An Approach on Applying the CSM for Risk Evaluation and Assessment of Significant Changes of the Railway System

Denitsa Kireva-Mihova [1]

Abstract – **The Railway Safety Directive (2004/49/EC) requires implementation of Common Safety Methods (CSMs) to ensure that a high level of safety in railways is maintained and improved. The absence of a common approach for specifying and demonstrating compliance with safety levels and requirements of the railway system among the Member States has proved to be one of the obstacles to liberalisation of the railway market.**

The objective of this paper is to propose a common approach on applying the CSM in its part of hazards classification and risk evaluation of significant changes of the railway system.

Keywords – **Railway System, Common Safety Method (CSM), Risk Assessment (RA)**

I. Introduction

In the common European legislation, the Railway Safety Directive (2004/49/EC) requires the railway companies operating in the EU Member States to manage risks systematically. They are doing this, following amongst others the requirements described in the "Regulation (EC) No.352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment" and repealed by the "Commission Implementing Regulation (EU) No.402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment" *(CSM RA).* The CSM RA describes a risk management process and framework. The demonstration of compliance with this process, which is accompanied by a report of an assessment body, is a prerequisite for mutual recognition of the respective process application, [1-3].

The CSM RA has applied to all significant changes to the railway system (modernisation or renewal) since 01 July 2012, [1]. The changes may be of a technical (engineering), operational or organisational nature, where the organisational changes could have an impact on the operation of the railway. The CSM RA also applies if a risk assessment is required by a technical specification for interoperability (TSI) and is used to ensure safe integration of a structural subsystem into an existing railway system in the context of an authorisation for placing in service in accordance with the Railway Interoperability Directive 2008/57/EC, [4]. The aim of interoperability legislation is to achieve a technical and operational harmonisation of the main structural and functional railway subsystems. The structural subsystems are:

- infrastructure
- energy
- trackside control-command and signalling
- on-board control-command and signalling
- rolling stock

The functional subsystems are:

- operation and traffic management
- maintenance
- telematics applications for passenger and freight services.

The CSM RA applies to significant changes to all railway subsystems.

For the purpose of this paper the following definitions will be used [1-3]:

railway system means the totality of the subsystems for structural and operational areas, as defined in Directive 2008/57/EC, as well as the management and operation of the system as a whole;

system means any part of the railway system which is subjected to a change whereby the change may be of a technical, operational or organisational nature;

risk means the frequency of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm;

risk assessment means the overall process comprising a risk analysis and a risk evaluation;

safety means freedom from unacceptable risk of harm;

fatality means death within one year of the casual incident;

proposer means the railway undertakings (RUs) or the infrastructure managers (IMs) in the framework of the risk control measures they have to implement in accordance with Directive 2004/49/EC.

consequences means the number of fatalities, major injuries and minor injuries resulting from the occurrence of a particular hazardous event outcome;

frequency of an event is the number of times an event occurs over a specified period of time e.g. number of events/year.

II. Problem definition

The CSM RA Regulation applies to the proposer (RU or IM) when making any change to the railway system in a Member State and applies only to *significant changes* of the railway system. If there is no notified national rule for defining whether a change is *significant* or not in a Member State, the proposer considers the potential impact of the change in question on the safety of the railway system using the significance criteria in the CSM RA Regulation [2]. In case the proposed change has no impact on safety, the risk management process need not be applied.

[1]Denitsa Kireva-Mihova is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: kireva@tu-sofia.bg

Whenever the railway system already in use is subject to a change, the significance of the change is to be assessed taking into account all safety-related changes affecting the same part of the system. The purpose is to assess whether or not the totality of such changes amounts to a significant change requiring the full application of the CSM RA.

The CSM RA management process comprises the following activities [3]:

- The proposer of a change produces a preliminary definition of that change, and the system to which it relates. It then examines it against the significance criteria in the CSM RA Regulation.
- The CSM risk management process starts with the system definition. This provides the key details of the system that is being changed (purpose, functions, interfaces and the existing safety measures that apply to it).
- All reasonably foreseeable hazards are identified and their risk is classified and analysed.
- Safety requirements are identified by application of one or more of the three risk acceptance principles to each hazard.
- A hazard record for the system that is to be changed is produced and maintained.
- Before acceptance, the change proposer demonstrates that the risk assessment principles have been correctly applied and that the system complies with all specified safety requirements.
- The assessment body provides its report to the proposer.

This risk management process is iterative and is depicted in the diagram on Fig. 1, [2]. The process ends when compliance of the system with all the safety requirements necessary to accept the risks linked to the identified hazards is demonstrated.

Hazard classification has a very particular meaning in the context of the risk management framework. It is based on an initial assessment of the risk associated with each hazard and is carried out as part of a hazard identification process.

It is very important that, at the considered level of detail, the hazard identification is complete and that hazards are neither forgotten nor wrongly classified to be associated with *broadly acceptable risk(s)*.

This is of prime importance because if hazards are not identified, they are not mitigated and are not dealt with further in the risk management, risk assessment and hazard management processes.

The classification of the identified hazards, at least into hazards associated with *broadly acceptable risk(s)* and hazards associated with risks that are not considered as broadly acceptable, enables the prioritisation of the risk assessment on those hazards that require risk management and risk control measures. The classification of hazards between these two categories is based on *expert's judgement* and does not have a quantitative measurement. Criteria are to be used to help decide whether the risk associated with a proposed change is low enough to proceed (Fig. 2).

It is the responsibility of the change proposer to evaluate whether the risk associated with each identified hazard is broadly acceptable.

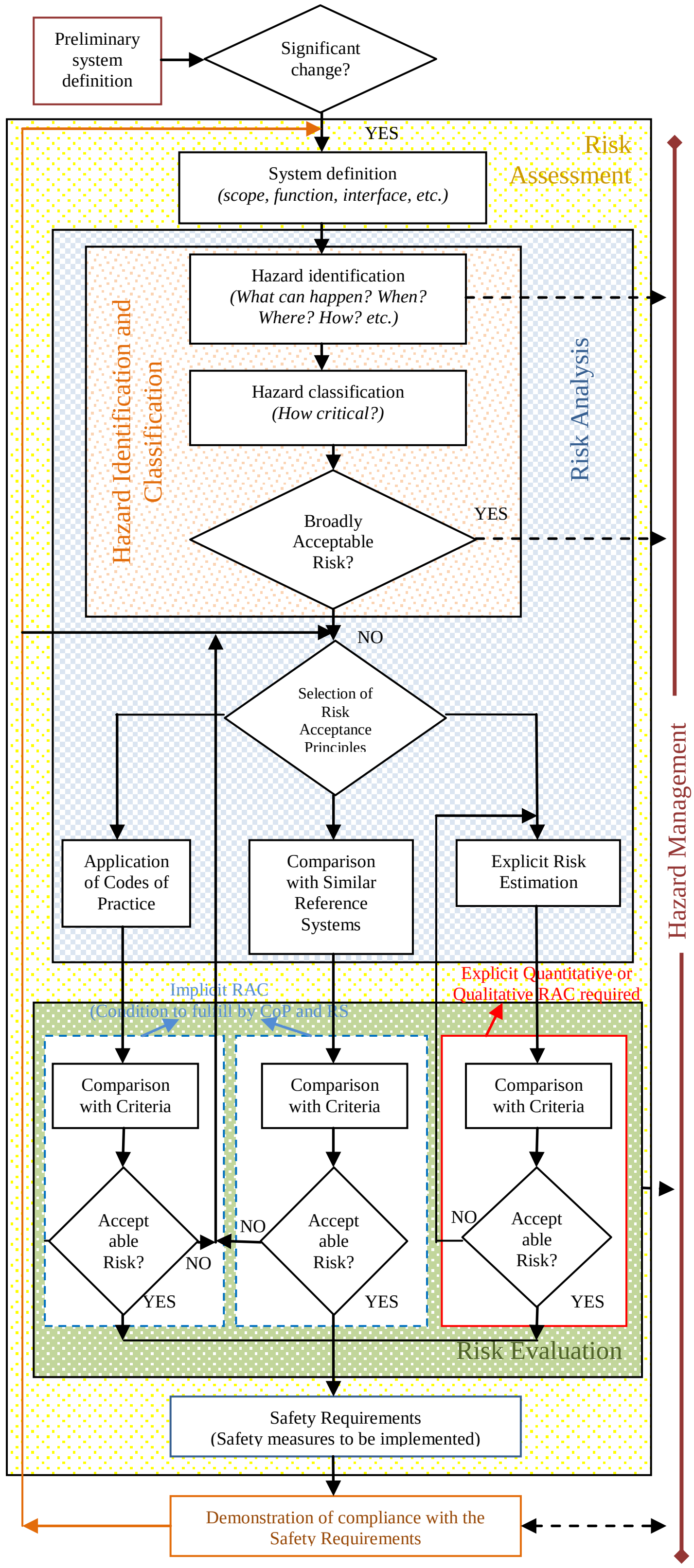

Fig. 1. Risk management framework in the CSM RA Regulation

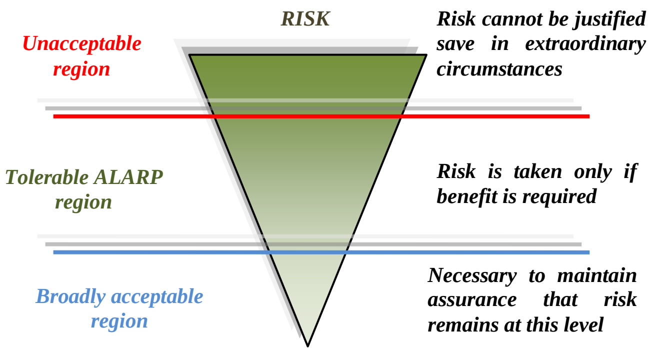

Fig. 2. Framework for tolerability of risk

The CSM RA enables the evaluation of the risk acceptability of a significant change to the railway system by using one or a combination of the following so-called *risk acceptance principles*, without giving priority to any of them:

- the application of *codes of practice (CoP)*
- the comparison with similar *reference systems (RS)*
- the use of *explicit risk estimation (ERE)*

The proposer of the change is responsible for the choice of the principle to apply, [2]. The risks, which are controlled by the application of *codes of practice* or by the safety requirements derived by a comparison with a similar *reference system*, are considered as acceptable provided that the conditions of application of these two risk acceptance principles are fulfilled and sufficiently documented as defined in the CSM RA. This means that explicit risk acceptance criteria need not be defined for the hazards controlled by these two principles. Additionally, whenever the third risk acceptance principle - the *explicit risk estimation* – is used and in order to be able to determine whether the residual risk is sufficiently low so that it is not necessary to take any immediate action to reduce it further, *risk acceptance criteria (RAC)* are used. *Explicit risk acceptance criteria* will therefore only be needed for evaluating the risk acceptability when applying the third principle - *explicit risk estimation* (Fig.3).

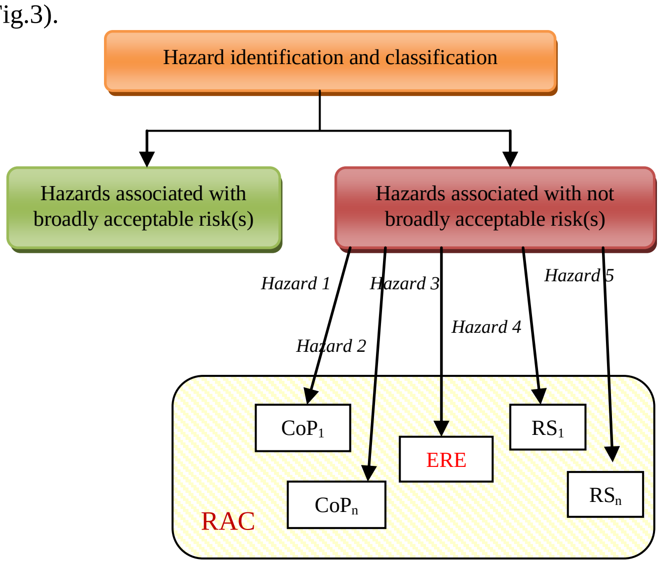

Fig. 3. Applying the risk acceptance principles

The *explicit risk estimation* is not necessarily always quantitative. The estimation of risks can be quantitative (if sufficient quantitative information is available in terms of frequency of their occurrence and severity), semi-quantitative (if such quantitative information is not sufficiently available) or even qualitative (e.g. in terms of process for management of systematic errors or failures, when quantification is not possible).

The *explicit risk acceptance criteria* that are needed to support the mutual recognition will be harmonised between the Member States by the on-going European Railway Agency work on the risk acceptance criteria. At this moment it is the responsibility of the proposer of the change to define such criteria and more frequently the inaccurate qualitative approach based on *experts' judgment* is used.

In cases the CoP and RS risk acceptance principles are not applicable an approach to *explicit quantitative risk estimation* is proposed in order to avoid the subjective disadvantages derived from the *expert's judgement*. Applying the quantitative approach the assumption is made that sufficient quantitative information for the hazards frequency and the consequences from the change of the railway system is available.

III. Explicit Risk Estimation and Evaluation

The *explicit risk estimation* principle is frequently used for complex or innovative changes of the railway system (modernisation or renewal). In order to evaluate whether the risks controlled by the application of *explicit risk estimation* is acceptable or not, *explicit risk acceptance criteria* are needed. These can be defined at different levels of a railway system. They can be seen as a *pyramid of criteria* (Fig. 4) starting from the high level risk acceptance criteria (expressed for instance as societal or individual risk), going down to subsystems and components (to cover technical systems) and including the human operators during operation and maintenance activities of the system and subsystems, [3].

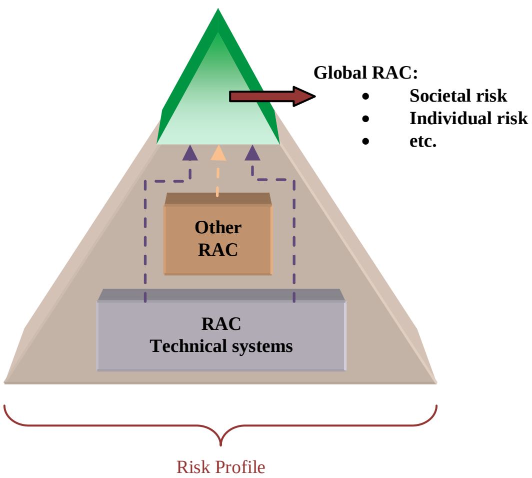

Fig. 4. Pyramid of risk acceptance criteria

Risks to people may be expressed in two main forms: *individual risk* – the risk experienced by an individual person, and *societal risk* – the risk experienced by the whole group of people exposed to the hazard.

Low-frequency high-consequence events might represent a very small risk to an individual, but they may be seen as unacceptable when a large number of people are exposed. Railway incidents are mainly referred to such type of events which are unacceptable for a large number of people, so the *societal risk* is considered in the proposed approach.

Societal risk can be represented:

- graphically, in the form of FN-curves, or
- numerically, in the form of a risk integral.

FN-curves: Generally, risk scenarios (S_i) to be included in a risk assessment can be characterised as having a frequency (f_i) and a consequence (c_i), i.e. number of casualties *(N)*. *F* is used to denote the sum of the frequencies of all the individual events that could lead to *N* or more fatalities, [5].

The risk is then defined by a set $\{S_i, f_i, c_i\}, i=1 \dots n$.

Associated with each risk scenario, the risk may be defined as:

$$r_i = f_i \times c_i \qquad (1)$$

and the risk of the changed railway system defined as:

$$r = \sum_{i=1}^{n} r_i \qquad (2)$$

The risk as defined in Eq. 2 offers a measure of the risk level over all the risk scenarios. It however hides the difference between two types of incidents: one of low frequency but high impact consequences; the other one of high frequency but low impact consequences. In fact, people have different attitudes toward these two types of incidents. It is therefore of interest to include the frequency and the severity profile in the risk assessment and can be represented by the FN-curve, where *N* stands for the fatalities in one incident and *F* stands for the yearly frequency of the incidents causing *N* or more fatalities (Fig. 5).

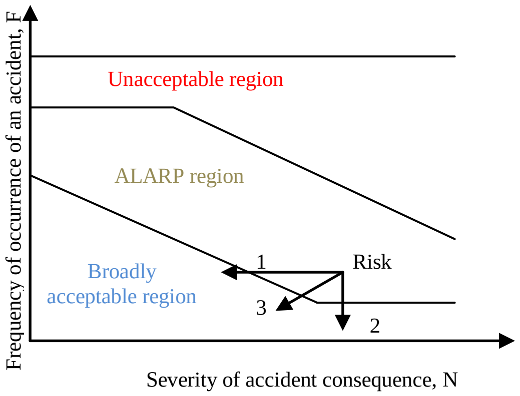

Fig. 5. Risk areas and risk reducing measures

The FN-curve can be built based on the frequencies and the consequences of the risk scenarios S_i, $i=1 \dots n$.

First the risk scenarios are ordered to satisfy $c_{i-1} < c_i$. then plot the cumulative frequency F_i against c_i for $i=1 \dots n$.

$$F_i = \sum_{k=1}^{n} f_k \qquad (3)$$

The *risk acceptance criteria* for societal risk are to be set up on the FN-diagram, which could be defined by the customer or authority or estimated. Two criteria lines divide the space into three regions – where risk is unacceptable, where it is broadly acceptable and where it requires further assessment and risk reduction as low as reasonably practicable (ALARP), as shown on Fig. 5. There are three options for reducing the risk: mitigate the consequences of an accident (Arrow 1), reduce the probability of occurrence of the accident by implementing additional safety barriers or by using more reliable components (Arrow 2) or both (Arrow 3).

Risk integral: A risk integral (RI) is a summary of the overall level of societal risk, taking account of the whole set of f-N pairs and is mathematically presented with Eq.4.

$$RI = \sum fN^{a} \qquad (4)$$

The calculation of a contribution to the RI can weight the value for N so as N increases, the RI contribution also increases but at a faster rate. Proposed values of α are generally in the range 1 to 2. So, the consequences of events are considered to be more important than the likelihoods.

An RI value is a summary statistic and so cannot, by itself, tell us anything about the various specific accident scenarios or their likelihood at any site. Moving from FN representation to RI sacrifices detailed information (f-N pairs) for ease of comparison and ranking - RI values are more easily and unambiguously ordered than FN-curves.

IV. Conclusion

CSM RA gives the responsibility to the proposer of the change to evaluate whether the risk associated with each identified hazard is broadly acceptable. If the identified hazards and the associated risks of the system under assessment cannot be controlled by the application of CoP or similar RS, an approach to *explicit quantitative risk estimation* is proposed in order to avoid the subjective disadvantages derived from the *expert's judgement*. With the criteria on the FN-curves we can judge whether more actions are needed to improve the safety of a given system subject to a change. It could be used by RUs and IMs to develop their safety management system (SMS) to manage the risks associated with their activities.

References

[1] *Railway Safety Directive 2004/49/EC*

[2] *Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009.*

[3] ERA/GUI/01-2008/SAF, *Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive,* ver. 1.1.,2009

[4] *Railway Interoperability Directive 2008/57/EC*

[5] Daosheng Cheng,*Uncertainty analysis of Large Risk Assessment Models with Application to the Railway Safety and Standards Board safety Risk Model,* 2009