Fast Forward to a Harmonized European Risk Assessment Process


by Dr. Birgit Millius
Braunschweig, Germany

Dr. Sonja-Lara Bepperling
Zürich, Switzerland

In 2004, the so-called “Safety Directive” \[Ref. 1\] was published. It demands the development of a common European safety concept. In 2009, the European Union regulation on the adoption of a common safety method was published and thus fulfilled the requirements of the Safety Directive. Even though it is already in use in some areas, not all aspects are as clear as they need to be for a coherent application.

As the regulation is based on the “Recommendation on the First set of Common Safety Methods,” which was developed by the European Railway Agency (ERA), this institution is introduced first. This paper discusses the main aspects of Commission regulation 352/2009 focusing on the most relevant changes in comparison to recent European standards on functional safety (e.g., European Committee for Electrotechnical Standardization (CENELEC) standards for rail applications). This gives an overview of the current European railway safety regulations and provides a glimpse of what is and what will be going on in the European rail safety world.

ERA — Why did the Europeans need it?

Modern rail transport systems first appeared in Europe in the 19th century. Traditionally, railway technology and, consequently, the associated safety regulations were nationally formed. Although there were attempts at creating common standards and rules, rail technology was usually developed specifically for each European railroad network, which contradicted an unreserved use. In addition, great differences in the certification processes handicapped the growth of the railway as a carrier and the railway industry as an economical sector.

When the European Union (EU) was established in 1993, EU law applied in all 27 member states (MS), guaranteeing the freedom of movement of people, goods, services and capital. Consequently, the goal for the EU now is the harmonization of railway technology and regulations. The European Railway Agency (ERA) states on its Web site: “The construction of a safe, modern integrated railway network is one of the EU's major priorities. Economic integration and rapid growth in trade have transformed the European Union's transport needs. In order to service this integrated market, railways must become more competitive and offer high-quality, end-to-end services without being restricted by national borders.” \[Ref. 3\].

Figure 1 — Legal Packages for European Rail Policy \[Ref. 4\]
In the scope of its transport policy, the European Commission has passed three "Railway Packages" (Figure 1) to improve the effectiveness of the existing legislation and to further open the railway markets in the EU. In recent years, several directives were passed from the European Council to support the interoperability of the Trans-European railway network. One of these directives (2004/49/EC) was passed in 2004 and is called the "Safety Directive" [Ref. 1], because it demands the development of a common European safety concept. To carry out this substantial work in the field of safety, the European Regulation 881/2004/EC established the so-called European Railway Agency (ERA).

by Dr. Birgit Milius
Braunschweig, Germany

Dr. Sonja-Lara Bepperling
Zürich, Switzerland

Pages 12345

It is important to note at this point that, legally, there are differences between a directive and a regulation. Directives require member states to achieve a certain result, while leaving them discretion as to how to achieve the result within a certain time period. Directives are generally used where it is thought preferable to leave the precise details of legislative implementation to national governments. Regulations, on the other hand, are legislative acts that become law in all member states the moment they come into force, without the requirement for any implementing measures to have been taken by member states. Once in force, their contents automatically override conflicting domestic provisions, having direct effect in the national law of the member states.

What does the ERA do?

The ERA has two main sites, both located in France. Its headquarters is situated in Valenciennes, while international conferences and meetings take place in Lille. One of the agency’s main assignments is to forward recommendations to the European Commission regarding decisions in the field of European railway safety and interoperability. “The European Railway Agency was set up (under EC Regulation No 881/2004) to help create [an] integrated railway area by reinforcing safety and interoperability. Its main task is to develop economically viable common technical standards and approaches to safety, working closely with railway sector stakeholders, national authorities and other concerned parties, as well as with the European institutions”[Ref. 3].

Within the scope of this task, the ERA received a mandate from the European Commission to develop recommendations for the so-called “Common Safety Methods” (CSM) under the consideration of the Safety Directive. Following Article 6, §3 of the European Safety Directive, “The CSMs shall 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, […]”[Ref. 1]. In addition, Article 6, §2 requires that “the draft CSMs shall be based on an examination of existing methods in the Member States”[Ref. 1].

The final EU regulation, which is now in force, sticks closely to the ERA-developed recommendation. To give guidance to the users of this regulation, the ERA has published a guide for the application of the Commission Regulation on the adoption of a common safety method for risk evaluation and assessment”[Ref. 9] which can be downloaded from the ERA Web site. All other regulations and legal documents are available online as well.

EU regulation on Common Safety Methods

The EU regulation was developed taking into account practices and experiences of the European railways. It says in Article 1 (2) [Ref. 2]:

“[The] purpose of the CSM on risk evaluation and assessment is to maintain or to improve the level of safety on the Community’s railways, when and where necessary and reasonably practicable. The CSM shall facilitate the access to the market for rail transport services through harmonization 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
In the Spotlight

Fast Forward to a Harmonized European Risk Assessment Process


by Dr. Birgit Milius
Braunschweig, Germany

Dr. Sonja-Lara Bepperling
Zürich, Switzerland

To achieve these purposes, a risk management process was defined, which is illustrated in Figure 2.

- Introducing the term “significant change”
- Introducing a hazard classification that may result in excluding hazards from a detailed analysis (broadly acceptable hazards)
- Defining three different risk acceptance principles within the risk management process
- Providing a semi-quantitative risk acceptance criterion for technical systems.

Significant change

For new systems, performing a risk assessment is mandatory. But how are system changes to be
Does every change in a system make a detailed risk assessment inevitable? For this purpose, the regulation introduces the term "significant change" and defines it as follows (Article 4 (2), [Ref. 2]): When the proposed change has an impact on safety, the proposer shall decide, by expert judgment, the significance of the change based on the following criteria:

(a) 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

(b) novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organization implementing the change

(c) complexity of the change

(d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions

(e) reversibility: the inability to revert to the system before the change

(f) additionality: assessment of the significance of the change, taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant

In the regulations application guidelines [Ref. 9], there is very little extra guidance on the application of the criteria for "significant" changes. The material mainly deals with the interpretation of the criterion which remains as fuzzy as it is in the regulation.

The given information is not sufficient for a practical application. Leaving such an important definition as what a "significant change" is to expert's judgment will lead to additional and unnecessary effort because cross acceptance\(^1\) of such a decision cannot be guaranteed. There is the need for a systematic approach to identify significant changes. It should be a qualitative, easy-to-use method or process. As long as there is no agreement on such a method or process, it will be the task of the risk assessor to give a plausible justification why changes are not "significant" and it will be the task of the safety authority to either believe or challenge this justification. Even though there is still research to be done, first results on how to define significant changes can be found; e.g., in a document published by the German safety authority Eisenbahnbundesamt (EBA) [Ref. 11].

\(^1\) Cross acceptance is understood to be the fact that by adhering to the relevant European safety documents safety cases and risk assessments that are accepted in one European country will also be accepted in any other European country.
Broadly acceptable risk

The risk management process asks not only for hazard identification, but also for hazard classification. Article 7 [Ref. 2] states: “To focus the risk assessment efforts upon the most important risks, the hazards shall be classified according to the estimated risk arising from them. Based on expert judgment, hazards associated with a broadly acceptable risk need not be analyzed further but shall be recorded in the hazard log. Their classification shall be justified in order to allow independent assessment by an assessment body.

As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgment shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.”

The principle of identifying hazards or hazardous events with a very low risk is already used in other industry sectors, such as reactor safety. As it is integrated in the risk management process — which will be mandatory — it is obvious to risk assessors and will probably be used often.

Unfortunately, the given information on broadly acceptable risk is not efficient enough for an immediate application. Is “broadly acceptable” qualitative or quantitative, an absolute or a relative risk? Who is responsible for setting a broadly acceptable risk benchmark? There are several articles discussing broadly acceptable risk [e.g. Ref. 5], but no European conclusion has been finalized yet.

The guidelines [Ref. 9] give the following information:

Given that a detailed risk quantification cannot always be possible during the hazard identification phase, in practice an expert judgment can enable assessors to decide whether the considered hazard could be associated with a broadly acceptable risk in the following cases:

(a) either if the hazard frequency of occurrence is judged to be sufficiently low due to, e.g., physical phenomena (such as fall of meteorites on the track) regardless of the potential severity

(b) or/and if the potential severity of the hazard consequence is judged to be sufficiently low, regardless of the hazard frequency of occurrence

Furthermore, the guidelines emphasize the importance of choosing hazards on a correct level as otherwise all hazards (when working on a low system level) are categorized as "broadly acceptable."

Risk acceptance principles

The ERA risk management process distinguishes three different risk acceptance principles (Figure 2) and gives a ranking order:
If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional safety measures shall be identified applying one of the two other risk acceptance principles."

[2].2.5.1: "When the hazards are not covered by one of the two risk acceptance principles described in sections 2.3 and 2.4, the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account."

The acceptability of hazards is given when they are appropriately covered by codes of practice. There is no list given as to what will be recognized as a code of practice but only qualitative aspects of such documents are named. Technical Specifications of Interoperability (TSI)\textsuperscript{2} are explicitly named as an example of codes of practice.

The acceptability of a hazard can also be demonstrated by comparing it to a hazard of a reference system. Such a procedure might be especially relevant for the railway system, as most functions are already performed by technical systems and most of the "new" developments are improvements in existing technologies, rather than completely new developments.

Only when neither of the presented risk acceptance principles can be applied should a detailed risk analysis be carried out. As this is probably the most costly and time-consuming option to show risk acceptability, risk assessors should try to apply one of the other options.

First results from the application of the regulation show that which risk acceptance principle will be used seems to depend on the best practice of each member state. Some member states might always pick the detailed and highly costly explicit risk estimation just because they are used to this methodology and have formed certain standards and tools for this approach. This should be anticipated, and the focus should be on choosing the best risk acceptance principle for an application — not the most convenient one.

\textsuperscript{2} Definition for TSI given in [Ref. 8]: "Technical specifications for interoperability (hereinafter TSI\textsuperscript{2}) means the specifications by which each subsystem is covered in order to meet the essential requirements by establishing the necessary reciprocal functional relations between the subsystem. The TSIs are based on the Directives 96/48/EC and 2004/50/EC for the interoperability of the trans-European high-speed railway system and the trans-European conventional railway system. The TSIs have to be adopted into national law by each member state."
Vol. 46, No. 4 • November-December 2010

In the Spotlight

Fast Forward to a Harmonized European Risk Assessment Process


by Dr. Birgit Milius
Braunschweig, Germany

Dr. Sonja-Lara Bepperling
Zürich, Switzerland

Pages 1|2|3|4|5

Risk acceptance criterion for technical systems (RAC-TS)

Up to now, the common procedure to derive safety requirements for explicit risk analysis is to analyze railway operation and to calculate a tolerable risk which is then used as a basis to derive safety requirements [Ref. 6]. This procedure gets more and more difficult, as the results are valid only for the member state from which data and operational information were taken. Furthermore, obtaining relevant statistical data is difficult. Several European research projects are dealing with risk apportionment on a high system level, but top-down risk apportionment is not always feasible [Ref. 7].

The regulation states a semi-quantitative risk acceptance criterion for the application of technical systems: “For technical systems where a functional failure has a credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to \(10^{-9}\) per operating hour” ([Ref. 2], 2.5.4). The criterion is referred to as RAC-TS.

Using RAC-TS, a risk apportionment is no longer necessary. The criterion is similar to that used in civil aviation, where an international risk acceptance criterion has been successfully used for several years [Ref. 7].

RAC-TS is one of the rare occasions where an official document gives a quantitative number for a tolerable failure rate that can be used when carrying out an explicit risk analysis. Interestingly, the number is not linked to an explicit risk. An associated risk might be derived when the given qualitative information is translated into values, but it can be assumed that different people would probably derive different risk numbers.

It is assumed that RAC-TS might be interpreted differently by users, but the guidance given in [Ref. 11] and especially [Ref. 10], should be sufficient to make sure that such derivation is small. In the guidelines, detailed information on how to understand the qualitative terms of RAC-TS is given. The analysis level for its application is stated, and examples to understand the possible handling and implementation of RAC-TS are explained.

Implications for the future

The new European regulation adds to the development of the European railways. Risk assessments will probably be less cost intensive, as all efforts can be focused on hazards with major impact on the overall risk. The whole process is well structured and helps to avoid misunderstandings and unnecessary discussions. Unfortunately, the given information is not enough to allow a straightforward application. Even by taking into account the information given in [Ref. 9] and [Ref. 10] some areas need more effort to come to an extensive description, which is necessary for a coherent application and subsequent acceptance and cross acceptance by safety authorities. This might be
where European standards like CENELEC (EN 50126 family) will play a role in defining how the European safety framework can be applied in practice. Nevertheless, this will only be possible when some detailed research is done to solve any remaining issues.

**About the Authors**

Sonja-Lara Bepperling studied civil engineering at the Technical University of Braunschweig, Germany. She specialized in transportation engineering and received her Master of Science from the University of Rhode Island, USA. Her Ph.D. focused on validating a semi-quantitative approach for railway risk assessments, which she has done at Siemens Transportation Rail Automation Academy as a graduate student. Since 2009, she is a post-doc at the Institute of Traffic Planning and Systems at the Swiss Federal Institute of Technology, Switzerland. Recently, she has started a part-time job at Ernst Basler + Partner, which is a consulting company working in the field of railway safety.

Birgit Milius has studied civil engineering at the Technische Universität Braunschweig, Germany, specializing in railway engineering. Since 2000, she has worked in the field of railway risk and safety analysis. She is now an assistant professor at the Institute for Railway Engineering and Traffic Safety at the TU Braunschweig. Her main research interest still lies with all questions concerning risk and risk assessment.

**References**


« previous page