

# Protecting critical rail infrastructure from cyber attacks



Digital transformation of the rail and mass transit industries offers unique opportunities to transform the passenger experience and movement of goods, enhance train operations and energy efficiency, optimize traffic management and control, and predict and prevent failures in critical rail assets. The result is a more reliable rail network with more on-time train departures and fewer outages from equipment failures.

However, digital technology also introduces risks and expands the cyber threat landscape. Technologies such as cloud and the internet of things (IoT) connect once-isolated operational technology (OT) such as railway signal control systems to the internet so IT can be used to do things like track and trace locomotives and rail cars to optimize rail traffic.

This convergence exposes OT systems to the same cyber threats faced by IT systems. Nation-state attacks and denial-of-service hacks can affect rail operations through OT systems, significantly disrupting and even damaging critical rail infrastructure, with potential loss of life.

### **When rail networks and IT networks converge**

OT systems such as industrial control systems (ICS), SCADA systems and programmable logic controllers (PLCs) are used to control transportation networks and were once the exclusive domain of the operator's engineering department. Digital technologies enable us to take operational data from these systems and process the data in real time to optimize train operations and the movement of passengers and goods.

Predictive maintenance solutions, for example, take data from IoT sensors that measure temperature, pressure, amperage, vibration and other key data points on critical rail assets, and apply analytics and machine learning to monitor and predict equipment failures, raise alerts for maintenance intervention, and even take control of an asset and shut it down. Such solutions reduce the amount of unplanned downtime, which ultimately improves on-time train performance.

Energy optimization solutions monitor the movement of trains on the rail network using analytics to optimize the speed of trains across the network and minimize the occurrence of stoppages outside rail terminals. Train operators can realize significant energy cost savings by minimizing these unplanned stoppages simply by controlling the speed of the trains.

Rail car monitoring solutions track the location of rail cars, trace the contents in each rail car, and report on the condition of goods. For example, refrigerated rail cars carrying a load of fruit or vegetables can use this type of track, trace and condition solution to adjust the temperature remotely under certain conditions.

The one thing all these solutions have in common is the need to be connected to the internet so that OT can be integrated with IT to take advantage of deep analytics and intelligent automation to improve business operations performance.

These types of next-generation solutions are digitally transforming rail and mass transit organizations to optimize and improve operations, but it is these solutions that can be breached from a remote location with the goal of disrupting, disabling and destroying operations.

In December 2017, a Middle Eastern oil and gas petrochemical company had its plant operations shut down by malware known as Triton that specifically targeted the organization's OT safety system. In 2016, threat actors North Korea were believed to orchestrate multiple attacks against metro and train control systems in South Korea. A year earlier, hackers are suspected of seizing control of a Massachusetts Bay Transportation Authority train, which passed through five stations with operator behind the controls. Such attacks are unfortunately not an anomaly, and last year the Industrial Control Systems Cyber Emergency Response Team (headed by U.S.-CERT) received reports of cyberattacks and malware affecting up to 47.2% of computers for some industrial organizations. Losses can be severe. A 2016 ransomware attack that crippled the payment system of the San Francisco Municipal Transportation Agency resulted in free rides for MUNI customers. In 2019, losses from a ransomware attack against a European manufacturer topped \$41 million.

### OT systems still vulnerable

OT systems have traditionally lagged IT systems when it comes to keeping up with the latest trends in cyber security and vulnerability management. In many instances we are talking about operational assets whose life has spanned more than 20 years. Access and login information has been rudimentary at best, and many systems still use default passwords, relying on physical security to prevent unwanted access.

The data associated with these systems usually travels unencrypted over the network, and the systems are rarely patched, since this can require taking critical systems offline. As OT and IT systems converge, it is important to segment the data networks to control access from remote locations. Treating this as an afterthought can have serious consequences in the face of cyber attacks.

Here are five key steps to securing critical rail infrastructure:

- **Step 1:** Establish a comprehensive understanding of the rail operational technologies, the systems, assets and networks supporting the critical rail infrastructure.
- **Step 2:** Identify key risks, threats and vulnerabilities across all operational technologies, industrial control systems, SCADA systems and programmable logic controllers.
- **Step 3:** Assess the organization's current capabilities to secure everything on the OT network.
- **Step 4:** Develop a prioritized strategic and tactical roadmap of initiatives to improve the security posture of the OT network.
- **Step 5:** Deploy cyber defense solutions that protect the OT systems, detect security incidents within the network and respond with the same level of rigor provided to IT systems.

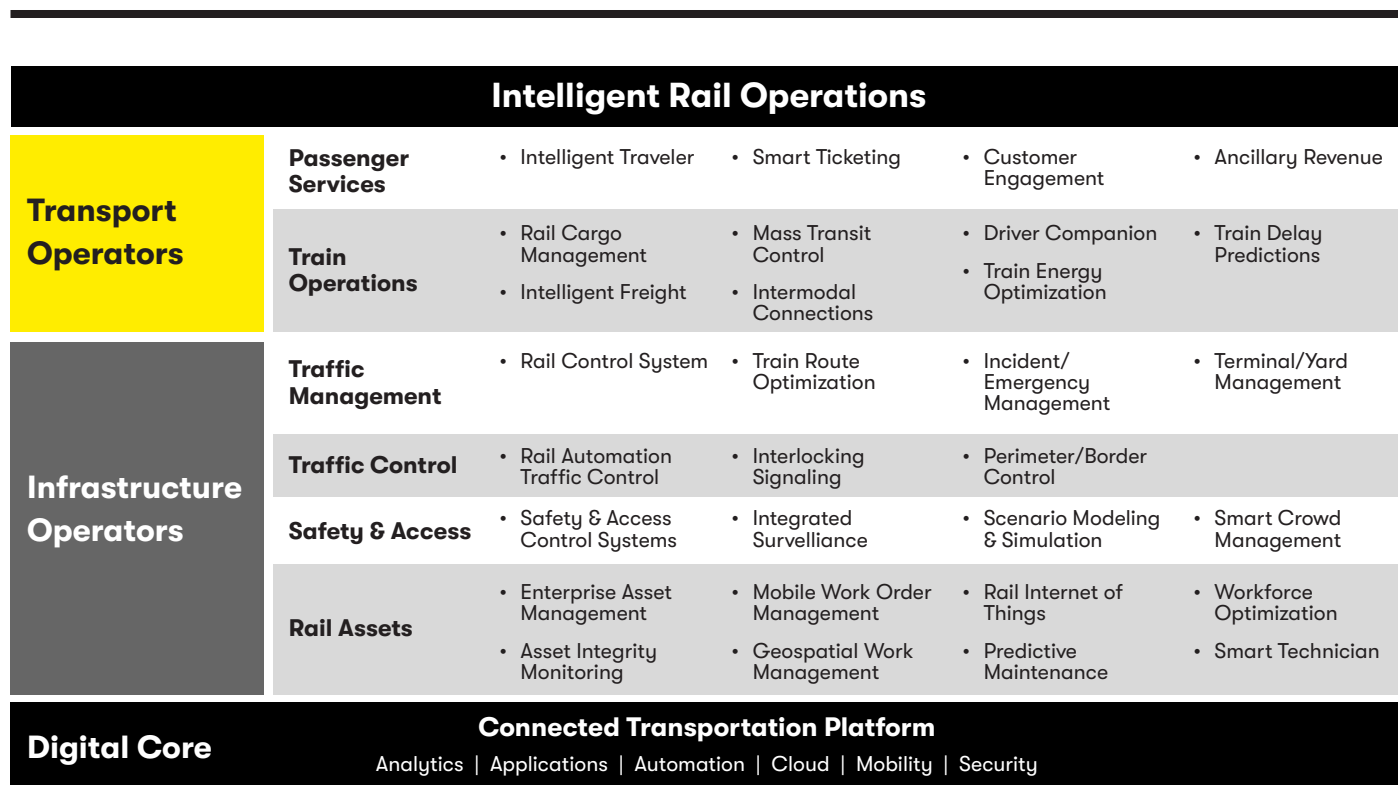


Figure 1. DXC Digital Railways Framework

### Managing risk across next-generation intelligent rail operations

In steps 1 and 2 we establish a comprehensive understanding of the attack surface for rail operations, identifying where the biggest risks, threats and vulnerabilities are within the systems.

In today's digital world of intelligent rail operations, we must assess risk across all layers of rail transport and infrastructure operations, including:

**Passenger services.** Transport operators are redefining the passenger experience with intelligent traveler and smart ticketing solutions that take advantage of mobile devices to assist passengers with their tickets, routes and connections to create a seamless travel experience. Passenger movement is greatly enhanced by these types of solutions. However, they have also become the victim of distributed denial-of-service (DDoS) attacks, where bad actors use malware to affect the online services and cause significant disruption to passengers.

In May 2018, the Danish rail system (DSB) was hit by a DDoS attack that left passengers unable to purchase tickets online or from ticket machines. Analysis showed that the attack was conducted from outside the organization and that the goal was to bring the system down, making the online service unavailable by overwhelming it with traffic from multiple sources.



**Remote access by bad actors can have a devastating impact.**

**Train operations.** Train operators are implementing next-generation systems for rail cargo management, intelligent freight, mass transit control systems, and intermodal connections systems that monitor and control the location, speed and condition of trains and cars, and connections to other forms of intermodal transportation. These systems are used to optimize the movement of passengers and goods on trains and buses, making them high-risk targets for activists looking to disrupt operations.

In October 2017, a DDoS attack hit Sweden's transportation network, crashing the system that monitors the trains' locations, as well as taking down email systems, websites and road traffic maps. Passengers were unable to make reservations or receive updates regarding train status and delays.

**Traffic management and control.** One of the most significant areas of risk for OT security in critical rail infrastructure is the traffic management and control systems that operate the rail network. Rail control systems enable real-time management of platforms, connections, tracks and lines. The systems can be fully integrated with interlocking signaling systems, delivering remote control of automatic route setting and interlocking with a real-time live view of rail operations.

Modern railway control systems enable a high level of automation and make a considerable contribution toward optimal usage of existing infrastructure. Besides enabling the implementation of optimized timetables and flexible interlocking control, the systems relieve operators of routine tasks.

However, remote access by bad actors can have a devastating impact. It is imperative to verify the identity of every user and entity trying to gain access to these systems. In many instances the main vulnerability comes down to passwords and firewalls. Applying standard IT security principles and policies is a simple remedy to prevent unauthorized access. More sophisticated approaches would model typical user and entity behavior analytics and raise security alerts when access requests go outside normal bounds.

**Safety and access management.** For years, physical security has been the primary defense used to protect industrial control systems. Chain-link fencing, padlocked control boxes, closed-circuit television and security patrols kept analog signaling systems safe from attack. Today, cyber security is of equal importance, especially when “digital twins” of physical assets are used for monitoring and optimization. These twins can be accessed remotely, requiring additional safety and access management steps.

Train operators and infrastructure operators need a security transformation roadmap that: includes elements of cyber defense and threat intelligence to monitor everything on the OT network; uses digital identity and authentication and access management to verify identities of people and machines accessing the OT network; data protection to encrypt data across the OT network; and secured infrastructure for endpoints such as ICS, PLC, SCADA, and IoT sensors.

**Rail asset management.** Industrial IoT has paved the way for the Fourth Industrial Revolution, also called Industry 4.0. Industrial IoT connects assets and equipment to the internet to monitor asset performance, control asset operation and predict asset failure. The data collected by a virtual sea of sensors enables us to optimize operations across the rail infrastructure and increase the capacity of the rail network. The result is more trains running on time for more passengers and a more reliable transportation network.

Condition-based monitoring of rolling stock and predictive maintenance programs for rail assets will organize maintenance based on remote diagnostic data. Such data is used to predict asset failures, but hackers seek to gain access to this same data, with the potential to introduce the opposite effect — complete disruption of the rail network by misdirecting and shutting down critical pieces of equipment.

Next-generation enterprise asset management solutions offer mobile access to critical information needed at the point of service. Privileged access management and multifactor authentication are required to secure such solutions so that this information does not fall into the wrong hands.

### Cyber threats to industrial control systems

By establishing a comprehensive understanding of the attack surface and identifying the biggest risks, organizations can establish a roadmap of initiatives to enhance security based on level of risk and priority (steps 3, 4 and 5 in securing critical rail infrastructure).

As part of the roadmap to transform OT security we should adopt the best practices and controls of the National Institute of Standards and Technology (NIST), which has published NIST 800-82 ICS Security, containing 177 controls for OT/ICS Security.

This guide to ICS Security lists the following cyber threats and incidents as the major concerns for train and infrastructure operators:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation
- Unauthorized changes to instructions, commands or alarm thresholds, which could damage, disable or shut down equipment, create environmental impacts and/or endanger human life

- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects
- Modification of ICS software or configuration settings, or infection of malware into ICS software, which could have various negative effects
- Interference with the operation of equipment-protection systems, which could endanger costly and difficult-to-replace equipment
- Interference with the operation of safety systems, which could endanger human life

Cyber resiliency should be part of a holistic approach to IT and OT security that takes all aspects of business operations into consideration, from employees and partners to the board of directors. Improving security is not a one-time project, but a program of continuous improvement.

NIST defines cyber resiliency as “the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that include cyber resources.” More realistically, cyber resiliency is also about establishing a policy and process that help an organization to survive and continue to execute its long-term strategy in the face of evolving security threats.

To become cyber resilient, the rail industry must strike a balance between protecting critical assets, detecting compromises and responding to incidents. Making the IT and OT landscape cyber resilient requires investments in areas such as infrastructure, design and development of integrated systems, applications and networks. At the same time, organizations must create and foster a resilience-conscious culture, of which security is an essential part.

### **Vigilance is needed**

Digital transformation of operational technologies is enabling aging rail infrastructure to be optimized in ways that increase the capacity of the rail network without the need to add expensive new locomotives. These same digital technologies, however, have greatly increased the attack surface, and while most attacks to date have resulted in disruptions of service, the potential for a cyber attack that causes serious damage, even death, is imminent.

In recent years, the Honey Train Project was created by a group of cyber security experts as a model of a virtual rail transport control and operating system, to gain information about the quality, quantity and aggressiveness of possible cyber attacks. In just 6 short weeks, this virtual rail infrastructure was hit by a staggering 2.7 million attacks.

And while the majority of attacks were computer-generated malware and dictionary attacks searching for common passwords used in rail control systems, some of the attacks were able to gain access to certain control systems and data used for train operations.

By applying the same level of rigor in OT cyber security (policies and best practices) that we do for our IT systems, we can prevent most of these attacks. The cyber security imperatives of monitor everything, verify everything and encrypt everything used in IT today need to be applied to operational technologies.

### **More information**

To learn more about how digital technology delivers intelligent rail operations and next-generation passenger experiences, and how cyber defense solutions are being used to secure operational technologies, please go to:

- **Digital Railways**
- **OT Security**

**Learn more at [www.dxc.technology/travel\\_and\\_transportation](http://www.dxc.technology/travel_and_transportation)**

 **Get the insights that matter.**  
[www.dxc.technology/optin](http://www.dxc.technology/optin)

#### **About DXC Technology**

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at [www.dxc.technology](http://www.dxc.technology).