Limits and opportunities of risk analysis application in railway systems

R. Licciardello[1], A. Baldassarra[1], P. Vitali[1], A. Tieri[2], M. Cruciani[1] & A. N. Vasile[1]
[1]*DICEA – Sapienza University of Rome, Italy*
[2]*DITS srl, Italy*

Abstract

Risk analysis is a collection of methods widely used in many industrial sectors. In the transport sector it has been particularly used for air transport applications. The reasons for this wide use are well-known; risk analysis allows us to approach the safety theme in a stochastic – rather than deterministic – way, it forces us to break down the system in sub-components. Last, but not least, it allows a comparison between solutions with different costs, introducing de facto an element of economic feasibility of the project alternatives in the safety field. Apart from the United Kingdom, in Europe, the application of this tool in the railway sector is relatively recent. In particular, Directive 2004/49/EC (the "railway safety directive") provides for compulsory risk assessment in relation to the activities of railway Infrastructure Managers (IMs) and of Railway Undertakings (RUs). Nevertheless, the peculiarity of the railway system – in which human, procedural, environmental and technological components have a continuous interchange and in which human responsibilities and technological functions often overlap – induced the EC to allow wide margins of subjectivity in the interpretation of risk assessment. When enacting Commission Regulation (EC) No 352/2009 which further regulates this subject, a risk assessment is considered positive also if the IM or RU declare to take safety measures widely used in normal practice. The paper shows the results of a structured comparative analysis of the rail sector and other industrial sectors, which illustrate the difficulties but also the opportunities of a transfer towards the railway system of the risk analysis methods currently in use for the other systems.
Keywords: railway risk assessment, comparison with road and industry.

WIT Transactions on The Built Environment, Vol 134,
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE130131

1 Introduction: recent developments in the European railway system organization

The studies in the field of the railway operations move along an ideal hyperbole describing the inverse relationship that exists between safety and supply capacity in the railway systems [1–3]. During railway system's development, the necessity of maximum safety often prevailed against the target of maximum capacity, both for cultural approach and for the fact that every European rail company, apart from enjoying a monopoly on the entire national system, had in itself the whole chain of industrial and commercial process, from the line construction and management to the traffic organization, even the commercial services.

In recent years, social events and technological developments changed this setting. For example, focusing on the Italian situation, first the privatization of the "Ferrovie dello Stato" group and then the corporate unbundling, that did the group splitting between engineering services (Italferr), infrastructure manager (RFI) and railway undertaking (Trenitalia), entailed an increasing attention to economic processes' efficiency. Moreover, the market liberalization for railway undertakings caused the births and, in a few years, the multiplication of companies operating in goods transport, while in passenger transport a real competition with Trenitalia comes true only now, after many years of a de facto monopoly.

Also the construction of lines and trains that can reach speeds of about 200 km/h changed in some important cases, as Rome – Milan, the service of rail transport in substitution of the plane, forcing an increase of traffic frequency on some routes.

Over the years the concept of safety changed too. It's increasingly closer to become in acceptance of risk, but not yet in the current Italian legislation. This does not mean that there is less focus on the central theme of transport safety, but rather the attempt to insert a standard of feasibility in the railway system.

2 Railway liberalization and safety in Europe

Railway liberalization in the European Union is still growing after two decades. The adoption of technical specifications for interoperability (TSIs), designed to make interoperable the various national systems and to uniform level of safety EU Member States, helped the European Commission to open to free competition between companies that manage the transportation service.

The first point to highlight is the system of authorisation and certification of railway safety, because the coming of the independence of RUs from State control (privatization process) and a first separation between RUs and IMs (process of industrial chains unbundling) indirectly delegated procedure implementation of system safety to the same RUs and IMs, so no more to the States, guarantor "super partes" of the population safety.

This package also contains the Directive 2004/49/EC, called "Railway Safety Directive". This Directive lays down general guidelines for the definition of

common European policies relating to railway safety, presenting the fundamental "purpose" (art.1) of harmonising the regulatory structure in the Member States. This legislation represents a significant turning point in the field of railway safety: on the one hand (art.4, par.1) "Member States shall ensure that railway safety is generally maintained and, where reasonably practicable, continuously improved", on the other the same (art.4, par.3) "Member States shall ensure that the responsibility for the safe operation of the railway system and the control of risks associated with it is laid upon the IMs and RUs, obliging them to implement necessary risk control measures, where appropriate in cooperation with each other, to apply national safety rules and standards, and to establish safety management systems (SMSs)".

This must be based on Common Safety Methods (CSMs), that (art.2, par.2-f) "means the methods to be developed to describe how safety levels and achievement of safety targets and compliance with other safety requirements are assessed", to reach the Common Safety Targets (CSTs), that (art.2, par.2-e) "means the safety levels that must at least be reached by different parts of the rail system and by the system as a whole, expressed in risk acceptance criteria", that is expressed through the Common safety indicators (CSIs), introduced by the same Directive, that means indicators of occurrence that can standardize the assessment of the system safety and give an indication on the achievement of CSTs, in order to facilitate monitoring.

It is important to highlight the issue of Commission Regulation (EC) No 352/2009 on the adoption of a CSM on risk evaluation and assessment. By now, even the culture of the railway world must address the risk analysis, after decades that the approach to accident prevention was always deterministic. The Regulation, conforming to Directive 2004/49/EC, requires RUs and IMs to apply, in case of new systems introduction or in case of "significant change" of a system, a CSM to effectuate a risk management process and independent assessment about system safety, based on risk assessment and analysis. In Regulation annex I "the risk assessment process is the overall iterative process that comprises: a) the system definition; b) the risk analysis including the hazard identification; c) the risk evaluation."

Regarding point b), regulation requires three possible criteria to apply for evaluating the acceptability of risk that are: use of codes of practice, use of reference system and explicit risk estimation both qualitative or quantitative. From this it follows that if you want to implement a new technology or a new system, the only way forward is the application of an extended risk analysis.

3 Application of risk analysis in the railway sector

3.1 Common safety method for the rail risk assessment

As mentioned above, the Commission Regulation (EC) N. 352/09 has the aim of introducing a Common Safety Method (CSM) for risk evaluation and assessment methods in railway sector mentioned in Article 6(3)(a) of Directive 2004/49/EC.

The CSM, favouring the access to the rail transport service market, promotes (Article 1(2)) "the harmonisation of:

a) the risk management processes used to assess the safety levels and the compliance with safety requirements;
b) the exchange of safety-relevant information between different actors within the rail sector in order to manage safety across the different interfaces which may exist within this sector;
c) the evidence resulting from the application of a risk management process."

The iterative process of risk management is framed in three main phases:

1. systematic identification of hazards, on basis of system definition and corresponding safety measures and requirements.
2. analysis and evaluation of risks;
3. demonstration of the compliance of the system with identified safety requirements.

The hazards are identified by wide-ranging expertise from a competent team and they are registered in the "hazard record".

The classification of the hazard is carried out according to their evaluated risks, to focus the assessment on the main risks.

For this assessment the CSM identifies the following three criteria of risk acceptance, to be applied during the phases of risk evaluation and analysis:

1. Use of codes of practice and risk evaluation (compliance to TSI, national and European);
2. Use of reference system and risk evaluation (uniformity between safety level of reference system and the system to be evaluated)
3. Explicit risk estimation and evaluation (risk estimation deriving from hazard, in qualitative and/or quantitative manner).

The codes of practice shall at least: a) have a wide recognition in the rail sector, otherwise, these codes must be accompanied by any necessary explanations and must be deemed acceptable to the assessment, b) be relevant to the containment of the considered hazards in the system under assessment; c) be available for all those who want to use them.

A reference system shall at least: a) has already been proven in practice, to ensure an acceptable level of safety and to be approved in the Member State in which the change is to be introduced, b) has similar functions and interaction similar to those the system under assessment, c) it is used under similar operational conditions as the system under assessment, d) be used under similar environmental conditions as the system to be evaluated.

The explicit and accurate determination of risk must meet at least the following requirements: a) the methods used must faithfully represent the system under assessment and its parameters (including all operational modes), b) the results should be sufficiently accurate to serve as a solid basis for decision making.

The guidelines [4] show different examples of the application of the previous criteria; in the next section we report one in which all three criteria are used,

while in the next there is the suggested methodology for risk analysis in extended tunnel, the only legislated example in Italy.

3.2 An example of use of all criteria

The example concerns a technical change to the control-command system: the substitution of a loop located on the ground before a signal with a subsystem "radio infill + GSM." The function of the "loop + encoder" in the existing system is to output the signal at the approach of a train when the stretch behind the signal (i.e. in front of the approaching train) is free. The evaluation of the risk has to demonstrate that the system maintains the same level of safety pre-modification. In the following paragraphs are presented the logical scheme of the risk assessment.

The change is considered significant due to two criteria: complexity and novelty. For the identification of hazards, applying the iterative process of risk assessment and the identification of hazards on the basis of a brainstorming carried out by a group of experts in order to: (1) identify hazardous events with substantial influence on the risk determined by the desired change, (2) identify possible actions to control the risk. Since the loop, and then the radio infill, emits the signal, there is the risk of giving an unsafe movement authority to the approaching train, when the previous train still occupies the block section in front of the signal. The risk must be controlled to an acceptable level. To do this, we use the following criteria:

a) Use of a reference system: the level of safety of the system before the change (loop) is considered acceptable. It is then used as a "reference system" to derive the safety requirements for the subsystem radio infill.
b) Explicit risk assessment: the explicit risk assessment analyzes the differences between the subsystems "loop" and "radio infill + GSM". For the subsystem "radio infill + GSM" are identified the following new hazards: (i) transmission by hackers of information since the "radio infill + GSM" is a subsystem of open transmission; (ii) delay in transmission or transmission of data packets stored in the air gap;
c) Use of codes of practice: the standard EN 50159-2 provides the security requirements to control new hazards to an acceptable level, while EN 50128 provides guidelines for the development of the software of the control device of the radio infill.

At this point the person in charge of the change can demonstrate the conformity of the system (in the design and installation) safety requirements and manage the hazards that are identified, noting the latter, the security measures and the resulting safety requirements resulted from the evaluation of the risk and the application of the three principles of risk acceptance in a hazard record.
Finally is also carried out an independent assessment by a third party in order to verify that the management and risk assessment are carried out correctly and that the technical change is appropriate and maintains the same level of security /safety before the change itself.

In this way the risk assessment in the example fulfills all the requirements of the CSM, including the management of the hazard record and the independent safety assessment performed by a third party.

3.3 An example of extended risk analysis methodology for the safety of railway tunnel

The Ministerial Decree of 28 October 2005 on Safety in Railway Tunnels defines that the risk analysis for railway tunnels should be conducted identifying the train-tunnel system as set of three main components: Infrastructure, Rolling Stock, Operating procedures; and also considering traffic features (operational model and frequency) and traffic typology (passenger or freight).

The tunnel system may describe two typologies of path:

- successful path, in operational condition;
- accident path, in emergency condition.

The typical structure of risk analysis used is a classical bow tie diagram, composed of two "wings" linked to a central body that represents the hazard from which starts the accident path. The hazard is characterised in terms of occurrence probability and potential danger on the basis of statistical data of tunnel systems, integrated by available data of the gallery analysed.

The left wing identifies the successful path of the gallery where the application of Fault Tree Analysis (FTA) permits to recognize the causes of abnormal event sequences that can lead the occurrence of hazard. This hazard is conditioned by the preventive measures adopted.

In the right wing the application of Event Tree Analysis (ETA) allows to identify the events that may cause the tunnel system development towards different accident paths, considering the influence of protection and mitigation measures on achievement of the state of "emergency-end".

The Decree identifies reference accident scenarios mainly related to the occurrence of 3 hazards: Fire (S_1), Derailment (S_2), Collision (S_3).

The possible developments of the scenarios identified are related to the performance (effectiveness and efficiency) of preventive, protective or mitigative safety measures and devices carried out for the infrastructure, rolling stock and operational procedures.

The schematisation of an extended risk analysis procedure provided by the same Decree reflects the structure is shown in Figure 1.

The extended procedure of Figure 1 allows us to analyze the different causes that can trigger the reference accident scenarios (fire, derailment and collision) through the application of usual techniques of Fault Tree. Similarly the application of Event Tree techniques allows us to study the different system development paths that can be generated by the reference accident scenarios.

The risk analysis is therefore based on the application of probabilistic methods for assessing the risk level linked to the occurrence of complex events using Fault and Event Tree Analysis techniques, integrated with the study of accident scenarios for the assessment of consequences related with each possible state-of-emergency end.

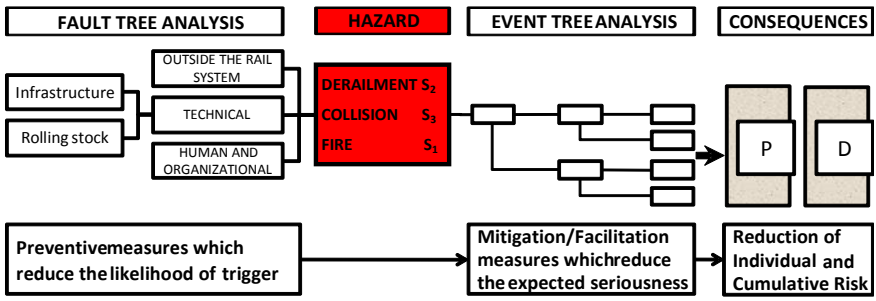

Figure 1: Schematisation of extended risk analysis.

Considering the probabilistic approach, the reference accident scenarios, identified by Ministerial Decree of 28 October 2005, must be a complete group of incompatible events so as to involve an overall risk for the emergency in tunnel equal to the sum of the risks related to each scenario.

The reference source of the input data of procedure is the Report on Safety State of Railway Tunnels, integrated by information on accident indices and failures or malfunction rates of system components collected in an officially accredited database.

The applicability of this risk analysis procedure to railway tunnel system is mainly linked to two factors:

1. The railway tunnel system can be considered closed and well defined;
2. The Ministerial Decree of 28 October 2005 has codified a reference accident scenarios and it has defined the risk parameters that mainly depend on the geometrical configuration of the tunnel (length, cross section, spacing between the pedestrian exits, width of the escape routes, etc.).

Risk analysis is therefore hard to generalize and to apply for open systems and however in case it has not been properly codified the accident scenarios.

An open system creates difficulties mainly related to the development of fault and event trees, which may have a higher or lower detail level depending on the expert carrying out the analysis, entailing a higher subjectivity and a different end result.

In the absence of a general regulation of risk analysis, such subjectivity also has consequences on the verification process by a third party, that could be considered significant, and as reference, fault and event trees different from those developed by the audited entity, could not obtain the approval of the applied procedure.

For example analysing the event “lifting stones” from the ballast caused by the speed and aerodynamics of the train it may have a different development of the Event Tree Analysis by two experts. In fact an expert might consider that a consequence of stone lifted could be only the damage of floor or bogies of the train, while another expert could consider as a consequence also the throwing out of the stone to the railway bordering areas with potential injury of a person.

The detail level achieved in the development of the fault and event tree can also cause a problem in case of identification of the responsibilities following the occurrence of an accident scenario.

For instance, the Decree identifies 8 main causes of trigger for accident scenario "collision". If the procedure of risk analysis carried out by the expert has properly taken into account of these 8 causes, but the occurrence of collision is due to another cause not provided by Ministerial Decree, a possible question is what should be the decision of the judge on the assignment of responsibilities.

The lack of identification of reference accident scenarios and their codification makes difficult the finding of input data of the procedure and of all data that, given the probabilistic approach of the process, are significant to evaluation of consequences related to each development path of accident scenarios analyzed.

In addition the identification and codification of accident scenarios could lead to the creation of a database that could allow:

1. the standardization of the information collection on accidental events;
2. the proper filing of data relating to accident events;
3. to collect information on events which to date do not have historical data, cause of an incorrect filing of accidental information, but may have significant data in the future.

4 Comparison with other sector in terms of risk analysis responsibility

Critical safety aspects were analysed in comparison with road transport and industrial plants. This analysis was performed by classifying causes according to an extended SHEL model [5]. The extension regards Trespasser. The definitions used for the purpose of this article are the following.

Software refers to the set of rules, procedures, symbol, and tasks. It represents all the laws and regulatory support of the individual workers or team.

Hardware means machines, tools, equipment and materials, so the "physical" components of the system. Each of us who have a computer at home, know what is hardware: the keyboard, screen, main memory.

Environment includes all external influences and factors such as policies, cultural restrictions, etc. So, the environmental in the broadest sense refers to the climate, meteorology, topography, *stricto sensu* in the social environment of work and physical place of work, with their limitations and social and economical aspects.

Liveware are the operators, defined as the human component of the system [6], having a personal relational style.

Trespasser is people who do not take part in the functioning of the system, but that may interact with this voluntary or involuntary.

The following table, according to SHELT scheme resumes responsibilities and competences in risk assessment in the different sectors.

The comparison shows as in the industrial plants, once technological products are homologated (H), there is a single subject (IM) which must assess the

operation risk in a closed system. Also in road sector, once technological products are homologated (H) and obliged transport companies and private users to respect road rules, there is an only subject (IM) for risk assessment but the system is totally open.

Table 1: Who does risk analysis in different sectors.

	Railway	Road	Industrial Plants
S	To assess risk, it is necessary information exchange between IM and RU because safety procedures have cross-party responsibilities	Really only IM assesses risk for their responsibilities, other stakeholders are free from mandatory risk assessment	IM assesses risk for their responsibilities
H	Risk assessment is scope of RIs	Risk assessment is scope of the industries	Risk assessment is scope of the industries
E	IM assesses risk but the system is half-open, it must choose where (network critical point)	The system is totally open and IM is not obliged to risk assessment (it cannot?)	IM assesses risk for their responsibilities in closed system
L	To assess risk, it is necessary information exchange between IM and RU because safety procedures have cross-party responsibilities	IM assesses risk for their responsibilities, transport companies assess their own (w/o interaction with IM), private users are free from assessment	IM assesses risk for their responsibilities
T	IM assesses risk but the system is half-open, it must choose where (network critical point)	The system is totally open and IM is not obliged to risk assessment (it cannot?)	IM assesses risk for their responsibilities in closed system

Railway is the only sector where, once technological products are homologated (H), two subjects interact in half-open system and so a single subject is not sufficient to carry out a whole risk analysis on rail operation.

5 Conclusion

Some peculiarities of railway systems respect to other sectors emerge clearly from the previous chapter. In particular two aspects are crucial: the system is open, i.e. railway is vulnerable most of all for the Trespasser component, and different subjects have roles and functions regarding safety and risk analysis application.

The following considerations identify critical aspects and responsible bodies which risk assessment related to rail operations is filled.

I) There are different subjects related to rail operations and nobody covers the whole system. In Europe these subjects are railway industries (RIs),

infrastructure managers (IMs), railway undertakings which manage transport services (RUs) and the national safety authorities (NSAs).

II) A specific role (and only this) of safety responsible is assigned to each of these subjects, but many relationships between them exist. So, from one hand is impossible to identify an unique subject capable to develop an all-embracing risk analysis of rail operations, from the other hand the rail actors cannot ignore the relationships with other actors in safety procedures. This fact is true in particular for the continuous links between an IM and the different RUs that have trains on a same infrastructure.

III) Considering the SHELT scheme, risk analysis of hardware components do not have big difficulties; in fact the problem is reduced in a reliability analysis of technological components by RUs; they must respect homologation rules or technical standards enacted by NSAs.

IV) After technological aspects, the first responsibility of risk assessment of rail operations falls on IMs; since system is open and Trespassers are the main safety problem as shown in previous chapter, IMs have the necessity of circumscribing their analyses; one possible method, perhaps the more simple, is to identify critical nodes in their infrastructures. In this sense, for example in Italy, there exists a specific law regarding railway tunnel risk analysis, a very vulnerable node of rail network. Other possible nodes, where a specific law could be desirable, are level crossing, stations, crossing points and however where an high traffic level and a big social and environmental impact surrounding the rail infrastructure (for example where houses are near the line).

V) Knowing infrastructure characteristics, with its risks, to obtain a Safety Certificate, which allows train circulation, RUs must do their risk analysis and this must be applied exclusively internal procedures (component S) and staff training (L), with the only exception of a Rolling Stock Dossier that really is just validated by RIs and accepted by IMs. Although the Commission Regulation (EC) No 352/2009 concerns railway risk analysis and in Italy there are guidelines for risk analysis application enacted from Italian NSA (ANSF), RUs have big difficulties in this activity because on one hand the Regulation does not include specific methodologies for an extended risk analysis and in general it has an high level approach, on the other hand the guidelines, underlining the importance of interactions between RUs and IM, avoid a clear demarcation of the area of interest to be analysed. The result is RUs are not stimulated to modify the status quo (which is intrinsically safe for Commission Regulation (EC) No 352/2009) because each innovation should be checked through a risk analysis and its assessment seems uncertain and, most of all, it has a methodology not consolidated in rail scientific literature. This is a problem also for IMs, at least in Italy where the NSA does not reach the workforce imposed from Directive 2004/49/EC and so it is very difficult to assess new risk analysis.

VI) To guarantee the good quality of risk analyses of RIs, IMs and RUs, NSAs must assess them, checking the compliance with the laws and standards of the technological components of the RIs, giving the Safety Authorisation to the IMs and the Safety Certificates to the RUs. Beyond this general check on risk

assessments of RUs, NSAs must guarantee that these assessments are suitable for the portion of infrastructure of the IM requested from RU.

The following figure shows the area of interest, according to the SHELT schematisation, of the different subjects in charge of carrying out, assessing and checking railway risk analyses.

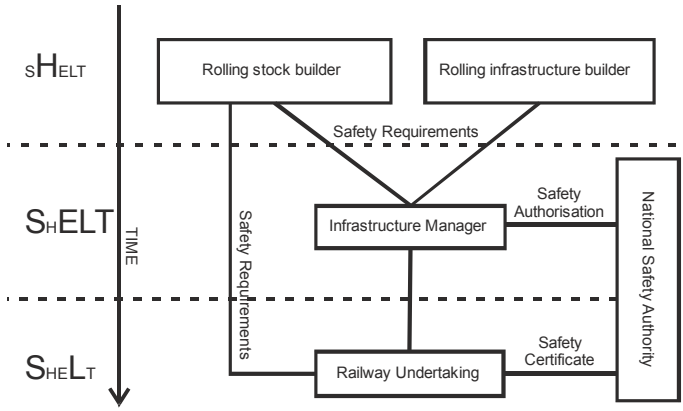

Figure 2: Safety responsibilities for different operators.

Nevertheless, risk analysis represents an opportunity for rail world. In fact:

a) IM can better assess the critical points of their network, in particular where different stakeholders interact (level crossing, station, etc);
b) RUs can have a greater awareness of their safety procedures, both internal and interface with IM and other stakeholders;
c) Risk analysis allows an univocal identification of responsibility of RIs, RUs and IMs.

But the possibility of carrying out quantitative railway risk analysis has the following main limits:

a) In railway sector there are very little frequency of hazards and very big damage, in economic and social terms, when hazards become accidents;
b) In the railway accidents the human factor is predominant, both Liveware and Trespasser;
c) Imposing to RUs and IMs a risk assessment on each new component of their systems which potentially influence safety, woolly definition but inserted in the European laws, stops the technological innovations because RUs and IMs incline to ensconce their self in status quo.

In order to avoid this potential limitation to technological innovations, it is important that the railway researchers work in the future on operational methods for performing risk analysis and assessment criteria that are widely shared and specifically legislated and which relate to concrete cases, in analogy with what has been done in Italy for risk analysis and assessment in the railway tunnels.

References

[1] Ricci, S. “Safety, availability and capacity of electronic interlocking”, COMPRAIL VI, 1998. ISBN 1-85312-598-9.
[2] Ricci, S., Affidabilità e sicurezza degli apparati centrali a logica programmata: metodi sintetici di valutazione. Rivista Ingegneria Ferroviaria n. 9 september 1999.
[3] Malavasi, G., Ricci, S. Carrying capacity of railway networks: interaction of line and node models, COMPRAIL VII, 2000. ISBN 1-85312-826-0.
[4] ERA, Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation, Rif. ERA/GUI/02-2008/SAF, Valenciennes 2009.
[5] “Risk analysis models for level crossing operation” (A. Baldassarra, S. Impastato), FORMS/FORMAT 2007 Formal Methods for Automation and Safety in Railway Automotive Systems, Braunschweig, 25 – 26 gennaio 2007. BRAUNSCHWEIG (Germania): p. 231-241, ISBN/ISSN: 978-3-937655-09-3.
[6] Ricci, S., Tecnologie e comportamenti umani nella sicurezza della circolazione ferroviaria. Rivista Ingegneria Ferroviaria n. 5 di maggio 2001.