



---

# MODURBAN

EC Contract n°: TIP4-CT-2005-516380

---

---

## MODSYSTEM WP23 SUBPROJECT

### – DELIVERABLE REPORT –

---

Deliverable ID:	<b><i>D93</i></b>
Deliverable Title:	Conformity assessment, guidelines for functional and technical specifications
Responsible partner:	INRETS
Contributors:	University of Budapest, RATP, LUL, <i>etc.</i>

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



## Document Information

**Document Name:** Conformity assessment, guidelines for functional and technical specifications  
**Document ID:** D93  
**Revision:** V3.1  
**Revision Date:** 13/2/2009  
**Author:** Vincent BENARD, El Miloudi EL KOURSI  
**Security:** PUBLIC

## Approvals

	Name	Company	Date	Visa
<i>Technical Management Committee</i>	B. VON WULLERTSORFF G. POITRASSON-RIVIÈRE D. DIMMER G. LEGOFF L. LINDQVIST A.PRICE / U. HENNING M. NOCK JP RICHARD/D. COINEAU Y. AMSLER C. GOUTORBE	UNIFE ALSTOM THALES ANSALDO STS BOMBARDIER SIEMENS KNORR BREMSE RATP UITP ALMA	13/10/08	OK
<i>Coordinator</i>	B. VON WULLERSTORFF	UNIFE	13/02/09	OK
<i>Subproject Coordinator</i>	JP. RICHARD	RATP	13/02/09	OK
<i>Quality Manager</i>	B. VON WULLERSTORFF C. GOUTORBE	UNIFE ALMA	13/02/09	OK

## Documents history

Revision	Date	Modification	Author
Draft 1	9/6/2008	First version	Vincent Benard El Miloudi El Koursi
Draft 2	21/7/2008	Second Version	Vincent Benard El Miloudi El Koursi
Draft 3	2/10/2008	Final Version	Vincent Benard El Miloudi El Koursi
V3.1	13/2/2009	Final Version	Vincent Benard El Miloudi El Koursi



The scope of the document applies to:

Metro systems only	Metro and Light Rail		Light Rail only
	<i>With no differentiation</i>	<i>With specific adaptation(s)/recommendation(s) (1)</i>	
		<i>For metro</i>	

(1) – Put a [D] if these adaptations/recommendations are present in the document and a [L] if they will have to be detailed later.



## SECTION I – DELIVERABLE SUMMARY

### Conformity assessment, guidelines for functional and technical prescriptions

<b>Deliverable ID , associated WP &amp; Subproject</b>	<i>D93 MODSYSTEM / WP23</i>
<b>Type of Deliverable</b>	<i>Report</i>
<b>Input / Starting stage</b>	<i>D92 + D89 + UGTMS D10</i>
<b>Output / Final stage</b>	<i>Report D93</i>

<b>Lead partner(s)</b>	<b>INRETS</b>
<b>Achievement to date (%)</b>	-
<b>Expected date of achievement</b>	-
<b>Type of exploitation</b>	-
<b>Exploitation potential</b>	-
<b>Protection</b>	<i>No specific IPR protection foreseen</i>
<b>Protection date</b>	-

<b>IP's</b>	<b>Partners, (type, identification, date)</b>
<b>Pre-existing Know-How</b>	<i><u>D92</u>, D89, UGTMS experience</i>
<b>Exploitation Rights</b>	Not relevant

<b>Associated Risk analysis</b>	<b>Type, solution envisaged, action, actors</b>	<b>Actual Reduction</b>
<b>Before start</b>	Not relevant	
<b>During task implementation</b>	Not relevant	



**Conformity assessment, guidelines for functional and technical prescriptions**

**Deliverable Abstract**

*The development of urban guided transport has quickened in the European Union with the deployment of tramway networks in many cities, the extension or renewal of subway lines for large cities. This expansion has been accompanied by a strong involvement of the European Union in terms of resources and investments in research projects. In this context, the European authorities want to support strengthening and harmonizing rules applied to urban guided transport.*

*This document is intended to consolidate the reports D89 and D92. A first part is devoted to remind the main guidelines, major key players and documents in the certification of urban guided transport. The second part refers to the work performed in this project and concludes with a proposal for approval process.*

**Associated Milestone (if relevant):**

- 
- 

**Contribution to MODURBAN Objectives as mentioned in the Description of Work**

<b>Objective Definition</b>	<b>Comments</b>	<b>Quantification</b>
Objective 1 – To define existing safety principles	-	-
Objective 2 –To produce guidelines on how to use existing and new safety concepts.	-	-
Objective 3 ...To assess the safety of prescriptions for guided transport system	-	-

## CONTENTS

<b>1. Introduction: Problematic of safety certification for urban guided transport system .....</b>	<b>8</b>
<b>2. Glossary .....</b>	<b>10</b>
<b>2.1. Abbreviations.....</b>	<b>10</b>
<b>2.2. Definitions .....</b>	<b>11</b>
<b>3. Safety impact during the system life cycle .....</b>	<b>13</b>
<b>3.1. Rules and laws.....</b>	<b>13</b>
3.1.1 European Directives [1,2,3,4].....	13
3.1.2 European Standards [5,6,7] .....	16
3.1.3 National laws and Decrees .....	18
<b>3.2. Concepts and safety policies.....</b>	<b>18</b>
3.2.1. ALARP principle (As Low As Reasonably Practicable) .....	18
3.2.2. GAME Principle (Globalement Au Moins Equivalent) .....	20
3.2.3. Comparison between ALARPS and GAME Principles .....	21
<b>4. Approval processes for certification of urban guided transport systems.....</b>	<b>26</b>
<b>4.1. Approach by questionnaire.....</b>	<b>26</b>
<b>4.2. Relational matrix between various safety elements stemmed from the questionnaire.....</b>	<b>27</b>
4.2.1. Spain.....	28
4.2.2. Portugal.....	29
4.2.3. Czech Republic.....	30
4.2.4. Poland.....	31
4.2.5. Italy .....	32
4.2.6. Germany .....	33
4.2.7. France.....	34
4.2.8. The UK.....	35
<b>4.3. Extraction of common elements/ Proposal of a sketch for the safety approval .....</b>	<b>35</b>
<b>5. Conclusions and perspectives.....</b>	<b>38</b>
<b>6. References .....</b>	<b>38</b>

### Figures

Figure 1 - Illustration of the ALARP concept .....	19
Figure 2 - ALARP decision process .....	20
Figure 3 - GAME Decision process .....	21
Figure 4 - Content of the safety case .....	23
Figure 5 - Results about the questionnaire .....	27
Figure 6 - Relational Matrix .....	28
Figure 7 - Matrix for Spain.....	28
Figure 8 - Matrix for Portugal.....	29
Figure 9 - Matrix for Czech Republic.....	30
Figure 10 - Matrix for Poland.....	31
Figure 11 - Matrix for Italy .....	32
Figure 12 - Matrix for Germany .....	33
Figure 13 - Matrix for France.....	34
Figure 14 - Matrix for the UK.....	35
Figure 15 - Proposition of a generic approval process.....	37



**Tables**

Table 1 - Description of the European directives ..... 15  
Table 2 - Description of the main CENELEC Standards ..... 17  
Table 3 - Examples of decrees/laws used in different European countries..... 18  
Table 4 - Criteria used for each safety policy ..... 21  
Table 5 - Safety policies example ..... 22  
Table 6 - Examples of some notified bodies in Europe ..... 25  
Table 7 - Provided documents in approval process ..... 36

## SECTION 2 – DELIVERABLE DETAILED DESCRIPTION

### 1. Introduction: Problematic of safety certification for urban guided transport system

Today, public transport meet a tremendous success in many cities, probably linked to economic reasons and environmental issues. In addition to an increasing deployment in space and time, the transport facilities provided on a daily basis in urban and sub-urban areas must meet the quality of service requirements, particularly in terms of reliability, safety, comfort and durability. The introduction of innovative policies is now an imperative for the authorities in charge of urban public transport.

The European Union aims at increasingly promoting the use of public transport. However European legislation which applies to railway systems is making a clear distinction between the interoperable rail systems which are governed by the European (rail) directives and regulations, and rail systems which are excluded from the scope of this legislation. The interoperability directives 96/48/EC and 2001/16/EC amended by Directive 2004/50/EC exclude from their scope “functionally isolated systems”. The Safety Directive 2004/49/EC may cover all rail modes, including urban modes (metro, tram, etc.), but all Member States (except partially Portugal) have excluded urban guided systems when transposing the directive into their national legislation. Local transport aspects as a matter of subsidiarity are in the responsibility of local authorities. It is the duty of the national governments to consider the national and local specific features in the corresponding legislation. Subsidiarity is one of the fundamental principles of the European Union. The European legislation shall and will not take over the responsibility of national governments.

As a consequence of these principles, the new interoperability directive adopted by the Parliament on 11 December 2007, and by the Council on 14<sup>th</sup> May 2008, has a scope intended to be aligned to that of the Safety Directive, which shall lead again Member States to exclude urban guided systems when transposing the directive into their national legislation.

In addition, the new regulation on Public Service requirements (1370/2007/EC) clearly recognises the very large responsibility of national competent authorities as regard public transport services operated under public service contracts, which is the case for all urban guided systems (“In keeping with the principle of subsidiarity, competent authorities are free to establish social and qualitative criteria in order to maintain and raise quality standards for public service obligations, for instance with regard to minimal working conditions, passenger rights, the needs of persons with

reduced mobility, environmental protection, the security of passengers and employees as well as collective agreement obligations and other rules and agreements concerning workplaces and social protection at the place where the service is provided. In order to ensure transparent and comparable terms of competition between operators and to avert the risk of social dumping, competent authorities should be free to impose specific social and service quality standards.”)

As a consequence, the European legislation developed for the Trans-European railway networks cannot apply to urban guided systems.

There are currently no standardised procedures for the putting into service of urban guided transport at the European level, and such procedures most often differ even within a given country. It is not the responsibility of the European Union to change this situation. However, although there are no common standard procedures in Europe for the safety evaluation (each country applies their own safety conformity assessment), the recent applications are assessed more and more taking into account the European standards EN 50126/50128/50129.

Most urban guided transport stakeholders believe that the development of European (and even worldwide) standards should be encouraged, in order to facilitate the voluntary reference to such standards by relevant national authorities. The European Commission is favouring this approach, notably through its support to major European Research projects like UGTMS, MODURBAN, and soon MODSAFE.

This deliverable proposes firstly an overview of the certification process in regard to the safety. It complements and refers to the Deliverable D126 about the safety plan. The studies focus, in general, on the various aspects of certification used in the different member countries of the European community through:

- Laws and guidelines,
- Documents which should be given to safety authorities,
- Safety policies,
- Safety Key players in the certification process.

Then the approach by questionnaire is detailed and a proposition of a sketch of approval process from the elements of the questionnaire is made.

## 2. Glossary

### 2.1. Abbreviations

<b>ALARA</b>	As Low As Reasonably Achievable
<b>ALARP</b>	As Low As Reasonably Practicable (UK safety principle)
<b>AOT</b>	Autorité Organisatrice de Transports (Transport Organising Authority)
<b>BOStrab</b>	Straßenbahn Bau- und Betriebsordnung (Federal Regulation for Construction and Operation of Urban Guided Transport System)
<b>CENELEC</b>	Comité Européen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardisation)
<b>DDS</b>	Dossier de Définition de Sécurité (Safety Definition Case)
<b>DPS</b>	Dossier Préliminaire de Sécurité (Preliminary Safety Case)
<b>DREIF</b>	Direction Régionale de l'Équipement Ile de France (Regional Department of Equipment for Ile de France area)
<b>DS</b>	Dossier de Sécurité (Safety Case)
<b>EC</b>	European Community
<b>EN</b>	European Standard
<b>EOQA</b>	Experts ou Organismes Qualifiés Agréés (Independent Assessor Body accredited by the National Safety Authority)
<b>EU</b>	European Union
<b>GAME</b>	Globalement Au Moins Equivalent - Globally at least as good as the one offered by an existing system - French safety principle
<b>HMRI</b>	Her Majesty's Railway Inspectorate
<b>HSE</b>	Health and Safety Executive
<b>ISA</b>	Independent Safety Assessor
<b>LU</b>	London Underground
<b>PPP</b>	Public Private Partnership
<b>RAMS</b>	Reliability, availability, Maintainability and Safety
<b>RATP</b>	Régie Autonome des Transports Parisiens (Autonomous Paris Transport Authority)
<b>RSC</b>	Railway Safety Case
<b>RSPG</b>	Railway Safety Principles and Guidance
<b>SC</b>	Safety Case
<b>SIL</b>	Safety Integrity Level
<b>SMS</b>	Safety Management System
<b>STRMTG</b>	Service Technique des Remontées Mécaniques et des Transports Guidés (French Technical Agency for Ropeways and Guided Transports safety)
<b>TAB</b>	Technische Aufsichtsbehörde (Technical Supervisory Authority)
<b>UGTMS</b>	Urban Guided Transport Management System

## 2.2. Definitions

<b>Assessment</b>	The undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product (EN 50126).
<b>Authorisation/Approval</b>	The Formal permission to use a product within specified application constraints (EN 50129).
<b>Availability</b>	The proportion of time that an item is capable of operating to specification within a large time interval.
<b>Competent Authority</b>	Person or organization that has the legally delegated or invested authority, capacity, or power to perform a designated function.
<b>Interoperability</b>	Interoperability refers to the ability of a transport network to operate trains, and infrastructures to provide, accept and use services so exchanged without any substantial change in functionality or performance. This ability rests on all the regulatory, technical and operational conditions which must be met in order to satisfy all the defined requirements applicable to the given grade of automation, irrespective of which supplier provides which components or systems.
<b>Local Safety Assessor</b>	Independent safety assessor accredited by local safety authorities
<b>Maintainability</b>	The probability that a failed item will be restored to operational effectiveness within a given period of time when the repair action is performed in accordance with prescribed procedure.
<b>Notified bodies</b>	The bodies which are responsible for assessing the conformity or suitability for use of the interoperability constituents or for appraising the EC procedures for verification of the sub system (96/48/EC).
<b>Regulation</b>	Document providing binding legislative rules that is adopted by an authority (EN 45020).
<b>Reliability</b>	The probability that an item can perform a required function under given conditions for a given time interval.
<b>Risk</b>	The rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm. (EN 50126-2).
<b>Safety</b>	Freedom from unacceptable level of risks of harm (EN 50129).
<b>Safety approval</b>	The safety status given to a product by the requisite authority when a product has fulfilled a set of predetermined conditions (EN 50129).



<b>Safety assessment</b>	The process of analysis to determine whether a product meets the specified safety requirements and to form a judgement as to whether the product is safe for its intended purpose.
<b>Safety authority</b>	The body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements (EN 50129).
<b>Safety case</b>	The document demonstration that the product complies with the specified safety requirements (EN 50126, EN 50129).
<b>Sub-system</b>	A combination of equipment, units, assemblies, etc..., which performs an operational function and is a major subdivision of the system.
<b>System</b>	A composite of equipment, skills and techniques capable of performing or supporting an operational role, or both. A complete system includes all equipment, related facilities, material, software, services and personnel required for its operation and support to the degree that it can be considered a self-sufficient unit in its intended operational environment.

### 3. Safety impact during the system life cycle

The certification is an activity whereby a notified body, independent of the involved entities, gives a written assurance that a product, process or service conforms to specified requirements. The safety certification rests on European or national directives, which are part of the safety plan. The operating license of an urban guided system becomes effective after the approval of documents by the safety key players involved in the process.

This clause describes mainly the European legislation on safety aspects for railways and the consequences. National and local governments have the responsibility for Urban Guided Transport Systems. Because of the subsidiarity principle urban guided transport is (without on special example in Portugal) excluded directly or by the national legislation in the process of transposition of the European directives. That means that all aspects of urban guided transport systems including safety fall under the Member States responsibility at the national or regional level. Any kind of European harmonisation has to be supported and accepted following a bottom-up approach where proposals for harmonisation are agreed by operators and manufacturers (especially through the common UITP-UNIFE Urban Rail Platform) and accepted by relevant authorities within Member States.

The following points remind the definition or detail all elements related to the safety in the approval process.

#### 3.1. Rules and laws

##### 3.1.1 European Directives [1,2,3,4]

EU directives and regulation which have been adopted or are still under negotiation have been developed in order to facilitate the operation of freight and passenger trains throughout Europe, and to improve the development of new or more efficient services thanks to the opening of the international – and to some extent the domestic - rail market. For this rail traffic mostly ruled by commercial competition, a strong European Community action was required in order to overcome the numerous obstacles created by national barriers of all kind.

Some of these directives and regulations also address urban guided transport:

- Directives 2001/13/EC and 2001/14/EC, the latter being amended by the Safety Directive 2004/49/EC and soon by a new version of the Safety Directive, allow for the exclusion of urban guided transport by Member States. All Member States but – partially- Portugal have excluded urban guided transport in the national transposition of the directives.

- Directives 2001/16/EC and 2004/50/EC automatically excluded urban guided transit from their scope. They shall be repealed by a new Interoperability Directive adopted by the European Parliament on 11<sup>th</sup> December 2007, and by the Council on 14<sup>th</sup> May 2008. This Directive is expected to be published very soon in the Official Journal of the European Union.
- The Regulation 1370/2007/EC on Public Service Requirements has a wider scope than urban guided transport. It also includes other rail systems and other public transport services, provided that they follow public service requirements. This Regulation shall repeal Regulations 1191/69/EEC and 1107/70/EEC when entering into force in 2012. As mentioned earlier, it acknowledges the responsibility of [national or regional] competent authorities in the definition of services operated under public service contracts, which shall be the case for all urban guided transport services, in application of the subsidiarity principle.
- Last but not least, Directives 2004/17/EC and 2004/18/EC set up the rules to be applied to procurement procedures. The first one coordinates the procurement procedures of entities operating in the water, energy, transport and postal services sectors, repeals Directive 93/38/EC, and has been modified by the Regulation 1422/2007/EC. The last one regulates the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, repeals Directives 92/50/EEC (except Article 41), 93/36/EEC and 93/37/EEC, and has been modified by Regulation 1422/2007/EC. They notably clarify the use of standards.

The different European directives are described in the Table 1.

**Table 1 - Description of the European directives**

Directives	Description
<b>91/440/EEC</b>	<p>It is dedicated to the single European market for rail operation. One of its articles lists the stakeholder Organisations with the key actors and their responsibilities. An example is the <i>separation</i> between the Infrastructure owner and the Operator. (In France, the Infrastructure owner is RFF –Réseaux Ferrés de France and the main operator is SNCF – Société Nationale des Chemins de fer Français).</p> <p>Furthermore, this directive gives an introduction to CENELEC to draw up, since mid- 1990s, the safety standards dedicated to railway (the EN 50 126, 28, 29)</p>
<b>2004/49/EC</b>	<p>It is dedicated to guide the progressive setting-up of a single EU railway market. To this scope and for harmonising differences between safety requirements in EU states, it became a necessity to build a common regulatory framework for rail safety. This safety directive is designed to facilitate :</p> <ul style="list-style-type: none"> <li>• Horizontal integration, i.e. interoperability of the networks facilitating smooth movement of passenger and freight trains,</li> <li>• Vertical separation, e.g. between management of infrastructure and train operation and outsourcing of maintenance and support functions,</li> <li>• A due and transparent certification process to improve safety approval and equipment acceptance.</li> </ul>
<b>2008/57/EC Directive</b>	<p>It is related to the <i>Interoperability for Railway system</i></p> <p>Both directives 96/48 and 2001/16 have been superseded by the directive 2004/50/EC. This last directive has been itself revised on 14 May 2008 with the Directive 2008/57/EC in order to simplify and to bring together the rules in a single text.</p> <p>This directive provides for an optional exclusion of urban guided transport (metros, trams and other light rail systems).</p>

In this context, the European Commission began to develop several railway initiatives in order to harmonise the railway in Europe with interoperability and market opening as goals. These goals cannot be achieved without setting out high common safety standard. This European Safety Directive aims at harmonising the regulatory structure that enforces railway operation to ensure the development and improvement of safety on the Community's railway by:

- Maintaining the global railway safety in each Member State,
- Harmonising the regulatory structure in the Member State,
- Defining responsibilities between the actors,
- Developing common safety methods, safety indicators, safety targets,
- Requiring the establishment in every Member State of national safety authorities and national bodies for accident investigation,
- Defining common principles for the management, regulation and supervision of railway safety.

This directive describes the actors involved in the management of railway safety, including:

- the European Infrastructure Managers,
- the European Railway undertakings,
- the Railway Safety Authorities of European Member States,
- the Investigating Bodies of European Member States,
- the European Members States,
- the European Railway Agency,
- the European Commission.

### **3.1.2 European Standards [5,6,7]**

A standard is a reference document that provides answers to technical questions that have key players about products, or services. It is developed by consensus. A standard has a voluntary and contractual application. In fields related to safety, it is often made compulsory by relevant authorities.

The CENELEC (European Committee for Electrotechnical Standardisation) European Standards have been developed to define requirements for the acceptance of safety-related numerical control and protection systems in the railway field.

These CENELEC standards have been published and are updated or completed in line with the European Railway Directives and Regulations. These safety standards are notably used in the certification processes in the field of interoperable railway (on the administrative side of the certification and authorization bodies (notified bodies) and cross acceptance rules throughout Europe.

Table 2 summarizes the main CENELEC Standards concerning safety in railway field.

**Table 2 - Description of the main CENELEC Standards**

<b>Standard</b>	<b>Description</b>
<b>EN 50126</b>	<p>The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS). This standard defines a management process ensuring the development and the demonstration of the system' RAMS aspects. It is based on a life cycle approach to safety requirements derivation and allocation.</p> <p>The application of this standard should be adapted to specific requirement of the system considered. To apply this standard to the system being considered, it is necessary to :</p> <ul style="list-style-type: none"> <li>• Specify and justify the phases,</li> <li>• Specify the obligatory activities and the requirement of each phase.</li> </ul> <p>Sometimes, it is difficult for the assessors to understand and apply this standard. One of the major difficulties is the interpretation of the different life cycle phases of the RAMS, e.g. for one product, there is a common agreement between the assessment body and the industrial and the phases (concept, system definition, risk analysis) are global system phases and the activities of certification could not start before the phase 4 "system requirements".</p> <p>A second important difficulty is in the indisputable vagueness around the SIL notion.</p>
<b>EN 50128</b>	<p>Software for railway control and protection systems.</p> <p>This European standard specifies the procedures and technical requirements applicable to the development of programmable electronic systems used in command and railways protection applications. It is aimed to be used in all domains involving safety implications. These applications may range from the very critical, such as safety signalling, to the non critical such as management information systems. These systems can be implemented with dedicated microprocessors, programmable logical controllers, distributed multiprocessors systems, big systems equipped with a central computer or with other architectures.</p>
<b>EN 50129</b>	<p>Safety related electronic systems for signalling. This last standard is applicable to safety-related electronic systems (including sub-systems and equipment) for railway signalling applications. All safety-related components of a system produced in different countries by different railway industries have to be strictly compliant with the same safety requirements given by the European Standard. The target of European Interoperability Railway Community is to develop compatible railway systems and sub-systems based on common standards. All these evidences shall be included in the Safety Case, the masterpiece of an authorisation process.</p>

The standards EN 50126, 50128, and 50129 are currently under maintenance at CENELEC level and are subject to evolve in a few months.

### 3.1.3 National laws and Decrees

With the construction of Europe, national regulations had to adapt to the European centralization. Decrees have been added to the national legislation to transpose EU directives about safety. Table 3 presents some laws and decrees used in European countries.

**Table 3 - Examples of decrees/laws used in different European countries**

Country	Decrets/Laws
Czech Republic	Act on Rail system N° 266/1994 Coll.
Denmark	Bekendtgørelse af lov om jernbane, LBK 1171 af 02/12/2004
France	Decree 730 (22 March 1942) Law LOTI 82-1153 (30 December 1982) Decree 21 (February 2000) Law SIST 3 (4 January 2002)
Germany	Basic Law (Grundgesetz) Passenger Transport Act - PBefG (2001) Federal Regulation for construction and operation of Light Rail BOStrab 1987 (updated in 2000)
Italy	Minister Decree 138/T DLgs 188/2003
Poland	Railway transport Act (28 March 2003)
Sweden	The Railway act, 2004:519 Railway Ordinance, 2004:526 Instruction Ordinance, BV-FS 1996:2, Regulations on applications for certificate and license Instruction Ordinance, BV-FS 1996:1, Regulations on Internal Control (SMS)
United Kingdoms	Transport & works Act 1992 Construction (Design & Management) regulations 1995 Railways (Safety Critical Work) Regulations 1994 Railways (Safety Case) Regulations 2000 (Revised in 2003 and 2005)

If the objectives of European directives are explained, means and methods to achieve them are different according to rules in each country.

### 3.2. Concepts and safety policies

In this part, it is explained what are the most useful safety concepts (ALARP and GAME principles)

#### 3.2.1. ALARP principle (As Low As Reasonably Practicable)

This principle illustrated in Figure 1 is the same principle as ALARA (As Low As Reasonably Attainable/Achievable) which is used in the nuclear field [1]. It includes a zone of risk acceptance, a zone of risk rejection, and an intermediate zone, named ALARP zone, in which the overall goals are set according to the ratio of improved risk on the investment costs. This area can be defined by frequencies contained in Figure 1. If the analyzed risk is in this area, the means to implement in order to achieve the desired level of safety must be evaluated and so the obtained risk reduction. Indeed,

there is no need to use huge resources (financial, human, material) for a small improvement.

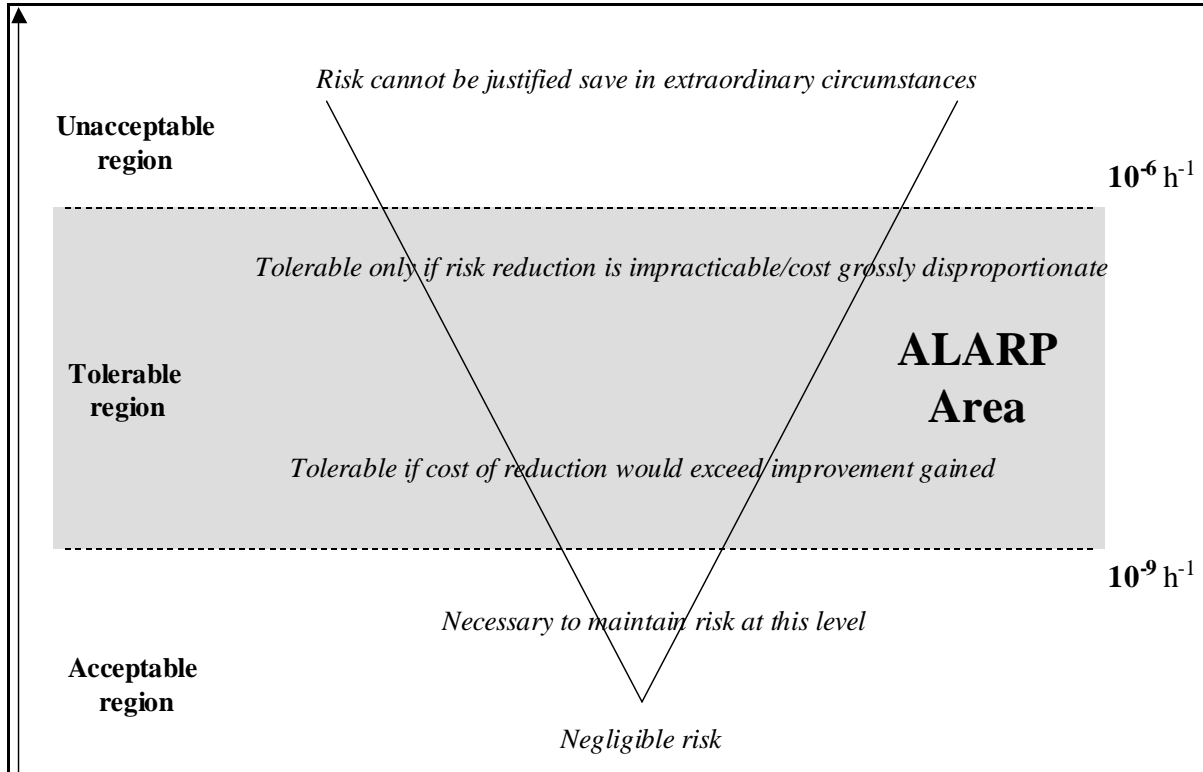


Figure 1 - Illustration of the ALARP concept

At each step of the system design, the ALARP concept must be justified. The Figure 2 illustrates the ALARP decision process.

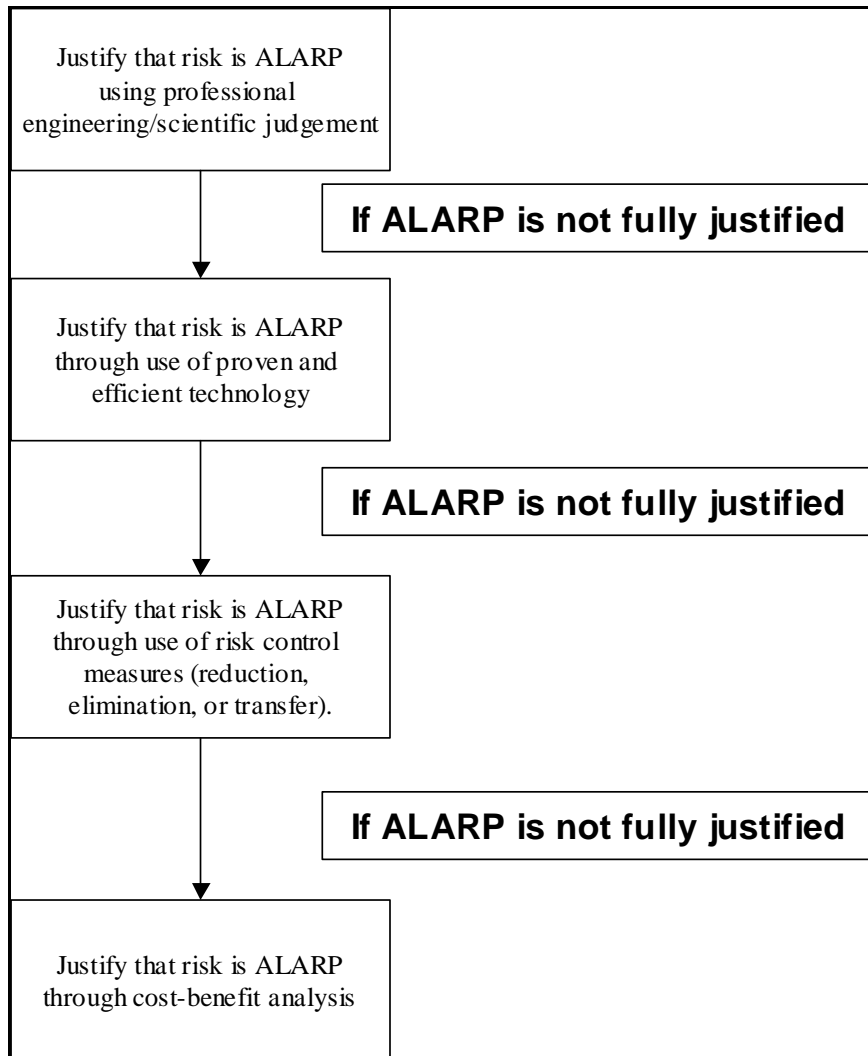


Figure 2 - ALARP decision process

### 3.2.2. GAME Principle (Globalement Au Moins Equivalent)

The GAME French principle is a concept introduced by Decree 2003-425 of 9 May 2003 on the safety of public guided transport:

*“Any new public guided transport system, or any modification on an existing system, is designed and done so that the overall safety level in respect of users, operating staff and third parties is at least equivalent to existing safety level or to the safety level of existing systems providing comparable services”*

This principle aims to provide to the new system the same safety requirements as an equivalent existing system. This principle requires knowing of course the safety objectives and the behaviour of the safe referent system. The application of the GAME principle has recently evolved. It rests first on the regulatory and technical referential and just after on the use of a reference system. The Figure 3 shows the use of the GAME principle in a safety study.

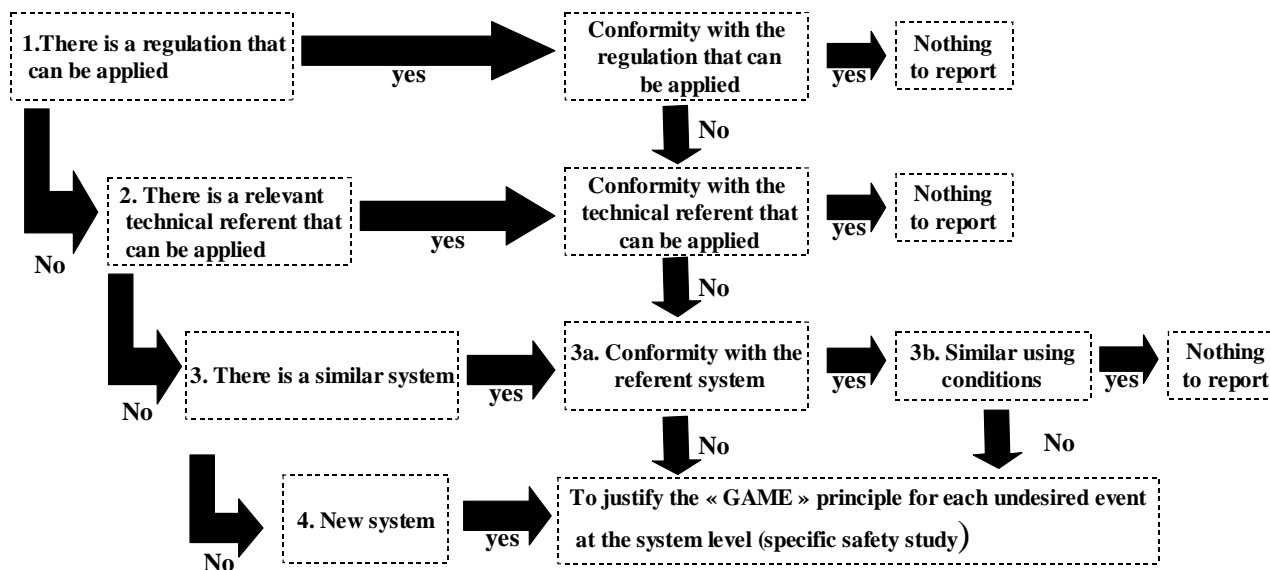


Figure 3 - GAME Decision process

### 3.2.3. Comparison between ALARPS and GAME Principles

To most Southern European countries, the concept of ALARP is not accepted. The different criteria of the Table 4 have probably an impact about the acceptance of the ALARP safety policy.

Table 4 - Criteria used for each safety policy

Criteria	ALARP	GAME
Reference system	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Statistics and probability	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Consideration of costs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Value on "a life"	<input checked="" type="checkbox"/>	<input type="checkbox"/>

By applying ALARP for each component of the system, and applying it at the time of commissioning, the overall effect is to add much more delay, cost and uncertainty

than would result from a GAME approach applied at the overall system level and mainly at the design stage.

ALARP is more appropriate for improving safety performance that is near the intolerable level, but GAME is more appropriate where the risk is at least in the middle of the tolerable range.

Table 5 shows the safety policy of several European countries.

**Table 5 - Safety policies example**

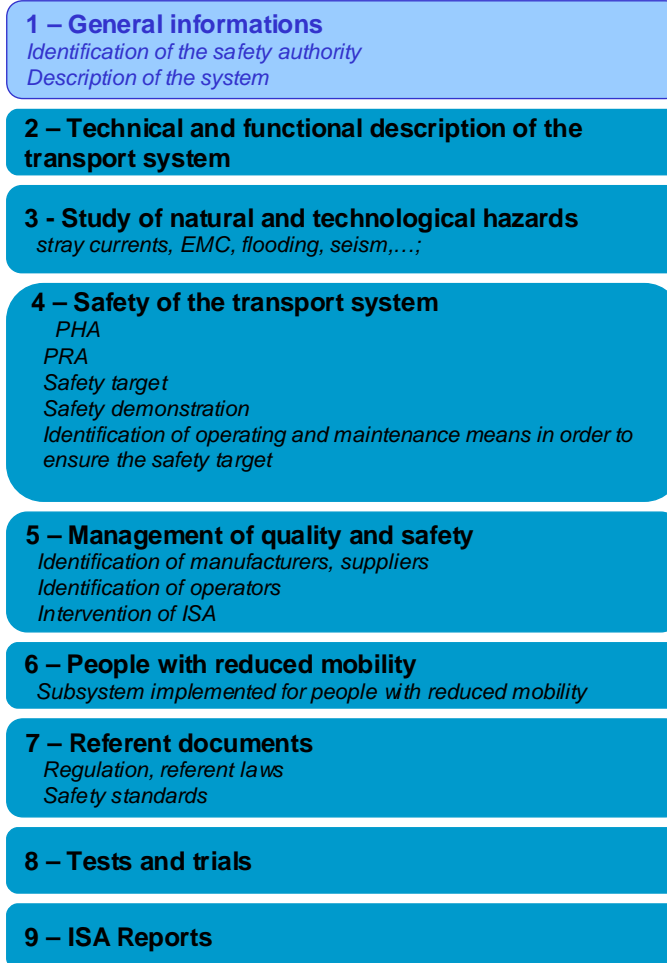
Country	Safety principle
Czech Republic	no safety policy
France	GAME
Germany	GAME
Ireland	ALARP
Poland	no safety policy
Sweden	GAME
United Kingdoms	ALARP

### **Safety Case**

The safety case is the most important safety document that operators, manufacturers must provide to safety authority in order to put into service a new system. It is a referent documented demonstration provided by the manufacturers on the management of safety and is based around a description of its safety management system. The safety case also includes a description of the company's operations and details of a systematic risk assessment, including results and analysis of actual accident statistics.

The Safety Case sets out the adequacy of the system's safety management system by specifying prevention measures as well as strategies for reducing the effects of a major incident if one does occur. It can only be prepared following a full examination of a site's activities to identify hazards and all potential major incidents, and to determine the necessary control measures (see Figure 4).

## New system



**Figure 4 - Content of the safety case**

If the purpose of the safety case is well defined, the demonstration of safety targets is left to the manufacturer who often has to call an expert to check that the system meets the safety requirements. However, there are structures in each country guiding the manufacturer or the editor of the safety case to provide a uniform document to the system owner.

### **Safety Key players**

#### **Notified Body**

A notified body is a certification organisation which the national authority (the competent authority) of a member state designates to carry out one or more of the conformity assessment procedures. A notified body must be qualified to perform all

the functions set out in any annex for which it is designated. The designation may be restricted to specified type of devices and/or Annexes.

A competent authority may designate as a notified body only organisations that come under its own jurisdiction. The competent Authority notifies those bodies it selects as being suitable to the European commission

The selection criteria are designed to ensure impartiality and expertise of prospective Notified Bodies. After a notified body is appointed the Competent Authority periodically audits it to ensure the expected criteria are still being met. Notified Body status may be withdrawn if these criteria are no longer met.

A notified body's tasks will vary depending on the classification of the products concerned and the conformity assessment route a manufacturer has chosen within the framework of the directives (does not apply to urban guided transit).

Typical activities that can be undertaken by a notified body include:

- Full quality assurance (the Notified Body will carry out an assessment of the manufacturer's quality system, including design. They will sample across the range of products and processes to ensure that the requirements are being to met).
- Examination of the design (the notified Body will assess the full design relating to each type of product to ensure that they meet the requirements).
- Type examination (the Notified Body will assess the full technical information relating to each type of product and carry out appropriate testing of a representative sample of production to ensure that it meets the requirements).
- Verification (the Notified Body will either test every unit or every batch of product to ensure that they are meeting the requirements before the manufacturer can place them onto the market).
- Production and Product Quality Assurance (the Notified body will carry out an assessment of either the manufacturer's quality system covering production and inspection or final inspection. They will sample across the range of products to ensure that relevant technical files are available as well as ensuring that the relevant processes being undertaken meet the requirements).

**Table 6 - Examples of some notified bodies in Europe**

Notified Body	Country
TUV Industrie Service GMBH	Germany
Asociacion Española de normalizacion y certificacion	Spain
TUV Österreich	Austria
Electrical Inspection FIMTEKNO OY	Finland
Strojirensky Zkusebnni Ustav S.P.	Czech republic
TUV CZ RSO	Czech republic
Dipl-ing Hubert schupfer Zivilingenieur für wirtschaftsingenieurwesen im Maschinenbau Sachverständiger für	Austria
OQS - Zertifizierungs - und Begutachtungs GMBH	Austria
TUV Slovakia S.R.O	Slovakia
Technicka Inspekcia	Slovakia
Skusobna ocel'ovych lan	Slovakia
VYSKUMNY USTAV DOPRAVNY AS	Slovakia
WPK	Austria
TRANSPORTOWI DOZOR TECHNICZNY	Poland
2XM ZERTIFIZIERUNGS GMBH	Austria
CERTRA S.R.L.	Italy

### **Independent safety assessor (ISA):**

The Independent Safety Assessor role (known as “functional safety assessment”) is part of IEC 61508 (IEC 1998). The ISA also has an important role in the railway sector, where best practice as detailed in the Yellow Book (Railtrack 2000, RSSB 2003) recommends that Independent Safety Assessment is conducted with a level of rigour and independence that is related to the degree of safety criticality of the change. Use of an ISA is not mandatory, except in France (see 4.2.7) but automotive manufacturers see it as protection.

The various safety standards and guidelines devote a considerable amount of space to whether the ISA should be from a separate department, separate organisation, etc., in order to be sufficiently independent. Formal requirements for independence based on Safety Integrity Level (SIL) are provided in IEC 61508 (IEC 1998) and the Yellow Book (Railtrack 2000) requires that the ISA is from an independent company, or is at least managerially independent up to board level.

However, the key consideration is that the ISA needs to be able to provide an expert, professional opinion without vulnerability to commercial, project or other pressure. Informally, this means that the ISA needs to be sufficiently independent so they are sheltered as far as possible from pressure to modify their opinion, and so that their career prospects are enhanced rather than damaged by carrying out a searching assessment.

The organisation that contracts the ISA must respect this independence. They should give the ISA substantial freedom to conduct the safety audit as the ISA judges to be appropriate.

## **National Safety authority**

In application of European railway legislation, which does not apply to urban guided transit, each Member State must establish a safety authority which is independent from manufacturers, infrastructure managers, operators, applicants for certificates and procurement entities. It may be any individual or collective entity, public or private, with power to decide on safety. It will respond promptly to requests and applications, communicate its requests for information without delay and adopt all its decisions within four months after all requested information has been provided.

The safety authority will carry out all inspections and investigations that are needed for the accomplishment of its tasks and be granted access to all relevant documents and to premises, installations and equipment of infrastructure managers and manufacturers.

Generally, the State is the decision-making authority concerning the safety.

## **4. Approval processes for certification of urban guided transport systems**

### **4.1. Approach by questionnaire**

In the approval process of a urban guided system, all the key players are concerned (suppliers, manufacturers, operators and obviously the authorities in charge of safety). Each of these key players can perceive differently regulations, including those related to safety. The approach is to understand the approval process for each country by analyzing the experience of each of the actors involved in this process.

For this, a questionnaire, based on a study led by an English firm about the state of the art of approval process in the rail environment, has been devised [8]. This questionnaire is divided into 3 parts. Each part seeks to get the process initiated by each key player for the design phase and the phase of putting into service.

The questionnaire whose characteristics are described in the deliverables D89 and D92 was sent as a priority to the project partners and various operators, manufacturers or safety entities of European countries.

The responses cover the approval process for 10 European countries. Among these responses, there are: 9 operators, 4 manufacturers, 7 safety entities.

Figure 5 summarizes the type of responses received.

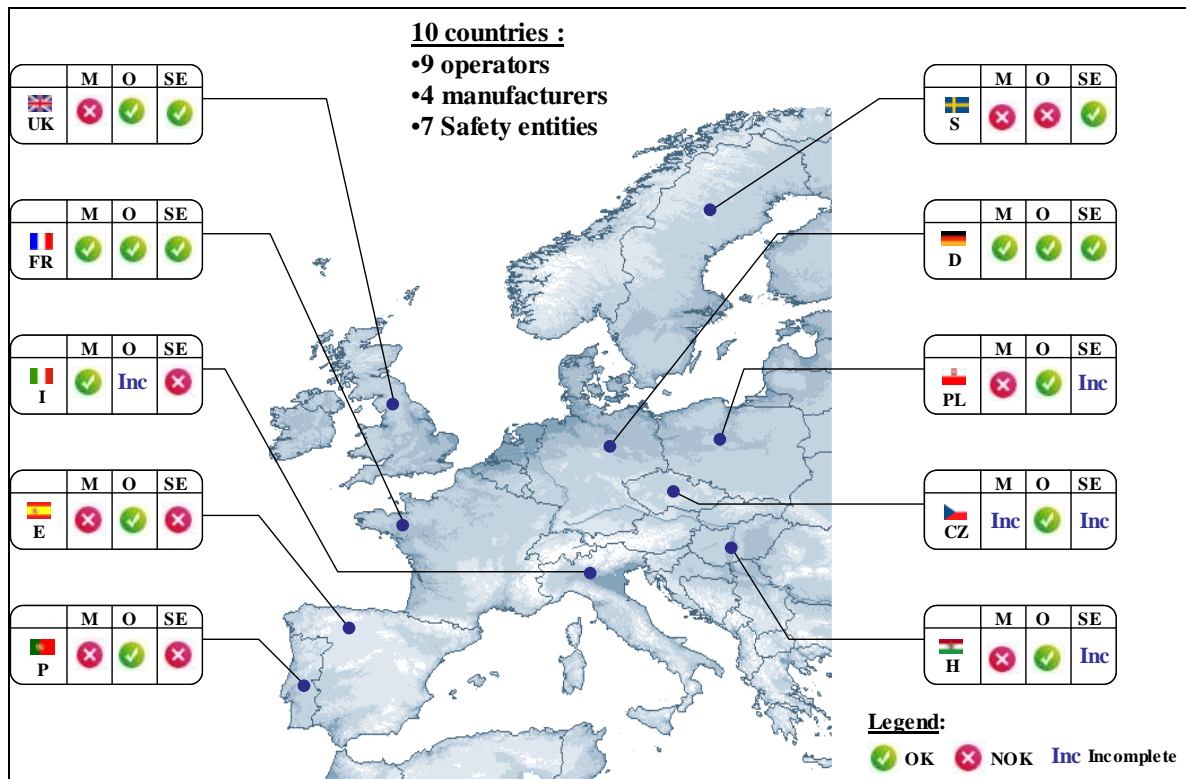


Figure 5 - Results about the questionnaire

#### 4.2. Relational matrix between various safety elements stemmed from the questionnaire

The objective of the questionnaire is to establish a state of the art for approval processes in Europe in order to determine the essential elements to consider in a scheme of a certification harmonized process. Each process is associated a two-dimensional matrix (life cycle focused on the design and putting into service and key players). All items concerning the certification process (relations, documents, etc.) are embedded in the matrix (see Figure 6).

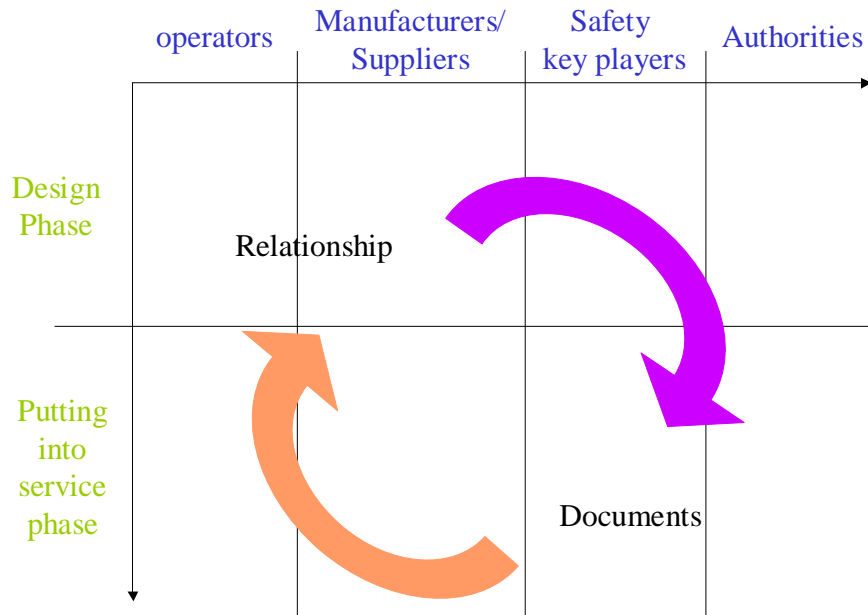


Figure 6 - Relational Matrix

The matrices for some European countries are shown in the following subclauses.

4.2.1. Spain

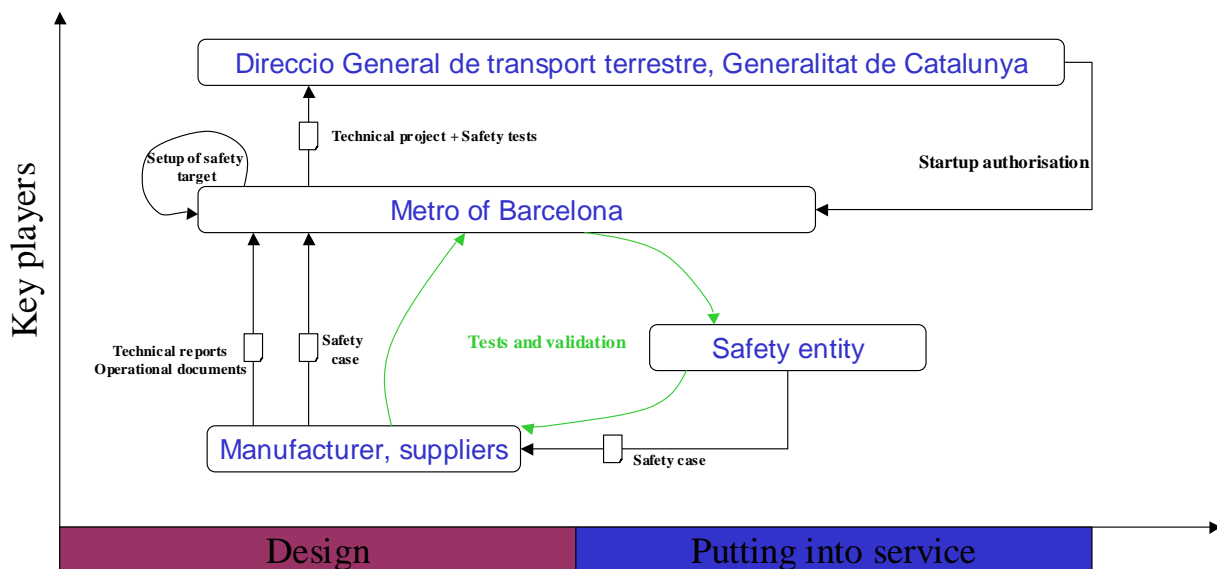


Figure 7 - Matrix for Spain

The operator sets itself the safety targets. It provides to the different manufacturers of the future system the technical and operational documents. It waits in return the

safety case that the manufacturer has written either by itself or with a safety entity. All technical documents and other documents inherent to the safety like the safety case are transmitted by the operator to the safety authority (“Direccio General de Transport Terrestre, Generalitat de Catalunya” in the case of Barcelona Metropolitan and “Consortio de Transportes de Madrid” in the case of Madrid Metropolitan). During the commissioning phase, operator, manufacturer and safety entity get on together in order to test, check and validate the system in accordance to the documents and procedures. Then the authority delivers the user licence of the new material.

#### 4.2.2. Portugal

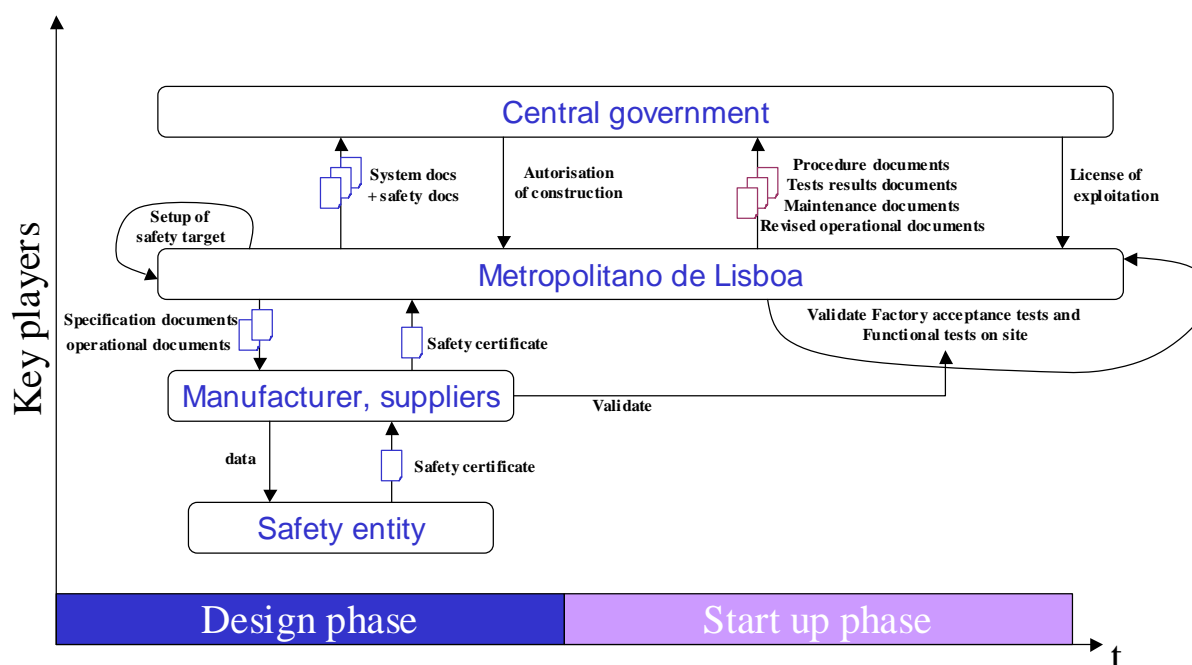


Figure 8 - Matrix for Portugal

During the design phase, the operator provides to manufacturers and suppliers all data concerning specifications and operational documents. These last ones can resort to a safety entity in order to establish the safety case. Once the operator has received the safety case, it transmits it to the central government which is the authority referent as regards safety. From this time, the central government can, according the documents provided by the operator, allow the construction of the new or renewed system. During the commissioning phase, the operator must validate in collaboration with the manufacturer factory acceptance tests and functional tests on site. Then, it delivers the following documents to the central government in order to obtain the license of exploitation: Procedure documents, Test results documents, Maintenance documents, Revised operational documents.

### 4.2.3. Czech Republic

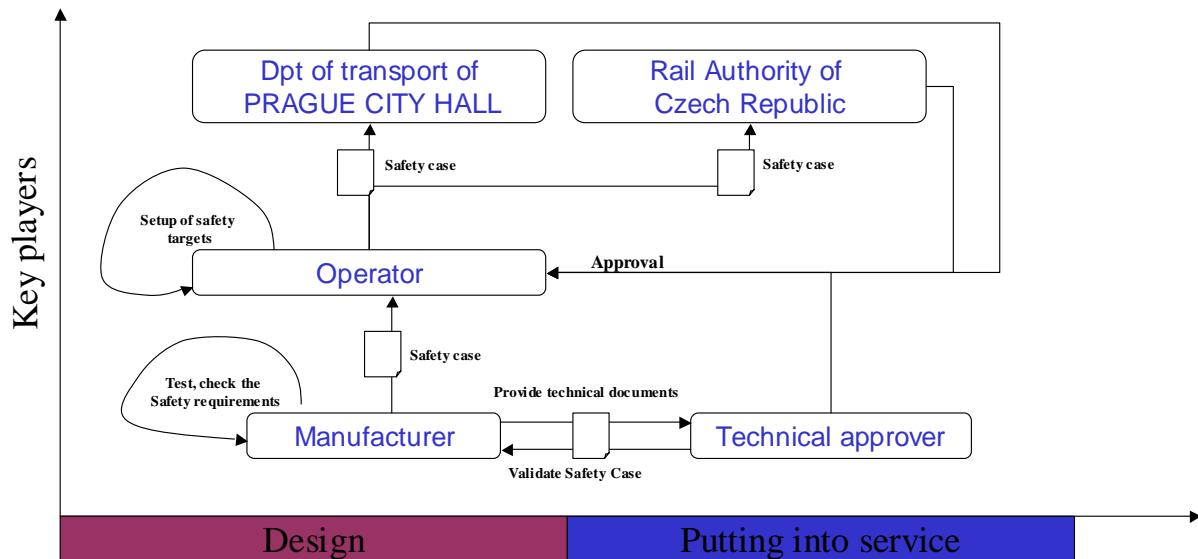


Figure 9 - Matrix for Czech Republic

The operator sets up the safety targets for the putting in service of a new system. As specified by the Figure 9, the chosen manufacturer must provide to the operator a complete safety case that may be designed or checked by an external technical approver. This final document is transmitted by the operator to the transport authority (in the case of Metro of Prague, the authorities are both Dpt of transport of PRAGUE CITY HALL and the Rail Authority of Czech Republic). During the commissioning phase, all tests (static and dynamic) are achieved by night or by simulation in all possible operational situations. The system is at end certified for the putting into service by the technical approver and next by the Special building Department of The Transport Section of PRAGUE CITY HALL and the Rail Authority.

#### 4.2.4. Poland

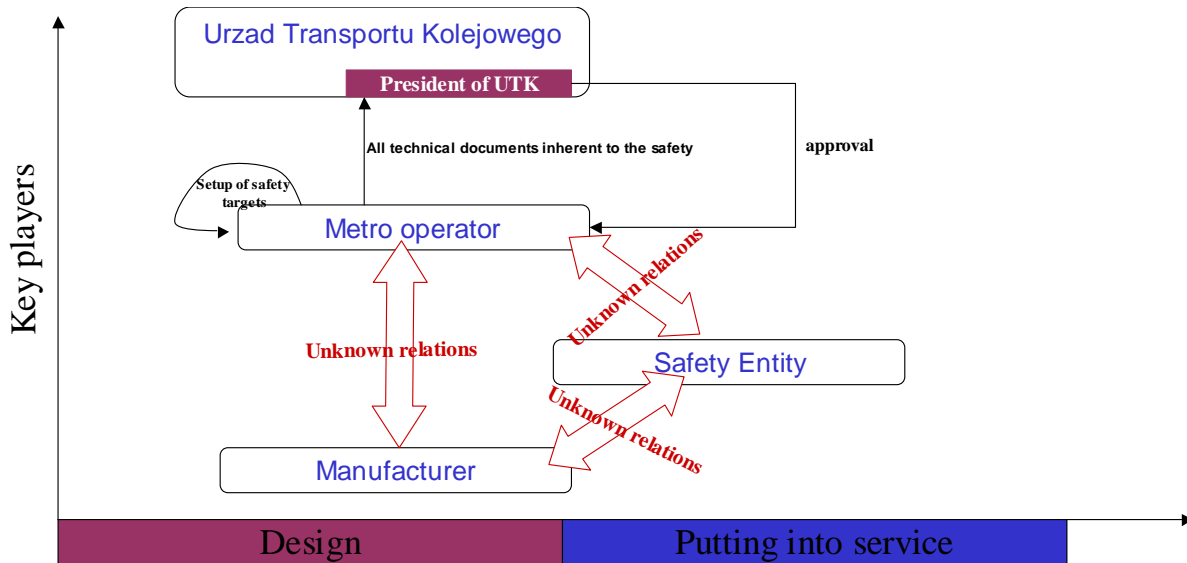


Figure 10 - Matrix for Poland

During the design phase, the operator records the safety targets of the system in a document called “Technical instructions for designing”. All data included in this document rest on the Railway Transport Act of 28 March 2003 and a few ordinances of the Minister of Transport and Minister of Infrastructure. These documents are then transmitted to “Urząd Transportu Kolejowego” that allows the construction of the system. During the Commissioning phase, the operator must provide to the safety authority the following documents for the setting into service of the new material: Licences for exploitation of a type of buildings or type of installations designed for railway traffic operation and licences for exploitation of a type, a statement about the technical efficiency certificates for the exploited railway vehicles, a list of internal regulations specifying rules and requirements concerning safe railway traffic operation and railway infrastructure maintenance, a statement confirming that the jobs linked to the railway traffic operation and safety are filled with employees meeting the conditions specified in regulations issued under Article 22 of Railway Transport Act.

### 4.2.5. Italy

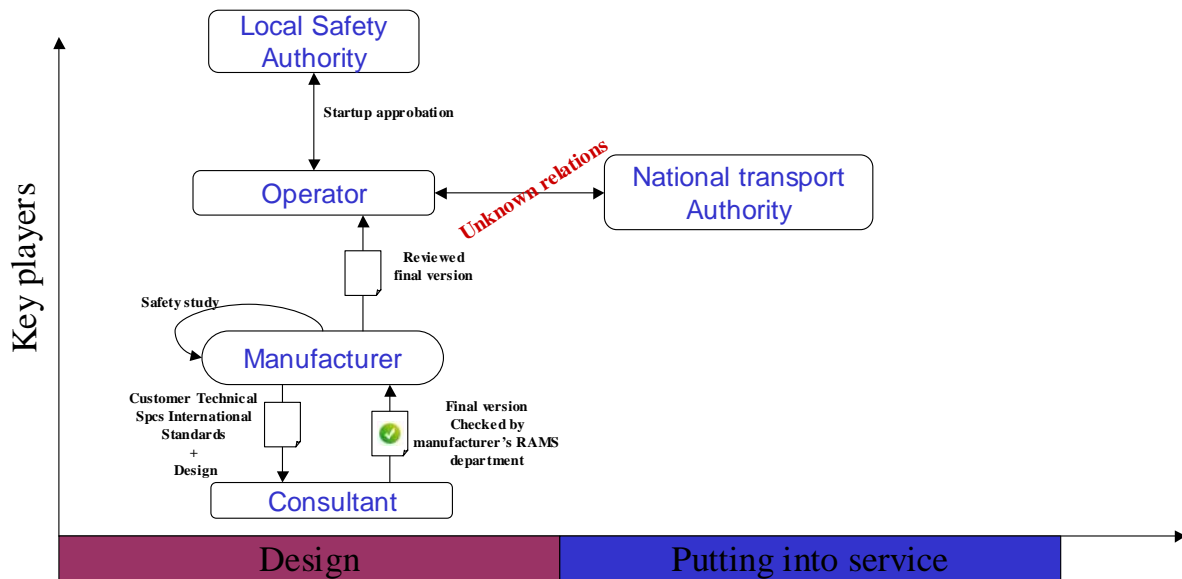


Figure 11 - Matrix for Italy

When a manufacturer needs to define a new guided transport system, it must provide a document called Customer Technical Specs. International standards. It can carry out itself the safety study or delegate to an external consultant chosen by his RAMS department. This safety study must include both qualitative and quantitative evaluations by preliminary hazard identification list, subsystem and system hazard analysis, interface hazard analysis, operating and support hazard analysis, Failures Modes Effects an Critically Analysis, fault tree analysis. The responsibility of this study is incumbent on the manufacturer itself, the consultant activity being constantly monitored by the manufacturer's RAMS department. After having checked the safety abilities of the system, the manufacturer must provide the safety study to the operator or to other entities when requested. To have the approval for the start-up of the project, the operator must have the authorisation of the local safety authorities. Relations between safety entities and applicant (manufacturers or operators) are not well known, the legislation about safety of transportation systems being in Italy a priori in process of development.

#### 4.2.6. Germany

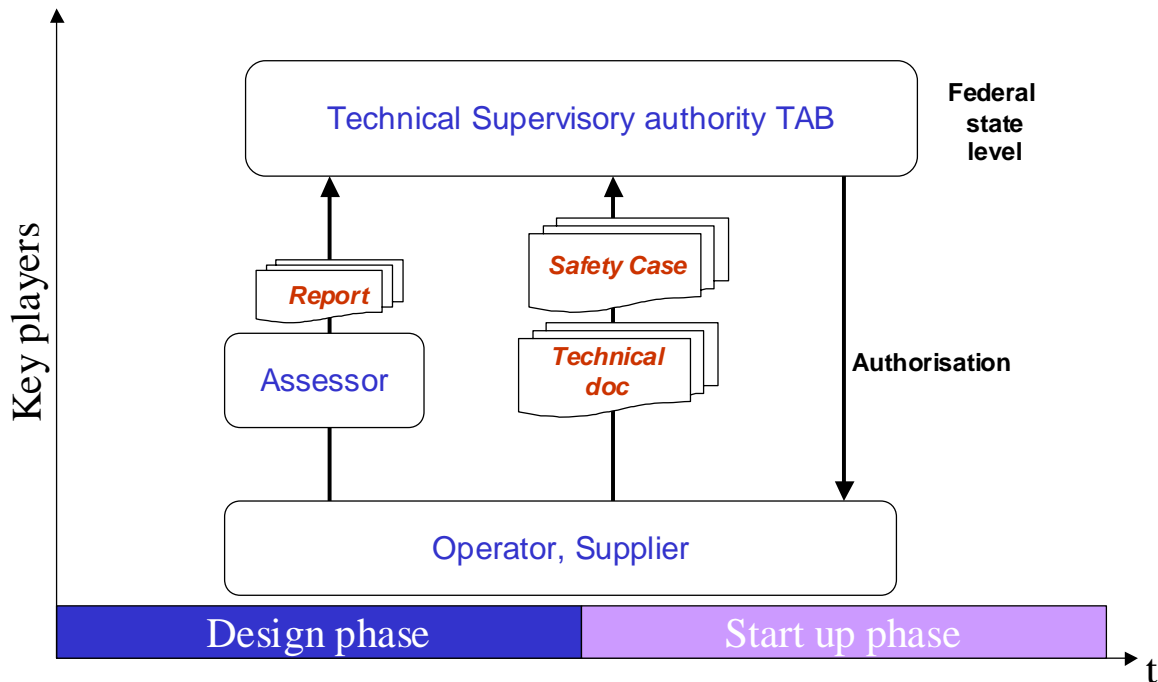


Figure 12 - Matrix for Germany

To operate a urban guided transport system, it is necessary to have a license granted by the Safety Authority in agreement with the Technical Supervisory Authority (TAB) [5]. The TAB and the licensing authority are determined by the government of a federal state (Länder). All infrastructures and vehicles must be constructed and operated in accordance with, in the one hand, the specific regulations of BOStrab, and in the other hand, the instructions of the TAB, and the licensing authority, and lastly in accordance with the commonly acknowledged rules of technology. It further states that it may deviate from the commonly acknowledged rules of technology, if at least the same safety is guaranteed. Building works can not start until the TAB report demonstrated that statutory safety requirements have been met. A continuous monitoring of works and supporting documents must be carried out by the TAB (checks, tests, inspections especially for the Safety related part). TAB may delegate to competent individual (assessors) in order to examine the design, the material to be used, the safety requirement, the Safety demonstration, the Quality Plan provided by operator and supplier.

#### 4.2.7. France

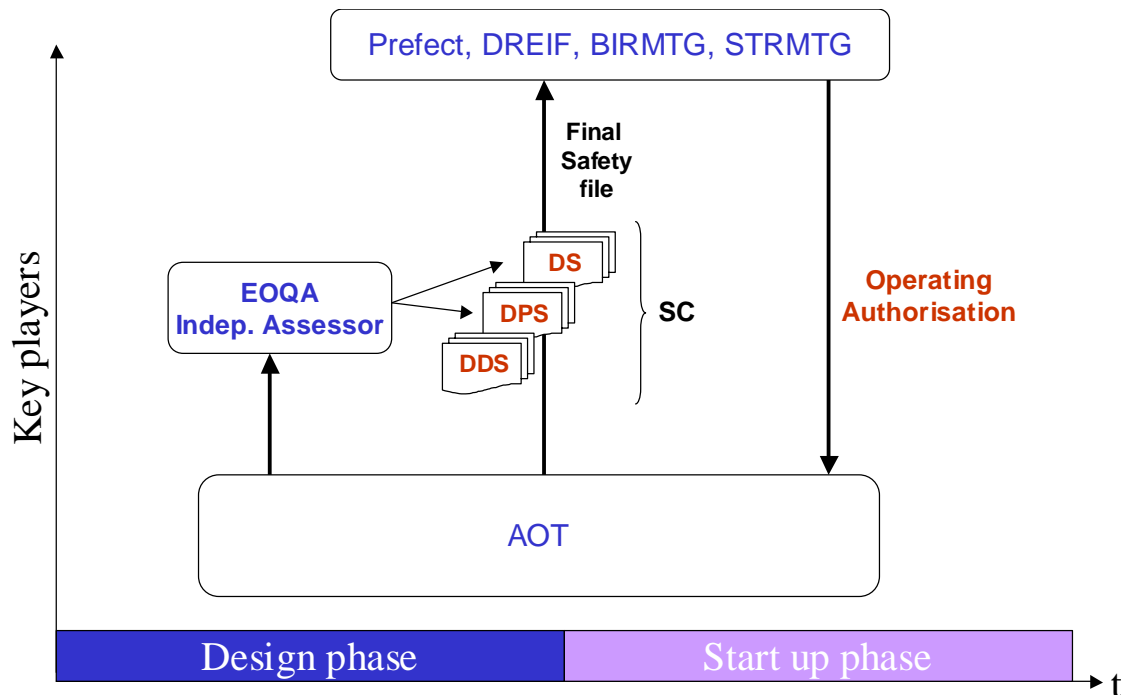


Figure 13 - Matrix for France

The safety Definition Case (DDS for Dossier de Définition de Sécurité) is the first step to initialize a dialog between the Local safety Authority (AOT for “Autorité Organisatrice du transport”) and the National Safety Authority (Prefect, DREIF, BIRMTG, STRMTG). It establishes the legal framework proposing the preliminary Safety and Quality Plans and the main characteristics (functional, technical, the general Safety targets). It may be considered like a concept submission to the Safety Authority who accepted it or not. Then, the Preliminary Safety Case (DPS for Dossier Préliminaire de Sécurité) specifies in details the Safety targets, the requirements, the methods and the principles used to reach them. A Preliminary Hazards Analysis is included. An independent safety assessor report delivered by an EOQA (Experts ou Organismes Qualifiés Agréés, kind of ISA recognised and accredited by the National Safety Authority) is added to the file. The National Safety Authority approves the DPS, the starting point of works is given by supplying the funds. The Safety case (DS for Dossier de Sécurité) is the final and most important document. It includes the DDS and the DPS updated, and has to demonstrate that the requirements described in the DPS are fulfilled. A second independent safety assessor report delivered by the same independent Assessor Body (EOQA) is added in this file. Simplifying, it can be stated that the DS file gives the assurance that the system reached the safety targets. It is constantly updated and managed by the operator during the whole life cycle of the concerned system(s).

#### 4.2.8. The UK

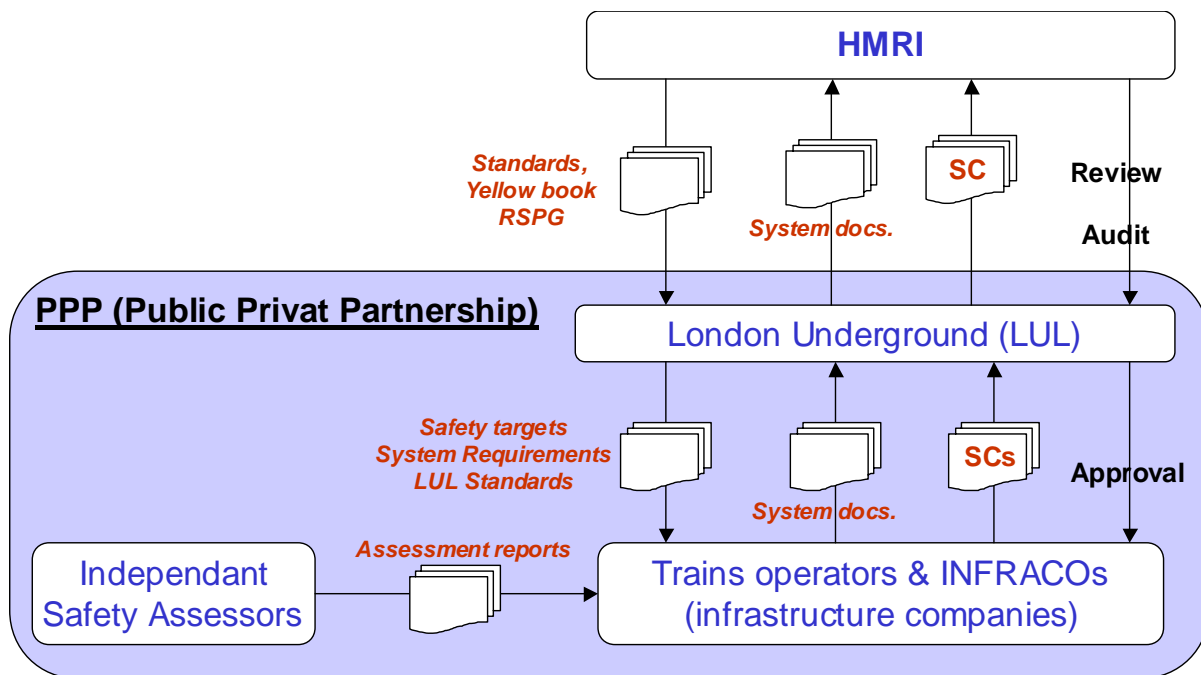


Figure 14 - Matrix for the UK

London Underground is both Infrastructure Controller and Train Operator, which means that it is responsible for the provision and management of staff and activities associated with the running of stations, trains and control of the service utilising the infrastructure and systems provided by the Infracos. In its RSC, London Underground sets out how it discharges its duties under these regulations by taking a systematic approach to operations, significant risks, risk control systems, and its programme of further improvements. There is no legal requirement for Infracos to have a Safety Case, but under the PPP, LU has required each Infracos to produce a Contractual Safety Case, which is approved by LU. LU holds a Safety Certificate (from the HMRI), and is responsible for putting in place an appropriate Safety Management System (SMS), and complying with it. LU also assumes that its suppliers have appropriate SMS, which comply with LU requirements. LU accredits suppliers to provide assured products (systems) and LU audits the suppliers to check that they comply with their SMS.

#### 4.3. Extraction of common elements/ Proposal of a sketch for the safety approval

Although there are a lack of information and uncertainties on some matrix, some elements are redundant in each process. A preliminary analysis shows a certain

convergence in the use of European standards, in particular IEC 50126/8/9, IEC 50121-2/4 (see Table 7), and safety policies (GAME or ALARP).

**Table 7 - Provided documents in approval process**

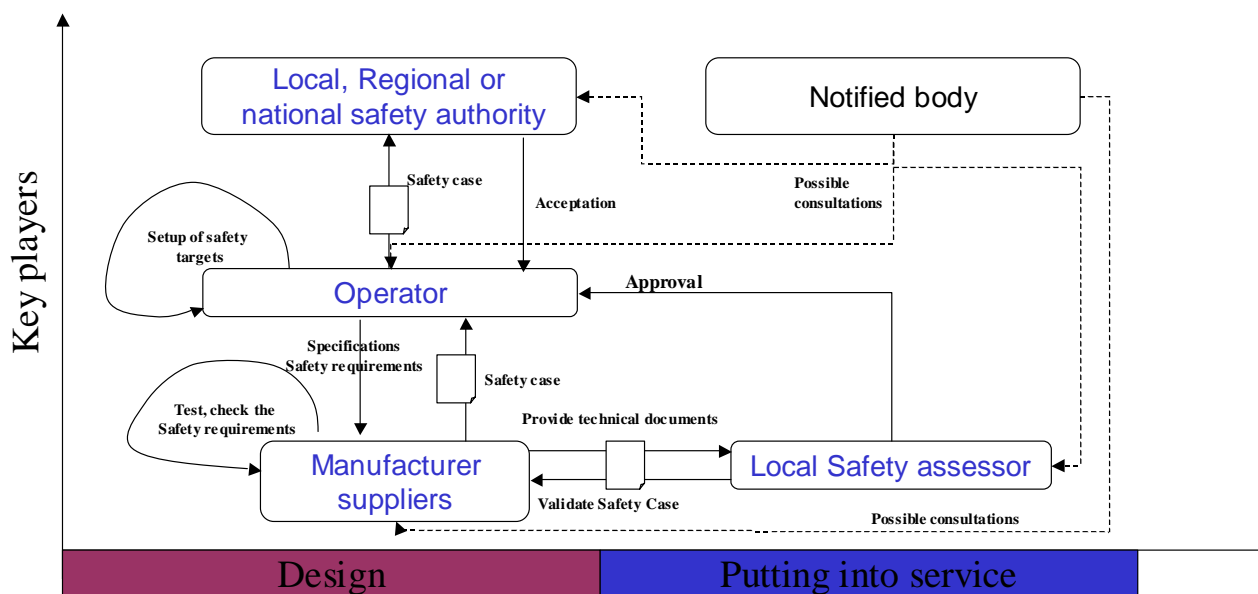
Country	Provided documents	Remarks
Czech Republic	Safety Case Requirement documentation	Provided documents rest on : EN and UIC standards
France	<b><u>Local Safety Authority (or operator in case of a delegation):</u></b> Safety Definition Case Preliminary Safety Case Safety Case	Provided documents rest on : National Decrees and Laws; EOQA reports; Safety Case of the Supplier/Manufacturer
	<b><u>Supplier/Manufacturer</u></b> Safety Case	Provided documents rest on : EN 50126 EN 50129 EN 50128
Germany	Safety Case Technical Documents	Provided documents rest on : commonly acknowledged rules of technology as: EN 50126 EN 50128 EN 50129 and several directives based on the relevant laws.
Hungary	System Requirement Specification Safety case Safety assessment report	
Italy	Customer Technical Spcs. International standards Safety case	
Portugal	Specifications document operational documents Safety certificate Procedure documents Test results documents Maintenance documents	Provided documents rest on : EN 50126 EN 50129 EN 50128 EN 50121-2/4
Spain	Technical Documents operational documents Safety Case	no approval process at national level but only at a regional level
Sweden	Specification of requirements Risk analysis Safety inspection Safety Case Validation plan	
United Kingdoms	Safety case	Provided documents rest on : EN 50126 EN 50129 EN 50128

It is also highlighted that the document of reference between the different key players (either during the design phase or the commissioning phase) is the Safety Case. Only the means to demonstrate that security objectives are achieved are at the discretion of the manufacturer/supplier.

The patterns also highlight recurring relationships between the various players. Globally, during the design phase,

- operators often set up themselves the safety targets for the putting into service of the new system,
- manufacturers often resort on an external safety entity in order to realize the safety study and to write the safety case.

There are exchanges between manufacturers and operator about the safety case. Once checked by the operator, this last one submits it to the legal authority that can allow the start-up of the system. In the same way, during the commissioning phase, the same approach is applied but in performing tests on the system under normal operating conditions and degraded modes.



**Figure 15 - Proposition of a generic approval process**

A notified body could give one's opinion concerning the safety case, the documents and ensure that the evaluation is established according to the same referees (documents, means and methods) between the different key players. It could be a first step toward a harmonized approval sketch.

## 5. Conclusions and perspectives

The works carried out in this document is a synthesis about the certification process in regard to the safety in urban guided transport system.

Through a questionnaire, different approval processes of urban guided systems were studied. In this study, a generic certification process has been extracted from common elements.

This proposal deals with design and putting into service phases of the lifecycle.

It is obvious that it is necessary to improve this study at all stages of the life cycle to and analyse the responsibilities allocation of an incident/accident during the operational phase of the system.

Future research works may focus on the part of the safety authority concerning not only the design level but also the operation level. Indeed, the contribution of the safety authority may also concern actions such as:

- The validation of the safety rules and the human operator task
- The validation of the procedures to check that rules are being respected.
- The validation of the procedures to control the staff competences, qualifications and training.
- The validation of the operational safety procedures in case of accidents.
- The validation of the procedures to evacuate passengers in case of incidents or accidents
- The validation of the facilities for easing the bringing of assistance.
- The validation of the reporting process when an accident occurs.
- Etc.

Some tools are already available to support such studies [9, 10]:

- The D128 concerning the integration of the positive and negative contributions of human factors to the occurrence of particular events,
- The D91 concerning the data reporting system when an incident or an accident occurs

## **6. References**

[1] Council Directive 91/440/EEC on the development of the Community's railways, commission of the European Communities, Brussels, 29 July 1991.

[2] Directive 96/48/EC on the interoperability of the trans-European high-speed rail network, 23 July 1996.

[3] Directive 2001/16/EC on the interoperability of the trans-European conventional rail system, 19 September 2001.

[4] Council Directive 2004/49/EC on the safety of the community's railways, 29 April 2004.

[5] CENELEC: Railway Applications - The Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). EN 50126, 2000.

[6] CENELEC: Railway Applications- Communication, signalling and processing systems- Software for railway control and protection systems. EN 50128, 2001.

[7] CENELEC: Railway Applications- Safety related Electronic Systems for Signalling. EN 50129, 2003.

[8] Safety regulation and standards for European railways, report for DG Energy and Transport, prepared by NERA February 2000.

[9] D91: Database of non conformity events, Project MODURBAN, 6e PCRD, December 2007.

[10] D128: Risk assessment based on human factors. Project MODURBAN, 6e PCRD, November 2007.

### **HTML Links**

French decrees [http://www.legifrance.gouv.fr/html/frame\\_lois\\_reglt.htm](http://www.legifrance.gouv.fr/html/frame_lois_reglt.htm)

Council Directive <http://europa.eu.int/eur-lex/en/lif/dat>

Rail track: Engineering Safety Management Yellow Book, London 3  
<http://www.yellowbook-rail.org.uk>

Lul Safety Case  
<http://www.hse.gov.uk-railway/lulsafecase.pdf>

ROGS Regulation  
<http://www.rail-reg.gov.uk/upload/pdf/283.pdf>

Directive 96/48/EC on the Interoperability in Great Britain  
<http://www.railways.detr.gov.uk/consult>

Railway safety  
<http://europa.eu/scadplus/leg/en/lvb/l24201a.htm>

STRMTG : Service Technique des Remontées Mécaniques et des Transports Guidés.  
[http://rp.equipement.gouv.fr/strmtg/organismenotifie/accueil\\_on.htm](http://rp.equipement.gouv.fr/strmtg/organismenotifie/accueil_on.htm)  
<http://www.strmtg.equipement.gouv.fr/>

UITP and European Rail Legislation impacting local rail networks (urban, suburban and regional)  
<http://www.uitp.org/mos/brochures/40-en.pdf>