# The New Challenges of Security in Railway Stations

Zakaryae Boudi, ClearSy

Intermodality growth and prosperity rely on effective transport systems. Any attacks and disturbances to land freight and passenger transport will have significant impacts on economic growth, territorial cohesion, social development and environment. As is witnessed by historical data pertaining to the security of land transportation, there are unfortunately specific weaknesses in affecting this mode in terms of security.

Historically, several attacks have deliberately targeted the rail transportation, especially metro systems, within major European cities. These attacks have been specifically designed to cause maximum disruption and a high number of fatalities. Attacks on subways and local trains have shown that the rail network is an attractive target for attackers to spread fear and terror in the population. In fact, the rail open architecture has a core role in the development of future stations as intermodal hubs and integrated parts of cities, but may offer multiple attack points, access at all hours and easy escape. The terrorist attacks of the 2004 Madrid train bombings and the 2005 London bus bombings claimed the lives of 191 and 52 innocent civilians, respectively. Recently, the Thalys incident has strongly brought back railway stations security into the limelight for European and international transportation actors. Because of the high passenger density of railway stations, criminals and terrorists have taken the transport sector to be an easy target, knowing that, for example, the measures used to secure airports are likely to be impractical. Furthermore, according to TAPA[1], the theft of high value and high risk products moving in supply chains costs business about € 8.2 billion a year in Europe.

Security issues related to land transport are diverse and complex. In the context of rail transportation and in order to effectively tackle the threats posed by terrorism and other forms of crime, it is important for the authorities and operators to investigate the past attacks perpetrated against railway systems and acknowledge preferred tactics, means and procedures, in order to provide pre-emptive answers to be adopted in case of attack. Moreover, it is crucial that end-users have a wide knowledge of security measures currently implemented by transportation entities that have suffered from attacks or which have confront with high levels of threat, in order to determine the most appropriate practices to face such critical circumstances.

However, the increasing evolution of railway systems, such as the new European signaling ERTMS system (European Rail Traffic Management System) and IT business systems, leads up to new generation of threats and requires a continuous updating of the corporate practices to face these threats. Today, the growing risk of cyber-crime puts in fact the authorities and the railway stakeholders in front of new security challenges, where the main purpose is to minimize the risks from both existing and emerging threats, and provide better security solutions in order to avoid catastrophes.

With this respect, this NEXTSTATION 2015 lecture discussed an overview on the existing and emerging threats facing railway stations and the co-existing security measures. A number of key challenges of railway stations security, supported by the CARONTE project conclusions, were formulated as follows:

---

[1]Transported Asset Protection Association (TAPA), http://www.tapaemea.com/

- Increase the resilience
  - Design security solutions as resilient as possible to any possible scenario (since they keep evolving)
  - The availability of secure and cost-efficient fall-back systems in order to survive a successful attack
  - Emergency management - Recovery management
- Find mitigation solutions with acceptable costs, delays and need of resources
- Motivate and convince politicians about the value of transport security
  - The vital importance of stations in economic activity depends on their attractiveness
- Find a balance between safety and security
  - A security measure shouldn't compromise safety => **Integrate Safety and Security by design**
- Define immediate measures to take after the detection of threat (detection of a kamikaze or an armed person)
- Define an organization approach to human and technology at a local level for crisis management
- Add cybersecurity awareness and cyber defense measures to the transport operators culture
- Reduce the growing cyber risks led by technology advance
  - Communication based train control / Automatic train supervision,
  - European standards: ERTMS/ETCS,
  - Migration to a computer based safety: CBI, ATC/ATP
  - Remote control/maintenance
- Consider security as a business issue, and not only as a technical issue
- Re-think Risk assessment methodologies (I.e. include motivation …)