Nov. 2025

Cybersecurity Management in railway projects (CLC/TC 50701)

Table of Content

A. General knowledge

1. End goals / essential functions → be conscious of why we do cybersecurity and what it serves : link with Safety/Availability/Integrity/Confidentiality
2. Internal interdisciplinary collaboration / synchronisation → synchronise cybersecurity w/ other departments : Design and development / Purchasing : specs ; Cahiers des charges ; RAMS (CENELEC 50126/8/9) ; Project management ; Operations and maintenance (after putting in service)
3. External collaboration → Asset owners / Operators ; IM RU ; System integrator ; Maintenance suppliers ; Product suppliers
4. Asset breakdown : cascade / architecture → SuC ; essential functions ; HW vs SW ; System (IACS) vs Components ; Configuration management ; System vs products / components
5. Activities and chronological distribution of cybersecurity activities → do things at the right moment : Process ; Procedures ; Program (cybersecurity program) ; Activities : define system, configuration management, setting targets (SL-T / SPR-T), risk assessment, verification and validation / acceptance ; monitoring ; Life cycle management

B. Applicable Standards

1. CENELEC EN 50126/8/9
2. Cybersecurity specific
    a. IEC 62443 series
    b. CLC/TS 50701:2023 : Railway applications – Cybersecurity
    c. EBIOS (ANSSI) France
    d. NIST Special Publication (SP) 800

C. Focus TS 50701 for Railway

1. Threats and related Vulnerabilities
2. Link w/ RAMS characteristics
3. Railway system overview : SuC (System under Consideration); configuration management; zones and conduits
4. Life cycle based on 50126-1 12 phases (V cycle)
    a. Cybersecurity context and cybersecurity Management plan for asset owner
    b. Defence in Depth / layers
    c. Priority : Essential functions / Integrity / Availability
    d. SecRAC vs SRAC
5. Synchronisation between Cybersecurity team w/ Design team and Safety team
6. Definition of the SuC (System under Consideration)
    a. Link w/ Essential functions for Safety and Availability
    b. Separation in Zones and Conduits → ZCR : zones and conduits requirements
    c. Initial risk assessment
    d. Threat log
7. Detailed Risk assessment :
    a. CRS (Cybersecurity Requirements Spec)
    b. Establishment of SL-T + SL-T based on IEC 62443 -3-2 ZCR 3.6
    c. 7 foundational requirements classes (FR)
    d. Risk management along the V cycle