ON TRACK: CONNECTIVITY AND CONTROL AT THE CENTER OF RAIL'S FUTURE

Every player in the rail industry is looking to deliver the best possible experience for their passengers. But it can be a challenge trying to attract more passengers and create a more connected experience while at the same time trying to keep operational costs down and expand safety and security measures. It may seem like a catch-22, but crossing this digital divide requires a rethink on how data systems operate and how subsystems are managed.

By **Urs Seiler,** Sales Engineer, ALE, Zürich Switzerland, **Alcatel-Lucent Enterprise.**

Improved connectivity is enabling transportation systems to evolve to meet the needs of a world on the move. From high-speed trains to self-driving cars, the transportation industry is harnessing the power of IP connectivity and the Internet of Things (IoT). Sensors are being rolled out to feed streams of real-time information to applications, which in turn provide operators with live information feeds, and provide passengers with up-to-the-minute travel announcements.

EVOLVING SERVICE DELIVERY – GETTING IOT-READY

Applying analytics to data from IoT devices is a great revenue opportunity for transportation operators. For example, data from location-based services can reveal information such as how much traffic is going through different locations, when passengers visit, how long they stay, what path they take and whether they return. Similarly, analysis of the real-time data from IoT devices can immediately identify travel problems before they cause delays or accidents, and provide warnings when maintenance is required. The implementation of predictive maintenance for rolling stock or track-switches is one of the most important developments in the transportation industry with regard to increasing safety and reducing operational costs.

Systems such as signalling, video surveillance, emergency call and alarm detection, telephony, wireless LAN, ticketing, passenger info systems and announcements, infotainment and internet all contain various devices and applications that may be operated and maintained by different groups or vendors and may require communication with third parties. Rail network operators will have to reassess how best to deploy the supporting infrastructure to achieve the level of connectivity required for the industry and to ensure improved services for passengers.

Whether it is bringing Wi-Fi to passengers on the *New York City* subway, or *connecting the longest rail in the world,* rail networks are undergoing a connectivity transformation. The question many rail operators are asking is, "How do we cost-effectively manage and maintain the growing IT and digital footprint needed to support transformation?"

KEEPING UP WITH CONNECTIVITY – THE MODERNIZATION OF DATA INFRASTRUCTURE

Although traditionally serial-based, rail and metro communications networks are quickly moving towards IP/Ethernet. As a result, a modern rail network now typically operates sub-systems off an access backbone network within the core network. A single, unified IP network infrastructure for most systems, immediately enables better connectivity between people, smart 'things' and processes. One data network that can carry traffic for multiple systems over a common infrastructure provides a manageable digital footprint with simplified IT administration.

Moving railway operations from multiple separate networks to a converged mission-critical architecture reduces the number of networks that need to be supported and dramatically simplifies network command and control requirements. Being able to integrate open platforms, such as new cloud-based applications, into the operations control center can further accelerate day-to-day operations.

However, a poorly planned and ineffective data infrastructure, as well as the introduction of new devices, can potentially place a strain on network resources, resulting in poor performance and the introduction of new vulnerabilities which could ultimately affect a travellers' experience.

CYBER RISK: THE COST OF CONNECTIVITY?

The connectivity boom and the growing number of possible points-of-entry and devices to protect is beyond what most IT teams can manage. Like all businesses, railways are vulnerable

"WHETHER IT IS BRINGING WI-FI TO PASSENGERS ON THE NEW YORK CITY SUBWAY, OR CONNECTING THE LONGEST RAIL IN THE WORLD, RAIL NETWORKS ARE UNDERGOING A CONNECTIVITY TRANSFORMATION."

to cyber-attacks. These can cut off access to commercial and business applications, compromise passenger information, and even put railway operations at risk.

It is nearly impossible to manage all of the different devices when they are rooted in individual subsystems that require their own management and maintenance. While Ethernet, IP and converged networks bring many benefits to railway operations, integrating subsystems also increases the risk that an isolated threat could become a much bigger problem. However, security risks should not be seen as the cost of doing digital business. Containing IoT without constraining it is one of the core principles behind building a secure network for rail, or any other intelligent transport system.

KEEPING AN EYE ON CONTAINMENT

Network segmentation lets operators create virtual isolated environments, known as IoT containers, on a single network. These are data traffic containers, where common devices are grouped together and only a select group of users and servers, called IoT platforms, can interface with them. An example of this in a rail network would be the IP security cameras. Deployed in and around a station, operations facilities or at the track-side, these IP cameras are relegated to their own virtual container and are only accessible by authorized staff responsible for security.

These cameras can then only interface with the server that controls them, and the traffic patterns associated with them can be monitored. When IP security cameras are only allowed to transmit video data, anomalies in the traffic pattern can be immediately detected and flagged to management and those devices quarantined if necessary. If one IoT container suffers a security breach, it cannot be used to break into other sensitive areas of the network that may be attractive to hackers. For example, if the HVAC system is compromised by a cyber-attack, sensitive systems such as financial booking systems, security systems, passenger signage, and administration are kept logically separate and safeguarded. This security strategy reduces threats without incurring the cost or complexity of operating separate networks.

A SMARTER INFRASTRUCTURE PAVES THE WAY

New technologies deployed at the edge of the network can make daily operations faster and less expensive. Power over Ethernet can simplify and encourage device and sensor installation as it eliminates the need for wiring in difficult places, making it easier to extend an organization's digital reach. However the transformation of operations and improvements of services available to passengers requires a rethink of the infrastructure behind them. Without a smart infrastructure in place to manage them, nothing will work. A focus on converging networks ensures that costs are lower than conventional networks, roll-out is easier and expanding and amending the network in the future is straightforward. ■

ABOUT URS SEILER

Urs joined the ALE team in 2007. As a technical sales expert, he assisted in advancing data sales in the Swiss marketplace. Today, Urs continues to provide his expertise in the Transportation industry as a Sales Engineer focused on rail. Urs has a Bachelor's degree in Electrical Engineering and an Executive Master of Business Engineering.