Next Stop, Future-Ready Mass Transit

How to Ensure Your Trackside (Wayside) Networks Meet the Demands of Tomorrow

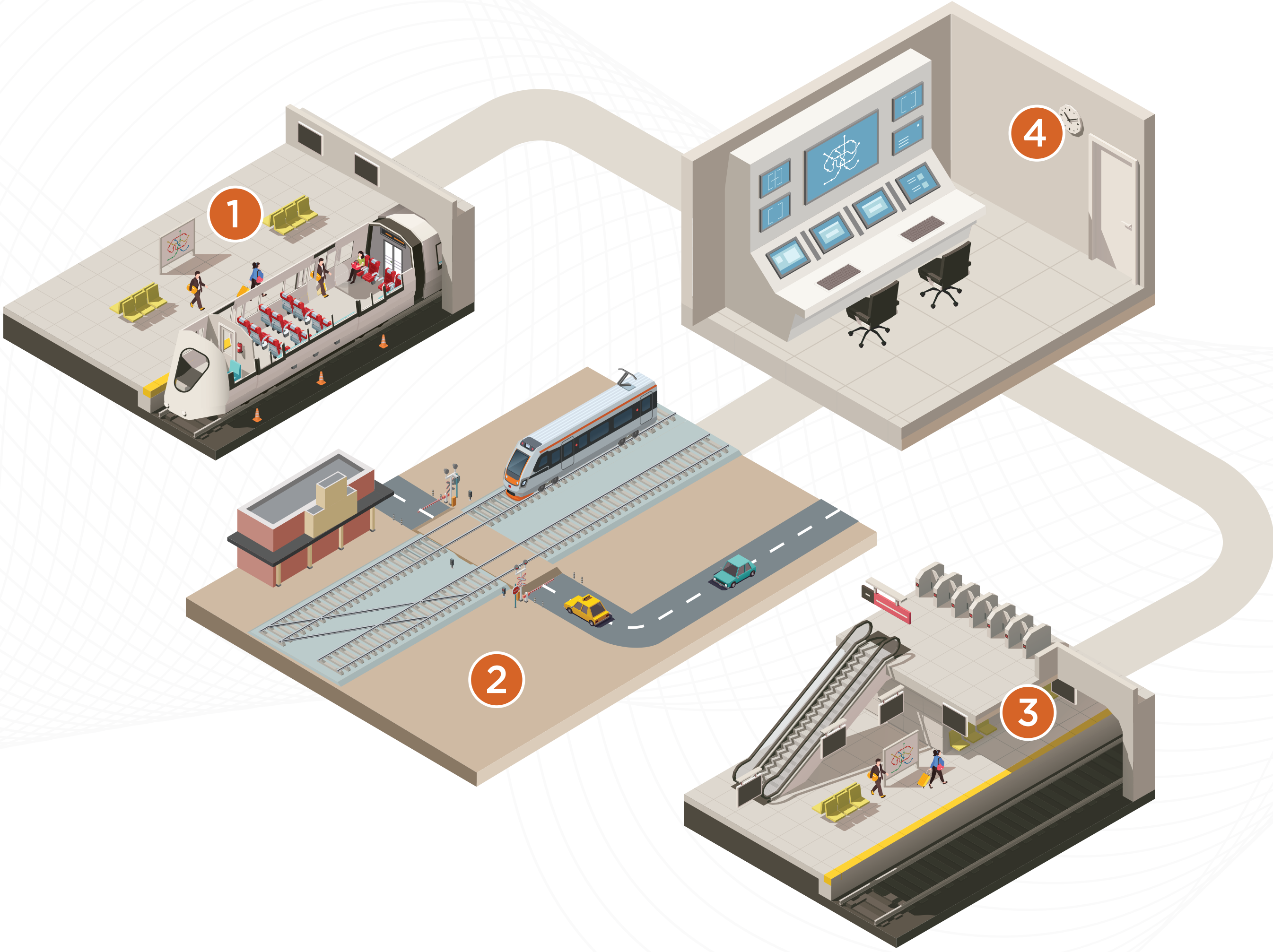
Sven Burkard | Solution Consultant

With the worst of the impacts of the COVID-19 pandemic in the rear-view mirror[1], the mass transit sector is rebounding as the industry works toward a more connected, efficient, and passenger-friendly future. The pandemic put the brakes on mass transit, with ridership declining by 40% to 100% depending on the region, and a global average drop of about 70%[2]. The lull in travel, however, offered many operators an opportunity to implement new technologies to improve their mass transit systems[3]. These updates enable railroads to better harness the massive volumes of data available to them and use insights from that data to improve safety, security, and reliability[4].

Against this backdrop, experts expect wayside infrastructure to become even more significant. Future-thinking owners and operators are looking to wayside infrastructure as the key to reducing costs and improving performance.

- They seek to reduce the number of safety and security incidents through surveillance and monitoring improvements.
- They're looking to monitor and automate rail infrastructure assets to reduce unplanned failures and maintenance costs.
- They're automating train operations to increase ridership and reduce headway without negatively impacting operations, maintenance, or safety.

[1] "Next Stop, 2023: Rail Trends and Predictions for the Coming Year." Railway Technology, Jan. 17, 2023.
[2] "Boosting Passenger Preference for Rail." International Union of Railways, June 2022.
[3,4] "How Digitalization and New Tech Drives the Rail Transport Beyond 2023." Draup, Dec. 9, 2022.
Note: Trackside and Wayside can be used interchangeably



Element 1:

The Connected Train Network

Establish connections onboard rolling-stock assets

Element 3:

The Connected Station Network

Enable communications for in-station systems

Element 2:

The Connected Trackside Network

Provide connectivity for track-side equipment

Element 4:

The Connected Backbone and OCC Network

Create a backbone for the OT network

At Belden, we understand the critical importance of networks and connectivity to driving outcomes across all these areas. As owners and operators increasingly adopt automation technologies enabling end-to-end communication and real-time data exchange, the demands on networks will only increase. In this white paper, we detail what you need to know to build a wayside network that's not only suited for the needs of today, but also ready to deliver what we haven't yet imagined for tomorrow.

How Trackside (Wayside) Infrastructure Fits in the Connected Mass Transit System

The signaling and communications networks typically consist of multiple interconnected networks all connected to a common backbone. Together, these elements allow devices within one network to communicate with devices within the same or other networks, including:

- **The onboard train network** of communication systems and the devices installed on a train to support its operation and communication with the outside world, including:
  - » Train control systems—automatic train control (ATC), communication-based train control (CBTC), etc.
  - » Train operations services—signage and infotainment, public address (PA) systems, cameras, etc.
  - » Onboard services for passenger use—for a cellular signal, public Wi-Fi internet access, etc.
- **The trackside (wayside) network** of communication systems and devices installed alongside the tracks to support the operation of trains and provide connectivity for trackside equipment, including:
  - » Train-to-ground communications—cellular networks, Wi-Fi/radio, driver advisory system (DAS), etc.
  - » Trackside control systems—crossings, interlockings, track switching, etc.
  - » Trackside operation systems—axle counters, thermal imaging, emergency phones, etc.
- **The station network** of systems and devices installed in train stations to enable communication for in-station systems, including:
  - » Station network infrastructure for control—platform gates, ticketing/revenue collection, etc.
  - » Operations systems—video cameras, PA, signage, etc.
  - » Passenger experience—public Wi-Fi internet access, infotainment, etc.
- **The backbone network** connects all the various systems and devices within a train or mass transit system and serves as the foundation for the communication and data transmission between the system networks—onboard train, wayside network, and station networks—and the control center, including:
  - » Area of operation (AO) interconnections—automatic train protection (ATP), automatic train supervision (ATS), automatic train operation (ATO), etc.
  - » Operations control center—scheduling systems, dispatching systems, etc.
  - » Remote connectivity—remote terminal units, remote sensors, etc.

Of these four networks, the **trackside (wayside) is often deemed the most critical for control and safety** because it connects the train with the rest of the system. A loss of communication for more than four seconds can disrupt operations, negatively impacting safety and revenue.

Note: Trackside and Wayside can be used interchangeably

Designing the Trackside (Wayside) Network

Wayside operations are exceedingly complex, involving many components and systems that must work together seamlessly to ensure safe and efficient train movement. Railway networks operate in harsh environments, requiring enhanced performance characteristics and resilience. Some of the many challenges faced by system operators related to wayside operations are

- Maintaining wayside infrastructure, such as tracks, signals, and track-switching systems.
- Ensuring network availability throughout the system to ensure the safety and reliability of wayside equipment and systems.
- Coordinating and managing train traffic and movements at stations, rail yards, maintenance facilities, and other wayside locations.
- Managing and mitigating the operational impact of inclement weather, which can damage tracks and signals.
- Managing the cost and budget for wayside operations and maintenance.
- Ensuring redundancy, reliability, and data security.
- Sourcing equipment that can tolerate wide operating temps, vibration, and even high radio frequency interference (RFI) or electromagnetic interference (EMI).
- Keeping up with advances in technology and implementing new systems and equipment to improve wayside operations.

How Will You Structure Your Network?

Trackside (Wayside) Network Topologies

Trackside networks face more hazards than other parts of a mass transit system's data network due to the distance between connection points and being more exposed to temperature extremes and susceptible to power outages. The way wayside network devices and communication systems connect depends on the specific requirements of the train system, such as the communications infrastructure, needed throughput/bandwidth, failure tolerance, and budget. Depending on the applications served—such as train control versus infotainment—and the rail vendor, the wayside network(s) may be a ring, two parallel linear networks or a combination of both—a primary and a secondary ring network. Building in the necessary redundancy requires twice as many switches and radios.

Vital systems—for example, train control, safety, and signaling—are typically redundant, with built-in mechanisms for fault tolerance and automatic failover in case of equipment or media failure. Having multiple systems or devices that can perform the same function reduces the risk of service interruption and boosts the train system's overall performance.

In contrast, nonvital equipment—such as onboard infotainment or cameras—does not require a ring topology with a dual backbone. Non-vital equipment may need redundancy, but not necessarily complete fault tolerance and automatic failover.

Creating ring topologies for vital and non-vital system networks provides more fault tolerance to mitigate potential safety and operational issues and disruptions. Deploying ring topologies, devices are connected in a circular path, with data flowing in one direction, until a fiber break, localized power loss, or switch failure requires it to revert in the opposite direction. The same ring topology is frequently applied to the dual (or redundant) backbone, which typically consists of two separate networks that work together to provide a backup, allowing operations to continue even if one network fails. While this topology increases the complexity of managing the wayside network, it greatly increases reliability.

What Networking Devices Do You Need?

Trackside (Wayside) Hardware

Wayside hardware encompasses the physical equipment and devices installed alongside the tracks to communicate with the onboard train network and the control center, supporting the operation of trains. Typical hardware includes:

- **Trackside networking switches that connect various wayside devices.** These switches must be hardened as they are typically mounted on DIN rails in wayside enclosures that also house the radios for train-to-ground communication. They experience environmental extremes and seasonal temperature variations. Depending on the application, and given their proximity to rail traffic, they also experience periodic and recurring vibrations from passing transit

Note: Trackside and Wayside can be used interchangeably

trains and, in extreme cases, even from Class 1 freight carrying heavy loads. Such switches must meet EN 50121-4 to address the requirement for tolerance and shielding from interference and electric noise, such as RFI/EMI. They must also be protected against transient power surges from nearby lightning strikes. These switches typically feature at least two 1-Gigabit single-mode fiber ports and support non-proprietary industrial redundancy protocols, such as media redundancy protocol (MRP) with a sub-200 ms reconvergence time.

- **Trackside (Wayside) radios** used to communicate with trains. They maintain the seamless communication connections between the train and the ground, while being passed from one radio to the next as the train moves down the track. Most wayside radios use the 802.11 Wi-Fi standards, along with the appropriate antennas—directional for long straight track sections, sectoral in turns, omni at stations, and leaky coax (radiating cables) in tunnels to ensure strong signal quality.
- **Power supplies** that take available AC or DC power and convert it to the power required for switches and radios – typically 24VDC. These filter out transient noise, which can disrupt the operation of the equipment and cause communication problems.
- **Fiber optic cables** suited for indoor as well as outdoor applications, including use in conduit, direct burial, lashed aerial, and trunking applications. They are typically run on both sides of the track, building in redundancy and physical separation.
- **Category 6 or better Ethernet cables** that offer consistent and reliable performance in even the harshest environments. Unshielded twisted pair (UTP) cables work well for short segments using patch cables, while shielded twisted pair (STP) cables work well for connections outside of an enclosure in environments with RFI and EMI. Like the fiber cables, Category Ethernet cables need to have the appropriate jacketing material — LSZH (low-smoke, zero-halogen), armored, burial, or even rodent protection.

Note: Trackside and Wayside can be used interchangeably

Industry Standards

EN 50121-4 applies to any signaling and telecommunication apparatus installed in the railway environment. The standard specifies requirements for the electromagnetic compatibility (EMC) of the railway system to ensure that equipment:

- Does not interfere with other electronic equipment.
- Is not affected by electromagnetic disturbances from other equipment.

Equipment must also be able to operate reliably within -40°C to +70°C without any active cooling and be able to withstand short-term temperature spikes up to 85°C. The standard also outlines the measurement methods and limits for vibration levels to ensure that railway equipment can withstand the vibration loads experienced during decades of operation without degradation of performance or safety.

How Will You Secure It?

Security Considerations for the Trackside (Wayside) Network

Trackside assets play a critical role within mass transit networks because they help ensure the safe, reliable operation of trains. Most are housed and connected in field-level outdoor cabinets, making attention to cybersecurity safeguards imperative. Often interconnected and interdependent, which means that a failure or malfunction in one asset can have a cascading effect on other parts of the network or lead to costly service disruptions, trackside assets' cybersecurity considerations include:

- **Physical security:** Robust, locking cabinets prevent unauthorized physical access and generally include momentary door contact switches that alert to any access, which nearby cameras can confirm and document. Technicians should disable any unused ports and use 802.1X or other network access control (NAC) solutions to prevent unauthorized users from connecting directly to the field network.
- **Switch management access:** Placing the switch management into its own dedicated VLAN and requiring the use of non-default access credentials and maintaining whitelists of authorized terminals' IP and/or MAC addresses helps further restrict access to the equipment's management interface.
- **WLAN encryption:** IEEE 802.11i keeps WLAN exchanges and associations secure. It specifies security mechanisms for wireless networks, including wireless authentication, encryption, key management, and detailed security.

Note: Trackside and Wayside can be used interchangeably

- **Network segmentation:** Keeping network segments originating from the core backbone virtually segmented using VLANs prevents errors, broadcasts, and malicious traffic from spreading to the entire network. It also simplifies management and network traffic analysis.
- **Data segmentation:** Subdivision of the data pipeline using technologies like Multiprotocol Label Switching - Transport Profile (MPLS-TP) provides channels of user-definable bandwidth and data paths for different services or applications, preventing one from overwhelming the system and stealing resources from another.
- **Network management:** Enabling real-time monitoring and notifications of physical and logical network changes on a network management system (NMS) ensures the continuous safety, security, and reliability of the backbone network via observance of key network metrics such as link utilization, detection of insecure protocols, and preemptive maintenance recommendations.
- **Passive intrusion and anomaly detection:** Monitoring and analyzing network traffic for unusual patterns or anomalies that may indicate a security threat and alerting of any risks detected help maintain uptime without adding additional network traffic.
- **Firewalling:** Employing dedicated firewall hardware, where network interfaces connect to external entities and on branches of the internal automation network that require additional levels of security enhances security. Firewall hardware commonly creates demilitarized zone (DMZ) interfaces to safely operate devices requiring access to both internal and external networks or users.
- **Patch management:** Verifying timely updates to critical backbone devices, especially those with external connections, prevents attacks targeting networks or connected devices with out-of-date software revisions.
- **Access control lists (ACLs):** Maintaining a curated list of authorized users and devices with access to different layers and segments of a network adds a layer of security beyond network segmentation.

Your Connected Trackside (Wayside) Roadmap

Follow these steps to deploy a connected wayside network ready for the challenges of today, as well as tomorrow.

Installation

- Ensure redundancy of the control network at both the physical and logical levels, avoiding the use of a single bundle for primary and redundant fiber pairs. Cabling paths for redundant connections should differ from the primaries so that catastrophic physical damage has less opportunity to affect both connections.
- Install antennas in their preferred orientations to maximize coverage and performance, especially multiple-input multiple-output (MIMO) antennas that combine two or more antenna elements. For example, most wireless access points use two antennas oriented in different directions to maximize wayside coverage.
- Deploy wireless systems with appropriate cabling and install properly grounded surge arresters for outdoor installations.
- Keep the distance between the radio and the antenna to an absolute minimum to ensure less signal loss, significantly helping to maximize the output power that translates to wireless distance and throughput.

Configuration

- Ensure that each networked device has a static IP address, that the latest approved firmware has been loaded, and that the default password has been changed to one that uses a mix of uppercase/lowercase letters, numbers, and special characters.
- Configure wireless access point parameters to coincide with those of the wireless clients. This includes the frequency (typically 2.4 or 5 GHz), channel, service set identifier (SSID), and password. Most industrial access points work with a centralized controller that simplifies this process for larger deployments.

Note: Trackside and Wayside can be used interchangeably

Go-Live and Validation

- Be sure, as the devices are deployed, to save and back up their configurations and record the location of each asset along with its properties (manufacturer, model and serial numbers, firmware revision, port connections, etc.), then safely and securely archive for reference when performing future maintenance and upgrades.
- Validate the signaling and communications connections, ensuring that all end devices communicate as expected and that machines perform their tasks as intended. The system should establish the necessary connections when brought online, but more vigorous testing should be performed to confirm that everything runs as expected. Check several parameters at endpoints and all network infrastructure devices for issues:
  - **Collisions and cyclic redundancy check (CRC) fragment errors** point to connection speed, duplex mismatch settings, and even poor cabling terminations on devices at either end of a single link.
  - **Link flaps** indicate problems with link media and connections or the end device's network interface controller (NIC).
  - **Speed settings listed at values that are lower than expected** indicate termination issues with the connection media or misconfigured end devices.
  - **High-bandwidth** usage indicates excessive traffic, such as unfiltered multicasts that are flooding the network.
  - **Network outages** may indicate unmanaged loops that result in broadcast storms. Frequent or intermittent network outages may also indicate media problems—breaks in cabling, low-quality Category cables, long cable runs, excessive RFI or EMI noise, or a combination of factors.

Belden: Your Connected Trackside (Wayside) Specialist

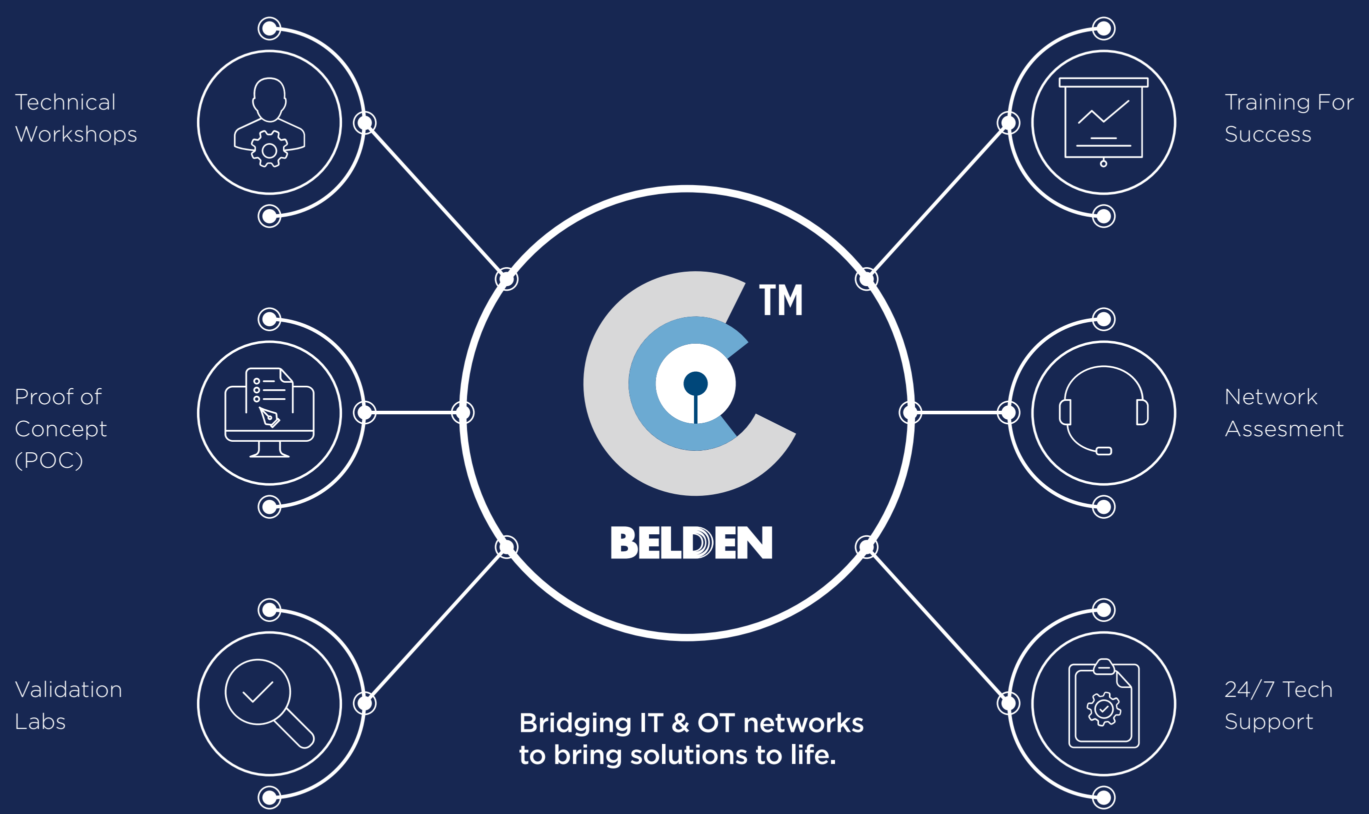
Railways will continue to play an important role in moving people and goods while shaping the future of communities and regions around the world. As demand for sustainable, efficient transportation grows, it's the perfect opportunity to reach out to Belden to ensure that you have the wayside network infrastructure in place to support your mass transit systems.

As an end-to-end network solution provider, we offer the most comprehensive networking profile for your mass transit system. From industrial cables and trackside fibers to WLAN controllers, switches, and cybersecurity appliances, our experts can assess your evolving needs and help you imagine and prepare for what the future may bring.

Note: Trackside and Wayside can be used interchangeably

Enabling Customer Success

Customer Innovation Center



How Belden Supports Your Digitization Journey

With all the other priorities you manage, you shouldn't be expected to serve as a digitization and network expert too. Finding a trusted partner makes your journey faster and more cost-effective—and ensures that you achieve the outcomes you expect.

Our in-house team of domain experts and solutions consultants has decades of experience in industrial automation and railway environments. Together, they crafted a step-by-step process to get your digitization project off the ground.

1. Identify your goals

A digitization project should start with talking about your needs, challenges, goals and inefficiencies. Where do you struggle? What do you hope to accomplish? What needs to change about current processes? What's working really well? And why is it working? What do you wish you could achieve, but can't due to technology or system limitations?

2. Conduct assessments

Our network assessments explore six technical elements to uncover opportunities for optimization in:

- Industrial cybersecurity.
- Network infrastructure.
- Edge computing.
- Wireless.
- Data management.

3. Present the results

After we complete the network assessments, our experts document the results and present them for you.

We report on things we notice, such as a lack of network segmentation, utilization, and optimization, so you can better understand your network infrastructure's availability, security and redundancy.

We also look for things like excessive network latency, outdated hardware, lack of security/authentication, lack of network and device visibility, and how you can maximize your network availability through redundancy and lowest MTTR (mean time to replace) solutions.

Recommendations about tools and software to help you visualize your network and monitor equipment 24/7 are also included.

The goal of providing you with this information is to empower you to succeed and make the most of your data, people, and processes. Together, we can build a blueprint that acts as your guide to meeting your KPIs and requirements.

Let's build the future.

When you're ready to move your automation initiatives forward, our team is ready to help. Visit **www.belden.com/mass-transit** to learn more.

About Belden

Belden Inc. delivers the infrastructure that makes the digital journey simpler, smarter and secure. We're moving beyond connectivity, from what we make to what we make possible through a performance-driven portfolio, forward-thinking expertise and purpose-built solutions. With a legacy of quality and reliability spanning 120-plus years, we have a strong foundation to continue building the future. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia, and Africa. For more information, visit us at www.belden.com; follow us on Facebook, LinkedIn and Twitter.

Learn More

For more information, visit us at: www.belden.com

www.belden.com/mass-transit

Follow us on LinkedIn and Facebook