Solution brief
Cisco public

The bridge to possible

Cisco Rail Communications-Based Train Control and Safety Solution Brief

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at https://www.cisco.com/site/us/en/about/contact-cisco/index.html.

Contents

Improving Safety, Maximizing Capacity, and Transforming Passenger Experience with Secure, Reliable Connectivity

According to the UITP World Metro Figures 2021 report, approximately 2,050 miles (3,300 km) of new rail infrastructure was put into service between the start of 2018 and the end of 2020, representing an infrastructure growth of 25% globally. During this time, 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, an increase of 20% from five years ago. Rail operators are constantly striving to keep their trains moving safely, provide superior and reliable services to their riders, and lower their operational cost.

Legacy fixed block signaling systems—systems that use signals to prevent a train from entering an occupied fixed section of track—can no longer meet the increasing demands for safety and efficiency. 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 meeting safety requirements. CBTC is used primarily in urban railway lines and automated people movers (APM), although it can be deployed on commuter lines.

On October 18, 2022, the United States Transportation Security Administration (TSA) released a new security directive, Enhancing Rail Cybersecurity -SD 1580/82-2022-01, due to the ongoing cybersecurity threat to surface transportation systems and their associated infrastructures. This security directive regulates passenger and freight railroad carriers through the implementation of layered cybersecurity measures, with a goal of reducing the risk that cybersecurity threats pose to critical railroad operations and infrastructures. Similarly, the European Union (EU) signed their second version of the Network and Information Security (NIS2) Directive, an EU-wide legislation on cybersecurity, in December 2022. It provides legal measures to boost the overall level of cybersecurity in energy, transportation, water, banking, financial markets, healthcare, and digital infrastructures. The deadline for EU member States to incorporate the NIS2 Directive into applicable, national law is October 17, 2024.

To successfully deploy CBTC and implement a cybersecurity plan, rail operators need a foundational network capability that is secure, scalable, reliable, and resilient. The Cisco Industrial IoT products are proven to meet the unique demands of operating in a rail environment, and the Cisco Rail CBTC and Safety solution provides a Cisco Validated Design (CVD) for reliably interconnecting high-speed trains, trackside infrastructure, stations, and operations centers across all of a rail operator's sites and regions.

Cisco Validated Designs provide the technologies, features, and applications that help you build the foundation for your intelligent transportation system priorities. 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 case requirements and integrated with Cisco and third-party technologies. The solution is intended to reduce deployment risks, improve reliability, and confidently set performance expectations with documented best practices.

Benefits of CBTC

Key benefits that CBTC offers rail operators include the following:

- **Improved safety**: With the implementation of CBTC, the location of a train can be determined accurately, independent of track circuits. The speed of a train can be regulated to protect trains against collision and excessive speed and maintain a safe braking distance and train separation. With additional functions such as programmed stopping, door control, route interlocking, work zone protection, and highway grade-crossing warnings, accidents and hazardous conditions can be significantly reduced.
- **Maximized capacity**: The key objective of deploying CBTC is to allow rail operators to better utilize their railway infrastructure, maximizing capacity by keeping the headway between operating trains at minimum while maintaining safety requirements.
- **Enhanced passenger experience**: CBTC enables trains to run closer together at higher speeds, meaning faster service to riders. With increased precision of train location information, the accuracy of real-time arrival information can be improved significantly. Riders can enjoy smoother rides and more consistent train operations because acceleration and braking are controlled by the system.
- **Reduced capital and operational expenses**: As CBTC technology evolves, the system is becoming more compact, and the architecture is getting simpler. With this evolution, less equipment is required at the wayside, and the equipment 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 schedules. CBTC provides flexibility that allows 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 operations. With automatic speed regulation provided by the system, unnecessary acceleration and braking are avoided, which leads to significant energy savings. With reduced power consumption and less air pollution, environmental sustainability is improved.

Network Challenges

Although CBTC brings tremendous benefits to rail operators, there are some key networking challenges that a rail operator needs to consider when deploying this solution:

Ultra-Reliable Train-to-Wayside Wireless Connectivity

Successful operation of CBTC relies on ultra-reliable, bidirectional, train-to-wayside wireless communication technologies when trains operate at high speeds. 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 across many locations, including rail cars and locomotives, maintenance vehicles, wayside, yards, terminals, and stations. A scalable and resilient network is needed to connect all 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. The network requires proven end-to-end security, high reliability, and scalability to many geographically separated locations. Managing network policies and assuring that they are properly implemented can be burdensome if done manually for each network node, so effective tools for automation and provisioning, centralized network management, service assurance, analytics and assurance, policies, and security are needed.

Due to the mission critical nature of CBTC operation and regional compliance requirements, rail operators typically deploy CBTC within a dedicated Data Communication Systems (DCS) whose sole responsibility is to deliver a highly redundant, reliable, and secure network that supports only CBTC operations. With proper technologies and designs in place, CBTC providers and rail operators can then implement a converged, multi-service network architecture to support both mission critical applications, such as CBTC, and non-mission critical applications, such as passenger Wi-Fi, video surveillance, ticketing, and so on. Network segmentation, zoning, and conduits are some of the key considerations for operating CBTC on a converged network infrastructure.

Cybersecurity

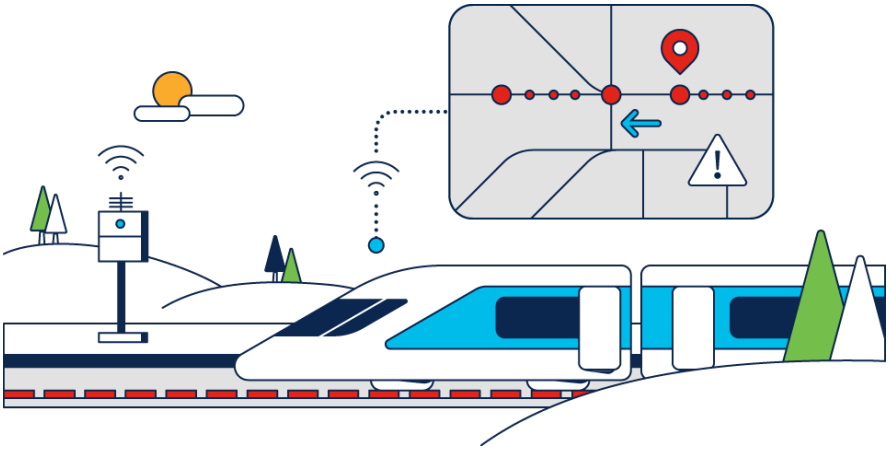
Cybersecurity attacks on rail systems can disrupt the flow of goods on freight lines, completely stop train operations, and degrade passenger services, disappointing the customers that rail operators are seeking to delight. Attacks on vital rail systems can cause shutdowns or, even worse, harm to human safety. With the digitization of operations that rail providers must achieve to remain viable and competitive, the need for strong cybersecurity is 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 considerations 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 to monitor whether users and devices on the network comply with those policies. These activities must be done in a way that enables a quick response to new threats and intrusions as they emerge.

Challenging Environment

Equipment that is installed onboard trains and on the trackside must meet industry standards that are established for protection against temperature variations, vibration, ingress of metallic dust and other particles, moisture, fire, electrical surges, and other challenges that are associated with rail operations. Equipment that does not meet the required specifications can result in costly system disruptions and repairs, shortened lifespans of assets, 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 an unpredictable and dynamic radio frequency environment.

The Cisco Rail CBTC and Safety solution validates the architecture that supports a high-speed, robust wireless connectivity between train and trackside. This solution also delivers a resilient and scalable access and backhaul transport infrastructure that connects wayside, stations, and operations centers across a rail operator's regions.



As shown in Table 1, rail operators and Cisco solution partners use the Cisco Rail CBTC and Safety solution as a secure foundation on which to build their solutions to support use cases that include 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	• CBTC • Data Communication System (DCS)	• Core network that supports data center applications for CBTC • Next generation 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 Automatic Train Supervision (ATS) servers, wayside zone controller, diagnostic data collector, and ATS workstations • Wayside network to support wireless trackside radio connectivity for train-to-wayside wireless communication • Onboard network to support connectivity to onboard CBTC components including train-bone controllers, operator displays, and onboard radios

Use Case	Type of Services	Description
Non-vital application	• Video surveillance • Passenger Information System	• Video surveillance at station and 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	• Integrate with axle counter for train detection • Integrate with axle counter for CBTC interlocking • Provide 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

Why Cisco for Transportation

Rail operators are modernizing to stay competitive. Cisco transforms rail operations for increased safety and efficiency, while boosting cybersecurity and operational agility. We understand the challenges that you face. We move the industry forward by bringing you technologies that can be integrated into both existing and new infrastructure to create safer, more efficient, sustainable, accessible, and equitable mobility. Our expanded portfolio offers practical, forward-thinking solutions for every mode of transportation.

Everything than you as a rail operator do, from roadway safety and trackside maintenance to asset visibility and logistics, depends on a strong, secure network. Your passengers, your employees, your cargo, and certainly your continued operations rely on it. Cisco offers intent-based networking built on the Cisco Digital Network Architecture that serves as your first line of defense, opens a wealth of knowledge to granular data insights, and equips you for mobile experiences on the go.

Growing social networks for transportation can expose thousands of endpoints that attackers can potentially use to get inside organizations' networks. Cisco's deep portfolio offers the industry's most comprehensive advanced threat protection across the broadest set of attack vectors. We help you build cyber resiliency into your networks, allowing you to stay agile enough to adapt and get creative.

Intelligent transportation systems are becoming increasingly popular as a foundation for connecting people, communities, and nations. And when implemented correctly, these systems can support technological growth by bringing disparate applications together. Technologies that enable these intelligent transportation systems can be only as powerful as those who wield them. And we want to help you build that bridge to solve, create, move, and inspire.

The pursuit of digital innovation involves a great number of moving parts. We work with an extensive and trusted ecosystem of partners that contribute unmatched industry expertise. These collaborators help us build technology solutions that matter to you.

Rail CBTC and Safety Reference Architecture

The primary function of the CBTC system is to provide high precision determination of a train location independent of track circuits. CBTC requires real-time train location and speed information so that it can send accurate instructions directly to a train operator, who relies on these instructions instead of trackside signals to operate the train. Continuous, reliable, bidirectional train-to-wayside data communications are needed to meet this requirement. A CBTC system is composed of three functions:

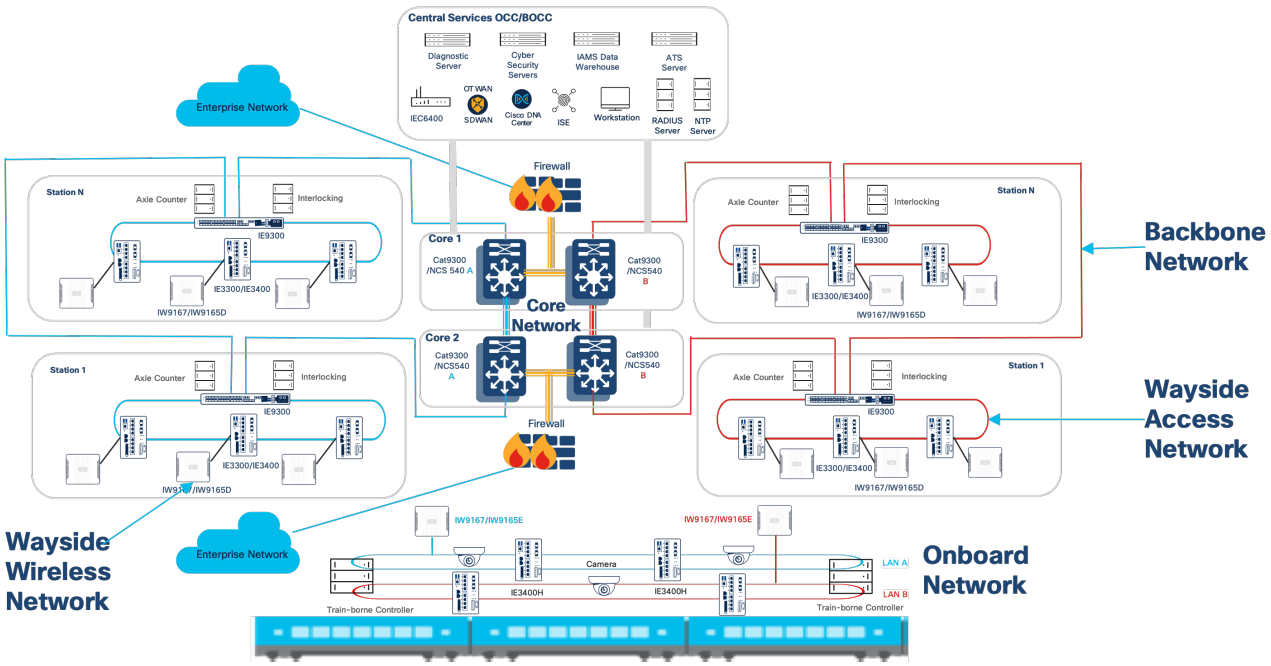
- Automatic Train Protection (ATP): Provides fail-safe protection against over speed, collisions, and other hazardous conditions.
- Automatic Train Operation (ATO): Responsible for automatic speed regulation, automatic station stopping and alignment, and train and platform door control.
- Automatic Train Supervision (ATS): Monitors and controls train movements in the entire rail operating system. ATS is responsible for tracking and displaying trains, providing route setting capabilities, and regulating train movements.

A CBTC should comprise major subsystems that include the following. As a recommended practice, the CBTC system is assumed to interface with an external separate interlocking system, which provides conventional interlocking functions based on train position.

- CBTC ATS system: Includes equipment that is responsible for ATS functions. This equipment is installed at central and wayside locations
- CBTC wayside system: Consists of a network of processor-based wayside controllers that are installed at central and/or wayside locations. Each wayside controller interfaces to the CBTC train-borne equipment via DCS and may interface to external interlocking and ATS equipment. The wayside also performs ATP functions.
- CBTC train-borne systems: Consist of one or more processor-based controllers and associated speed measurement and location determination sensors. The CBTC train-borne systems interfaces to the train subsystems and wayside equipment and ATS equipment via the CBTC DCS. The CBTC train-borne systems is responsible for CBTC train location determination, the enforcement of permitted speed and movement authority limits, and other ATP and ATO functions.
- CBTC data communication system (DCS): Includes network communication equipment at central and wayside locations and onboard trains to support data communications between the different subsystems. The data links between the major subsystems should provide bidirectional data transfer with sufficient bandwidth, ultra-low latency, and an extremely low packet drop rate, which are required by CBTC functions. The CBTC DCS should support timely and secure delivery of train control messages. DCS does not perform any CBTC vital functions itself, but careful network design is needed to ensure that DCS can meet the CBTC requirements.

The Rail CBTC and Safety solution is built on the premise that vital traffic must have redundancy built in at every level. This redundancy is achieved by designing a network with two completely separate physical networks. The packets traversing between every subsystem are duplicated on both networks to avoid any service disruption due to a single point of failure. This architecture, shown in the following figure, is designed with hierarchy and modularity in mind. It has a multi-tier model and functions that are grouped into modules so that it can easily be deployed and managed. The following sections describe these modules in detail.

The following figure shows the Rail CBTC reference architecture.



Onboard Train Network

The onboard train network provides ethernet connectivity to CBTC devices such as train-borne controllers and to non-CBTC systems such as CCTV cameras, passenger information systems, and passenger facing WIFI access points. The train-borne controller is installed on a specific car in a train. Each train has its own train-borne controller. Onboard train networks are fully redundant to ensure a reliable connection between components with no single point of failure. Each onboard train network is equipped with a rail certified Cisco Catalyst IE3400 Heavy Duty series switch and Cisco Catalyst IW9165E or Cisco Catalyst IW9167E Heavy Duty Series Access Points. Access points are connected to dedicated antennas that are installed on the top of the car in which the train-borne controller is installed.

Often, a train is composed of multiple train sets. A train set is composed of a fixed number of cars. Each train set could potentially join other train sets in different configurations, depending on the schedule for peak and off-peak hours. Each train set has one train-borne controller. A reliable and redundant DCS onboard network is required to facilitate communications between train-borne controllers in different train sets.

Wayside Wireless Network

The wayside wireless network is built with the Cisco Catalyst IW9165D Heavy Duty or IW9167E Series Access Points using Cisco Ultra-Reliable Wireless Backhaul (URWB) Fluidity technology. The Cisco Wireless Backhaul train-to-ground solution delivers continuous throughput at multiple Gigabits per second (Gbps) with seamless handoff and less than 10 ms latency for train speeds up to 217 mph (350 kmh). With its Fluidity make-before-break technology, Cisco URWB delivers zero packet loss during the handoff.

The RF design is largely dictated by the traffic requirements and a site survey of the train path. Each access point on each onboard network must use a different frequency to prevent interference between the two redundant onboard networks. At the wayside, there are redundant wayside wireless networks, and each one communicates with its respective onboard radio. Each wayside wireless network is responsible for coverage in two directions, up track and down track, and the overlap between two wayside wireless networks should be minimized. We recommend that the Cisco directional 2-port high gain panel antenna

(IW-ANT-PNL-515-N) for use at the wayside. And we recommend the rugged and low profile Cisco Directional Train Top Antenna (IW-ANT-SKS-514-Q) and Cisco Bi-Directional Train Top Antenna (IW-ANT-SKD-513-Q) for use onboard a train. The onboard access point antennas must be installed far enough away from the other access point antennas to prevent interference.

The mesh network design can use either layer 2 or layer 3 Fluidity. We recommend layer 2 for a smaller deployment where all radios in the mesh network are in the same broadcast domain and the data VLANs on the train are trunked end to end. If the mesh points or mesh end must cross a layer 3 domain, layer 3 Fluidity must be used. Seamless roaming in layer 3 is enabled between the mesh networks by using an IEC6400 Global Gateway.

Wayside Access Network

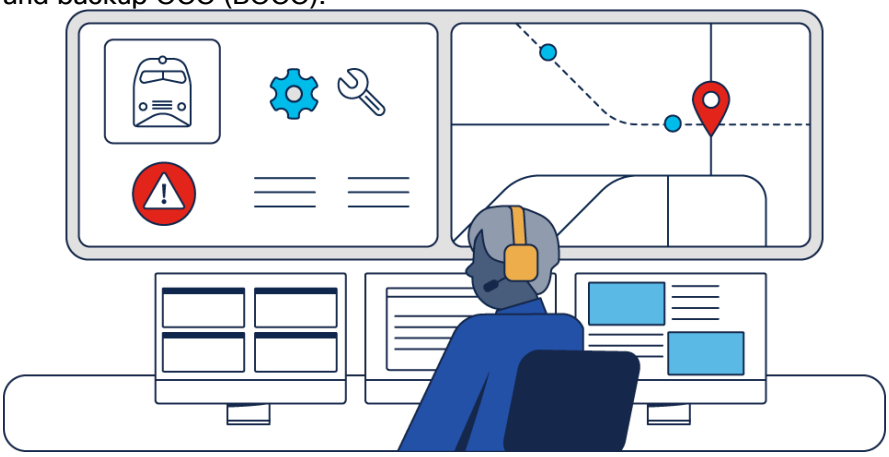
The wayside access network is composed of wayside switches that deliver ethernet connectivity to wayside servers such as local ATS servers and workstations, diagnostic servers, local zone controllers, and external systems such as interlocking and axle counters. It also provides connectivity to the wayside wireless network. The wayside access network is situated along the track or within bungalows near the track. In a bungalow, the wayside switches may be in unconditioned space or in a dusty environment subject to vibration from passing trains, depending on the bungalow construction. We recommend the Cisco Catalyst Industrial Ethernet Rugged series switch in the wayside access network because of its fanless and rugged design. When determining the model, it is important to size the switch for current use and future expansion. While the vital traffic may be low bandwidth, supporting CCTV and passenger traffic may be a future business need that requires much more bandwidth. We recommend the use of the Cisco Catalyst IE3400 or Cisco Catalyst IE3300 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, the wayside access network can be implemented as a ring or hub and spoke topology. A ring topology can most closely follow the layout of the track because the fiber can be installed in the same direction as the track and connect adjacent wayside switches. In this solution, Cisco Resilient Ethernet Protocol (REP) ring topology is deployed. which minimizes convergence during a failure. A hub and spoke design connects each wayside switch directly to the backbone switch and reduces the overall bandwidth compared to a ring topology. The disadvantages of this design include increased installation and fiber costs and decreased port density on the backbone switch.

Backbone Network

The backbone network connects the wayside access network to the core network. It carries CBTC wayside devices traffic and onboard traffic to the core network and delivers control messages and instructions to wayside and onboard devices. The backbone network provides high-speed, highly redundant forwarding services to move packets between access-layer devices in different sites of the network. The backbone network is composed of layer 3 network switches that typically are deployed at every station. Depending on the environmental conditions at 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. The stations are logically grouped into several rings, which terminate at the core switches. In this Cisco rail CBTC 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. These switches are the layer 3

gateway for all the wayside networks and have layer 3 reachability to the Operation Control Center (OCC) and backup OCC (BOCC).



Core Network

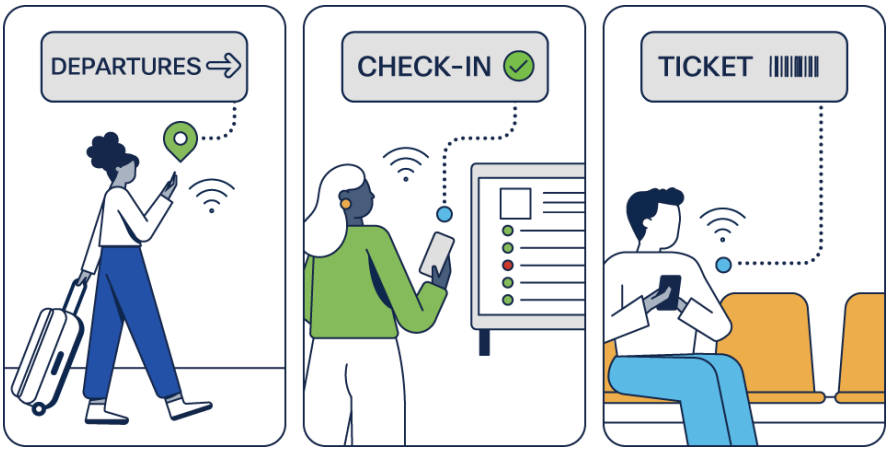
The core network is designed to enable the connection of the entire CBTC infrastructure. For redundancy, it has two core networks: OCC and BOCC, which are physically located at two different stations or buildings. Each core should have redundant power supplies, application servers, tools, and services enabled to operate the entire CBTC system in case either of the cores is completely down. There are two core network designs: layer 3 routing and Multi-Protocol Label Switching (MPLS) with Segment Routing (SR).

A layer 3 routing design is most similar to a standard enterprise core network that offers high performance and is highly resilient. In this solution, each OCC and BOCC core network has two nodes, with each node supporting a LAN path. Each node is a Cisco Catalyst C9300 that supports links that are greater than 10 Gbps. The node in OCC and BOCC supporting the same LAN are connected to each other via a portchannel., The nodes have full route reachability with each other to ensure that the best path is chosen through the core.

Large rail operators have adopted MPLS as the WAN transport network. MPLS is available in different variations, including IP/MPLS, MPLS – Transport Profile (MPLS-TP), and MPLS – Traffic Engineering (MPLS - TE). An MPLS-based transport network offers significant service capabilities but comes with a complex protocol stack, which makes it difficult to troubleshoot and operate.

Segment routing is a technology that is designed to address these pain points and can be applied to MPLS directly. Segment routing relies on extensions to Cisco Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) protocols. It simplifies the MPLS transport by removing the need for Label Distribution Protocol (LDP), Resource Reservation Protocol (RSVP), and Boarder Gateway Protocol-Labeled Unicast (BGP-LU) for inter-domain traffic. Segment routing reduces operational complexity and hardware requirements on the core devices while adding SDN capabilities for better network intelligence and insight.

Segment Routing is supported on several IOS-XR platforms In this solution the MPLS core with segment routing is built around the Cisco Network Convergence System (NCS) 540 Series. The NCS540 in the core forms a ring topology with backbone switches. The NCS540 does not support REP, so it requires a feature called REP Access Gateway (REP-AG) to tunnel the ring state information between them to ensure that a loop does not occur.



Security

Some transit agencies have been running their systems for periods that range from decades to more than 100 years. In the past, systems were composed primarily of proprietary hardware and software that communicated using non-standard protocols. These legacy systems either have no need to communicate with each other or the connections between the systems are over privately owned or leased dedicated wire connections.

In today's transit systems, control systems are starting to use commercial off-the-shelf hardware and software. Industry standard protocols and wired or wireless connections are used in architectures and system designs. Communications between different systems across large geographic areas are often required for operational efficiency. This communication requirement presents additional security vulnerabilities to transportation systems because of an increased attack surface.

Shared and converged infrastructure for IT and OT provides an effective approach to reducing capital and operational expenses and streamlining network management, and helps IT to gain OT asset visibility, understand communication patterns, detect vulnerabilities, and apply policies to secure the OT environment. The control systems for rail, as other industrial control systems (ICS), have real-time requirements for maintaining operational reliability, uptime, and safety. Due to the real-time requirement of the control systems, it is often required to carefully evaluate the delays introduced by the application of cybersecurity technologies.

The Cisco Rail CBTC and Safety solution leverages the design that Cisco Industrial Automation (IA) Security Design Guide 2.0 describes to implement zero trust network access (ZTNA) and a defense-in-depth approach to secure a rail transit systems. The approach is as follows:

- **Build a security foundation:** In a transit system that, OT traffic often needs to reach the enterprise zone or the Internet directly (for example, fare payment systems at stations or remote access to OT assets over the internet). Industrial zones and enterprise zones should be separated to prevent compromised IT or OT operations from affecting each other. Similar to the industrial cybersecurity framework that is defined in ISA/IEC 62443, the transit cybersecurity framework includes an industrial zone, industrial demilitarized zone (IDMZ), enterprise zone, and external zone. Cisco Secure Firewall helps build the security foundation to segment industrial zones and enterprise or external zones, detect and block threats faster, and gain deeper visibility with greater performance.
- **Gain asset visibility and device posture:** A transit system is a complex system that involves many different subsystems that are designed and manufactured by different vendors and installed by different partners. It is a combination of legacy, modern, proprietary, and standards-based systems. To properly implement cybersecurity in a transit system, it is imperative for an organization to have full visibility of their OT assets and understand the normal state of the communication patterns between the assets. Cisco Cyber Vision automatically builds a comprehensive inventory of assets and their communications activities. These assets include onboard automation and trackside electrification devices. Cyber Vision combines protocol analysis, intrusion detection, vulnerability detection, and behavioral analysis to help

better understand security posture. Cyber Vision also calculates risks scores to help prioritize risks to be remediated. It integrates the Snort IDS engine in select platforms, leveraging Talos subscription rules to detect known and emerging threats such as malware or malicious traffic.

- **Define zone and conduit:** ISA/IEC 62443 Part 3-3 requires segmenting a network into small zones of trust where assets can communicate only with other assets needed to run the industrial process. In the context of this rail CBTC solution, the industrial process can be referred as CBTC communication between train-borne controllers and wayside local ATS server. There are three zoning models used in the industry:
    - According to technique specification CLC/TS 50701 – Railway applications – Cybersecurity, the Purdue model, a structural model for industrial control system (ICS) security, can be used to put subsystems, functions, and assets into zones.
    - The European Union Agency for Cybersecurity (ENISA) recommends that assets be allocated into four zones that corresponding to physical areas that 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 its functional class: signaling network, command and control network, auxiliary network, comfort network, and public network.
    - Similarly, the American Public Transportation Association (APTA) zoning model assigns each asset to one of the following zones: external zone, enterprise zone, Operational Critical Security Zone (OCSZ), fire and life-safety security zone (FLSZ), and Safety Critical security Zone (SCSZ).

  A conduit supports and defines allowed communication between two or more zones. The objective for grouping assets into zones and defining conduits is to identify the assets that share common cybersecurity requirements and group them to share the means of mitigation. Cyber Vision, together with Cisco Identity Services Engine (ISE), can build these segmentation policies and work with Cisco industrial network equipment to enforce them without the need for additional hardware.
- **Implement zero-trust remote access:** As part of separation between the industrial zone and enterprise zone, cybersecurity technical specifications such as TSA measure C – "Implement access control measures, including those for local and remote access" often requires zero-trust remote access to secure and prevent unauthorized access from an external network zone to the OT assets that are inside the Industrial zone. This approach requires implementation of policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Cisco Secure Equipment Access (SEA) enables Zero Trust Network Access (ZTNA), a security solution 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 applications users are authorized to access per need-to-know-based policies.
- **Develop an incident investigation and response plan:** Develop an incident investigation and response plan to reduce mean time to detect (MTTD) and mean time to respond (MTTR). Solutions such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) emphasize logs and analysis. Cisco Extended Detection and Response (XDR) solutions deliver 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.

Management

Rail transit systems are highly distributed systems that cover wide areas and distances over a complex network infrastructure. Different use cases have various network performance requirements, including requirements for latency, bandwidth, packet loss, redundancy, reliability, and scalability. Different connectivity options are needed for different deployment scenarios. These options include internet, cellular 4G or 5G backhaul, fiber, Ethernet, and MPLS. In addition, the rail transit system is considered to be a national critical infrastructure, and cybersecurity requirements for these infrastructures are becoming more

stringent. Network management solutions are required to simplify network operations and to enable a broad set of cybersecurity capabilities.

Cisco Catalyst SD-WAN

Cisco Catalyst SD-WAN helps transit agencies simplify their WAN operations and enables security with the following benefits:

- Simplified network operations with automated provisioning and centralized configuration, management, and monitoring
- Deployment of a WAN over any type of connection, including internet, MPLS, 5G or LTE
- On-premises or cloud-delivered deployment model
- Application visibility and application-aware routing with real-time Service Level Agreement (SLA) enforcement
- Robust, comprehensive, and integrated security with consistent centralized security policy enforcement across a distributed transit network

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 (available with the Cisco IR1835 Router and Cisco Catalyst IR8340 Rugged Series Router).

Cisco Catalyst Center

Cisco Catalyst Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across a network environment. The Cisco Catalyst Center UI provides network visibility and uses network insights to optimize network performance and deliver improved user and application experiences.

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 that 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, which provide continuous telemetry about application performance and user connectivity in real-time. This capability, coupled with automatic path-trace visibility and guided remediation, allows network issues to be resolved in minutes—before they become problems.
- Consistent security policies for endpoints connecting to the network: The Rail CBTC and Safety Reference 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 policies to segment the network.

Cisco Industrial Wireless Service

Cisco Industrial Wireless Service (IW Service) is an OT service in the Cisco IoT Operations Dashboard and offers a suite of tools for configuring, deploying, provisioning, and monitoring Cisco URWB devices from a single cloud-based dashboard. It helps operations team by simplifying device configuration, improving scalability and efficiency with zero-touch provisioning, providing visibility into configuration mismatches and versions, and offering advantages even in cases where offline configuration is necessary.

Crosswork Network Controller

Cisco Crosswork Network Controller (CNC) offers a unified platform for seamlessly deploying, managing, and monitoring end-to-end transport networks with real-time visibility and control. Crosswork Network Controller enhances the customer experience by enabling real-time visualization of networks and UI-driven deployment of policies, VPN services, and traffic engineering with advanced SLAs over multi-vendor and multi-domain transport networks. CNC is Cisco's integrated automation product for the effective management and operation of end-to-end networks. It combines some key capabilities, such as Cisco Network Services Orchestrator (NSO) and Segment Routing Path Computation Element (SR-PCE).

Ecosystem Partners

Ecosystem partners are vital in the successful deployment and operation of Cisco Rail CBTC and Safety solutions. Frauscher Sensor Technology has been a world leader in the design and manufacturing of cutting-edge wheel sensors and axle counting technology for more than 35 years. They have successfully completed major projects worldwide and installed their solutions for rail operators in all categories, including freight railroad, major transit, metro, light rail, commuter rail, and short lines. Their applications range from CBTC secondary systems to primary train detection, speed enforcement, grade crossing warning, yard automation, and more.

The Cisco Rail CBTC and Safety solution provides ecosystem partners with a fully validated network architecture that is secure, segmented, and highly available, It is the ideal solution for vital applications such as CBTC and axle counting, which require ultra-low latency, minimum packet loss, and full redundancy. Each of Frauscher's applications can build on the Cisco rail architecture. Together, Cisco and Frauscher can deliver a better solution that can be offered to our mutual rail customers.

"We recognize Cisco's dedication to the rail industry through its validated solutions and extensive product portfolio. Cisco's CVD initiative allows industry partners to establish a safe and reliable network interface between Frauscher axle counters and higher ranking signaling systems. We appreciate Cisco's emphasis on fostering strong relationships with ecosystem partners and are confident that our collaboration will yield enhanced solutions for our joint customers' evolving needs."

- Michael Parzer
Executive Director, Frauscher Sensor Technology

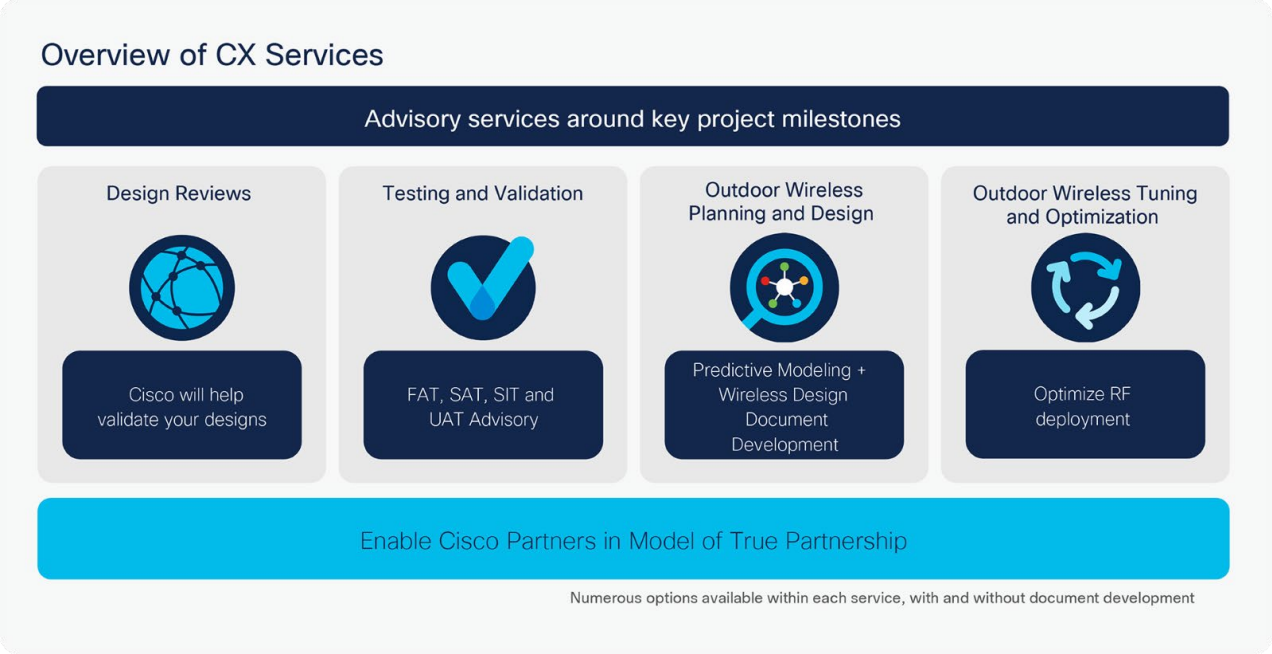
Cisco Customer Experience

In today's rapidly evolving OT and industrial spaces, customers and systems integrators are challenged to keep pace with new technology trends to ensure that projects are delivered in a cost-effective manner. With Cisco's suite of, our partners and customers can reduce solution implementation risk on projects that leverage Cisco IoT technologies in a true model of partnership with Cisco. With simplified packaging, a flexible consumption model, and advisory services covering each key project milestone, this suite of services allows operators to enter new markets with the confidence to expand and grow their businesses.

Cisco's CX Industrial Networking and Security services help rail and transportation operators accelerate the digitization of their existing operations by using a unique architecture-based approach to service delivery. Cisco CX leverages strategy development, architectural assessments, network design, migration and deployment assistance, and support services to help Cisco's key ecosystem partners plan, build, and manage solutions.

These partner-built solutions focus on business outcomes that result in improved worker and passenger services and safety, risk mitigation, higher productivity, improved operational efficiency, and deeper intelligence and insights, with security at the core of the end-to-end solution.

The following figure shows an overview of the Cisco CX services.



With more than 30 years of industrial networking experience, Cisco is uniquely positioned to address new demands on industrial networks, which require a greater need for improved interconnectivity across industrial equipment and enterprise networks. Our proven processes and tools deliver consistent results based on best practices and strong communication. Our experts deliver services that allow organizations to accelerate the integration and transformation of their current infrastructure to the next-generation network, which is capable of evolving operations to continue to meet the evolving demands of the business.

Conclusion

Cisco's global experience working with transportation operators is unmatched. For more than 20 years, our comprehensive solutions have enabled 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 infrastructures with the most stringent requirements of mission-critical applications and enables integrated security and easy WAN management with Cisco Catalyst SD-WAN.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.