The protection of a national critical infrastructure: the Italian Railways

Franco Fiumara
Chief Security Officer
Ferrovie dello Stato Italiane SpA

Workshop on Critical Transport Infrastructure and Cyber Security
UNECE Geneve 5-6 September 2016

Cyber Threat

- Represents the most demanding challenge for the Nation-system
- Its potential consequences may be worser than those of a traditional attack
- It spreads more quickly than its countermeasures do

'IT threats, all the more refined, fall on all operating systems, from the complex and organized ones pertaining to Governments and big Companies, to PC's and smartphones of single citizens'

FERROVIE DELLO STATO ITALIANE

Attack aims

Sabotage and industrial espionage

Extortion,
illicit commercial advantage,
political / ideological activism etc.…

FERROVIE DELLO STATO ITALIANE

Attack aims

- Cybercrime for profit
- Activism for social-political aims
- Industrial espionage for competition
- Sabotage for terrorism
- Cyberwar for international damage strategy

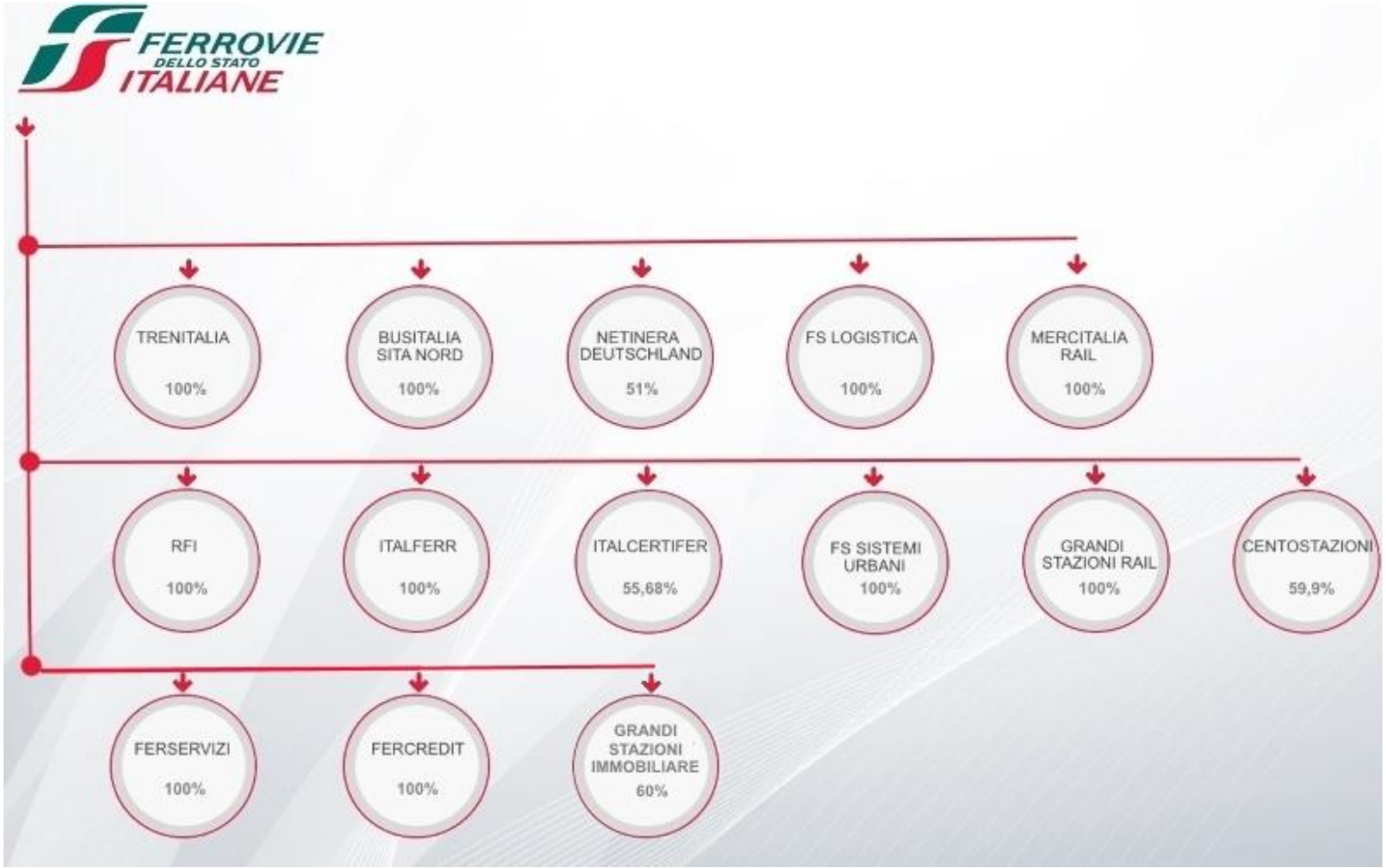
FERROVIE DELLO STATO ITALIANE

FS Group defence motivation

- Business protection and homeland security depend on the integrity and resilience of IT systems
- The customer's satisfaction and our competiveness depend on the capability to protect our information and IT systems
- Due to "critical IT infrastructure" we have an institutional commitment

FERROVIE DELLO STATO ITALIANE

The FS Italiane Group



FERROVIE DELLO STATO ITALIANE

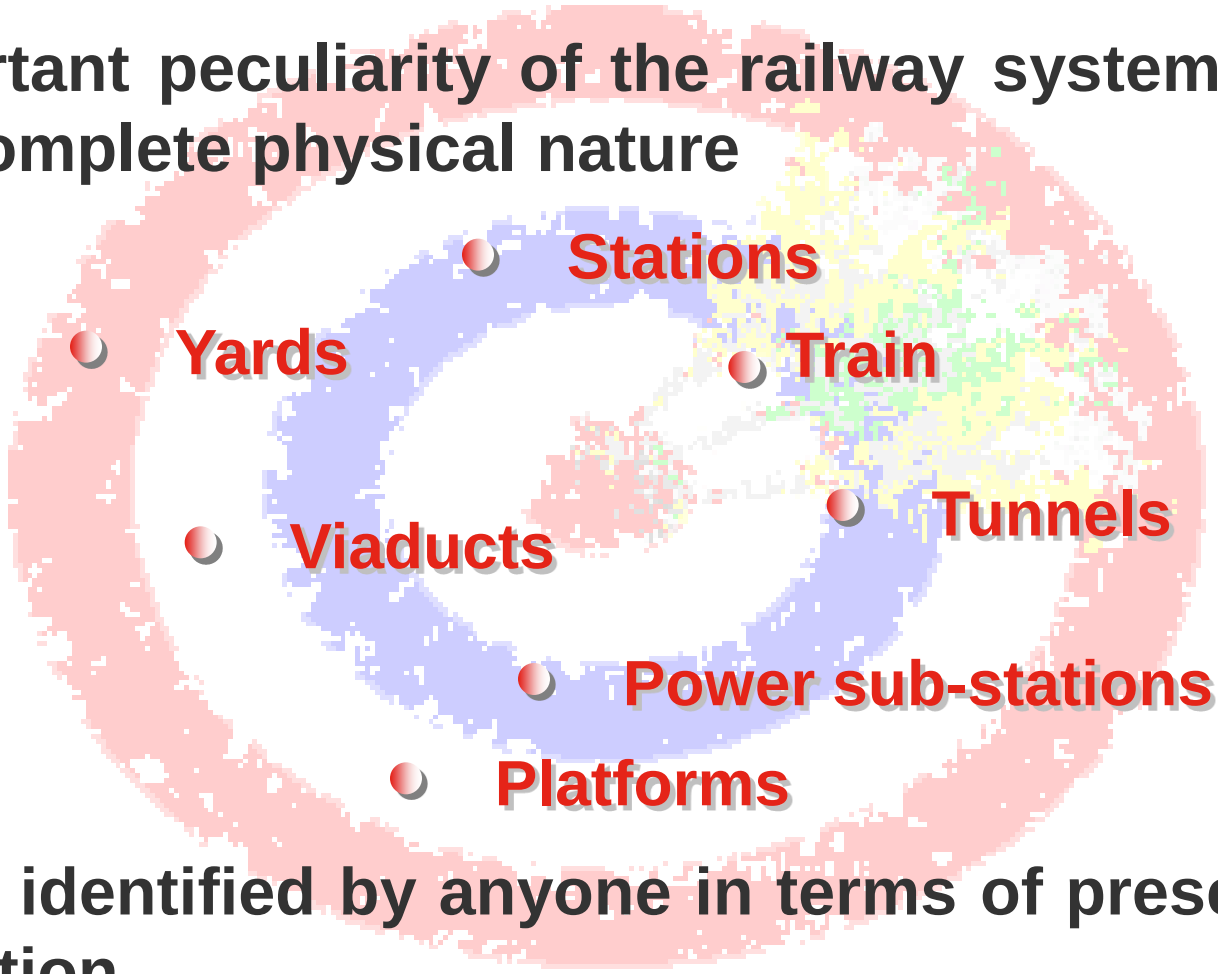
Figures

- **1.500.000** daily passengers
- **3.000.000** daily presences (in stations only)
- **60.000** employees
- **9.000** daily trains
- **24.300** km tracks
- **1.350** km High Speed Lines
- **1.380** km tunnels
- **530** km bridges and viaducts
- **2.209** railway stations
- **375** power-stations
- **218** freight terminals
- **3** ferry-boats

FERROVIE DELLO STATO ITALIANE

Critical components of railway infrastructures

An important peculiarity of the railway system is its almost complete physical nature

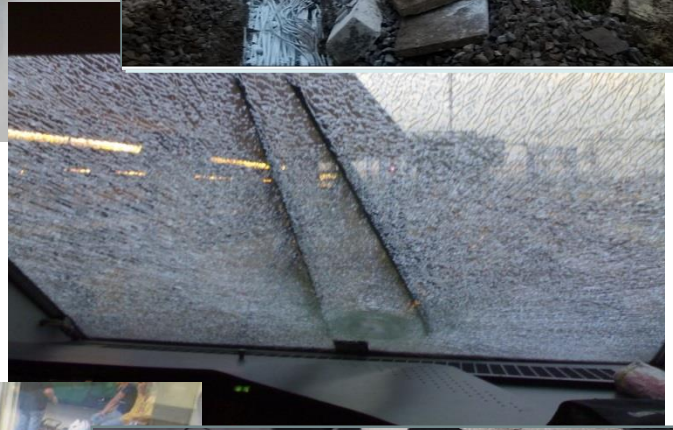


It can be identified by anyone in terms of presence and function

FERROVIE DELLO STATO ITALIANE

The threats: human origins

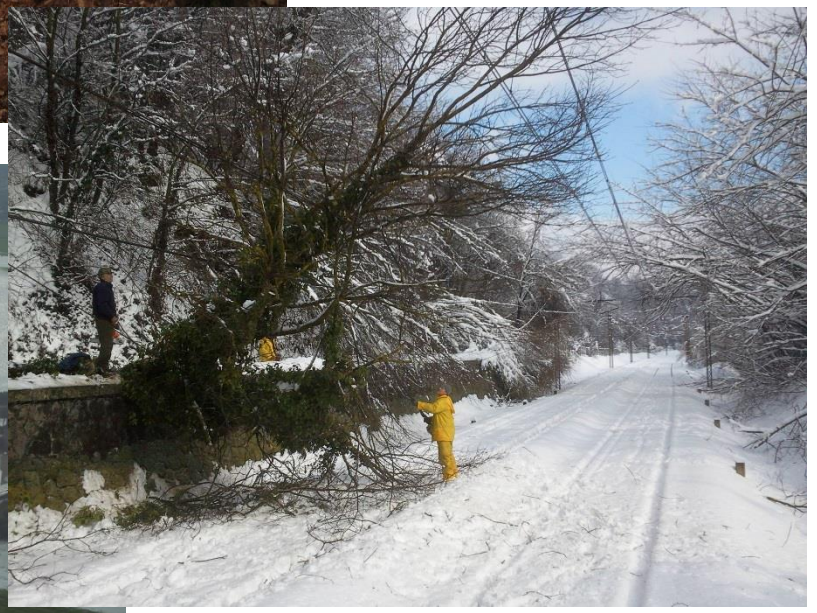
- THEFT
- ROBBER
- AGGRESSION
- GRAFFITI
- FIRE
- RUNNING OVER
- STONE TRHOWING
- OBSTACLE ON THE LINE
- UNDUE PRESENCE
- SABOTAGE
- LEVEL CROSSING
- VANDALISM
- TERRORISM



FERROVIE DELLO STATO ITALIANE

The threats: natural disaster

- FLOOD
- FIRE
- LANDSLIDE
- SEISMIC
- SNOW
- WIND



FERROVIE DELLO STATO ITALIANE

The threats: IT and technical problems

- TROUBLESHOOTING
- FAULT SYSTEMS
- CYBERCRIME
- BLACKOUT

FERROVIE DELLO STATO ITALIANE

FS Security Regional Departments

The Security Department of the FS Group is composed of:

- One HQs in Rome;
- Several RFI and Trenitalia security departments on the national territory

- 13 RFI Territorial Departments
- 10 Trenitalia Territorial Deparments

FERROVIE DELLO STATO ITALIANE

Corporate Security training programme

Complete security educational program on security aspects: security laws, privacy, technical methods, risk analysis, crisis management, etc.

The topics of the 5 training sessions:

1. Scenarios, foundations and security reference legal frameWORK
2. Security organizational system
3. Security management and operational tools – Part 1
4. Security management and operational tools – Part 2
5. Effective communication and behavioural methodologies

Training on the job

Practical overview and training on the jo

FERROVIE DELLO STATO ITALIANE

Railway Police and Departments

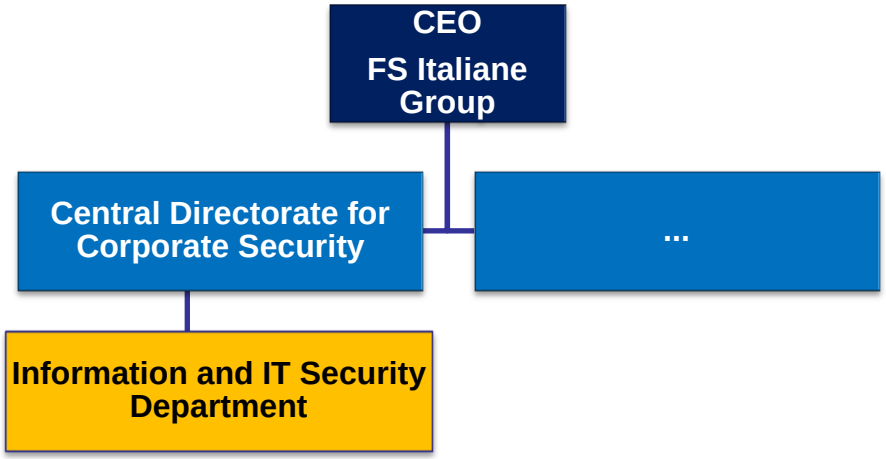
FERROVIE DELLO STATO ITALIANE

Italian Railway Police Activities

Stations - Trains

- Surveillance in stations
- Check of critical points and railway lines
- Check of the flow of passengers from / to trains
- Check of left-luggage
- Train patrolling

ICT Security in FS Italiane Group



- IT Risk Analysis and Management for the FS Italiane Group
- Information Security policies, guidelines, methodologies and standards definition and implementation
- IT Security legal and corporate compliance
- Monitoring and reporting on the state of IT security at FS Italiane Group
- Security Incident Management
- Crisis management
- Program Management in IT security solutions' design and development
- Establishment of the Italian Railways IT Security Competence Center

FERROVIE DELLO STATO ITALIANE

What are we doing?

- Study attack scenarios to improve our resilience, reaction and defence
- Use real-time detection tools in order to reduce an attack's damage and spread
- Analyze open source on the Internet to find out the possibility of an intentional attack
- Co-operate with law enforcement administrations to increase our capability to fight against attacks and their causes

FERROVIE DELLO STATO ITALIANE

Agreement with the Communication Police

On January 2015 an agreement was renewed with the Communication Police, the first one was signed on July 2003, for the prevention of IT crime on management IT systems used by the FS Group.

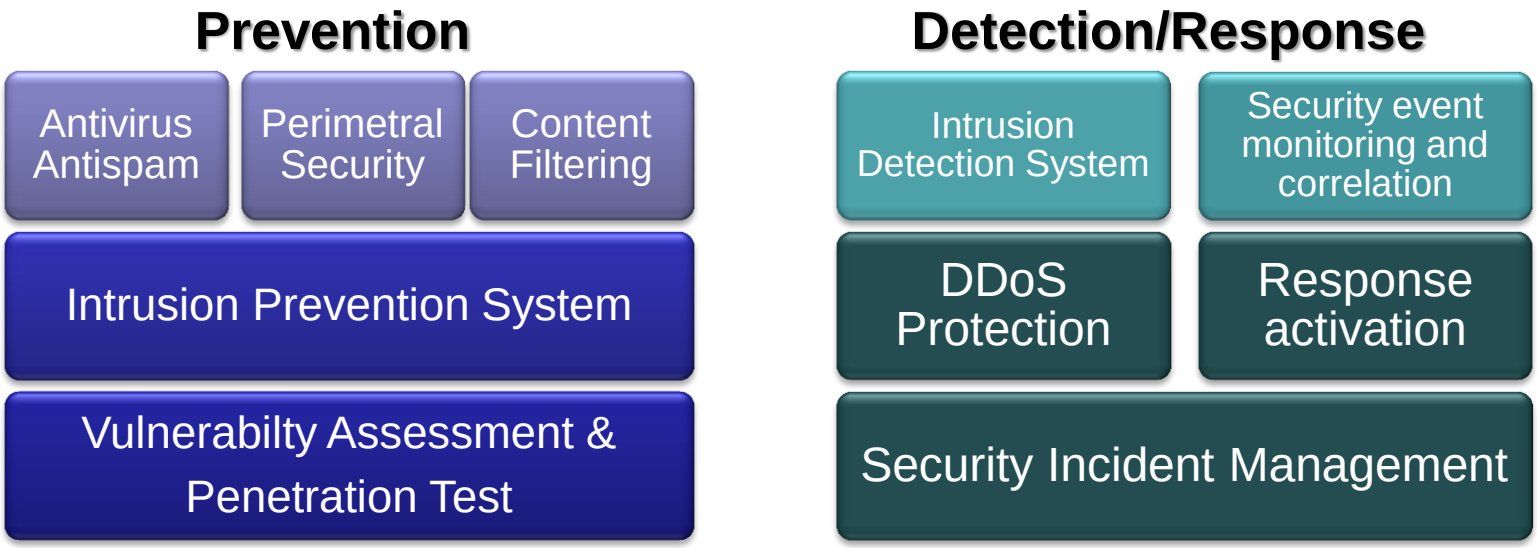
This agreement provides continuous information exchange and operational coordination between Security Department and CNAIPIC (National Crime Information Technology for Critical Infrastructure Protection).

FERROVIE DELLO STATO ITALIANE

Cyber attacks management

- ✓ **Prevention:** indentify and apply countermeasures to prevent attacks and / or fraudulent actions that could threaten the Company
- ✓ **Detection and Response:** identify cyber attacks and activate responses for mitigating the potential impacts.

The damage is inversely proportional to the speed of reaction



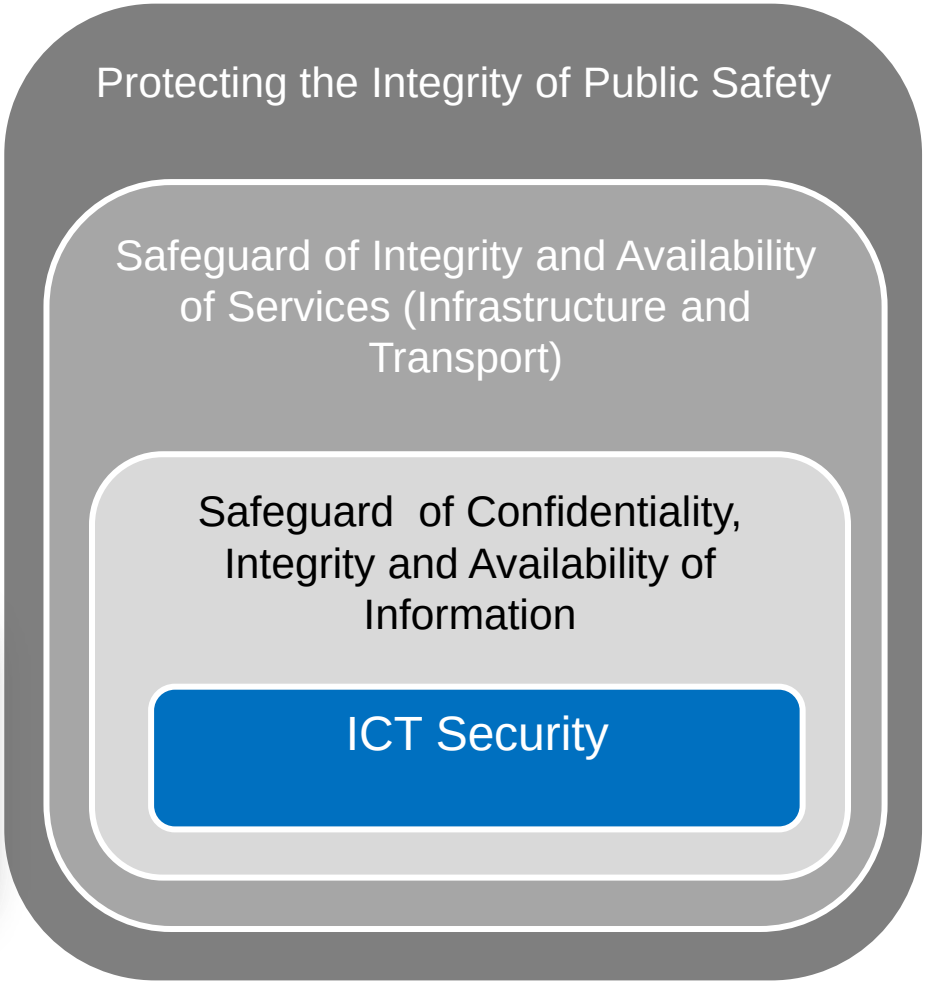
FERROVIE DELLO STATO ITALIANE

Protecting Critical Infrastructures and the Information

The protection of critical infrastructure:

- depends on IT security
- limits the damage caused by the alteration of:
  - Integrity
  - Availability
  - Confidentiality

  of information assets and IT



FERROVIE DELLO STATO ITALIANE

COLPOFER

COLPOFER: the security operational answer

www.colpofer.org

Email: colpofer@fsitaliane.it

COLPOFER Member Countries

COLPOFER is made up of representatives of **security departments** of railway companies and **police authorities** responsible for the surveillance of the railway environment from the following Countries:

- Austria
- Belgium
- Bosnia Herzegovina
- Croatia
- Czech Republic
- Denmark
- France
- Hungary
- Italy
- Latvia
- Lithuania
- Luxemburg
- The Netherlands
- Poland
- Portugal
- Romania
- Russia
- Serbia
- Slovakia
- Slovenia
- Spain
- Switzerland
- United Kingdom

COLPOFER *(Collaboration of railway police and security services)*

COLPOFER was created in 1980, when a group of railway companies and railway police decided to join forces and set up a European association.

COLPOFER mission is to improve the protection of persons, premises, trains and information within the railway system through a strong cooperation between railway police forces and railway companies security organizations.

COLPOFER's mission is to improve the protection of persons and premises by:

- *The **exchange of information and shared experiences** between members in the fight against crime in the railway environment*
- *The defining of a **common railway security strategy***
- *The **elaboration of recommendations** aimed at improving the security level within the railway environment and **the public perception of security** (customers, railway staff, contractors and suppliers)*

COLPOFER is a UIC Special Group.

COLPOFER operational activities

- Information exchange on crimes and prevention solutions
- Security Incidents Statistics (Graffiti, Metal Theft, Aggression against Railway Staff, Vandalism, etc.)
- International special transport flow (sport events, demonstrations, etc.)
- Guidelines for security solutions
- Collaboration with Police Forces
- Participation within the following International Institutions:
  - LANDSEC (Land Transport Security Expert Group) c/o European Commission DGMOVE
  - IWGLTS (International Working Group on Land Transport Security)
  - UIC Security Platform

COLPOFER Working Groups

- PROTECTION AGAINST TERRORIST AND EXTREMIST ACTIVITES
- CYBER CRIME
- METAL THEFT MONITORING CELL
- FRAUD/TICKET FORGERY
- GRAFFITI
- TECHNOLOGICAL INNOVATION
- LARGE EVENTS
- CONTROL ROOMS
- INTERNATIONAL FREIGHT TRAFFIC
- PAN-EUROPEAN CORRIDOR X

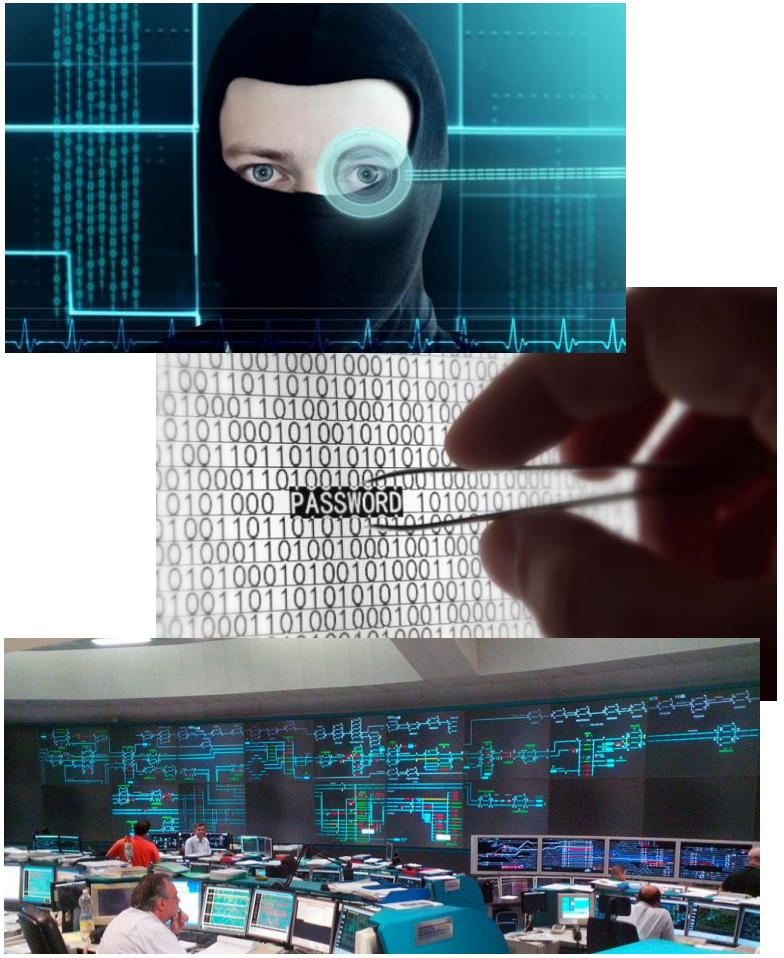
WG Protection against Terrorism and Extremist Activities

- Security organisation and procedures of railway companies (es. harmonisation of procedures concerning cross-border security threats)
- Cooperation with Police and other partners
- Best practices
- Case studies

WG Cyber crime

Objective

- Information Exchange between IT Security Organisation in railway companies
- Guidelines for Application of Means and Assets for Mitigation of Computer Attacks against Railway Information Infrastructure
- Scouting of IT security solutions



WG Fraud/Ticket Forgery

Objectives

- Ticket Forgery and Credit Card Fraud information sharing
- Creating alerts and training materials about tickets forgeries and international ticket fraud (in cooperation with EURAIL Group, CIT ecc)
- Promoting staff training in accordance with UIC Code 361 ("*Revenue security in international passenger traffic for application in the fields: passengers, IT department, internal audits, finance and all other fields concerned*")
- Testing product development (e.g. CIT 2012) concerning security features and forgery detection tools
- Collecting information on ticket forgeries and information sharing among Members
- Best practices exchange on preventive measures
- Exchange of information about possible successful police operations
- Exchange of information concerning how fraudster behavior changes
- Promotes real-time information exchange about suspected frauds

WG Technological Innovation

Objective

- Analyse the technological and legislative aspects of technology related to security and to develop and implement them from an operational point of view by looking at the advantages and disadvantages of using them.

Organisation

- The Chairman of the WG is the COLPOFER Board
- The members of the WG include technicians, engineers, IT professionals and legal professionals from within the COLPOFER organisation
- The WG “Technological Innovation” members can change according to the needs of the specific projects
- The WG “Technological Innovation” meetings can vary according to the needs of the members

WG Big Events and Sub WG Control rooms

Objective

- Information sharing on railway transport requirements of Big Events at a national and international level
- Security plan of railway transport during Big Events (physical, technological and operational measures)
- Operational communication between railway companies
- Best practices exchange regarding Control Room management and technological instruments

WWW.COLPOFER.ORG