TOP TEN

Ravdeep Kour
Luleå University of Technology

Category: **Rail**   Country: **Sweden**

Research Area 3: **Innovative Infrastructure for Europe 2030**   Idea Number: **21**

SecureDigiRail: A Framework for Improvement of Digital Asset Security in Railway

Digital technology is expected to improve railway systems sustainability, dependability, capacity, safety, and security including cybersecurity. In the digitalised railway, however, cybersecurity is essential to achieve overall system dependability. Gaps in cybersecurity lead to cyber incidents (Figure1 indicates categorised incidents of cyberattacks in railway) with negative consequences, including reputational damage, heavy costs, service unavailability and risk to the safety of employees and passengers. The current standards and guidelines related to cybersecurity in railways are proprietary and are followed by most railway organisations. These proprietary standards and guidelines lack a holistic approach to enable interoperability, scalability, orchestration, adaptability, and agility for railway stakeholders. Therefore, there is a need to develop a generic cybersecurity framework for digitalised railways to facilitate proactive cybersecurity and threat intelligence sharing within railways. The framework proposed by the project enhances cybersecurity maturity level (CMM) (Figure2 indicates current CMM in railways) to enable proactive cybersecurity to improve information assurance in the railway. The proposed framework integrates existing models, technologies, and standards to minimise the risks of cyberattacks on railways (Figure3). The framework uses different layers of open system architecture for condition-based maintenance in the context of cybersecurity to deliver threat intelligence. The framework also incorporates cyber kill chain models to detect cyberattacks and railway defender kill chain to enable proactive cybersecurity. The overall contribution is to help railways to implement solutions developed in a more scientific way to enhance overall dependability.