
# Rail High Speed Network
# SECURITY HANDBOOK

INTERNATIONAL UNION
OF RAILWAYS

978-2-7461-2454-7

# CONTENT

# RAIL HIGH SPEED NETWORK SECURITY HANDBOOK

## Scope and context of the document

**The contents of this document shall not be cited as requirements, bylaw or any other kind of legal or paralegal enforcement. The Rail High Speed Network Security Handbook is intended for guidance only.**

The guidance drafted in this document provides use for application in a worldwide geographical scope. Its generic security concepts, consider to advisement in this handbook are to be regarded in coherence with the technical, legislative or operational rules in place, nationally and/or internationally.

The generic security concepts presented, consider both rail conventional lines as well high speed on regards to any existing, renewed, upgraded and new railway networks.

It is designed in particular for Rail Security Directorates, Security Managers, technical project teams and/or any security experts involved in the process of designing, assessing or choosing appropriate security preventative or mitigation measures *for*:

- Rail infrastructure and Rail services planning and development;
- Rail infrastructure and rolling stock design and maintenance;
- Rail infrastructure and Rail high speed networks services implementation, evaluation, and management of security.

# EXECUTIVE SUMMARY

Protecting passengers, staff, trains, and stations from threats that are constantly arising in different shapes and forms, is a permanent challenge for the rail system actors and beyond. Therefore, railways cannot afford to protect their costumers, their human and structural resources from innovative and resourceful threats, with solutions of yesterday. The railways comprehensive protection and particularly its security management must go beyond the most obvious of scenarios! A true understanding of the cultural, social, economic environment where railways are implemented and operating is the first step towards the railways comprehensive protection itself.

The arising diversity of threats is nowadays the entire "playing field of *security*"; from a wide range of daily crimes (pick-pocketing, graffiti's, vandalism, metal thefts, etc.) to sophisticated threats (organized crime, conspiracy plots, cybercrime, terrorism); this demands a comprehensive, coherent and collaborative response!

That response will be only effective when the roles and responsibilities between the rail sector and national and international authorities are clear.

The Railway networks are spread over many different geographic, cultural and organizational backgrounds being difficult to monitor permanently. Thus, the networks' extension and their technical and operational complexity increase the difficulty of an effective risk-based approach security management, as security is not a railways core activity. However the complexity of the risks and threats towards passengers, staff and rail property demands for an enhanced and comprehensive railway systems protection which needs joint actions between the railways and the relevant national and international authorities.

Against this background the current handbook is meant to provide guidance in support to better frame the security policies and measures, in regard to national and international specific requirements, demands and needs.

# 1. High Speed Rail (HSR)

High Speed Rail (HSR) is a type of public transport system that is becoming more and more popular world-wide.

Fundamentally, a HSR system is designed and built with the intention of moving an increasing number of people and goods in a fast, safe and secure manner.

Considering the various stakeholders involved, threats that the system is exposed to (e.g. crime), as well as all the technical and operational requirements, it becomes more and more complex to develop, build, operate and maintain a secure HSR system.

As a symbol of industrial and technological age, HSR can be an attractive target for criminal organizations that with their actions wish to have the greatest impact in terms of victims or disruption of the rail system.

This is critical since HSR represents to nations, a big social, political and cultural reputation regarding its transportation systems state of the art as well as major public and private financial investments.

In all events, *high speed is a combination of all the elements* which constitute the "system": infrastructure (new lines designed for speeds above 250 km/h and upgraded lines for speeds up to 200 or even 220 km/h, some worked with tilting trains, some not), rolling stock and operating conditions.

**TOTAL KM WORLD:**

In operation = 20,722
Under construction = 14,610
Planned = 16,348
Total Other Countries 2025 = 51,681

Figures from UIC High Speed Department under constant update

## 1.1. The speed factor

The rail commercial market-based definition of high-speed rail put emphasis on the door-to-door travel time instead speed as the key factor of customer interest in high-speed rail systems, but, of course, travel time is closely related to speed.

In view of the fact that many high speed trains are also compatible with the conventional network, the term "high speed traffic" is also frequently understood as the movement of this type of train on conventional lines but at speeds lower than those permitted on the new high speed infrastructure. Consequently, on some lines which are claimed to be high speed lines it is very difficult to specify a threshold when, in certain very densely populated regions, the speed is restricted to 110 km/h in order to avoid noise nuisance, or where, as in special tunnel sections or on long bridges, the speed is limited to 160 or 180 km/h for obvious reasons associated with capacity or safety.

Also the marginal cost of increases in maximum speed (in system design, construction, operating costs, and so forth) grows more than proportionately with speed increases.

In other words, the level of infrastructure investment increases significantly as the maximum speed increases.

Finally, in many countries where the performance of the conventional railway is not very high, the introduction of some trains capable of operating at 160 km/h and offering a significant level of quality - often as a first step towards a future genuinely high speed service - may already be considered as high speed.

So understanding “the speed factor” is essential when preparing and planning the rail infrastructure to be safe, secure and resilient.

### 1.2. HSR global experience context

The very first HSR line was Japan’s Shinkansen service between Tokyo and Osaka. This line was opened in 1964 with a maximum speed of 210 km/h. It is a dedicated HSR system, meaning that it was built especially for high-speed trains and only high-speed trains operate on it. The line has been extended and its maximum speed increased to 300 km/h. Today it carries more than 400,000 passengers per day. The Shinkansen line is a dedicated high-speed rail system, meaning that it was built especially for high-speed trains and no other types of trains operate on the line.

One reason the Japanese decided to build a dedicated line was that there was no capacity on the existing railway network available for adding high-speed trains.

In France, the first TGV line was opened between Paris and Lyon, a distance of 417 km in 1981. It was a dedicated line with shared-use segments in urban areas. Trains operated at a maximum speed of 270 km/h.

The TGV is a partial shared-use high-speed rail system because it uses both dedicated high-speed tracks and shared-use tracks. On shared-use segments, it travels under the same restrictions as other trains; on the dedicated segments, it now reaches top speeds of 188 mph (300 km/h) on some lines. France has continued to improve its system, adding new lines and technical improvements to the TGV trains themselves. Today’s TGVs are faster, more comfortable, and more efficient than the original trains, and there is even a double-deck version on the heavily travelled Atlantique line.

The high-speed program in Germany included extensive work to upgrade many of its mainline tracks for speeds of 200 km/h, continuing an earlier effort to improve the nation’s railroad network. This later effort comprised a coordinated program of improvements in infrastructure, rolling stock, and service.

Today Germany is building new, dedicated high-speed tracks along many shared track segments to improve service by adding capacity and increasing speed. Germany has also continued development of the ICE trains and has developed a tilting version (ICE-T)

for use on lines with many horizontal curves, as well as faster versions. The latest-generation trains (ICE3) travel at speeds above 330 km/h.

Spain opened its first high-speed rail line in 1992, in connection with the World Fair in Seville. The line between Madrid and Seville is interesting because although it was built for high-speed rail trains it allows some other trains to use the high speed line (for example, the TALGO overnight service from Barcelona).

As an example of extending high-speed networks, the Thalys high-speed trains serve a network including France, Belgium, The Netherlands, and Germany. The Dutch trains run on existing tracks with other passenger and freight service, operating as regular passenger trains. Thalys trains operate at speeds higher than 300 km/h, and its rolling stock is designed to operate on all four countries' different signalling and power distribution systems. That is recognized as rail interoperable systems.

One other example is the English Channel Tunnel high-speed line that opened in 1994. This engineering project has provided excellent rail service between the European continent and Great Britain, significantly reducing travel times and attracting a large number of former air passengers. The system is directly linked to France and Belgium's HSR network.

What this brief survey indicates, is that there has been much activity in developing high-speed rail systems in Europe. There are two key reasons for this: Europe contains many large city-pair markets that can be served easily by HSR, and Europe has a long history of support for intercity passenger rail services. Because high-speed rail is important in Europe, the European Commission adopted a European high-speed network which links the individual national systems into an integrated network.

### 1.3. Rail security in HSR European context

The development of the trans-European high-speed rail network has been a major European achievement. Furthermore, considerable work has been undertaken to harmonise safety requirements for the railway sector across the EU. However, no similar exercise has been done as regards railway security.

In the rail sector the European Commission considers to develop EU-wide security recommendations and guidance for the high-speed rail network. Consideration should also be given to having EU legislation that requires security features to be incorporated into the design of rail rolling stock and infrastructure. EU level baseline security recommendations and guidance will provide a common and adequate level of protection to the rail transport for the benefit of both passengers and freight, ensuring consistency on the approach to cross borders operations. This intends to minimise the risks of duplication and incompatibility of rules associated with the implementation of

local or national systems, thus assisting the good functioning of the EU Single Market. Nevertheless, mandatory requirements for transport security at the EU level must be imposed only in conformity with the principle of subsidiarity and must create clear added value for the security of transport as a whole.

## 2. Planning Rail Security

Unlike other transport modes, the rail sector depends on efficient and effective 24/7 management of a range of core internal interfaces such as the interface between wheel and rail and external internal interfaces between third parties. A safe and secure high speed or conventional railway relies on effective management of this and many other core interfaces. Keeping these interfaces working effectively whilst encouraging technical innovation will be a core challenge as the sector models the future rail system.

## 3. Rail Security prevention

When an attack occurs, the public and the newspapers naturally ask the authorities why more security measures and detection systems were not installed in the past in order to reduce the occurrence not to detect and stop the perpetrators. Every attack is followed by a political debate and some mitigation plans are proposed to balance the risks and to satisfy the public requests.

This is mainly considering the railway traffic statistics growth, the security systems and organisations costs and the legal and ethical standard that it is possible to understand investment history in the domain over Europe states. One main trend is to define security plans able to adjust the response to the current security threats. The needs vary with the traffic evolution, the international contexts, the geopolitical movements, politics elections and decisions, budget constraints and other reasons.

## 4. Rail Security main threats

Facing the challenge of enhancing the railway security by taking a systematic top-down approach (i.e. to search for an all-inclusive solution valid for all possible threat scenarios), the Rail High Speed Network Security Handbook addressees four areas of threats: terrorism, violent crime, property crime and cyber crime.

### 4.1. Terrorism

Terrorism is the systematic use of violence (terror) as a means of coercion for political religious or ideological purposes. In the international community, terrorism has no legally binding, criminal law definition. Common definitions of terrorism refer only to those violent acts which: are intended to create fear (terror); are perpetrated for a religious, political, or Ideological goal; and deliberately target or disregard the safety of non-combatants (civilians). Some recent definitions include acts of unlawful violence and war. Whenever it happens, terrorism is a crime with a purpose and it is often violent and catastrophic in consequences. Terrorists use violent crimes as the key tool to make everybody aware of their presence and aims. Terrorists believe that, without violent crime, their presence and message would go unnoticed and not reach the level of public importance they seek. Every business, organization, geographic location, and building poses some opportunity for terrorists to exploit their specific agenda. Therefore, terrorism is a premeditated crime that embraces violent and forceful acts with the purpose of supporting a group's political, religious, or ideological agenda by rapidly promoting fear and a lack of confidence in one's personal security, creating sudden and unexpected social and economic hardships in many sectors such as private, commercial, and government.

Terrorism threatens the society to its foundations and challenges the fundamental sense of security and the conviction that it would be possible to learn to work and live together in spite of differences in religious, social, or political beliefs.

Behind terrorism, there are often large organizations or perpetrators that are linked to these organizations. Therefore, security against terrorism involves collaboration between government intelligence, and law enforcement authorities and critical infrastructures such as the railways.

### 4.2. Violent Crime

A violent crime is a type of criminality in which the offender uses or threatens to use violent force upon the victim. This entails both crimes in which the violent act is the objective, such as murder, as well as crimes in which violence is the means to an end, (including criminal ends) such as robbery. Violent crimes include crimes committed with weapons. A violent crime may end with injury or death, both on the part of victim and offender.

Violent crime is also increasing within the railway context particularly in the urban areas. The complex social and economic environments contribute to that. It is often that in big cities stations and in specific railway lines the number of events associated with violent crime is directly linked with poor social and economical conditions.

Also daily incivilities on the railway premises like littering, spitting, smoking on trains, using abusive language etc. can lead to violent crime against other users and railway staff.

### 4.3. Property crimes

Property crime is a category of crime that includes, among other crimes, burglary, larceny, theft (from minor pick-pocketing to major motor vehicle theft), arson, shoplifting, and vandalism. Property crime only involves the taking of money or property, and does not involve force or threat of force against a victim. Although robbery involves taking property, it is also classified as a violent crime, as force or threat of force on an individual that is present is involved in contrast to burglary which is typically of an unoccupied dwelling or other unoccupied building.

These crimes are committed when someone with an opportunistic, wilful and premeditated action, damages, destroys or steals someone else's property. Regarding the railway property these crimes include metatheft or vandalizing a building or an asset.

Property crimes are within the railway context by far the most commonly committed crime and represent the daily delinquency and concern of the rail infrastructure managers, rail operators and industry.

### 4.4. Cybercrime

According to the European Cybercrime Centre, we all face challenges coming from the rapid development of the Internet. More than 24 billion devices will soon be connected 24/7 to the Internet and, with the innovation of sensors and the ability to connect "things" (cars, train, fridges, boats, medical tools, homes), considerable amounts of data will be generated about our behaviour, locations, health, web searches and so on.

The Internet and its huge potential will revolutionise our lives and developments in society, however in the process lots of potentially personal information will be accumulated. The report and movie highlight the pros and cons and will hopefully also trigger a discussion on privacy, how much information we should share, and how to secure our data.

Railways are nowadays particularly dependent on computerised management systems. For example railway signalling system ERTMS will be the key element in ensuring all traffic coordination within the EU. With the full deployment of ERTMS a successful cyber-attack could for example close down one or several railway international connections with a substantial impact on EU rail passenger and freight movements.

Railways as well as many other critical sectors are realizing that the cyber security threats to business operations is a growing concern; not just to governments, private enterprises and other businesses.

Setting basic principles will help to develop and put in place Cybersecurity strategies but keeping in mind that a comprehensive policy framework ensuring citizens' trust and online privacy is needed. These can be developed in order to create the ability to detect and respond to threatening cyber activity; to develop and maintain a detailed understanding of risk exposure to support cyber defence and business change activities.

### 4.5. New challenges in coping with threats

An analysis of stakeholder's input reveals that alongside "traditional" threats there are new perceived threats such as the use of social networks for malicious acts.

Social networking has the potential to touch relevant aspects of security including gathering and vetting publicly available open source information, gauging and influencing public opinion as well as distributing "false information" (such as how to respond after a terrorist attack). The flow of misleading information during crisis management can be either malicious or involuntary; in any case it has a severe impact on the consequences of an attack.

Stakeholder's requirements for assets protection include a wide range of technological systems, policies and human resources. However, they generally converge towards the following conclusions:

- Open-access to trains and stations and free flow of passengers is a strict requirement to guarantee a large passenger flow, but represents a weakness for the railway transportation system as well.
- Security improvements that would cause an increased level of disrupting false alarms will probably not be accepted, both by the operators and by the passengers.
- Passenger tracking, abnormal behaviour detection and automatic surveillance systems are considered to be worthwhile in order to increase railway security levels as well as citizens' security perception.
- Access control to rail infrastructure (bridges, tunnels, etc.), critical rail systems (plants, data centres) and to rolling stock (locomotives, wagons etc.) is a strong requirement.
- Surveillance systems are considered beneficial and particularly suitable for railway applications if sufficiently non-intrusive and respectful to privacy.

### 4.6. Threat perception and acceptability of security measures

In particular throughout Europe there is an increased presence of security technologies and procedures in the everyday lives of the citizens. Politicians and decision-makers seem to assume that citizens want increased security at any cost and are prepared to sacrifice their personal privacy to achieve it. However the idea that citizens seem to be willing to trade-off their privacy for enhanced security is still complex and difficult to accept in the extent to which privacy infringing surveillance measures and technologies really increase security.

There is a need to explore alternatives where security can be achieved without compromising fundamental rights.

One hypothesis regarding future security for railway systems is that, in order to increase the security levels, it is important to seek rail-specific solutions, as aviation's security approach is not possible for rail. If there is still a major step to pass regarding public acceptance, some air security concepts have demonstrated abilities to increase the security level. Besides, some recent research is focusing on seamless security concepts in order to propose an improved trade-off between the application of numerous security measures and passengers' constraints. Indeed, those concepts aim at integrating and combining several technological solutions in a way to improve the global security while limiting at the negative travelling experience for passengers.

An overall analysis of customer perception of rail services highlights many common themes across Europe. Rail users want services that are reliable: passengers and freight should reach the destination safely and on time, and facilities should be provided as advertised. In addition, the customer's value convenience is important, since clients want to be able to access their preferred service at the time they want, thus preserving the railways as open access system.

## 5. Rail Security assessment and planning

In response to the main threats, the security functions must be integrated and harmonized addressing specific responsibilities in terms of directing and orienting security reactions:

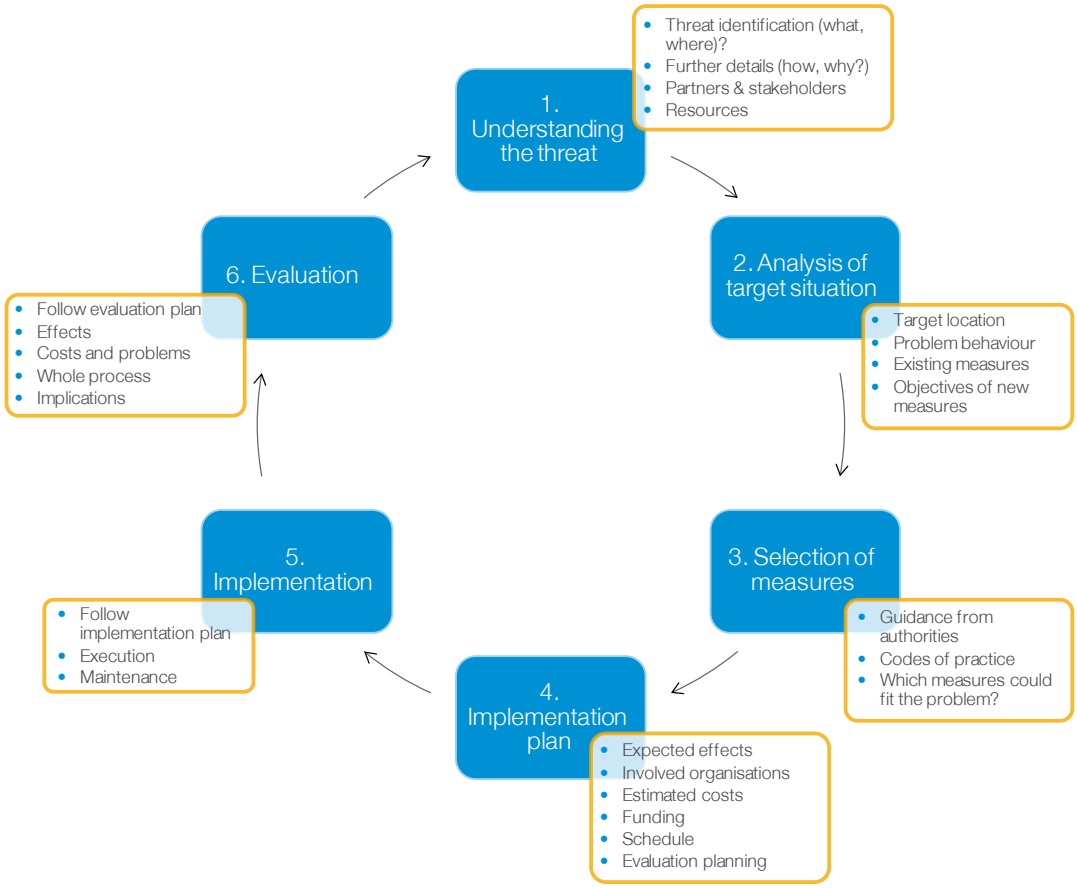
- within the rail managers and operators security organization,
- by supporting other departments during normal operations and during emergency responses,
- by training of staff within the organization,
- by providing mutual support among the organizations and local, state, and federal government bodies, etc.

To do this it is necessary to plan realistic strategies, as thoroughly as possible, in a vision of possible changes in market requirements, business approach, and key technologies in the rail sector. When regarding terrorism, one should keep in mind that:

- the perception of security threats is mainly based on past terrorist attacks,
- every moment these perceptions may be reversed by new unexpected events,
- new technologies can open new and unexpected forms of threats.

Developing a structured analysis and understanding of the problematic situation demands to have in place a process which integrates several steps, before any measure is actually implemented and evaluated. This multistep approach can provide general guidance and answers the following questions:

- What is the threat to cope with?
- How to select the best measures against the threat?
- What should be taken into account when planning the implementation?
- How can the effects of the implemented measures be estimated?




**Assessment and planning framework**

## 6. Rail Security Threat Scenarios

In order to support the assessment and planning framework there are already references to rail security threats. These provide a better understanding of the threat by being presented in scenario profiles helping the initial phases of the threat analyses, description and security measures implementation.

The threats reported in the following list have been identified through the inspection of the source material provided by European railway operators. Other sources, as European projects, conferences, etc. have been taken into account. For example, TRIPS (Transport Infrastructures Protection System) and PROTECTRAIL (The Railway-Industry Partnership for Integrated Security of Rail Transport) EU projects results consider different kinds of threats:

- Explosives & Chemical Weapons
- Biological, Radiological & Nuclear Weapons
- Illegal access
- Metal/other theft
- Robbery
- Unattended luggage
- Aggressions to staff
- Aggressions to customers
- Cybercrime
- Vandalism (e.g. graffiti, stone throwing, setting fire to railway assets, etc.)
- Obstacles on the line
- Sabotage
- Major malicious technical failure
- Improvised Explosive Devices – IED (both small and large scale)
- Improvised Incendiary Devices – IID
- Social Networking during crisis management
- High Tech Weapons (e.g. graphite bombs, e-bombs)

## Threats and rail assets

| # | Threat category | Code | Selected threat |
|---|---|---|---|
| 1 | Explosives attack of small scale | SSIED | IED |
| 2 | Explosives attack of large scale | LSIED | IED |
| 3 | Hijacking of trains or service vehicles and hostage taking | HIJ | Hijacking |
| 4 | Sabotage of tracks / equipments | SAB | Generic sabotage |
| | | | Obstacles on the line |
| | | | Major malicious technical failure |
| | | | High Tech Weapons (e.g. graphite bombs, e-bombs) |
| 5 | Arson | ARS | IID (Improvised Incendiary Devices) |
| 6 | Chemical, biological, radiological, nuclear agent | CBRN | Explosives & Chemical Weapons |
| | | | Biological, Radiological & Nuclear Weapons |
| 7 | Use of a train as a weapon | WEP | Use of a train as a weapon |
| 8 | Intrusion in the information system | CYB | Cybercrime |
| 9 | Criminal actions | CRI | Metal/other theft |
| | | | Robbery |
| | | | Illegal access |
| 10 | Black Mail | BLA | Unattended luggage |
| | | | Social Networking during crisis management |
| 11 | Vandalism | VND | Generic vandalism |
| | | | Graffiti |
| | | | Stone throwing |
| 12 | Violent acts on people | VAP | Aggression to staff |
| | | | Aggression to customers |

The aim of the Security Scenario Assessment (SSA) is to provide a list of scenarios identified by analyzing the threat resulting from the analysis of the attacks occurred in railways worldwide and on the information on past experiences of the partners involved within the project in particular. Threats are therefore combined with the resources that are deemed most critical for the railway business operation and to these resources in order to define a rail security scenario.

| Class of threat | Title of the Scenario |
|---|---|
| Terrorism | ◆ Bomb hidden on a train of dangerous goods passing in a tunnel<br>◆ Hijacking of a passenger train<br>◆ Hijacking of a cargo train<br>◆ Explosion in a station<br>◆ Mine placement within a tunnel<br>◆ Terrorist bomb attack to a railway station<br>◆ Terrorist attempted attack to the train<br>◆ Terrorist sabotage on the track and derailment of a passenger train |
| Theft and robbery | ◆ Theft of catenaries between two stations<br>◆ Violent robbery at a station<br>◆ Fuel theft from diesel locomotive within a depot<br>◆ Fuel theft from diesel locomotive on open tracks<br>◆ Metal theft from a freight train<br>◆ Theft of goods from freight cars and containers in railway operations |
| Vandalism and Illegal access | ◆ Unauthorized access to a tunnel<br>◆ Illegal immigrants on a train passing in a tunnel<br>◆ Unauthorised access to the track area<br>◆ Object throwing into the railway area<br>◆ Aggressive person on-board a train<br>◆ Aggressive person at a station<br>◆ Intruders on-board a train<br>◆ Attempt to break into traffic management centre and disrupt rail traffic management |

## 7. Railway Security Management System

A Railway Security Management System (RSMS) is purely a conceptual tool for managing security within the railway systems covering both conventional and high speed networks.

The RSMS guidance can contribute to the effective design, planning, implementation and monitoring of the security events within the railway operations.

The RSMS may offer a comprehensive picture of all the known threats (external and internal), system protection requirements (legally mandatory and voluntary basis), as well as all the measures and actions to react and recover operations in case of an attack.

The concept tool can be designed to provide a comprehensive management framework to:

- Rail Infrastructure Managers,
- Railway Undertakings,
- Railway integrated companies,
- Railway Station Managers.


**The Railway Security Management System wheel**

# International Union of Railways

240 members
Across 5 continents...

2 500 billion passenger-kilometres

9 500 billion tonne-kilometres

More than 1 000 000 kilometres of lines

Prepared by: UIC Security Division and UIC High Speed Department
Published by: UIC-ETF
Design: Coralie Filippini
Editor: Audrey Mignot
Photo credit: Fotolia


ISBN: 978-2-7461-2454-7

INTERNATIONAL UNION
OF RAILWAYS