MODSafe

European Commission
Seventh Framework programme
MODSafe Modular Urban Transport Safety and Security analysis

WP1 – D1.2
Final Report - State of the art on Safety Responsibilities and Certification

Deliverable No.	D1.2

Contract No.	218606
Document type	DEL
Version	V3
Status	Final
Date	13012010
WP	WP1
Lead Author	Vincent BENARD - INRETS
Contributors	Latifa Furlan, El-Miloudi El Koursi, Frédéric Vanderhaegen, Peter Wigger, Holger Hölscher, Walter Schön, Gab Parris
Reviewer	
Description	Deliverable D1.2 Final Version V3
Document ID	DEL-D1.2_INRETS_WP1_13012010_V3
Dissemination level	RE
Distribution	WP10 members

Document History:

Version	Date	Author	Modification
Draft	30/09/2009		First version for comments
Draft2	10/11/2009		Respect comments on first version
Final	13/01/2010		Respect comments on second version

Approval:

Authority	Name/Partner	Date	Visa
EB members	WP 10	22.01.2010	via email
WP Responsible	Inrets	25.01.2010	via email
Coordinator	TRIT	26.01.2010	ok

Table of Content

Figures

Tables

1. Executive summary

The objective of this report is to review the state of the art in safety, to identify how the safety approaches are used in a large number of European Member States, and to compare among these safety approaches and those used in other safety critical industries.

This document is divided in 5 parts:

- The first part presents, as a general rule, the definition of a safety management system (SMS) and the way to use a SMS in different critical industries. The security concepts are presented.

- The second part describes the keys players involved in a safety management system and briefly presents their tasks and responsibilities.

- The third part is dedicated typically to the importance of Human factor during the safety lifecycle of an urban guided transport system (Human errors, use of barriers, tools and methods to evaluate Human reliability).

- The next part deals with accident/incident analysis environment. The indicators used in railway sector are detailed and a comparison between three urban guided transport networks is made.

- Then the last part concerns the certification and presents some approval processes applied in the European Union and in Australia.

2. Definitions/Glossary

2.1. Definitions[1]

Term	Description	Source
Assessment	The undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product.	EN50126
Assurance	Level of guarantee that a security system will behave as expected.	
Authorisation/ Approval	The Formal permission to use a product within specified application constraints.	EN 50129
Availability	The proportion of time that an item is capable of operating to specification within a large time interval.	MODURBAN
Competent Authority	Person or organization that has the legally delegated or invested authority, capacity, or power to perform a designated function.	MODURBAN
Countermeasure	Way to stop a threat from triggering a risk event	
Defence in depth	Never rely on one single security measure alone.	
Exploit	A vulnerability that has been triggered by a threat - a risk of 1.0 (100%)	
Maintainability	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.	MODURBAN
Notified bodies	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
Regulation	Document providing binding legislative rules that is adopted by an authority.	EN 45020
Reliability	The probability that an item can perform a required function under given conditions for a given time interval.	MODURBAN
Risk	The rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm.	CLC/prTR 50126-2
Safety	Freedom from unacceptable levels of risks of harm.	EN50129

[1] Some definitions are under review in the current standard working group

Safety approval	The safety status given to a product by the requisite authority when a product has fulfilled a set of predetermined conditions.	EN50129
Safety assessment	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.	MODURBAN
Safety authority	The body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements.	EN50129
Safety case	The document demonstration that the product complies with the specified safety requirements.	EN 50126 EN 50129
Sub-system	A combination of equipment, units, assemblies, etc., which performs an operational function and is a major subdivision of the system.	MODURBAN
System	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.	MODURBAN
Threat	A threat is a method of triggering a risk event that is dangerous. It is characterized by the intention and the ability to achieve a risk event.	
Vulnerability	A weakness in a system that can potentially be exploited to become a threat	

2.2. Abbreviations

ACIH	Analysis of Consequences of Human Unreliability
ALARP	As Low As Reasonably Practicable (UK safety principle)
AOT	Autorité Organisatrice de Transports (Transport Organising Authority)
ASME	American Society of Mechanical Engineers
ATM	Air Traffic Management
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATSP	Air Traffic Services Provider
AS	Australian Standard

AZF[2]	AZote Fertilisants
BCD	Benefits/Costs/potential Danger
BIRMTG	Bureau Interdépartemental des Remontées Mécaniques et des Transports Guidés
BOStrab	Bau- und Betriebsordnung für Strassenbahnen (German Federal Regulations on the construction and operation of light rail transit systems)
CAA	Civil Aviation Authorities
CENELEC	Comité Européen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardisation)
CIRAS	Confidential Incident Reporting and Analysis System
COR&GEST	Driving on Rails and traffic management Platform (Plate Forme de Conduite sur Rail et de Gestion de Trafic)
CSI	Common Safety Indicators
DAE	Authorization Application Testing (Dossier d'Autorisation d'Essais)
DAuTE	Authorization Application Testing and tests (Dossier d'Autorisation de Tests et Essais)
DB	Deutsch Bahn
DDS	Dossier de Définition de Sécurité (Safety Definition Case)
DOC	Document Of Compliance
DPS	Dossier Préliminaire de Sécurité (Preliminary Safety Case)
DREIF	Direction Régionale de l'Equipement Ile de France (Regional Department of Equipment for Ile de France area)
DS	Dossier de Sécurité (Safety Case)
E/E/PES	Electrical/Electronic/Programmable Electronic System
EASA	European Aviation Safety Agency
EC	European Community
ECAC	European Civil Aviation Conference
ECSS	European Co-operation for Space Standardisation
EIRF	Electronic Incident Investigation Form
EN	European Standard
EOQA	Expert ou Organisme Qualifié Agréé (Independent Assessor Body accredited by the National Safety Authority)
EPSF	French Railway Safety Authority (Etablissement Public de Sécurité Ferroviaire)
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
EU	European Union
EUROCONTROL	European Organisation for the Safety of Air Navigation
GAIN	Global Aviation Information Network

[2] Armed group that has threatened attacks on the French rail company SNCF and whose name it bears the Toulouse plant that exploded in 2004

GAME	Globalement Au Moins Equivalent - Globally at least equivalent
HF	Human Factors
HMRI	Her Majesty's Railway Inspectorate
HSE	Health and Safety Executive
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IEC	International Electrotechnical Commission
IM	Infrastructure Manager
IMO	International Maritime Organisation
INCA	Incident Capture and Analysis
INFRACOS	Infrastructure Companies
INRETS	French National Institute for transport and safety research (Institut National de Recherche sur les Transports et leur Sécurité)
IRF	Incident Report Form
ISA	Independent Safety Assessor
ISM	International Management Code for the Safe Operation of Ships and for Pollution Prevention
ISO	International Organization for Standardization
LPF	Loss of Process form
LU	London Underground
LUSATS	London Underground Safety Action Tracking System
LUSEA	London Underground Safety and Environmental Analysis database
NSW	New South Wales
PHA	Preliminary Hazard Analysis
PPP	Public Private Partnership
PTC	Public Transport Safety
RAMS	Reliability, availability, Maintainability and Safety
RAND	Research and Development Corporation
RATP	Régie Autonome des Transports Parisiens (Autonomous Paris Transport Authority)
RER	Réseau Express Régional (Express Regional Network)
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulation
RSPG	Railway Safety Principles and Guidance
RSSB	Rail Safety and Standards Board
RU	Railway Undertaking
RWIIF	Record of Workplace Injury or Illness Form
SARF	Staff Assault Report Form
SC	Safety Case
SD	Railway Safety Directive
SECUREMETRO	Inherently secure blast resistant and fire safe metro vehicles
SIL	Safety Integrity Level

SMC	Safety Management Certificate
SMS	Safety Management System
SNCF	Société Nationale des Chemins de Fer
SPAD	Signal Passed At Danger
SPICA-RAIL	Simulation platform of the university of technology of Compiègne
STPG	Safety of Public Guided Transit
SRC	Safety Regulation Commission
SRS	System Requirement Specifications
STRMTG	Service Technique des Remontées Mécaniques et des Transports Guidés (French Technical Agency for Ropeways and Guided Transports safety)
TAB	Technische Aufsichtsbehörde (Technical Supervisory Authority)
THERP	Technique for Human Error Rate Prediction
TRANSPAL	TRANSformation de PALettes
TSO	Technical standard Order
TU	University of Technology
TUD	Technische Universität Dresden
TV	TeleVision
UGTMS	Urban Guided Transport Management System
WP	Work Package

3. Introduction

Today, public transport is a tremendous success in many cities, probably linked to economic reasons and environmental issues. In addition to an increasing deployment, guided transport must meet requirements for quality of service, particularly in terms of safety, security, comfort and sustainability.

Currently, the European Urban Guided Transport sector (Light Rail, Metros, Tramways and Regional Commuter trains) is still characterized by a highly diversified landscape of Safety Requirements, Safety Models, Roles and Responsibilities and Safety Approval, acceptance and Certification Schemes although there are convergences between some architectures and systems. Even so, the safety life cycle still differs from country to country and sometimes even within one country.

There are currently no standardised procedures at the European level for bringing urban guided transport into service, 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, IEC 62278/62279/62425).

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 now the MODSAFE project.

This deliverable proposes a state of the art in safety, to identify how the safety approaches are used in a large number of European Member States, and to compare among these safety approaches and those used in other safety critical industries.

4. Safety management systems approaches/principles/regulations

Scientific and technological advances often involve innovations, but the latter can also be sources of new hazards, new risks, creating new vulnerabilities, with impacts on equipment, systems, processes, organizational and Human factors, information systems, etc. In a very strong international economic framework, issues of safety, security and performance are quickly becoming essential for companies, and it is clear today that the risk management concerns every industrial sector.
The consequences of an undesired event (accidents or incidents) are also often the subject of extensive media coverage, increasing the perception of risk by the society. This part aims to identify the safety culture in different sectors such as aeronautics, nuclear energy, maritime, etc.

4.1. Safety management systems in different safety critical industries [2]

In many sector of industry, a Safety management system is defined as a documented risk management process that integrates operational and technical systems for the financial and Human resources management in order to ensure system and public safety (figure 1). The system of safety management should include:

- a safety policy on which the system must rest on;
- a process in order to establish goals to improve the system safety and to assess how they were achieved;
- a process that can detect hazards for system safety and to assess and manage risks associated with them;
- a process which ensures that staff are trained and competent to perform their duties;
- a process used to report hazards associated with internal incidents and accidents and to analyze and take corrective measures to prevent them;
- a document containing all the processes of Safety Management System and a process which ensures that staff are aware of its responsibilities to them;
- a process to carry out periodic audits or review of the Safety management system;
- any additional requirements on the safety management system which is contemplated with the regulation inherent to the system itself during operation.

Figure 1 - Illustration of Safety Management System

Bibliographical research identifies three types of models for Safety Management System (SMS):

Regulatory model is the first type of model of SMS. There are two types of regulatory model:

- the single headed regulatory model (the director assumes chief responsibility for the functioning of the regulatory agency and is assisted by professional support staff and possibly consultants),
- the collegial bodies regulatory model (several members are referred to as councillors or commissioners.

In the framework of governmental legislation, companies (entities which are mandated for the operation) develop their own safety management systems including specification, implementation and evaluation of detailed preventive measures. Government inspectorates could then confine themselves to assessing these safety management systems, linked to sample checks to see that they are being implemented. In practice, different regulatory authorities have adopted this model which aligns/agrees with their legal and political institutional framework.

Implicit Safety models are the second kind of models of SMS used in an industrial context. Two implicit Safety models are presented in this part for different industrial fields, in particular, in nuclear and space industries.

In the nuclear field, the safety management for applications is associated with the design for processes and equipments. There are two main standards for safety and quality management:

- *ASME NQA-1-2000 quality Assurance Requirements for nuclear Facility Applications 2000 (US standard),*
- *Series of nuclear safety Standards commission rules (German series of standards)*

These standards cover all stages of lifecycle from design to decommissioning. The responsible governmental Authorities for nuclear facilities set up fundamental safety requirements and issue an operating licence, once the plant operator has checked that the equipment fulfils these requirements. The governmental Authority employs competent independent Assessors in order to review the verification process in technical detail and the plant Operator manages his suppliers by means of contractual requirements for quality and safety, as well as respective verification procedures.

In the space field, the European Co-operation for Space Standardisation (ECSS), organism, created by European and national space agencies in cooperation with space industries, has established a set of standards (ECSS-M-20, ECSS-M-30, ECSS-Q-40, for example) for areas that have potential damaging effects including, in particular, safety management issues, without defining safety principles in technical details. Following these quality and safety standards, the customer is responsible for definition of technical requirements to his direct suppliers. A general review including a safety review takes place at the end of each step of the lifecycle in order to determine whether the requirements for this step have been fulfilled. The safety policy rests on a deterministic safety programme, supported by a probabilistic risk assessment. All potentially hazards and failures are subject to a hazard reduction. The adequacy between hazard and risk control measures needs formal verification in order to support safety validation and risk acceptance. All verifications and investigations are documented in an Accident/Incident database throughout the systems' life .The responsibilities, operations and equipment of the space industry are not directly regulated by governmental agencies. The responsibilities are defined by contractual agreements rather than legal requirements.

SMS Based models are the last models presented in this document. These type of models concern maritime, civil aviation and railway sectors.

In the maritime sector, the International Maritime Organisation (IMO) adopted in 1993 the International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code). The first objective of this code is to ensure safety, to prevent Human injuries or loss of life, and to avoid damage to the environment. It establishes the safety management goals and requires a safety management system which will be established by the ship's owner or any person who has to assume the responsibility for operating the ship in accordance with mandatory rules, regulations,

guidelines and standards. The IMO formulates and adopts safety codes, prepares the basis for legislation. Governments of the European Union are responsible for implementing them. When a Government accepts an IMO convention, it agrees to make it part of its own national law. Each member state has a regulatory body for carrying out these tasks. The shipping industry regulates itself and checks the maintenance of ship safety through the organisation called Classification societies. SMS certification comprises two statutory certificates, the first one is the Document of Compliance (DOC) and the second is the Safety Management Certificate (SMC).The DOC is issued to the company following a successful audit of the shore side aspects of the safety management, while the SMC is issued to an individual ship after an on board audit of the SMS. Both the ship and the company, which owns or operates, require certification, which is done by the flag states of the ship. The port state control provides additional surveillance. The use of centralised databases of port state audits have helped to identify and control substandard ships. There are no requirements for products, equipment or subsystems certification in the maritime sector. Acceptance of shipboard equipment generally is covered under self regulation.

In the aeronautical sector, international organizations have been developed through the years, in which standardisation has played a significant role. The organisational framework of the aeronautical sector can be shared between 5 actors:

- *the international organisations, whose functions are to coordinate the processes between the different countries and international entities; they can sometimes implement as law the conventions set out by the standardisation organisations (for example, these organisations are ICAO (International Civil Aviation Organisation), ECAC (European Civil Aviation Conference), JAA (Joint Aviation Authorities), EUROCONTROL (European Organisation for the Safety of Air Navigation) IATA (International Air Transport Association), EASA (European Aviation Safety Agency), GAIN (Global Aviation Information Network)),*
- *the standardisation organisations, which are entities that report according to the different kind of flights all standards related to different subjects (safety, quality, and so on….). These standards do not qualify as law until the corresponding CAA (Civil Aviation Authority) implements them as such,*
- *the CAA, which is a governmental entity specific to each country; its function is to make sure that the complete aviation process is carried out safely in its country. Moreover it is responsible for implementing as "national law" the conventions agreed on the standard Organisations at the international level,*
- *the operators, commonly referred to as "airlines", which work with governments, standard bodies and air traffic service providers,*
- *Air Traffic Services Providers (ATSP) helped by Airports, is an entity in charge of providing traffic services and maintaining the navigation aids and responsible of the infrastructure in which the aircraft operates.*

In the aeronautical framework, a SMS ensures a formalised and proactive approach to systematic safety. The safety regulation Commission (SRC) of EUROCONTROL is responsible for the development of harmonised safety regulatory objectives and requirements for the ATM system. The certification in civil aviation aims to get a consistently high level of safety. There is a separation between onboard elements and supporting infrastructure in the way that certification is made. Certification in onboard elements is based on three steps: first of all, a Technical standard Order (TSO), which is a design certification, is required, then an Airworthiness Approval, equipment installation certification, and finally an Operational Approval, in order to certificate the application for which the equipment have been designed. For supporting infrastructure, the regulation framework and the certification are not as well defined as for onboard elements. First of all, the air traffic service providers shall make tests to check the equipment and system themselves; these parts are equivalent to TSO and an Airworthiness Approval in the onboard elements. After that, an operational approval is required in order to get full certification. When elements are not compliant with the existing regulations, it is possible to perform risk analyses as an alternative means of compliance to demonstrate that the safety intent of the regulations are met. These analyses are submitted to the CAA for approval.

Finally, in the railway field as part of the potentially interoperable European railway system, there is a generic SMS [21]. This model is used in different countries by various operators such as SNCF, DB. A SMS should contain a set of elements linked into two feedback loops: risk control and learning system loops. The risk control loop includes business process, risk evaluation, risk barriers and control during lifecycle. In the same way, the learning loop integrates inspections and monitoring system over the barriers and controls, auditing and management review in order to determine how the risk management system is performing, how incidents and accidents are analyzed [33]. The annex 1 compares this model of SMS used in different railway undertakings and international organizations. All steps of the SMS are analysed.

4.2. Generic standards for safety critical industries

The IEC 61508 standard is a generic standard, and is used today as reference by all major industrial sectors. Since its creation, several derivatives of this standard were created. These declinations aimed to make IEC 61508 applicable for different sectors. The IEC 61508 standard deals with the functional safety of electrical/electronic systems and programmable electronic systems (E/E/PES). This is a generic standard approach, which is decomposed in 7 parts (general requirements, requirements for systems E/E/PES safety related, software requirements, definitions and abbreviations, example of Methods to determine the SIL (Safety Integrity Level), guidelines for the application of the parts 2 and 3, presentation of techniques and measures). The standard has helped to define the levels of integrity for systems E/E/PES which take into account risk management, as well the quantitative and qualitative aspects. In addition, the standard integrates the

safety activities, in parallel to the life cycle of the system E/E/PES, and these are adapted according to Safety Integrity Level desired. By its generic aspect, the IEC 61508 standard briefly describes tools, methods and techniques of implementation.

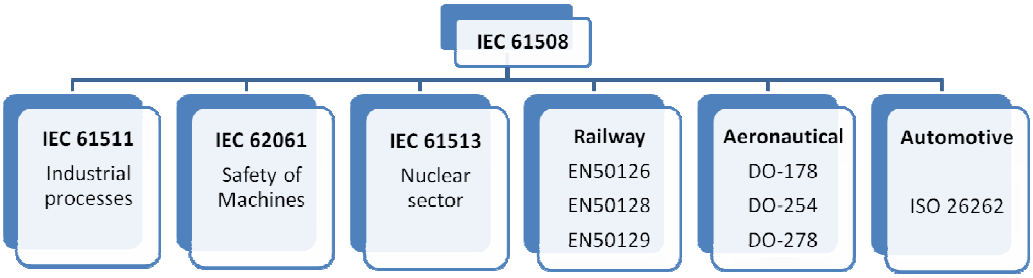


Figure 2 - Declination of the IEC 61508 Standard in various industrial sector

The figure 2 presents the IEC 61508 and its derivatives. The IEC 61511 standard, introduced in 2003, is adapted from the IEC 61508 standard for industrial processes. The IEC 61513 standard, introduced in 2001, is adapted for the nuclear sector. The IEC 62061 standard, introduced in 2005, is the standard adapted from the IEC 61508 standard for the safety of machines. The declinations of the IEC 61508 in the aeronautical field are summarized in the DO-178/254/278 standards. The EN 50126/ EN 50128/ EN 50129 standards, established respectively for the latest versions, in 1999/2001/2003, are standards adapted from the 61508 standard for the railway sector. Then, the ISO 26262 standard is being developed and its release is foreseen for 2009, and it is the adaptation of the IEC 61508 standard for the automotive sector.

The next section describes the standards concerning railway sector (EN 50126/ EN 50128/ EN 50129) [3]. These standards are notably used in the certification processes in the field of interoperable railway (on the administrative side of the certification and authorisation bodies (notified bodies) and cross acceptance rules throughout Europe. They are regularly being updated, but remain independent of European directives and regulations.

EN 50126 – « Specification and demonstration of the reliability, availability, maintainability and safety»:

This standard allows the implementation of a consistent approach to management of reliability, availability, maintainability and safety called RAMS. This standard can be applied in the rail industry throughout the life cycle because it integrates the requirements RAMS specific to this field. 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". It can be note that, if the definition of SIL is clear, the means to evaluate it are fuzzy.

EN 50128 – « Railway applications – Software for railway control and protection systems »:

This standard deals, in particular, with methods that are necessary to be used to produce software that satisfies the requirements of safety integrity level for the railway field. These software solutions may range from the very critical, such as safety signalling, to the non critical such as management information systems. The integrity of a software is distributed on five levels SIL, ranging from SIL 0 to SIL 4. These levels SIL are the association of:

- the occurrence of a hazardous event and,
- its consequence on the system and its environment.

The SIL is a requirement associated to a function. Once the SIL determined for this function, some technical tools and measurement resting on software languages, formal methods, methodologies, recommendations are used to check that the evaluation of the function met the SIL. In order to produce softwares consistent with the Functional Requirements Specification, the technical requirements need to be met in accordance with the standard.

EN 50129 – « Railway applications - Safety electronics systems for signalling»:

This standard addresses all the issues related to the verification and validation process of individual systems, that can be software or hardware, and which may exist in the framework of a global system. This standard defines the evidence to provide for the acceptance of each individual system in the light of its SIL integrity level. Actually, there are two aspects to distinguish:

- the determination of the safety requirement for a component produced in different countries. According to EN50129 (annex A4 in particular), the safety requirements for a component depend on the context of use. It shall be note that this context of use could be different for each country (e.g. platform

screen doors do not offer the same protection in a crowded station in Paris than in a little-used station in another country). So it must be considered that the same component can be classified SIL X in a country and SIL Y in another one due to different contexts of use.

- the SIL cross-acceptance of a component from a country to another one. Once a component is certified SIL X in a country, it should be accepted in different countries without further assessment as long as the European standards used for certification are the same (cross-acceptance principle).

The target of European Interoperability Railway Community is to develop compatible railway systems and sub-systems based on common standards. All of this evidence shall be included in the Safety Case, the masterpiece of an authorisation process.

The standards EN 50126, 50128 and 50129 are currently under maintenance at CENELEC level and are subject to change.

4.3. Safety during lifecycle and SMS for urban guided transport systems

As for other critical industries, based on the different essential requirements and with no need for interoperability between networks, urban guided transport systems are concerned by safety management. In this section, in a first point, the tasks inherent to the safety are described all along the lifecycle (from the concept of the system to the decommissioning phase of this system). In a second point, the presentation of a SMS is evoked.

4.3.1. Safety along the Lifecycle

Safety must be assured throughout the lifecycle of a transportation system to protect passengers, workers, and public from hazardous and unacceptable event (cf. figure 3).

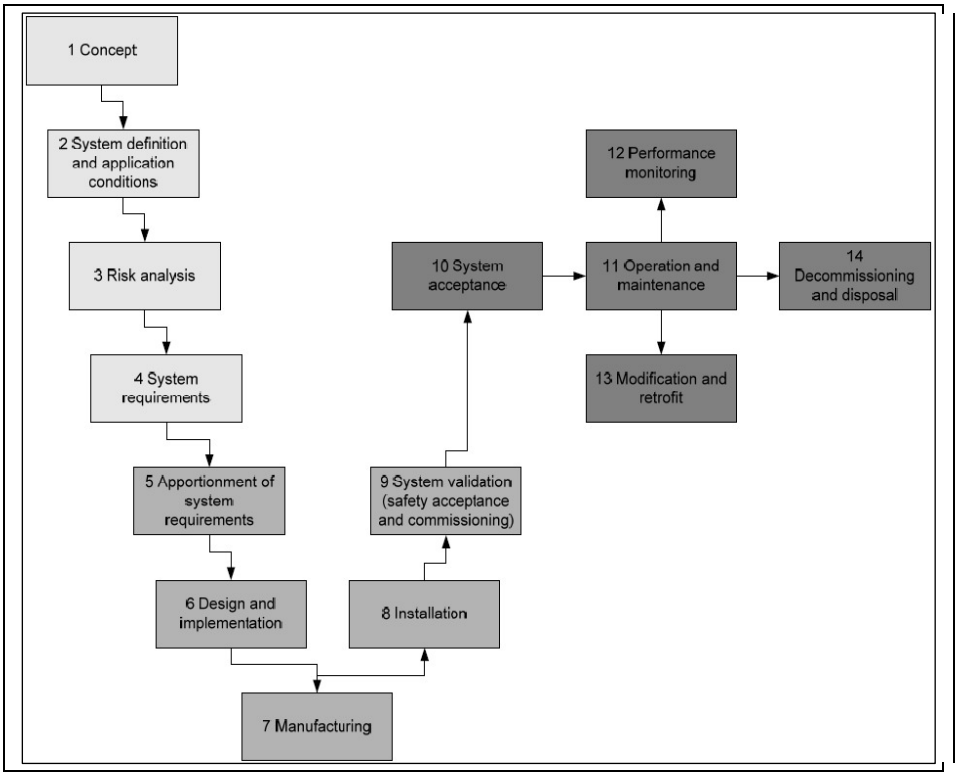


Figure 3 - Steps of a system lifecycle integrating safety aspects

At each step of the system lifecycle, tasks inherent to safety are specified:

1- **Concept :**
   - review of previously achieved safety performance,
   - consideration of safety implications of project,
   - review of safety policy and safety targets

2- **System definition and application conditions :**
   - Evaluation of past experience data for safety,
   - Achievement of preliminary hazard analysis,
   - Establishment of safety plan,
   - Definition of tolerability of risk criteria,
   - Identification of influence on safety of existing infrastructure constraints,

3- **Risk analysis :**
   - Achievement of system hazard and safety risk analysis,
   - Setup of hazard log,
   - Achievement of risk assessment,

4- **System requirements :**
   - Specification of system safety requirements,
   - Definition of safety acceptance criteria,
   - Definition of safety related functional requirements,
   - Establishment of safety management,

5- Apportionment of system requirements:
- Apportionment of system safety targets and requirements :
  - *i. Specification of subsystem and component safety requirements,*
  - *ii. Definition of subsystem and component safety acceptance criteria,*
- Update of safety plan,

6- Design and implementation:
- Implementation of safety plan by review, analysis, testing and data assessment, addressing,
- Hazard log,
- Hazard analysis and risk assessment,
- Justification of safety related to design decisions,
- Undertaking of programme control covering:
  - *i. Safety management,*
  - *ii. Control subcontractors and suppliers,*
- Preparation of generic safety case,
- Preparation of generic application safety case,

7- Manufacturing:
- Implementation of safety plan by review, analysis, testing and data assessment,
- Use of hazard log,

8- Installation:
- Establishment of installation programme,
- Implementation of installation programme,

9- System validation (including acceptance and commissioning):
- Establishment of commissioning programme,
- Implementation of commissioning programme,
- Preparation of application specific safety case,

10-System acceptance:
- Assessment of application specific safety case,

11-Operation and maintenance:
- Undertaking of safety centred maintenance,
- Achievement of safety performance monitoring and hazard log maintenance,

12-Performance monitoring:
- Collection , analyses, evaluation and use of performance and safety statistics,

13- Modification and retrofit:
- Consideration of safety implications for modification and retrofit,

14-Decommissioning and disposal:
- Establishment of safety plan (for decommissioning and disposal),
- Achievement of hazard analysis and risk assessment,
- Implementation of the safety plan.

4.3.2. The Safety Management System

The safety management system must be documented in all relevant parts and shall in particular describe the distribution of responsibilities within the organisation of the infrastructure manager or the operator. It shall show how control by the management on different levels is secured, how staff and their representatives on all levels are involved and how continuous improvement of the safety management system is ensured.

The basic elements of the safety management system are [21]:

- a safety policy approved by the organisation's chief executive and communicated to all staff;
- qualitative and quantitative targets, plans and procedures for reaching these targets, organisation of the operation and maintenance to maintain and improve safety;
- procedures to meet existing, new and altered technical and operational standards or other prescriptive conditions and procedures to assure compliance with the standards and other prescriptive conditions throughout the life-cycle of equipment and operations;
- procedures and methods for carrying out risk evaluation and implementing risk control measures whenever a change of the operating conditions or new material imposes new risks on the infrastructure or on operations;
- provision of programmes for training of staff and systems to ensure that staff competence is maintained and tasks carried out accordingly;
- arrangements for the provision of sufficient information within the organisation and, where appropriate, between organisations operating on the same infrastructure;
- procedures and formats for how safety information is to be documented and designation of procedure for configuration control of vital safety information;
- procedures to ensure that accidents, incidents, near misses and other dangerous occurrences are reported, investigated and analysed and that necessary preventive measures are taken;
- provision of plans for action and alerts and information in case of emergency, agreed upon with the appropriate public authorities;
- provisions for recurrent internal auditing of the safety management system.

The Deliverable D126 [22] of MODURBAN project proposes guidelines and elements to be integrated in the safety management of an urban guided transport. Globally, the Safety Management system rests on CENELEC Standards and national regulations.

4.4. Relationship between Safety and Security Management system

4.4.1. Security definition

In order to make a clear distinction between safety and security (distinction not sufficiently made in the standards EN 50126, EN 50128 and EN 50129), we propose the following definitions:

Safety: ability of the system to avoid generating unacceptable risks, consecutively to events other than those due to human malevolence
Security: ability of the system to avoid generating unacceptable risks, consecutively to events due to human malevolence.

Safety therefore deals with events whose cause can be physical (hardware component failure, environment perturbation…) or due to non malicious human actions (design bug, operating error…)

Security deals with events whose cause is explicitly due to malicious human actions (terrorism with classical means such as bombs etc. but also by intrusion in information processing that is controlling the system : hacking of communications by various means for example).

Both aspects are clearly linked and are sometimes globally taken into account (some notions like “defence in depth” apply in both cases).

Evaluation of Safety sometimes refers to probabilities (Tolerable Hazard Rate), and sometimes does not (e.g. Software Safety Integrity Level).

Evaluation of Security usually does not refer to probabilities and remains a qualitative study. A notion of “Security Integrity Level” trying to characterize the robustness of the system to attacks of various kinds could usefully be introduced in a near future. In the same way, the notion of risk is shared by security and safety and it is not impossible to see in a near future emerge combined method.

Some concepts recur throughout different fields of security:

- Assurance : Level of guarantee that a security system will behave as expected,
- Countermeasure : Way to stop a threat from triggering a risk event,
- Defence in depth : Never rely on one single security measure alone,
- Exploit : A vulnerability that has been triggered by a threat - a risk of 1.0 (100%),
- Risk : Rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm,

- Threat : method of triggering a risk event that is dangerous. It is characterized by the intention and the ability to achieve a risk event.
- Vulnerability : A weakness in a system that can potentially be exploited to become a threat

4.4.2. Evaluation of security in transportation systems

According to [26], the security evaluation in transportation systems is based on 4 aspects:

- Terrestrial transport of products that must deal with acts of predation,

- Criminal risks in public transport. Evaluations are leaded by criminologists and by public bodies that have legal land financial resources to conduct statistical studies. Concerning the terrorist threat in itself, the need to protect sensitive information often makes research difficult,

- Illegal acts. This approach focuses on the acts committed by an individual or group who wish to capture a resource owned by the victim. In the transportation field, illegal acts may involve frauds, physical assaults, damage operator's equipment, products theft, itinerant delinquency or voluntary violation of the provisions of road code,

- Terrorism can be defined as the use of violence or the threat to use violence by individuals or groups in order to achieve a political or social goal by using intimidation on a large audience beyond immediate victims. Two elements characterize any modern definition of terrorism: the presence or threat of violence and political or social grounds. For example, hostage taking, hijacking, aircraft or ship's destruction, but also damage to transport can be mentioned.

There are reports on the terrorist risk evaluation in a specific mode of transport. In [27], the RAND Corporation summarizes the various terrorist threats, their consequences and responsibilities, before detailing the risks specific to cruise ships to ferries and containers. The evaluation of the security in railway field must consider the impact of deregulation in this sector. Another possibility is to assess the vulnerability of the transportation system during a terrorist attack. The evaluation of the economic costs of terrorist actions is the subject of several studies [28, 29].

4.4.3. Towards a Security Management System

In the corporate world, various aspects of security were historically addressed separately - notably by distinguishing departments such as IT security department, physical security department, and fraud prevention department). Today there is a greater recognition of the interconnected nature of security requirements through an approach variously known as holistic security. It also appears that the concepts of safety and security are interdependent.

A table in annex 2 summarizes the declination of the Security from the governance to the crisis management.

The threats for the national security, the corporate world and the industrial organisations have significantly increased by bearing many aspects (international terrorism, communalism, strikes, sabotage, espionage, subversion, thefts, cyber & white collar crimes, bomb threats, natural and manmade disasters etc…). Authorities often are unable to predict disaster and protect corporate, industry and business resulting in colossal avoidable losses.

Thus, industrial security has become an all-pervasive management function of asset protection, loss prevention and crisis management (cf. figure 4)

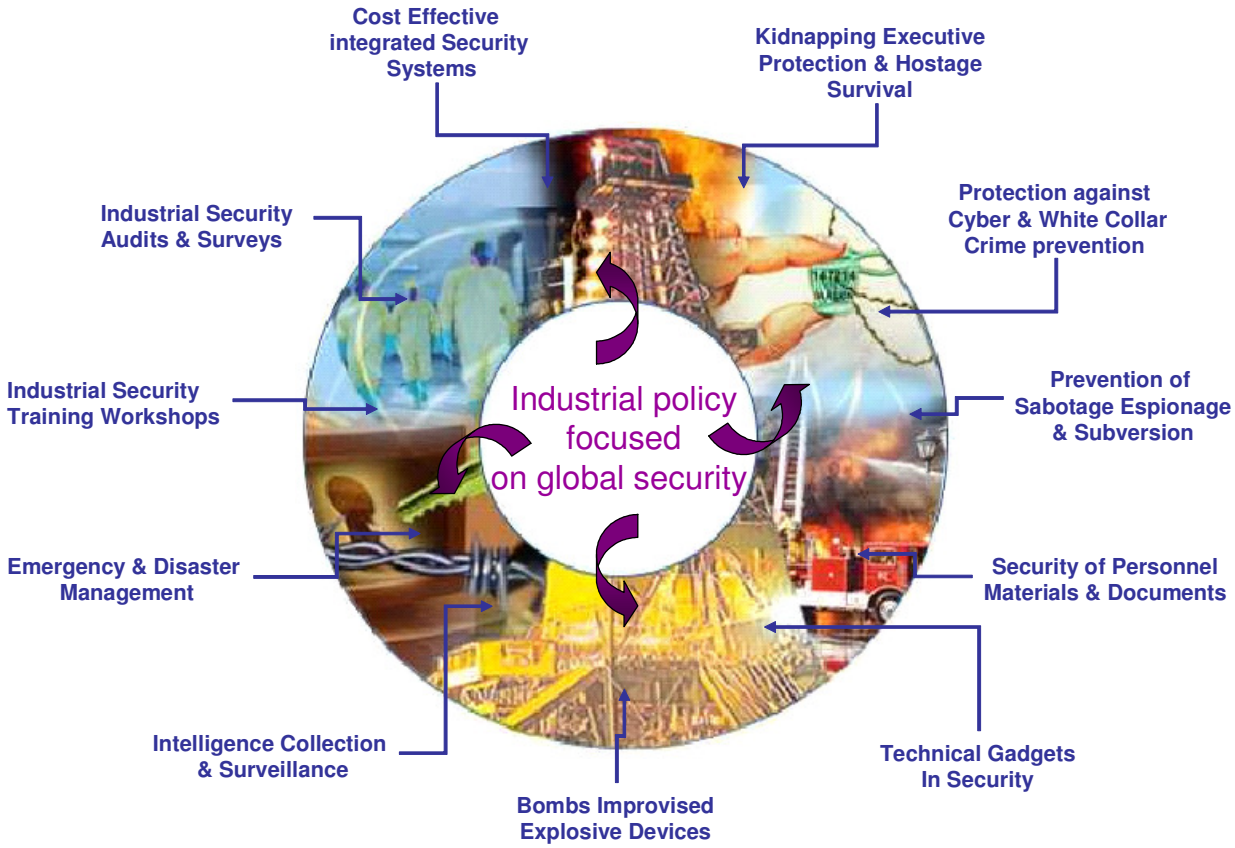


Figure 4 – Taking into account of threats in the global security approach which is integrated to the general policy of the companies.

4.5. SMS Harmonization for urban guided transport system

As a part of SMS, the figure 5 presents a proposal to harmonize the approval process of urban guided transport. The figure 5 also highlights 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 to an external safety entity in order to realize the safety study and to write the safety case (which concerns the technical aspects of the system).

The operator provides a SRS to the manufacturer. This last one redacts the safety case, system documentation (with or without the help of a safety entity (ISA)). But beyond the purely related to safety aspects, there are exchanges between

manufacturers and operator for other criteria such as performance, comfort, cost, which could impact on safety.

Once checked by the operator, this last one submits a safety case for operation (this document integrates the procedures, management aspects, etc…) to the legal authority that can allow the start-up of the system. In the same way, during the commissioning phase, the same relational schema is applied but in performing tests on the system under normal operating conditions and degraded modes.

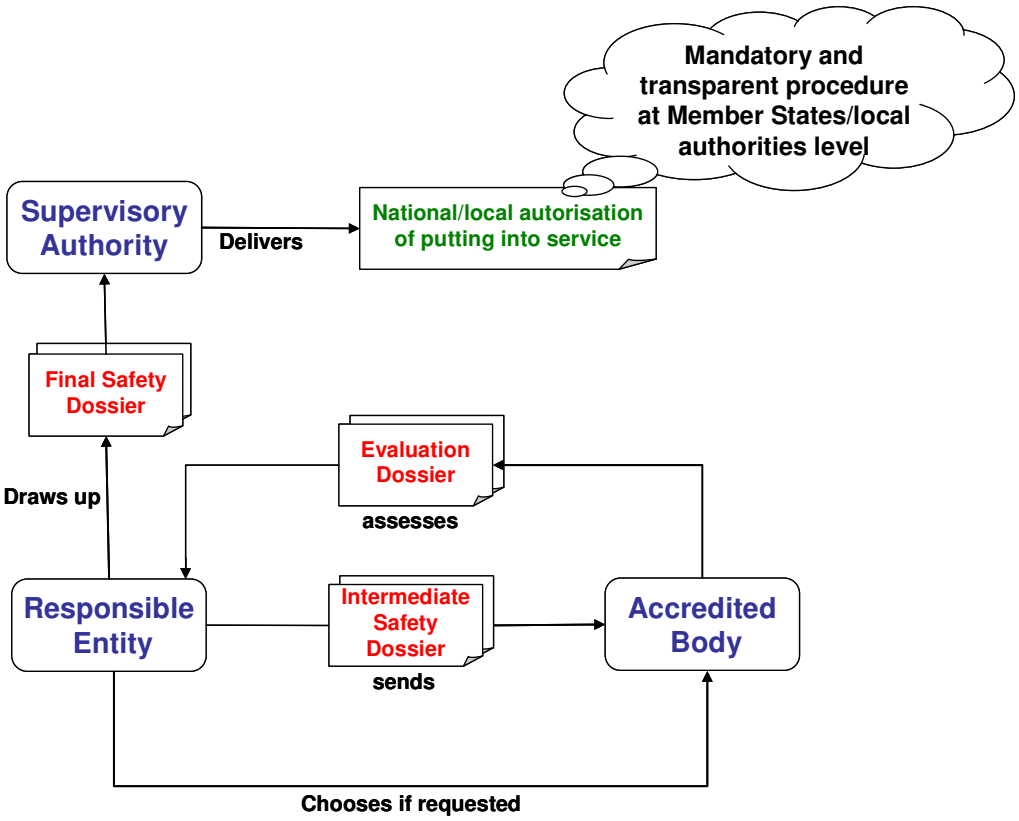


Figure 5 – Proposal of a generic approval process

As for product to be placed on the European market by manufacturers, 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.

This brief presentation can be an input for the MODSAFE Deliverable D6.1.

5. Involved parties and responsibilities

The introduction of SMS means to define relationships between different key players and their responsibility at each stage of the lifecycle. The next two sections detail the different actors and their tasks and responsibility in the lifecycle of, in the first section, the European railway system and, in the second section, urban guided transport system. Depending on the country we can find key players like the following.

5.1. Key players for the interoperable European railway system

Notified Body (as an independent safety assessor)

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 met).
- Examination of the design (the notified Body will assess the full design dossier 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).
- Validation (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 put 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).

Independent safety assessor (ISA) :

The Independent Safety Assessor role (known as "functional safety assessment") is part of IEC 61508 (IEC 1998) and its declination (in particular EN 50128/50129 for the railway field). The ISA also has an important role in the railway sector, where best practice as detailed in the Yellow Book (Railtrack 2000, RSSB 2003) and in CENELEC 50128/50129 standards 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 but automotive manufacturers see it as protection; in railway field, the ISA is request to help manufacturers to redact the safety case with a technical point of view.

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); in EN 50128/50129 and in 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 that they are sheltered as far as practicable from pressure to modify their opinion, and 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 transport, 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 apply 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.

Investigation body
Each Member State shall ensure that investigations of accidents and incidents referred to in Article 19 are conducted by a permanent body, which shall comprise at least one investigator able to perform the function of investigator-in-charge in the event of an accident or incident. This body shall be independent in its organisation, legal structure and decision-making from any infrastructure manager, railway undertaking, charging body, allocation body and notified body, and from any party whose interests could conflict with the tasks entrusted to the investigating body. It shall furthermore be functionally independent from the safety authority and from any regulator of railways.

Infrastructure Manager (IM)
Any body or undertaking that is responsible for establishing and maintaining railway infrastructure which may also include the management of infrastructure control and safety systems. Current infrastructure managers in the EU are companies like network Rail in the UK, Pro-Rail in the Netherlands and departments within national railway organisations such as DB and SNCF.

Railway Undertaking (RU)
Any public or private undertaking licensed according to applicable community legislation, the principle business of which is to provide services for the transport of goods and/or passengers by rail with a requirement that the undertaking must ensure traction; Business referred to as 'Trains Operating Companies' in the UK and Netherlands are typical examples of railway undertakings.

5.2. Key players for urban rail systems

Although there is no European harmonized process for certification and operation concerning urban guided transport system with regard to safety, it appears that the use of EN 50126/8/9 standards and safety policies (ALARP or GAME) for these type of systems is common. Globally operators establish the safety targets for bringing new systems into service. Manufacturers and suppliers are responsible for performing safety studies and for writing for their products the safety case which is the documented demonstration that the product complies with the specified safety requirements. This last document is the reference between the different key players (either during the design phase or the commissioning phase). The means to demonstrate that safety objectives are achieved are at the discretion of the manufacturer/supplier.

6. Human Factors Integration

With respect to rail accidents, analysis showed that the major causes of accidents are caused in large part by Human error (and more generally Human factors). The standards, regulations on guided systems safety are mainly focused on technical and technological aspects of this type of systems by systems, by bypassing completely Human aspects. It is therefore necessary to explore ways of integrating Human factors in the regulation and standardization.

6.1. Analysis and prediction of Human errors on procedure application

A definition of Human reliability may be associated to the technical reliability, i.e. it is the capacity of the Human operators to achieve correctly their allocated functions, in given conditions and on a given interval of time. Nevertheless, different adaptations of such a definition occur in literature. Some authors prefer defining Human reliability as the capacity of Human operators to achieve their allocated tasks instead of speaking on functions. The function concept is then related to the system mission whereas the task concept relates to the Human factor contribution to achieve the mission. This task may be more or less detailed. It can be only an objective, i.e. to supervise a process, or a very detailed procedure, in this case the task leads to the definition of a prescribed behaviour. For these reasons the Human error can be identified by the comparison between:

- the prescribed behaviour with the observed one, or
- the expected performance or result with the obtained one.

Some authors consider that Human operators are unreliable if and only if they do not achieve recovery actions of erroneous tasks. The Human reliability concept is sometimes confused and assimilated to the technical availability, i.e. it is the capacity of Human operators to be ready to achieve their allocated tasks, in given conditions and at a given time. Moreover, related to the Human reliability, the technical maintainability can be associated to the capacity of the Human operator to recover their own erroneous tasks or to maintain their own knowledge. Those characteristics cannot be applied to technical components for which the definitions of reliability, availability, maintainability or safety (i.e. RAMS concept) do not consider the possible evolution of their knowledge and the possibility not to respect voluntarily any prescriptions! Human operators, on the other hand, are able to decide to modify given prescribed tasks, to create new tasks or not to achieve tasks. Therefore, the following definition of the Human reliability adapted from Swain and Guttmann (1983) [11] might be applied for designing systems taking into account possible Human error occurrence and consequence. The Human reliability is then the capacity of Human operators:

- To achieve correctly their prescribed tasks, in given conditions, during an interval of time or at a given time,
- Not to achieve any additional tasks that may damage the Human-machine system, this damage may be associated to many criteria such as safety, quality, production, workload, etc.

The Human error concept is the complementary of the reliability one. Therefore, it relates to the capacity of Human operators:

- Not to realize correctly their allocated tasks in given conditions during a period of time or at a given time, or
- To realize additional tasks that may affect the Human-machine system functioning in terms of safety, quality, production, workload, etc.

Even if several quantitative or cognitive methods exist to assess and predict Human errors, they present operational limits ([5], [7], [8], [9], [10], [12], [13]):

- The results they give are not homogeneous. Studies have shown that a given method used by several groups or different methods used by a same group do not produce reliable results.
- The Human behavioural model they use is sometimes difficult to apply.
- The Human error based risk analysis process made by the designers, the users or the employers of a given Human-machine systems can diverge because of their different objectives or different organisational or individual interests they take into account.
- The analysis of the tasks does not integrate all the dependencies between tasks (e.g. temporal dependencies, causal dependencies, functional dependencies).
- They focus mainly on the analysis of non-intentional errors without taking into account intentional errors such as violations or additional tasks.
- They are off-line processes without taking into account the on-line risk control process requirements made by the Human operators on field.
- The feedback to assess the Human error probability is insufficient.
- Even if probabilities on Human errors are available, they usually cannot be compared because they do not have homogeneous assessment unit.
- The process of Human error analysis is much more a retrospective one than a prospective one. Instead of focusing on the incident or accident prevention, the investigation effort related to Human errors is done after the occurrence of a danger due to Human factors.
- The databases on accidents or incidents focus mainly on the negative contributions of the Human operators reporting their errors without taking into

account the possible positive ones, i.e. the contribution of Human operators to avoid or recover an incident or an accident.

- Human error assessment is done without taking into account the dynamic evolution of the Human-machine system, e.g. the learning effect. These methods do not consider that the system users who have to analyze the risks they are facing to and who have to control them on-line can learn from their own errors and behaviours.

Despite these problems, some supports can be used to prevent and protect urban guided transport systems from these Human errors and against consequences of these errors. Three of these supports are mentioned hereafter:

- Even if the results given by the method of assessment of the occurrence or the consequences of Human errors are not homogeneous, they can be used to compare several Human erroneous behaviours. The errors of calculation occur for all the analyzed behaviours. Therefore, the results are comparable.
- Studies on simulation to verify hypotheses on Human error occurrence and consequences, to study the genesis of hazardous scenarios or to propose situation awareness based programs for future staff.
- Analysis of incident and accident regarding national reporting systems. A joint framework for analysis non-conformity events involving Human factors may be useful for identifying the contribution of the staff on safe and unsafe event occurrences.

6.2. Railway barriers and barrier efficiency (for urban or not urban systems)

The deliverable D128 of the MODURBAN project proposes a combined approach to assess the barrier efficiency [6]:

- The THERP method is used to compare the probability of success of a prescribed procedure and possible erroneous ones involving barrier removals, i.e. non respect of barriers,
- The ACIH method is used to compare all the erroneous procedures in terms of benefits, costs and possible deficits or dangers regarding the prescribed procedure that is the referential situation.

Table 1 - THERP and ACIH methods to assess the efficiency of barriers

	Prescribed procedure: N barriers are respected	Erroneous procedure 1: respect of N-1 barriers upon N	Erroneous procedure 2: respect of N-2 barriers upon N	Erroneous procedure 3: respect of N-3 barriers upon N	…
THERP	Probability of success	Probability of success	Probability of success	Probability of success	…
ACIH	Reference situation	Benefits, Costs, Deficits	Benefits, Costs, Deficits	Benefits, Costs, Deficits	…

For instance, the train speed procedure involved several barriers and elementary tasks such as:

- Speed signal (80) perception,
- Speed signal (80) interpretation,
- Button action (slowing down),
- Sound perception if the speed is not respected,
- Sound interpretation,
- Zone signal (Z) perception,
- Zone signal (Z) interpretation.

The driver works to degraded procedure: the two first barriers, i.e. the speed signal and the sound signal are removed and only the last Z barrier is respected.

The probabilities of success p(S) and failure p(F) calculated with THERP for the speed procedure in normal mode are: p(S) = 0,99900 and p(F) = 0,00100. The probabilities of success and failure calculated with THERP for the degraded speed procedure (i.e. by respecting only the Z signal) are: p(S) = 0,99790 and p(F) = 0,00210. This degraded behaviour can generate a benefit in terms of time delay without any additional deficit or danger because the last signal is respected.

Such feasibility study for assessing Human error probability or for analyzing Human erroneous actions might be used for managing a global risk analysis process integrating both technical and human factors. This might concern different system lifecycle steps and might be applied not only for operational tasks such as driving or supervisory tasks.

6.3. Procedure validation: simulation and technological platforms

The use of simulators (cf. figures 6, 7, 8, 9) can be an efficient way to validate future operating systems and to analyze the impact of new technologies on the Human behavior.

Regarding European interoperable rail system, the TRANSPAL micro-world was used to study the feasibility of human errors such as violations or barrier removals by using the BCD model framework [14]. The human errors were then analysed in terms of benefit and cost (i.e. acceptable loss) and of potential deficit (i.e. unacceptable loss) when the human erroneous behaviours may cause a failure. This analysis was a multi-criteria based analysis and has taken into account the safety criterion, the quality of transport services (i.e., respect of the time scheduling), the respect of the stops at stations (i.e., the respect of the passengers' flow in stations) and the human workload (i.e., the number of interactions with the control interface).

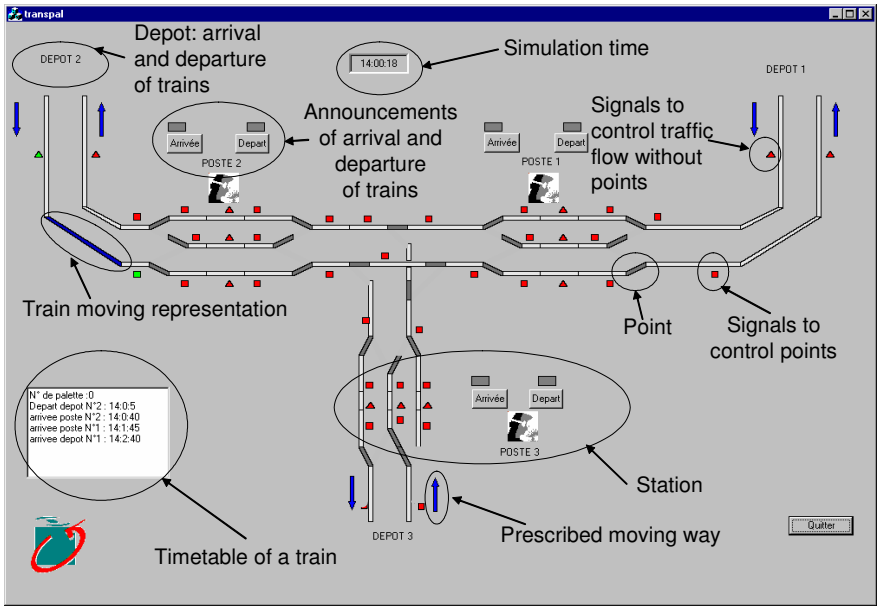


Figure 6 - The micro-world TRANSPAL to simulate the railway traffic flow control activities and used in the UGTMS project

The experimental platform ERTMS (cf. figure 7) developed at INRETS Villeneuve d'Ascq simulates a train (freight or passengers) for various driving modes in the framework of ERTMS and traffic supervision.

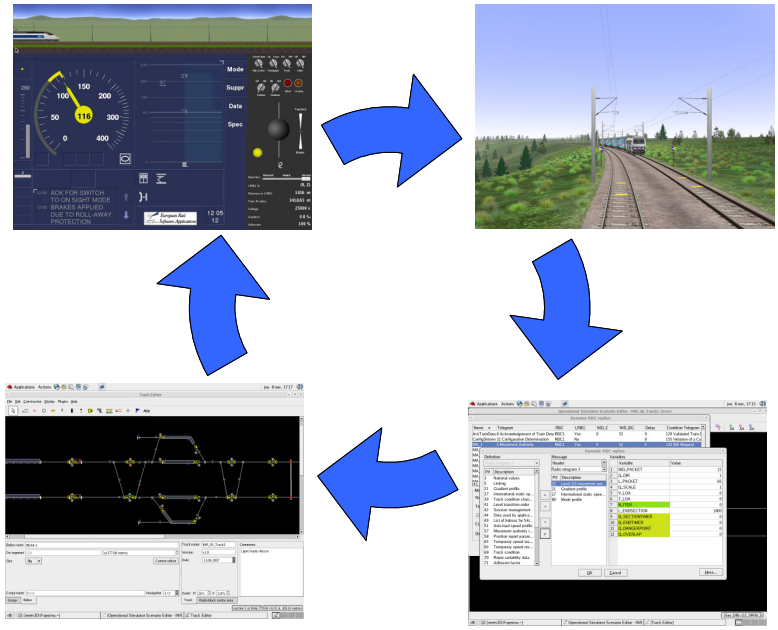


Figure 7 - ERTMS Simulator

Another experimental platform SPICA-RAIL (cf. figure 8), addressing both urban or non urban rail systems, and developed at the University of Compiègne simulates an automated train supervision process and aims at studying the Human behavior interacting with such a process [4].

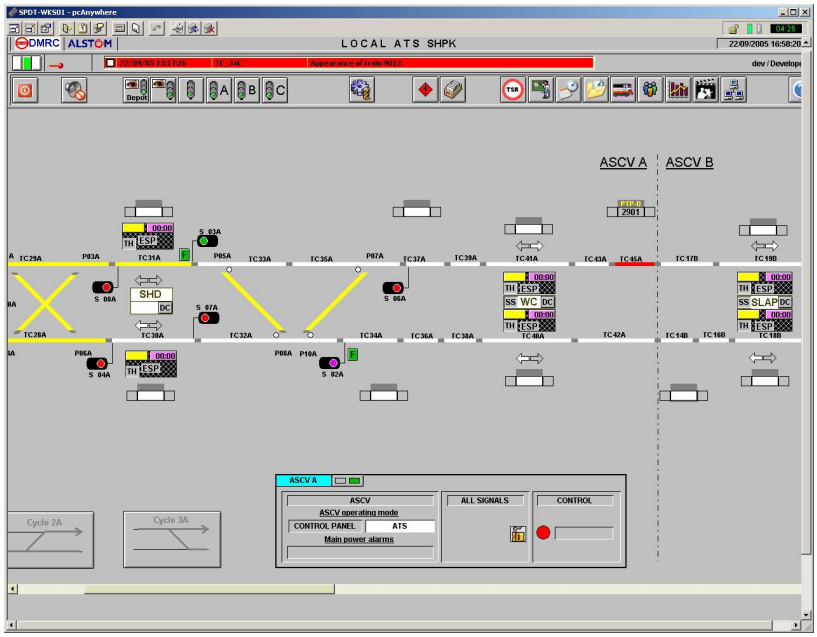


Figure 8 - The SPICA-RAIL Simulator

Regarding urban rail systems, the experimental platform COR&GEST (cf. figure 9) developed at the University of Valenciennes, aims at simulating the train driving and supervision tasks for tramway, suburban train and metro. Experiments are organized in order to study Human reliability with or without disturbances [14].

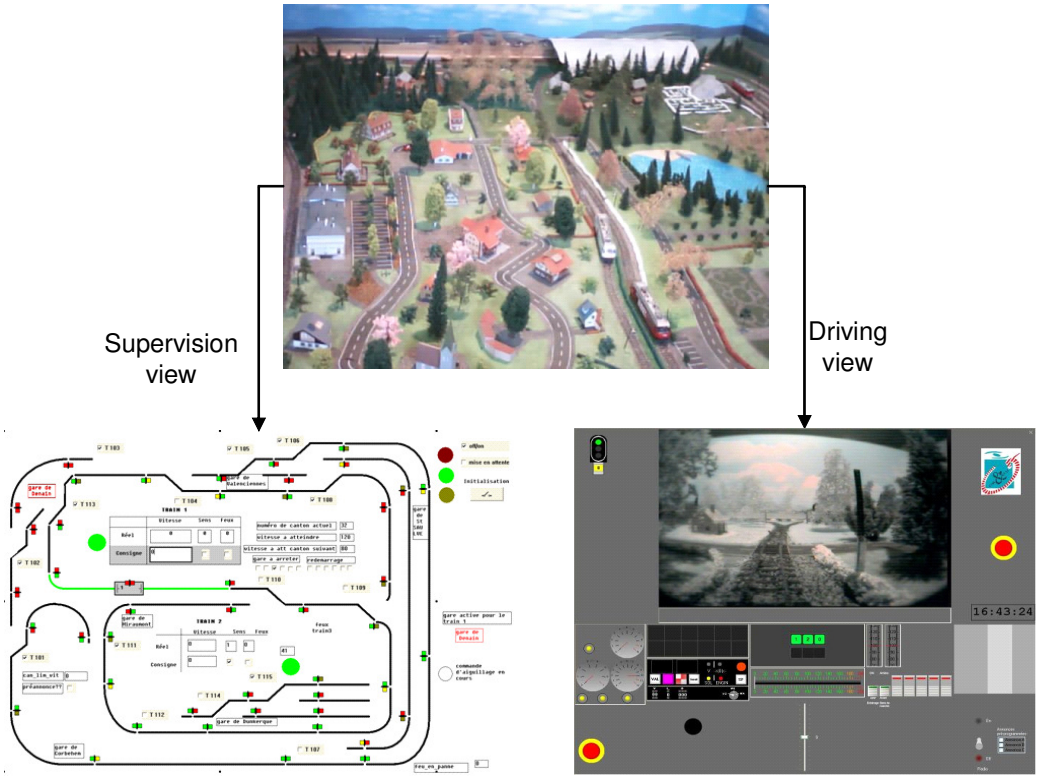


Figure 9 - The COR&GEST platform to simulate the railway control and supervision activities

6.4. Incident or accident analysis involved erroneous procedure application

As for the interoperable European Rail system, organizations have been set up at national level by European legislation to deal with safety analysis. These organizations receive the safety analysis reports related to the unsafe events that occurred on field and are a basis for operational retrospective analysis to identify the impact of Human factors on the system safety management.

These organisms also produce annual safety reports that may be useful to validate the probability assessment of Human errors.

Other European organisms have in charge national registration and investigation of incident or accident reports, Table 2.

Table 2 - List of national organisations in charge of safety and of registration and investigation on accidents or incidents [source: works done by ERA to identify the safety units of European countries].

Country	National Safety Authority/Website	National Investigation Body/Website
France	Etablissement Public de Sécurité Ferroviaire *www.securite-ferroviaire.fr*	BEA-TT Land Transport Investigation Body *www.bea-tt.equipement.gouv.fr*
UK	Office of Rail regulation (ORR) *www.rail-reg.gov.uk*	Rail Accident Investigation Branch *www.raib.gov.uk*
AUSTRIA	Bundesministerium für Verkehr, Innovation und Technologie *www.bmvit.gv.at*	Unfalluntersuchungstelle des Bundes *http://versa.bmvit.gv.at*
BELGIUM	Service Public Fédéral de Mobilité et Transports Service sécurité ferroviaire *www.mobilit.fgov.be*	Service Public Fédéral de Mobilité et Transports *www.mobilit.fgov.be*
GERMANY	Eisenbahn-BundesAmt (EBA) *www.eba.bund.de*	Eisenbahn-BundesAmt (EBA) *www.eba.bund.de*
ITALY	Ministero dei Trasporti – Dipartimenti per I trasporti Terrestri – Direzione Generale del Trasporto Ferroviario *www.infrastrutturetrasporti.it*	Railway Safety Commission *www.infrastrutturetrasporti.it*
NORWAY	Norwegian Railway Inspectorate *www. sjt.no*	Havari Kommisjonen *www.aibn.no*
THE NETHERLANDS	Railway Safety Authority *www.ivw.nl*	The Dutch Safety Board *www.safetyboard.nl*
GREECE	Ministry of Transport and *www.yme.gr*	Federal Railway Authority *www.yme.gr*
SWEDEN	Swedish Rail Agency *www.jvs.se*	Swedish Accident Investigation Board *www.havcom.se*
SPAIN	Ministerio de Fomento *www.mfom.es*	Ministerio de Fomento *www.mfom.es*
PORTUGAL	INTF (Instituto Nacional do Transporte Ferroviário) *www.intf.pt*	INTF (Instituto Nacional do Transporte Ferroviário) *www.intf.pt*

POLAND	Urzad Transportu Kolejowego *www.utk.gov.pl*	Urzad Transportu Kolejowego *www.utk.gov.pl*
HUNGARY	HASB *www.hasb.hu*	HASB *www.hasb.hu*
CZECH REPUBLIC	Drážni úrad (Rail Authority) *www.du-praha.cz*	Drazni Inspekce (The Rail Safety Inspection Office) *www.dicr.cz*

6.5. Maintenance and modifications impact

6.5.1. Human errors and maintenance process

6.5.1.1. Examples in aeronautics

From 1988 to 1997, amount 1 472 accidents, the contributions of human error in maintenance to the occurrence of accidents or incidents are about 20% per year [23].

These maintenance related accidents are due to several causes such as:

- Installation
- Maintenance inspection
- Annual inspection
- Repairing
- Adjustments
- Design change
- Replacements
- Overhaul

The main causes of the maintenance related accidents are the installation problems. Different types of errors of installation may occur:

- A wrong part relates to the installation of a part of the system that does not comply with the manufacturer's specifications or any supplementary service bulletins.
- The reversed installations are the installations of some components that are cross-connected or reversed.
- The incorrect attachment relates to improper installation.
- The omission relates to installations that did not include a required component.
- Incorrect connection relates to installations involving the logical system flows.

6.5.1.2. Examples in nuclear power plants

From 42% to 65% of human performance problems occur during maintenance. More than 50% of potential serious events occurrence are due to maintenance errors [24]. They are mainly errors such as omissions of maintenance actions (e.g., repairing, modification, testing, calibration, inventory control).

6.5.1.3. Examples in rotary press control

This study concerns the use of a rotary press and relates to the observation and the analysis of deviated behaviors of human operators on the spot [8].

37 human errors were observed and analyzed and 7 of them concerned maintenance process. The maintenance based human errors are called system migrations resulting from maintenance problems or constraints.

For instance, the quality process of current productions was affected because cleaning operations were omitted during the previous ones. Another example relates to some operations during the running of the production.

Human operators are not allowed to intervene into the rotary press during functioning. Sometimes, they do not respect this rule in order to avoid an interruption of the production and a loss of time due to potential maintenance operations. For instance, they operate on some blocked or failed components of the machine whereas rolls and cylinders are moving in high speed in order to avoid an intervention of the maintenance services that oblige them to stop the machine and sometimes to wait for a long period of time.

6.5.2. Toward the management of Human errors in maintenance

Maintenance procedures may interact with operation ones and facilitate the occurrence of human errors. For instance, rail speed restrictions are due to several reasons:

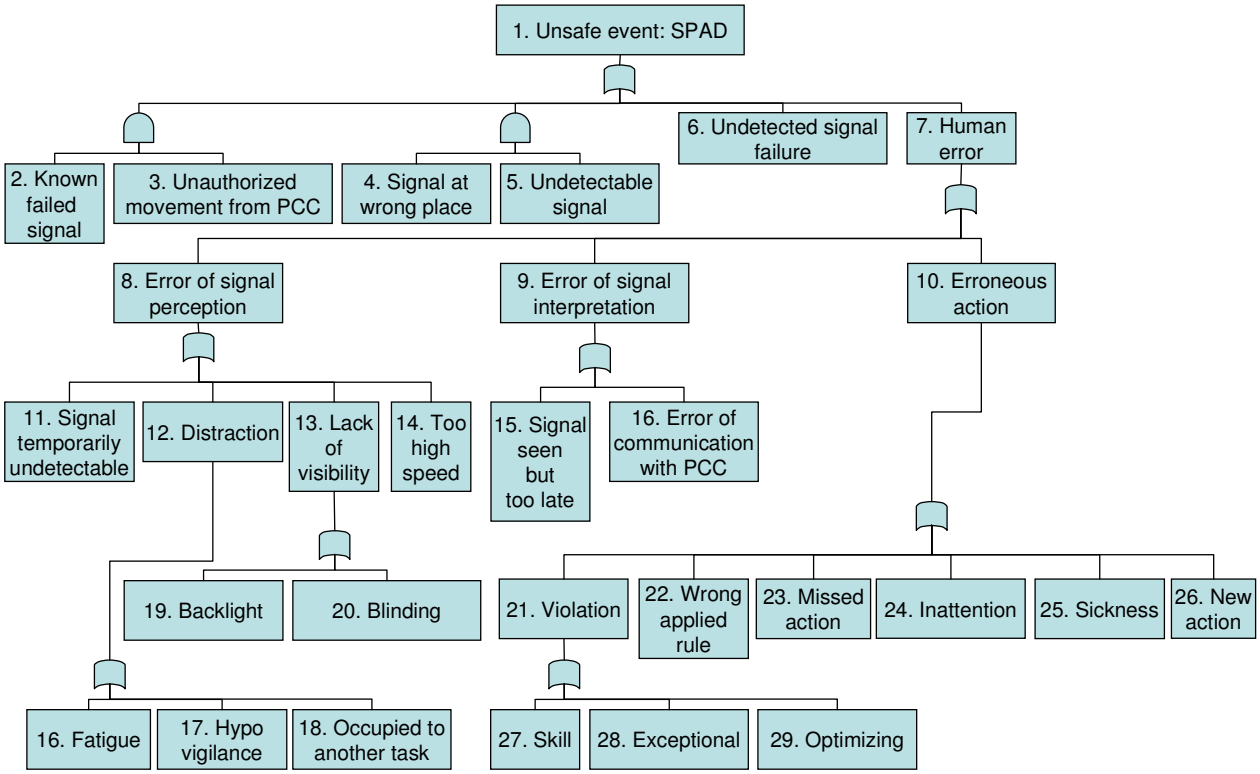
- The permanent speed restrictions relate to track curves or some existing infrastructure conditions on a particular section of a track.
- The temporary or emergency speed restrictions relate to track maintenance work or temporary track failure conditions.
- The conditional speed restrictions relate to train route setting at a junction or station and the signalling system characteristics.

A human error in maintenance works may degrade the operational functioning of trains.

Furthermore, some maintenance errors may affect future operation procedures. For instance, with regard to the accident at the “Notre Dame de Lorette” station in Paris, the train was driven manually because the ATO system had been in maintenance for several days.

When safety based barriers are set up to control dangerous events, they can be removed voluntarily in order to damage the system: this affects the security of the transport system. All the identified scenarios that may affect the safety system could then be a basis for system security based analysis and control.

For instance, considering the occurrence of an undesirable event such as a SPAD that may lead to a potential accident, the specification of technical barriers, maintenance procedures, training program, human competence control procedures, or operation procedures is required in order to avoid the occurrence of the events generating a SPAD or to limit their consequences relatively to a safety based viewpoint, Figure 10. On the other hand, from a system insecurity point of view, the occurrence of a SPAD becomes the objective to be achieved and facilitated: some means can be developed in order to damage the system functioning.



References of the event	Positive view (without the intention to damage): to control safety	Negative view (with intention to damage): to provoke insecurity
2+3	Optimization of the maintenance of the communication systems	Degradation of the communication systems
4+5	Optimization of the infrastructure design and maintenance	Degradation or modification of the infrastructure
6	Improvement of the on-line failure detection and diagnosis	Avoidance of failure detection
7	Improvement of human competences	Degradation of human competences
…	…	…

Figure 10 - Example of a security and safety based analysis for a SPAD occurrence (adapted from [25]).

As maintenance may interact with operation and may affect system safety and security, three levels of future investigations may therefore be developed:

- Impact of maintenance procedure errors on operations. Some maintenance error consequences are latent because their detection are delayed and then may affect the normal operational functioning.
- Coherences between maintenance procedures and operation procedures. Sometimes, maintenance procedures relate to and/or affect partial operational objectives e.g., regulation of depot; management of the works on tracks, etc.)
- Human factors impact on maintenance for safety and security controls. Some security affecting scenarios may be similar to the safety affecting ones, except that the intention of the actors differs. Indeed, the safety based analysis process aims at identifying unacceptable unsafe scenarios and at proposing

technical or immaterial tools such as physical barriers or procedures in order to make these scenarios acceptable. The intentional removals of such safety barriers may then affect the system security when these removals are done in order to damage the system.

7. Accidents and incidents (including Security) analysis environment

7.1. European interoperable railway system

The railway Safety Directive (SD) [16] requires that the safety performance of the member state railways and at the EU level be monitored and reported regularly, and for this purpose it has identified a set of Common Safety Indicators (CSI). A tentative list of CSI is given in Annex I of the SD. The IM and RU will have to collect data on these indicators and use them to prepare their yearly safety performance reports. Safety indicators are essential for monitoring safety performance of individual organisations such as IM and RU, of the member state railways or of the EU railways as a whole. The annex 1 of railway safety directive defines a list of events and elements to be recorded in the database. They are related to:

7.1.1. Indicators relating to accidents

1. Total and relative (to train kilometres) number of accidents and a break-down on the following types of accidents:
- collisions of trains, including collisions with obstacles within the clearance gauge;
- derailments of trains;
- level crossing accidents, including accidents involving pedestrians at level crossings;
- accidents to persons caused by rolling stock in motion, with the exception of suicides;
- suicides;
- fires in rolling stock;
- others.

Each accident shall be reported under the type of the primary accident, even if the consequences of the secondary accident are more severe, e.g. a fire following a derailment.

2. Total and relative (to train kilometres) number of persons seriously injured and killed by type of accident divided into the following categories:
- passengers (also in relation to total number of passenger-kilometres);
- employees including the staff of contractors;
- level crossing users;
- unauthorised persons on railway premises;

- others.

7.1.2. Indicators relating to incidents and near-misses

1. Total and relative (to train kilometres) number of broken rails, track buckles and wrong side signalling failures.

2. Total and relative (to train kilometres) number of signals passed at danger.

3. Total and relative (to train kilometres) number of broken wheels and axles on rolling stock in service.

7.1.3. Indicators relating to consequences of accidents

1. Total and relative (to train kilometres) costs in euro of all accidents where, if possible, the following costs should be calculated and included:
- Deaths and injuries;
- Compensation for loss of or damage to property of passengers, staff or third parties – including damage caused to the environment;
- Replacement or repair of damaged rolling stock and railway installations;
- Delays, disturbances and re-routing of traffic, including extra costs for staff and loss of future revenue.

From the above costs shall be deducted indemnity or compensation recovered or estimated to be recovered from third parties such as motor vehicle owners involved in level crossing accidents. Compensation recovered by insurance policies held by railway undertakings or infrastructure managers shall not be deducted.

2. Total and relative (to number of hours worked) number of working hours of staff and contractors lost as a consequence of accidents.

7.1.4. Indicators relating to technical safety of infrastructure and its implementation

1. Percentage of tracks with Automatic Train Protection (ATP) in operation, percentage of train kilometres using operational ATP systems.

2. Number of level crossings (total and per line kilometre). Percentage of level crossings with automatic or manual protection.

7.1.5. Indicators relating to the management of safety

Internal audits accomplished by infrastructure managers and railway undertakings as set out in the documentation of the safety management system. Total number of accomplished audits and the number as a percentage of audits required (and/or planned).

7.2. Urban guided transport

In urban guided systems, currently, there is not a common tool which is used by all European countries to record accident and incident. Each country has an internal

system used for collecting the information about non-conformity events, for analysing the data and monitoring the implementation of the resulting recommendations and corrective actions. In particular the form that is utilised for inserting the data about occurrences is somewhere a paper form, somewhere an electronic form and has a different structure in each country.

This section describes the preliminary research conducted on the "non-conformity event reporting systems" used by the MODURBAN Operators, and in particular it focuses on three major aspects of the reporting systems:

- Type of general information recorded
- Classification of the event
- Classification of the causes

According to D88 MODURBAN deliverable [15] two reporting systems were analysed:

1. ERIF-Electronic Incident Reporting Form used by LU for reporting Metro non-conformity events and the INCA-Incident Capture & Analysis data base.
2. NEFERTARI, which is the system used by RATP to report non-conformity events related to regional express trains. NEFERTARI has basically the same architecture of OSIRIS, which is the RATP Urban Metro Reporting System.

7.2.1. French metro network database:

Methodology of data collection

Decree STPG 2003-425/9 May 2003 ***(safety guided transportation):***
Article 41 of this STPG decree describes the formalisation of the synthesis of the safe operation events: "The organizing authority of transport forwards annually a report about the safety of system operation to the prefect of the department where the system is located. "

This article indicates that the annual reports of the operation are established by the operators and, for most networks, submitted to the BIRMTG (Bureau Interdépartemental des Remontées Mécaniques et des Transports Guidés) by the organizers authorities. In addition to the annual reports, article 39 of Decree STPG requires that "Significant events" related to safety are reported to the supervisory authority: "Any significant event related to security is covered immediately by the operator to the knowledge of the prefect of the department where the system operates. This information includes the sequence of the event and its severity. The operator sends a report on the event to the prefect and to the transport organizing authority within two months from the occurrence or discovery of the event. The report examines the causes and consequences of this event found, the risks potential and indicates the lessons that have been learned and measures taken

to prevent its renewal. The Prefect may require the operator to analyse any significant event related to security of which he has knowledge. In all cases provided by this article, the prefect may request any additional information»

List of events

The events included in the reports of safe operation are (generic list):
- Collision between train
- Collision with fixed barrier
- Derailment
- Panic
- Fire explosion
- Electrocution / electrifying
- Collision between a train and a person
- Beginning of a fire
- Tunnel evacuation
- system malfunctioning: system crash, power outage, ...
- rolling stock problem: aging of a component, assembly of a wrong element, mechanical failure ...
- Vandalism
- Other events: passenger falls, flood, ...

Example of RATP [15]

NEFERTARI is the reporting system used by RATP for the Regional Express network service. It uses an electronic standardised form to enter and record information about non-conformity events.

The 'data entry form' is divided into two main parts.
The first part records the general information about the occurrence, such as date, time, location (track, station, inter-stations, previous station). Then, the type of event is selected from a drop down list (operational incident, rolling stock failure, fixed installation failure, crime, passenger minor injury…). Finally, the data about the delay are recorded in this first part of the form as well.

The second part of the 'data entry form' makes use of pre-established sentences on scroll menu, which avoid subjectivity and foster standardisation. This criterion is used for developing the text/description about the event, its causes, actions taken, consequences, complementary information ("free text") and comments.

Risk Management Tool

RATP has implemented an operational tool to steer transport risks management, the so-called "Tableau de bord d'Alerte des Dangers" (or hazard alert monitoring

dashboard). This monitoring dashboard is prepared every month and periodically reviewed with operation and maintenance departments at a railway safety observatory meeting.
This tool is effectively operational for metro and RER operations. Tests are also being run for tramway operations. The hazard alert monitoring dashboard is also progressively expanded to include new data. Relevant data are those that are the precursors of incidents. They are drawn from the whole range of protection measures put in place to ensure that the level of risk associated with our transport systems remains acceptable. The principle is to anticipate incidents-collision, derailment, people being run over by a train, electrical contact, fire, panic, etc., by analysing data relevant to safety and by putting in place specific measures for those systems whose data have moved out of the safety range.
Eventually, once validated, the necessary data will be directly provided from NEFERTARI and OSIRIS. Complementary data will also be provided by maintenance activities.

Additional Comments
Within both its reporting systems, i.e. NEFERTARI and OSIRIS, the RATP operational structure is involved at various levels in both inputting (lower tiers), but also in validating (management tiers) the information which has been inputted. It is obvious that following the importance of the event (i.e. incident or accident) the time for validation approvals depends on the proactive involvement of all tiers at stake. Specific interventions by police fire departments, justice may be required in the most serious cases Standardisation of language is of the utmost importance for day to day incidents solutions and corrective action implementation. The level of specificity of serious happenings does definitely require additional reporting/validation provided from elsewhere under a complementary responsibility.

Given the operational features of each line, the systems at stake are to be only considered as tools. The importance and the quality level of operations shall always remain primarily dependent on the appropriation of the reporting requirement by operators. This should be guiding principle in devising such a tool, which is by essence both internal-structure dependent, and external-environment subjected.

7.2.2. London Underground Incident database

In LU, different integrated systems than for mainlines railway are used for collecting the information about non-conformity events, for analysing the data and monitoring the implementation of the resulting recommendations and corrective actions.

First, different forms are used to record details of incidents and capture the findings of immediate investigations:

- IRF-Incident reporting Form
- RWIIF-Record of Workplace Injury or Illness Form

- SPAD-Signal Passed at Danger
- SARF-Staff Assault Report Form

All incidents, including those relating to contractors, shall be recorded on an IRF, at the very earliest opportunity, by the person responsible for the location or activity giving rise to the incident. Recently, the paper-based forms listed above have been replaced by the EIRF database. The paper versions are only used in the case of a failure of the EIRF System.

Second, INCA(Incident Capture and Analysis) database is used to capture, classify and analyse safety related incidents data, which have been obtained through the IRF suite of forms.

Third, the LUSATS(London Underground Safety Action Tracking System) database is used to ensure that all major safety issues affecting the LU group are addressed in a controlled and coordinated manner and to provide a clear traceable audit trail from initial decision making thorough to the assured close-out of an issue. It tracks the progress of any safety related workstreams.

Then, CIRAS(Confidential Incident Reporting and Analysis System) is also used. "CIRAS is for front line railway staff to report safety concerns that they feel unable to report through normal company channels. It offers a completely independent and confidential way to report those concerns without fear of recrimination" [http://www.ciras.org.uk/index.aspx]. It is now compulsory, for all UK rail companies to be involved in a confidential reporting system. In 2000, CIRAS became a National System and has since received over 3000 reports. For more information see the CIRAS WEB page. CIRAS is independent of INCA and may happen any time after the incident occurs.

Finally, the whole LU reporting system is aligned with RIDDOR, (Reporting of Injuries, Diseases and Dangerous Occurrences Regulation) which is a Health & Safety Executive (HSE) Regulation.

INCA –(Incident Capture and Analysis)

The INCA system, used by LU, uses an electronic standardised form to enter and record the information about the non-conformity events.
First, some general information about local and temporal setting is recorded in the Incident Nucleus area. In particular, the date, time, location, "sector" and area where the incident occurred are entered. The sector and area are selected from a drop down list. Then, a free text field is used to give details of where the incident happened.
Second, the event is described through a free text narrative and classified according to its primary cause.
Third, in case of injury, the "employee injury" area is filled in with information about the personnel (name, surname, sex, age at incident, service start date, grade start

date, grade) and the injury (status, severity, activity, method, Agent, Nature, Body Part, taken to hospital/first aid given/…). In case of "lost time injury", the "lost time" is recorded (absent start, absent end, day lost, shift lost). Another area is dedicated to collect the data about the "other people involved".
Then, for every incident involving fire/smoke alerts, the "fire report details" (fire category, fuel type, fuel description, ignition source, description) must be completed.
Finally, the INCA system records the data (local ref., completed, received) about the document type (for example, IRF or LPF-Loss of Process form…). INCA has recently been replaced by LUSEA.

7.2.3. German metro network database:

German laws

- Law on Transport Statistics (Verkehrsstatistik Gesetz, [Verk. Stat. G], last version 06112008), based on EU regulation 91/2003 and EU Regulation 1192/2003

- Law on Transport of Persons (Personenbeförderungsgesetz, [PBefG],version 07092007), with the Regulation on Construction and Operation of Tramways (Verordnung über den Bau und Betrieb der Straßenbahnen, [BOStrab], version 08112007).

§1 of the Law on Transport statistics stipulates:

To evaluate the structure and development of waterborne transport on the sea and inland waterways, transport of goods, airborne transport as well as the rail transport and the commercial transport of persons on roads statistical surveys are done on:
1. the traffic of ships, transport of goods and persons on the sea and on inland waterways (statistic on waterborne traffic),
2. the companies of the inland waterway transport (statistic of companies of the inland waterway transport),
3. the transport of goods on roads (statistic on transport of goods on the roads),
4. the enterprises of the transport of goods on roads (statistic on enterprises of the transport of goods on roads),
5. airborne transport (statistic on airborne transport),
6. the companies of airborne transport (statistic on companies of airborne transport),
7. Transport of persons with railways, metros, trams and buses (statistic on transport of persons),
8. the transport of persons on long distance railways (statistic on transport of persons on long distance railways),
9. the transport of goods on railways(statistic on transport of goods on railways),
10. the infrastructure of railways (statistic on railway infrastructure),
11. the accidents in railways transport (statistic on accidents in railway transport),

12. the traffic flow inside the railway network

as a federal statistic.

- In §21 Statistic on accidents in railway transport (Schienenverkehrsunfall- Statistik)
  - The statistic is done once per year
  - It includes number of accidents causing damages to persons or properties (objects)
  - It includes number of casualties (persons involved in an accidents), differentiated
    - Per mode of railway transport
    - Per kind of accident
  - Number of casualties (persons involved in an accident) differentiated by
    - Gravity of injury (light or heavy)
    - Persons being killed
    - Person subgroup
    - Type of involvement in transport

- § 24 The relevant authorities transfer to the regional statistic office (In German: Land) and to the federal statistic office the names and addresses of all Companies with licenses for operating transport of persons on railways. They transfer as well the information on companies whose licenses were withdrawn.

- § 27 The federal statistical office collects the data for the statistic

The Regulation on Construction and Operation of Tramways (Verordnung über den Bau und Betrieb der Straßenbahnen, [BOStrab],

Accidents are additionally reported on the basis of the Regulation on Construction and Operation of Tramways (Verordnung über den Bau und Betrieb der Straßenbahnen, [BOStrab],
§§ 7 and 8:

The entrepreneur has to appoint a “chief operating officer” (Betriebsleiter)
The “Betriebsleiter” has to inform the authorities immediately (without delay) about accidents where persons were killed or where substantial damages to properties or vehicles occurred.

He has to inform immediately the authorities as well about accidents and incidents causing public attention.

The information by the “Betriebsleiter” is done with special letters beginning with a form:
-Date
-Time
-N° of line
-N° of train in schedule
-Name of station
-Casualties (person in accident) Gender/ Age
-Short description of what happened
-Measures taken (quick acting brake yes/no; setting signal at danger yes/no; using short-circuiter for air pressure yes/no; using short-circuiter for power supply yes/no);
-Information about acting police and fire brigade (definition of the unit and arrival time).
-What about the person being injured/ grade of injury/ hospital (name)
-Transaction key n° of the police document
-Period of cut off of traction power
-Replacement of Rail transport by Bus

7.2.4. *Causes of the event*

1. According to the reporting forms and databases, the causes reported are only technical causes. Both LU and RATP stated that their systems take into consideration the Human Factors (HF) cause. However, we noticed that the HF issues are not mentioned in the forms and in the data bases. According to LU, they “do take account of Operator / Staff error but not the root cause of the error”.
2. In NEFERTARI, the RATP system, the general categories under which the event causes are classified correspond to different technical systems/devices/components, e.g. electrical system, braking system, etc. The system which failed is considered as the cause of the event.
3. In INCA, the LU reporting and database system, the list of possible causes is actually made up of causes (e.g. “alcohol related”) as well as consequences (e.g. “person injury” or “damage to personal property”) – these usually refer to the state of the passenger involved in the incident rather than the staff member. The list of causes in LU contains some items which actually describe the ‘type of event’ instead (e.g. “Escalator Incident”). As stated by the INCA experts in LU, “this list is something that has evolved over a number of years and as such represents both cause and consequence”.
4. The typology of causes to be taken into consideration (for example: active and/or latent cause) should be agreed. From our point of view, when a trend is identified, the analysis should surely focus on the latent causes as well.

The analysis of state of the arts shows that it is important to identify the following attributes associated with each event:

- Type and category of related accident or incident
- Person (or role) responsible for reporting the event (event owner), could be a staff of operator
- Structure of reporting:
  - How the event details should be recorded (by verbal, written or electronic means)
  - To whom the reports should be sent and copied
  - When reporting responsibility can be regarded as complete
- Event data:
  - Time and location of the event
  - Involved parties and individuals and their roles, such as passengers, staff, bystanders, etc.
  - Systems, structure or equipment that could be directly involved or effected by the event
  - Possible causes
  - Conditions and situations before the event and after the event
  - Normalising or reference data
  - Secondary events related to the event
  - Findings from the investigation
  - Corrective measures to avoid reoccurrence

Modurban consortium suggested in the deliverable D 88 [15] and D91 [17] to develop common database system that harmonises different European approaches for collecting information about non-conformity events in urban guided transport system and to develop learning approaches by sharing information.

7.3. Learning from accidents and incidents (both urban and non urban rail)

According to Andrew Hale's papers, there are three different uses of indicators to supervise the safety performance [18]:

1. Monitoring the level of safety in a system (whether that is a department, a site, or an industry)..
2. Deciding where and how to take action.
3. Motivating those in a position to take the necessary action to take it.

Learning from accidents, incidents and failures is a process applied in a large variety of forms in the urban transport. It is a recognised difficulty to directly and concretely identify the use of safety indicators in the learning approaches in the urban transports sector. The variety of the urban transport technological and operational mode in Europe requires the development of common understandable indicators to share experiences and to develop a high organisational learning from accidents and incidents [19]. Harmonised investigation and reporting systems have to be introduced to obtain robust, reliable and comparable data for international use.

The general requirements for data quality for learning are related to the following aspects:

- **Suitability** of the indicators to monitor and to check efficiency of a safety measure across the organisation structure.
- **Consistency** of the indicators to reflect the sufficiency and relevance to use one indicator to represent one cause or a similar cause.
- **Observable, quantifiable and reliable** based on observations and reports to be used to determine cause-effects processes.
- **Sensitive to change** for use in pro-active approach for monitoring and understanding the effects of corrective measures.
- **Transparent and easily understood**. The data on accidents, incidents and failures are collected and processed and must be clear and stable. Data must be validated and recognised for their objectivity and competence.
- V**alid for the scope** it serves. The validity can be interpreted as the reinforced and unanimously recognised suitability and relevance of the indicator for the scope of the use.

Monitoring accidents and other incidents is an important function within any organisation. The purpose of Accident and Incident reporting is to provide information to the public and the regulator about system performance. Learning from incidents and accidents is an activity that not only requires skills, but also perseverance and resources. The lessons learned by or for a user at operational level may be made shareable for reuse by other organisations or organisational units that run similar business processes using similar or same products.
It is vital for an indicator to be valid and to have enough instances occurring that it is sensitive to change and the following issues should be addressed:

1. Proper indexation and normalisation of the collected data is needed to identify the reference event space against which the accident related events are assessed and analysed.

2. Classification of accident related events on the basis of types and categories are important for the purposes of investigation, corrective measures and organisation learning. More work is needed to uniquely define the types and categories identifying their roles in improving safety performance.

3. Indicators relating to incidents, near-misses, consequences of accidents, technical safety and management of safety require more detailed analysis and discussion. Currently available data on these events may not be suitable for predicting safety performance level at a global level. More research is also needed to standardise the indicators relating to consequences of accidents, and individual definitions of incident related indicators.

7.4. Indicators relating to security (both urban and non urban)

Some accidents or incidents are provoked by terrorist actions or vandalism. Such actions are sometimes recovered when they are detected and controlled in time.

In France, for instance, the case of the AZF terrorist group is a practical example that shows how the railway system can be affected by terrorism or vandalism [31]. This AZF group had set up some bombs on the French railway infrastructures and required an important amount of money to the French Government in order to stop their terrorist actions! Because of such actions affecting security, the French railway company had to check manually more than 32000 km of tracks!

Another kind of example concerns the case of the tramway control in Poland: a malicious act using a TV remote controller that affected the switch control [32].

Other more dramatic events that have occurred in recent years are also mentioned:

- In London in July 2005, 52 people in addition to four suicide bombers were killed, and about 700 people injured,
- In Madrid on 11th March 2004 the figures were 191 people killed and 1755 wounded.

Future actions are then required in order to facilitate the prevention or the recovery and control of such security affecting actions.

Several European projects are emerging on this topic, and especially, the SECUREMETRO project. The goal of this research project is to develop validated materials selection and design strategies for building metro vehicles with intrinsic

security features. These will complement and support current standards for vehicle structural integrity and fire performance, and will be accomplished through application of existing materials and technologies which have not yet been applied in rail vehicle construction. The outcomes of this project will allow security to be "designed-in" to rail vehicles, achieving security through design against the threat of blast, smoke and firebomb attacks.

A Mass transport demonstration programme was held recently in Berlin to complement the works of the demonstration programme for freight (Logistic and supply chain security) and the integrated project dedicated to Airport security. The security terminology for "Mass transport" used in the European Union is "urban transport security" and includes Metro, Tram, Short distance regional rail transport, city buses, inter modal critical sensitive nodes.

8. Authorisation process

The authorisation is an activity whereby a body, independent of the involved entities, gives a written assurance that a product, process or service conforms to specified requirements. The safety authorisation rests on national or regional legislations. The safety plan, which is a simple written document outlining how to manage safety during the contract makes easier the authorisation process. The operation of an urban guided system becomes effective after the approval of documents by the safety key players involved in the process.

The following paragraphs describe for several European countries these key players involved and the process implemented (milestones, safety cases, applicable regulations…).

8.1. Current approaches for authorisation in some European countries [20]

8.1.1. Czech Republic

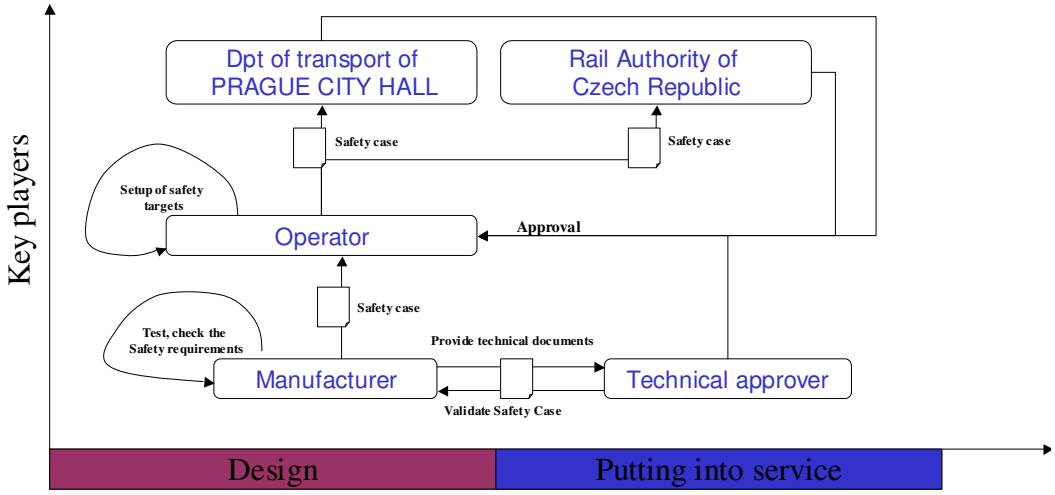


Figure 11 - Approval process in Czech Republic

The operator sets up the safety targets for the putting into service of a new system. As specified by the Figure 11, the chosen manufacturer must provide 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 Dept 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.

8.1.2. Denmark

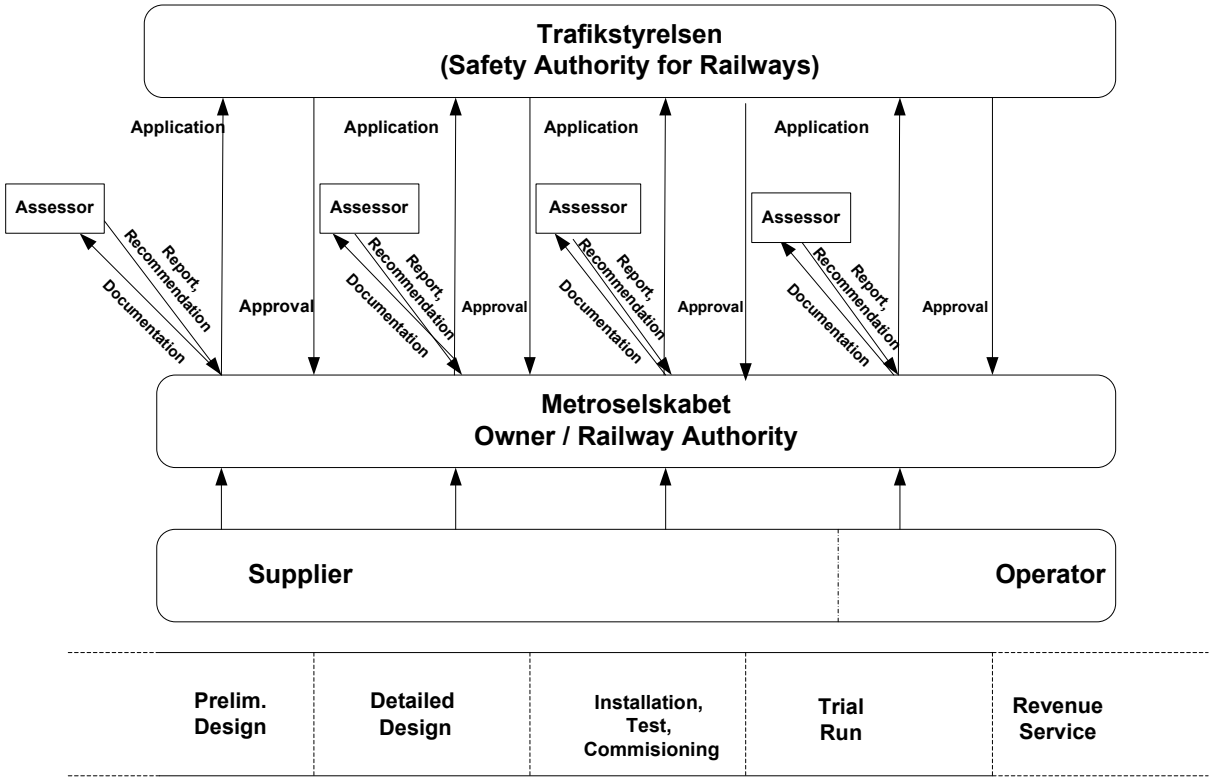


Figure 12 - Principle Overview of the Approval Process for the Metro Copenhagen

Danish Roles and Responsibilities

Denmark has a rather simple system for the technical supervision of rail-bound transportation systems. “Trafikstyrelsen” is the only authority for technical supervision, approval, and acceptance of rail-bound transportation systems. The only Metro system in Denmark is the Copenhagen Metro. The undertaker is “Metro-selskabet”, the operator is currently “MetroService”.

Approval Process for the Copenhagen Metro

The Copenhagen Metro is the first and only urban guided system in Denmark. The last tramway was taken out of service in the early 1970s. In the 1990s a new Metro

was planned for Copenhagen. Since there was no special law or regulation for urban guided until the 1990s, the Railway Authority (according to EN 50126), the owner Ørestadselkabet (now Metroselskabet), decided to follow the German regulations for light rail systems (BOStrab) and its guidelines as a set of requirements. For the planning, construction, approval, and operation processes of the Copenhagen Metro the Owner / Railway Authority decided, that all processes should follow the CENELEC standards EN 50126 / 50129 / 50128. This is in accordance with BOStrab §2, since these CENELEC standards have been recognised as "generally accepted rules of technology". The Danish Safety Regulatory Authority (according to EN 50126) Jernbanetilsynet (now Trafikstyrelsen) agreed to this decision. So the complete life-cycle of the Metro was set up according to these standards. This implied that an Independent Safety Assessor was established. According to the life-cycle a milestone plan was established, which foresaw a couple of approval milestones. For each milestone, all relevant documentation was inspected by the Safety Assessor, accompanied by audits and site inspections. For each milestone the Safety Assessor issued an Assessment Report with a recommendation to the Safety Regulatory Authority. Based on the recommendation and their own activities the Safety Regulatory Authority issued the approval for the respective milestone. This was the allowance to continue establishing the Metro. With the last approval the Copenhagen Metro was allowed to start revenue service.

So the Approval Process for the Copenhagen Metro accompanied step-wise the lifecycle according to the CENELEC standards EN 50126 / 50129 / 50128.

8.1.3. France

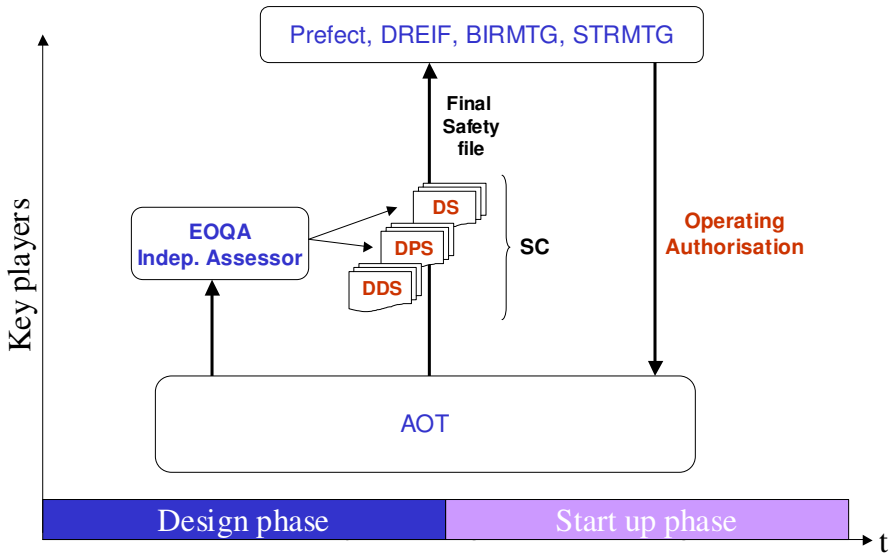


Figure 13 - Approval process in France

In France the authorisation process is governed by a the decree n°2003-425 (May 9 2003) relative to the safety of public guided transit (STPG), consolidated version of December 14 2008. This decree defines the different phases described hereafter and the content of these different phases. Two legislative orders (French word "Arrêtés") of May 23 2003 precise the content of the different safety case, for the first one and the procedure for the agreement of Independent Safety Assessors (French word : EOQA : Experts ou Organismes Qualifiés Agréés), for the second one.

The safety Definition Case (DDS for Dossier de Définition de Sécurité) is the first step to initialize a dialog between the Transport Organising Authority (AOT for "Autorité Organisatrice du Transport") and the relevant representatives of the national safety authority (Prefect, DREIF, BIRMTG, STRMTG). Its structure and content (as well as the structure and content of the subsequent Safety Cases) is imposed by the legislative order of May 23 2003). It establishes the legal framework proposing the preliminary Safety and Quality Plans and the main characteristics (functional, technical, the general Safety targets). It also include an important point (subject of chapter 7) namely the reference system (French word: Référentiels): set of regulations, standards, instructions… applicable for the system. It may be considered as a concept submission to the Safety Authority who accepts it or not. The assessment of the DDS by an Independent Safety Assessor is not mandatory (not an imposition of decree 2003-425)

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 (PHA) is included in chapter 4 "Safety of the project". The DPS also includes an update of all chapters of the DDS, in particular for the most important chapters regarding safety aspects : Natural and Technological Risks (chapter 3), Safety of the project (chapter 4), Organisation for Safety and Quality (chapter 5), Reference System (Chapter 7), Test program (Chapter 8). An independent safety assessor report delivered by an EOQA (Experts ou Organismes Qualifiés Agréés, kind of ISA recognised and accredited by the French government) is added to the file. In some cases several EOQA can be involved for a same project for different subsystems (e.g. infrastructure, track, rolling stock…) or at different levels (transportation system, overall or global system including infrastructures. The French government representative 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. It classically includes in chapter 4 a Hazard Log (French word "Registre des Situations Dangereuses"), to keep track of the coverage of all Hazards identified in the PHA, including the reference of the justification documents (detailed safety analyses, calculation notes, test reports, operating and maintenance requirements…). A second independent safety assessor

report delivered by the same independent Assessor Body (EOQA) is added in this file. To summarize, 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).

In some cases another safety case must be added prior to the beginning of the onsite tests. This is the case if some tests are performed on parts of a public domain (frequent case for trams) or more generally, if third parties are involved (typically if it is planned to perform public demonstration prior to put officially the system into service. In such cases a specific case (DAE or DAuTE, Dossier d'Autorisation d'Essais ou Dossier d'Autorisation de Tests et Essais) : for authorizing these tests must be provided, in order to demonstrate that appropriate precautions are taken to ensure the safety of the public during the tests.

The safety level of all public transportation systems must be periodically (every 10 years) re-evaluated. An updated safety case must therefore be produced and submitted to the assessment of an Independent Safety Assessor (EOQA) to keep the authorization to operate the system.

In case of subsequent significant modifications ("substantial modifications" to follow the decree terminology), the complete process (DDS, DPS, DS) relative to these modifications, must be performed.

8.1.4. Germany

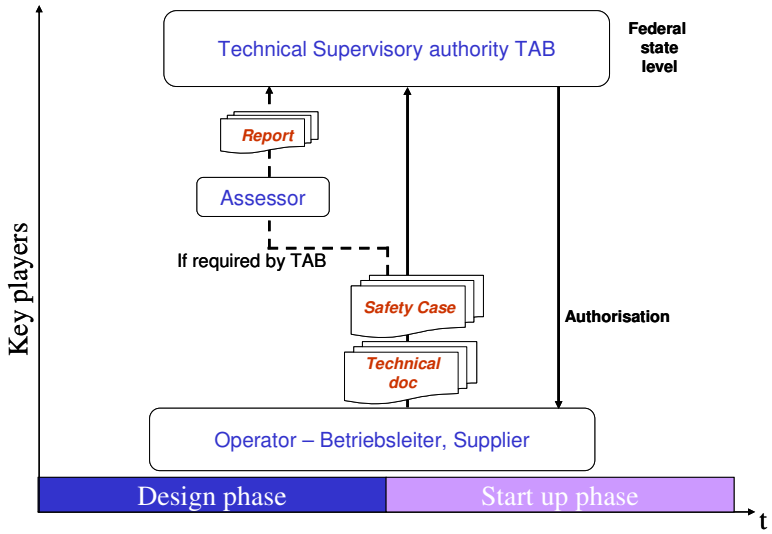


Figure 14 - Approval process in Germany

To operate an urban guided transport system, it is necessary to have a license granted by the Safety Authority in agreement with the Technical Supervisory

Authority (TAB). 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, on 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 (in reference of the GAME safety policy, the commonly acknowledged rules of technology are the referent model on which rests on the study). It further states that it may deviate from the commonly acknowledged rules of technology, if at least the same safety is guaranteed. Building works cannot 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.

8.1.5. Italy

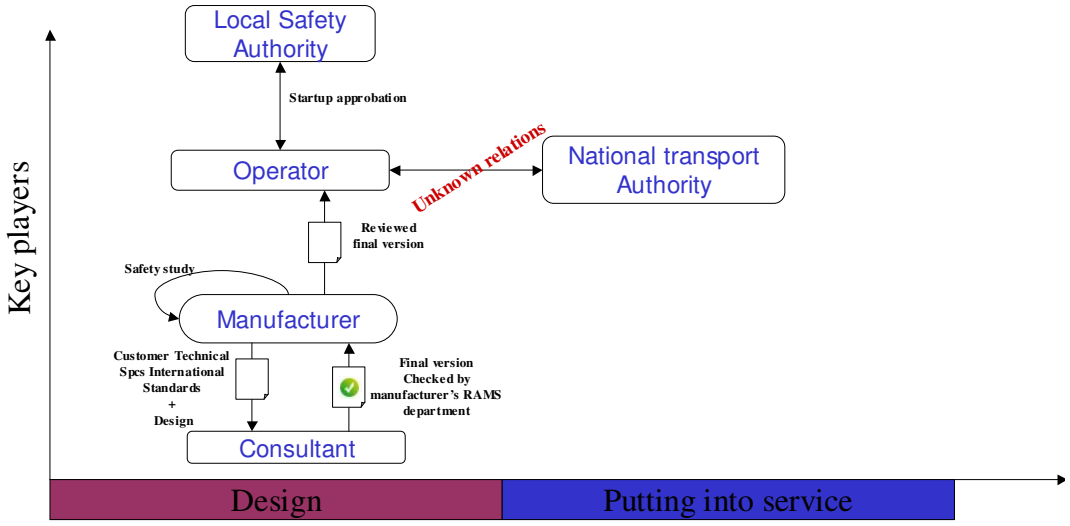


Figure 15 - Approval process in Italy

When a manufacturer is asked to deliver a new guided transport system, it must provide a document called “Customer Technical Spcs. International standards”. It can either carry out the safety study by itself or delegate to an external consultant chosen by their RAMS department. The safety study itself 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 and Criticality Analysis, fault tree analysis. The responsibility of this study is incumbent upon 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 get 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.

8.1.6. Poland

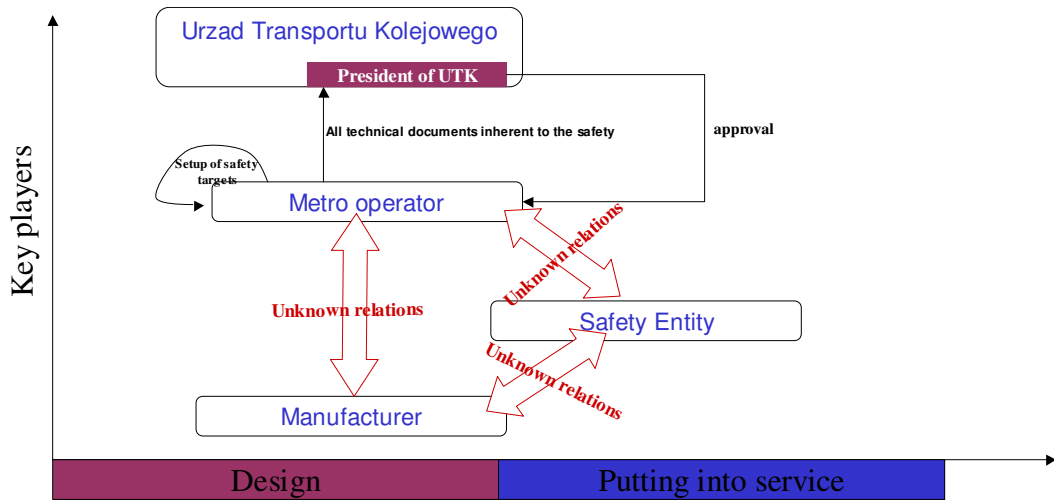


Figure 16 - Approval process in Poland

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 "Urzad 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.

8.1.7. Portugal

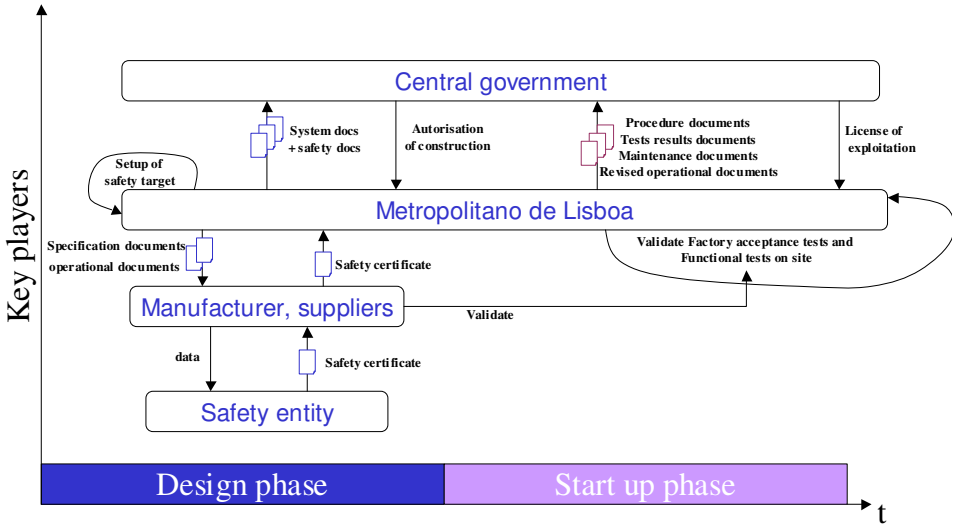


Figure 17 - Approval process in Portugal

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.

8.1.8. Spain

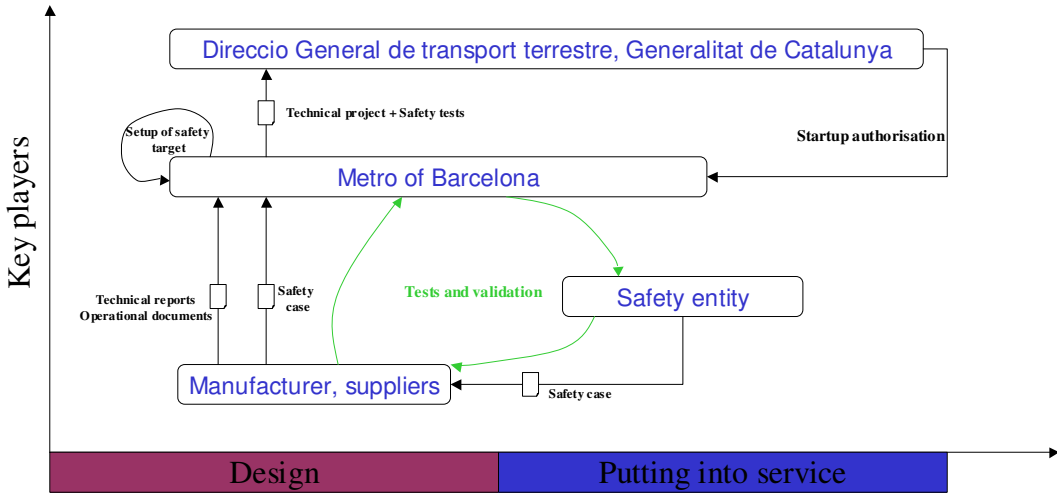


Figure 18 - Approval process for the Metro of Barcelona (Spain)

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.
The manufacturer (or safety entity, which can be an expert in the safety field or an ISA) will be in charge of the system validation (operator and Safety authority could participate in the validation task).
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 "Consorcio de Transportes de Madrid" in the case of Madrid Metropolitan).
The operator/safety authority will accept the new material taking into account the safety case, the test acceptance and, if they require it, an Independent Safety Assessment (ISA).

8.1.9 The UK

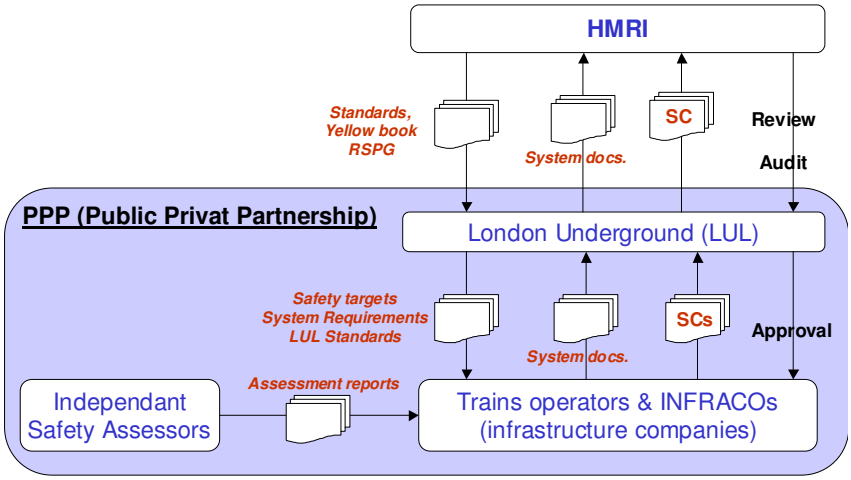


Figure 19 - Approval process in London

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 Safety Management System, 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 (part of the Office of the Rail Regulator), 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. The HMRI audits LU to assess compliance with the SMS.

8.2. Current approaches for certification in others worlwide countries

The Australian case study [30]

The next section describes the main procedures for rail in Australia, but documents indicate that the described processes are rigorously similar for urban guided transport.

There are three important aspects of railway safety oversight, and these are considered by:

- **standard-setting** in technical systems and operational practices,
- **accreditation**—or licensing-systems,
- **incident investigation**.

Figure 20 presents an overview of the safety regulation system. At the heart of the process are the operating procedures and standards. They are influenced by a government-based Australian Standard (AS 4292) and the industry-owned Code of Practice for technical and operational specifications. In Victoria, the PTC Rule Book is also a parameter in regulations and operating procedures and standards. Safety regulators can set technical standards and operational practices that railway firms must abide by. They accredit track managers and operators. Their suitability is assessed on criteria such as the comprehensiveness and robustness of their Safety Management Systems. These systems are designed to identify and manage risks. These standard-setting and accreditation issues are considered here.

Incident investigations are considered separately. In NSW and Victoria apart, the investigating entities are part of the safety regulatory authority; and that the findings of an incident investigation influence future safety strategy.

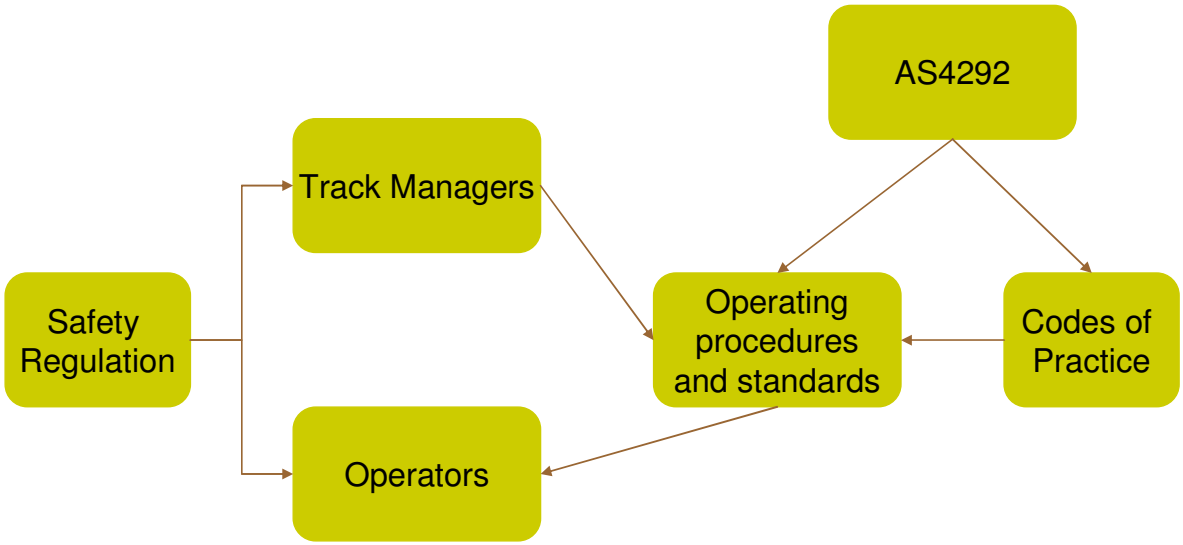


Figure 20 – Relationship between safety regulation, operating procedures, standard and code of practice

Safety regulation model

The industry has therefore moved away from a system based on railways' self-regulation, or oversight, of safety. One model that could have been adopted would have been to fully-prescribe safety systems.

In this model, the risk-makers are required to comply with systems set by the regulator. As illustrated in Figure 20, the model adopted in Australia is less prescriptive than that used in Britain and North America and is State-based rather than national. Under co-regulation, the risk-takers—the railway industry players—propose safety systems. They must be able to demonstrate to a safety regulator that such system are fit-for-purpose and meet standards specified by that regulator. By implication, if standards are prescribed but are safety deficient for a given circumstance, then the risk arguably lies with the prescribing authority rather than the rail entity. Co-regulation is a combination of self-regulation and prescribed government regulation and involves some discretion in the regulatory process. Consequently, the procedures are flexible and the details are determined by the infrastructure managers.

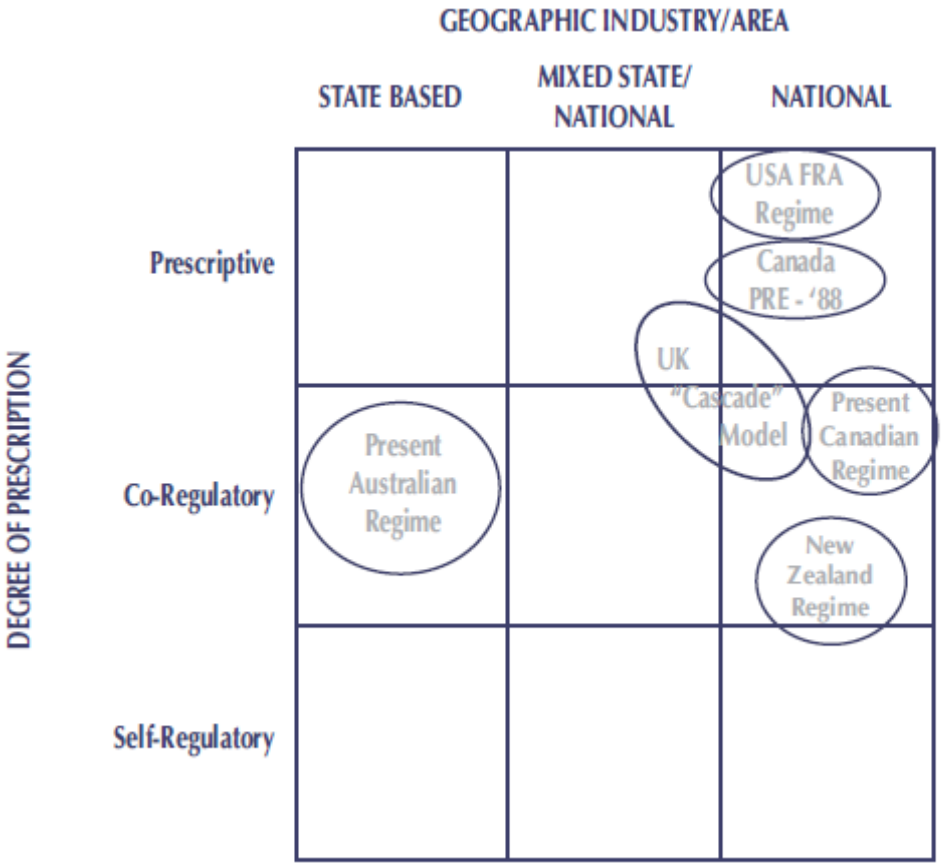


Figure 21 – The basis of railway safety regulation in Australia

As it has evolved, this co-regulated safety system can be considered to consist of a number of processes: accreditation of industry players and of physical assets, operational procedures and rules, certification of workers, and safety monitoring and investigation. The processes are applied as follows:

• accreditation of organisations:
  - infrastructure managers;
  - train operators;
  - maintainers, manufacturers and constructors of rail assets;

• accreditation of physical assets:
  - operating equipment;
  - infrastructure assets;

• accreditation of processes:
  - operating rules and procedures;
  - risk management systems;

• operational procedures
  - rules and procedures related to railway operations, such as incident reporting;

• rules for control of train movements;

• certification of labour force:
  - train drivers, track workers, signallers etc; and

• safety monitoring and incident investigation. (Safeworking Services1999, p. 2 and Affleck 2003, p. 20)

Certification of the labour force can be (but is not) undertaken by the safety regulator. The DOI notes that the Victorian Safety Regulator takes the view that accreditation or licensing of safety critical workers (such as drivers and signallers) is '...well outside the scope of [the rail safety regulator's] role' (DOI 2004, p. 68). Alternatively, the regulator may accredit an organisation to undertake training and certification. These processes were also influenced by the setting of the Australian Standard on Rail Safety Management (AS 4292) and industry codes of practice.

9. Conclusion

The Directive 2008/57/EC of the European Parliament on railway interoperability provides an opportunity for excluding urban guided transport system from its scope. Member States may exclude metros, trams and other light rail systems from the measures they adopt in the implementation of this Directive [1].

In this context and in order to provide a basis for the work of WP6, this deliverable D1.2 presents a state of the art concerning the safety management in different areas (marine, aviation, space, nuclear, rail) including many details concerning railway and complemented by a presentation of the current approach in Europe for safety management of urban guided transport systems.

This report demonstrated that Member States should apply for exclusion of urban guided rail installations from the scope of the interoperability and safety directives. The urban rail sector requires for safety and security a dedicated approach in line with the recommendations made by the European Commission to Member States in a letter to RISC (Railway Interoperability and Safety Committee) members sent on 13th October 2009 (see annex 3).

"The option in article 1(3) could be interpreted as if the rail systems mentioned therein are presumed to be a part of the general scope of the Directive, unless excluded. This means that for the rail, could be subject to interoperability requirements, depending on the choice made by individual Member States when transposing the directive at national level.
This is an unintended effect of the new interoperability directive not only because it is not consistent with the objectives pursued by the legislation, as set out in article 1, but also, among other reasons, because the so-called "essential requirements" for interoperability have not been developed for urban and suburban transport and the procedure for placing in service prescribed by the directive is not appropriate to such rail systems."

The Commission therefore discussed this issue with Member States representatives at a meeting of the RISC, where the following three step approach was agreed:

- Member States were invited, when transposing the directive, to exclude the rail systems mentioned in article 1(3) (a) and (b),
- The Commission would issue a mandate to the relevant European standardisation bodies in order to develop harmonised standards for rail systems referred to under Article 1(3) (a) and (b),
- The Commission would review the situation with the Committee after the standards had been developed. Where appropriate, Directive 2008/57/EC could be modified in order to include specific provisions for the above mentioned rail systems or, on the contrary, to clarify in scope in order to exclude such systems.

10. References

[1] AMSLER Yves, *UITP and European Rail Legislation impacting local rail networks (urban, suburban and regional)*, UITP, March 2008.

[2] TIFSA, *SAMRAIL (Safety Management in Railways), WP2.1: Analysis of existing approaches*, Draft Final Report 2.1, March 2003.

[3] BLAS Alain, BOULANGER Jean Louis, *Lot 1 – Etat de l'art*, Secuguide project, November 2006.

[4] Belmonte, F.,Boulanger, J.-L. & Schön, W. (2007). *Human Reliability Analysis for Automatic Train Supervision*. Proceedings of the 10th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine systems, Seoul, Korea, 4-6 septembre, 2007.

[5] Cepin, M. (2008). *DEPEND-HRA A method for consideration of dependency in Human reliability analysis*. Reliability Engineering and System Safety, 93, 1452-1460.

[6] Chaali-Djelassi, A., Vanderhaegen, F., Cassani, M. (2008). *Risk assessment based on Human factors*. Deliverable D128 of the European Project MODURBAN, 6e PCRD, March 2008

[7] Kirwan, B. (1997). *Validation of Human reliability assessment techniques: part2 - Validation results*. Safety Science, 27, pp. 43-75.

[8] Polet, P., Vanderhaegen, F., Amalberti, R. (2003). *Modelling Border-line tolerated conditions of use (BTCUs) and associated risks*. Safety Science, 41, 111-136.

[9] Polet, P., Vanderhaegen, F., Wieringa, P. A. (2002). *Theory of safety-related violations of system barriers*. Cognition, Technology & Work, vol. 4, pp. 171-179, 2002.

[10] Reer, B. (2008). *Review of advanced in Human reliability analysis of errors of commission – Part 2: EOC quantification*. Reliability Engineerring and System Safety, 93, 1105-1122.

[11] Swain, A. D., and H. E. Guttmann (1983). *Handbook of Reliability Analysis with emphasis on Nuclear Plant Applications*. NUclear REGulatory Commission, NUREG/CR-1278, Washington D.C.

[12] Vanderhaegen, F. (2001). *A non-probabilistic prospective and retrospective Human reliability analysis method – application to railway system*. Reliability Engineering and System Safety, 71, 1-13.

[13] Vanderhaegen F. (2003). *Analyse et contrôle de l'erreur humaine* (Analysis and control of Human error), Lavoisier - Hermès Science Publications: Paris.

[14] Vanderhaegen, F., (2009). *Rail simulations to study Human reliability*. Proceedings of the 3rd Conference on Rail Human Factors, 3-5 March 2009, Lille, France.

[15] Modurban project MODSYSTEM WP23 subproject – *Deliverable report – D88, "Requirements and Specifications for data collection tool of non-conformity events"*, 18 December 2008.

[16] Directive 2004/49/EC (2004). *Safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railways undertakings and*

Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive), L164 p44-113, 29 April 2004, Official Journal of the European Union.

[17] Mirella Cassani et al, Modurban project MODSYSTEM WP23 SUBPROJECT – DELIVERABLE REPORT – *D 91, "Database of non-conformity events"*, 14th December 2007

[18] Andrew Hale, *Process Safety Indicators*, Safety Science, Volume 47, Issue 4, April 2009

[19] George Barbu, El Miloudi EL Koursi, Floor Koornneef, and Laura Lopez, SAMRAIl project, *D2.6.1 "Accident and incident reporting system for the EU railways"* July 4, 2004

[20] Benard and al, Modurban project MODSYSTEM WP23 SUBPROJECT – DELIVERABLE REPORT – *D 93, "Conformity assessment, guidelines for functional and technical specifications."*, July 2008.

[21] ERA, Safety Management System : Assessment Criteria for Railway Undertakings and Infrastructure Managers", European Railway Agency; May 2007.

[22] Modurban project MODSYSTEM WP23 subproject – *Deliverable report – D126, "Preliminary Safety Plan"*, 29 May 2008.

[23] Goldman, S. M., Fieldler, E., R., King, R. E. (2002*). General aviation maintenance-related accidents: a review of ten years of NTSB data*. Office of Aerospace Medicine Washington, U.S. Department of Transportation, FAA, DOT/FAA/AM-02/23.

[24] Reason, J., Hobbs, A. (2003). *Managing Maintenance Error - A Practical Guide*. Ashgate Publishing Company.

[25] Richard, P., Quéva, S., Dahyot, R., Vanderhaegen, F. (2008). *Prise en compte des facteurs humains dans la démonstration de la sécurité ferroviaire*. Conférence Internationale Francophone d'Automatique, Bucarest, Roumanie, September.

[26] LEGE Philippe, *Sécurité et sûreté des transports : un état de l'art méthodologique*, Les collections de l'INRETS, Synthèse n°58, ISBN 978-2-85782-670-5, Décembre 2008.

[27] Greenberg MD, Chalk P, Willis H, Khilko I, Ortiz DS, *Maritim Terrorism : Risk and Liability*, RAND Center for Terrorism Risk management Policy, 2006.

[28] Murray-Tuite, *Transportation Network Risk Profile for an Origin-destination pair : security measures, terrorism, and target and attack method substitution*, presentation at the 87th annual meeting of te TRB, 2008.

[29] Gordon P, Richardson HW, *the economic impacts of terrorist attacks*, Cheltenham : Edward Elgar, 2005

[30] BTRE, *Optimising harmonisation in the Australian Railway industry*, report 114, 2006

[31] Escorsac, P. (2007). *Terrorisme. Le groupe AZF menace à nouveau les trains*. La Dépêche, http://www.ladepeche.fr/article/2007/03/07/2279-Terrorisme-Le-groupe-AZF-menace-a-nouveau-les-trains.html
[32] Baker G., (2008) Schoolboy hacks into city's tram system, www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html#
[33] El Koursi., E.M, Mitra,S, Bearfield,G, 2007, Harmonising Safety Management Systems in the European Railway Sector, Safety Science Monitor, Issue 2, Vol 11, p 01-14

Annex 1

Table 3 - Railway SMS Comparison

	RENFE	UK	SNCF	DB	UIC
Business process	•Safety central commission •Safety plan	NR Safety planning	Each Business Unit	No explicit	
Risk inventory	Not yet implemented	Included into the safety case	Systematic approach into risk assessment	•Investigate and evaluation of statistics •Advice of EBL •Input of the research programme	
Risk barriers and control	•Safety directorate:Traffic rules, Safety standards, Safety Autorisation •Infrastructure manager : technical barriers •Chairman : safety policy	Included into the safety case to be submitted by RU's and IM	•Safety division establishes : safety policy •State regulation : IM and RU operating rules •FMECA (risk analysis)	•Safety policy:executive board and safety department •Regulation and instruction by national safety authority •EBL orders for safety •Risk assessment establishes the risk reduction strategies	
Risk management system	•The UN's (Business Unit) provide the resources to ensure that the barriers and controls are applied • safety rules, approval organisation	Included into safety case submitted by each RU for approval of HSE	Each operator is responsible for risk management and has to demonstrate that it's SMS enables to reach safety objectives defined by national safety authorities	under responsability of EBL appointed at each RU and IM	

Inspection and monitoring	Safety plan organised by safety inspectorate sets up an inspection visit plan that each UN has to apply	Safety case is used to support the inspection and monitoring	The safety division by delegation of CEO coordinate and check	• Internal monitoring audited • Audits of singles procedures concerning safety : technical process, operational instruction, maintenance process, acceptance process	
Auditing	Safety action plan established by safety directorate	• NR has procedures to ensure that its safety policy and all the components of its SMS are regularly reviewed • All duty holders (NR) are required to procure an annual audit	Safety division review periodically the SMS	Not yet implemented	
Incident and accident	• Safety directorate is responsible of the definition an operation of I&A reporting system • Legal basis : the RENFE's technical standard "accidentes e incidentes en la circulacion"	• RSSB is responsible of I&A • Legal basis : RIDDUR 1995 • Application name : SMIS	safety research department manages a database for I&A which covers the whole system: technical issues database,operation issues database,freight passenger, motive power, rolling stock	• DB obliged by law to notify accident to EBA • Type of event defined by EBA • Tend to implementation a IP • Application name :	• European safety database • Legal bases : signed agreements betweens UIC and railways • Used a IT tolls, internet access • Envisaged 33IM and 102 RU

	•Application name : SICA			STABAG	•Reports structure : declarant and identifies, events description, cause, consequence, type of correction, action initiated, corrective action details

Annex 2

Table 4 – Security management

Goals	Functions	Tasks
To govern		
	Identify and understand the threat	• Characterizing the threat, • Measuring the threat, • Measuring the perception of threats.
	Identify and formulate actions to be undertaken	• Develop and propose responses, • Knowing all concerned interests.
	Deciding on actions to be undertaken	• Having a comprehensive approach to decision making.
	Implement decisions	• Coordinate actions, • aggregating interests • Manage, • Inform, communicate, warn, • Select and train the security professionals
	Assessing the results of implemented actions	• Analyse and determine the implemented actions, • Making public the result of the evaluation.
To prevent		
	Identify the threat	
	Eliminate the threat	
	Localize	Location of transport systems, containers,personnel and passengers
	Assess the infrastructure and transportations systems	• Analyze the risks, impacts, vulnerabilities. • Assess measures
	Adapt	Adapting emerging technologies
	Synthetize	Managing networks of different natures
	Train	
	Watch	
	Simulate	
To protect		

	Access control	
	Intrusion detection	• Detecting human • Automatic detection
	Detection of illicite objects	• Detecting human • Automatic detection
	Detecting aggression	• Detecting human • Automatic detection
	Detection of unusual events	• Detecting human • Automatic detection
	Inspection	Inspection of personels, inspection of passengers
	Data protection	
	Infrastructure resilience	• Mechanical resilience • Organizational resilience
	Transportation systems resilience	• Mechanical resilience • Organizational resilience
To respond		
	Assessing the impact	
	Minimizing the impact	• Networks management • Means management • Decision support • Simulation
	Support	• Communication • Victim assistance
	Restore	• Moral people

Annex 3

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY AND TRANSPORT

DIRECTORATE E - Inland Transport
The Director

Brussels, 13 OCT. 2009
TREN/E/2-PG/as D(2009) 66217
03.13.02.04.09.F002.13

LETTER TO THE DEPUTY PERMANENT REPRESENTATIVES

Subject: Directive 2008/57/EC on the interoperability of the rail system within the Community – transposition and clarification of the scope

The scope of Directive 2008/57/EC on the interoperability of the Community rail system, which has to be transposed into national legislation by 19 July 2010, is described in very broad terms in annex I to that Directive.

However Article 1(3) gives Member States the option to exclude from the measures they adopt in implementation of the directive:

"a) metros, trams and other light rail systems;

b) networks that are functionally separate from the rest of the railway system and intended only for the operation of local, urban or suburban passenger services, as well as railway undertakings operating solely on these networks;

c) privately owned railway infrastructure and vehicles exclusively used on such infrastructure that exist solely for use by the owner for its own freight operations;

d) infrastructure and vehicles reserved for a strictly local, historical or touristic use".

The option in Article 1(3) could be interpreted as if the rail systems mentioned therein are presumed to be part of the general scope of the Directive, unless excluded. This means that for the first time certain infrastructure and vehicles, and in particular urban and suburban rail, could be subject to interoperability requirements, depending on the choice made by individual Member States when transposing the directive at national level.

This is an unintended effect of the new interoperability directive not only because it is not consistent with the objectives pursued by the legislation, as set out in article 1, but also, among other reasons, because the so-called "essential requirements" for interoperability have not been developed for urban and suburban transport and the procedure for placing in service prescribed by the directive is not appropriate to such rail systems.

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium (Office : DM24 2/137)
Telephone: direct line (+ 32-2) 295.62.03 - switchboard : (+32-2) 299.11.11- Telefax: (+ 32-2) 299.58.87
Internet: http://europa.eu.int/comm/dgs/energy_transport/index_en.html

The Commission therefore discussed this issue with Member States representatives at a meeting of the Railway Interoperability and Safety Committee (RISC), where the following three step approach was agreed:

- firstly Member States were invited, when transposing the directive, to exclude the rail systems mentioned in Article 1(3) (a) and (b) ;
- secondly the Commission would issue a mandate to the relevant European standardisation bodies in order to develop harmonised standards for rail systems referred to under article 1(3) (a) and (b);
- and, thirdly, the Commission would review the situation with the Committee after the standards had been developed. Where appropriate, Directive 2008/57/EC could be modified in order to include specific provisions for the above mentioned rail systems or, on the contrary, to clarify its scope in order to exclude such systems.

In addition, a number of inconsistencies have been identified between several linguistic versions of article 1(3) of the new interoperability directive. For example the term "*other light rail systems*" in the English version (the working language in which the original was drafted) has been translated as "*andere Stadt- und Regionalbahnsysteme*" in the German version whilst regional lines were never intended to be excluded. The impact of such mistakes is considered to be critical and the Commission intends to request Council and Parliament to issue a linguistic corrigendum.

As the deadline for transposition of the Interoperability Directive is approaching (19 July 2010) I confirm the line agreed with the Member States that they should exclude rail systems identified under Article 1(3) (a) and (b) from the scope of their national law transposing Directive 2008/57/EC.

At the same time Member States should clearly define to which rail systems a given line belongs on a section per section basis; this would clearly define the borderline for the application of the Interoperability Directive, in addition to the present declared TEN lines. Such indication could be done by the Member States on a map or any other tool when notifying their national measures.

The issue of the borderline between "not interoperable" and "interoperable" rail systems will be further analysed in the context of the extension of the scope of TSIs, in cooperation with Member States and the European Railway Agency.

Yours sincerely,

Enrico GRILLO PASQUARELLI

cc: RISC Committee members, Mr Verslype (ERA), Mr Castelletti (DG TREN)

2