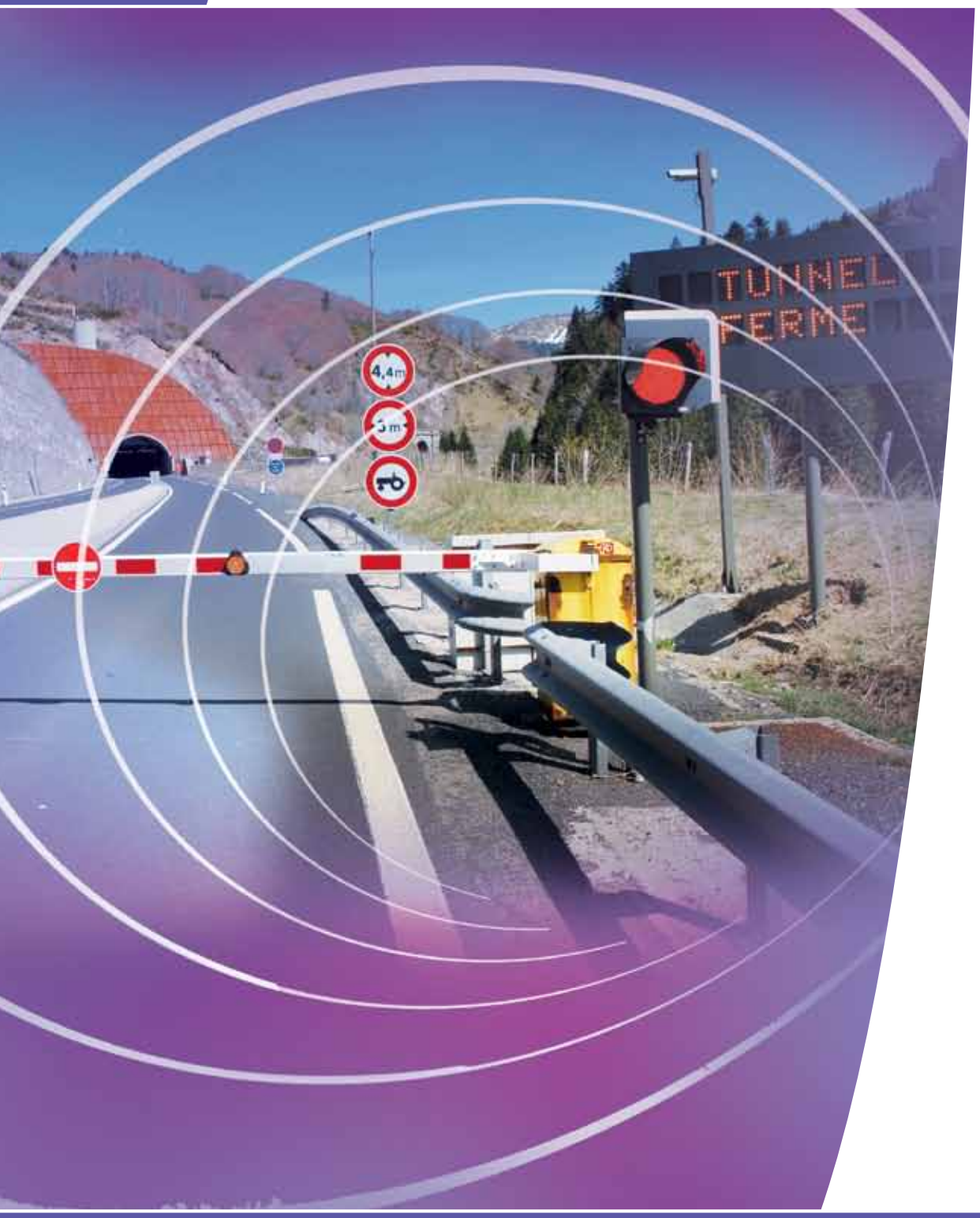
CETU

INFORMATION MEMO No.23

Definition of safety functions Application to degraded operating modes and minimum operating requirements



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère
de l'Écologie
du Développement
durable
et de l'Énergie

July 2014,

Centre d'Études des Tunnels

www.cetu.developpement-durable.gouv.fr

Safety in road tunnels is based on complex technical, human and organizational systems which may be subject to failure and lead to a more or less degraded operating situation. It is important therefore to take these failures into account in a preventive manner to ensure that the operational response is effective and appropriate in the event of an accident.

Given the wide variety of equipment present, a comprehensive approach based on safety functions has been applied to ensure continuity of operations while providing a satisfactory level of safety for users.

This memo follows on from the Guide to Road Tunnel Safety Documentation, in particular booklets 4 and 5 relating respectively to Specific Hazard Investigations (SHI) and the Emergency Response Plans (ERP). It has two objectives: contribute to work on the reliability of systems and help develop degraded operating modes and minimum operating requirements.

Table of contents

1 Introduction

The special features of each tunnel, the specific operating modes, the wide variety of equipment installed (age, characteristics, maintenance procedures, etc.), as well as the varied communication and electric power network architectures mean that we are faced with complex organizational and technical systems that differ greatly from one tunnel to another. Therefore it is not easy to define a methodology to characterize the minimum levels of system reliability required to ensure the best possible level of safety for users.

To achieve this goal, the first step is to introduce and define the safety functions that correspond schematically to the generic actions to be performed by the operator to ensure the safety of tunnel users. A second step is then to identify the resources the operator needs to implement these safety functions. Finally, the approach results in identifying how each safety function is provided by combining different resources.

This document is based on practices observed by analysing French road tunnel safety documentation and in particular booklets 4 [1] and 5 [2] of the CETU Guide to Road Tunnel Safety Documentation. These booklets help clarify the concept of tunnel safety with respect to the events to be taken into account, the hazards to be identified, degraded modes and Minimum Operating Requirements (MOR).

2 Definition of the main safety functions and means of prevention and protection

2.1 The main safety functions

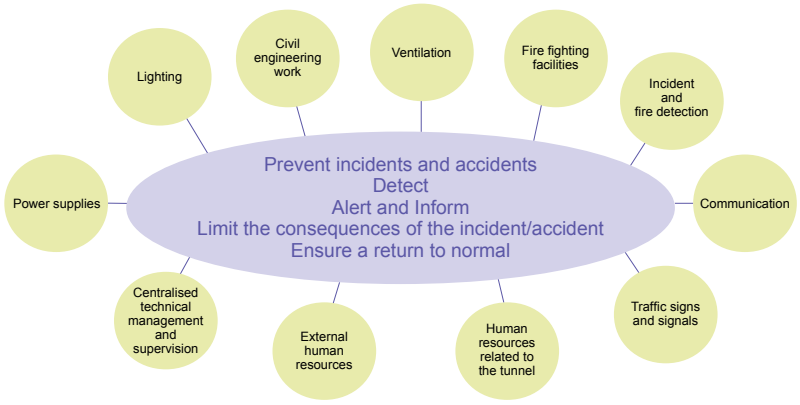
Safety functions are defined in light of the hazards such as identified in Appendix A of the booklet on specific hazard investigations [1] and hazard treatment in operations. [2] They correspond to the goals and major challenges of safety management. They enable this safety management to be streamlined. Some functions concern prevention, others protection, while others apply to both.

These functions can be grouped into five main safety functions:
- prevent incidents/accidents,
- detect incidents/accidents,
- alert and inform,
- limit the consequences of an incident/accident,
- ensure a return to normal.

2.2 The means of prevention and protection

Function implementation requires human and material resources.

Eleven resources have been identified:
- Civil engineering work
- Centralised technical management and supervision
- Power supplies
- Lighting
- Ventilation
- Fire fighting facilities
- Incident and fire detection
- Communication
- Traffic signs and signals
- Human resources related to the tunnel
- External human resources



The main safety functions and means of prevention and protection

The table on the following page sets out the main functions broken down into smaller functions as well as the means for their implementation. It shows that each safety function requires several resources acting simultaneously. Conversely, each resource contributes to one or more safety functions or even to all functions. It thus appears that maintaining certain resources in working order is essential for the safety of the structure and requires stringent operating constraints in case of failure.

3 Correspondence between safety functions and resources

Resources			Safety Functions: F1: prevent incidents/accidents			
			F1-1 monitor the structure, its equipment, the traffic in the tunnel	F1-2 monitor weather conditions, traffic and the external environment	F1-3 ensure safe, comfortable driving conditions	F1-4 keep users informed of traffic conditions
M1: Civil engineering	M1-1	roadway and emergency stopping lane			■	
	M1-2	walkways			■	
	M1-3	drainage			■	
	M1-4	emergency exits - shelters				
M2: Centralised technical management and supervision	M2-1	Sensors and actuators	■	■	■	■
	M2-2	Site network	■	■	■	■
	M2-3	programmable logic controller (PLC)	■	■	■	■
	M2-4	Transport and transmission network	■	■	■	■
	M2-5	Tunnel Control Station (supervision)	■	■	■	■
M3: Power supplies	M3-1	external electricity supply	■	■	■	■
	M3-2	electrical substations and low voltage master distribution panel	■	■	■	■
	M3-3	uninterruptible back-up power supply	■	■	■	■
	M3-4	water supply				
M4: lighting	M4-1	normal lighting	■		■	
	M4-2	emergency lighting	■		■	
	M4-3	emergency-evacuation equipment lighting				
	M4-4	marker lights			■	
M5: ventilation	M5-1	sanitary			■	
	M5-2	smoke extraction				
	M5-3	emergency exits - shelters				
M6: Fire fighting equipment	M6-1	Fire extinguishers				
	M6-2	fire pipe and hydrant				
M7: incident and fire detection	M7-1	closed-circuit television	■	■		
	M7-2	automatic incident detection (AID)				
	M7-3	smoke opacimetres and gas sensors	■		■	
	M7-4	anemometers	■		■	
	M7-5	fire detection (equipment rooms)	■			
	M7-6	fire detection (tunnel)				
	M7-7	safety door opening and fire extinguisher removal	■			
	M7-8	loop-based counting system		■		
M8: communication	M8-1	emergency call network (ECN)				
	M8-2	tunnel operator and emergency service radio broadcasting facilities			■	
	M8-3	user FM radio broadcasts and message insertion			■	■
	M8-4	mobile telephone broadcasting facilities				
M9: traffic signs and signals	M9-1	stop lights				
	M9-2	tunnel closure barriers				
	M9-3	variable message signs			■	■
	M9-4	lane allocation signals			■	
	M9-5	safety and evacuation equipment signage				
M10: human resources related to the tunnel	M10-1	tunnel operator	■	■	■	■
	M10-2	patrols	■	■		■
	M10-3	inspection team				
	M10-4	In-house fire service				
M11: external human resources	M11-1	emergency services				
	M11-2	law enforcement services			■	■
	M11-3	traffic control centre		■	■	■

F2: detect		F3: alert and inform			F4: limit the consequences of the incident/accident				F5: ensure a return to normal
F2-1	**F2-2**	**F3-1**	**F3-2**	**F3-3**	**F4-1**	**F4-2**	**F4-3**	**F4-4**	
detect an incident/accident	classify the incident/accident	alert the emergency services	alert users in the tunnels and at tunnel heads	inform users on the network outside the tunnel	minimise the number of users in the tunnel and avoiding subsequent accidents	limit escalation of the incident while waiting for the emergency services to arrive	facilitate evacuation, get users to safety (self-evacuation)	facilitate emergency service access and actions	check the condition of the structure and perform any urgent work that may be necessary to restore traffic

4 Compensatable and non-compensatable resources and link with degraded operating modes

The analysis of the previous table highlights two types of resources depending on whether or not their failure can be compensated for by resorting to the use of a different type of system.

Whereas for certain resources, membership of one family or another is clear-cut, other resources may be attached to one or the other depending on the particular circumstances of each tunnel.

The definition of compensatable resources (4.1) and non-compensatable resources (4.2) facilitates the development of the degraded operating modes that must be defined when preparing the Emergency Response Plan (ERP).

4.1 Non-compensatable resources

The resources considered here are those whose malfunction or consequent unavailability cannot be offset by the use of equipment of a different type. Hence their unavailability prevents one or more safety functions from being correctly provided and most often results in the tunnel being closed to all or some traffic.

In particular, this category includes all resources which are essential to a large part of, if not all of the safety functions: electric power supplies, centralized technical management, operators in the tunnel control centre, etc..

Some resources, while only contributing to a single function, must also be considered as non-compensatable, such as smoke extraction.

Such equipment is typically scaled taking account of redundancy levels(1), enabling backup solutions to be available.

Example of a non-compensatable resource: smoke extraction ventilation system

4.2 Compensatable resources

These are resources for which malfunctions or unavailability may be temporarily compensated for by other types of equipment or by operating measures. They contribute to a safety function, but this may be provided in another way. Their failure leads to compensatory measures being implemented and routine or non-scheduled maintenance(2) actions being initiated.

For example, the following can be included in this category depending on the case: user communication systems such as radio, lane usage signals and variable message signs, detection systems such as emergency telephones, video surveillance cameras, automatic incident detection systems, pollution sensors, (opacimetres, carbon monoxide and nitrogen oxide sensors) etc.

Example of a compensatable resource: emergency telephone

4.3 Degraded operating modes

The definition of a degraded operation mode requires consideration of:

- The nature of the defect (description and quantification of the loss of functionality admissible for an equipment family), possibly specifying the location of the equipment (to avoid the simultaneous loss of several nearby systems);

- The compensatory measures likely to be implemented: other equipment, human resources (first response team to act, patrols, various on-call resources, etc.) or restriction of traffic;

- The duration beyond which the degraded operating mode can no longer be tolerated.

The three criteria above are used to define thresholds below which the tunnel must be closed.

(1) - Redundancy involves doubling up an equipment item in the event of the failure of one of them.

(2) - Maintenance aims to maintain or restore the item to a specified condition to enable it to perform the function specific to it.

5 Development of minimum operating requirements

The degraded modes of operation in 4.3 will result in the description of the Minimum Operating Requirements (MOR) as defined in booklet 5 of the Guide to Road Tunnel Safety Documentation.

5.1 Development of MORs for non-compensatable resources

In general, non-compensatable equipment is always more or less completely redundant enabling its contribution to safety functions to be relayed in case of a failure. Such provisions are planned at the design phase.

Several redundancy levels are then possible. For example, there may be a backup system that performs at the same level as the normal system (e.g.: a normal power supply and a backup power supply that could take over in the event of a failure), almost complete redundancy (e.g.: a normal power supply and a backup power supply that would only take over some of the nominal capacity in the event of a failure), alternatively, there may be partial redundancy (e.g.: for an extraction system consisting of several fans, an additional extractor fan, via a set of dampers, could provide backup in the event of the failure of one of the other fans). The introduction of partial redundancy leads to a degraded operating mode which may require more or less substantial compensatory measures.

The drafting of an MOR for a non-compensatable equipment item must take account of the level of redundancy implemented:

- If there is a backup system that performs at the same level or almost the same level as the normal system, the MOR is relatively easy to define insofar as the equipment failure will lead to the activation of partial or total redundancy. If the initial failure persists and if the redundancy system malfunctions at the same time, then the tunnel must be closed.

- If the redundancy is partial, the MOR must be defined by taking account of the level at which the system is performing when the redundancy is activated.

Let's take the example of a longitudinal ventilation system consisting of several booster fans and designed to fight HGV fires. We define the minimum number of booster fans required to fight an HGV fire (Sp) and then define the minimum number required to fight a light vehicle fire (Sv). From this, we obtain two degraded operating modes and one closure situation:

• In the first mode, one or more booster fan(s) is/are faulty, but the number of functional booster fans is higher than Sp so the tunnel remains open to HGVs and light vehicles.

• In the second mode, one or more booster fan(s) is/are faulty, but the number of functional booster fans is higher than Sv and lower than Sp so the tunnel remains open to light vehicles only.

• The tunnel will be closed to all types of vehicle as soon as the number of functional booster fans falls below Sv.

Whenever possible, the preference is given to redundancy systems capable of being activated instantaneously and/or automatically. However, in certain circumstances, the implementation of redundancy could lead to an isolated closure of the tunnel.

Two important points need to be made concerning redundancy. The first point relates to the implementation conditions: joint modes must be avoided at all costs (e.g.: two separate data transmission networks supported by the same optic fibre cable). The second point has to do with maintenance. By its very nature, a redundancy system is rarely used. Regular functional tests and trials must therefore be scheduled to check that it is operating properly.

5.2 Development of MORs for compensatable resources

By its very nature, a compensatable equipment item does not need redundancy. Consequently, if it fails, there will need to be another way of performing the safety function that it performed across the entire tunnel or in just a part of it. This raises two questions: what was the equipment's function(s) and what equipment can take over this function in place of the one that has failed?

The table in Chapter 3 highlights five essential safety functions and eleven means of implementing them.

In some cases, both of the questions raised above are quite easy to answer, especially if just one of the equipment items is faulty (e.g.: the failure of a door-opening switch in a safety recess could be compensated for by permanently showing the images from a camera monitoring this recess on the screens in the Tunnel Control Centre). The correspondence between the five functions and eleven resources is useful in determining compensation means. This table can either be used to assess the contribution of a resource to the various safety functions, or to identify the resource(s) that is/are capable of performing a given safety function.

A given device (e.g.: cameras or emergency exits) are only "effective" within a geographically restricted area and are normally installed on a modular basis. Consequently, from a practical standpoint, this table should be used in relation to homogeneous sections of tunnel. For each basic tunnel section thus defined, this approach leads to a more simplified reasoning by applying the grid in Chapter 3. As in the previous chapter (dealing with non-compensatable equipment), various risk analysis methods can be used to lead this discussion. In practise, a basic section is often a portion of tunnel that is longer than 300 metres, shorter than 500 metres and includes one or more intermediate exits, with this portion being delimited by two emergency exits or by one end of the tunnel and an emergency exit.

For information, this approach has been applied by the DiRIF (the operator for tunnels on the national road network that are located within the Île-de-France region),which has adopted the principles set out above. This reflection led to the development of MORs for compensatable or non-compensatable resources.

6 Conclusion

This first step has enabled the major safety functions in a road tunnel to be clarified and set against the technical and human resources required to provide them with the purpose of establishing the contribution of each resource to achieving safety objectives and continuity of operations.

This document sets out five major functions for road tunnel safety:

- prevent incidents/accidents,
- detect,
- alert and inform,
- limit the consequences of the incident/accident,
- ensure a return to normal.

Means of prevention and protection are associated to these functions. These are both technical systems as well as human and organisational resources and can be broken down into eleven resources.

Not all the resources required to implement safety functions are of equal importance.

A matrix of the functions to be provided and the resources available has resulted in these resources being classified into two families. The first contains non-compensatable resources, the second resources compensatable by other systems. Usually, non-compensatable resources should be doubled up (be redundant) in order to ensure optimum tunnel safety and availability.

The approach adopted has led to MORs being specified for compensatable and non-compensatable resources.

At the end of the day the purpose of this matrix is to enable managers to identify the resources they must focus on in order to enable users to travel through the tunnel in safe, free-flowing and comfortable conditions.

Bibliography

[1] Centre d'Études des Tunnels, Guide to Road Tunnel Safety Documentation. Booklet 4: specific hazard investigations (SHI), 2003

[2] Centre d'Études des Tunnels, Guide to Road Tunnel Safety Documentation. Booklet 5: the Emergency Response Plan (ERP), 2006

Written by: *Jérémie BOSSU, Eric CHARLES, Didier LACROIX, Thierry MANUGUERRA, Jean-Claude MARTIN, Hélène MONGEOT, Marc TESSON and Christophe WILLMANN (CETU).*

Contact: *eeg.cetu@developpement-durable.gouv.fr*

Photo credits: CETU - Devised by: PEMACO - Printed by: VASSEL GRAPHIQUE

Centre d'Études des Tunnels
25, avenue François Mitterrand
Case no. 1
69674 BRON - FRANCE
Tel. 33 (0)4 72 14 34 00
Fax. 33 (0)4 72 14 34 30
cetu@developpement-durable.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Écologie du Développement durable et de l'Énergie

CETU

www.cetu.developpement-durable.gouv.fr