IJR International Journal of Railway
Vol. 1, No. 4 / December 2008, pp. 157-168

The Korean Society for Railway

Safety Levels Apportionment in Railway System

Meriem Rafrafi†, El Miloudi El Koursi, and Thomas Bourdeaud'Huy*

Abstract

The creation of a single European rail transport market it is important to increase confidence between the actors on the market and between member states who shall ensure that railway safety is generally maintained and, where reasonably practicable, continuously improved. For this purpose the European railway safety directive introduces a mechanism to adopt a Common Safety Targets (CST) expressed in risk acceptance criteria for individuals and for society. This paper focuses on the apportionment of safety targets for European railway system. We develop a generic approach based on the Functional Hazard Analysis (FHA), to analyse the safety of railway systems for a unified European network and to comply with the CSTs required by the European railway Safety Directive. We suggest to combine the FHA technique with the functional railway architecture to allocate the safety targets to the railway functions.

Keywords : *Risk Management, Safety Targets, Railway, Interoperability*

1 Introduction

The major changes within the European railway industry, the division between the management of the infrastructure and the exploitation, the need of enhancing the efficiency and the reduction of costs have an impact on the management of safety and on responsibilities of the management. The differences between the member states of the European Community (i.e. structure and organisation of care for safety) can create barriers for interoperability of the European railways and can frustrate the creation of one open market. The differences in the national structure of the railway industry, differences in responsibilities and differences in the decision-making and policymaking. Different dimensions can be distinguished in the process of developping railway safety:

- *The railway system meets the requirements for interoperability as expressed in Technical Specifications for Interoperability (TSIs)*
- *The European railways meet an acceptable level of safety and improve continually the level of safety. To keep the industry competitive with other modalities of transport, with the acceptable level of safety, at not to any price as expressed in Safety Directive.*
- *The process of demonstrating that the safety requirements are meet according to existing standards and regulation (e.g. cenelec standards 50126 and 50129).*

The key aspect of maintaining and improving, where possible, the safety is to supervise the safety targets at European and national levels. The Safety Directive is aiming to set Common Safety Targets (CSTs) that must be reached by the different parts of the rail system (such as conventional rail system, high speed rail system, long railway tunnels or lines solely used for freight transport) and the system as a whole, expressed in risk acceptance criteria. The demonstration of the meeting safety targets and measuring the actual risk that are in conformity with the established safety targets. Therefore, the process of risk management should undoubtedly demonstrate that the risks can be managed, meet and shall meet over time the criteria and targets set [1,2]. The qualitative and quantitative targets for enhancing safety need to carry out risk evaluation and to implement risk control measures.

This paper focuses on the apportionment of safety targets for European railway system. We develop a generic approach based on the Functional Hazard Analysis (FHA), to analyse the safety of railway systems for a unified European network and to comply with the CSTs required by the European railway Safety Directive. We suggest to

† INRETS, 20 rue Elisée Reclus 59666 Villeneuve d'Ascq, France.
E-mail: el-miloudi.el-koursi@inrets.fr, meriem.rafrafi@inrets.fr
*LAGIS, Ecole centrale de Lille, Cité Scientifique, 59650 Villeneuve d'Ascq, France.
E-mail: thomas.bourdeaud_huy@ec-lille.fr

combine the FHA technique with the functional railway architecture, developed by the AEIF (European Association of Railway Interoperability), to allocate the safety targets to the railway functions.

2. Risk Acceptance Criteria

Several international standards make comments about risk and how to define risk. The European Commitee for Electrotechnical Standardization CENELEC publishes standards dealing explicitly with safety and risk in the railway field. In EN 50126 [7] the risk is defined as the probable rate of occurrence of hazard causing harm and the degree of severity of harm. The risk in general consists of two components, severity of an event and the probability of occurrence. The severity of an event is usually measured by assessing the damage that occurred. The probability of occurrence is the frequency. In most cases frequency is given as the number of relevant events in a certain period. Generally spoken, the risk analysis, passengers, staff, third party are considered.

2.1 Groups at Risk

A way to get hold of risks and risk management is to look at the risks for the different groups that are put at risk by thee railway system. The following groups can be distinguished:

- Passengers who make use of the railway system as a mean of transportation (on trains and at stations). They have only little influence on the risk they are exposed to.
- Staff who is responsible for the operation of the railway system. Staff is defined as train drivers, dispatchers, train managers, track workers, shunters and so on.
- Public behaving in a legitimate matter (living/working outside the physical boundary of the railway, using level crossings or meeting people at stations) or behaving in a illegitimate matter (e.g. trespassers).

For each group at risk, the risks can be identified, analysed and compared with the goals set for these groups at risk. It is important that the definition of the targets set for these groups and the way in which it is measured if these targets are reached and are common over the member states.

2.2 Acceptability of Risks

The acceptability "tolerability" of risks, in CENELEC standard [7] is defined as the maximum level of risk of a product that is acceptable to the Railway authority. The tolerable risk level has to be set by the Safety authority of the relevant country. It usually takes into account the risk acceptance of the society. It is usually, in the past, that the Railway companies makes suggestions for a acceptable risk to the Safety authority based on their accident statistics.

The process of risk management can also be demonstrated by use of a 'risk matrix'. This kind of matrix is already discussed in EN 50126. The concept of risk is the combination of two elements:

- *the probability of occurrence* of an event or combination of events leading to a hazard, or the frequency of such occurrences;
- *the consequence of the hazard.*

These elements can be considered as the x and y axis of a risk matrix. In this guideline the word hazard, used in both elements, is often replaced by top event or accident/ incident (i.e. a hazard that actually occurs as result of an event or combination of events). As described in EN 50126 [7], both frequency and possible consequence of a particular hazard (severity level) can be described in qualitative terms. The table 1 represents a matrix that combines both elements. Such a risk matrix could be the result of a qualitative analysis and evaluation of risks.

This gives the upper limit of tolerability criteria for the

Table 1. Risk Matrix

Frequency	**Risk levels**			
Frequent	**Undesirable**	**Intolerable**	**Intolerable**	**Intolerable**
Probable	**Tolerable**	**Undesirable**	**Intolerable**	**Intolerable**
Occasional	**Tolerable**	**Undesirable**	**Undesirable**	**Intolerable**
Remote	**Negligible**	**Tolerable**	**Undesirable**	**Undesirable**
Improbable	**Negligible**	**Negligible**	**Tolerable**	**Tolerable**
Incredible	**Negligible**	**Negligible**	**Negligible**	**Negligible**
	Insignificant	Marginal	Critical	Catastrophic
	Consequence (Severity levels)			

Table 2. Severity and Frequency Categories from CENELEC 50126

Severity		Frequency	
Catastrophic	*Fatalities or multiple severe injuries*	***Frequent***	*Appears frequently during system life*
Critical	*Single fatality or Severe injury, loss of a major system*	***Probable***	*Appears several times during system life*
Marginal	*Minor injury, Severe system damage*	***Occasional***	*Appears very rarely during system life*
Insignificant	*Possible single minor injury.*	***Remote***	*Does not normally appear during system life*
		Improbable	*Highly improbable during system life.*
		Incredible	*Extremely unlikely to occur*

hazards, at least in qualitative terms. The standard EN 50126 [7] indicates that any quantification of the frequency ought to be decided on a case by case basis depending on the application, which is consistent with the frequency classes.

The combination of the consequence of hazard or sequence of hazards and the probability of its occurrence determine the risk classification. The main goal of the process is to set barriers in order to reduce or even eliminate the risk of incident and when it is not possible to eliminate the risk to reduce the final consequences of the incident. These barriers may be of different kinds:

- Technical barriers, e.g. ATP systems;
- Operational barriers, e.g. procedures;
- Organisational barriers, mainly found in the SMS, e.g. emergency organisation including links with local authorities and rescue teams in case of incident/accident.

The organisation must monitor all of its barriers to ensure that failures or weaknesses in the barriers are identified and rectified before an accident actually occurs. The barriers in an organisation are its safety requirements. Each different type of barrier should be monitored using a different process. For example, where the safety requirements are operational procedures they can be controlled and monitored using safety inspections, and auditing. Where the safety requirements are functional system requirements they can be monitored by inspection or they may also have diagnostic functions which aid in understanding where safety requirements are no longer being met or are ineffective.

2.3 Existing Safety Targets

The objectives of railway organisations is to maintain and to improve their safety performance. The achievement of this objective is usually checked by monitoring safety performance with indicators based on accident and incident data. Many countries and organisations also set relative targets for particular type of accidents or incidents using statistical data.

The survey of existing safety targets shows that a majority of state members adopted a qualitative targets combined with quantified safety targets expressing criteria for individual or collective risks. The way to formulate it is different from one country to another, but on the whole, the formulations are different facets of the same idea. Three of them are considered in the following : the French principle GAME, the English one ALARP and the German one MEM. These three principles, described in the railway standard Cenelec 50126 [7] are used to define the global safety targets:.

- *ALARP principle* dictates that risks should be managed to be "As Low As Reasonably Practicable". Low refers to the effectiveness of safety processes (i.e. are they making systems and software safe?) and Practicable refers to the efficiency of safety processes (i.e. how much is enough?). Alarp is a term often used in the milieu of safety-critical and high-integrity systems. Both risk levels and the cost associated with mitigating the risk are considered, and all risk reduction measures should be implemented as long as the cost of implementing them is within the reasonably practicable area/region according to cost effectiveness considerations. Before this principle can be used in establishing risk acceptance criteria, there is thus a need to compare the risk level to some standard measures. Three regions of risk can be distinguished : **Intolerable Region** (Unacceptable risk must be reduced at least); **Alarp Region** where risk level is acceptable only if further reduction would be impracticable and **Broadly Acceptable Region** where continued operation must not cause more costs than benefits [8].
- *GAME principle (Globalement Au Moins Equivalent)*, "globally at least as good", can be applied when looking at either individual or collective risk. This criterion is based on the requirement that the total risk inherent in any new rail borne transport system must not exceed the total risk inherent in comparable existing systems. It is assumed that the risk level of existing systems can be assessed (e.g., using existing statistics). The respective risk levels of an existing system and a new system can only be compared if

both systems have comparable performance characteristics and operating conditions.

- *MEM principle (Minimum Endogenous Mortality)* accounts for death rates in the society caused by technological systems (defined as entertainment, sport, yourself activities, transport, etc.), excluding death by illness, disease or congenital malformation. Mem principle is based on an individual risk. Consideration starts at the point of the lowest rate of mortality for human individuals. For instance, the expression bellow represents the lowest Endogenous Mortality Rate, Rm, which is observed in developed countries, for the age group 5 to 15 years.

  $R_m = 2.10^{-4}$ *fatalities/person.year.*

In general, the GAME and ALARP principles are commonly used with cost benefit analysis.

3. Requirements and Approaches for Safety Targets Harmonisation

3.1 Common Safety Targets Requirements

According to article 7.4 of the Safety Directive [6], CSTs shall define the safety levels that must at least be reached by different parts of the railway system and by the system as a whole in each Member Sate, expressed in risk acceptance criteria for:

- Individual risks relating to passengers, staff including the staff of contractors, level crossing users and others, and, without prejudice existing national and international liability rules, individual risks relating to unauthorised persons on railway premises.
- Societal risks.

CSTs can refer to different "groups at risk" such as passengers, staff, track workers etc. Besides these groups a distinction can be made between individual risk and collective or societal risk. Individual risk defines the chance of a person dying due do to a certain activity. This is most often expressed in the chance of a fatality per year. Individual risk is measured in terms of the chance of a fatality per individual per year. However, societal risk deals with the consequences of a railway accidents on the society (in terms of harms and damages). The Common Safety Targets definition should fulfil the following objectives:

- CSTs should push forward the opening of the railway transport market
- CSTs should preserve the competitiveness of the railway sector
- CSTs must not reduce the existing level of safety within Member States
- CSTs should when and where necessary and reasonably practicable lead towards improved safety levels
- CSTs must be achievable at Member States Level

To develop common safety targets is needed to establish basic commonalities.

- *Commonality of Base Units of Risk. 'Risk' is accepted to be the product of the probability of occurrence of an accident and the severity of that accident. However there are various and different approaches adopted across each member state for quantifying risk and a number of units of risk used. If the base units for risk are standardised (such as SI units of Risk) then the results of any analysis should ultimately be comparable. Establishing common base units of risk is therefore a key area of concern in establishing a common and comparable approach to risk assessment and safety management.*
- *Commonality of Conceptual Model used to undertake Risk Assessment. The bow-tie concept [7] is the generally accepted conceptual model used to structure risk analysis and assessment. There are various tools and techniques that can be used to elaborate this conceptual model and undertake more detailed risk analysis depending on the depth of analysis required and the nature of the accident and its various causes.*
- *Commonality of the System Definition. The System Definition activity provides the scope of all subsequent risk identification, analysis and management activity. The description should then be translated into sets of functional models which describe and represent the sub-system functionality. This is to provide a suitably detailed set of models for subsequent risk analysis. A railway system can also be divided in partial systems, subsystems and components. Each 'level' demands for another approach in risk identification and risk control. In order to put on most suitable methods and to obtain most reliable results these levels should be taken into account during the whole process of risk (based) management. A combination of functional and structural division of a (generic) railway system is needed.*
- *National Reference Values. The specification of Common Safety Targets should push forward the opening of the railway transport market, preserve the competitiveness of the railway sector and must be achievable at Member States Level Therefore, the reference svalies would in this case correspond to the safety level in each member state and will be for the 1st Set of CSTs. The Member States are assumed to undertake activities such that current (or trend-adjusted) safety levels are maintained and approach where possible. The CST can be set as the weighted average of the MS national reference value and which will be valid for*

the EU27 Community as a whole and not for a single Membet state. The national reference values are based on Eurostate data [10]. If we consider the European Community, the safety level of each member state is different from a country to another. In the first step, the approach proposed by the ERA is to make states with low safety level reach an average of safety. In other words, according to interoperability principle, the highest level of safety must be maintained and, in the second step, it should be highered.

3.2 CST Development Principle

According to Art 7.4, the Directive [6] requires at least **five different Safety Targets** that must be reached in each Member State. The CST shall define the safety levels that must be reached by different parts of the railway and by the system as a whole in each Member Sate, expressed in risk acceptance criteria for:

(a) individual risks relating to:
- *passengers*
- *staff including the staff of contractors*
- *level crossing users and others,*
- *and,....., unauthorised persons on railway premises*

(b) societal risks

As the societal risk isn't clearly defined, a proposal to consider it as being the sum of risks relating to the different individual risks listed in the Safety Directive. In this proposal, "global safety targets" indicates "societal risks". The global safety targets is the sum of different safety targets (CSTs) identified by the safety directive.

For this purpose the EU Safety Directive introduces a mechanism to adopt a minimum CST expressed in risk acceptance criteria for individuals and for society. Different targets could be valid for different parts of the rail system (such as the high-speed system, the conventional rail system or lines dedicated to freight traffic). The resulting safety targets will describe the minimum safety level, so that member states could apply more demanding targets, for example for infrastructure, as long as they do not impose requirements above CST on railway undertakings.

In accordance with EC Directive 2004/49 (Safety Directive), CSTs are to be developed over the next 5 years:
- The 1st set shall be adopted by the Commission before 30 April 2009
- The 2nd set shall be adopted by the Commission before 30 April 2011.

In order to assess if the CSTs are met, the CSMs will be developed [9]. The CSM could harmonise the use of independent safety assessors for checking compliance with essential requirements or for assessing conformity with requirements of safety certificates. The CSM have to describe how the safety level and the achievement of safety targets and compliance with other safety requirements are assessed by elaborating and defining: risk evaluation and assessment methods, methods for assessing conformity with requirements in safety certificates and safety authorisations and methods to check that the structural sub-systems are operated and maintained in accordance with the relevant essential requirements. CSTs mean the safety levels that must be reached by the different parts of the rail system (such as conventional rail system, high speed rail system, long railway tunnels or lines solely used for freight transport) and the system as a whole, expressed in risk acceptance criteria". Each member State shall ensure that railway safety is generally maintained and, where reasonably practicable, continuously improved, taking into consideration the development of Community legislation and technical and scientific progress and giving priority to the prevention of serious accidents.

The targets and their associated indicators should be comparable to the safety level of other modes of transport. If, for example, the risk acceptance criteria are defined as

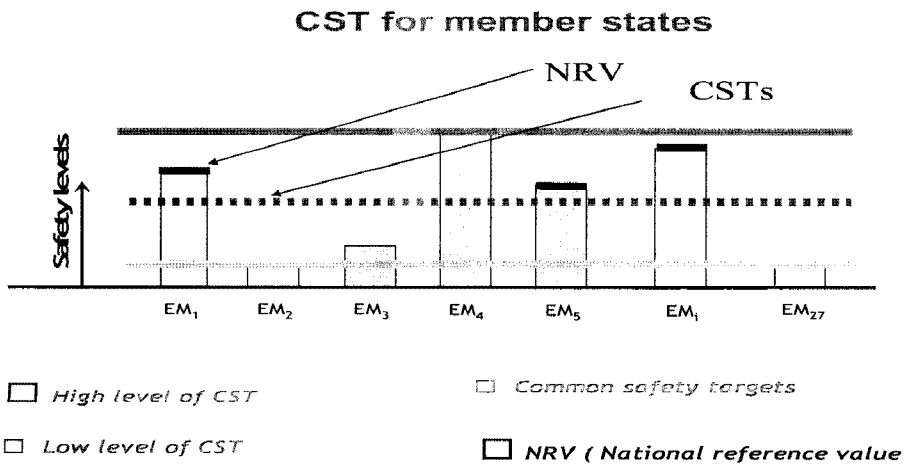

Fig. 1 CST versus NRV

average values at European level and they are regularly revised and adapted to technical advances, then they should not continue to spiral upwards with no upper limit, but should take an asymptotic approach to a generally accepted level. Starting with CSTs at system level, related to each national railway system as a whole, based on European official statistical data. The definition of common safety targets requires to obtain a picture of the current safety levels in Europe by determining the National Reference Value (NRV) [Fig. 1] for each Member State on the basis of Eurostat and CSI accident data. Then it will be possible to set the values of the CSTs according to the requirements of the safety directive [1] at system level for each national system, for high speed networks, conventional networks, long tunnels and lines solely used for freight transport.

The ERA "European Railway agency" in its feasibility study [19] assessed the possibility of apportioning common safety targets to subsystems and constituents of the railway system, one of the aims of this apportionment is to help defining the safety levels of subsystems in the TSI, in line with the CST.

The study concluded that the apportionment of CST to define common safety requirements is not feasible due to insufficient official data on accident causation. It is suggested to agree on common risk acceptance criteria directly applicable to the sub-systems or constituents being assessed (e.g by defining as a convention some calibrated risk matrices at the appropriate indenture level). Alternatively or in complement, it might be useful (subject to further analysis of feasibility and reliability) to look directly into the statistics of accident precursors, in order to obtain reference quantitative figures for deriving the safety levels of new sub-systems and constituents.

3.3 Discussion

The method for apportioning system level CSTs to categories of stakeholders, such as infrastructure managers and railway undertakings and for subsystems and constituents as defined by the interoperability directives, Deriving acceptable risk levels for the various parts of the railway system requires first a classification of all the risks into various categories, and then the assignment of a target or acceptable risk level to each category with respect to each group exposed to the risk. Such a process is also called risk apportionment. There are several ways of classifying risks depending on their various characteristics. Based on the investigations it can identify 5 distinct approaches for the classification of risks and derivation of acceptable risk levels for parts of the railway system [19]:

- ***System breakdown approach.*** *The approach consists of decomposing the whole railway system into its major constituents (organisational and/or physical) parts and assigning a risk portion of the overall risk to each part, depending on the estimated contribution of each part to global risk. This approach was taken for instance for defining risk levels for the Train Control System ETCS. The safety target for ETCS was determined and further apportioned between wayside and train-side equipment. This approach is closely linked to the type and the operating environment of the system.*
- ***Functional breakdown approach*** *The Functional approach looks at all the functions taking place in the operation of a railway system and identify the potential resulting risks associated with each function and subsequently the phase of operation (bottom-up), or alternatively apportioning the global risk to each functions (top-down). CST independent of technical realisations and implementation and provide reference values for deriving safety requirements at constituent level.*
- ***Breakdown by categories of hazard causes.*** *The approach classifies risks not according to the part of the system they emanate from, nor to the function or process they may appear through, but according to the nature of the cause creating the risk.. For instance one can differentiate risks depending on whether they arise because of technical faults or human errors, and assign different targets to them according to statistics.* The difficulties are to link the apportionment to the system constituents.
- **Breakdown by hazard types.** The hazard types approach allows the apportionment of CST independent of technical realisations and implementation . The difficulties are to link the apportionment to the system constituents.
- ***Breakdown by accident types.*** *The approach allows unambiguous apportionment·classification of accident easy and uncontroversial.* The difficulties are to link the apportionment to the system constituents.

In the following section we are suggesting to develop a new approach based on functional analysis and FHA approaches to allocate safety targets to railway system, sub-systems and constituents.

4. Functional Breakdown Approach for CSTs Apportionment

4.1 Functional Railway System Breakdown

The AEIF has elaborated a group of TSIs. That was very important and innovative work, applied to the whole tran-

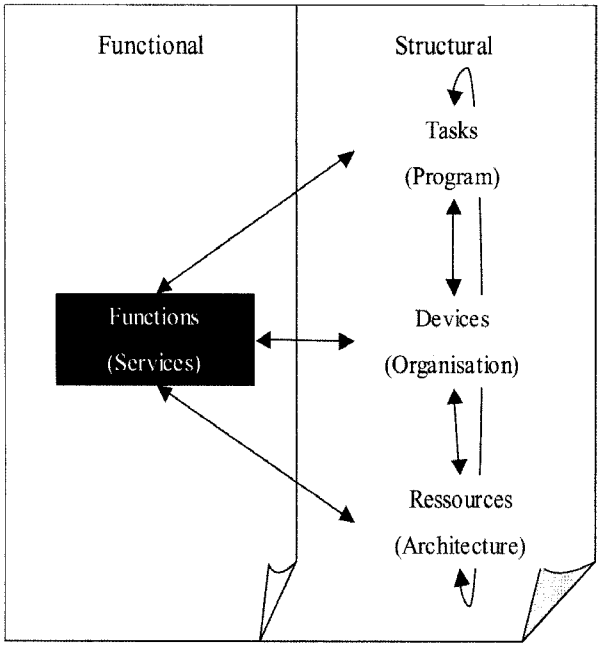

Fig. 2 Railway Analysis Matrix

sEuropean railway system. It was made possible by the large coverage of the fields of expertise necessary for its realisation. The AEIF has produced starting functions for generic railway architecture. These functions contain most of the Basic Parameters (BP) for interoperability. The BP are the basic constituents of the railway system.

The functional system analysis of railway systems, developed by the AEIF, is covering the full chain of railway transport. This analysis represents also a systematic and coherent decomposition of functions (functional breakdown) up to four levels of decomposition fulfilling the requirements of a functional breakdown.

The functional analysis method is based on a strongly structured analysis of a system from several points of view. Each point of view is dedicated to a particular aspect of the system: Functional and Structural [Fig. 2]. Each point of view defines unambiguously a type of specifications and a category of requirements. Simply put, the functional breakdown approach uses the railway architecture [10] developed by the AEIF, which is a functional system analysis of a conventional railway system covering the full chain of railway transport. This analysis represents a systematic and coherent decomposition of functions up to four levels. Next the hazards and ensuing accidents related to each function must be identified and quantified if accident statistical data is available.

The method of system analysis is based on a matrix consisted of two perspectives: functional, and structural [9].

- *Functional aspects.* This analysis aims to identify the functions of the system and their definitions, specifications and relations. It does not take into account any notion of implementation.
- *Structural aspects are mainly related to constituents that are allocated to perform the functions of the system. The network of resources constitutes the railway architecture. All constituents of the architecture must operate under a set of constraints like safety and interoperability.*

Functional Aspects

In order to facilitate the drawing of the borders between different TSIs and to check the consistency of the basic parameters and interfaces, an analysis taking into account only functions and resources had been considered as sufficient. Due to the enormous scope of the overall railway system, AEIF has selected specific functions relevant for interoperability for in depth analysis. The identified func-

Table 3. Railway Functions, by AEIF

Function	Description
F1	Support and guide the train
F2	Supply the train
F3	Load freight
F4	Load passengers
F5	Move rolling stock
F6	Maintain and provide data on rolling stock, infrastructure and timetable
F7	Prepare operation of train
F8	Operate a train
F9	Evaluate transport quality
F15	Provide service for passengers
F16	Provide service for freight
F17	Manage human resources

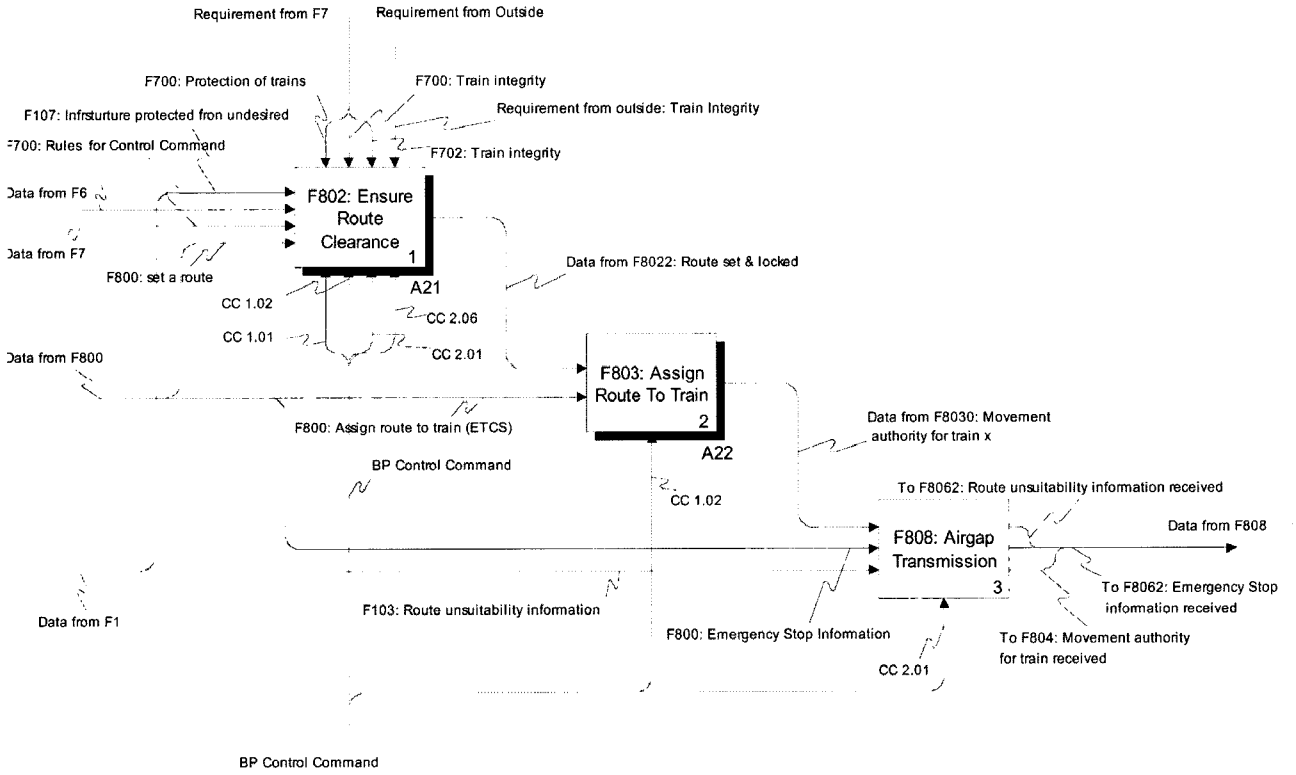

Fig. 3 SADT Model for Function "F8"

tions and their four sub-functions levels represent the railway system architecture. Table 4 provides the list of railway first-level functions.

The functional railway architecture has been created following the rules of SADT methodology [13] to model the decisions, actions and activities of a system. The models help to organise the analysis of a system and to promote good communication between the analysts and the users. SADT is useful in establishing the scope of an analysis, especially for a functional analysis [14].

The apportionment of global safety targets to railway functions needs to complete the description by FHA technique. The FHA provides CSTs [15], independent of technical realisations and implementation. Moreover, it provides reference values for deriving safety requirements at constituent level.

The Fig. 3 aims to show the interaction between the different levels of railway functions. To illustrate this example, we have chosen the function F8 "Operate a train" and 3 of its sub-functions.

The functional approach looks at all the phases, functions and processes taking place in the operation of a railway system. It identifies the hazards that may occur in each of these functions before evaluating the potential resulting risks associated with each function, process and subsequently the phase of operation (bottom-up).

Alternatively, it allows apportioning the global risk to each function.

A function uses input data, assuming that these verifying some conditions. It creates outputs that has to respect a number of requirements (safety, interoperability). Each function is represented by four elements.

- *Input data exist permanently. They can only be used if the conditions are fulfilled.*
- *Condition strongly influences the way the function is executed. It is closely linked to the input data.*
- *Requirement represents obligatory information associated to the output data, e.g. a safety requirement to be validated before or after execution.*
- *Output data is the result of the function.*

There are two ways to compose functions:

The first, with inputs and outputs, is common used and will not be listed here. Only data flow shall be checked between functions.

The second use conditions and requirements. All the sufficient conditions must be established by at least one function or an operational procedure. The way to proof if the conditions are complete can be either a mathematical demonstration, or some other specific test methods.

Structural aspects

Once the whole railway system has been described using SADT, the completeness of the given functional architecture can be clearly examined. In particular, undefined or

unspecified requirements are shown. Moreover, the huge quantity of information makes the architecture too complex. Thus, a clear separation between functions has to be done and requirements traceability has to be clarified with structural aspects [16].

When it comes to structure of railway systems, distinction can be made in:

- *Context: It is important to define the boundaries of the railway system with its environment;*
- *Operation: The operational structure refers to the operational process and the position of the players that make the system work;*
- *Techniques: The technical infrastructure refers to the hardware and to the physical means of production.*

A railway system can also be divided into partial systems, subsystems and components. Each level demands for another approach in risk identification and risk control. In order to put on most suitable methods and to obtain most reliable results, these levels should be taken into account during the whole process of risk management.

4.2 Functional Hazards Analysis

In his section, we present both principles of FHA and the methodology used to allocate safety targets to railway functions. FHA is an inductive hazard analysis technique. Inductive reasoning moves from specific observations to broader generalisations and theories. Informally, it is sometimes called a "bottom up" approach. In inductive reasoning, we begin with specific observations and measures, begin to detect patterns and regularities, formulate some tentative hypotheses that we can explore, and finally end up developing some general conclusions or theories.

In safety analysis, an inductive hazard analysis might conclude more than the given data [17]. It tends to be for hazard identification and not for the root cause identification. Moreover, as FHA is a qualitative approach, for a large system with many hazards, it is more interesting than quantitative risk characterisation. In system safety, it has been proved that qualitative techniques are very effective and provide generally decision-making ability comparable to quantitative analysis.

The FHA process involves performing a detailed system functions analysis. A key element for this methodology is to identify and understand all system functions. A function list must be created, and the use of functional flow diagrams is recommended because they provide an aid to the analysis. Each of these functions should be evaluated for the effect of the failure state on the system [18]. FHA process consists of 10 main steps :

1. Define Operation
2. Acquire Data
3. List Functions
4. Conduct FHA
5. Evaluate system Risk
6. Identify safety critical functions
7. Recommend correctiv action
8. Monitor corrective action
9. Track hazards
10. Document FHA

It is recommended to perform FHA using a worksheet. It makes the analysis more structured and rigorous. Typically, columnar-type worksheets are used [18].

The information required under each column in this worksheet deal with [Table 4] :

1. *Function & Sub-Function.* These columns list and describes each of the system functions and sub-functions.
2. *Hazard (H).* This column identifies the specific hazard evaluated for the functional failure.
3. *Effect (E).* This column identifies the effect and consequences of the hazard. The worst result is stated.
4. *Causal factors (CF).* The factors causing both the functional failure and the final effect.
5. *IMRI* It stands for Initial Mishap Risk Index. This column provides a qualitative measure of risk, where risk is a combination of severity and probability.
6. *Recommended Action (RA).* It is related to preventive measure to control identified hazards.

The principles of FHA seem to be very simple and it is continually updared as new information becomes available.

4.3 Performing FHA in railways

As the FHA method is based on researches on a proof oriented systems, we have adopted a modelling framework derived from the general system theory. This framework provides us with a set of generic modelling points of view of railway system in which they are represented as network of process [17].

A railway system is constituted by a set of functions that are executed by tasks. They are supported by the railway

Table 4. FHA Worksheet

System		Hazard Analysis			Safety Targets	
Function	Sub-function	Hazard	Effect	Causal factors	IMRI	Recommended Action
①	①	②	③	④	⑤	⑥

representative architecture. The tasks are influenced and characterised by several modes. In fact, the tasks, which will be carried out, will depend on the current mode and operational context. The components of the architecture will be organised in set of devices assigned to the tasks in close relation with available resources. These subsets of resources architecture will be allocated to tasks. Such subsets of resources allocated to tasks will be denoted hereafter as "devices" in our terminology. The system itself works in various operational contexts (strategic, control and managements) requiring an adaptation of the resources ensuring the functions.

To go over these limits, the combination of FHA with the railway architecture is proposed. In fact, this representative architecture is considered as a basis of our work. We try to exploit this architecture in order to go over the limits of the available breakdown. It can be assumed that when functional analysis is useful in allocating the risk, it should be possible to modify it to perform the system functionality. Thus, it allows the technical components needed to achieve the allocated functionality.

Based on the functional breakdown approach, a five-steps approach (Fig. 4) has thus been conducted [8]:

- *Given the functional railway architecture breakdown proposed by the AEIF, build the corresponding SADT model;*
- *Choose the safety acceptance criteria (Safety Target) to be adopted in the European Community in order to comply with European Safety Directive;*
- *Transform the safety acceptance criteria into specific safety target (qualitative and quantitative);*
- *Propagate the specific safety target through the functional breakdown;*
- *Check the consistency with the Safety Integrity Levels (SILs) and other safety requirements of constituents and subsystem levels.*

The described functional analysis methodology is applied on all of these subsystems. These subsystems are performed by a number of functions, which are implemented by a number of resources and programmes. All these elements constitute the Representative Architecture of the conventional rail system [11].

4.4 CST apportionment of rail sub-systems

The aim of this work is to respond to the European directive [19] on the interoperability of the transEuropean conventional railway system. The continuation of this objective should lead to the definition of a minimal level of parameter. The railway system is decomposed in six sub-systems that are: energy, infrastructure, control command and signalisation, rolling stock, operation and telematic. The maintenance is specific in every sub-system.

At the first level of the decomposition [11], 12 functions have been identified (Table 3). The second and the third level of the functions breakdown can then be detailed in further steps. For the first two functional levels, the link with the sub-systems (e.g. operations) is defined via the basic parameters.

This approach showed that if some functions can clearly be allocated to the IM or to the RU, responsibilities within other functions are shared. The shared responsibility aspect of some functions may derive from the goal of the function that involves both the IM and the RU or from the way it is implemented. Ensuring safe railway operations can also be expressed in a qualitative way. Both qualitative and quantitative safety targets can be allocated from a bottom-up approach as well as a top-down approach. A global CST is expressed as a risk (i.e. a combination of frequency and severity of harmful events). This implies that the specific CST should also be expressed as a risk, namely as a portion of the global residual risk. What would however be most useful for operators and suppliers alike is to know what should be the acceptable frequency rate of events such as an accident, a hazard, and more importantly, a function fault, a constituent dangerous failure, etc., so as to determine specific safety requirements on parts of the railway system, particularly for new systems. Thus it is important to stress that whichever way the risks might be apportioned for defining CSTs, there will still be some rather complicated safety allocation process necessary behind in order to derive (qualitative and quantitative) safety requirements.

The CSTs are the reference to derive CSTs for the various parts of the railway system because the specific acceptable risk levels should be derived for these different parts of the railway system as well as for the global safety targets. This suggests an apportionment of global safety targets to specific parts of the railway system although we would stress that this should not become a method that is adopted too generally.

According to the European Railway Safety Directive [6], the CSTs shall define the safety levels that must at least be reached by different parts of the railway system and by the system as a whole in each Member State for :

- individual risks relating to passengers, staff including the staff of contractors, level crossing users and others, and, without prejudice to existing national and international liability rules, individual risks relating to unauthorised persons on railway premises;
- societal risks. As the societal risk isn't clearly defined, a proposal to consider it as being the sum of risks

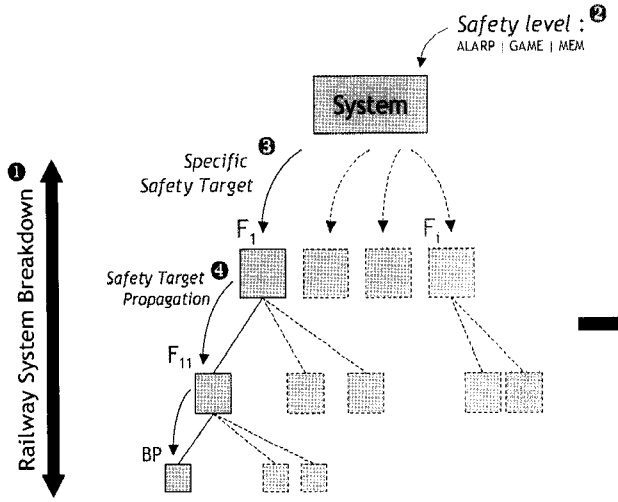

Fig. 4 Functional Risk Apportionment

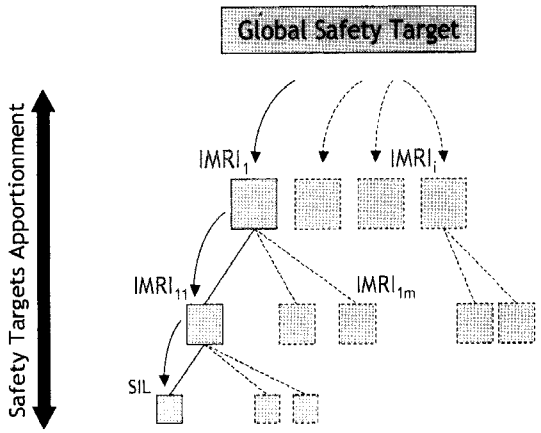

Fig. 5 Global Risk Apportionment

relating to the different individual risks listed in the Safety Directive. In this proposal, "global safety targets" indicates "societal risks". In other words, assumed that global safety target allocated to a function is IMRI.

$$IMRI_i = \sum_{j=1}^{j=n} IMRI_j \quad (1)$$

The equation (1) represents the apportionment of global safety targets where i is the considered function and n the number of sub-functions of a same level, related to the function i.

Table 4 illustrates the application of FHA to determine IMRI in railways. The adopted IMRIs will be based on the CENELEC standards [7] which define different levels of risk.

The lowest level of functions concerns the basic parameters of railway system. These components mean any regulatory, technical or operational condition which is critical to interoperability [5]. The risk level for the BP has been defined as Safety Integrity Level (SIL). SILs are measures of the safety of a given process. They are defined by means of the probability for fault. Great importance is also attached to methods in order to avoid design faults and methods in order to deal with faults that occur during operation [19]. The table differs between continuous use of safety functions and functions that are seldom used. Specifically, to what extent can the end user expect the railway system to perform safely, and in the case of a failure, fail in a safe manner?

According to these basic parameters and SIL concepts, the FHA methodology would be useful in the functional risk apportionment approach. In fact, if we consider the societal risk as the risk allocated to the railway system, it would be evident that the lowest level of functions - which is the basic parameters level - would contain both of IMRI and which SIL that is connected to every function.

- *The first step to create this approach is to decide what is to be regarded as basic functions, of lowest level. When the BP are known, it is time to start discussing how well done this functions have to be.*
- *The second step is to assign an IMRI to every function. The different functions of the railway system can have different IMRIs depending on the importance of the function.*

The extension of this approach by integrating the other requirements (e.g. SIL) in the IMRI takes into consideration the subsystems and constituents safety requirements. To make the developed approach applicable in practice, certain quantitative considerations and breakdown rules have to be established.

5. Conclusion

The common safety targets, indicators and methods are closely linked and can not be treated separately. It shows also that the basic element to develop the common safety targets and methods is the establishment and the agreement on common definition of railway system. The use of the functional architecture of railway system as basis for safety tergets apportionment is the most promising approach. The approach proposed allows the definition of global safety targets and the development of safety targets related to specific parts of the system. The functional representative architecture developed by AEIF to define a railway generic system to be used by all stakeholders [11]. This architecture defines a number of functions covering all railway system. Based on the railway functional representative architecture, the FHA can be used to define the safety targets allocated to the functions. The paper high-

lights the use of Functional Hazards Analysis for risk apportionment in railway systems. The suggested approach is based on functional breakdown of railway systems and the use of FHA to the apportionment of the global safety targets. The IMRI (Initial Mishap Risk Index) is used to cover both qualitative and quantitative analysis of the railway functions. The qualitative approach of this analysis is examined in this paper using an example of railway function. The combination of qualitative and quantitative risk apportionment is under development combining functional analysis and stochastic Petri Nets as a basis for simulation and tool for. evaluating the dynamic propagation of specific safety targets.

Reference

1. Cassir C., Dupont, P.-J., Galley, P., Kuijlen, H., Lemaire, E., Lopez, L., Patacchini, A., Vanstaen, G., Reinartz, S. and Salander, C. D.1.3.3 : Specific CSTs report Case study, www.samnet.info, 31p., June 2005.
2. Kuijlen, H., and VanDerBerg, P. D.2.3.0 : Common Safety Methods. www.samnet.info, 37p., September 2004.
3. European Commission. Directive 2001/14/EC of the European Parliament and of the Council on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification. 26 February 2001.
4. European Commission. Directive 96/48/EC on the interoperability of the trans-European high speed rail system. 23 July 1996.
5. European Commission. Directive 2001/16/EC of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system. Official Journal of the European Union, L110, pp. 1-27, 20 April 2001.
6. European Commission. Directive 2004/49/EC on 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). Official Journal of the European Union, L164, pp. 44-113, 29 April 2004.
7. European Committee for Electrotechnical Standardization. CENELEC EN 50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Saftey (RAMS). 1 September 1999.
8. Rafrafi, M., Bourdeaud'Huy, T. and El Koursi, E.-M. Risk Apportionment Methodology Based On functional Analysis. *Proc. IMACS Multiconference on Computational Engineering in Systems Applications* CESA'2006, Beijing, 4-6 October 2006, Vol2, pp. 1103-1109.
9. Chatel, V., El Koursi, E.-M., Felliot, C. and Huismann, U. Functional analysis of the sub-system of energy and infrastructure of conventional rail. *Proc. IEEE International Conference on Systems, Man and Cybernetics IEEE SMC*, Hammamet, 6-9 October 2002, Vol 3, 6p.
10. www.epp.eurostat.ec.europa.eu
11. Gigantino, A. Report on the Representative Architecture. AEIF, September 2002.
12. Guldenmund, F.W., Hale, A.R. and Bellamy, L.J. The development and application of a tailored audit approach to major chemical hazard sites. In *SEVESO 2000. Risk Management in the European Union of 2000: The Challenge of Implementing Council Directive 96/82/EC "SEVESO II"*, European Conference in Athens, 10-12 November 1999, European Commission, Brussels, 2001, pp. 275-288.
13. El Koursi, E.-M. and Tordai, L. Common approach for supervising the railway safety performance. *Proc. COMPRAIL*, Prague, 2006.
14. Rafrafi, M. and El Koursi, E.-M. Functional Hazards Analysis for Railway Safety. Proc. Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems FORMS/FORMAT, Braunschweig, 25-26 January 2007, pp. 164-173.
15. Wilkinson, P. J. and Kelly, T. P. Functional Hazard Analysis For Highly Integated Aerospace Systems. *Proc. IEE Seminar on the Certification of Ground/Air Systems*, London, 17 Februrary 1998, Vol 4, pp. 1-6.
16. Ericson, C. A. Hazard Analysis Techniques for System Safety. Wiley, 2005.
17. European Commission. Directive 91/440/EEC on the development of the Community's railways. 29 July 1991.
18. Ben, J.M. Ale. The Occupational Risk Model. Final Report of the Workgroup on ORM. Risk Centre, Technical University Delft, 2006.
19. Christophe Cassir "Apportionment of Safety targets (to TSI sub-systems) and Consolidation of TSIs from a safety point of view" WP1.1 Assessment of the feasibility to apportion Common Safety Targets, February 2007.