to distribute labels. It can also be BGP which has been extended to MP-BGP to support other address families like multicast and VPN with label distribution.

Instead of assigning a label to a FEC for every LSR and distributed through LDP, Segment Routing uses the concept of a Segment ID (SID) to describe every path in a network. A segment could be a switch (node), or a link. With Segment Routing, the labels are not distributed using a specific protocol but are rather added directly to the packet at the ingress MPLS router using an IGP like IS-IS or OSPF. Both these protocols have been extended to support adding segment definitions into the packet structure. In this way, Segment Routing is characterized as a source-based routing architecture. Now when a packet enters the MPLS network, the IGP can determine the best routed path and append the full list of SIDs to the packet. Then at every hop, the LSR pops off the top SID before sending it to the next hop.

Since the list of SIDs is appended to the packet at the LER, another benefit of Segment Routing is revealed. As stated previously, MPLS-TE allows finer granularity in the path selection of an MPLS packet by predetermining which routers will be in the LSP. This requires another protocol to ensure the path matches the requirements. However, with Segment Routing, the specific LSP is already computed without any extra protocols and present in every packet. This LSP can be created according to the best routed path computed by the IGP or it can be manually manipulated by an external controller. Using a Software Defined Networking (SDN) approach, the LSP can be manipulated according to specific policies, application requirements, etc. and then pushed down to the Segment Routing devices.

A traditional MPLS network which also uses MPLS-TE may need LDP, RSVP, IS-IS/OSPF and BGP to function properly. With Segment Routing, LDP and RSVP are no longer needed and BGP no longer needs to distribute labels. This reduces operational complexity and hardware requirements on the core devices while adding SDN capabilities for better network intelligence and insight.

More details about Segment Routing can be found here: https://www.cisco.com/c/en/us/solutions/segment-routing.html.

Segment Routing is supported on several IOS-XR platforms and in this solution the MPLS core is built around the NCS540. The NCS540 supports a variety of interface speeds and configurations while also being temperature hardened for suitability inside or outside. Like the L3 routed design, there are two core networks, one for each LAN path. The backbone switches connect to an NCS540 in each core forming a ring. With an MPLS core, L2 and L3 VPNs are supported based on the networking needs. These features can be incorporated into the single technology called EVPN. EVPN provides Ethernet multipoint services over MPLS and can create L2VPN topologies with the advantages of L3VPN such as multihoming and per flow load balancing. Since the backbone ring is dual-homed to the core through the NCS540 core switches which are acting as Provider Edges (PE), EVPN can be used to support a dual-homed L2 ring without loops and with high resiliency.

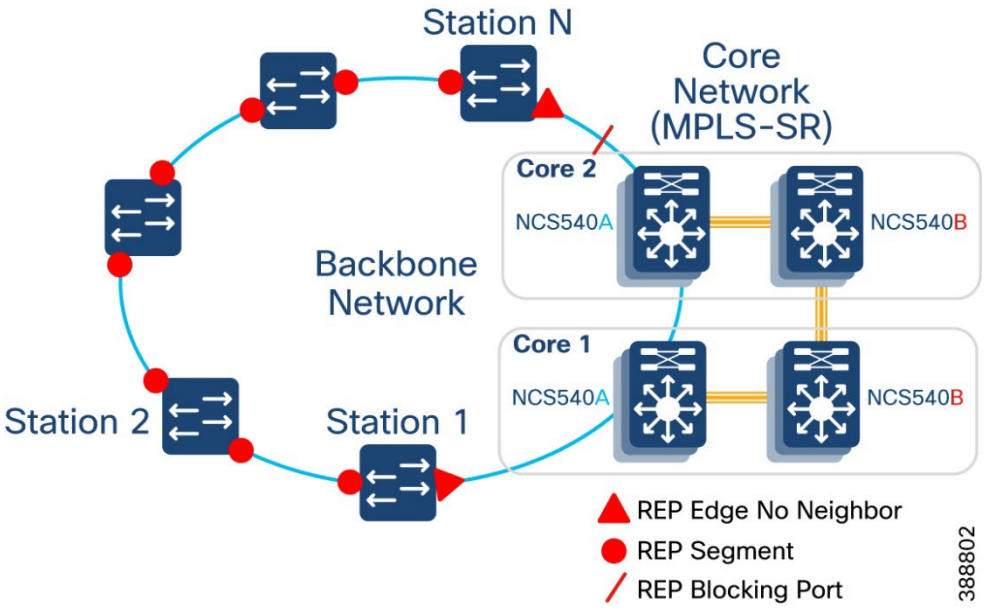
The NCS540 does not support REP so there must be a way to communicate the status of the REP ring between the two NCS540 routers connected to the backbone switches. A feature called REP Access Gateway (REP-AG) allows the core devices to tunnel the ring state information between them and ensure that a loop does not occur. The directly connected backbone switches are configured with REP Edge No-Neighbor and need to communicate any topology change notifications to the core switches with a Segment Topology Change Notification (STCN).

When a device is multi-homed to the pair of NCS540s, there needs to be a mechanism to use the dual paths effectively. One option is to use single-active which treats the core devices as active/backup. All VLANs use a single active node while the other stands by. This behavior contrasts with a standard REP ring where different VLANs can be blocked on different ports to achieve load balancing on the switches in the ring. Additionally, only one of the PE nodes learns the MAC addresses of the hosts and after a failure, the standby PE would have to learn them all which increases convergence time. Another multi-homing option is all-active which sends traffic to both nodes at the same time. In a ring environment this is undesirable since it will cause loops.

Using the single-flow-active feature of EVPN, the traffic can be load balanced per flow instead of using a single node which is similar behavior to REP. In this configuration, a blocked ring port for VLANs will cause the traffic to arrive at one of the PEs first. This PE becomes the active node for this flow and sends the MAC address to the other PE as a standby node. If there is a failure in the ring such that the traffic must go to the other PE, the PE will flush the MAC table and learn it again from the connected host. This keeps the table up to date with no outdated information. A BVI with the same IP address is also configured on both PE nodes to provide L3 gateway redundancy for the backbone switches.

An example of this network follows.

Figure 27 *Backbone REP ring connected to MPLS-SR Core*



High Availability Design

The Rail CBTC and Safety architecture is designed to be fully redundant with separate traffic paths from the train to the OCC and BOCC. Even with a complete failure in one path, the other traffic path will still be accessible for the vital traffic. Within each layer of the separate paths, there are further steps to increase the availability of the network.

Core

Within the core, there are numerous ways to achieve high availability. Each core node should have redundant power supplies on separate power circuits if possible. Each core node should be connected to its neighbor with a port-channel of at least two links for extra throughput and resiliency against a fiber or SFP failure. The Cisco Catalyst 9300 also supports physical stacking through exterior stacking cables which increases port density and when connected to neighboring devices with port-channels on different stack members, increases the overall availability.

Backbone

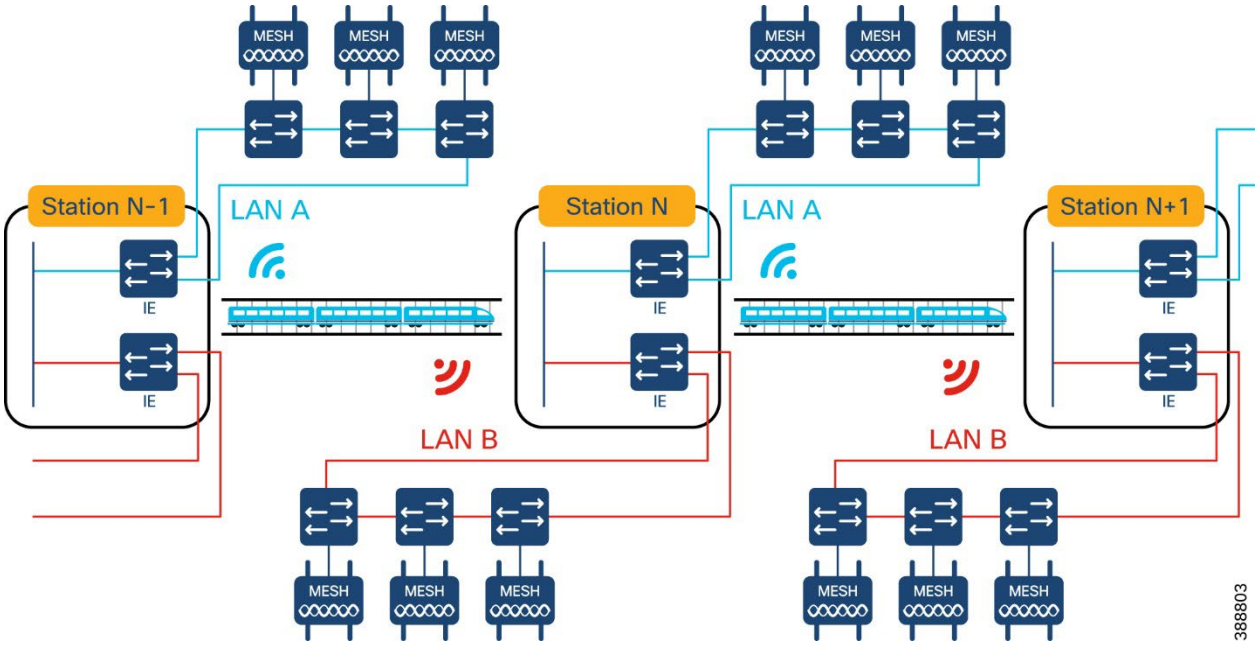
The backbone switches are connected in a REP ring which reduces the fiber costs associated with a hub and spoke design while being resilient to traffic loss due to a failure in a node or link failure. Like the core nodes, the backbone switches should have multiple power supplies connected to different electrical circuits.

Wayside Access

The wayside access switches are like the backbone switches in terms of high availability. These switches are connected in a REP ring or hub and spoke. If connected as a hub and spoke, the wayside access switches should connect to the backbone switch using a multilink port-channel for increased throughput and resiliency against a fiber or SFP failure. The switches also support multiple power supply inputs for power redundancy.

As illustrated in Figure 28, two separated wayside access networks A and B cover each section of trackside between stations, and the power cables of the two networks connect to opposite stations. With this design, a radio, switch, and fiber cut will not prevent train to ground communications. Even in the event of failure of an entire station, coverage is still maintained and there is no impact on service.

Figure 28 *Wayside access network redundancy*



Train to Wayside RF

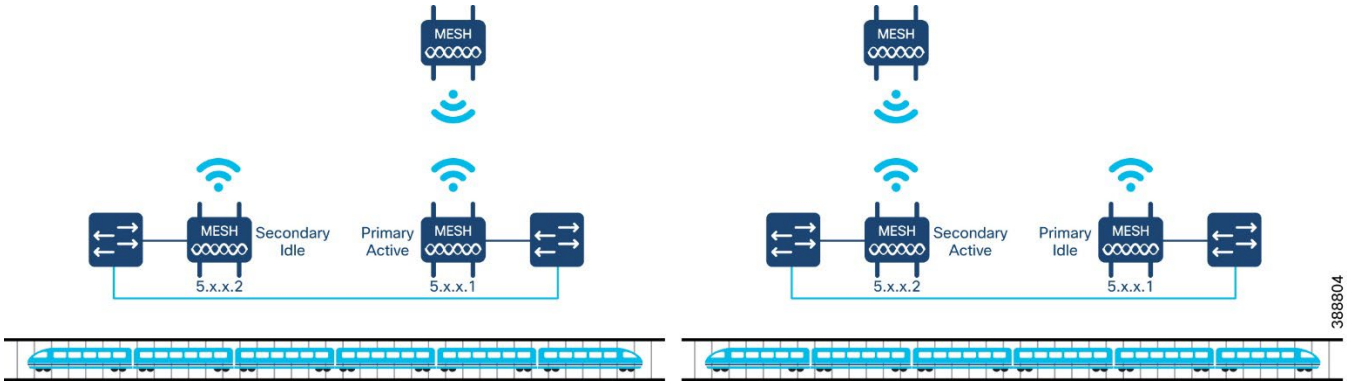
Each function of the URWB mesh network can be made more resilient using fast failover which operates in an active/backup mode. Fast failover enables convergence times of less than 500ms in the case of active radio failure. The feature also supports preemption with delay to restore the radio network to a known good state upon recovery.

Since the Mesh End is the demarcation between the mesh network and wired network, it is recommended to configure a second one with fast failover mode as a backup. In a small deployment, an IW9167E could serve as the dedicated Mesh End with the radio interfaces turned off. In deployments with greater then 2Gbps aggregate throughput, the IEC6400 should be used. A pair of IEC6400s configured as Global Gateways in each Operations Center is also recommended with the added feature of a virtual IP address (VIP). When the Global Gateways are configured with a virtual IP address, all the Mesh Ends form L2TP tunnels to this address and all traffic coming into the mesh use the VIP as the entry point. It is recommended to split the active and backup Global Gateways between the OCC and BOCC to ensure that regardless of any failure encountered, the Global Gateway will always be accessible.

The onboard train radio can also be deployed as a redundant pair using fast failover. When two radios are configured in the same broadcast domain with the same passphrase, they will act as a single radio. The radio with the lowest mesh-id will become the primary while the other radio will be the secondary. The primary radio will then constantly evaluate the signal between the wayside infrastructure and the pair of onboard radios. Whichever train radio has the better signal will become the active one, while the other radio will be the idle. All traffic from the LAN side goes to the primary radio while all RF traffic goes to the active one.

The image that follows shows a train where the primary radio (5.x.x.1) has the stronger signal and is the active forwarder. The next image shows the secondary radio (5.x.x.2) having the stronger signal and becoming the active forwarder while the primary is now idle. Fast failover makes this process seamless.

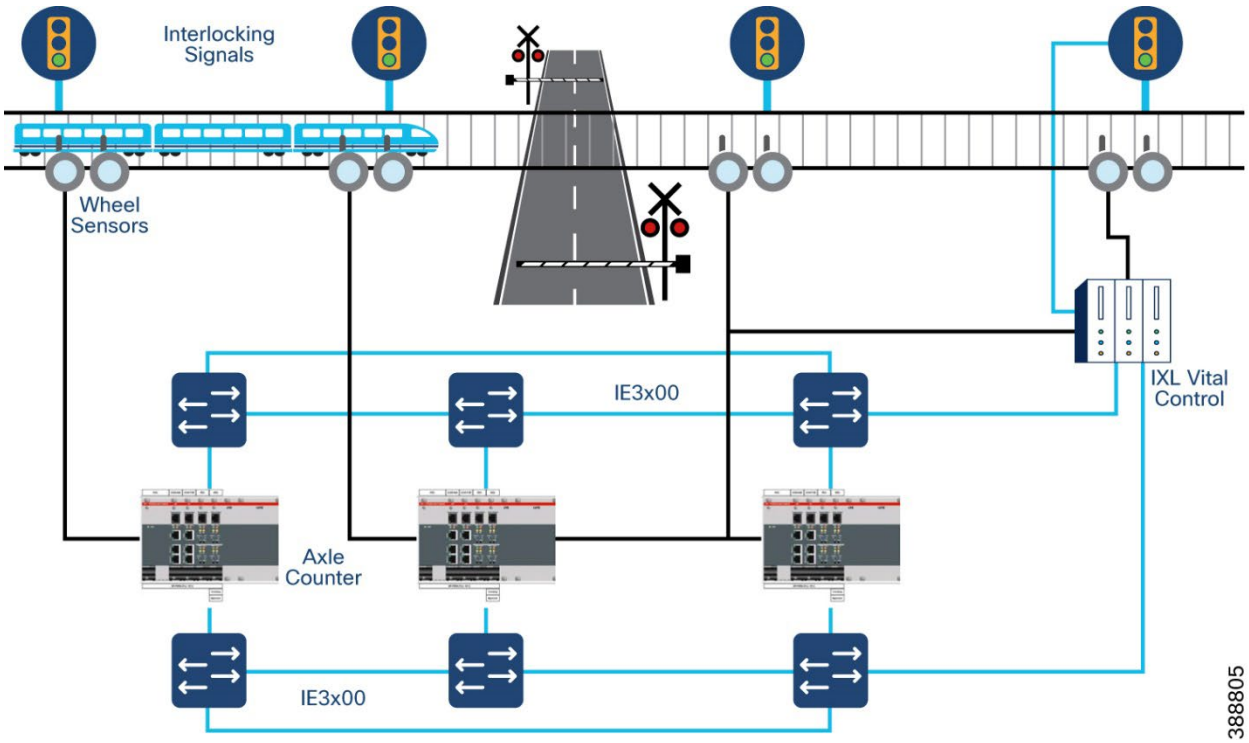
Figure 29 *Onboard radio fast failover*



Frauscher Axle Counter Network Design

The Frauscher Axle Counting system connects to the wayside access network directly at the track. It enables reliable detection of the train including clear/occupied notifications, number of axles, direction of travel, speed, and wheel diameter. The system can be integrated into interlockings, level crossings, and signaling equipment. This integration requires low latency (<10ms end to end) and fast convergence of the underlying network (<500ms). The equipment also allows network connectivity to the two separate LAN paths for maximum reliability.

Figure 30 *Frauscher Axle Counter network integration*



Meraki People and Vehicle Detection Design

Cisco Meraki cloud-managed MV smart camera family brings simplicity and data-powered intelligence to the security camera world. Every MV model comes with a powerful processor—the same kind found in many of today's smartphones—and an innovative architecture that minimizes physical infrastructure as well as software requirements. These smart cameras not only help ensure physical safety and security, but also provide advanced business intelligence. MV smart cameras pack fast processing power, robust security features, and sophisticated analytics into a refreshingly simple package.

All second-generation MV cameras, equipped with industry-leading processor, are not only capable of providing high-definition video, but they also allow for machine learning-based analytics, and are capable of processing powerful analytics on the camera itself and transmitting the metadata to the Meraki cloud. This revolutionary architecture dramatically reduces the cost and complexity of gathering detailed analytics in any environment, by removing previously required additional software and heavy-duty hardware. Harnessing the power of computer vision and machine learning, MV smart cameras can detect objects which includes people and vehicle detection. This allows you to understand how objects are moving through and using your physical spaces.

Object Detection is a feature that allows you to narrow down your search to detect people and vehicles (bikes, cars and trucks) in the camera field of view (FoV). MV Analytics can leverage both object detection and motion metadata to analyze information about how many people/vehicles entered or were present at a specific time. The dashboard can show you this data at a minute, hourly, or daily scale, which allows you to identify time-based trends and anomalies in the usage of your space. Here are some of the object detection features:

- Time Resolution, Date, Start Hour and End Hour: Configure the scale for the slices of your histogram and the time range for your analytics.
- Object Detection by Zones: you can set Zones on your camera on the Zones page under camera settings tab. Use this to separate object detection according to areas within the camera FoV
- Estimate peak occupancy: This value takes the maximum of the estimated occupancy of the scene across the selected time range. The estimated occupancy of a scene is calculated every minute and is an average of the number of objects detected for every second of the minute.
- Entrance (bar chart/histogram): Presents the total number of entrances per hour/day for the hour/date range specified. This can be up to 24 hrs., 7 days or 1 hour - depending on the selected time resolution.
- Total Entrance: This value represents the number of entrances of objects detected within the scene

MV Sense, one of the camera APIs, includes REST and MQTT API endpoints which provide historical and real-time people and vehicle detection data. It allows you to enhance or create an application which features the object detection data to build intelligent business solutions. Here are some of the example of use cases that rail operators can benefit from MV camera object detection analytics:

- People counting at access gates
- Station, platform, and toilet occupancy
- Social distancing
- Gateline queuing, queue management
- Crowd management
- Person on tracks
- Perimeter security at restricted areas
- Trespassing
- Station people dwelling time
- Heatmaps for passenger flow and dwell time for station planning
- People and vehicle detection at level-crossing
- Worker safety at trackside
- Suicide prevention and detection

For this solution guide, we recommend cloud-managed MV63x, MV72x, and MV52 smart cameras.

Figure 31 *MV52 Ultra-long-range telephoto bullet camera*

- 12-40 mm varifocal lens with 12-37° horizontal field of view
- 4K video recording with H.264 encoding
- f/2.3/16 aperture
- 1TB high-endurance solid-state storage
- IR illumination up to 50 m or 164 ft

Figure 32 *MV72X Outdoor varifocal dome camera*

- With up to 3x optical zoom and IP67 and IK10+ ratings
- 512GB high write endurance solid-state storage
- 4MP video recording with Smart Codec encoding
- 3-9 mm varifocal lens, IR illumination up to 30 m or 98 ft
- 802.11ac wireless
- Microphone for audio recording

Figure 33 *MV63x Outdoor wide-angle fixed lens mini dome camera*

- 1 TB high write endurance solid-state storage
- 4K video recording with smart codec encoding
- Fixed lens with IR illumination up to 20 m or 66 ft
- 802.11ac wireless
- Microphone with external hardware switch for audio recording

QoS Design

Within the Rail CBTC and Safety architecture, vital traffic is considered as highest priority while all other traffic is best effort. The vital traffic should then be matched and classified as close to the source as possible to make sure it has priority treatment end-to-end while all other traffic is remarked with the lowest QoS value.

URWB

The URWB devices support eight levels of priority when classifying traffic. When inspecting a packet, the DSCP/TOS value is translated into one of eight queues based on the three most significant digits. This translation follows.

Figure 34 *Cisco URWB QoS*

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Priority			X	X	X	X	X
0	0	0	Priority 0 (lowest)				
0	0	1					
0	1	0	.				
0	1	1					
1	0	0	.				
1	0	1					
1	1	0	.				
1	1	1	Priority 7 (highest)				

388809

This priority value is copied into the MPLS EXP bits which is maintained throughout the mesh network until it leaves the mesh. When this data is transmitted over the wireless interface, the eight priorities are further mapped into four access categories based on the 802.11e WMM standard.

In a L2 Fluidity network, a VLAN header is also appended to the packet. The priority value that was copied into MPLS EXP is also copied into the 802.1p field of the VLAN header as the COS (Class of Service) value. When this traffic reaches the wayside network from the train, the VLAN header is maintained until it reaches the Mesh End. This means that all switches in the path can match on the COS value to differentiate between traffic of differing priorities coming from the train network.

In a L3 Fluidity network, there is no VLAN header on the traffic from the train. The priority value is copied into the MPLS EXP bits but is transmitted to the Mesh End as MPLS traffic. At the Mesh End, the traffic is encapsulated with an L2TP header with the EXP bits translated into the DSCP field. Since the IE-3x00 cannot match on MPLS EXP, there is no differentiation between traffic of differing priorities coming from the train network between the Mesh Point and Mesh End.

If the wireless network was used for multiple services on the train network, the vital and non-vital traffic would be given the same priority once it reaches the wayside network. In the case of congestion on the wired network, this could have an adverse effect on the vital traffic end to end latency. This can be mitigated in several ways. On the train, the vital traffic can use a separate wireless network from the non-vital and then the traffic from the different wayside radios can be marked accordingly. Another option is to have the wayside access switches directly connected to the backbone switch which eliminates the chance of congestion on a ring.

Multicast Design

Multicast design for a traditional campus is well known and well documented here: https://www.cisco.com/c/en/us/tech/ip/ip-multicast/index.html. In the Rail CBTC and Security architecture, it is important to understand where the multicast sources and receivers are to optimize the traffic flow.

For multicast traffic that must traverse the URWB mesh network, multicast must explicitly be configured on the Mesh End. The multicast address can either be forwarded to all mesh nodes in the network or strictly to the current primary Mesh End.

When using multicast with MPLS and Segment Routing, traditional methods of multicast routing can be used, including PIM, mLDP, RSVP-TE, and ingress replication. Another option is to use TreeSID which uses Segment Routing Path Computation Element (SR-PCE) to create the point to multipoint tree using Segment Policies. Using TreeSID eliminates the use of RSVP, mLDP, and PIM. These policies can be created and deployed using the Cisco Crosswork Optimization Engine or the TreeSID CLI on the SR-PCE which can run on a Cisco IOS-XR router. The Crosswork Optimization Engine enables SR-PCE HA and is the preferred implementation.

Rail Zero Trust Network Access Design

The Rail transit system is very complex and combined with dozens of systems that are deployed on the moving trains, stations, and railroad tracks that can extend to thousands of miles. Cybersecurity attacks on rail systems can disrupt the flow of goods on freight lines, completely stop train operations, and degrade passenger services, disappointing the customers that rail operators are seeking to delight. Attacks on vital rail systems can cause shutdowns or, even worse, harm to human safety. Government agencies, standard bodies, rail industry professionals, and cybersecurity experts are working together to drive initiatives, set the regulations, guidelines, best practices, and technical specifications to help transit agencies manage cybersecurity issues in the transit industry. Some examples of the agencies are the U.S. Department of Homeland Security (DHS), the Transportation Security Administration (TSA), the National Institute of Standards and Technology (NIST), American Public Transportation Association (APTA), EU NIS2, and European Union Agency for Cybersecurity (ENISA).

Cybersecurity Challenges in Rail Control Systems

Transit agencies have been running their systems from decades to more than 100 years. In the past, the transit systems were primarily composed of proprietary hardware and software communicating in a non-standard protocol. They either have no need to communicate with each other or the connections between the systems are over privately owned or leased dedicated wire connections. It has no practical connection to Information Technology (IT) business systems or Internet. Securing the rail operations in these scenarios can be done by limiting the physical access to the components of the control systems. To compromise the system also requires specialized knowledge because of the proprietary nature of it. In today's transit systems, there are new challenges to implement cybersecurity.

- Connectivity changes: The latest control systems start using commercial off-the-shelf hardware and software. Industry standard protocols and wired or wireless connections are used in the architecture and system design. Communications between different systems across large geographic area are often required for operational efficiency. This presents additional security vulnerabilities to transportation systems because of an increased attack surface.
- Shared and Converged infrastructure: Even though safety critical applications like CBTC or interlocking in the rail Industrial Control System (ICS) usually runs over a dedicated closed system, there is a tendency to operate it along with the non-critical part of Operation Technology (OT) ICS systems and business systems (IT) over the shared infrastructure. IT Business systems is most concerned about information integrity and confidentiality, and consider information availability a lower priority. ICS systems on the other hand, take information availability and integrity as high priority, but are less concerned about the information confidentiality. Therefore, the approach to secure the business systems and control systems is different. Converged infrastructure provides an effective approach to not only save the Capex and OpEx, and streamline network management, but also help IT to gain OT asset visibility, understand communication patterns, detect vulnerabilities, and apply policies to secure the OT environment.
- Malware infection: even with unconnected or closed systems like rail control ICS, malware infection can happen. This could happen at the supply chain where it has been embedded or pre-loaded in off-the-shelf equipment, unauthorized data transfer via portable USB, inadequate physical security and configuration management, or unexpected connections.
- Legacy systems with long life cycles: transit systems operate with long life cycles measured in decades. The legacy systems were not implemented according to the security requirements defined in EN IEC 62443-4-2. However, detection of most cyber attacks is possible by applying technical and organizational countermeasures defined by the Annex B in CENELEC CLC/TS 50701 "Railway applications – Cybersecurity". These include processes like zoning and defense-in-depth.
- Real-time and time sensitive information: control systems in rail like other ICS systems have real-time requirements to maintain operational reliability, uptime, and safety. The security solution implemented requires careful evaluation of the delays introduced by the application of cybersecurity technologies.

Cybersecurity Requirements for Rail

To provide an acceptable level of protection for all identified threats and known vulnerabilities for rail operation, it is important to identify and structure the cybersecurity requirements for a given system under consideration (SuC) in the rail system. The security requirements (SR) for rail are largely derived from the System Security Requirements defined in IEC 62443-3-3. The structuring of the rail security requirements matches the seven Foundational Requirements (FR) class defined in the IEC 62443-1-1. The definition of each SR is not the scope of this guide, please refer to CLC/TS 50701 Chapter 8 Table 6. for detailed description. Following table 4 lists a few examples of the system requirements, security level (SL), and FR. This also includes part of cybersecurity measures defined in TSA Security Directive 1580/82-2022-01.

Table 4 *Sample Rail Cybersecurity Requirements*

Security Requirement (SR)	SL	Title	TSA Measure	TSA Description
FR 1 Identification and Authentication Control (IAC)				
SR 1.1	1	Human user identification and authentication	C.1	Identification and authentication policies and procedures to prevent unauthorized access
SR 1.1 RE(3)	4	Multifactor authentication for all networks	C.2	Multi-factor authentication, or other logical and physical security controls that supplement password authentication
SR 1.3	1	Account management	C.4	Enforcement of standards that limit the availability and use of shared accounts
FR 2 Use Control (UC)				
SR 2.1	1	Authorization enforcement	C.	Implement access control measures, including those for local and remote access
SR 2.1 RE(2)	2	Permission mapping to roles	C.3	Policies and procedures to manage access rights based on the principles of least privilege and separation of duties
SR 2.2	1	Wireless use control		
SR 2.6	2	Remote session termination	D.1.b	Block ingress and egress communications with known or suspected malicious IP addresses
SR 2.8	1	Auditable events	D.2.a	Audit unauthorized access to internet domains and addresses
FR 3 System Integrity (SI)				
SR 3.1 RE(1)	3	Cryptographic integrity protection		
SR 3.2	1	Malicious code protection	D.1.d	Block and prevent unauthorized code
SR 3.2 RE(2)	3	Central management and reporting for malicious code protection		
SR 3.8	2	Session Integrity		
FR 4 Data Confidentiality (DC)				
SR 4.1	1	Information confidentiality		
SR 4.3	1	Use of cryptography		
FR 5 Restricted Data Flow (RDF)				
SR 5.1	1	Network segmentation	B	Implement network segmentation policies and controls designed to prevent operational disruption to the OT systems if the IT system is compromised or vice-versa
SR 5.2	2	Zone boundary protection	B.2.a B.2.b	Prevent unauthorized communications between zones Prohibit OT system services from traversing the IT system and vice versa
SR 5.3	1	General purpose person-to-person communication restrictions		
SR 5.4	1	Application partitioning		
FR 6 Timely Response to Events (TRE)				
SR 6.1	1	Audit log accessibility	D.3.b	Ensure data is maintained for sufficient periods
SR 6.2	2	Continuously monitoring	D.3.a	Logging policies that require continuous collection and analyzing of data for potential intrusions and anomalous behavior
FR 7 Resource Availability (RA)				
SR 7.1	1	Denial of service protection		
SR 7.2	1	Resource management		
SR 7.3	1	Control system backup		
SR 7.6	1	Network and security configuration settings		

SR 7.8	2	Control system component inventory		

Cybersecurity Zoning and Conduits for Rail

Securing transit system is similar to protect industrial automation and control systems (IACS) in industries like manufacturing and utility. This guide leverages Cisco Industrial Automation Security Design Guide 2.0 as the foundation to help transit agencies successfully connect and secure their operational environment.

CLC/TS 50701 and ENISA Zoning Model

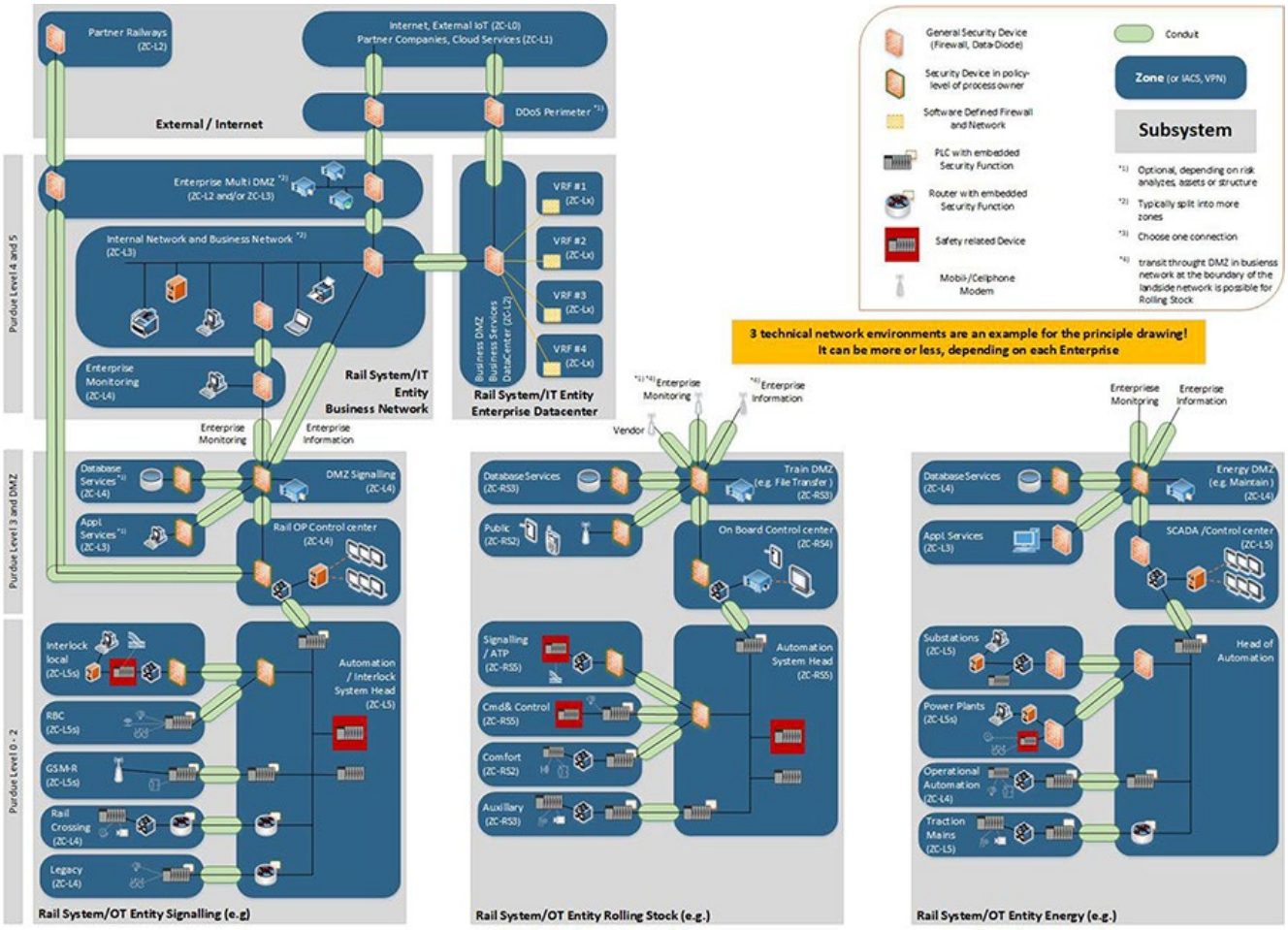
According to CLC/TS 50701, the Purdue model can be used to group the subsystems, functions, and assets into zones. The standard process of defining zones is documented in CLC/TS 50701 and EN62443-3-2, and leveraged in ENISA publication "Zoning and Conduits for Railways" as depicted in Figure 35:

- Zone and Conduit Requirements (ZCR) 1: Identify assets and Systems under Consideration (SuC)
- ZCR 2: Identify global corporate risks through an initial risk assessment
- ZCR 3: Perform zoning: zone, conduits, zone criticality (ZC) levels, communication matrix (CM), target security level (SL-T) for each conduit, and establish high-level zone model
- ZCR 4: Performance high-level risk assessment with the high-level zone model and the designated SL for exceeding risk
- ZCR 5: Check threats, identify countermeasures, and modify the high-level zone model to become final zone model
- ZCR 6: Document all information and results
- ZCR 7: Get alignment and approval from all stakeholders.

Figure 35 *Zoning and conduit methodology (source: ENISA "Zoning and Conduits for Railways")*

During the ZCR1 phase, assets shall be allocated in four groups corresponding to physical areas which include rolling stock, onboard, trackside, infrastructure, and the Operational control and maintenance center. Each asset is identified by its function and assigned a color using a five-color scheme to represent their functional classes: signaling network, command & control network, Auxiliary network, Comfort network, and Public network. In addition, assets should be grouped according to entity subsystems and process functions such as signaling and power energy. The result of this is an input to define the SuC and zone. Figure 36 illustrates the example of an individual railway zone model.

Figure 36 Example of an individual railway zone model (source: ENISA "Zoning and Conduits for Railways")



The objective for grouping the assets into zones and conduits is to identify the assets that share common cybersecurity requirements and group them to share the means of mitigation. The following aspects should be considered for the process of defining zones and conduits:

- The business assets (IT) and control assets (OT) should be separated into different zones.
- Safety-related assets shall be grouped in dedicated zones which are logically or physically separated from zones which are not safety related. However, if non-safety assets are allocated to such a zone, the complete zone is considered as safety related.
- Temporarily connected devices should be included in zones separated from assets that are permanently connected.
- Wireless devices should be included in zones separated from the ones with the wired devices.
- (Remote) Devices that are permitted to make connections should be grouped into a separate zone(s).
- Zones should contain the security device protecting the perimeter at the edges of conduits.

[Source: CLC/TS 50701]

After zones and conduits are defined, each zone should be assigned a Zone Criticality (ZC) based on the initial risk assessment. The criticality represents the security demands in a simplified expression to define the allowed communication between zones. Some of the basic rules in defining a communication matrix are in the following list.

- Direct communication between zones with well-known risks (e.g. zones with well-known and fixed mounted OT devices) and unknown risks (e.g. office zones with laptops, printer, internet connectivity) should be refused
- In general, direct communication is only allowed between zones with the same or a subsequent zone criticality
- The communication generally should be kept in the subsystem in order not to pass zones with other system responsibilities or different criticality.
- If border crossing communication between subsystems is necessary, data shall flow via the corresponding two DMZ.
- Communication into and out of zones should be well defined and be supervised for detecting unauthorized communication (e.g. by an intrusion detection system).
- Communication between different subsystems should be controlled by a security device (e.g. by a firewall).
- Communication between zones with the same criticality within a subsystem should be controlled by a security device.
- Communication between zones with different criticality within a subsystem should be controlled by a security device.
- All communication into and out of a subsystem should pass the same security device (or device group if redundant). No backdoors or parallel communication paths (like ISDN modem, etc. for direct remote maintenance), bypassing the corresponding security device, are allowed.

[Source: CLC/TS 50701]

- Remote maintenance access with a possible impact on system operations: direct access from business zones or from external sources to OT zones with higher security demands should not be allowed; external maintenance access (e.g. via Internet) should be grouped, controlled and forewarned in a separate internal zone, e.g. maintenance access via a B2B proxy in the technical DMZ
- Remote maintenance access without a possible impact on system operations: direct access from business zones or external to control zones without control by an internal security device or similar (e.g. proxy server) is allowed if the source (sensor, device, IoT-edge) and the sink (collecting server) are in special and separated zones; it is highly recommended, in order to guarantee the integrity of data, to encrypt communications via unsecure or untrusted networks

[Source: ENISA Zoning and conduits for railways]

APTA Zoning Model

This section summarizes the process of defining a security zone architecture based on the recommended practice from APTA – "Securing Control and Communications Systems in Rail Transit Environments, Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones". APTA has two working groups: APTA Enterprise Cyber Security Working Group and APTA Control and Communication Security Working Group, who is responsible to address the cyber protection requirements in different zones. See Table 5 for the definition of each zone.

Table 5 *APTA List of Zones Definition [Source: APTA]*

APTA Enterprise Cyber Security Working Group	
External Zone	The external zone includes Internet-accessible services, remote operations and facilities, and remote business partners and vendors. It is not trusted.

Enterprise Zone	The enterprise zone, or corporate zone, includes, where applicable, hardware and services that are made available to the control system via the agency's corporate network and includes agency business systems, fare collection systems, email, VPN, central authentication services, etc.
APTA Control and Communications Security Working Group	
Operationally Critical Security Zone (OCSZ)	The control center zone includes the centralized supervisory control and data acquisition (SCADA), train control, transit passenger information system, and other centralized control hardware and software, and the equipment from these control center zones extending out to remote facilities such as train stations and trackside equipment.
Fire, Life-Safety Security Zone (FLSZ)	The FLSZ contains any system whose primary function is to warn, protect or inform in an emergency. Examples are: emergency management panel, emergency ventilation systems, fire detection and suppression systems, gas detection systems and seismic detection systems.
Safety Critical Security Zone (SCSZ)	The SCSZ contains any system that if "hacked" and modified would cause an immediate threat to life or safety—for instance cause a collision or derail a train. Examples are vital signaling, interlocking and automatic train protection (ATP)

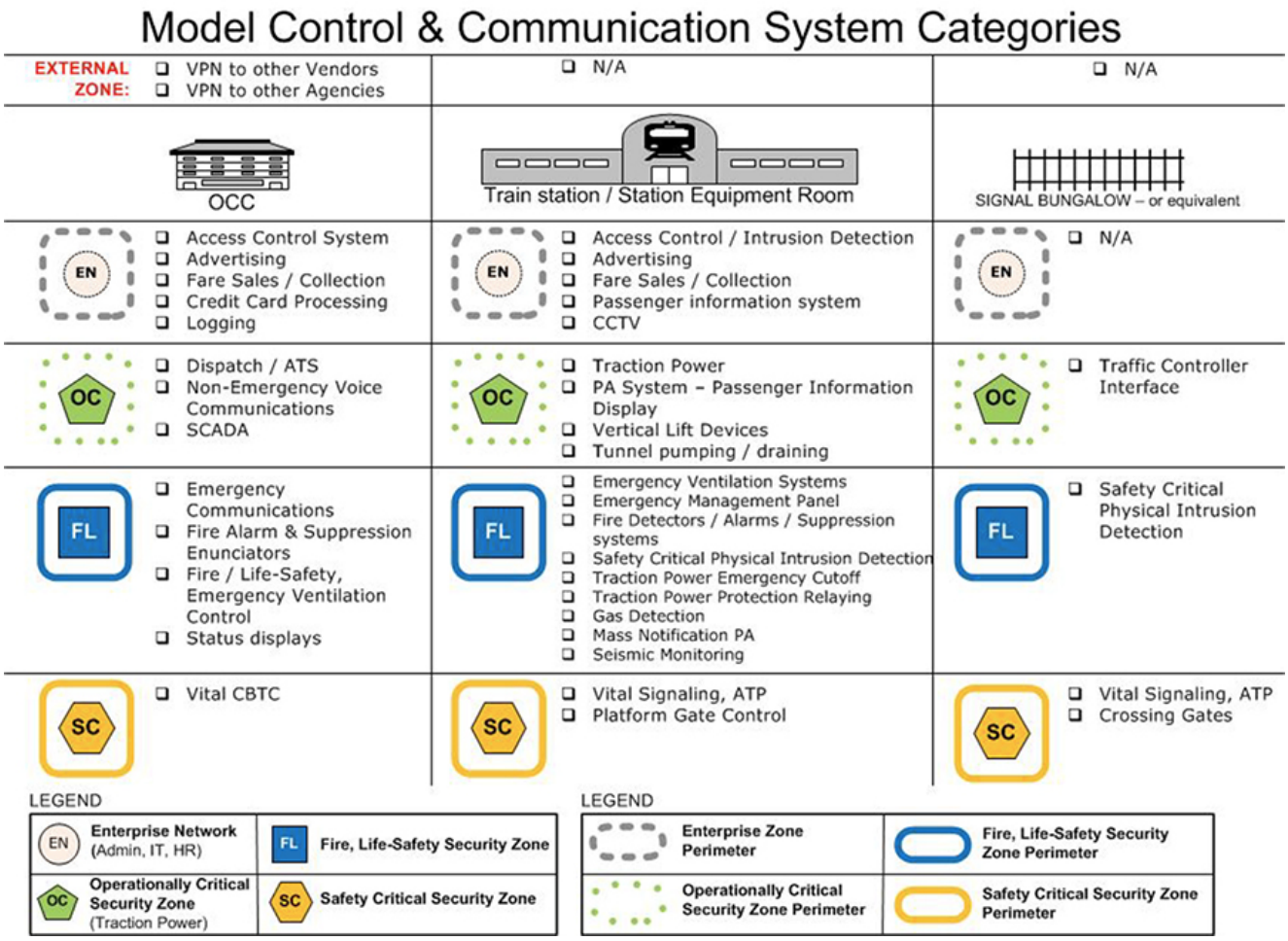
The zone model in rail transit is very similar to a well-defined manufacturing Purdue model, but there are some differences with a single manufacturing site:

- Distance: A rail transit systems covers much wide area and distance. It has various equipment deployed along the rail track that spans between a few to even thousands of miles.
- Communication: various communication methods are required to provide reliable connections between assets in different segments of the transit systems and control centers
- Power: Additional power is required to run all equipment including trains, signaling, and communication devices
- People access: The transit system needs to provide various access levels to different type of people, and large areas are open to the public
- Access to property: Transportation system assets are mostly out in the public; physical security needs to be applied to prevent and detect people accessing key areas such as bungalows and wayside equipment

Transit agencies must implement secure zones that cover vast space and distance. The following Figure 37 presents the allocation of different zones across different physical locations:

- Operation Control Center (OCC) and backup OCC (BOCC)
- Train Station
- Trackside (Signal Bungalow)

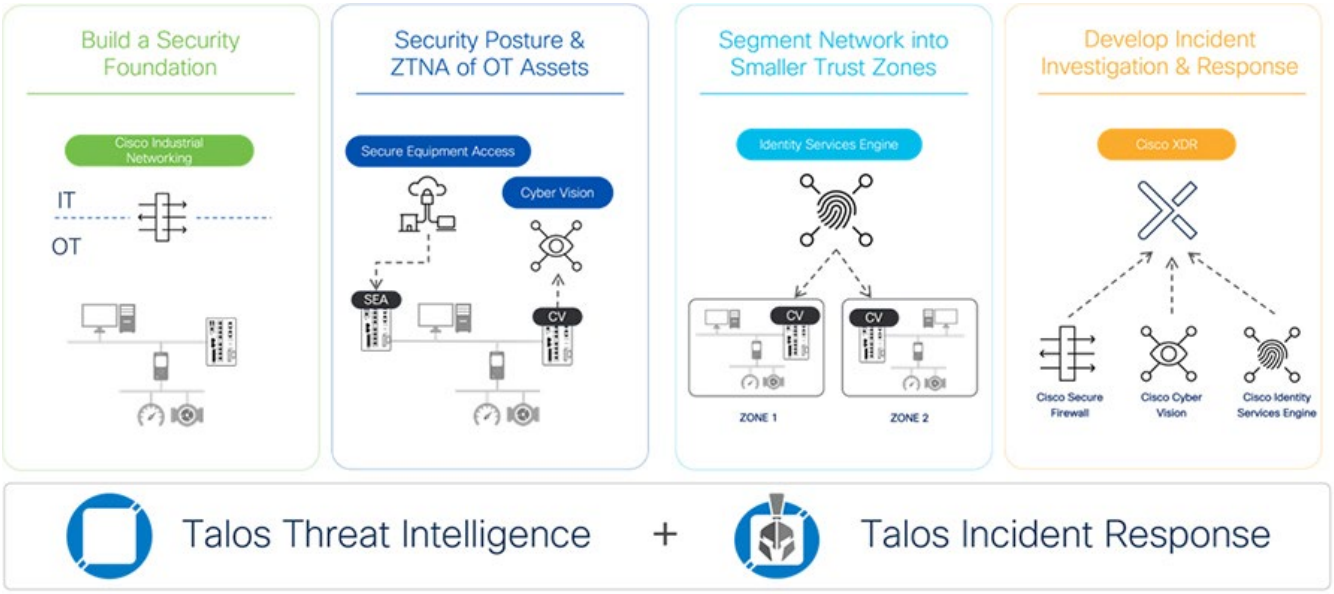
Figure 37 *APTA Model Zone Chart for Transit System*



Industrial Security Journey for Rail

This guide follows the industrial security journey defined in [Cisco Industrial Automation (IA) Security Design Guide 2.0] to help transit agencies build a secure industrial network in a phased approach. The design principles documented in Cisco IA security guide can be applied to transit agencies.

Figure 38 *Industrial security journey*



Building a Security Foundation

As depicted in Figure 38, building a security foundation is the first step in securing the transit systems. It is not uncommon in a transit system that OT traffic needs to reach the enterprise zone or the Internet (e.g. fare payment systems at station or remote access to the OT assets over the Internet). Industrial zones and enterprise zones should be separated to prevent any compromised IT system from impacting the OT operations and vice versa. To achieve this, a common deployment method is to create an Industrial Demilitarized Zone (IDMZ) network with a firewall to prevent traffic traversing directly between the IT enterprise network and OT operational network.

There are many industrial zones in a transit system, as depicted in Figure x, it has examples of signaling, rolling stock and Energy industrial zones. Similar to the industrial cybersecurity framework defined in IEC 62443, Figure 39 represents the cybersecurity framework for transit systems which includes the Industrial Zone, IDMZ, Enterprise Zone and External Zone. The Industrial Zone is composed of the cell/area zone and the site operations and control zone. Here are some definitions for each zone and each level:

Industrial Zone [Source: CLC/TS 50701]

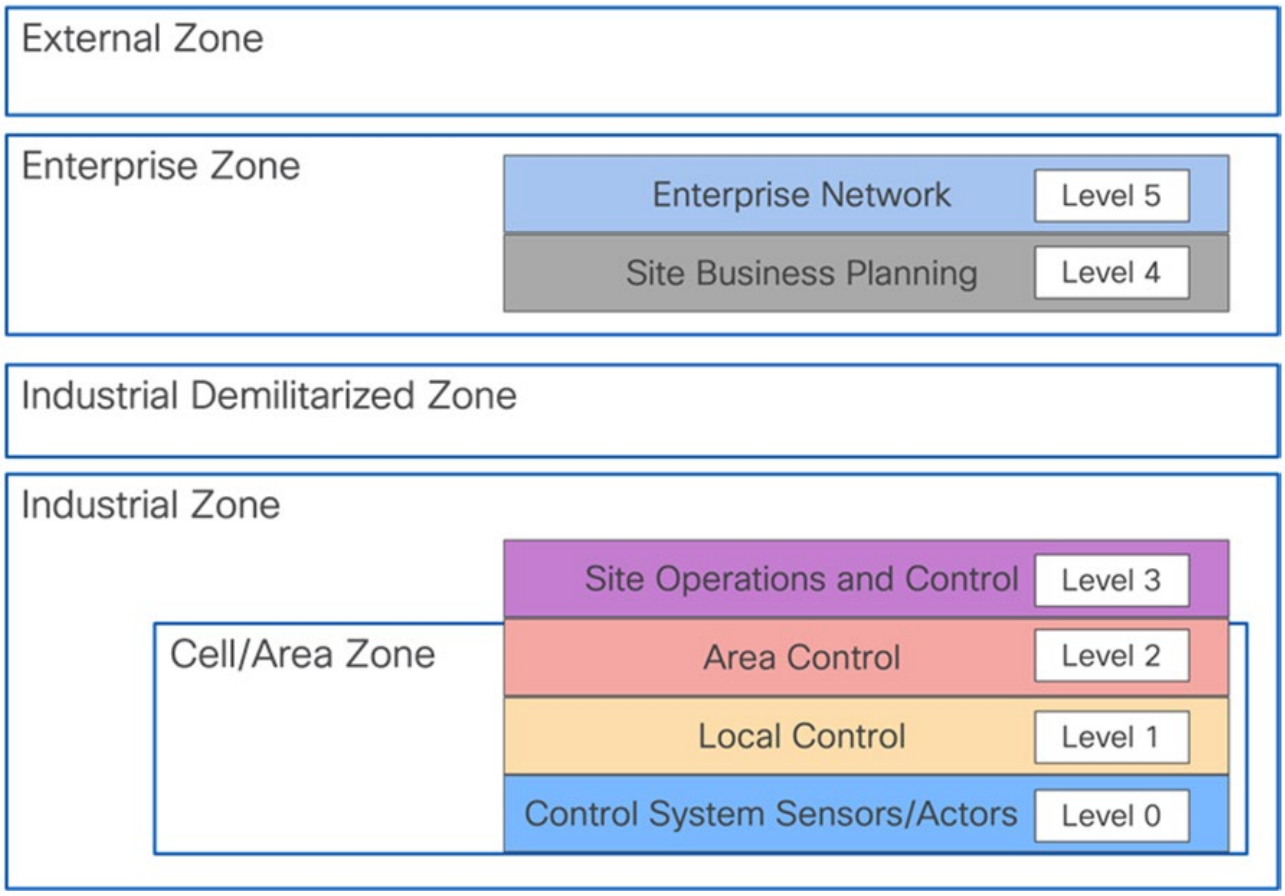
- Level 0: All (for example, axle counters, track circuits, odometers) and actors (for example, point machines, signals, brakes) that provide basic input and output of the control system
- Level 1: Local Control: All elements that receive input from sensors or provide output to actors, elements that process data and elements that send or receive data to or from an area control element.
- Level 2: Area Control: All elements that are required for area control or train control functions.
- Level 3: Overall Control: All elements that are needed for central control and business logic (as planning and disposition).
- Level 4+5: The Enterprise/Office network of the asset owner.

IDMZ and DMZ: IDMZ is used to separate industrial zone and enterprise/external zones. It restricts data transmission to that which is defined by the rules. There are DMZs at certain levels inside industrial zone, whose purpose is to control data flow between different subsystems. For instance, the traffic between rolling stock onboard systems and trackside signaling system needs go through the corresponding DMZ in each subsystem.

External Zone: This is external network that support business cloud services and partner companies.

For more information about design guidance for IDMZ, see Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense.

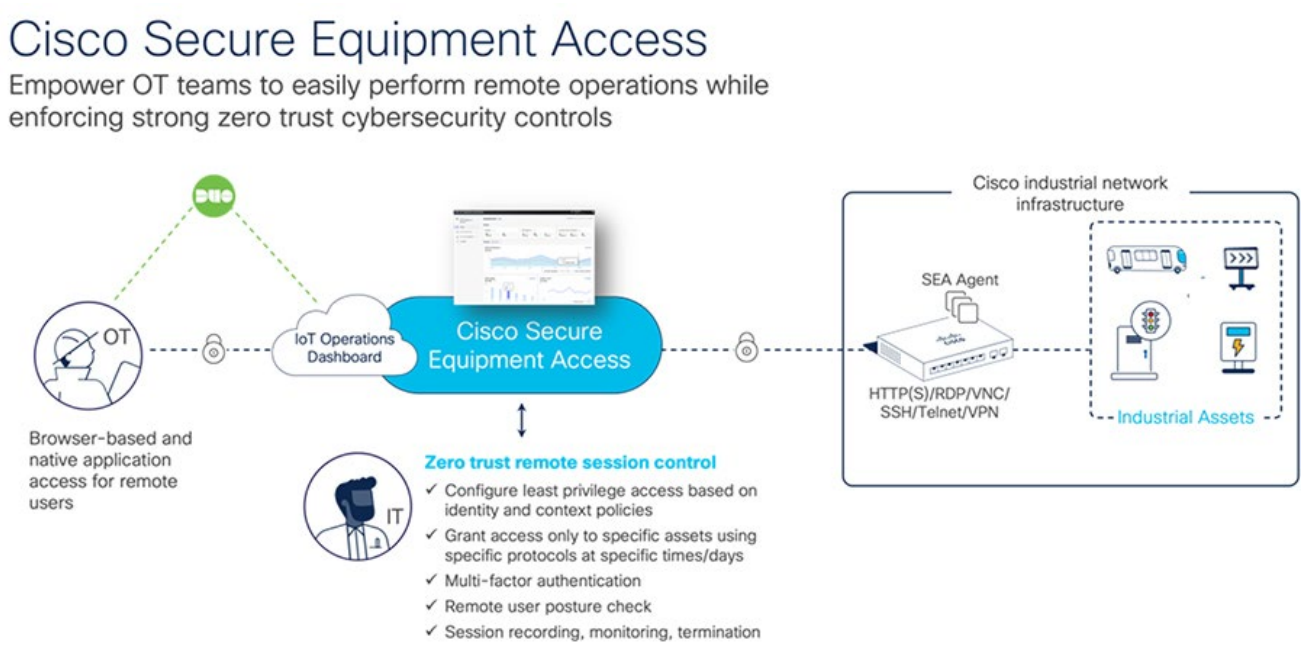
Figure 39 *Industrial Cybersecurity Framework for Transit System*



As part of separation between the Industrial zone and Enterprise zone, cybersecurity technical specifications like TSA measure C – "Implement access control measures, including those for local and remote access" often require remote access to the OT assets inside the Industrial zone from an external network zone. Cisco implements Zero Trust Network Access (ZTNA), a security service that verifies users and grants access to specific applications based on identity and context policies. ZTNA solutions connect authorized users directly to applications rather than to the network—and only to those applications they are authorized to access on need-to-know-based policies.

Cisco Secure Equipment Access (SEA) and SEA Plus as depicted in Figure x. are IoT Operations Dashboard services that enable operations teams to easily connect to remote assets or machines for configuration, monitoring, and troubleshooting. These services provide granular access controls that can easily be managed by an operations administrator, and secure connectivity for authorized users, including internal employees and external workers.

Figure 40 *Cisco Secure Equipment Access*



Using SEA, a worker can access a remote asset from anywhere simply by using a browser, without needing to install any additional software on their laptop. The remote equipment can be accessed using either GUI- or CLI based methods. Supported protocols are HTTP(S), SSH, RDP for Windows-based systems, VNC, and Telnet.

SEA Plus provides further flexibility by enabling users to configure any type of equipment that supports IP connectivity. With SEA Plus, a direct, secure data connection is created between client software on the user's computer and the remote asset, enabling the user to easily interact with and exchange files with the asset. SEA Plus supports IPv4 TCP, UDP, and ICMP based protocols. The feature provides users with the advanced ability to define specific channels for communications between a user and the remote system and block everything outside.
See Secure Remote Access for Industrial Networks guide for design guidance of SEA, Cisco DUO and Cisco Secure Endpoint.

Gain Asset Visibility and Device Posture

The second step of the journey is to provide complete visibility of all assets within the transit system. The transit system is a complex system that involves many different subsystems designed and manufactured by different vendors and installed by different partners at very dispersed locations. It is a combination of legacy and modern, proprietary and standards-based systems. To properly implement cybersecurity in the transit system, it is imperative for the organization to have full visibility of their OT assets and understand the normal state of the communication pattern between the assets.

Deep Packet Inspection (DPI) of the communication is a key means to visibility. 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. Solution providers generally provide DPI solutions in the following three architectures:

- Send all traffic to a central server that performs DPI
- Deploy dedicated sensor appliances on each network switch
- Send traffic to dedicated sensor appliances deployed throughout the network

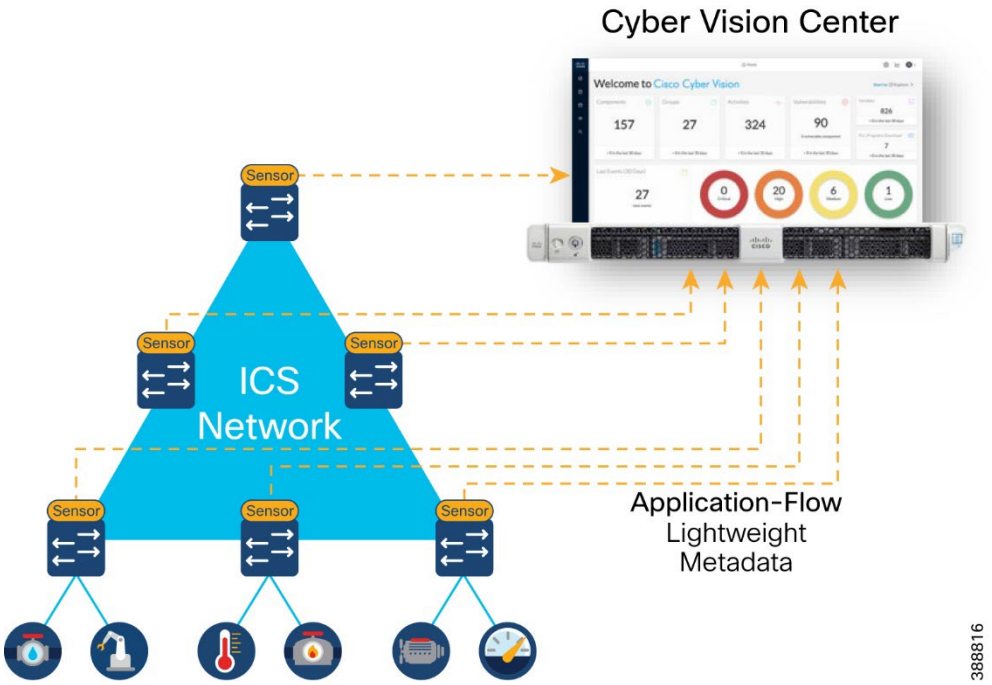
While these methods provide asset visibility, they also bring challenges. Sending all traffic to a central server requires duplicating communication flows which means double the bandwidth requirements and often requires a new out-of-band network to carry this traffic, which is costly and difficult to manage. Deploying a dedicated appliance on each network switch does remove the limitation of duplicating the traffic, but it is costly to scale. Cisco Cyber Vision delivers a better way to provide the complete visibility by embedding DPI capability into existing network hardware such as Cisco Catalyst Industrial Ethernet switches and Cisco Catalyst Industrial Routers.

Cisco Cyber Vision, illustrated in Figure 41, is composed of the Cyber Vision Sensor and Cyber Vision Center. Cyber Vision sensors are embedded in selected Cisco networking equipment as an IOx application and decode network traffic using DPI of industrial control protocols. It does not require dedicated appliances or an out-of-band SPAN connection. It only sends lightweight metadata to a central server which is called Cyber Vision Center. Cyber Vision Center stores data coming from the sensors and provides the user interface, analytics, behavioral analysis, reporting, API, and more. It may be run on a hardware appliance or as a virtual machine. This architecture only adds from 2% to 5% load to your industrial network. Some of the key features are:

- **Comprehensive Visibility:** Cyber Vision leverages a unique combination of passive and active discovery to identify all your assets, their characteristics, and their communications.
- **Security Posture:** Cisco Cyber Vision combines protocol analysis, intrusion detection, vulnerability detection, and behavioral analysis to help you understand your security posture. It automatically calculates risk scores for each component, device, and any specific parts of your operations to highlight critical issues so you can prioritize what needs to be fixed.
- **Operational Insights:** Cisco Cyber Vision automatically uncovers the smallest details of the production infrastructure: vendor references, firmware and hardware versions, serial numbers, rack slot configuration, etc. It identifies asset relationships, communication patterns, and more.
- **Incident Investigation and Response:** Cisco XDR is a security investigation and incident response application. It simplifies threat hunting and incident response by accelerating detection, investigation, and remediation of threats.
- **Snort IDS:** Cyber Vision integrates the Snort IDS engine in select platforms leveraging Talos subscription rules to detect known and emerging threats such as malware or malicious traffic.

For more information on Cisco Cyber Vision see the Cisco Cyber Vision Datasheet. The list of protocols supported by Cyber Vision are categorized by Field Network Communications, Distributed Control Systems, Automation and SCADA vendors, and Active Discovery Protocols. Some of the rail OT system relevant protocols are DNP3 and Goose for Power system automation, BACnet for Heating, Ventilation, Air conditioning (HVAC) systems, Rockwell Automation Ethernet/IP, Schneider Electrics Modbus, and Siemens Profinet. See Cisco Cyber Vision Protocol Support Datasheet for a complete list.

Figure 41 *Cisco Cyber Vision*



Cyber Vision design consideration is out of scope of this document. Please see [Cisco Industrial Automation (IA) Security Design Guide 2.0] for detailed information including Cyber Vision Center architectural recommendation, Cyber Vision sensor options and deployment model, brown and green field deployment considerations, ring topology considerations, passive and active discovery considerations, vulnerability assessment, risk score, Cyber Vision groups visualization, presets and baselines, and Cyber Vision IDS.

Segment Network into Smaller Trust Zones

Segmentation between the enterprise and industrial network is the foundation, but risk of breach remains. Malware could be introduced to the network using a rogue USB storage drive. This step of journey is to further segment the network into smaller trust zones. ISA/IEC 62443 defines a set of principles to be followed in Industrial environments:

- Least Privilege: to give users/devices only the rights they need to perform their work, to prevent unwanted access to data or programs and to block or slow an attack if an account is compromised
- Defense in Depth: multiple layered defense techniques to delay or prevent a cyberattack in the industrial network
- Risk Analysis: address risk related to production infrastructure, production capacity (downtime), impact on people (injury, death), and the environment (pollution)

Based on these principles, ISA/IEC 62443 recommends segmenting the functional levels of an industrial network into zones and conduits. In the previous sections of this chapter, the process of defining zones and conduits has been discussed, with examples of ENISA and APTA zoning model being given.
Different networking technologies can be used for segmentation:

- VLAN: A virtual local area network (VLAN) can be created on a Layer 2 switch to reduce the size of broadcast domains. A good security practice is to separate management and data traffic into different VLANs.
- VRF-lite: virtual routing and forwarding lite (VRF-Lite). The use of virtual routing and forwarding (VRF) technology allows you to virtualize a network device from a Layer 3 standpoint, creating different “virtual routers” in the same physical device.

- Access Control List: An Access Control List (ACL) is a series of statements that are primarily used for network traffic filtering. When network traffic is processed by an ACL, the device compares packet header information against matching criteria.
- Stateful Firewall: A firewall is a network security device that monitors the incoming and outgoing network traffic and decides whether to allow or block the traffic based on a defined set of security rules. a stateful firewall allows or blocks traffic based on the connection state, port, and protocol. Stateful firewalls inspect all activity from the opening of a connection until the connection is closed. Next-Generation Firewalls (NGFW) are stateful firewalls with additional features such as Application Visibility and Control (AVC), Advanced Malware Protection (AMP), URL filtering, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) decryption, and IDS/IPS.
- TrustSec: Cisco TrustSec (CTS) defines policies using logical device groupings known as Scalable Group Tag (SGTs).
    - Classification is the assignment of SGTs to an IP address. This assignment can be accomplished either dynamically or statically. In OT networks, where devices tend not to have 802.1X capabilities, dynamic classification can be done using MAC Authentication Bypass (MAB). Static classification is configured directly on the switch in which tagging occurs. Options for static classification include the mapping of Subnet, IP address, VLAN, or port to an SGT.
    - The transport of security group mappings can be accomplished through inline tagging or the SGT Exchange Protocol (SXP).
    - Enforcement is implementing a permit or deny policy based on the source and destination SGTs. This implementation can be accomplished with security group access control lists (SGACLs) on switching platforms and security group firewall (SGFW) on routing and firewall platforms.

To implement segmentation within the OT environment, two segmentation methods can be used:

- Macro-segmentation: Network infrastructure is divided into functional modules. Policy can be applied to larger functional zones based on subnet, VLAN or other network information. For example, assets in interlocking require no communication with assets in video surveillance.
- Micro-segmentation: micro-segmentation can be considered as segmentation within a VLAN segment. Cisco TrustSec role or SGT can be used as the means to describe permissions on the network, allowing the interaction of different systems to be determined by comparing SGT values.

Cisco Identity Service Engine (ISE) does not natively contain profiling services for industrial OT devices. Cisco Cyber Vision shares endpoints and attributes with ISE using pxGrid. When devices and components are placed inside groups, the group tag is also shared with ISE via pxGrid. After the group tag has been shared with ISE, a change of authorization (CoA) is sent to the access switch that the OT asset is connected to. This results in the asset reauthenticating with ISE, ultimately matching the new AA policy defined for this asset.

See Cisco Industrial Automation (IA) Security Design Guide 2.0 for detailed information about how to implement macrosegmentation and microsegmentation with Cisco Cyber Vision, TrustSec, and ISE.

Develop an Incident Investigation and Response Plan

The last step of the journey is to develop an incident investigation and response plan to reduce Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR). Solutions like Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) emphasize logs and analysis. The Extended Detection and Response (XDR) solution delivers a unified security incident detection and response platform that automatically collects and correlates data from multiple security components. It provides automation and orchestration capabilities to maximize operational efficiency.

Network Management Design

Rail transit systems are highly distributed systems that cover vast wide areas and distances with many use cases over a complex network infrastructure. Different use cases demand various network performance requirements such as latency, bandwidth, packet loss, redundancy, reliability, and scalability. Different connectivity options are also needed for different deployment scenarios that include Internet, cellular 4G/5G backhaul, Fiber, Ethernet, and Multiprotocol Label Switching (MPLS). In addition, the rail transit system is considered a national critical infrastructure and cybersecurity requirements are becoming more stringent than ever before. The network management solutions are not only required to simplify the network operation but also enable a broad set of cybersecurity capabilities.

Cisco Catalyst SD-WAN

Cisco Catalyst Industrial Routers offer the most reliable and secure connectivity for all your rail transit operations. Cisco Catalyst IR1100 rugged series routers are the most compact and modular SD-WAN router that support fixed deployment and provide secure connectivity to the assets along the track, at the station, and yard. It offers a variety of WAN options and expansion modules including Copper/SFP Gigabit Ethernet (GE), Next-generation 5G supporting standalone (SA) and non-standalone (NSA), a Cat-18/Cat-7/450 MHz LTE module, a LoRaWAN module, and an asynchronous serial port.

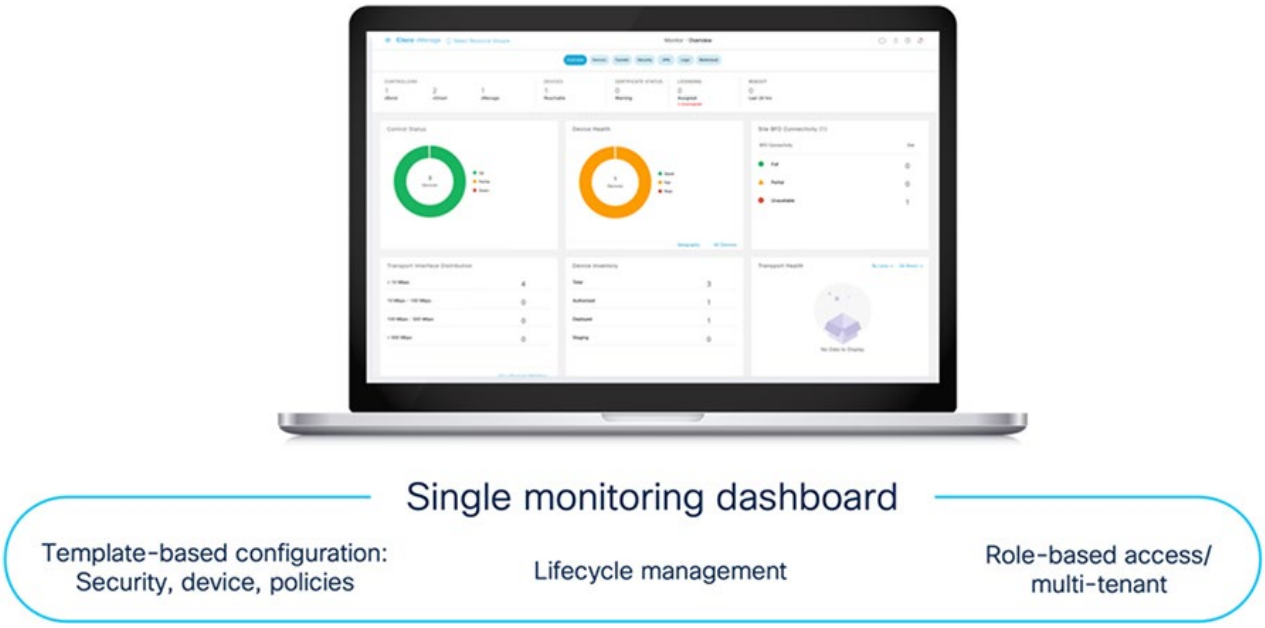
The Cisco Catalyst IR1800 rugged series router connects assets at gigabit speeds with 5G and Wi-Fi 6, supporting both mobile (e.g. onboard the train with M12 adapter, equipment handling vehicles at yard, fleet or high-rail maintenance vehicle) or fixed deployments with next-generation firewall capabilities built-in.

The Cisco Catalyst IR8300 rugged series router supports all-in-one routing and switching. It supports 5G, Catalyst SD-WAN, robust cybersecurity, and more. It integrates Cisco QuantumFlow and Unified Access Data Plan that delivers outstanding performance and can serve as a regional hub router.

By combining rail compliant and purposely built industrial ruggedized routers and the enterprise-grade market-leading Cisco Catalyst SD-WAN solution, Cisco offers a solution that can help transit agencies simplify their WAN operations and enable the security with the following benefits:

- Simplify network operations with automated provisioning and centralized configuration, management, and monitoring
- Deploy the WAN over any type of connection including Internet, MPLS, or 5G/LTE.
- Support on-premises or cloud-delivered deployment model
- Support application visibility and application-aware routing with real-time Service Level Agreement (SLA) enforcement
- Enables robust, comprehensive, and integrated security with consistent centralized security policy enforcement across a distributed transit network

Figure 42 *Cisco Catalyst SD-WAN Simplifies Network Operation and Enables Integrated Security*



Cisco Catalyst SD-WAN helps deliver integrated security to Cisco Catalyst Industrial routers:

- Next-generation firewall (NGFW) capabilities with application awareness and control, granular control, and integrated intrusion prevention
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) with Snort IPS *
- Advanced malware protection provides prevention, detection, and response in an all in one solution with behavior-based and artificial intelligence (AI) enabled malware detection *
- URL filtering to enable user to control the access to the Internet and protect against rogue web traffic *

*only available in IR1835 and IR8340

For design and configuration of key IoT related features available in Cisco Catalyst SD-WAN, refer to IoT Industrial Router Design Guide Extension to SD-WAN Small Branch Design Case Study.

Cisco Catalyst Center

Cisco Catalyst Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco Catalyst Center GUI provides network visibility and uses network insights to optimize network performance and deliver the improved user and application experience. A lack of network health visibility to network administrators and manual maintenance tasks like software upgrades and configuration changes are some of the common network challenges in enterprise networks. Software Defined Access (SDA) provides automated configuration and end-to-end segmentation to separate user, device, and application traffic without redesigning the network. However, SDA is not yet validated for deployment to support railway industry signaling applications like CBTC in this solution. This guide focuses on non-SDA (non-fabric) design.

Benefits of Cisco Catalyst Center include:

- Simplified deployment and automation of network maintenance and configuration tasks—Cisco Catalyst Center automation provides Zero-touch device provisioning, software image management, device replacement flows, and network provisioning tasks to facilitate device deployment, configuration, and maintenance at scale. Additionally, compliance checks are provided to guarantee the network is compliant with business intent.

- Network monitoring and analytics for proactive remediation—Cisco Catalyst Center Assurance enables every point on the network to become a sensor, sending continuous telemetry on application performance and user connectivity in real time. This, coupled with automatic path-trace visibility and guided remediation, means network issues are resolved in minutes—before they become problems.
- Consistent security policies for endpoints connecting to the network—The proposed architecture uses Cisco Catalyst Center, Cisco Identity Services Engine (ISE), and Cisco Cyber Vision to enhance the visibility of assets and interactions and create security policy to segment the network.

Key considerations when integrating Cisco Catalyst Center for a Rail Transit System:

- Cisco Catalyst Center is recommended to be placed in the industrial zone at Operation Control Center (OCC) and backup OCC (BOCC) with the following reasons:
    - Catalyst Center performs critical functions to maintain the operational status of the transit operation environment. Those critical functions include assurance and monitoring of the production network, guided remediation of identified problems and device replacement.
    - A separate instance for industrial environments helps ensure operational requirements are maintained. Industrial production environments have significantly higher and different operational requirements than an Enterprise system. A Catalyst Center instance that supports both Enterprise and Operation networks may lead to inadvertent changes or updates impacting the production system that could lead to downtime.
- Cisco Catalyst Center requires connectivity to all network devices it manages. That means that all devices that need to be discovered and monitored should have an IP address assigned that is routable and able to reach the Cisco Catalyst Center.
- Cisco Catalyst Center requires Internet connectivity to download software updates, licenses, device software, up-to-date map information and user feedback etc. It is recommended to use an IDMZ-based proxy service to provide this external communication. It is also recommended that you allow secure access via the proxy service only to URLs and fully qualified domain names required by Cisco Catalyst Center. For more details refer to *Cisco Catalyst Center Security Best Practice Guide*.
- If there is a firewall between Cisco Catalyst Center and managed devices, ensure that the required ports are allowed on the firewall. See “Required Network Ports” in *Cisco DNA Center Second-Generation Appliance Installation Guide* for a list of network ports that are required to be allowed by the firewall.
- Latency should be equal to or less than 100 milliseconds to achieve optimal performance for all solutions provided by Cisco Catalyst Center. The maximum supported latency is 200ms RTT. Latency between 100ms and 200ms is supported, although longer execution times could be experienced for certain functions including Inventory Collection and other processes that involve interactions with the managed devices.
- Cisco ISE must be deployed with a version compatible with Cisco Catalyst Center. Refer to the following link for compatibility information https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Some known limitations of Cisco Catalyst Center include the following:

- Cisco Catalyst Center does not support managing network devices with management IP address behind a Network Address Translation (NAT) boundary.
- Firewalls running Firepower Threat Defense (FTD) software are not supported on Cisco Catalyst Center. However, devices that are connected behind an industrial firewall can be provisioned and managed by Cisco Catalyst Center.
- REP ring provisioning using REP automation workflow is supported by Cisco Catalyst Center. However, the ring of rings (also known as a subtended ring) REP provisioning is not automated in Cisco Catalyst Center workflows. We recommend using the Day-N template feature in Cisco Catalyst Center for all day N configurations and subtended REP ring provisioning.
- Cisco Catalyst Center cannot manage products from third-party vendors.

Cisco Catalyst Center Network Management Flow

This section covers Cisco Catalyst Center network management flow including prerequisites, device discovery, device onboarding with Plug-n-Play (PnP), REP Ring provision, and Day N operations.

Prerequisite

- Establish the role-based access control in Cisco Catalyst Center, which is required to create users with correct privileges to perform Cisco Catalyst Center tasks introduced in the guide.
- Cisco Catalyst Center assigns users to roles that determine what types of operations a user can perform in the system. The following predefined roles are some of the roles supported by Cisco Catalyst Center:
    - Network Admin: Provision the network
    - Observer: Need assurance and inventory visibility
    - Super Admin: Only Cisco Catalyst Center system administrator
- Define a network hierarchy by creating sites. Sites group devices by physical location, function, or both in a network. The network hierarchy represents your network locations. It allows for a hierarchy of sites, which contain areas, and areas contain buildings and floors. A site on Cisco Catalyst Center determines which network settings, software images, and customized templates are applied to a device. We recommend that you create a network hierarchy in Cisco Catalyst Center based on area, train lines, and station names per different places in the network. Additionally, you can further define the site by its placement at the transit network architecture (Enterprise, IDMZ, Core, Backbone, Wayside wire, wayside wireless, and onboard network)
- Configure network settings that apply to created sites, including settings for device credentials, DHCP, and NTP servers. These network settings may be applied to devices that belong to a site as part of automation workflows.
- Create network profiles. For switches, network profiles link configuration templates to sites.
- A network profile is a key concept in Cisco Catalyst Center and is used to standardize configurations for routers, switches, and WLCs in one or more sites. A network profile is used to assign configuration templates to devices based on their site information, device product family, and associated tags. For devices that require similar configuration, a template helps to reduce configuration time by enabling configuration re-use and using variables and logic statements as placeholders for any unique settings per device.
- We recommend that you manage software images within the Catalyst Center image repository for network infrastructure upgrades. Cisco Catalyst Center stores all unique software images according to image type and version. It is possible to view, import, and delete software images.
- Establish network connectivity between Cisco Catalyst Center in the industrial zone and core switches (Catalyst 9300), the backbone aggregation switches (Catalyst Industrial Ethernet 9300), and the Wayside access switch (Catalyst Industrial Ethernet 3400/3300) network so that these devices can reach the Cisco Catalyst Center network. The switches in the core and station aggregation require some initial manual configuration to be discovered and added into the Cisco Catalyst Center inventory.

Device Discovery and onboarding

- The core switches (Cat9300) at OCC and BOCC in the CBTC reference architecture are discovered and added to Cisco Catalyst Center manually. This includes manual configurations of basic SSH, SNMP, user credentials, and routing configuration required to connect to Cisco Catalyst Center.
- Backbone station switches (IE9300) are connected to the core switch stack in a REP ring topology. They are onboarded using the Cisco Catalyst Center Plug-and-Play (PnP) feature. Day 0 templates must be created that include the trunk and allowed VLAN configuration, then power up the new switch to trigger the PnP process. For this to succeed, the ring must first be broken into two daisy

chains to ensure there is only one upstream switch (seed device) for the new switch to reach Cisco Catalyst Center for PnP. The ring can be broken at any desired point. For optimization, we recommend that the ring be broken in the middle. The switches are sequentially onboarded to Cisco Catalyst Center until the entire topology onboarding is complete. After completing the onboarding of all the station aggregation switches in the two daisy chains, verify they topology in the Catalyst Center. Lastly, connect the interface of the end nodes of the two daisy chains, which then transforms these two daisy chains into a backbone ring. Day N templates are then used to configure all interfaces as REP segments.

- If there are multiple REP rings required for the backbone network, repeat above steps for other backbone ring devices.
- Wayside access switches (IE3400/IE300) are connected to the station backbone switch as a REP ring or hub-spoke. In the REP ring topology, the process to onboard them is the same as the backbone station switches.
- Onboard train switches cannot be automatically onboarded using PNP because of the wireless network between the train and the wayside network. They must be configured manually and then discovered using the Discovery workflow in Cisco Catalyst Center.

REP Ring Provisioning Using Cisco Catalyst Center REP Automation Workflow

The Cisco Catalyst Center REP configuration workflow feature automates the provisioning of multiple IE switches in a ring topology. The ring topology is set up though a physical connection between two IE (base) switches that are onboarded into the Cisco Catalyst Center through PnP. The Cisco Catalyst Center non-fabric REP automation workflow feature considers an IE9300 switch as a REP edge device to form a closed REP ring with the IE switches that are connected to the same IE9300 switch. Here are some design considerations, limitations, and restrictions:

- Only new REP ring (greenfield) deployments are supported. An existing REP ring topology, if any (one may have been configured using Day-N templates), in the CBTC DCS backbone, can not be migrated to a new REP ring configuration using the Cisco Catalyst Center REP automation feature.
- Considering the IE9300 switch as the STP root bridge, a maximum of 20 nodes (including IE9300 switches and up to 19 IE switches) is supported in a ring with default STP ring parameter values.
- A switch that is connected in a REP Ring cannot be deleted from the Cisco Catalyst Center inventory until the REP ring that the switch is part of is deleted.
- Multiple rings within a REP ring are not supported. For example, multiple backbone REP rings or wayside access REP rings within a backbone ring cannot be provisioned using the Catalyst Center REP automation workflow. Using Day-N templates to provision such subtended rings.

Day N Operations and Templates

Cisco DNA Center provides an interactive template hub to author CLI templates. You can easily design templates with a predefined configuration by using parameterized elements or variables. After creating a template, you can use the template to deploy devices in one or more sites that are configured anywhere in your network. Templates allow you to define a configuration of CLI commands that can be used to consistently configure multiple network devices, reducing deployment time.

In this rail CBTC solution, the following day N configurations can be pushed to devices using the templates features in Cisco Catalyst Center:

- Configuration of additional VRFs and VLANs.
- Configuration of subtended REP ring
- Configuration of NetFlow monitor and flow exporter for Cisco Secure Network Analytics flow collection.

Additionally, network devices lifecycle management, which includes running configuration compliance checks, guided troubleshooting, software image management (SWIM), and network assurance features are included in day N operations and management.

See following guides for more information about Cisco Catalyst Center in Industrial IoT applications:

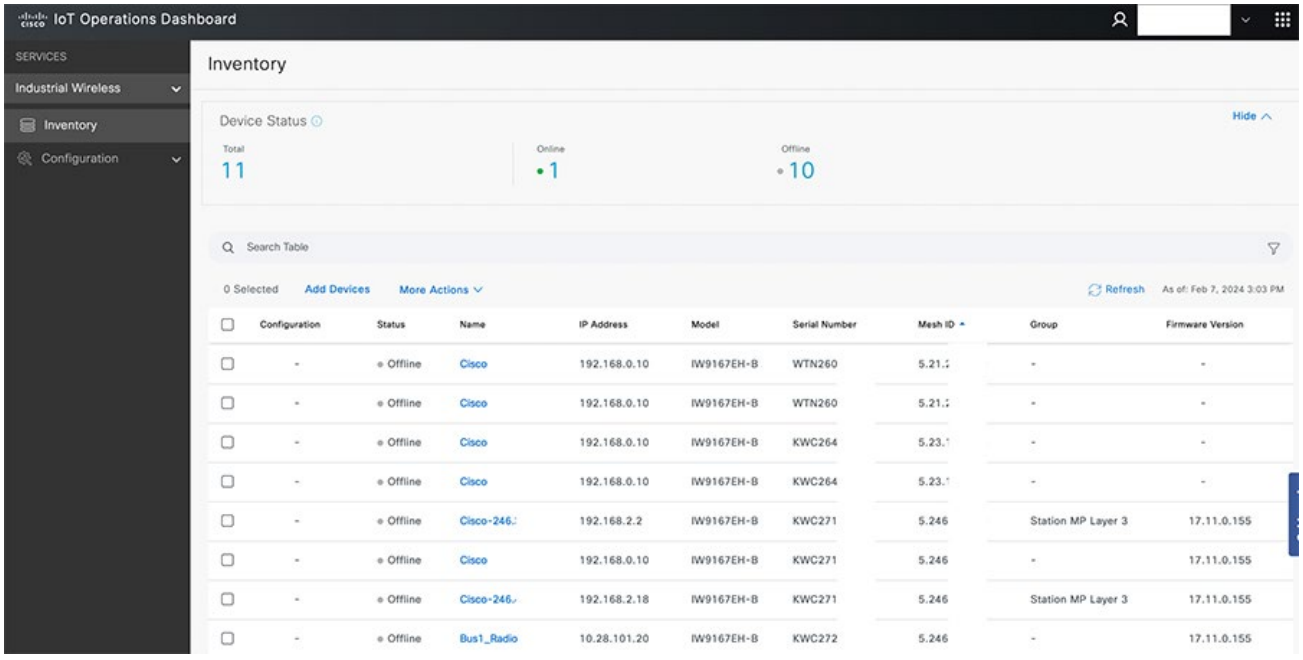
- Renewable Energy – Offshore Wind Farm Design Guide
- Renewable Energy – Offshore Wind Farm Implementation Guide
- Industrial Automation Network Design Guide

Industrial Wireless Service

Industrial Wireless Service in IOT Operations Dashboard (IoT OD) is an OT service used for configuring, provisioning, and monitoring URWB devices in a centralized location. The URWB devices can be onboarded through the wizard and all configurations and image versions are managed through the Dashboard. These configurations can then be manually pushed down to the URWB devices which will load the config, upgrade the firmware if necessary, and then automatically reboot with the new configuration. Additionally, configuration templates can be created to bulk configure devices with similar configuration parameters instead of maintaining a separate configuration per device. The dashboard also checks that the configuration running on the URWB device matches what is configured in the dashboard ensuring consistency across the mesh network.

By default, all URWB devices are configured to connect to the Dashboard which eases the process of provisioning new devices. If the URWB devices are unable to connect to the cloud dashboard, the service can still be used offline. When the devices are onboarded into the dashboard, they will show as offline if they have not connected to the Internet. All configurations can then be created and downloaded as a file. This file can be manually uploaded to the radio from the local GUI where it will apply the config and update the image if necessary. The radio will then reboot with the updated config. This is an effective way to reliably configure the URWB devices in case the mesh network is air-gapped or otherwise disconnected from the Internet.

Figure 43 *IW Service on IOT Operations Dashboard*

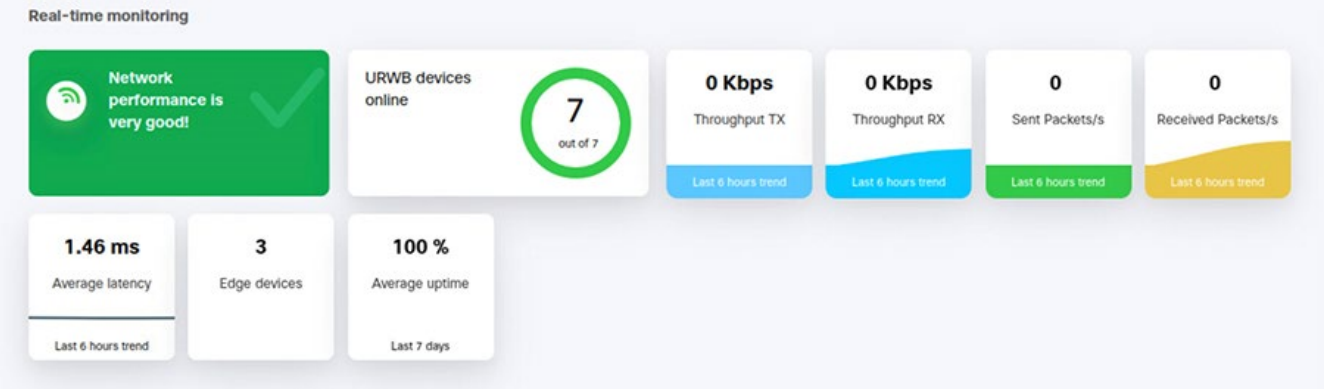


IW Monitor

IW Monitor is an on-prem application that monitors the mesh network real-time status and performance based on customizable KPIs without relying on SNMP. It can graphically display all URWB devices and the connections between them to see a bird's-eye view of the mesh network. This can also be overlaid on a scale map of the service area to show where devices are physically located.

The application is delivered as a Docker container instead of a dedicated appliance and requires reachability to all URWB devices. At the time of this writing, the IEC6400 cannot be monitored using IW Monitor.

Figure 44 *IW Monitor*



Crosswork Network Controller

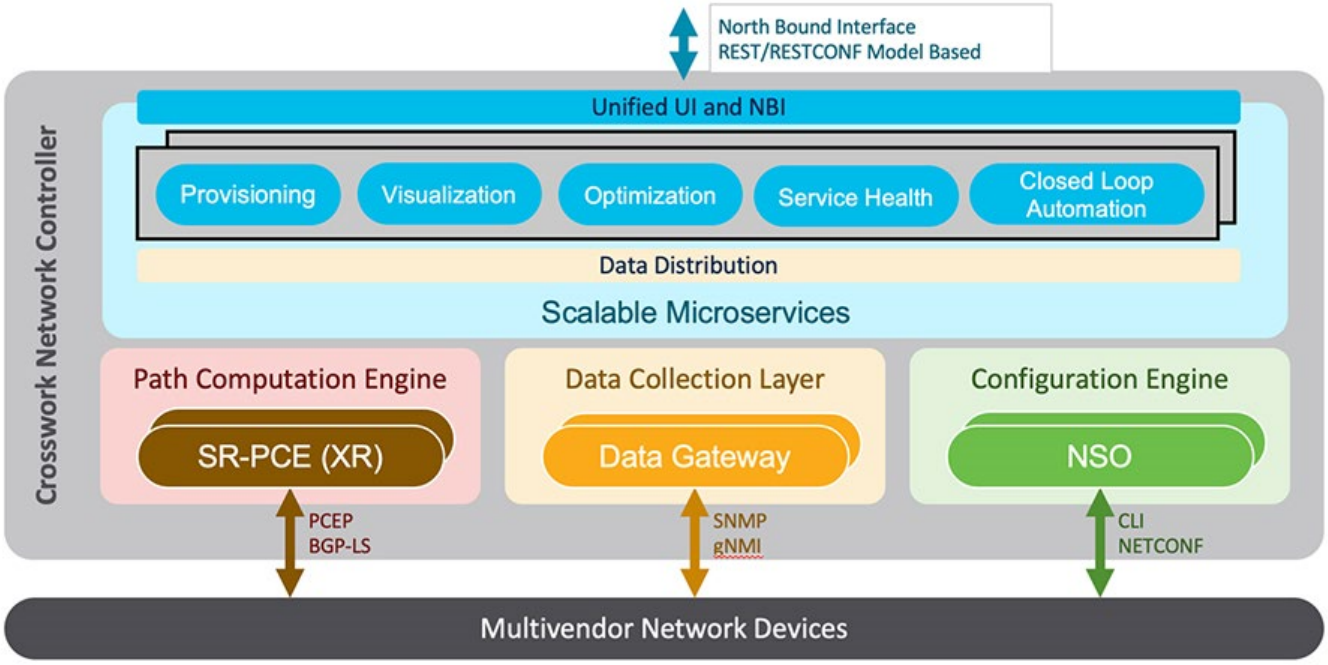
Cisco Crosswork Network Controller (CNC) automation suite offers a unified platform for seamlessly deploying, managing, and monitoring end-to-end transport networks with real-time visibility and control. Crosswork enhances customer experience by enabling real-time visualization of networks, and GUI-driven deployment of policies, VPN services, and traffic engineering with advanced SLAs over multi-vendor & multi-domain transport networks.

The Crosswork Infrastructure is a microservices-based platform, leveraging a cluster architecture to provide scalability and high availability (HA). Cisco Crosswork Data Gateway (CDG) is a foundational component of Crosswork. CDG is responsible for collecting device and interface statistics from the deployed network devices managed by Crosswork. This data is then analyzed and processed by the Crosswork applications, enabling efficient management of the network and adaptation to changes. The number of CDGs required to be deployed in the network is contingent on factors, for example, the number of devices, amount of collected data, network topology, and redundancy requirements.

CNC is Cisco's integrated automation product to effectively manage and operate end-to-end networks that includes key external components, such as Cisco Network Services Orchestrator (NSO), Segment Routing Path Computation Element (SR-PCE):

- SR-PCE: Cisco's IOS XR SR-PCE functionality enables real-time reactive feed via BGP-LS/ISIS/OSPF from the deployed topology's headend nodes across multiple domains. SR-PCE computes inter-area/domain/AS paths and enforces the computed SR-TE policies.
- NSO: NSO facilitates provisioning of services using service packages for VPN – L2VPN, L3VPN and Traffic Engineering Tunnels – SR-TE, SRv6-TE, RSVP-TE, and CS SR. NSO service packages use Network Element Drivers to provision device-level config across various vendors. A comprehensive ecosystem of NEDs is available supporting Cisco and other vendors, allowing for enhanced capabilities in multivendor service provisioning.

Figure 45 *Crosswork Network Controller Overview*



There are several other applications included with the overall Crosswork Network Automation suite which can optimize the overall Rail CBTC and Safety deployment.

- Crosswork Active Topology: CAT enables topology & service visualization via logical and geographical maps.
- Crosswork Optimization Engine: COE communicates with SR-PCE and NSO providers and makes the information available to Crosswork applications. COE offers real-time network optimization by leveraging SR-PCE and provides a graphical user interface for real-time visualization. The COE solution facilitates SR/SRv6 automation, congestion mitigation, traffic engineering through the user-friendly GUI.
- Crosswork Service Health: This component overlays a service level view and enables the customer to monitor the health of the services (for example, L2/L3 VPN) based on the rules established.

The MPLS transport network also benefits from these features:

- Intent-based Automated Provisioning: Services VPNs (L2 and L3VPN) & Transport SR-TE/SRv6/RSVP-TE
- Dynamic Traffic Engineering: Path Calculation for fine-grained path control and automated real-time optimization, BW aware path control, BW Congestion Detection & Mitigation, Scalable Telemetry collection for BW aware path calc, service and performance monitoring
- Integrated service lifecycle management: visualization demonstrating topology, overlay services & underlay p2p TE paths, automated Service Health Monitoring, Secure Zero Touch Provisioning, Monitoring performance and close loop automation to push changes
- Visualization of native SR paths: Visualizing the native path using the traceroute SR-MPLS multipath command to get the actual paths between the source and the destination can be achieved using Path Query. With Cisco Crosswork Network Controller, a traceroute command runs on the source device for the destination TE-Router ID and assists in retrieving the paths.
- Provision, Visualize, and Analyze Tree Segment Identifier Policies in Multipath Networks: Creating and visualizing static Tree-SID policies using the UI. Static mVPN Tree-SID policies associated with existing, or newly created, L3VPN service models (SR MPLS point-to-multi-point) using the Crosswork Network Controller that can also be visualized and analyzed to assist in efficient management and troubleshooting of your multicast network. Configuring link affinities used to specify the link attributes

that determine which links are suitable to form a path for the Tree-SID policy and maps each bit position or attribute with a color (making it easier to refer to specific link attributes). Modifying existing static Tree-SID policies and mVPN Tree-SID policies associated with an L3VPN service model – both edit and delete – using the UI.

For more details of the overall Crosswork Network Automation suite, go to this link: https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-automation/index.html

Conclusions

Cisco global experience working with transportation operators is unmatched. For over 20 years, our comprehensive solutions have been enabling more than 32,000 transportation organizations in 169 countries to drive digital transformation in transportation. With our partners, we continue to help our customers expand the boundaries of what is possible in transportation. As a global leader in networking and security, Cisco's Rail CBTC and Safety Solution incorporates the Industrial IoT portfolio that delivers end-to-end secure connectivity for the most extreme environments.

It leverages the industry-leading carrier-class version of the Cisco Network Convergence System portfolio to transform transit operators WAN architecture and deliver next-level business operation experiences. It also simplifies management and streamlines network operations with Artificial Intelligence (AI) powered Cisco Catalyst Center. This solution applies Cisco Zero Trust Network Access (ZTNA) industrial security guidelines to secure the nation's most critical infrastructure with the most stringent requirements of mission-critical applications and enables integrated security and easy WAN management with Cisco Catalyst SD-WAN.

The Cisco Connected Rail CBTC and Safety solution is built on a strong engineering process called Cisco Validated Design (CVD). The objective of the CVD is to deliver a well-designed, comprehensive, and fully validated end-to-end solution that is based on customer use cases requirements, integrated with Cisco and third-party technologies, to reduce the deployment risk, improve reliability, and confidently set performance expectations with documented best practices.

Acronyms and Initialisms

Term	Definition
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AI	Artificial Intelligence
AMP	Advanced Malware Protection
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
AVC	Application Visibility and Control
BGP	Border Gateway Protocol
BOCC	Backup Operational Control Center
CBTC	Communications-Based Train Control
CCI	Cisco Connected Communities Infrastructure
CCTV	Closed Circuit Television
CDG	Crosswork Data Gateway
CM	Communication Matrix
CNC	Crosswork Network Controller
CoA	Change of Authorization
CoS	Class of Service
CTS	Cisco TrustSec
CVD	Cisco Validated Design
DC	Data Center
DC	Data Confidentiality
DCS	Data Communications System
DHCP	Dynamic Host Configuration Protocol
DMZ	De-militarized Zone
DNS	Domain Name System
DPI	Deep Packet Inspection
EIGRP	Enhanced Interior Gateway Routing Protocol
ENISA	European Union Agency for Cybersecurity
FEC	Forwarding Equivalence Class
FHRP	First Hop Redundancy Protocol
FoV	Field of View
FP	FirePower
FR	Functional Requirements
FTD	Firepower Threat Defense
FW	Firewall
GE	Gigabit Ethernet
GoA	Grades of Automation
HA	High Availability
HSRP	Hot Standby Router Protocol
IA	Industry Automation
IAC	Identification and Authentication Control
IACS	Industrial Automation and Control Systems

IDS	Intrusion Detection System
IE	Industrial Ethernet
IoT OD	IOT Operations Dashboard
IPS	Intrusion Prevention System
ISE	Identity Services Engine
LER	Label Edge Router
L2TP	Layer 2 Tunneling Protocol
ICS	Industrial Control System
LSP	Label Switched Path
LSR	Label Switched Router
IT	Information Technology
MAB	MAC Authentication Bypass
MAC	Media Access Control
ME	Mesh End
MP	Mesh Point
MPLS	Multi-protocol Label Switching
MSN	Multi-service network
MTTD	Mean Time To Detect
MTTR	Mean Time To Repair
NAT	Network Address Translation
NIS2	Second Version of Network and Information Security
NIST	National Institute of Standards and Technology
NGFW	Next General Firewall
NGIPS	Next-Generation Intrusion Prevention System
NSA	Non-standalone
NSF/SSO	Non-Stop Forwarding with Stateful Switchover
NSO	Network Services Orchestrator
NTP	Network Time Protocol
OCC	Operational Control Center
OSPF	Open Shortest Path First
OT	Operation Technology
PCE	Path Computation Element
PE	Provider Edge
PnP	Plug and Play
PSN	Policy Services Node
pxGrid	Platform eXchange Grid
RA	Resource Availability
RADIUS	Remote Authentication Dial-In User Service
RDF	Restricted Data Flow
REP	Resilient Ethernet Protocol
RSVP	Resource Reservation Protocol
RSZW	Reduce Speed/Work Zone Warning
SA	Standalone
SCMS	Security Credential Management System
SD-Access	Software-defined Access
SDN	Software Defined Networking

SEA	Secure Equipment Access
SFC	Stealthwatch Flow Collector
SGACL	Security Group-based Access Control List
SGFW	Security Group Firewall
SGTs	Scalable Group Tags
SI	System Integrity
SIEM	Secruity Information and Event Management
SID	Segment ID
SL	Security Level
SLA	Service Level Agreement
SMC	StealthWatch Management Console
SOAR	Security Orchestration, Automation, and Response
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SR	Segment Routing
SR	Security Requirement
STCN	Segment Topology Change Notification
STP	Spanning Tree Protocol
SuC	System under Consideration
SVI	Switch Virtual Interface
SVL	StackWise Virtual Link
SWIM	Software Image Management
SXP	SGT eXchange Protocol
TE	Traffic Engineering
TLS	Transport Layer Security
TRE	Timely Response to Events
TSA	Transportation Security Administration
UC	Use Control
UCS	Cisco Unified Computing System
UDP	User Datagram Protocol
URWB	Ultra-Reliable Wireless Backhaul
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VN	virtualized network
VoD	Video-on-Demand
VRF	Virtual Routing and Forwarding
VXLAN	Virtual Extensible LAN
WLC	Wireless LAN Controller
WLAN	Wireless Local Area Network
XDR	Extended Detection and Response
ZC	Zone Criticality
ZCR	Zone and Conduit Requirements
ZTNA	Zero Trust Network Access
ZTP	Zero Touch Provisioning