UITP ADVANCING PUBLIC TRANSPORT

→ Report

Designing for Security: Rail Safety-Critical Systems

Detailed cybersecurity design guidelines

Under most jurisdictions, Rail Duty Holders are obligated to guarantee 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.

Given that attacks are increasing in rail, safety assurance documents must integrate security into their scope. Since security vulnerabilities can result in a safety hazard, designing secure safety-critical systems covers good practices during the entire lifecycle of a Safety Instrumented System (SIS).

Volunteer experts in the UITP Cybersecurity Committee joined to inform this Report, bringing together the knowledge of public transport authorities, operators, manufacturers, consultants and engineers with expertise in cybersecurity in a public transport context.

→ Considerations along nine key stages, from system initiation to disposal

→ Recommended practices & guidelines

→ An overview of regulations & standards

→ A guide to future risk assessments