ECONOMIC COMMISSION FOR EUROPE Informal document SC.2 No. 1 (2009)

INLAND TRANSPORT COMMITTEE

Working Party on Rail Transport

Sixty-third session 13 November 2009
Geneva, 18-20 November 2009
Item 3 of the provisional agenda ENGLISH ONLY

TASK FORCE ON RAIL SECURITY

Report by the Chairman

I. INTRODUCTION

1. The Working Party on Rail Transport (SC.2) considered first the issue of security while implementing the February 2002 decision of the Inland Transport Committee (ITC) that requested its subsidiary bodies to identify the differences between "security" and "safety" concepts and the relevant concrete questions that could be addressed in this respect (ECE/TRANS/139, paragraph 19). Subsequently, the SC.2 Chairman sent in April 2002 a letter to all member governments, asking for their views on definitions of railway safety and security. After an in-depth discussion at its fifty-sixth session in October 2002, the Working Party decided to adopt the definition of railway safety as *"the socially required level of absence of risk of danger in the rail transport system where risk relates to personal accident, injury or material damage"* and the following definition of railway security: *"the protection of human beings, transport means and transport infrastructure against unauthorized and unexpected actions of any kind."* The Working Party further decided to await outcomes of relevant discussions in other international organizations before undertaking any new initiative pertaining to security in railway transport.

2. At its fifty-eighth session in October 2004, the SC.2 noted a document prepared by the secretariat (ECE/TRANS/SC.2/2004/2), which outlined the ways in which it could contribute to the ongoing work on railway security. At its fifty-ninth session in January 2006, the Working Party decided to address the question of safety and security at its next session in the light of the results of the ITC Round Table on Transport Security that was to take place in February 2006 and related developments. At its sixtieth session in November 2006, the SC.2 took note of the information provided by the International Union of Railways (UIC) about its security platform created in June 2006.

3. At its sixty-first session in November 2007, the Working Party invited the UIC to organize a Workshop on rail security that would take place during the SC.2 session in November 2008. Following the 2008 Workshop,[1] the Working Party asked its Chairman and Vice-Chairman to incorporate the main conclusions, in cooperation with the secretariat, into the SC.2 review of security issues that should include the proposal to establish an informal task force to

[1] The Workshop presentations are available at <http://unece.org/trans/main/sc2/sc2_wkshp_genevaNov2008.html?expandable=3>.

follow-up on the major rail security issues identified by the workshop. The review was submitted to the Director of the UNECE Transport Division in December 2008.

II. THE MANDATE AND COMPOSITION OF THE TASK FORCE

4. The mandate of the informal task force states that it will collect and exchange information about best practices in securing heavy rail systems, cost-benefit assessments, regional and international cooperation, while focusing on the issues that have not been taken up by the EU, OTIF or OSJD.[2] All UNECE member states with rail systems as well as selected international organizations and railway companies were asked to nominate representatives to the task force. In the event, eight countries (France, Germany, Netherlands, Norway, Russian Federation, Switzerland, Turkey, United Kingdom of Great Britain and Northern Ireland), two agencies of the European Commission (ERA, Joint Research Centre), five international organizations (CER, EIM, OTIF, OSCE, UIC) and two railway companies (SNCF, TCDD) nominated representatives to the task force. A representative of the UNECE TER project also participated. The Netherlands agreed to chair the task force.

5. The task force met for the first time on 14 May 2009. Generally, it was agreed that a broad definition of security, including low-level crime as well as sabotage and terrorism, is most appropriate because low-level criminal activities are encountered daily by rail operators and standard crime-protection techniques can be used to thwart sabotage and terrorism threats as well. The task force decided that it would focus in particular on the following topics: (i) international regulations, (ii) exchange of good practices and (iii) the economics of rail security. The papers dealing with these issues, drafted by France, United Kingdom, UIC and EIM, as well as contributions of Norway and Switzerland were considered at the second session of the task force on 1 October 2009. The task force recommendations are based on these papers (annexed to this report) and related discussions that took place during the second session.

III. RECOMMENDATIONS

A. An international approach to rail security

6. In principle, an international approach to security in rail transport, based on effective cooperation of governments and stakeholders, is desirable just like in other transport modes. That is why the SC.2 decided to set up an international task force, including both representatives of governments and rail industry, to consider and analyse the rail security question. Having considered a number of specific rail security issues, task force members agreed that the best way forward is to work systematically on guidelines, best practices and standard security requirements before considering the development of detailed international regulations or framework agreements.

7. The task force concluded that for the time being mandatory rules and standards for railway security at the UNECE level are neither desirable nor necessary. However, best practice guidelines for the installation and use of specific security tools (e.g. CCTV cameras) could be useful for national authorities who would be most qualified to decide on specific deployment of such tools (e.g. at selected key train stations).

8. Mandatory rules at the national level, tailored to specific security needs, continue to be appropriate. Mandatory rules at the bilateral level or trilateral levels are appropriate, if needed. For instance, the agreement between governments of Belgium, France and United Kingdom

[2] The mandate is available at <http://unece.org/trans/doc/2009/sc2/SC2-ITF-Mandate.pdf>.

regulates security controls concerning the Eurostar trains connecting their national capitals. Such trains are likely to attract the attention of terrorists. Other international high-speed trains require less stringent agreements, given the apparently lower risk levels.

9. Industry representatives on the Task Force have emphasized that ordinary crimes present everyday problems for rail operators. Therefore, practically each network has set up an organisation involving stakeholders to control and reduce crimes. Counter-terrorism approaches ought to be based on such structures that have been already created for coping with ordinary criminal activities in order to be accepted by stakeholders. The challenge is to introduce new responsibilities to these organisations. The experience shows that most of these organisations already act against terrorism and nearly always the measures implemented to protect or prevent from these threats are also efficient against crimes.

10. With respect to international transport of goods and passengers, the task force agreed that guidelines and intergovernmental cooperation are important, although national security regimes need not be uniform. An effective combination of such national risk-adequate diversity and intensive cross-border cooperation is likely to change over time in response to technical progress and emerging threats. Effective methods of managing railway security should be shared and their adoption encouraged across the UNECE region. Further cooperation along these lines could lead to the elaboration of an international framework agreement that would leave enough scope for the individual approaches adopted efficiently to national conditions.

B. Security tool box

11. The task force recommends to national authorities to develop a suitable architecture for a toolbox of guidelines and good practices. This could be accomplished by setting up a Technical Working Group (TWG) that would become a unique internationally accepted focal point for rail security. The formation of a joint TGW should be proposed by the UNECE Working Party on Rail Transport to a number of international organizations dealing with inland transport security, including the International Working Group on Land Transport Security (IWGLTS) and UIC.

12. TWG would be tasked to analyze existing security requirements and practices, produce guidelines (requirements and implementation) and design strategies for an effective sharing of good practices by national authorities and railway industry professionals. It would also develop an international research agenda for rail security. Its mandate could be initially for a two-year period, with a possibility of renewal. Some members of the task force are prepared to participate in the Technical Working Group.

13. The main rail security guidelines, once developed by the TWG and approved by participating governments and industry representatives, ought to be promoted by the UNECE and other regional commissions of the UN system. Specific requirements and implementation details as well as sensitive research findings should be available only to authorized users of the rail security toolbox. Technically the toolbox would be a protected website that would help policy makers, law enforcement authorities and designated rail transport professionals to solve security problems. UIC is prepared to host the toolbox website and ensure adequate protection. The toolbox could include standard items such as policy briefs, promising practices, research publications, workshops and tutorials, but its actual composition remains to be determined by the UIC in cooperation with users.

C. Cost benefit analysis

14. The task force agreed that the cost benefit analysis of rail safety measures can be applied to a limited extent to security problems. Whereas plausible cost estimates of security measures can be generated easily, estimates of the associated benefits are rather difficult. Due to the scarcity of relevant statistical data and evolving nature of threats, subjective assessments are necessary. This entails a number of problems that make unbiased and accurate estimation hard to achieve. Given obvious advantages of the decisions based on reliable cost-benefit techniques, an appropriate model for appraising rail security risks needs to be developed, with the assistance of national and international transport research centres.

IV. FOLLOW-UP ACTIVITIES

15. The task force will organize a session on rail security during the UNECE inland transport security conference on 28-29 January 2010. The presentations will include task force recommendations to UNECE member States as well as contributions pertaining to the use of cost-benefit analysis, exchange of good practices, international regulations and secure architecture for railway projects.

16. The task force has been informed that the COLPOFER Association, whose 42 members include security experts from European railways and railway police forces, plans to create a working group to study the use of cost-benefit techniques in the area of rail security. This working group will further develop the assessment of cost-benefit analysis performed by the task force.

17. Following the creation of the Technical Working Group (TWG) mentioned above, a number of task force members are ready to participate fully in its activities. SC.2 should be represented in the TWG to ensure an effective cooperation between the Group and UNECE.

18. Capacity building in the area of rail security in UNECE transition economies in the Caucasus, Central Asia, Eastern Europe and Southeast Europe constitutes another potential follow-up activity. In response to specific requests, members of the task force would be willing to contribute to such activity by organizing peer to peer support and sharing of good practices for transport authorities and railway companies.

19. The 18th OSCE Economic and Environmental Forum process under the Kazakh 2010 OSCE Chairmanship will focus on “Promoting good governance at border crossings, improving the security of land transportation and facilitating international transport by road and rail in the OSCE region.” The first part of the Forum will take place on 1-2 February 2010 in Vienna, to be followed by a preparatory conference in Minsk on 15-16 March, and the second and final part of the Forum on 24-26 May in Prague. The objective of the Forum process is to stimulate a multi-stakeholder dialogue, build political will and help identify concrete follow-up activities, which could be implemented together with other partner organizations. The Minsk meeting in March 2010 will tackle issues related to railway co-operation and inland transport security. Members of the SC.2 task force on rail security are encouraged to actively contribute to this meeting and to further explore some of the recommendations of this report.

V. CONCLUSION

20. The task force has fulfilled its mandate to the extent possible. A number of policy recommendations for the consideration of the UNECE member States were developed during a relatively short time period without outside consultants. The Working Party may wish to adopt these recommendations and encourage their adoption by competent authorities.

Annex I (France)

International cooperation for rail transport security requirements

Background

Agenda of the first meeting of the informal task force on rail security:

Item 4 Discussion of issues

4. All participants are expected to intervene briefly in the moderated discussion of issues that could be considered by the Task Force, including

- actual approaches to security in rail transport (e.g. risk based, rule based, etc)
- focus on passenger transport (international traffic only?) and/or freight transport (all freight shipments or containers only)?
- costs, benefits and experience with security measures at the national level
- best practices in cross-sector cooperation (businesses, government agencies)
- key issues for international cooperation
- exchange of best practices and experiences
- focus on infrastructure (stations, rolling stock, control systems) and/or procedures?
- *need for new legislation (e.g. an annex to the AGC) or new organizations (e.g. An international rail transport security agency)?*
- is market structure (competition of vertically integrated firms vs. Above-the-rails competition) relevant to security?
- *aim for generic recommendations (for all 56 UNECE countries) or recommendations by sub-region (CIS, North America, Western Europe, etc)?*

Report or the first meeting of the informal task force on rail security

During the 14th may meeting, France volunteered to lead the work pertaining to regulatory guidelines and all members of the Task Force were encouraged to send to their assessment of advantages and disadvantages of the three possible options, i.e. international regulation or government regulation or guidelines for rail transport security (including relevant publications).

Final declaration of the UIC world congress on railway security

« They request the various international bodies to consider the possibility of taking international-level decisions on rail security, via the development of minimum security standards to be observed by all involved in rail transport, consideration as to the appropriateness of an international competent authority, the strengthening of partnerships with rail transport players, or any other means they think suitable. »

[UIC contribution to explain the rationale which lead to the final declaration requesting an international railway security authority and providing a potential way ahead:]

“The railways companies, infrastructure managers or railway undertakings have developed since the last ten or twenty years their own security policy, in partnership, because it was an increasing demands from their clients and often from their staff.

As public or semi-public entities they found various partnerships with their national authorities to share the responsibilities, the roles, the necessary budgets…and in addition they organized the complementary call on private security companies.

This balance is becoming insufficient or is questioned by two main events: the opening of the passenger market at the beginning 2010 and the development of the international traffic, specifically the high speed traffic

The opening of the passenger market will have important consequences on security. Foreign and private new entrants will have to define a security policy. If not, security could become a distortion of competition between on one side companies which are used or have chosen to have a security policy and which take in charge the related costs, and on the other side companies which don't have such a policy and benefit in fact of the policy and the expenses of the others. Beyond the sharing between infrastructure managers and undertakings has also to change or at least to be re-examined.

The development of the international traffic is a necessity for the railways. An efficient security of transport cannot be only organized by the addition of bi-lateral agreements but needs the organization of coherence between the national solutions

Which answer could be given to both these questions?

A dedicated international authority would of course be able to adopt various decisions its members would have to implement. But the creation of such an authority will take a lot of time and would raise a problem of competence, the States having in charge the security of people and goods on their territory.

A more efficient solution is to ask to an existing organization to launch this job of creation and enforcement of coherence between the national policies of rail security with the responsibility for it to find a common position between the States and the railways.

UIC agrees with the idea of a leadership of UNECE on this question.
UNECE could give a mandate to IWGLTS to build the answer from the side of the States, and to UIC to do the same on behalf of the railways, with the participation of UITP for the links with the urban transport. As UIC is stakeholder member of IWGLTS, UNECE should receive a common answer."

___________________[**end of quotation**]

.

There are two issues raised in this forum :

- the creation of a competent international security authority,
- the creation of minimum security standards

It is useful to recall that the UNECE Working Party on Rail Transport (SC.2) has defined security in railways as « the protection of human beings, transport means and transport infrastructure against unauthorized and unexpected actions of any kind. »

These question is how to increase the consistency among national security approaches and requirements in order to facilitate the development of international railway lines and competition inside Europe.

Since civil aviation and maritime transport have their dedicated international bodies that issue regulations, it is natural that the idea of creating an international authority for rail transport has been raised. Even if this question is here restricted to security, it is easily understable that such a body would also need to be competent in safety matters as security and safety can be contradictory, and also in most of the technical areas in order to be able to produce global positions while considering any and all the constraints.

There are fundamental differences between maritime transport, aviation and rail transport. Rail transport takes place on on land and every centimeter or inch of track is situated on the territory of a country. Moreover rail transport systems are open system which can be easily accessed. Maritime transport often takes place in international waters where no national law is applicable, and aviation has also to take into account the intercontinental flights which transit through the international airspace. Moreover maritime and air transport are often international transport and that means that they have to be consistent with regulations of the departure and arrival countries, and also of the transit countries. Considering this complexity, a unique international regulation cannot be avoided for the sake of simplicity and economy.

Security measures have been developed for national and international flights. These measures consist mostly of controls of passengers and freight at the departure. They are implemented in national laws.

While in transit through international waters or airspace, the Captain (of the aircraft or of the ship) is the legal representative, assuming that the law applicable on board is the law of the flag. In maritime transport this is the heritage of the past when the ships in the middle of the sea had no contact with land. Although the communication technology advanced, the Captain’s legal powers are still effective.

Obviously rail transport is very different from maritime and aviation transport. International lines are limited and often involving only a small number of countries. Moreover, most of the Nations consider as a strong element of sovereignty their responsibility for the security of people and freight on their national territory, and would not agree to the creation of an international authority on rail transport security. However, interoperability requires cooperation and alignement.

For aviation it had been agreed that passengers would have to be submitted to comprehensive controls in order to protect them from terrorist actions. Such controls are only possible because they have been introduced by national legislation and they nearly always go far beyond what is acceptable in everyday life in the same countries. The controls restrict the individual rights and liberties but are applied only when people want to enter a restricted area. It has been mentioned above that during travel the Captain is the representative of the flag state and has police powers. This is not the case in rail transport. Wherever trains are, they are always under national jurisdiction and even if the controller can have some limited powers, depending on the country, he or she is not responsible for enforcing the applicable local law and national laws. This means that a train is always on the territory of a sovereign state so that the local regulations concerning security must be applied.

Exceptions to this principle are very few. For example the Brussels-London direct line using the Channel Tunnel is covered by a trinational convention which allows the custom and frontier control to be made in Brussels. One may note that the convention has also been signed by France as the train leaves the Schengen space from France. Any other train using the tunnel to UK will be under the responsibility of France and controls must be organised by France except if multipartite conventions are signed between UK, France and the departure and transit states.

The security requirements defined in order to protect the Channel tunnel system from being damaged by a terrorist attack must be taken into account by the rail operators wanting to use it. These requirements, intrinsic to the tunnel system, are identical for all operators and do not depend on the origin of the train. That means that any and all operators of trains in the tunnel must comply with the same set of requirements agreed to by the UK and France. These requirements have consequences for the trains, stations and tracks operations in the UK and France but also in every country crossed by the line. Such uniform requirements do not differ according to the origin of journey or nationality, being defined to protect the tunnel system.

The level of the security requirements is directly linked to:

- the level of criminality in transports systems (vandalism, theft...),
- the social conscioussness of the terrorist threat in the two countries;
- the international events planned;
- the prestige of the asset as a target for a terrorist attack.

Taking these factors in consideration, it is normal that the Channel tunnel should have higher levels of security than the Perpignan-Figueras tunnel or the Lyon-Turin tunnel. It is also the responsibility of the British and French governments to define threats[3] and the maximum acceptable level of risk, and to specify consistent minimum security requirements.

The same assessment can be made for tracks. Threats are local political issues. Levels of threat are assessed by national intelligence service and cannot be used elsewhere. So the level of threat is a national indicator. Likewise, the maximum acceptable risk also reflects a national political decision. This type of decision making cannot be delegated to international bodies, and even more so if these bodies are not elected. The difference with aviation is that the accepted risk in air transport is assumed to be very low and the control constraints are very high so that the security philosophy is based on a list of forbidden objects and on the organisation of controls to ensure that these objects are detected before boarding. For rail transport such a balance will not be reached and the maximum level of risk must be defined by governments while operators can decide to go further and apply even stricter measures to lower the level of risk.

This implies that the rail security question can not be dealt with in the same way as in the civil aviation and maritime transport sectors, and an international authority is not acceptable in this field. Directives and international regulations based on security measures will not be appropriate for rail transport.

Is there a role for international bodies?

[3] Threat is defined on the basis of intelligence work whereas risk is a mix of the threats identified and their consequences.

International bodies can take a central place in the coordination of national security approaches and processes. They can provide the forum where the guidelines and best practices are assessed, structured and edited in a tool box in order to produce a set of requirements corresponding to different levels of security.[4] They can also provide the rail world with assessment methods customized to rail transport reality. They can finally be a forum of exchange of experience and support for the small or new actors in order to reach the international standard level quickly. In order to do that, they can provide audit or expert teams to help these actors to progress.

This responds to UIC demands:

- the production of a tool box to simplify security requirements,
- this international effort will also customize to rail reality and standardize the assessment methods, it can also provide a structure to organize peer to peer audits or expertise,
- this will create a structure which will be able to help the smallest countries or those who are newly confronted with terrorism to learn quickly from others the basic elements of security.

A new international body is clearly not an appropriate solution to develop such documentation as this body would not have any authority. What is needed is:

- an international « entity », involving States and operators,
- focusing on rail transport security,
- able to organize a technical international working group (more or less as IMO intersession web working groups produce new texts) to produce guidelines defining different set of requirements corresponding to increasing level of security (as TAPA or classification rules for ships safety),
- providing « expert » methods of assessment for security,
- able to organize peer to peer support for « beginers » and sharing of experiences.

The tool box should be divided into two parts: requirements and best practices. The first part deals with how to write security requirements using a unified approach. The second lists the best practices applied in the networks to reduce criminality and terrorist risks.

The tool box requirements part should be based on the « lego principle ». It contains individual bricks which can be chosen and include in any and all national security requirements. The development of the tool box will be based on the existing requirements; the first task is to analyse these requirements in order to highlight and to describe the shared requirements in order to fix the architecture of the documentation. Then the individual documents will be written.

In principle the tool box will be organized as a set of Russian dolls documentations. They will be thematic with themes such as: stations, rolling stocks, tracks, passengers, freight, high speed, urban transport, and potential additional requirements for transversal assets like bridges, tunnels, use of CCTV systems or blast resistant materials. On each theme, the documentation will describe several levels of security requirement (as TAPA EMEA FSR or TSR) fitting into each other. These can also differ to take into account different organisations and responsibility schemes between stakeholders in different countries.

[4] The typical example of that is given by the TAPA FSR and TSR standards which define several level of security and the operator can choose their level of certification.

The use of this set of technical requirements will be simple. It will be used as a basis for requirements, and it can be completed with additional requirements as needed. Every nation will have to decide which level they want to be consistent with and to add their extra requirements. A first high level box should consist in security management with also several levels possible, the highest being consistent with ISO 28000.

The benefits will be shared between operators and nations. Operators will be able to be certified to this documentation, and this certification process will limit and simplify the checking of the responses to requirements. It is similar to the process already existing for ships certification where flag nations mainly control classification societies and rely on the certificates they deliver, only controlling specific points which are not covered by the classification process. In this case the nations will continue to have to control their specific requirements.

The establishment of such a tool box and its use can be separated into two phases. The first one is the technical work, the second is the publication of the tool box as guidelines. For the second part UNECE, and others UN regional organisations are adequate places. For the technical part they must rely on a technical working group.

An issue that has been identified is to avoid any duplication of work on this subject and to create a unique technical working group inviting all of the international bodies involved in rail security to participate (IWGLTS, UIC, UE, COLPOFER...) to produce these documentation. This group should work using internet and a webmail as IMO, and should have two or three yearly meetings to validate the wordings and discuss the toughter points. These meetings should be organised in coordination with other UIC and IWGLTS meetings for example.

This forum represents nations and operators. This unique technical work will focus on solutions for the European continent. Organisations, regulations and habits can vary so much from one continent to another that it seems that such an approach must be made on a geographically limited area base.

The mandate should identify two steps :

- analysis of existing security requirements and definition of the structure of the documentation,
- production of the guidelines.

Annex II (United Kingdom)

The use of cost benefit analysis and economic assessment on rail transport security

Introduction

The use of economic assessment as a policy tool to assist decision makers within the transport sector is well established. There are well thought through arguments about how to apply economic assessment to the field of transport safety and more recently environmental concerns in this sector, such as the carbon footprint from travel. This paper considers whether similar economic assessment could be applied to security policy in the rail transport sector.

In order for policy makers to make decisions it is necessary to compare different policy interventions against one another and against a ‘do nothing’ option. For the majority of new policy interventions a financial cost will be imposed and policy announcements are often accompanied by a statement that extra money is being made available to fund the measures. Therefore there is a strong argument for analysing policy options using economic assessment.

Increasingly policy interventions are accompanied by an impact assessment, which identifies both likely positive and negative impacts. Often this comparison is on the basis of financial costs. For example financial values have been determined for peoples’ lives, injuries, journey time delays and interruption to business/economy. The most common method of economic comparison used by policy makers is cost benefit analysis or value for money comparisons.

As a general rule a policy intervention should show a positive cost benefit. However, there might be political or public pressure to introduce measures that outweigh financial considerations. Also it has to be recognised that not everything can be measured in pure economic terms. The level of certainty around some of the costs associated with particular factors might be questionable and need to have a sensitivity test to show how robust they are. Also sensitivity tests could be applied to other assumptions being made to improve their robustness.

Nevertheless, in the current climate when harsh financial decisions need to be taken by administrations and governments, having some form of mechanism to compare different policy areas is necessary. It therefore makes sense to start with the premise that economic assessment should be applicable to policy interventions including that of rail transport security.

This paper initially concentrates on economic assessment of a rail transport safety policy. It shows how a similar approach could be taken to rail security and also highlights its limitations. This paper also recognises that examining policy interventions that are directly linked to protecting passengers and rail assets are not the only security measures in place. Counterterrorism measures generally are likely to have a positive impact in improving rail transport security.

These measures range from de-radicalisation of people, gathering intelligence on suspects, to police led operations to intercept terrorist attacks. It is also possible to reduce the impact of an attack by being adequately prepared to deal with the aftermath. In an open mass transit environment like rail, where it is arguably impossible to be one hundred percent confident of preventing an attack, this is an important consideration.

Economic assessment of transport safety measures

For safety measures across all transport modes there are reasonably well established economic methodologies such as cost benefit analysis and value for money methods to evaluate policies. An example would be to evaluate measures to reduce fatalities and serious injuries to passengers involved in a train collision or derailment.

In this example there are potentially two areas of policy intervention, introducing safety measures to prevent the accidents occurring in the first instance or improving the crash performance of the train structure. Each one would have a financial cost associated with its implementation. This would involve capital investment and ongoing maintenance costs. A view on the effectiveness of each measure would also need to be determined by experts based upon past accident data. The financial benefit could be derived from preventing or reducing severity of the passenger injuries, damage to trains, delays to service, etc.

By understanding both sides of the cost and benefit equation, it is possible to conduct an economic comparison. However, to have a robust analysis there needs to be sufficient information on what happens in an accident and their frequency. This will provide the evidence upon which to assess the benefits that could be realised and enable a cost benefit analysis (CBA) or value for money (VfM) assessment of the proposed measures.

The assumption would normally be that the frequency of accidents would continue, unless the policy intervention is undertaken. This would not be an unreasonable expectation but care should be taken to discount any other external factors that could influence future accidents - past events are not always accurate indications of future events.

In conclusion a CBA or VfM analysis would be made up of the financial cost of introducing the measures compared with the benefit from preventing or reducing the effects of future accidents. This would be calculated on the basis of financial savings in reduced injuries, infrastructure damage, delays, etc.

Background information needed to conduct economic assessment of security measures

The key aspect in the above safety scenario is the availability of data from past accidents which supports robust evaluation of the expected benefits and thus confidence in the analysis. Unlike terrorism statistical trends relating to safety would normally change gradually over time rather than dramatically and this provides the necessary quantity of data. (The exception perhaps is a major safety incident that brings a disproportionate amount of publicity and pressure for government to act.)

Terrorism is dynamic and so unlike safety policy interventions, solutions have to take account or at least recognise that a terrorist could change their method of attack to circumvent any measures in order to still hit their target. Also there is a likelihood that the underlying probability of attack will change independently of an intervention. Terrorism is also dynamic in the sense that a previously inactive terrorist group or cell could commence attacks with little or no warning. They could be quite minor in nature or result in many hundreds of fatalities. An example of this is 11 September 2001 terrorist attacks on the World Trade Centre and Pentagon in the USA.

In Europe there have already been two notable terrorist attacks on the rail network. Madrid on 11 March 2004 where there were 191 fatalities and 1800 injured, and in London on 7 July 2005 where there were 56 fatalities and 700 injured. Whilst the method of attack was different in each case, in both instances it showed the desire by International terrorists to cause mass casualties and adverse economic impact by disrupting rail transport services.

Whilst there have been other attempted attacks on the transport sector in Europe by International terrorists or sympathisers they have been relatively infrequent. Where there is some similarity between terrorism incidents and major accidents is the public response for action, especially if there is significant loss of life on public passenger transport. This is likely to be down to the level of risk society will tolerate.

Nevertheless a similar economic approach of identifying financial costs could be applied to evaluating counter terrorist policies. Counter terrorism and safety measures can be viewed as having positive and negative aspects. A clear benefit would be in preventing an attack happening, thus saving loss of life, damage to property etc. A negative aspect would be time delays to a journey. But unlike a safety measure there is not usually a proven history of similar events upon which to evaluate the proposed measures and the threat landscape is changing. This means that proving that the proposed measures have prevented an attack is very difficult.

Terrorism threat - national/global level

An act of terrorism may be from national or international groups. The target of an attack, and the methodology used, is dependent upon the groups involved, their capability and aims. Currently the threat from International terrorism is predominantly from Islamic extremists. The threat is global, but the risk of attack is greater for some countries than others. The reasons for this vary, but could include cultural factors, historical events and/or current foreign policy.

At a country level the threat from International terrorism could vary between transport and non-transport sectors. Within the transport sector itself the threat might vary across the different transport modes. Rail stations are usually located across the whole of a country and differ in size and the type of services they provide. Rail lines might be for passenger, freight or both, whilst rail operation could be high speed, commuter or local service or a combination of each.

The actual method of terrorist attack can take many forms. The most common grouping of attack methodology is chemical, biological, radiological, nuclear and explosive (including improvised), (CBRNE). Within each of these the actual method of deployment or chemical agent used could be different. Consequently the security measures needed have to be relevant to the current threat or dynamic to a potentially changing situation.

An added dimension for some countries is that there is also a threat from national terrorism or extremism. This would be country specific but could be limited to a particular geographical region or locality. The type of threat and the target are not necessarily the same as the international threat; therefore the measures could be different. These would need to be factored into any economic assessment.

Financial cost of implementing security measures

The financial costs associated with the introduction of a policy could be defined as either capital or operational. For example capital cost for the private sector could include items such as screening equipment, hostile vehicle restraints and other security measures incorporated into the building. Business rules on how capital costs are depreciated would need to be observed. When estimating the financial cost of new security measures there is tendency to underestimate, therefore factoring in an optimism bias is normal. The figure of bias will depend upon the nature of the measure. The more innovative the measure the higher the bias would tend to be. Operating expenditure would be the ongoing maintenance of equipment and staff cost to operate the equipment. It would also include staff carrying out security checks as part of their duties, security staff deployed on the railways and their training. A key issue to consider is over what period of time these costs should be considered.

Any financial costs should also be identified for the public sector. If the capital expenditure is being met from the public purse then it should include the cost of capital – the benefit that would be gained if the money had been invested. There could also be a public sector cost from officials administrating the private sector carrying out security. This could include regular site inspections and where necessary taking forward enforcement activities for non compliance of the rules.

Depending on the security measures being implemented there might also be a need to include the financial costs imposed upon passengers and other businesses connected with the rail network. These could include delays to passengers' journeys caused by the measures and from revised business operating practices, such as restrictions on delivery times for goods. For major changes to a station building, e.g. installing hostile vehicle mitigation, there might be significant disruption to passengers and business during the actual construction phase. When costs are being accrued over several years, net present values (the value of money as of today) should be used to make suitable comparisons between options.

Financial benefits of security measures

Regarding these benefits, this will be derived from preventing an attack. These benefits should be considered at both the micro and macro level. By establishing different terrorist attack scenarios it is possible to determine the likely impact they would have if they were successful. At the micro level impacts would include number of casualties and their severity, infrastructure damage, clean up costs (if a chemical attack) and delay to passengers and train operations. An economic value can be attributed to each of these.

At the macro level, influencing travel behaviour (moving to private car from public transport), adverse impact on international tourism and financial market confidence should be considered. It should be possible to make an economic estimate of these factors. For example a 10% reduction in international tourism in the UK would equate to roughly 110 million Euros in a year.

In order to consider a range of scenarios it is necessary to have undertaken operational analysis on how detonating different sizes of explosive device would affect likely number of passenger casualties and the extent of damage to infrastructure. Quite clearly a person borne explosive device and a vehicle borne explosive device have different capabilities, both in terms of their impact on people and buildings. Nevertheless, the potential for mass casualties, disruption to passenger travel and the financial cost is potentially huge. Being able to detonate a vehicle inside a crowded station concourse as opposed to outside it could also have a significant difference.

Railway stations are inherently different, many are very old and they are normally located within densely populated urban environments, which place additional constraints on what security measures can be deployed. Also the precise location where an explosive device is detonated within a rail carriage or train station could make a significant difference. Nevertheless, with all these variables it is still possible, using operational analysis, to determine some representative scenarios using certain basic assumptions.

Railway stations and trains by their nature tend to attract large numbers of people both during the day and during the evening. Therefore, potential loss of revenue to shops, pubs and similar establishments would occur if there was an attack on a train station indicating that there is a potential saving here too.

Having effective regular security patrols, passenger screening and Close Circuit Television (CCTV) as counter terrorism measures also provide a benefit in reducing general crime on the transport network. There are also arguably other benefits that are not easily quantifiable. These include greater public reassurance from, for example, seeing security patrols and other overt security measures in place.

Comparing the financial costs and benefits of security

Having identified the financial costs of a security measure and the financial benefits that could be derived if an attack was prevented, it is necessary to compare them. The challenge is having a robust method of comparison. To understand whether the benefits would be materialised means assessing how likely an attack is to happen.

In the safety scenario outlined above the need to have good data showing a history of events was emphasised when undertaking economic analysis. Unfortunately unless the attack scenario is in a theatre of war - where the frequency of incidents is likely to be high - data from incidents are likely to be very low in number. Also policy decisions are actually needed before the attacks begin or very shortly afterwards if there has been no advance warning. The absence of historical data from past events presents a major problem. With a very small data capture there will be inherent uncertainty when evaluating any specific policy intervention.

Intelligence about terrorism groups should be more plentiful and assist in identifying which member states are likely to be targeted, how many terrorist groups there are and likely targets. However, this information by its very nature is sensitive and usually cannot be published, so it would be difficult to use in any financial evaluation that needed to be publically transparent. In the UK however the International terrorist threat to the country is published so this provides some degree of context for any assumptions. There are five threat levels ranging from ‘low’ to ‘critical’ with the highest meaning “an attack is imminent”. There would be a degree of subjectivity but using this information could assist to construct an argument for security measures, but as demonstrated in past attacks, absence of intelligence in a particular area does not necessarily mean that there is no threat.

Terrorist attacks are by their nature high impact low probability events. This means that it is not possible to predict with statistical confidence the likelihood of an attack taking place. The exception is when there is historical data on previous attacks. An analysis tends therefore to lend itself to a more subjective evaluation. An analysis of other forms of event, such as floods/national disasters suffer the same problem. Whilst this is true perhaps the key difference is that unlike the 100 year wave, terrorists are easily able to adapt their attack methodology so that the security measures in place may not be effective due to the variable nature of attacks.

The risk of an attack is made up of the threat, vulnerability and impact. When discussing risk, a judgement needs to be made on what is an acceptable level – ranging from risk management to risk avoidance. As low as reasonably practicable (ALARP) is a phrase commonly used in the safety environment to describe an acceptable risk level.

As some security measures could take a long time to implement consideration needs to be given to how long the current terrorist threat is likely to be issue. It has been stated that the current international terrorist threat is likely to be here for a generation. Also transport is a known target. On that basis it could be argued that there could be one or two attacks on the rail sector over a 30 year period. On the other hand if the security measures take a long time to install threat tactics could change over the time required to fit them.

There have previously been two successful attacks on the rail sector, so the question that should be asked is - could this be repeated? The intelligence services are perhaps best placed to answer this question. With the above information it should be possible to identify potential scenarios and make some broad assumptions on the frequency of attack. This information would at least provide an indicative cost benefit analysis using a given scenario.

The cost benefit analysis would be influenced by when an attack was presumed to have been prevented, so a sensitivity analysis with different years would need to be undertaken. The outcome would be a range of cost benefit ratios. If agreement could be reached on one it could then be compared with other competing measures either within the field of security or with other areas such as safety.

Alternatively if the uncertainty around predicting the frequency of an incident is too great, but the threat remains real and credible, having an agreed methodology for costing security measures and an understanding of the potential savings of an attack if it were to happen could allow a judgment to be made. For example if security measures are estimated to cost 10million Euros and a scenario benefit is estimated to be 200million Euros, a view could be taken on whether to make an investment decision. It might be that there is more than one security measure that is being proposed and so a comparison could be made between them.

Application and effectiveness of security measures

In examining a security measure, factors such as how effective it is likely to be in preventing a successful attack need to be considered. The assumption that has been taken so far in this paper is that the security measures would be successful in preventing an attack. A view needs to be taken on whether this is appropriate for any new security measure. For example this might be a reasonable assumption if all passengers are screened for explosives before entering the rail network, as in an airport style arrangement. However, if only a small percentage of railway passengers are screened this might not be a reasonable assumption. This needs to be factored into any economic assessment.

On the other hand consideration should be given to whether the measures need to be applied equally across the whole of the rail sector. Does the terrorist threat mean that only certain areas of the rail sector would be targeted and would this vary from one member state to another? This is especially relevant in the open mass transit environment where for example a hundred percent passenger or luggage screening might not be necessary even it were to be technically feasible and cause minimal delay to passengers.

The ability to get onto a railway line or train at any point and end up at a specific location which could be seen as an attractive target does present a major problem. Other aspects that are less clear are how much a relatively small degree of protection could deter a terrorist attack. This would very much depend upon what type of attack and aim of the terrorist organisation.

Whilst some of these points apply equally to other transport sectors the open nature of rail network, unlike say the aviation sector which is largely a closed system, is integrated into the built environment and therefore presents unique problems for designing in effective security.

Alternative methods of attack and displacement to another target

If the security measures are effective, this could force terrorist to concentrate upon either another method of attack, area or sector. An example would be terrorists changing from an improvised explosive device to using a chemical device, which the measure would not have necessarily been designed to detect. There are, after all, very few security measures that are effective against all types of attack. On the other hand not all terrorist groups have the capability easily to adapt to another method of attack, which could be at the harder end of the spectrum.

Similarly if the measures are successful, displacement to another sector could take place, especially as the current international threat is to crowded places and economic targets. Also it has to be recognised, that if the attack method or sector changes it could potentially be more disruptive and damaging. Arguably these factors should be factored into an impact assessment and cost benefit analysis, but there needs to a reasonable approach taken to the analysis.

Another aspect to consider is how effective a security measure is as a deterrent to the terrorist. Some overt measures such as screening people getting onto a train or vehicle restraint measures around a station could prevent a suicide bomber from undertaking an attack. Similarly the belief that there are covert security measures that would detect an attack might be a deterrent. However, this is a very difficult area to subjectively assess let alone quantify for any particular terrorist group.

Wider aspects of counter terrorism security

Security of the rail sector cannot be considered completely in isolation. There are other areas of government that actively engage in reducing the risk of terrorist attack. At one end of the spectrum there are measures to de-radicalise people. Preventing people from becoming terrorists reduces the dependence on security measures. Gathering intelligence on terrorist suspects is a key area that could prevent attacks from taking place. It also has a role, as outlined above, in providing information on which security measures should be in place in the rail sector.

Intelligence led operations to intercept terrorist activities are another key area that can add value. It is also possible to reduce the impact of an attack by being adequately prepared to deal with the consequences of a successful attack. In an open mass transit environment like rail, where it is arguably impossible to be one hundred percent confident of preventing an attack, consequence management is important. Overall therefore there is a suite of activities that together make rail transit safer.

Conclusion

The purpose of an economic appraisal should be to assist policy and political decision makers to make informed decisions. Assessments should therefore present the key financial findings, but also highlight risks and uncertainties, rather than making judgements for the decision maker. Unlike other areas of transport appraisal where economic models are regularly used there is not currently a recognised methodology for decision makers when it comes to counter terrorism security.

It is possible to introduce certain aspects of economic assessment similar to those used in transport safety to assist the decision maker. These would be along the lines of a cost benefit analysis and value for money analysis. To do this would mean understanding the costs of any proposed security measures and the potential financial benefits if incidents are prevented by those measures. The economic benefits would depend on being able to prevent successful terrorist attacks on the rail network.

The potential savings would include people’s lives, damage to infrastructure and service disruption at the micro level. There are already financial values for these; in the UK the estimated value within the transport department for a single life is roughly 1.3 million Euros, while damage to infrastructure and delay costs could also run into millions of Euros. At the macro level cost of lost international tourism and business confidence should be considered. The financial cost of these could easily run into hundreds of millions of Euros. Counter terrorism measures would also provide a benefit to general railway security and improving public confidence.

The attack scenarios that could be expected are many and varied. Therefore an operational analysis would be needed to determine what the likely impact is from the different forms of attack. This would provide some certainty on what damage would be caused to people and buildings should an attack be successful. However, as there are many different scenarios and methods of attack there would still be some uncertainty with any chosen scenario.

The predictability of terrorist incidents is where the real difficulty resides, and the lack of data is the crucial factor. Unlike policy interventions relating to safety, where there is normally a history of events this is not the case for terrorist attacks. This prevents a very robust cost benefit analysis or value for money assessment from being undertaken using a single existing evaluation method.

Therefore some form of subjective analysis to determine the predictability of a terrorist attack and understand the risk is an option. By understanding the threat using information from the intelligence services, an examination of the vulnerability of the network to an attack and the likely impact of an attack a view could be taken on the risk and the likelihood of an attack.

The alternative to this is to concentrate on aspects where there is a degree of certainty. The actual financial costs of installing the security measures can be determined with a good degree of accuracy. With suitable analysis the financial cost can be ascertained of different terrorist scenarios.

Economic appraisal can be applied to security measures but there are significant limitations. The lack of data on the frequency of incidents means that a cost benefit analysis or value for money assessment cannot be completed without a degree of uncertainty. However, understanding the financial cost of a proposed measure will assist policy makers to make comparisons and decisions.

Annex III (UIC and EIM)

Railway Security: Exchanges of best practices in the framework of the UNECE

Point of view of railway companies

1. Introduction

Over roughly the last twenty years, security issues of all kinds have grown in importance to such an extent that railway companies have had to take account of this new factor. Terrorism in particular has evolved from national terrorism to international terrorism that is quite different. To face these threats, rail companies have had to organise themselves and implement real security strategies in partnership with national authorities.

In this context the UIC security platform was structured in 2006 in order to share experiences but also to define common priorities and positions for the rail sector. In line with the needs expressed by members, six working groups were created.

With the opening of rail freight transport services in the EU since 2006 and the opening of rail passenger transport from beginning 2010, transport companies are evolving more and more in an international framework. Their objective is to develop their activities in Europe and beyond.

To address the demand for security of the rail transport system, legal and organisational devices are implemented at the national level with systems specific to each state.

On one hand European directives were created for safety, on the other hand the only legal instrument for security that exists at the European level for transport services is the one defined in the RID for the transport of dangerous goods.

It’s the same for the agreements (AGC - European Agreement on Main International Railway Lines or ATGC - European Agreement on Important International Combined Transport Lines and Related Installations) managed by the UNECE where no provision is made for security. AGC refers to security only in its Article 7 that states that Contracting Parties can limit temporarily the application of the Agreement, if they consider this necessary for external or internal security. A similar provision appears in Article 11 of AGTC.

During the world security congress organized by UIC in March 2009, the final declaration approved by all participants (70 railway representatives from 23 countries) requested the various international bodies to consider the possibility of taking international-level decisions on rail security, via the development of minimum security standards to be observed by all involved in rail transport, consideration as to the appropriateness of an international competent authority, the strengthening of partnerships with rail transport players, or any other means they think suitable.

It’s important to find the best solutions to reduce security risks and to study how to strengthen the legal framework and the necessary cooperation links at international level based on best practices. This conclusion was made during the first session of the informal taskforce on rail security. This paper provides an overview of organizations already working on best practices and proposes a guideline on sharing best practices.

2. Some existing exchanges of best practices

__**Global level**__

- **UIC**
    - **Security platform**
        - **Members**
          Membership of the Security Platform is open to all UIC active, associate and affiliate members (**200 members** from all 5 continents**:** companies involved in a railway transport chain or organisations whose activity is linked to railway operations)
        - **Annual Congress**, held alternatively in Europe and outside Europe.
        - **A steering committee** meeting (quarterly).
        - **6 Global working groups**

          __Permanent working groups__
          - Human factors
          - New technologies
          - Strategy, procedures and regulations

          __Theme-based working groups__
          - Border crossings, building on the work of the SchengenRail group
          - Security of international freight corridors
          - Terrorism, including institutional relations
    - **UIC security division :** Permanent structure at UIC to develop cooperation in security matters
        - **Tasks**
          - institutional representation of UIC on bodies active in the security area
          - development of research activities
          - support of the security Platform
          - Organisation of a seminar or working groups at the request of members
          - Formulation of technical positions on behalf of the rail sector in response to European or other initiatives
          - Dissemination of information
        - **Link** : **__http://www.uic.org/security__**

- **UITP (International Association of Public Transport)**

  - **Members**
    3100 public transport operators from 90 countries

  - **Security commission :**
    The Security Commission (SecCom) gathers members from around the world and is the UITP members' forum for professional discussions on all issues concerning Public Transport Security (PTS), including technological, operational and management aspects. The SecCom seeks to study, assess and promote innovative operation and technology for enhanced PTS.
    - 2 plenary meetings/year
    - 5 working groups:
      - ° Public Transport Security in stations
      - ° Technology
      - ° Risk assessment
      - ° Security questionnaire
      - ° CCTV Working Group

  - **Joint UITP-CUTA International Security Conference:**
    Public Transit Systems and Security: Achieving the right balance
    (*11-12 November 2009, Montreal, Canada)*

  - **Link** : **http://www.uitp.org/Public-Transport/security/**

- **IWGLTS (International Working Group on Land Transport Security)**

  - **Member States** : Australia, Canada, China, European Commission, France, Germany, India, Indonesia, Israel, Italy, Japan, Malaysia, Netherlands, Philippines, Republic of Korea, Russia, Singapore, Spain, UK, USA

    Observers: Associations: APEC, UIC

  - **Priorities:**

    Technology – Use of technology and technological advances in land transport security including, but not limited to CCTV, behavior detection, and travel document checking equipment.

    Public Awareness – Efforts to increase public awareness related to passengers recognizing and reporting suspicious behavior and items to appropriate transit and security officials; remaining alert and vigilant: knowing what to do and how to act during a land transport incident.

Risk Assessment – Systematic methodology for assessing the risk (threat, vulnerability and consequence) surrounding a land transport system in order to employ risk-based security and mitigation measures.

Stakeholder Partnerships – Guidelines regarding stakeholder roles and responsibilities; Improved communication and information sharing between governments and land transport security stakeholders; Guidelines for training and personnel background checks

Mitigation Actions – Preventative or response measures employed to minimize impact from a land transport incident including but not limited to the following: Design of rail stations and rolling stock to better withstand an attack; behaviour detection; canine programs; evaluation of stations for mitigation needs; and conducting exercises.

- **Link: https://webboards.tsa.dhs.gov/wb/default.asp?BoardID=71&action=0**

- **International Transport Forum (ITF)**

Inter-governmental organisation within the OECD family - Global platform and meeting place at the highest level for transport, logistics and mobility

- **Link** : **: http://www.internationaltransportforum.org/**

- **2009**
  • Seminar on overcoming border crossing obstacles
  • Forum « Transport for a global economy - challenges & opportunities in the downturn »

- **2010**
  • Forum on « Transport and Innovation »

- Intergovernmental Organisation for International Carriage by Rail (OTIF)

- 43 member states
- The **objective** is principally to develop **uniform systems of law** which apply to the carriage of passengers and freight in international rail transport (CIM, RID,AMTF ….)
- OTIF organises training events for managers and experts from member States

- **Link : http://www.otif.org/index.php?L=2**

<u>Pan-European level</u>

- **Organisation for Security and Co-operation in Europe (OSCE)**

  - 56 participating States
  - Economic and environment forum
  - ATU (Action against Terrorism Unit)

  - **Link: <u>http://www.osce.org/</u>**

- **United Nations Economic Commission for Europe (UNECE)**
  - 56 member States
  - Working Party on Rail Transport (SC.2)
  - Informal Task Force on Rail Security
  - **Link : <u>http://www.unece.org/trans/main/sc2/sc2.html</u>**

<u>European Union</u>

- **COLPOFER group**
  - 42 members : European railway security experts and railway police
  - European expert group of UIC security platform
  - 2 conferences per year
  - 8 working groups
    ° Fraud - ticket forgery
    ° Cooperation during major events
    ° Security in international freight traffic
    ° Protection against acts of terrorism and extremism
    ° "Brenner" group
    ° "Security in the South-East European area" group
    ° Pan-European Corridor X
    ° Metal theft

  - **Link : <u>http://www.uic.org/colpofer</u>**

- **EIM**
  - 10 members (independent infrastructure managers in Belgium, Denmark, Finland, France, Netherlands, Portugal, Spain, Sweden, UK and Norway).

  - **EIM Work Group Security & CIP**

  - **Link : <u>http://www.eimrail.org/</u>**

- **CER**
  - 72 members (railway undertakings and infrastructure managers)

  - **Link : <u>http://www.cer.be/index.php</u>**

- **European Commission**

  - DGTREN : security division of land transport and dangerous goods
    • EC Urban Transport Security Group: The European Commission established this in April 2008 to be an information sharing group at the European level. The EC established a 2-tier approach with a "National Focal Points" Group steering and providing guidance to 2 technical working groups: Working Group I: organisational measures and incident management; Working Group II: surveillance and detection. The focal points are nominated by interested member states, the working groups include national experts, either Government or industry based. There have been two meetings to date of the national focal point group. In the interim there have been 2 meetings of WGI and one of WGII.

  - DG JLS
    • EP CIP : European Programme for Critical Infrastructure Protection
  - FRONTEX – Schengen Acquis

  - Research projects
    • Trips
    • Counteract
    • Protectrail : 30 partners from industries, universities, research institutes and railway companies

    JRC
    • Railprotect project

° **CEN**: Feasibility study on the opportunity of a standard for the security of the freight logistic chain.

North America

- **TSA** : Transportation Security Administration
  http://www.tsa.gov/what_we_do/layers/rail/index.shtm

- **FTA** : Federal Transit Administration (FTA)

- **Transport Canada :** Transit-Secure Contribution Program - Guidelines and Best Practices : http://www.tc.gc.ca/railsecurity/tscp/guidelines.htm

3. Rail sector expectations of the UNECE

These expectations are described in the mandate of the Informal Task Force on Rail Security that is available at http://www.unece.org/trans/main/sc2/sc2_itf_mandate.html

4. Railway sector needs

The list above illustrates the considerable magnitude of the exchanges of good practices in the area of rail security, both at national and international level. Therefore, care should be taken to avoid duplication of work. Nevertheless, there are very few international rules or recommendations in place which serve to improve railway transport security.

A general security framework would make it possible to adopt an integrated approach to security in terms of international railway transport for both freight and passenger traffic. The aim of this framework would be to establish a common level of security for different countries and railway operators, both inside and outside Europe. In order to meet these needs, exchanges of existing practices could be organised on two different topics:

- Responsibility sharing between States, railway companies and infrastructure managers, taking into account changes in administrative requirements and procedures.

- Special needs of high speed rail, given its development on an international scale.

- Dedicated guideline for best practices to share between various participants in the railway system.

• **First topic: Dividing the burden of responsibility between States, railway companies and Infrastructure managers.**

- ▪ Given the large number of new entrants and fragmentation of railway companies, the number of railway operators is growing fast. The types of question which could arise in relation to security are as follows:

  o What is the responsibility of each player?
  - ▪ *For example: if a station belongs to one Infrastructure Manager and a security incident occurs as a train arrives in that station, who takes responsibility for the problem?*

  o How are current security services going to evolve?
  - ▪ *For example: currently, SUGE is accountable to SNCF, but with the liberalisation of the EU passenger market from 2010, how will its status be affected?*

  o Should there be an initiative to create a ‘security certificate’ as a guarantee of a minimum level of security (in the same vein as safety certificates)?

- ▪ Security transcends national borders

  o EU directives aim to create an integrated European railway area which will contribute to the opening of the market: freight services are open to competition on all networks and passenger traffic will follow suit in 2010. These directives aim to stimulate international traffic within the EU and beyond. Security therefore is for the majority of operators an issue which transcends national borders.

o The responsibility of the State also remains to be defined, for example in the case of a security operation involving a foreign train on the national territory.

o What is the role and needed coordination between Infrastructure Managers across borders.

- Distribution of costs: Implementation of security measures requires major investment into infrastructure, technical equipment and human resources. Who should bear the burden of these security related costs? The taxpayer or the customer?

• **Second topic: Special needs of high speed rail systems**

The needs related to high speed systems are special in several ways:

- In terms of the threats weighing upon it:

  High speed, as a showcase activity for most railway companies is often singled out as a target for common vandalism and other ill-intentioned acts but also for international terrorism.
- In terms of its needs:

  - Customer expectations (time, cost...)
  - Competition with other modes of transport
  - Certain infrastructures require special protection (e.g. the Channel Tunnel)
- And opportunities: a system undergoing rapid development allows for forward planning. Security constraints can be integrated into the design and operation of stations (new or restored), and even into rolling stock in line with changing customer needs and profiles. The JBV contribution, entitled Secure Architecture - Securing Railway by Pro Active Design, is attached (Annex IV).

• **Third topic: Dedicated guideline for best practices to share between various participants in the railway system**

The question is how to ensure a ‘secure’ exchange of information between the several participants. Even though there are differences in responsibilities, approaches, solutions and so on, there is a lot of information available that can be of value to others.

Creating a secure environment (https with access codes) for those entities that will share information will be very helpful. Questions to be answered: what is needed to be shared, which entities, how to secure and so on.

These topics should be prepared and discussed with all stakeholders. This work can be undertaken in a number of ways, depending on the level of in-depth discussion desired:

- Open conferences
- Specialised seminars
- Working groups
- Online shared working area which enables the sharing of contacts, documents and other useful links.

Annex IV (Norway)

SECURE ARCHITECTURE - SECURING RAILWAY BY PRO ACTIVE DESIGN GUIDELINES FOR PROJECT MANAGERS

I. SECURE ARCHITECTURE

A. Introduction

Securing Railway by Pro Active Design and introducing Secure Architecture in the railway business, means planning of physical measures for surveillance of critical infrastructure and traffic management systems, protection of public areas, cargo terminals, objects, buildings and personnel against terrorism and other evil minded actions.

Security measures should be taken into consideration in all types of building projects, including general infrastructure, station areas, platforms, public areas, terminals with adjacent roads and gates, technical installations for electricity, signalling and communication.

B. The concept of Secure Architecture

The reduction of crime and the fear of crime are key objectives of Secure Architecture.
The architecture is the starting point for the solution of protection.

One of the key objectives for the planning of construction of a new development or the refurbishment of buildings and estates, is to secure high quality sustainable places where people will choose to work or travel, and where they can be safe. To achieve this, a much greater emphasis needs to be placed on the quality of design and planning. Designing for community safety is a central part of this, and the core principles apply not only to residential but also to other forms of development.

Secure Architecture is an initiative to encourage the building industry to adopt crime prevention measures in the design of developments, in order to assist to the reduction of opportunity for crime and the fear of crime, thus creating a safer and more secure environment. Secure Architecture *aims* to achieve a good overall standard of security for buildings, technical installations and public spaces around them.

Crime and anti-social behaviour are more likely to occur if the following seven attributes of sustainable communities are not incorporated:

1. Access and movement

Places with well defined and well used routes with area and entrances that provide for convenient movement without compromising security

2. Structure

Places that are structured so that different uses do not cause conflict

3. Surveillance

Places where all publicly accessible areas are overlooked

4. Ownership

Places that promote a sense of ownership, respect, territorial responsibility and community

5. Physical protection

Places that include necessary, well-designed security features

6. Activity

Places where the level of human activity is appropriate to the location and creates a reduced risk of crime and a sense of safety at all times

7. Management and maintenance

Places that are designed with management and maintenance in mind, to discourage crime in the present and the future.

II. EARLY STAGE PLANNING - INTEGRATED APPROACH

A. Well-designed environment - community cohesion

In an environment which is well designed, attractive, clearly defined and well maintained people are likely to take pride in their surroundings, will tend to feel comfortable and safe and have a sense of shared ownership and responsibility.

A well designed environment is one that fulfils all its intended functions in an effective and harmoniously co-ordinated manner.

An attractive environment in this context means one which has evolved or has been successfully designed to meet the needs of its legitimate users, such as the need for safe convenient means of access, the need to enable social interaction, to cater for recreational needs, etc. Legitimate users (ie the responsible majority of the population) will naturally find the environment attractive because it is responsive to their needs. The greater the attraction for legitimate users, the less will be the attraction for the criminal minority.

A clearly defined environment means one in which there is no ambiguity as to which areas are private, which are public, and how the two relate to one another. There may be transitional zones of semi-public or semi-private space [often referred to as buffer zones], or there may be strong physical demarcation between public and private areas by means of a wall, fence or hedge. The critical point is that the environment should be easily understood by those experiencing it.

B. Anonymity

Crime is always easier to commit where offenders cannot be recognised, so in consequence they will take opportunities to offend where they are likely to benefit from this anonymity. The built environment, including areas of open space, can be organised so that it either creates the potential for, or alternatively reduces the level of anonymity. In busy public areas strangers will naturally tend to be ignored, and offenders can take advantage of this anonymity, and therefore take the opportunity to commit offences. This can lead to problems where public space directly abuts private space because it can allow potential offenders to come into close proximity with private property without being noticed. This problem can be addressed by changing the nature of the part of the public space nearest to the private land or property, by reorganising it so that residents/property owners are able to exercise a degree of control over it, in effect creating a buffer between the wider public space and the private space. This buffer might or might not still be legally public space, but if it is reorganised or redesigned in such a way as to create a zone of more defensible space, anonymity will be reduced and potential offenders will correspondingly be discouraged.

Incorporating sensible security measures during the construction of a new development or the refurbishment of buildings and estates, has been shown to reduce levels of crime, fear of crime and disorder. By bringing the crime prevention experience of the police more fully into the planning and design process, a balance can be achieved, and the government's desire to create better places to live and travel can be fulfilled. The relationships between the design of the built environment and criminal and antisocial behaviour are complex. The two main influences on criminal and antisocial behaviour in this context, are firstly the nature of the physical environment, and secondly the nature of the social environment, i.e. how local communities interact with each other and with their environment.

C. Planning of security measures

Planning of security measures should be taken into consideration in 4 steps:

1. Periphery security

Fences, gates, access control, parking areas

2. Shelter security

Architecture of the construction (barriers), type of materials (glass, concrete, steel, fireproof materials etc)

3. Room security

Placing the rooms in the building and securing them from burglary and illegal access.

4. Object security

Physical security of critical infrastructure or systems

Probably the single most important aspect of new development is ensuring that all significant components of its design, planning and layout are considered at an early stage, so that potential conflicts between security and other major objectives can be resolved. Good design and early co-ordination can avoid the conflicts that may be expensive or impossible to resolve once the construction is complete.

D. All Hazard Risk Approach

For the Railway the "All Hazard Risk Approach" is an adopted principle (EU). This means that all hazards which can lead to accidents should be identified. The Hazard identification should take into consideration the following 10 scenarios:

1. Collision train - train
2. Collision train - object

3. Fire
4. Passengers injured on platform / public areas
5. Passengers injured at level crossings
6. Passengers injured on –and besides track.
7. Derailment
8. Crime
9. Sabotage
10. Terrorism

E. Risk analysis

Risk analysis should be carried out as a basic platform for necessary actions to be taken in the design process. It must be decided whether the risk analysis should be a restricted document or not.

Early informal pre-application discussions between developers, the local planning authority and the police, can be a very effective means of ironing out potential problems. Different people will need to be involved at different stages, but the sooner those responsible for design and site layout on behalf of developer and local planning authority (e.g. planners, architects, landscape architects, urban designers, engineers) enter into dialogue with the police and the Railway Safety Authority, the sooner potential problems can be identified and addressed. At the detailed design stage, there will be a need for this dialogue to be extended to a range of other specialists such as railway consultants, architects, building consultants, lighting engineers, etc.

- Investment in a well integrated and co-ordinated approach to design and project planning will pay dividends through resolution of potentially conflicting interests.
- The best available advice should be utilised, from the earliest stages of a project.

III. MAIN PLAN

A. General

During the work with the Main Plan on a superior level, security analysis should be performed in an early stage if considered to be needed. The analysis should identify possible threats and which physical actions should be taken to obtain a minimum-solution as a basic protection for the object. The Main Plan should as a result of the analysis, contain information about proposed solutions and cost. Technical solutions and more detailed plans should be carried out in later plan phases.

The Main Plan should identify the security threats linked to planned infrastructure as buildings, objects, stations etc. and propose alternative solutions to reduce security risks from sabotage, terrorism or other crime.

B. Strategies for the built environment

The strategies rely upon the ability to influence offender decisions that precede criminal acts. Research into criminal behaviour shows that the decision to offend or not to offend is more influenced by cues to the perceived risk of being caught than by cues to reward or ease of entry.

Consistent with this research, the strategies emphasise enhancing the perceived risk of detection and apprehension.

Built environment implementations seek to dissuade offenders from committing crimes by manipulating the built environment from which those crimes proceed or occur. The three most common built environment strategies are natural surveillance, natural access control and natural territorial reinforcement.

Natural surveillance and access control strategies limit the opportunity for crime. Territorial reinforcement promotes social control through a variety of measures.

C. Natural surveillance

Natural surveillance increases the threat of apprehension by taking steps to increase the perception that people can be seen. Natural surveillance occurs by designing the placeing of physical features, activities and people in such a way as to maximize visibility and foster positive social interaction among legitimate users of private and public space. Potential offenders feel increased scrutiny and limitations on their escape routes.

- Place windows overlooking sidewalks and parking lots.
- Leave window shades open.
- Use passing vehicular traffic as a surveillance asset.
- Create landscape design that provides surveillance, especially in proximity to designated points of entry and opportunistic points of entry.
- Use the shortest, least sight-limiting fence appropriate for the situation.
- Use transparent weather vestibules at building entrances.
- When creating lighting design, avoid poorly placed lights that create blind-spots for potential observers and miss critical areas. Ensure that potential problem areas are well-lit: pathways, stairs, entrances/exits, parking areas, ATMs, phone booths, mailboxes, bus stops, children's play areas, recreation areas, pools, laundry rooms, storage areas, dumpster and recycling areas, etc.
- Avoid too-bright security lighting that creates blinding glare and/or deep shadows, hindering the view for potential observers. Eyes adapt to night lighting and have trouble adjusting to severe lighting disparities. Using lower intensity lights often requires more fixtures.
- Use shielded or cut-off luminaries to control glare.
- Place lighting along pathways and other pedestrian areas at proper heights for lighting the faces of the people in the area (and to identify the faces of potential attackers).

Natural surveillance measures can be complemented by mechanical and organizational measures. For example, CCTV cameras can be added in areas where window surveillance is unavailable.

D. Natural access control

Natural access control limits the opportunity for crime by taking steps to clearly differentiate between public space and private space. By selectively placing entrances and exits, fencing, lighting and landscape to limit access or control flow, natural access control is obtained.

- Use a single, clearly identifiable, point of entry
- Use structures to divert persons to reception areas
- Incorporate maze entrances in public rest rooms. This avoids the isolation that is produced by an anteroom or double door entry system
- Use low, thorny bushes beneath ground level windows.
- Eliminate design features that provide access to roofs or upper levels
- In the front yard, use waist-level, picket-type fencing along residential property lines to control access, encourage surveillance.
- Use a locking gate between front and backyards.
- Use shoulder-level, open-type fencing along lateral residential property lines between side yards and extending to between back yards. They should be sufficiently unencumbered with landscaping to promote social interaction between neighbours.
- Use substantial, high, closed fencing (for example, masonry) between a backyard and a public alley.

Natural access control is used to complement mechanical and operational access control measures, such as target hardening.

E. Natural territorial reinforcement

Territorial reinforcement promotes social control through increased definition of space and improved proprietary concern. An environment designed to clearly delineate private space does two things. First, it creates a sense of ownership. Owners have a vested interest and are more likely to challenge intruders or report them to the police. Second, the sense of owned space creates an environment where "strangers" or "intruders" stand out and are more easily identified. By using buildings, fences, pavement, signs, lighting and landscape to express ownership and define public, semi-public and private space, natural territorial reinforcement is obtained. Additionally, these objectives can be achieved by assignment of space to designated users in previously unassigned locations.

- Maintaining premises and landscaping so that it communicates an alert and active presence occupying the space.
- Provide trees in residential areas. Research results indicate that, contrary to traditional views within the law enforcement community, outdoor residential spaces with more trees are seen as significantly more attractive, safer, and more likely to be used than similar spaces without trees.
- Restrict private activities to defined private areas.
- Display security system signing at access points.
- Avoid cyclone fencing and razor-wire fence topping, as it communicates the absence of a physical presence and a reduced risk of being detected.
- Placing amenities such as seating or refreshments in public areas in a commercial or institutional setting helps attract larger numbers of desired users.

- Scheduling activities in common areas increases proper use, attracts more people and increases the perception that these areas are controlled.

Territorial reinforcement measures make the normal user feel safe and make the potential offender aware of a substantial risk of apprehension or scrutiny.

F. Buildings and parking areas

Traditionally, railway stations have been open public areas, often in close connection with build-up areas and towns. Mixed use of the public area with traffic and business hand in hand is normally the situation at a station.
Flexible use of the station areas should not obstruct efficient measures against crime actions when it is planned well ahead. Public security can be taken care of by a combination of surveillance and well arranged station areas, as a “clean station”- concept.

Parking areas for cars and bicycles should be designed –and placed away from buildings and public areas with large populations of passengers.

Parking areas for cars should not be places near buildings and constructions, as this can lead to a disaster in case of an explosion.
Entrance to platforms should have a physical obstruction (concrete, fences) to prevent access of vehicles. On the other hand there must be access for ambulances, fire brigade etc to enter the station areas via automatic gates.

Bicycle parking should not be planned outside room for traffic management, security guards etc.

Where sheltered security is not possible to obtain, reinforced constructions against burglars should be considered, for example for technical rooms. Outdoor cabling should be secured in sufficient distance from public areas.

Guard rooms for security personnel should not be placed near public areas. The guard room could be a target before a possible terror action against a passengers / business area etc at the station. One must also be secured that the guard room can be operative under an evacuation in a threat situation.

G. Entrance and emergency exits

To avoid accumulation / crowd and distress of passengers at the entrance and emergency exit in a situation of evacuation, the exits must be well marked with good signboards for efficient public information.

Public areas should be well lighted, also for the purpose of giving good pictures from the surveillance cameras.
Research confirms that where public lighting is weak or patchy, increasing the levels and consistency of illumination reduces the fear of crime and makes people feel more secure. The relationship between lighting and crime itself (as opposed to fear of crime) is somewhat more complex, but recent research indicates that improved lighting can indeed result in crime reduction, particularly when this has been combined with other community safety initiatives.

Cargo terminals

Cargo terminals normally consist of large areas, many buildings, different companies and a complex ownership.
A risk security analysis should be performed for these areas. The analysis should include an overview of the activity and the companies inside the cargo terminal. A special focus should be on the access control and identification of traffic in –and out of the terminal. This should include both vehicle control and personnel control. Also topics like crime activity as burglar, exchange of containers, sabotage should be highlighted.
Critical infrastructure inside the terminal also needs protection. Logistic systems, signalling systems, crane control, etc, should therefore be identified and analysed.

H. Role of landscape design

Secure Architecture sees sensitive landscape design as essential to achieve an environment that creates a sense of place and community identity. Landscape design. in this context encompasses the planning, design and management of external spaces, especially public areas in the urban environment. It is one of the key disciplines involved in successful urban design. Both hard landscapes (constructional elements) and soft landscape (planting) are important in this respect. Care must be taken in the design of the external environment to avoid inadvertent creation of opportunities for crime through, for example, providing hiding places or facilitating access to the upper floors of buildings. The positioning and choice of planting should be such that the potential for such problems is minimised.

It is vital that open space is positively designed, i.e. that function, location, layout and detailed design are all carefully thought through with due regard to the social and environmental context. To simply accept leftover undevelopable parts of a site as public open space is an invitation to future crime and disorder problems. Positive design and planning is equally important in the case of footpaths, and here professional landscape design skills can be particularly valuable.

- Sensitive design that takes full account of the social and environmental context and encourages positive community interaction can help foster community spirit and a sense of shared ownership and responsibility. Where possible, the local community should be involved in the planning and design process;
- Provision of high quality landscape settings for new development and refurbishment, where external spaces are well-designed and well integrated with the buildings, can help create a sense of place and strengthen community identity;
- Well designed public areas which are responsive to community needs will tend to be well used and will offer fewer opportunities for crime;
- Long-term maintenance and management arrangements must be considered at an early stage, with ownerships, responsibilities and resources clearly identified.

I. Maintenance standards

In general maintenance standards send powerful signals that undoubtedly influence people’s behaviour. It is vitally important that ownership and responsibilities for external space are clearly identified, and that design should facilitate ease of maintenance and management. Sufficient resources must be made available to adequately maintain buildings and public areas, including open spaces and footpaths. High standards of maintenance will encourage active use and enjoyment by the community, and engender a sense of civic pride and vitality. On the other hand, poor maintenance (such as failure to sweep up broken glass or remove graffiti, damaged paving and street furniture, failure to repair walls and buildings etc) can lead to a downward spiral of neglect, loss of environmental quality and reduced levels of use by the community, leaving the door open to vandalism and other anti-social or criminal behaviour.

IV. DETAIL–AND BUILDING DESIGN

A. Design parameters

When starting the detailed design, the chosen security measures should be described in detail as a part of the planning. It must be considered if part of this planning should be defined as restricted information.

The following topics should be documented if relevant for the planned object:

- Architecture & Design
- Access control & Electronic security
- Video surveillance
- Public information
- Lighting
- Sign boards
- Choice of building materials
- Litter bins
- Ticket automats
- Platform –and station furniture
- Emergency equipment
- Maintenance standards

B. Architecture & Design

Suitable design of public areas, platforms, platform shelters, technical units and buildings can contribute to lower risk and reduce the damage caused by crime, sabotage or terrorism.
Clear line of sight is important for the video surveillance cameras to catch un-normal situations and suspicious objects.

A well designed station will contribute to an efficient distribution of the surveillance cameras.
Station furniture must not be placed in line of sight. Avoid weather shelter in line of sight.
Station equipment must in general be set up according to the security plan.
Station equipment must not provide hiding places for explosives or dangerous objects.
Waiting rooms must be clearly vivible from outside (social control).

Security measures planned to be implemented with increased threats, and which is expensive and will take time to implement, should be established as a part of the basic protection measures (green alert level).

D. Access control & Electronic security

Access control, combined with intrusion-detection system, should be planned where it is necessary to control legal access to offices, guard rooms etc.
Electronic security should be used if physical protection (lock, gates etc.) is insufficient.
Electronic access control should be combined with a personal identification card (name, picture, employer, etc).
In general there should be access control to restricted areas (not public areas).
Areas/offices for graded information and equipment should have special access procedures.

E. Camera surveillance

Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.
The cameras must be installed with free line of sight.
CCTV could be used for surveillance in areas that may need monitoring such as public areas, platforms, technical installations, lifts, luggage boxes, restricted areas, gates etc.
New technology enables the traffic management to supervise the infrastructure from defined central control rooms, and combine CCTV with alarms.
Surveillance of the public using CCTV is particularly common in the UK, where there reportedly are more cameras per person than in any other country in the world. There and elsewhere, its increasing use has triggered a debate about security versus privacy.

F. Public Information

In an emergency situation with evacuation from stations and public areas, it is important that information via PA system is done in a proper way. The PA installation must be planned and operated from a control room. The control room must be placed to enable the operators to remain in the control room as long as possible before evacuation. The control room / traffic management operating room should therefore be separated from public areas. The PA system should also be connected to siren in case of gas-alarm etc.

G. Lighting

Research confirms that where public lighting is weak or patchy, increasing the levels and consistency of illumination reduces the fear of crime and makes people feel more secure. The relationship between lighting and crime itself (as opposed to fear of crime) is somewhat more complex, but recent research indicates that improved lighting can indeed result in crime reduction, particularly when this has been combined with other community safety initiatives.

Different sources and patterns of lighting need to be considered for different environments. Recent research suggests that for a given lighting intensity, white light is more beneficial in terms of safety than coloured light such as from sodium lamps.

Care must always be taken to ensure that the environmental impact of light spillage or light pollution is kept to a minimum, and does not create problems for residents or motorists or have a harmful effect on the ecology or local character of an area.

- Improved lighting can be effective in reducing fear of crime, and in certain circumstances reducing the incidence of crime.
- Proper lighting is very important in a situation of evacuation
- Different lighting sources need to be considered for different environments – the character of the local environment must always be respected.

H. Sign boards

All public areas should have proper sign boards that indicate emergency exits, emergency equipment etc.

I. Choice of building materials

Materials used at stations and other public areas should be fireproof. In case of heat and fire it should give out as little toxic gas as possible.
All sorts of materials should be easy to keep clean (tagging). Materials used in critical infrastructure (windows / glass) should be explosion-proof. Broken glass is often the cause of personnel injuries

J. Litter bins

Public litter receptacles should be avoided on a station or on public areas. These could be hiding places for explosives. Preferably refuse sacks of clear transparent plastic should be used. If litter receptacles are used, there should be procedures for removing them if the threat level rises. Under no circumstances should litter boxes be placed near critical columns or concrete constructions.

K. Luggage lockers – Left luggage

Lockers and left luggage offices should preferable be placed away from public areas. It should also be placed away form critical concrete structures, guard rooms or technical rooms.
At larger stations the lockers and left luggage offices should be place to provide easy control of the luggage and the access under higher threat levels.

L. Ticket machines (ATM) and sales automates

It should not be possible to hide dangerous objects or explosives behind –or on top of ATM’s and sales automates. There must therefore be a strategy where to place these.
The equipment must be placed to make it possible for surveillance cameras to supervise movements around the machines and automates. Also it should be possible to watch them from the guard rooms. If several machines and automates are placed together, they should be placed into a wall or in groups.

M. Platform –and station furniture

Platform –and station furniture should be placed away from the passenger track and should be well maintained. I must be possible to get a clear view under the furniture to avoid hiding dangerous objects under –or behind the furniture.

N. Emergency equipment

Emergency equipment such as fire extinguishers, first aid equipment etc, should be clearly visible and properly maintained. The equipment must be sealed.

V. REFERENCES

Norwegian National Rail Administration Security Programme

Wikipedia – the free encyclopedia

Annex V (Switzerland)
A contribution to the debate on innovation strategies for security in rail transportation

Introduction

Switzerland, in the Centre of Europe, is part of the European rail and road Network. It is linked to the European Union and its member states by International and bilateral agreements which regulate inland and transit transport of passengers and goods. Transit routes such as the rail links through the Alps and the Gotthard road tunnel with its access from both sides are part of the critical infrastructures. That means that they are exposed to various dangers such as environmental and natural disaster, for instance earthquakes, water floods, rock fall, snow and ice and could be blocked for hours, weeks and even months. In addition we have to cope with man-made disaster for instance increased radioactive radiation, spread of toxic chemicals, pandemic diseases, violence, terrorist attacks and so on. There are also safety problems coming from the transported goods (dangerous goods) and the means of transport itself such as trains and trucks. Security is one of the main international problems in transport and we all have to take measures in order to enhance security in ordinary and extraordinary situations.

Innovation strategies

What could be “innovation strategies” in this context? We cannot avoid or regulate disasters. Some of them are not very frequent but, nevertheless, need to be considered as a real threat because of the great damage that they will cause. On the other hand we have limited financial resources to finance our measures. So, we have to reduce our state of readiness in normal times and have to be able to adapt our degree of readiness corresponding to circumstances and a possible escalation in a worsening situation.

In conclusion, if we think of innovation strategies in connection with security, we have to think in two directions: 1) How to maintain a reasonable state of readiness corresponding to the pending range of threats in ordinary times. 2) How to manage escalating threats or the crises in case of major events.

Particularities of Switzerland

Most countries have to cope with particularities of their geographic situation or political exposure, their political and economical structures on the strategic level and their operational structures of transport. Swiss solutions are mainly due to Swiss conditions. We have to cope with our federal structures. In practice, the cantons are sovereign and are proud of their sovereignty. The central government can only go as far as the cantons have delegated the task to the Federal Government. As a matter of fact the cantons are responsible for public safety and the crisis management on their respective territory and the Federal Government provides aid only if the means of the cantons are exhausted and the Federal Government is asked.

However, as transport is international, the Federal Government has important tasks and competences in this domain on a strategic level. The Federal Office of Transport (FOT), which is in charge of public transport, coordinates large projects such as the Lötschberg and the Gotthard base tunnels and the connection with the European high-speed railway net work. The Federal Office of Transport exercises its authority by handing out or withdrawing concessions and regular controls guarantee the safety and security measures taken by the railway companies. A special decree regulates the coordination of traffic in the event of disasters and emergency situations (OCTE), which mainly consists of a Leading Organism (LO OCTE) and a permanent office, which is in charge of preparing regular meetings with all offices which have to do with transport security such as for prevention or for cooperating in the event of disaster and emergency situations. In this cooperation are included the 26 cantons, which are primarily responsible for the crisis management in case of an event and for the public safety within their territory.

In conclusion the responsibility and the competency remain where they are. There is no change in ordinary and extraordinary situations caused by major events but an obligation for all to cooperate in the prevention and crises management in case of an event of disaster and emergency.

- - - - -