Transportation Solution Guide

Market Dynamics Facing Public Rail Transportation

The infrastructure running modern public transportation rail systems has become increasingly digitized and interconnected to increase ridership. This is revolutionizing optimization with rail operations as well as all facets of the passenger experience inclusive of ticketing, scheduling, onboard wireless connectivity and life safety systems.

Digitization Brings New Risks

Similar to many other industries, digitization of public rail transportation systems is driving productivity though rail car on time performance, predictive maintenance, and public safety. The operational systems responsible for the control and movement of the train, track, and signals as well as life safety systems are all now interconnected where real time data can be collected to make faster decisions to optimize the passenger experience and reduce cost. As these operational systems have become increasingly interconnected, new risks have emerged to public rail from the world of cybersecurity.

Step One: **Visibility**

Having visibility of your entire rail transportation subsystems is the first step to a cyber-secure network. Tripwire Industrial Visibility and Tripwire Log Center provides this visibility:

- Understand all the devices on your operational system infrastructure inclusive of devices in train, track and signal control as well as the command center, what they are communicating with and when their configurations change
- Correlate log events from multiple sources and writing rules to flag events of interest. For example, if a failed login is attempted 5 times on a critical device in signal control, Tripwire Log Center emails an automatic notification to the command center

Step Two: **Protective Controls**

Once complete visibility has been achieved, the right protective controls to mitigate the risk or impact of cyber events can be put into place. Whether adopting a framework, such as American Public Transportation Association (APTA), UK Railway Safety and Standards Board (RSSB), or European Union Agency for Network and Information Security Railway Recommendations (ENISA), all transportation and industrial cybersecurity frameworks call for two basic, fundamental measures:

- Network Segmentation: Hirschmann EAGLE and Tofino Security appliances enable robust network segmentation, which is the process of organizing networks into smaller segments and explicitly permitting communication required for specific applications such as train, track, or signal control.
- Device Hardening: Ensure all devices – HMI, SCADA, engineering workstations, switches, routers, etc. – are configured to industry cybersecurity best practices and frameworks, such as APTA ENISA, or others such as NIST and IEC 62443.

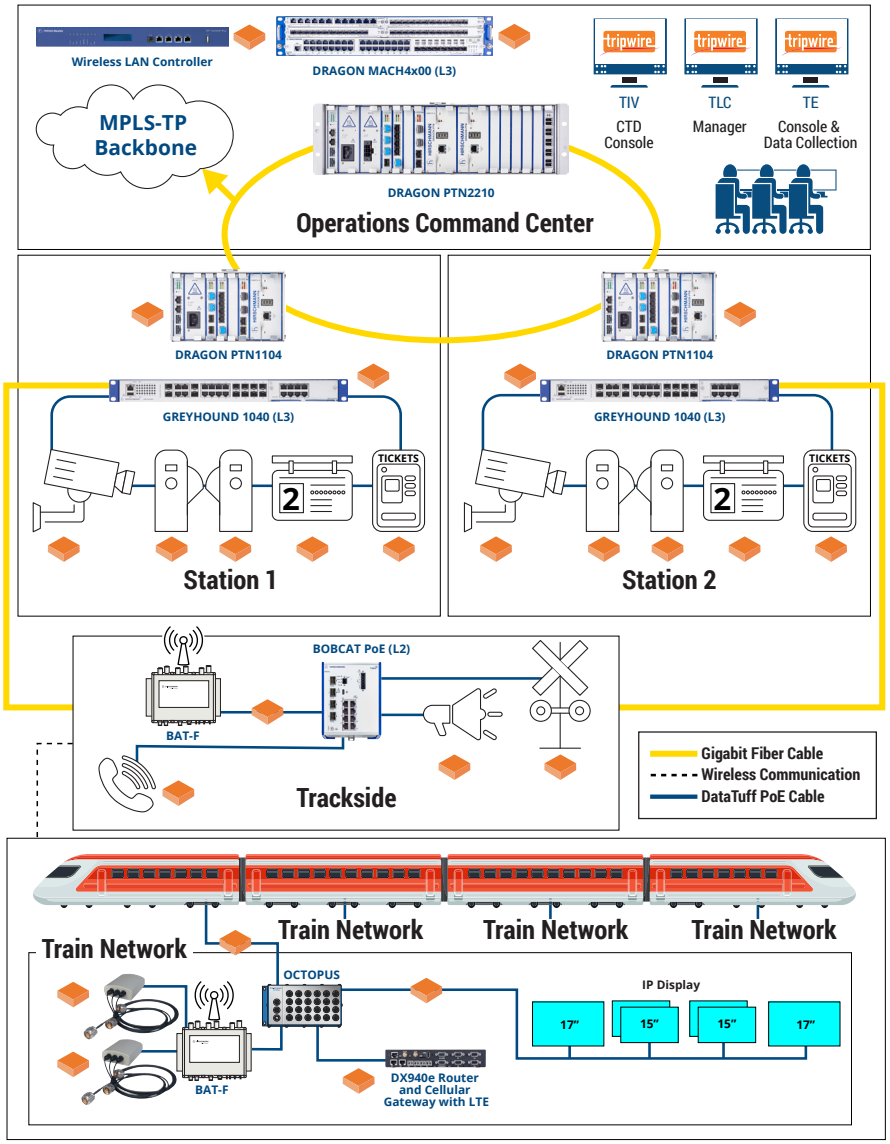
Step Three: **Continuous Monitoring**

Once a foundation of visibility and protective controls has been established, you can begin continuously monitoring the train, track, and signal control environments for ongoing situational awareness to manage abnormal or unexpected behavior. This awareness allows you to keep your control environments operational and avoid unnecessary or unplanned downtime. Tripwire solutions can enhance awareness via a continuous monitoring solution:

- Understand when controller modes or configurations have been changed that do not map to authorized work orders
- Know if a rouge asset has been connected to the network and is propagating malware or making connections to external networks
- Monitor engineering workstations and SCADA servers to ensure correct configuration against internal build specifications or selected cybersecurity framework

BELDEN
SENDING ALL THE RIGHT SIGNALS

Transportation Network Reference Architecture Example



TLC = Tripwire Log Center | TE = Tripwire Enterprise | TIV = Tripwire Industrial Visibility

Industrial visibility, protective controls and monitoring enabled through active and passive solutions: Tripwire Enterprise, Tripwire Log Center and Tripwire Industrial Visibility

Public Rail Transportation

Bottom Subheadline: Belden's solutions can:

- Provide complete asset inventory and industrial protocol communication
- Identify vulnerabilities to all assets
- Identify changes to controllers – configuration, mode and firmware
- Measure the configuration for HMI, SCADA, engineering workstations and network infrastructure to cybersecurity frameworks such as IEC 62443 or NIST
- Provide visibility to all log information from controllers, SCADA, HMI, engineering workstations and network infrastructure
- Provide network segmentation between the rail operational systems and enterprise systems, and between rail, track and signal control communication applications

Customer Successes

- Metropolitan Rail Line: Leveraged Tripwire Industrial Visibility to automate creating and sustaining an asset inventory of all of the devices in their rail train, traffic, and signal control networks as well as provide vulnerability and change configuration information related to those assets.
- Regional Railway: Harvested log events from all of their Hirschmann switches to pinpoint network inefficiencies such as master clock sync issues, duplex mismatches, and CRC errors.
- Subway: Used Tripwire Enterprise to ensure configurations of firewalls where not changed that could have potentially provided connectivity paths from the enterprise network to the operational train control network.

Call your Belden or Tripwire sales representative to schedule a demonstration or visit our websites at www.belden.com and www.tripwire.com.

Belden US 1-855-400-9071 ■
Tripwire US 1-503-276-7500

Belden EMEA +49 (0)7127 14 1809 ■
Tripwire EMEA +44 (0) 16 2877 5850

Belden APAC +65 6879 9800 ■
Tripwire APAC +65 6879 9839