Ensuring Cybersecurity in Modern Railway Infrastructure

Yasmine Benghename*[1], Ahmed Lounis[1], and Mohamed Sallak[1]

[1]Université de Technologie de Compiègne – UMR CNRS 7253, Heudiasyc – France

Résumé

The utilization of autonomous trains in rail transportation holds the promise of enhancing efficiency, reliability, and cost-effectiveness. Nevertheless, the adoption of new technology introduces novel risks and safety concerns, particularly in the realm of cybersecurity. Autonomous trains incorporate intelligent computer systems and data sensors to gather environmental information, enabling them to make real-time decisions for safe and efficient operation. However, the data collection process poses security risks. Railway networks are susceptible to various cyberattacks such as malware, denial-of-service, and network intrusions, which could endanger public safety, disrupt operations, or cause property damage. Moreover, cyberattacks may compromise the integrity and confidentiality of the acquired data. Security and safety are pivotal considerations in the design and operation of these critical systems. While security focuses on safeguarding systems from malicious activities, hacking, and cyber threats, safety ensures the absence of unacceptable risks to human health and the environment, emphasizing system reliability and efficiency under normal conditions. Given the critical interplay between security and safety, evaluating the cybersecurity framework in the rail sector is essential. Although safety evaluation and analysis have long been conducted in railway systems, cybersecurity is often overlooked due to various challenges. These challenges include the lack of harmonization in cybersecurity requirements, regulatory complexities in managing cybersecurity within the rail sector, and the sector's overall immaturity in cybersecurity practices. The objective of our research is to assess existing cybersecurity frameworks applied in the rail sector and propose a harmonized cybersecurity framework tailored to the European Union's railway sector. This framework aims to address the unique challenges and complexities of cybersecurity in rail transportation, thereby enhancing the sector's resilience to cyber threats and ensuring the safety and security of autonomous transportation systems.

*Intervenant