INFRASTRUCTURE SECURITY

Opportunities

- The exchange of best practice in security between IMs, especially on terrorist threats, improve the overall level of security;
- More /better security can also help diminish other risks (metal theft, vandalism, 'unsafe' feeling of more vulnerable passengers).

Challenges

- Digitalisation (cyberattacks) will increase the need for effective coordinated measures on EU level;
- Keep European railways accessible and open for passengers while ensuring adequate security (preventing unnecessary barriers).

Last revision: 27/05/2019

Objective

Infrastructure security covers several aspects: terrorist attacks, vandalism, suicides and metal theft. Risk mitigation and exchange of best practices are crucial for all sensitive sectors, including rail infrastructure. The latest developments in terrorism had a significant impact on the perception of security of public transport systems. While no specific binding European legislation exists in this domain, best practices and an "Action Plan" to improve the security of rail passengers are developed on European level.

Involvement of Infrastructure Managers

Each Infrastructure Manager (IM) ensures the security of its network by developing risk plans. For the IMs who manage stations this task is even more relevant as public places require greater security, more controls and more human resources. Moreover, other attacks against the infrastructure, like vandalism or cable theft, also increase the risk of degradation of the infrastructure assets, causing disruptions and additional costs. Risk planning represents an increasing challenge for IMs.

EIM in action

- EIM's Security Working Group (SEC WG) gathers security and cybersecurity experts who exchange on security and cybersecurity issues and measures;
- EIM advocates the importance of promoting security guidelines instead of mandatory measures due to the different systems in the EU;
- EIM participates in the EU "LANDSEC" meetings organised by the European Commission.