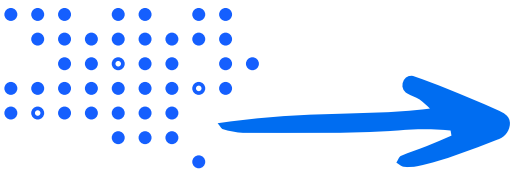
CYLUS

10 Cybersecurity Challenges

that European Metros Face in 2022

The railway industry is undergoing a digital revolution, becoming far more connected and advanced, and as a result, faces a rapidly growing threat landscape. For example, cyber-attacks against rail systems have increased by 173% over the last five years, resulting in billions of Euros in estimated losses. There is thus an urgent need for metro trains and urban transport operators to be mindful of these new challenges and adopt new solutions to defend their networks.

Here are the top-10 cybersecurity challenges for European metros using Communication-Based Train Control (CBTC) systems:



CHALLENGE 01

CBTC train-to-ground wireless communication is prone to cyber-attacks that may result in train hijackings

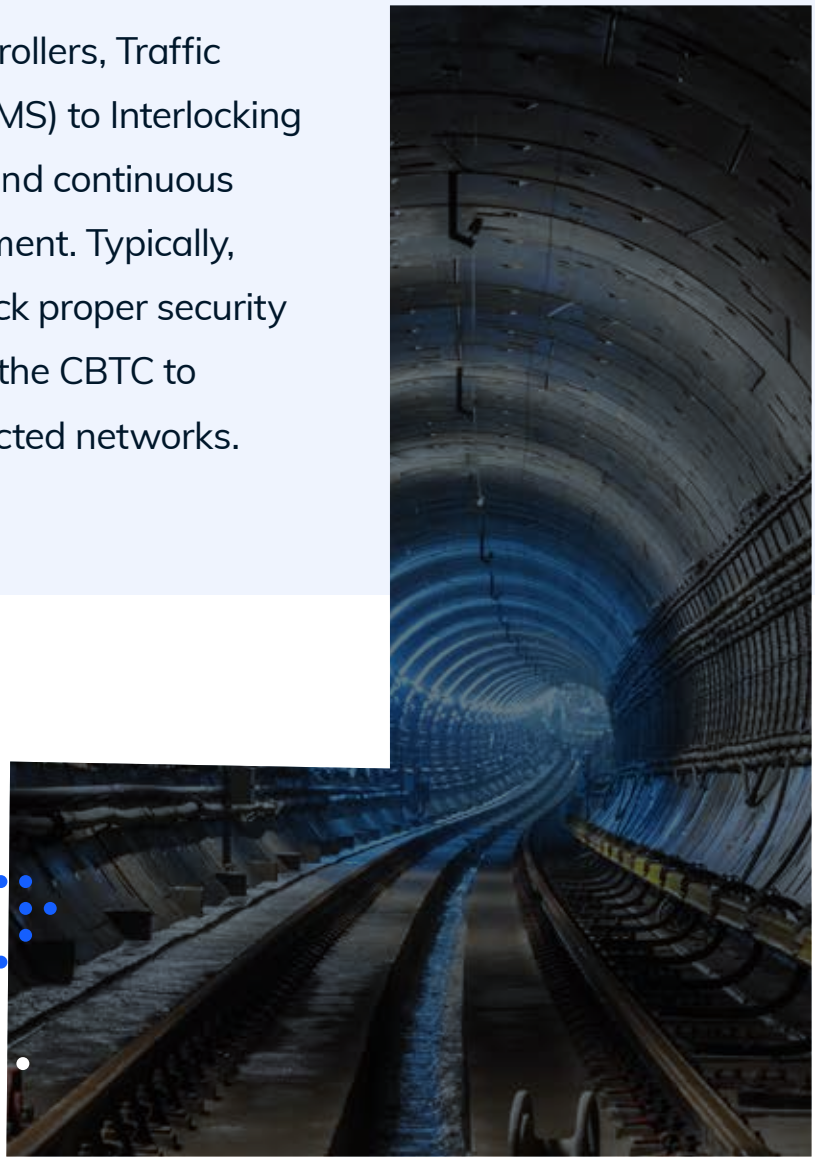
CBTC train-to-ground communication is often based on WLAN technology to perform train control. The bad news is that vulnerabilities in critical technologies such as authentication, encryption, and transmission expose WLAN to an array of risks. Furthermore, older CBTC implementations employ old Wi-Fi technologies with weak cyber protection. As a result, they may suffer from attacks such as sniffing, rogue AP, Man-in-the-Middle (MitM), and Denial of Service (DoS).

CHALLENGE

02

Insecure connections between CBTC networks and support systems

Railway applications require connectivity between systems with different safety levels. A good example would be the link between CBTC zone controllers, Traffic Management Systems (TMS) to Interlocking systems for dispatching and continuous monitoring of train movement. Typically, these implementations lack proper security measures, thus exposing the CBTC to penetration from unprotected networks.

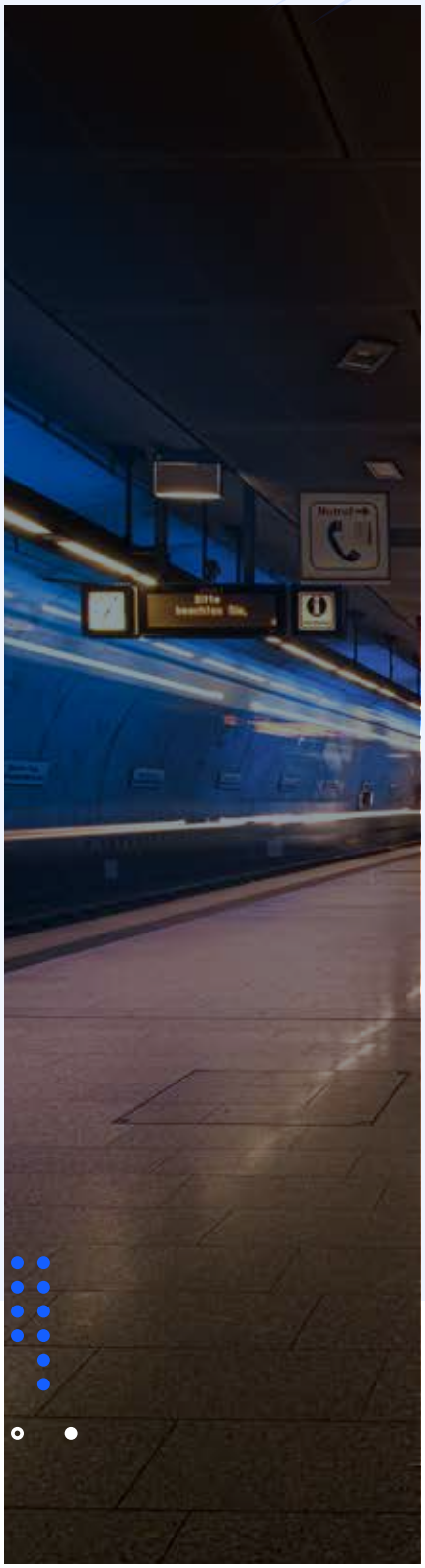


CHALLENGE

03

CBTC systems are hard to patch due to safety constraints, which expose them to common vulnerabilities

Railway systems are subject to rigid safety cases and standards. However, many of these networks include off-the-shelf components such as Windows-based machines and Unix-based servers in widespread use. These networks are exposed to common vulnerabilities and require periodic patching and software updates. As a result, those components usually use older versions that may expose the entire network to known vulnerabilities.



CHALLENGE

04

IT security measures are ineffective in CBTC environments, exposing these systems to attack

Most metros rely primarily on IT security measures in railway operational networks. In most cases, IT safeguards are not enough due to the widespread use of proprietary, industry-specific communications (over 80% of all traffic). Threat actors can exploit the weak protection of these applications to launch attacks against the critical rail infrastructure - and go undetected by the IT safeguards.

CHALLENGE

05

CBTC systems support commands that can override the network's safety logic. As a result, threat actors can maliciously trigger commands to damage safety functions

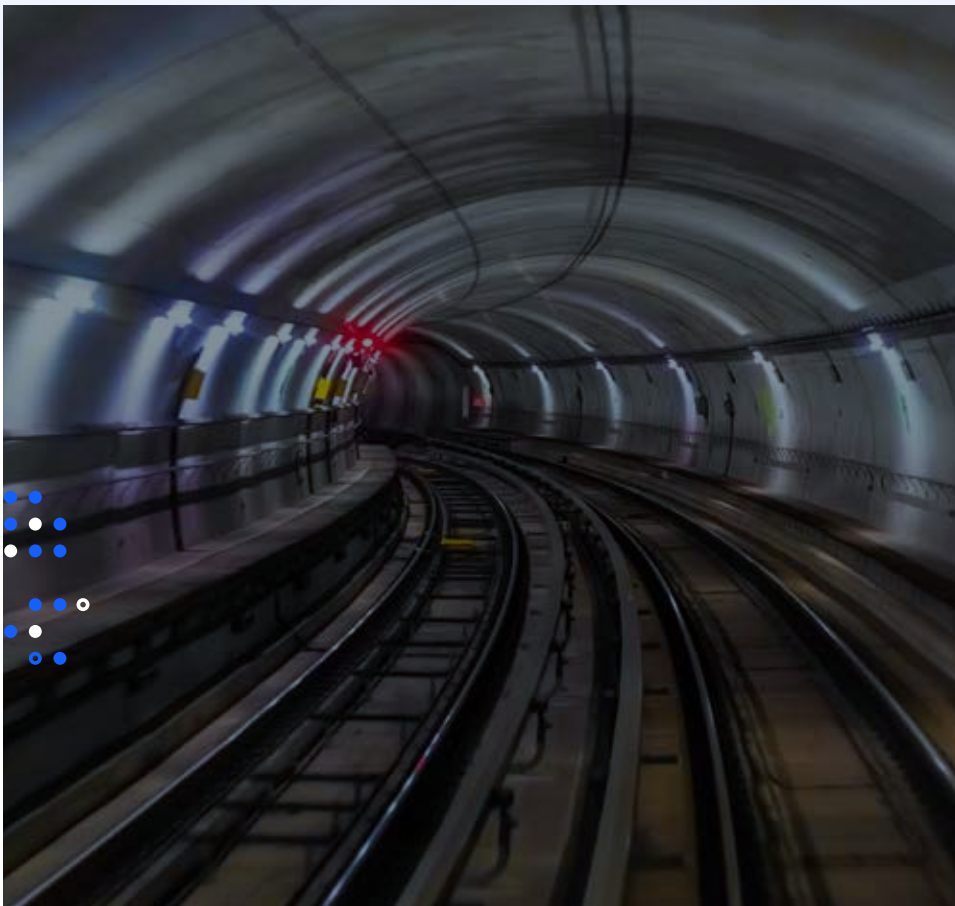
Safety-critical systems maintain the safety level and block commands that lead to risky situations. However, these systems have built-in controls that exist in the event of malfunctions and do not pass safety validations by the Interlocking system intentionally. As a result, threat actors can abuse such communications to cause dangerous situations.

CHALLENGE

06

Lack of cybersecurity standardization for metro systems exposes these networks to impending threats.

CBTC/metro train technology is typically proprietary and does not have interoperability standardization like ETCS. As a result, you cannot make any assumptions about the system's security. In addition, most designs were built without cybersecurity in mind and do not necessarily comply with any cybersecurity standards or regulations.

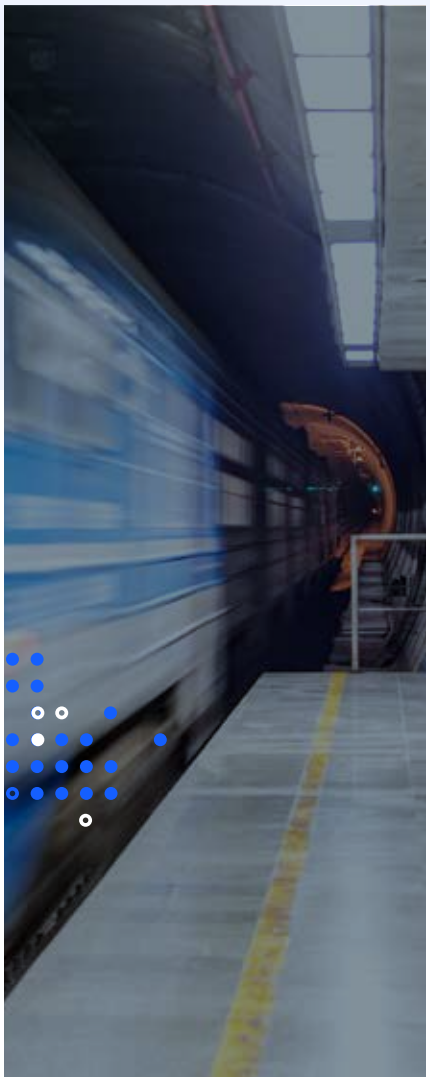


CHALLENGE

07

Cyber-threats against rail control systems originating in other companies may expose metro trains as well

In many cities in the EU, the signaling systems include interoperable connectivity to other railway companies. Trains from other companies (and potentially other regions) can connect to the metro's networks. Such trains could be corrupted by malicious commands or unwittingly carry malicious code.



CHALLENGE

08

CBTC systems often include hidden applications for maintenance and troubleshooting. As a result, threat actors can exploit these applications as an attack vector

Due to the closed and unstandardized nature of these devices and interfaces, vendors often include debugging ports or hidden features within the system. As a result, threat actors can exploit these applications and ports as an attack vector.

CHALLENGE 09

Rail control commands in CBTC networks are often unauthenticated, exposing them to malicious attacks

Authentication is usually not part of railway operational protocols' basic requirements because of total reliance on air-gapping. In addition, latency-related safety constraints prevent the implementation of authentication mechanisms. As a result, most railway operational equipment uses communication protocols without security measures, making them vulnerable to spoofing attacks.

CHALLENGE

10

Fail-safe mechanisms may cause the CBTC system to shut down in the event of a cyber incident

Primarily focused on safety, railways include fail-safe mechanisms that may trigger emergency braking and automatic equipment shutdowns.

About Cylus

Cylus is the global leader in rail cybersecurity, providing advanced solutions to protect mainline railways and metro companies from a wide array of threats and risks. Leading rail companies and operators use CylusOne to prevent safety incidents and service disruptions caused by cybersecurity events, without requiring any modifications to the network. With an unparalleled IP portfolio, Cylus has established itself as the pioneer and global leader in rail cybersecurity.

The company was founded by seasoned experts in cybersecurity, machine learning, traffic management, signaling, and onboard train systems, and is currently protecting some of the largest rail systems around the world.

www.cylus.com

Talk to one of our rail cybersecurity experts today.