UITP ADVANCING PUBLIC TRANSPORT

→ Report

Designing for Security: Rail Safety-Critical Systems

Detailed cybersecurity design guidelines

Under most jurisdictions, Rail Duty Holders are responsible for ensuring the safety of their operations. In short, they must establish a safety management system and implement a change management process to identify and control new risks.

However, a system that is not protected against external threats cannot be considered safe. As cybersecurity attacks on critical infrastructure increase in frequency and sophistication, they are increasingly targeting Operational Technology (OT), with the potential to disrupt safety-critical systems and create real-world hazards.

This Report addresses that reality. It provides practical guidance on designing for cybersecurity in Rail Safety Instrumented Systems (SIS), outlining key assumptions and emphasising the need for close integration between safety and security processes.

→ An overview of applicable regulations and standards

→ Lifecycle recommendations, including over 275 design principles and 75 management principles

→ Dedicated annexes on CCTV and cloud/IoT safety-related applications

The UITP Cybersecurity Committee welcomes feedback from the rail safety & cybersecurity expert community. As such, this Report is also available to non-UITP members of relevant profiles. Interested to receive a copy? Contact miryam.hernandez@uitp.org