Cybersecurity in Railways

"Industrial readiness for collective response“

UNIFE
Cybersecurity WG
Klemens Geiger – Vice-Chair

17th March 2021

Introduction

- **UNIFE is the European Rail Industry Association** represents the interests of more than 100 small, medium and large sized companies in the rail sector as well as national industry associations from across Europe.

  - **UNIFE's Cyber-security WG** is composed by 16 companies, aimed at improving and contributing to the new challenges in cybersecurity in the rail sector, from an Industry point of view.

Challenges and priorities

- The implementation of the proposed **NIS2 Directive;**
- The **TS 50701 Railway Applications – Cybersecurity**, considering the needs and requirements of the sector from a technical point of view;
- **Foster collaboration** among the different authorities and decision makers in cybersecurity, as well as rail stakeholders for the rail sector.

New Concepts of Safety & Cybersecurity

- Both, Safety and Cybersecurity, to be managed as far as possible interdependent
- However, always with close links to each other: **Cybersecurity shall not disable Safety and vice-versa**
- Always considering a different character of **Life Cycle**
  - ✓ **Safety demonstration according legislation** → in the long term should be costly
  - ✓ **Cybersecurity** → In the short term should be agile

New Concepts of Safety & Cybersecurity

- This converges into specific approach for the **Cybersecurity Framework for rail** in its core with a limited capability for patch management

  - ✓ Focus shall be on a Cybersecurity approach → with stricter Cybersecurity in depth from scratch. Means starts with the development lifecycle

  - ✓ To be able to harmonize the requirements i.e., RAMS and Cybersecurity on an essential function or service adequately

- Additional this conditions enforces
  - ✓ A stronger focus on resilience and Cybersecurity in depth
  - ✓ Tolerate a new vulnerability for a certain time, because of the lack of a rapid available patch, but with a strict control of the attack vectors

Railway homologation processes & legacy systems

- Specific character of the **rail homologation processes** lead to long living products in the field

  - ✓ Very positive approach from an ecological perspective

- This highlights the **legacy systems challenge** of existing railway infrastructure (i.e., signaling & rolling stock)

  - Existing fleet is outdated form the modern Cyber Security perspective . A refurbishment of all this legacy systems / equipment may need a completely new homologation process

    - ✓ For that an initiative for a minimum a risk assessment would be needed
    - ✓ The outcome would be translated into a refurbish/ substitution program.

Rail industry supply value chain: Wide and complex interaction

- The Cyber Security of the Supply Chain is essential for the overall Cyber Security of the railway ecosystem: Cyber Security regarding the value chain is a vertical topic.

- Consequently, there is a need for **the best-case standardized solutions** on subsystem and at component level.

- A way to solve this issue, could be:

  - ✓ Adequate Certification schemes on product level
    - e.g., according IEC 62443;
    - or as established in the NIS2 Directive draft ICT products and solutions based on EU CSA schemes

  - ✓ Specific protection Profiles on interfaces specific devices:
    - This would give guidance for the rail manufacturers and integrators

Thank you for your attention