UITP ADVANCING PUBLIC TRANSPORT

EXECUTIVE **SUMMARY**

EXECUTIVE **SUMMARY**

MANAGING CYBERSECURITY REQUIREMENTS IN PUBLIC TRANSPORT TENDERS

Cybersecurity protection of Operational Technology (OT) in Public Transport and Railways is a new and growing concern.

Nowadays, almost all transportation equipment includes software and many increasingly rely on commercial off-the shelf (COTS) solutions. Furthermore, to grasp the full benefit of digitalisation, transport operators are increasingly opening up their OT systems. Hence, it is now mandatory to consider cyber protection, whatever the system is under consideration for procurement.

ENISA top 15 threats of 2022

This report aims to provide public transport operators and authorities procurement officers and CISOs/CIOs with a comprehensive set of tools and good practices that can be adopted in their procurement process. This is to ensure that cybersecurity objectives are met.

In this context, the report explores the:

- Regulation and Legal Framework
- Procurement Process and Specification Framework
- Information Security System Specification
- Cybersecurity Technological Specification
- Quick Reference Guide For Cybersecurity Procurement
- References
- Examples of procurements for PIS/AVLS and Signaling System

"This report offers an easy-to-use guide for public transport professionals to improve their procurement process from a cybersecurity perspective."

ALIGNING BUYERS AND VENDORS

Integrating OT cybersecurity requirements is easier said than done. Currently, very few operators and authorities have OT specialists who can support the tendering process. Buyers don't even provide guidelines which are easily consultable to assist them in managing this cross-functional process. As a result, there is often a misalignment between the operator and authorities' cybersecurity expectations and the Vendors' cybersecurity deliverables.

To eliminate the gap, both parties should have well-defined responsibilities, clearly stated through contractual arrangements that consider cyber expectations in terms of Procedure, Personnel, and Technologies throughout the System's complete life cycle.

UITP CYBER REPORT BASED ON TS 50701

Acknowledging the wide discrepancy between what needs to be done during tenders and the resources available for ensuring an appropriate cybersecurity protection, UITP created the cybersecurity guidelines Report based on the European standard TS 50701, called **"Practical Guidance on Cybersecurity requirements in tenders".** TS 50701 complements IEC 62443, the international standard for Industrial Control System, by integrating rail specific requirements, especially safety. Written by cyber industry and PTO experts, the UITP report adapts this standard to Public Transport environments (i.e. metro, tramway and bus operation).

It provides a framework for legal, procurement, and specification processes. It recommends the drafting of a unique document for cybersecurity called Information Security System (ISS), which describes the issues to be addressed in the tender specification. Based on TS 50701's Seven Foundational Requirements, it explains the role of the various cyber technologies in attending these requirements.

UITP'S REPORT WALKS THE TALK

"Using an instructive approach, the report provides an easy-to-understand guideline to specifying cybersecurity for all OT system tenders."

Applying TS 50701 to a metro (i.e., CBTC signaling system) and Bus Rapid Transit (i.e., Passenger Information System/Automatic Vehicle Localization System) environment, it describes all the necessary steps that must be considered and suggests the technologies that must be considered, with their benefits and flaws. The report describes among other things technologies such as firewall, unidirectional gateway, Intrusion Detection System, Continuous Monitoring System, and their role in securing these environments.

Check out the Cybersecurity Report "Practical guidance on cybersecurity requirements", available on the UITP website!