INTERNATIONAL UNION
OF RAILWAYS

UIC Security Platform

New technology

Protection measures for railway assets

November 2013

Contents

This document results from the activity of the "New Technology" Working Group within the framework of the UIC security platform. This group is chaired by RFI (Italian railways).

The document aims at summarizing some guidelines, shared during the "New Technology" Working Group meetings held so far, dealing with the protection of railway assets against threats from daily delinquency to more sophisticated terrorist attacks. Stations, tunnels and technical premises will be addressed in order to decide the best technologies to help cope with the different threats.

This document is intended for guidance only. It should not be cited as a requirement.

Introduction

The strategic importance of the railway system in the economy of a nation and the growing focus on the issues of counter-terrorism, have increased the interest of railway companies in security systems and made it necessary to define clear and effective methods for fighting threats against railway assets.

In this regard, in 2008 a permanent international Working Group on "New Technology" (NTG) was created within the UIC Security platform. The major European railway companies participate in sharing experiences gained in the field of security with well-established methods and tools, proposing new helpful technologies.

In particular, the group has aimed to scout new technologies and define new methodologies, new solutions or even improve the ones already implemented, in order to contrast threats against railway assets and people.

Collaboration with PROTECTRAIL

The NTG has collaborated with the members of the Stakeholders Advisory & Validation Group (SA&VG) within the PROTECTRAIL project. PROTECTRAIL is a research project co-funded by the European Commission in the Seventh Framework Programme for Research and Technological Development. The task is to develop an integrated system to improve the security of rail transportation through better protection of railways and trains, and to reduce disparity in security between European railway systems.

Planning methodology for a security investment

A security intervention, aimed at protecting goods and people, requires a thorough and careful analysis of the problem. If the intervention lacks the planning phase, the risk is to implement an ineffective system that doesn't exactly meet the objectives.

Thanks to the progress of technology in recent years, many tools are now available for security aims.

However, the planning of an intervention is not just about choosing the most suitable technological device to deploy, instead is the result of a careful analysis that takes into account several factors.

Three main factors need to be taken into account:

Human Factors

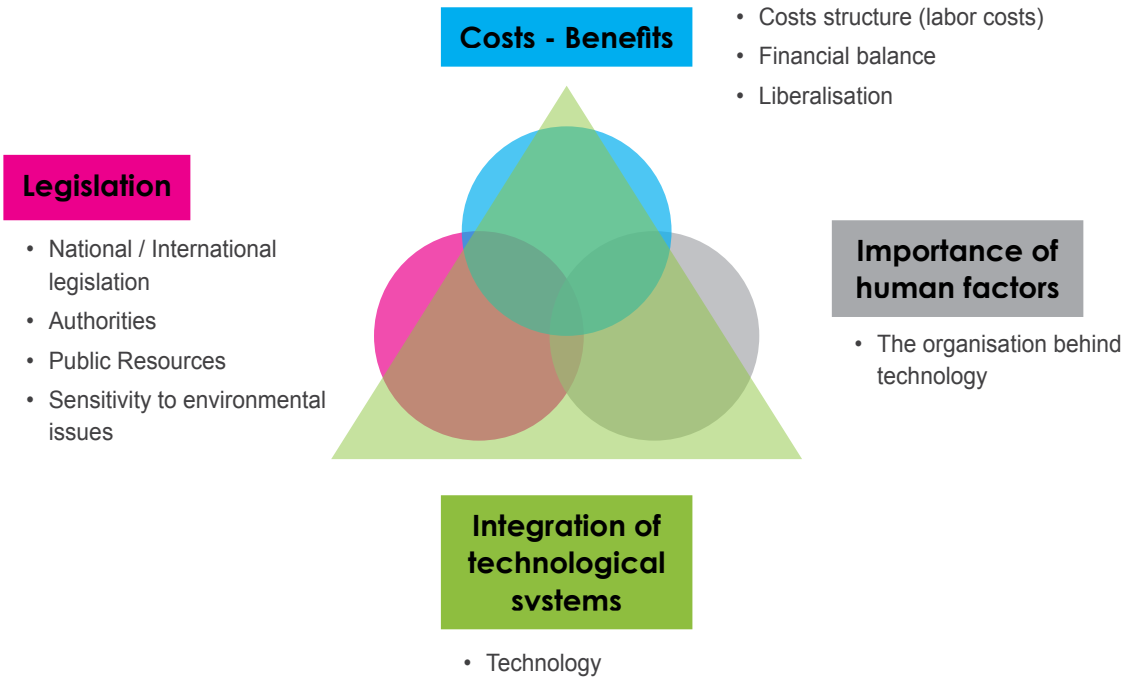
First of all, one must not ignore the importance of the human factor as a system of organization that supports the technology used to counter a threat. Every technology, in fact, must be supported by a proper organization of security which translates into a set of procedures to be followed in order to exploit the full potential of the technology. Therefore, the procedural and organizational security measures must be planned in parallel to technological measures.

Legislative framework and ethical aspects

It is necessary, while planning a security intervention, to make a careful analysis of the legislative framework to be applied, taking into account factors such as the available public financial resources, the privacy law and the common sensitivity to environmental problems.

Cost-benefit analysis

Finally, one has to consider a cost-benefit analysis; there must be proportionality between benefits and costs to be incurred.



1. Identify the vulnerabilities

The first step consists in identifying the vulnerabilities. In this regard it is necessary to understand who or what the threat is, when and where it can materialize and the reasons for such a threat to occur.

During the meetings organized by the UIC, railway companies have pointed out, based on their experience, the main threats that may occur in the railway field from minor crime to terrorist attack : Vandalism (graffiti, damage to equipment, stone throwing…), thieves (theft of copper, theft of equipment, theft of technology, theft of passenger property…), terrorist attacks (explosive, CRBN, fire, sabotage, …);

Further steps are as follows:

2. Define organizational procedures

The organizational procedures may include the planning of patrol on railway assets. They can be addressed by railway staff through the supervision activities, with or without the collaboration of the police.

Finally, a further organizational procedure could be the closure of the asset to be protected when rail operations are not carried out or procedures for controlling access in railway operational buildings.

3. Choose the most adapted technological and infrastructural measures

Infrastructural (passive protection):

They are composed of all physical tools interposed between the possible source of danger and what must be protected. The purpose of these tools is to counteract as much as possible the attempt to break into them, by overthrowing or overcoming them. The obstacle is the more effective the longer it takes to overthrow or overcome. The passive security systems includes measures such as fencing, bulletproof glass, shatter-proof windows, armour plating, gates, locks, barbed wire, and so on.

Technological tools (active protection):

They are composed of all the electrical and electronic devices that are able to perform the following functions:

- Monitor the area to be protected using detectors of events;
- Discourage the completion of criminal activity by deterring tools;
- Generate alarms and send them to a remote control room.

The active systems consist essentially of:

- Intrusion Detection Systems;
- Access Control Systems;
- Video Surveillance Systems with or without video analytics.

Guidelines for security plants

The protection of railway assets made by using technological tools could be realized through the installation of the following security measures:

- infrastructural measures,
- intrusion detection and access control systems,
- video surveillance systems.

Here below are some general guidelines to keep in mind when setting up a security plant.

A closer look on protecting some railway assets is proposed on the following pages:

- Railway stations;
- Technical premises;
- Tunnels.

Infrastructural measures used to protect railway assets

They mainly consist in fences and gates. The fencing should be installed on a reinforced concrete plinth in which the support poles are drowned; poles should be made of galvanised steel and fencing panels should be hooked up to poles by joints and unscrewing bolts.

Laying concrete plinth is necessary to give adequate resistance at fence thrusting. Panels should be made of horizontally or vertically meshed wires of suitable size in order to prevent climbing over and discourage cuts of the panel.

Starting from the plinth, fence panels should not be less than 2.5 metres high in order to make any attempt to climb over more difficult. In order to increase the level of protection, barbed wire could be installed on top of the fencing.

Intrusion detection systems and access control systems

Their purpose is to prevent unauthorized access of people in critical areas or premises.

They are generally composed of a control unit and a number of “field detectors and sensors” which are essentially of two different types:

- magnetic contacts, generally installed on doors, gates and windows;
- dual technology volumetric sensors (infrared and microwave) generally used in closed premises.

Such a system could work in combination with video analytic systems in order to detect unauthorized people moving in controlled premises.

The access control system could be used to allow authorized people to enter closed sensitive premises. Identification can be made by different tools, such as contactless readers (such as RFID technology), magnetic stripe card readers, keypads or electromechanical locks.

Video surveillance systems

They allow to monitor critical areas and to provide videos recorded for forensics. They are composed of different recording systems (DVR’s, NVR’s or servers), network devices, wiring and, of course, cameras of different types.

As a general rule, some precautions should be kept in mind when installing cameras:

- use vandal-resistant cases;
- place cameras as much as possible in a way that they look each other;
- place cameras at least at 3 metres high, where possible, to avoid them being vandalised;
- place protective films on case glasses to make it easier for them to be spray painted;
- install external cables in cut-resistant ducts.

1. Railway stations

When implementing security measures in a railway station you need to carefully design the lay-out of that station in order to identify where perpetrators could act. So forth, crowded areas, paths where people walk through and hidden or poor lit areas should be investigated in order to correctly outline the project lay out. Technical premises where rail traffic signalling or telecommunication devices are installed are also to be considered when laying-out your plant.

Main station areas to be protected are:

- areas in front of station entrances;
- external open areas (e.g. car park);
- entrances, hall and waiting rooms;
- underpasses;
- platforms.

CCTV System

The next table summarizes the main security measures to be implemented, also in order to increase perceived security by customers. Station areas to be subjected to surveillance are mainly the following:

Areas	Technologies	Advices
In front of station entrances	Dome cameras and fixed cameras	One or two dome cameras facing the external area, fixed cameras for main building entrances
External open areas	Dome cameras	Set the patrol function
Access gates to the station	Fixed or fixed dome cameras	According to your privacy law, you could use cameras for face detection
Entrance hall	Fixed and dome cameras	Fixed cameras on sensitive premises (ticket machines, ticket offices, etc.)
Waiting rooms	Fixed and dome cameras	
Passageways, stairs, lifts	Fixed or fixed dome cameras	
Underpasses	Fixed vandal resistant or fixed dome cameras	
Platforms	Fixed cameras	Maximum coverage of 35 - 40 mt per camera

Intrusion detection and access control system

The intrusion detection and access control systems could be used for protecting critical premises or to control entrances to the station, especially in night time closures.

For premises protection, see the section I.6.3 (Technological premises).

Infrastructural measures

Such protection of railway stations is to be intended only in very harsh security conditions, such as suburbs or in bad social contexts. Protection can be carried out by installing fences around the station, gates, shatter-proof glasses on windows and doors.

2. Tunnels

Usually tunnel protection is made up with fencing, access control systems, intrusion detection systems managed by appropriate access procedures and, in certain situations, CCTV systems.

Security interventions should interest:

- Tunnel entrances;
- Shafts.

But protecting a tunnel not only calls for a security analysis, but also requires a focus on safety conditions. So far the tunnel length becomes a driving factor for deciding security measures to be set up: different lengths call for different security measures! Keeping in mind average train lengths, their breaking distances and escape distances, we can find a breakeven point at the tunnel length of approximately 3 km.

The next table summarizes which security measures should be implemented, depending on the tunnel length, trying to meet security needs with a cost-efficient system.

	Security measures	**≤ 3Km**	**> 3 Km**
Tunnel entrances	Fences on the top of the tunnel entrances	h= 2,5 mt	reinforced h=3 mt
	Fences along the tracks	250 mt both sides	500 mt both sides
	CCTV system for tunnel entrance control	One camera for each entrance	At least two cameras for each entrance
Shafts	Alarm systems	Integrated with access control	Integrated with access control and TVCC system
	Fences around areas around entrances	h=2,5mt	h=2,5mt

Tunnel entrances - Length: ≤3km

Security measures at tunnel entrances should be infrastructural, with appropriate fences as described in the main guidelines, installation of which is provided along both tracks and on the top of the tunnel entrances. The latter case is limited to the tunnels where this area is easily accessible by potential intruders (see fig. 1 and 2), that may perform acts of sabotage on the line or against the train running.

It is best practice to provide this class of tunnels with at least “one camera CCTV system” per tunnel entrance, limited to critical situations, based on the analysis of the specific socio-environmental context.

Figure 1 – Example of tunnel to be protected with fence above the entrance

Figure 2 – Example of fence above the entrance

Tunnels entrances - Length: >3km

These areas should be provided with CCTV systems with at least 2 cameras, one each side of the track, in order to monitor entrance areas with a coverage of at least 60÷80 meters in front of the tunnel entrances.

It is best practice to install these cameras at such a height to frame the tunnel entrance, on sufficiently stiff frames to allow optional video-analytic systems work properly, installing cameras in vandal-resistant IP66 proof cases, equipped with deep infrared lightning systems (≥920m).

Shafts

Such accesses, usually used for managing services or for emergency situations, must be properly monitored on an ongoing basis to prevent the entry of unauthorized people.

As indicated in the previous table, the shaft must always be monitored by different systems depending on the tunnel length (L) as follows:

- for tunnels L ≤3km: setting up of intrusion detection and access control systems;
- for tunnels L >3km: setting up of intrusion detection and access control systems integrated with a suitable CCTV system.

For tunnels longer than 3 km, shafts should also be provided with fencing to protect the area around the shaft entrance. The gate of the protected area should be provided with an access control system allowing only authorized people entrance (fig.3).

Figure 3 – Shafts: example of a fence around shaft entrance

3. Technical Premises

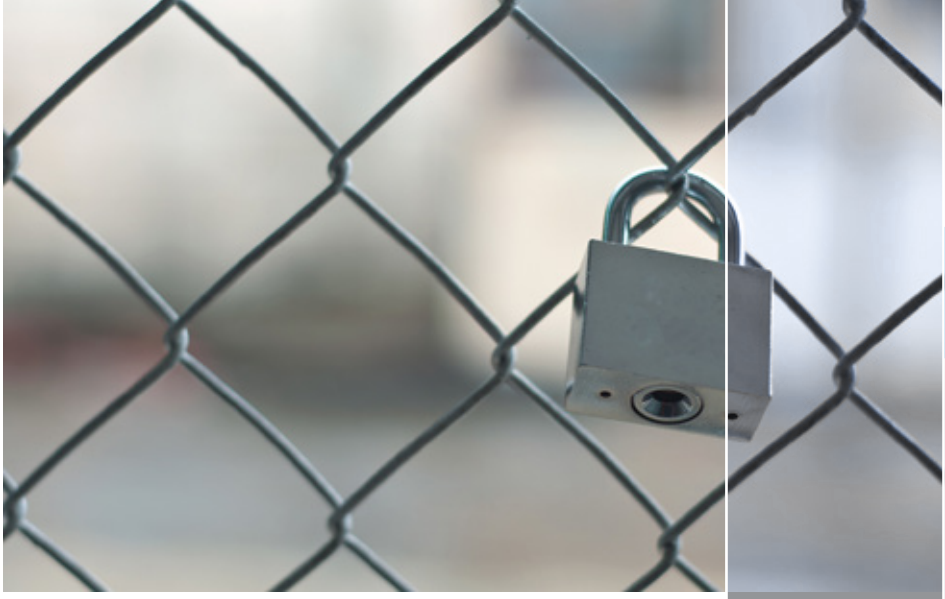
Protective measures for technical premises depend on the strategic level of importance, the analysis of the specific socio-environmental context of the area and on the following other criteria:

- sensitive documentation inside the premises;
- core business technical equipment, (such as rail traffic controls);
- unattended premises.

As for tunnels, the next table shows protection measures to be taken into account.

			Not attended		
	Security Measures / Critical Level	Attended h 24	Low	Medium	High
CCTV System	Fixed Dome on wall of premise			X	X
	External Fixed Camera				X
	Internal Camera				X
Intrusione Detection / Access Control System	Magnetic Contact		X	X	X
	Badge Reader / electric-mechanical locks				X
	Volumetric Sensors			X	X
	Inertial Sensors				X*
	Acoustic Device		X	X	X
Physical Measures	Security Door				X
	Gates				X
Alarm Management	Phone Dialer	X	X	X	X
	Control room			X	X

* optional



It is best practice to install one or two cameras in order to monitor the area around the premise and to frame the face of the intruder (according to your privacy law).

In some cases it is recommended to install cameras inside the premises.

For infrastructural measures and for intrusion detection and access control systems to be implemented you can refer to the specific section in the main guidelines.

For infrastructural measures to be implemented you can refer to the specific section in the main guidelines.

240 members
across 5 continents...

The worldwide association of cooperation for railway companies

2 500 billion passenger-kilometres

9 500 billion tonne-kilometres

More than 1 000 000 kilometres of lines

INTERNATIONAL UNION
OF RAILWAYS

Conception: UIC Communications Department | November 2013 | English editor: Helen Slaney | Design: Marina Grzanka | Photo credit: © Fotolia