LA SÛRETÉ ET LA SÉCURITÉ DES TUNNELS ET DES AUTRES INFRASTRUCTURES ESSENTIELLES

Ahmed KASHEF, Chef du groupe résistance au feu et gestion des risques, programme Recherche en incendie, Institut de recherche en construction, Conseil national de recherches du Canada (Canada)

Un pourcentage important des infrastructures de transport actuelles ont été conçues en fonction des connaissances et de l'expérience d'il y a plusieurs décennies. En attendant, les transports et la circulation ont considérablement augmenté en volume et ont également changé sur le plan de leur composition. C'est ainsi que le niveau de sécurité d'une bonne part des infrastructures actuelles a souvent baissé dans les cas où aucune mesure intermédiaire n'a été prise pour faire face aux changements de quantité, de type et de chargement des véhicules et du matériel roulant.

Qui plus est, les attentats du 11 septembre 2001 ont fait ressortir la nécessité de protéger notre réseau de transport contre les attentats terroristes. Avant le 11 septembre, ces menaces avaient toujours été considérées comme mineures et, à ce titre, on ne prêtait guère attention à la conception des infrastructures en fonction de la sûreté. Même si la menace est aujourd'hui admise, on lutte toujours pour définir des stratégies et des solutions afin de protéger le réseau de transport contre le terrorisme. Les codes et les normes de conception des routes ne tiennent pas compte des charges qui pourraient résulter d'attentats terroristes, même si des recherches sont amorcées avec une certaine lenteur pour modifier la donne. Il n'existe pas encore de procédure systématique pour évaluer la vulnérabilité structurale des principaux ouvrages.

Les tunnels représentent des cibles tentantes, car a) ils sont importants pour l'économie des localités avoisinantes, en particulier lorsqu'ils servent au transport des marchandises ; b) de nombreuses personnes s'y trouvent à des heures prévisibles et c) le milieu confiné accentue d'autant plus les risques de victimes résultant d'explosions, d'effondrement et d'inondations dans un espace clos. Comme exemples d'attaques délibérées et préjudiciables contre les réseaux et les usagers des transports, il faut mentionner l'attaque au sarin perpétrée en 1995 à Tokyo (12 morts et des milliers de malades), l'incendie criminel de 2003 à Daegu (198 morts et 147 blessés), l'attaque d'une gare ferroviaire en 2004 à Madrid (191 morts) et l'explosion de bombes en 2004 à Moscou (39 morts et 100 blessés) et en 2005 à Londres (56 morts). Ces attentats terroristes ont très nettement sensibilisé les gens à la vulnérabilité des réseaux de transport aux actes malveillants. Ils ont soulevé de nombreuses questions sur la gestion des questions de sécurité et de sûreté des infrastructures actuelles et prévues dans des espaces clos.

Les évaluations des besoins ont souligné les lacunes actuelles des connaissances dans les domaines de la vulnérabilité des ouvrages aux attentats terroristes ; la définition des menaces ; les charges structurales qui résultent de ces menaces ; les lieux possibles des attentats ; les méthodes d'analyse coûts-avantages et d'évaluation des risques ; l'optimisation de la conception pour la gestion des incidents ; les stratégies d'évaluation après un incident et enfin, la nécessité de techniques de réparation et de remise en état rapides.

Il est impossible de protéger toutes les infrastructures de transport contre toutes les menaces. C'est pourquoi il faut faire des choix dans la manière logique dont les infrastructures/le personnel/l'équipement (les actifs essentiels) ont le plus besoin d'être protégés et prendre les mesures qu'il faut pour assurer leur protection.

LEÇONS QUE L'ON PEUT TIRER DES RÉCENTS INCENDIES TRAGIQUES SURVENUS DANS DES TUNNELS

Les leçons que l'on peut tirer des récentes tragédies survenues dans le réseau de transport méritent toute notre attention et la formulation de recommandations crédibles et économiquement réalisables, notamment :

- pour concevoir intelligemment et évaluer la sécurité/sûreté des réseaux de transport, il faut une démarche holistique pluridisciplinaire, faisant appel à la contribution de tous les intervenants et des technologies en cause ;
- il est nécessaire de mieux comprendre les risques et les vulnérabilités pour bien planifier les mesures de prévention et d'atténuation ;
- les véhicules sont les principales causes des menaces, en raison de défectuosités techniques ou mécaniques

SECURITY AND SAFETY OF ROAD TUNNELS AND OTHERCRITICAL INFRASTRUCTURES

Ahmed KASHEF, Group Leader, Fire Resistance and Risk Management, Fire Research Program, Institute for Research in Construction, National Research Council of Canada (Canada)

A large percentage of the existing transportation infrastructure was designed based on the knowledge and experience of decades past. In the meantime, transport and traffic have grown considerably in volume and has also changed in terms of its composition. Consequently, the safety level in much of the existing infrastructures has often decreased in cases where no intermediate measures were taken to cope with the changes in quantity, type and loading of vehicles and rolling stock.

What is more, the event of September 11, 2001, helped bring into focus the need to protect our transportation network against terrorist incidents. Prior to September 11, these threats had always been perceived as minor, and, as such, little attention was paid to designing for security. Although the threat has been recognized, there is still a struggle to define strategies and solutions to protect our transportation network against terrorism. Highway design codes and standards do not address loadings that might be experienced from terrorist activities, although research is slowly getting underway to change this. Moreover, to this day there is no systematic procedure to consider structural vulnerability of key structures.

Tunnels make tempting targets because (a) they are important to the economic viability of surrounding communities, especially when they are used to transport goods; (b) many people are present at predictable times; and (c) the enclosed environment further compounds the potential for casualties from the effects of confined blast events, collapse, and flooding. Examples of intentional, harmful aggression against transportation systems and users are the 1995 sarin gas attack in Tokyo (12 deaths and thousands sick), the 2003 arson fire in Daegu (198 deaths and 147 injuries), the 2004 train station attack in Madrid (191 deaths), and the 2004 bombing in Moscow (39 deaths and 100 injuries) and London (56 deaths) in 2005. These terrorist attacks resulted in raised awareness of the vulnerability of transportation systems to malicious acts. They have raised many questions with regards to the management of safety and security issues of existing and projected infrastructure in enclosed spaces, which require consideration and solutions.

Need assessments have highlighted current gaps of knowledge in the areas of structural vulnerability to terrorist events; threat definition; structural loadings produced by these threats; possible attack locations; cost-benefit and risk assessment methodologies; optimization of design for incident management; post-event assessment strategies; and the need for rapid repair and restoration techniques.

It is not possible to protect all transportation infrastructures against everything. Therefore, choices must be made in a logical manner as to which facilities/personnel/equipment (critical assets) need most protection and what measures should be taken to protect them.

LESSONS LEARNED FROM RECENT TUNNEL FIRE TRAGEDIES

The lessons learned from recent transportation network tragedies require attention and implementation of credible and economically feasible recommendations, such as:

- in order to properly design and assess safety/security in transportation systems, a multi-disciplinary holistic approach is necessary, comprising input of all stakeholders and technology involved;
- better understanding of risk and vulnerability to properly plan prevention and mitigation measures;
- vehicles are the main causes of threats, due to technical or mechanical faults or due to people's negligence or malicious intentions;
- early detective means and interoperable communications networks are of paramount importance in controlling event size and limiting its impact;
- enhanced personnel training including tabletop exercises, onsite training, drills, and exercises;
- the protection systems must be capable of handling combinations of worst-case conditions;

ou de la négligence des gens ou encore d'intentions malveillantes ;
- des moyens de détection précoces et des réseaux de communication interopérables revêtent une importance cruciale pour limiter la taille de l'incendie et en atténuer les conséquences ;
- il faut améliorer la formation du personnel, notamment par des exercices de simulation, une formation et des exercices sur place ;
- les systèmes de protection doivent être capables de faire face aux combinaisons des pires scénarios ;
- il faut mieux comprendre et tenir compte des facteurs humains et du comportement de l'être humain dans les situations critiques. À cet égard, des issues et des passages de secours sécurisés représentent la priorité absolue dans toute situation de crise.

PROTECTION DES RÉSEAUX DE TRANSPORT

Les réseaux de transport sont vulnérables à tout un éventail de menaces qui peuvent aboutir à une dégradation opérationnelle. Par exemple, ils peuvent être perturbés par l'apparition de risques ou la concrétisation de menaces. Les risques sont des événements accidentels qui peuvent revêtir la forme d'un séisme, d'un incendie, d'une crue ou d'une tornade. Les risques peuvent être encore plus complexifiés lorsqu'on a affaire à des risques multiples, comme un incendie qui fait suite à un séisme ou un feu de friches qui provoque un incendie urbain. Pour ce qui est des menaces, celles-ci peuvent varier d'un incendie à une bombe artisanale, à un attentat terroriste de nature radioactive, chimique ou biologique. Même si des restrictions existent sur le transport d'engins explosifs ou d'autres substances dangereuses, ces restrictions sont inopérantes face à des menaces terroristes. Il n'est pas facile de se procurer de grandes quantités d'explosifs, mais il est relativement simple pour des terroristes de s'emparer de camions transportant de l'essence ou d'autres matières inflammables et d'y mettre le feu au milieu d'un long tunnel.

De par leur nature, la vulnérabilité des infrastructures souterraines doit être évaluée en tenant compte des effets interactifs de la déflagration ou des pressions de l'explosion, de l'ouvrage, du sol avoisinant et de l'attentat terroriste délibéré. La vulnérabilité des infrastructures de transport peut être liée à un aspect de l'ouvrage (p. ex. type de construction, géométrie, largeur, courbure, déclivité, insuffisance de l'épaisseur du revêtement du tunnel, recouvrement insuffisant du tunnel et proximité relative du danger ou de la menace pour le revêtement), être liée à la nature (p. ex. support géologique, conditions hydrauliques, crues subites, avalanches, chutes de roches, séismes, tsunamis et changements climatiques) ou être liée à la circulation (p. ex. accès non réglementé des véhicules, insuffisance des inspections des véhicules ou restrictions imposées aux cargaisons, circuits de circulation, opérations d'entretien, etc.).

ANALYSE D'ÉVALUATION DE LA VULNÉRABILITÉ

Une analyse d'évaluation de la vulnérabilité doit être effectuée sur les composantes essentielles des réseaux de transport. Le but de l'analyse est de fournir aux décideurs des renseignements sur les vulnérabilités, par exemple : sur l'endroit possible, la nature, les conséquences (p. ex. morts, blessés, dégâts matériels, interruption des services) et les mesures d'atténuation possibles. L'évaluation de la vulnérabilité devrait impliquer : opérateurs, les agents de renseignement, les sociétés et les inspecteurs de sûreté, gestionnaires d'installations, et les groupes d'utilisateurs.

Au cœur de l'évaluation de la vulnérabilité, il y a l'évaluation judicieuse des risques/menaces possibles qui permet d'établir des scénarios de risque crédibles. La probabilité d'un scénario peut varier de faible (l'incident ne s'est pas produit par le passé), moyen (l'incident ne s'est pas produit par le passé, mais peut se matérialiser avec un changement dans l'environnement) ou élevée (l'incident s'est produit dans le passé). Les scénarios de risque cernés sont alors traduits en chargements de calcul nécessaires à l'estimation des conséquences des vulnérabilités et à la détermination des niveaux de risque connexes. Les risques estimatifs sont ensuite évalués pour déterminer leur acceptabilité par rapport à des critères de risque qualitatifs ou quantitatifs. La mesure suivante consiste à atténuer ou à réduire le niveau des risques inacceptables. À cet égard, il existe deux stratégies distinctes : l'une qui cherche à réduire la probabilité d'apparition d'une menace (mesures préventives), la deuxième visant à réduire les conséquences de la vulnérabilité (mesures d'atténuation). Ces mesures sont itératives (*figure 1, page suivante*) et ont pour but d'optimiser la conception (à la fois dans l'optique du niveau de risque et des coûts-avantages).

Trois catégories d'incidents allant d'un risque modéré à un risque élevé peuvent être envisagées dans l'évaluation de la vulnérabilité, à savoir : évènements pris en compte dans le projet, les événements éminemment redoutables et les événements extrêmes. Les événements éminemment redoutables peuvent nécessiter des mesures de protection complémentaires. Les événements extrêmes, même s'ils ne sont pas utilisés pour la conception de l'ouvrage, doivent

- better understanding and consideration of human factors and behavior in crisis situations. In this regard, securing escape routes and passages is the top priority in any crisis.

PROTECTION OF TRANSPORTATION SYSTEMS

Transportation networks are susceptible to a wide range of vulnerabilities that can lead to an operational degradation. For instance, they can encounter disruption from either occurrence of hazards or successful conduct of threats. Hazards are unintentional events and may be a single event such as an earthquake, fire, flood, or tornado. The hazard events may be further convoluted when dealing with multi-hazards, e.g. fire following earthquake and wildfire inducing urban fire. As far as threats are concerned, these can range from a fire incident, improvised explosive devices, radioactive, chemical, to a biological terrorist attack. Although there are restrictions on carrying explosives or other hazardous materials into transportation infrastructures, these restrictions are irrelevant when dealing with terrorist actions. Large amounts of explosives are not easily obtained, but it is a simple matter for terrorists to hijack trucks transporting gasoline or other flammable materials, and ignite them in the middle of a long tunnel.

Because of their nature, the vulnerability of underground infrastructures must be assessed by considering the interactive effects of the blast or explosion pressure, the structure, the surrounding ground, and intentional terrorist attack. The vulnerability of transportation infrastructures could be structure-related (e.g. type of construction, geometry, width, curvature, gradient, insufficient tunnel liner thickness, inadequate tunnel cover, and relative proximity of hazard or threat to liner), nature-related (e.g. geological medium, groundwater conditions, flash floods, avalanches, rock fall, earthquakes, tsunamis, etc.) or traffic-related (e.g. uncontrolled access of vehicles, insufficient vehicle inspections and/or cargo restrictions, traffic flow patterns, maintenance operations).

VULNERABILITY ASSESSMENT ANALYSIS

A vulnerability assessment analysis should be conducted on critical components of transportation networks. The aim of the analysis is to offer decision-makers information on vulnerabilities for instance: possible location, nature, consequences (e.g. fatalities, injuries, property damage, interruption of services), and potential mitigation measures. The vulnerability assessment should involve: operators, intelligence officials, security companies and inspectors, facilities managers, and user groups.

Fundamental to the process of vulnerability assessment is the proper evaluation of possible hazards/threats in order to develop credible risk scenarios. The probability of a scenario could range from low (incident has not occurred before), medium (incident has not occurred in the past but may materialize with shift in the environment), or high (incident has occurred in the past). The identified risk scenarios are then translated into design loads necessary for estimating the consequences of vulnerabilities and determining the associated risk levels. The estimated risks are then evaluated to determine their acceptability against qualitative and/or quantitative risk criteria. The subsequent step is to mitigate or reduce the level of unacceptable risks. In this regards, there are two distinct strategies; one aimed at reducing the probability of occurrence of a threat (pre-emptive measures), while the second aimed at reducing vulnerability consequences (mitigative measures). These steps are iterative (*figure 1, next page*) with the goal of achieving an optimal design (both from risk level and cost-benefit perspectives).

Three categories of events that range from moderate to high risk could be considered in the vulnerability assessment, namely: normal design events, (all credible scenarios, relevant to specific infrastructure, that are possible to occur during its service life) high challenge events (i.e. low probability, high consequence events, such as BLEVE of an LPG tanker in road tunnel), and extreme events (e.g. natural disasters and terrorist attacks). High challenge events may require additional protection measures. Whereas, extreme events, while not used for design, should be considered in the design to minimize the probability of their occurrence by means of security provisions or prevention techniques. The Transportation Research Board (TRB) developed sets of 13 most critical hazard/threat scenarios for tunnels based on: tunnel type (road, transit, or rail); construction type (immersed tube, cut-and-cover, bored or mined, air-rights structure); and system types within infrastructure (ventilation system, life safety system, power distribution, command and control, and communications).

Risk analysis methods have been explicitly required by the European Directive 2004/54/EC on minimum

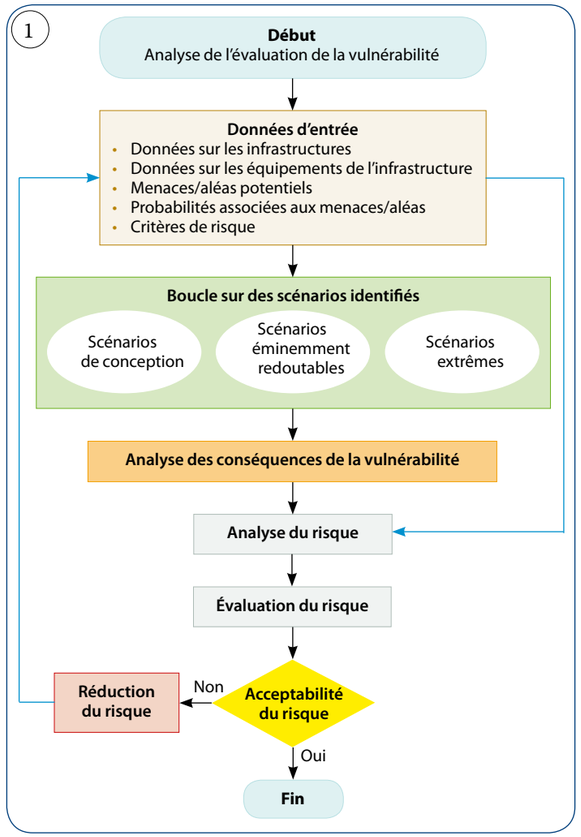

Figure 1 - Procédure d'évaluation de la vulnérabilité

être pris en considération dans le projet pour minimiser la probabilité d'apparition. Le *Transportation Research Board* (TRB) a élaboré des ensembles de 13 scénarios de risque/menace les plus critiques pour les tunnels en fonction : du type de tunnel (routier, transport en commun ou ferroviaire) ; du type de construction (caisson immergé, tranchée couverte, foré ou creusé, ouvrage aérien) et des types de systèmes dans l'infrastructure (système de ventilation, système de sécurité de personne, distribution d'électricité, commandement et contrôle et communications).

Des méthodes d'analyse des risques sont explicitement prescrites par la Directive de l'Union européenne 2004/54/EC concernant les exigences de sécurité minimales applicables aux tunnels du réseau routier transeuropéen. En vertu de cette approche, les risques des dangers cernés sont déterminés à partir du produit de leur probabilité et de leurs conséquences. Une fois analysés, les risques doivent être évalués et, s'ils sont inacceptables, il faut y remédier de manière optimale. Dans une démarche analogue, le risque, R_i, qui se rattache à une vulnérabilité quelconque face à un événement menaçant, V_i, peut être estimé à partir de l'équation suivante :

$$R_i = V_i P_i$$

où P_i désigne la probabilité d'apparition d'une menace et V_i est la vulnérabilité à la présence d'une menace. La vulnérabilité est la conséquence de la faiblesse dans la conception ou le fonctionnement d'un élément du réseau de transport (par exemple l'échec local, global ou progressif impliquant des ouvrages souterrains adjacents). En cas de menaces naturelles, la probabilité d'une menace et la vulnérabilité à la menace peut être considérée comme étant indépendantes l'une de l'autre. Au contraire, les menaces terroristes sont moins prévisibles et leur probabilité semble pouvoir être reliée au niveau de vulnérabilité (plus la vulnérabilité est élevée, plus la menace risque de se concrétiser). Cela est dû au fait que la vulnérabilité apparente suscite l'intérêt des terroristes pour provoquer un nombre de victimes important et/ou des dommages économiques considérables. Le *tableau 1* montre un exemple élémentaire de quantification des risques en conjuguant conséquences et probabilités. Plus le nombre est grand, plus le risque est élevé.

TABLEAU 1 -
EXEMPLE DE TABLEAU DE QUANTIFICATION DES RISQUES

Probabilité	Conséquence		
	Grave	Très Sérieux	Préjudiciable
Élevé	9	8	6
Moyen	7	5	3
Faible	4	2	1

CONTRE-MESURES

Il existe différentes façons d'atténuer les risques dans les réseaux de transport ; il peut s'agir de méthodes actives ou passives ; de mesures temporaires ou permanentes, dont la plupart dépendent d'une intervention rapide une fois qu'un incident s'est produit. Il est possible d'accroître la résistance structurelle des infrastructures ; d'introduire des obstacles pour limiter la quantité d'énergie dégagée par un incident (p. ex. barrières périmétriques, topographie, distances de sécurité) ; d'interrompre l'écoulement d'air nécessaire au maintien de la combustion ; d'assurer un environnement supportable pendant le plus longtemps possible ; de fournir un abri convenable aux personnes qui arrivent à s'échapper de l'environnement insupportable, etc.

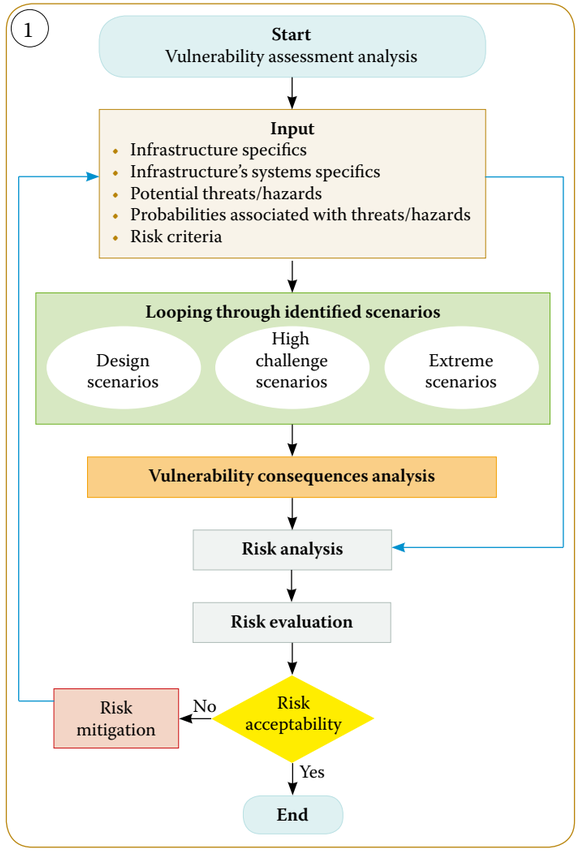

Figure 1 - Vulnerability assessment procedure

safety requirements for road tunnels in the Trans-European Road Network. In this approach, risks of identified hazards are determined from the product of their probabilities and consequences. Once analyzed, the risks need to be evaluated and, if unacceptable, then they need to be optimally addressed. In a similar approach, the risk, R_i, associated with any vulnerability to a threat occurrence, V_i, can be estimated from the following equation:

$$R_i = V_i P_i$$

where: P_i is the probability of a threat occurrence and V_i is the vulnerability to occurrence of a threat. Vulnerability is the consequence of weakness in design or operation of an element of transportation network (e.g. local or global failure or progressive failure involving adjacent underground structures). In case of natural threats, the probability of a threat and the vulnerability to the threat can be assumed to be independent of one another. In contrast, terrorist threats are less predictable and its probability seems to be related to the vulnerability level (the higher the vulnerability is, the more likely the threat is). This is due to the fact that apparent vulnerability attracts terrorists' interest in achieving substantial causalities and/or economic damage. *Table 1* shows a basic example of how risk is quantified by linking consequence and probability. The higher the number, the higher the risk is.

TABLE 1 -
EXAMPLE OF MATRIX
OF RISK QUANTIFICATION

Probability	Consequence		
	Grave	Very Serious	Injurious
High	9	8	6
Medium	7	5	3
Low	4	2	1

COUNTERMEASURES

There are different ways to reduce risk in transportation systems; these may consist of active or passive methods; temporary or permanent measures, most of them relying on a quick action once an event developed. It is possible to increase structural resistance of infrastructures; introduce obstacles to control the amount of energy released by an event (e.g. perimeter barriers, landforms, standoff distances); to cut off airflow needed to maintain combustion; to ensure a tenable environment for the longest possible time; to provide proper sheltering for people escaping from untenable environment; etc.

Countermeasures may include: lighting/signal systems; emergency ventilation system; systems to detect fire, incidents, intrusion, Chemical, Biological, Radiological, Nuclear, and Explosive, CBRNE (e.g. closed-circuit television, CCTV, guards, integrated CBRNE detection system, etc.); fire protection systems (e.g. fixed fire fighting systems); traffic control; hazmat restrictions; employee identification system; evacuation protocols; extend/heighten supply

Parmi les contre-mesures, il peut y avoir : des systèmes d'éclairage/signalisation ; un système de ventilation d'urgence ; des systèmes permettant de détecter les incendies, les incidents, les intrusions, les incidents chimiques, biologiques, radiologiques, nucléaires et explosifs (CBRNE) (p. ex. télévision en circuit fermé ou CCTV, gardes, système intégré de détection CBRNE, etc.) ; des systèmes de protection contre le feu (p. ex. des systèmes fixes de lutte contre les incendies) ; la réglementation de la circulation ; des restrictions des matières dangereuses SIMDUT ; un système d'identification des employés ; des protocoles d'évacuation ; la prolongation/le renforcement des prises d'air d'arrivée et des exercices d'intervention d'urgence grandeur nature.

La sûreté est impossible à assurer par l'utilisation de la technologie seulement. Les solutions détaillées envisagées doivent être évaluées notamment sur le plan des paramètres éthiques, juridiques et de protection des données. L'évaluation doit comprendre l'étude des exigences relatives à l'éducation et à la formation des secouristes et du personnel de sécurité ainsi que la conception d'aides à la prise de décisions pour les autorités et les secouristes. Au nombre des autres éléments à examiner, il y a l'analyse coût-bénéfice des mesures de sécurité individuelles. Enfin, les menaces ne s'arrêtent pas aux frontières nationales et nécessitent une coopération internationale.#

air intakes; and full-scale emergency response exercises.

Security cannot be achieved by the use of technology alone. The comprehensive solutions envisaged should be evaluated in terms of ethical, legal and data protection aspects, among others. The evaluation must include the study of the requirements regarding education and training of rescue and security personnel, as well as the development of decision-making aids for authorities and emergency personnel. Other aspects to be reviewed include the cost-benefit analysis of the individual security measures. Moreover, threats do not stop at national borders and require international government cooperation.#

RÉFÉRENCES - REFERENCES

[1] Transportation Research Board, *Transit Cooperative Research program (TCRP) Report 86/National Cooperative Highway Research Program (NCHRP) Report 525 – Making Transportation Tunnels Safe and Secure*, volume 12, 2006.

[2] Directive 2004/54/CE du Parlement européen et du Conseil du 29 avril 2004 concernant les exigences de sécurité minimales applicables aux tunnels du réseau routier transeuropéen, Bruxelles, Belgique.

[3] Association mondiale de la route (AIPCR), *Guide de bonnes pratiques pour l'exploitation et l'entretien des tunnels routiers*, 05.13.B, 2005.

[4] Bechtel/Parsons Brinckerhoff, *Memorial Tunnel Fire Test Ventilation Program, Comprehensive Test Report*, préparé pour le ministère de la Voirie du Massachusetts/Federal Highway Administration, 1995.

[5] Ernst, S., Patel, M., Capers, H., Dwyer, D., Hawkins, C., Steven, G., Lupton, W., Margro, T., Ralls, M., Rohena, J. et Swanson, M., *Underground Transportation in Europe: Safety, Operation, and Emergency Response*, Office of International Programs, FHWA-HPIP, ministère des Transports des États-Unis, FHWA-PL-06-016, juin 2006.

[6] Kashef, A., *Fire and smoke control in road tunnels – a case study*, ASHRAE Transactions, 114, (pt. 2), Assemblée annuelle 2008 de l'ASHRAE (Salt Lake City, Utah, 21 juin 2008), p. 1 9, 21 juin 2008 (NRCC-50543). Adresse URL : http://irc.nrc-cnrc.gc.ca/pubs/fulltext/nrcc50543/.

[7] Kashef, A., Liu, Z.G., Crampton, G.P., Lougheed, G.D., Hadjisophocleous, G. et Almand, K.H., *Findings of the international road tunnel fire detection research project*. Special edition of Fire Technology on the best detection papers and presentations of SUPDET 2008 (Orlando, FL, 11 mars 2008), p. 74 (NRCC-50837).

[8] Liu, Z.G., Kashef, A., Lougheed, G.D., Debs, A., Gottuk, D.T. et Almand, K.H., *Systèmes de détection d'incendie dans les tunnels routiers – Leçons tirées du Projet de recherche international*, Routes/Roads, (Revue de l'AIPCR/PIARC magazine - n°342), p. 60 69, 2009.

[9] Proulx, G., *To prevent panic in an underground emergency: why not tell people the truth?*, 3rd International Symposium on Fire Science, Elsevier Publications, Kidlington, 1991.

[10] Transports Canada, *Guide de référence sur l'évaluation des risques*, Sûreté du transport terrestre et intermodal, 1003753, 2010.

[11] RISIT (2004) RISIT, *Risk and safety in the transport sector – A state-of-the-art review of current knowledge*. White paper. The Research Council of Norway. Adler, H.A. Economic Appraisal of Transport Projects. Johns Hopkins University Press, 1987.

[12] Association mondiale de la route (AIPCR), *Analyse des risques des tunnels routiers*, Comité technique C3.3 de l'AIPCR 'Exploitation des tunnels routiers', 2-84060-202-4, 2008.#

Figure 2 - Tunnel du Somport © Rafael Lopez Guarga

Figure 2 - The Somport Tunnel © Rafael Lopez Guarga