Abstract—The paper presents an overview of the common regulatory framework for railway safety. Safety levels in the Community railway system are generally high, in particular compared to road transport. However, it is necessary to very least maintain safety during the liberalization process and, in line with technical and scientific progress, to further improve it, when reasonably practicable, taking into account the competitiveness of the rail transport mode. The paper will analyze the requirements present in the common standards and will propose a guide to choose the best method for the risk evaluation.

Keywords—railway systems; safety; risk; technical rules

I. INTRODUCTION

Transport is a key factor in modern economies. But there is a permanent contradiction between society, which demands ever more mobility, and public opinion, which is becoming increasingly intolerant of chronic delays and the poor quality of some transport services. As demand for transport keeps increasing, the Community's answer cannot be just to build new infrastructure and open up markets. The transport system needs to be optimized to meet the demands of enlargement and sustainable development and therefore it is necessary a new regulatory framework [1].

A modern transport system must be sustainable from an economic and social as well as an environmental viewpoint.

Plans for the future of the transport sector must take account of its economic importance. Total expenditure runs to some 1 000 billion euros, which is more than 10% of gross domestic product. The sector employs more than ten million people. It involves infrastructure and technologies whose cost to society is such that there must be no errors of judgment. Indeed, it is because of the scale of investment in transport and its determining role in economic growth that the authors of the Treaty of Rome made provision for a common transport policy [1].

A result of this policy was to develop the most modern techniques within a European framework of interoperability. Projects launched at the end of the 1980s are now bearing fruit, as symbolized by the trans-European high-speed rail network.

However, modern techniques and infrastructure have to be matched by modernization of company management, particularly in the railway field.


This directive assumes that safety levels in the Community rail system are higher than road transport. The liberalization process has to increase the competitiveness of the railway sector but it does not have to affect its safety. On the contrary, thanks to the improving in the technological solutions, the effort has to be addressed to its increasing.

However, it is necessary to very least maintain safety during the liberalization process and, in line with technical and scientific progress, to further improve it, when reasonably practicable, taking into account the competitiveness of the rail transport mode.

Requirements on safety were established imposing technical common standards (technical specifications for interoperability (TSIs)) and common methods (common safety methods (CSMs)).

At the same time performance indices (common safety indicators (CSIs)) were introduced, together with common safety objectives (common safety targets (CSTs)).

This standardization wanted to provide tools for assessment of the safety level and the performance of the operators at Community level as well as in the Member States.

All those operating the railway system, infrastructure managers and railway undertakings, should bear the full responsibility for the safety of the system, each for their own part. Every infrastructure manager has a key responsibility for the safe design, maintenance and operation of its rail network.

Therefore, in carrying out their duties and fulfilling their responsibilities, infrastructure managers and railway undertakings should implement a safety management system (according to requirements and criteria inside the Commission Regulation (EU) No 1169/2010 of 10 December 2010), fulfilling Community requirements and containing common elements. Information on safety and the implementation of the safety management system should be submitted to the safety authority in the Member State concerned.

In this context, the safety certificate should give evidence that the railway undertaking has established its safety management system and is able to comply with the relevant safety standards and rules.
In the case of railway safety, the safety management system can be defined as that part of the business system that allows to identify and minimize risks associated with the satisfaction failure of its customers, through a proper management of resources, rules and own organization. Attention is given to the functional safety that is that part of safety that is dependent upon the functions of a system in the normal operation, in response to external stimuli and under failure modes. In fact, with difference to the safety concept, that is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment, functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs [3]. As stated in [4], it looks at aspects of safety that relate to the function of a device or system and ensures that it works correctly in response to commands it receives. In a systemic approach functional safety identifies potentially dangerous conditions, situations or events that could result in an accident that could harm somebody or destroy something. It enables corrective or preventive actions to avoid or reduce the impact of an accident. Therefore, functional safety is the detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the fight consequence of the hazardous event. The IEC 61508 series are the International Standards for electrical, electronic and programmable electronic safety related systems [5].

The complexity of the subject is due to the intricacy of the system and the lack of standardization aspects. This is even more true for innovative transportation systems such as urban and suburban systems [6]-[8].

This paper aims to illustrate the main criteria and methods for controlling the risks involved in the current regulatory framework for the railway sector.

II. RISKS EVALUATION

Based on the rules mentioned above, each infrastructure manager and railway undertaking shall be made responsible for its part of the system and its safe operation, including supply of material and contracting of services, vis-à-vis users, customers, the workers concerned and third parties.

The main requirements for a correct approach in the risks evaluation concerning the railway field are described in the common methods for the management of the changes. It is important to take into account what told above regarding the high safety levels in the Community rail system, in particular compared to road transport. Therefore the focus is to control the changes processes.

The most important technical rules for this sector are the Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013, the CEN/CEI EN 50126/2000 and its guide to application CEI CLC/TR 50126-2 of 2007 [10]-[11]. Moreover there is the directive 2008/57/EC on the interoperability of the rail system within the Community, that repealed Directives 96/48/EC and 2001/16/EC from 19 July 2010.

The paper will present the main contents of these rules, trying to give an overview on the main safety aspects.

III. CHANGES MANAGEMENT PROCESS

The Commission Regulation (EU) No 402/2013 of 30 April 2013 describes a common safety method for risk evaluation and assessment [9]. This Regulation shall apply to the proposer (company or organization in charge of implementing the change) when making any change to the railway system in a Member State. Such changes may be of a technical, operational or organizational nature. Whether or not a change is significant for the safety in a Member State, proposer should initially consider the potential impact of the change in question on the safety of the railway system. If the proposed change has an impact on safety, the proposer should assess, by expert judgement, the significance of the change based on a set of criteria, such as:

- failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system under assessment;
- novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new for the organization implementing the change;
- complexity of the change;
- monitoring: the inability to monitor the implemented change throughout the system life-cycle and intervene appropriately;
- reversibility: the inability to revert to the system before the change;
- additionality: assessment of the significance of the change taking into account all recent safety-related changes to the system under assessment and which were not judged to be significant.

The evaluation lets to understand whether or not a change is significant. When a change is significant, the method described in the Procedure shall be applied and the risk acceptability of the system under assessment shall be evaluated by using one or more of the following risk acceptance principles:

(a) the application of codes of practice;
(b) a comparison with similar systems
(c) an explicit risk estimation

Based on the method application, the risk estimation means the process used to produce a measure of the level of risks being analysed, consisting of the following steps:

- hazards identification;
- estimation of frequency;
- consequence analysis;
- integration of the previous factors
- verification of the acceptability of the level of a risk, that means that it is not necessary to take any immediate action to reduce it further.

The hazard identification shall be carried out after the system definition, that shall address at least the following issues: (a) system objective (intended purpose);
The safety measures are a set of actions either reducing the risk of the system under assessment or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk.

IV. INFRASTRUCTURAL CHANGES

The Italian law D.Lgs 191/2010 sets out to establish the conditions to be met to achieve interoperability within the Community rail system. These conditions concern the design, construction, placing in service, upgrading, renewal, operation and maintenance of the parts of this system as well as the professional qualifications and health and safety conditions of the staff who contribute to its operation and maintenance.

Therefore, the concept of interoperability covers both tangible objects and intangible objects such as software. This law defines ‘interoperability constituents’ any elementary component, group of components, subassembly or complete assembly of equipment incorporated or intended to be incorporated into a subsystem, upon which the interoperability of the rail system depends directly or indirectly.

A TSI sets all the conditions with which an interoperability constituent must conform, and the procedure to be followed in assessing conformity. In addition, it is necessary to specify that every constituent must undergo the procedure for assessing conformity and suitability for the use indicated in the TSIs, and have the corresponding certificate.

It is important to discriminate the changes on the infrastructure, at least:
- upgrading, that means any major modification work on a subsystem or part subsystem which improves the overall performance of the subsystem;
- renewal that means any major substitution work on a subsystem or part subsystem which does not change the overall performance of the subsystem.

The interoperability constituents shall comply with the essential requirements if they obtain the EC declarations of conformity or suitability for use. The structural subsystems, on which the railway systems are based, can be considered as interoperable and laid down to the essential requirements when they have the EC declaration.

The general safety essential requirements regard safety, reliability and availability, health, environmental protection and technical compatibility.

The evaluation is performed by the notified bodies which are responsible for assessing the conformity or suitability for use of the interoperability constituents or for appraising the ‘EC’ procedure for verification of the subsystems.

Therefore the EC declaration of conformity or suitability for use is necessity and sufficiency to demonstrate the respect of what imposed by the law regarding the interoperability principles.

Finally, it is important to underline that Dgls 162/2007 imposes to the railway infrastructure manager to publically open a new or renovated railway line or a line with new structural subsystems, only after having all the certifications, homologations and authorizations requested by the directives and the EC declaration is considered as a homologation document and therefore as necessity.

The significant changes can be performed only after having the commissioning Authorization released by the national Authority.

Figure 1 depicts a flowchart of the changes management process with reference to the two rules above described.

A. Code of Practice

Code of practice means a written set of rules that, when correctly applied, can be used to control one or more specific hazards.

Analyzing the contemporary regulatory contest, it is possible to consider as code of practice:
- Technical specifications for interoperability (TSIs)
- National rules notified

If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional safety measures shall be identified by applying one of the two other risk acceptance principles.

B. Use of reference system

Based on this criteria, it is necessary to analyze whether one, several or all hazards are appropriately covered by a similar system that could be taken as a reference system.

A reference system shall satisfy at least the following requirements:
- it has already been proven in-use to have an acceptable safety level;
- it has similar functions and interfaces as the system under assessment;
- it is used under similar operational conditions as the system under assessment;
- it is used under similar environmental conditions as the system under assessment.
If a reference system fulfills the requirements, then for the system under assessment the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system.

If at least the same safety level as the reference system cannot be demonstrated, additional safety measures shall be identified for the deviations, applying the explicit risk estimation.

**C. explicit risk estimation**

When the explicit risk estimation is requested, a deeper analysis is necessary using the quantitative or semi-quantitative approaches, according with EN 50126:2000 Railway applications and CEI CLC/TR 50126-2 of 2007-06 “Parte 2: Guide to the application of EN 50126-1 for safety”.

The required method should be selected carefully to provide the degree of risk assessment required for the operations being considered. Qualitative ranking schemes for frequency and consequence may be appropriate as a first pass at assessing risk or for assessing risk in simple cases. Generally, a qualitative ranking approach would not be adequate in a risk assessment and a more explicit method is necessary.

All the methods for the risks evaluation are affected by uncertainties and their results have to be used only as input data for the decisional process. Therefore the risks evaluation process has to be considered as procedure that helps to strongly reduce the uncertainty grades. These methods have to be applied conveniently and they can be combined depending on the hazard and functional failure typologies and on the uncertainty grade in the input data.

The risks estimation process consists in the estimation of:

- frequency of occurrence of the hazard;
- evaluation of the consequences;
- combination of these factors.

Referring to the consequences, the European regulations define the Fatalities and Weighted Seriou Injuries (FWSI) index as a measure of fatalities. Based on this definition, a severe injury corresponds to 0.1 FWSI. The technical regulation has not fixed a specific value for minor injuries but the literature states a minor injury equal to 0.01 FWSI.

Similarly, starting from the definition of “significant accident” reported in the Commission directive 2014/88/UE, it is possible to quantify also the equivalent economic damage expressed in FWSI [14]. In fact it is reasonable to set equal to
0.1 FWSI a significant damage to stock, track, other installations or environment, that the regulation fix equal to EUR 150.000.

Based on these definitions, the qualitative classification table (CEI-EN-50126:2000) of the typical hazard severity levels and the consequences associated with each severity level can be quantified. Table I reports possible severity values G associated to each severity level.

Table I – Hazard Severity Level

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>FWSI Consequences to persons or environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>G&gt;1 Fatalities and/or multiple severe injuries and/or major damage to the environment.</td>
</tr>
<tr>
<td>Critical</td>
<td>0,1 &lt;= G &lt;= 1 Single fatality and/or severe injury and/or significant damage to the environment.</td>
</tr>
<tr>
<td>Marginal</td>
<td>0,01 &lt; G &lt; 0,1 More than one minor injury and less than one severe injury and/or significant threat to the environment</td>
</tr>
<tr>
<td>Insignificant</td>
<td>G &lt;= 0,01 One or less minor injury</td>
</tr>
</tbody>
</table>

D. Semi-quantitative Approach

When data are available or a good degree of judgment can be applied to estimate the frequency and consequences of each hazard, a greater level of accuracy and consistency in the risk estimation can be obtained by using a semi-quantitative risk ranking approach.

Risk evaluation shall be performed by combining the frequency of occurrence of a hazardous event (number of hazards per year) with the severity of its consequence (damages to persons and environment) to establish the level of risk generated by the hazardous event.

Figure 2 provides, in qualitative terms, typical categories of probability or frequency of occurrence of a hazardous event and a description of each category for a railway system.

The categories, their numbers and their numerical scaling to be applied shall be defined by the Railway Authority, appropriate to the application under consideration. An example of frequency ranking scheme derived from CEI CLC/TR 50126-2 is reported in Figure 3.

![Fig. 3. Example of frequency ranking scheme - CEI CLC/TR 50126-2](image)

Using the data available in the database, frequency of occurrence of each hazardous event can be calculated as the mean value of the number of events occurred in the last eight years, starting from the year previous the observation period. Once that F and G are estimated, the frequency - consequence matrix reported in Figure 4 lets to identify the risk level associated to the considered hazardous.

![Fig. 4. Frequency-consequence matrix](image)

The table reported in Figure 5 defines qualitative categories of risk and the actions to be applied against each category.

![Fig. 5. Frequency-consequence matrix](image)

E. Quantitative Approach

The semi-quantitative method presents limits concerning the uncertainty. The first problem is that, referring to the frequency, it is possible to estimate only events at least remote, since no more historical data are available. Improvable or incredible
values need the existence of a long-term database, since an improbable event happens every 100 years and an incredible event every 500 years.

A great care has to be addressed to that events that can be classified as improbable or incredible due to the available information, leading to underestimate events with consequences potentially serious. In these cases quantitative approaches are suggested.

The cases in which the semi-quantitative approaches cannot be considered as absolute are:

- the evaluation process identifies hazardous with fatalities and/or multiple severe injuries
- the risk evaluation denotes that the individual risk for one or more risk categories can fall in the intolerable area
- there is a significant contribution to the collective risk and there is an uncertainty grade in the frequency estimation

These cases require a deeper analysis using more suitable methodologies chosen and applied by qualified personnel. The technical regulation suggests to implement one of the following methods of quantitative evaluation: ALARP, GAMAP/GAMA, MEM, FMEA/FMECA, FTA.

V. GUIDELINES FOR THE CHOICE OF THE METHOD

After a deep analysis of the constraints set in the regulations and the positive and negative aspects of each method, a guideline is presented. Table II shows how to choose the best risk evaluation method, taking into account the presence of the event in the historical database and its impact.

Table II – Hazard Severity Level

<table>
<thead>
<tr>
<th></th>
<th>G &lt; 0,1 FWSI</th>
<th>≤ G &lt; 1 FWSI</th>
<th>G ≥ 1 FWSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitored hazards that are classified as frequent or probable</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Monitored hazards that are classified as occasional or remote</td>
<td>A</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>Unmonitored hazards or monitored hazards that cannot be classified as frequent, probable, occasional or remote but that have to be considered since their potential catastrophic consequence (unseen frequency)</td>
<td>C</td>
<td>B</td>
<td>B</td>
</tr>
</tbody>
</table>

The cases marked with the letter “A” present the possibility to maintain the reference to the historical data inserted in the database. Therefore the criteria based on the acceptability matrix before described can be applied.

The cases marked with the letter “B” require a deeper analysis using methods of quantitative evaluation, such as ALARO, GAMAP/GAMA, MEM, FMEA/FMECA, FTA.

In the cases marked with the letter “C” it is possible to use the criteria code of practice and reference system defined in the regulation UE 402/2013 and described in the previous Paragraph. When these criteria show that the risk can be considered as acceptable, no more deeper analysis is necessary. When these criteria do not confirm the acceptability of the risk, it is necessary to refer to the case “B”.

VI. CONCLUSIONS

The paper presented an overview of the common regulatory framework for railway safety. The liberalization process of the railway transportation system meant to find common standards without affecting the safety level. On the contrary, it is necessary to very least maintain safety and, in line with technical and scientific progress, to further improve it, when reasonably practicable, taking into account the competitiveness of the rail transport mode.

The paper analyzed the indication given in the common standards regarding the risk evaluation and safety management in order to underline the most important warnings and limits. The different methods that can be adopted are described, highlighting the assessment of the adequacy of the methods.

Finally, guidelines for the choice of the right method, considering the regulatory constrains, has been proposed.

REFERENCES