Chapter 3

Semi–Quantitative Risk Assessment of Technical Systems on European Railways

Jens Braband
Siemens AG, Germany

ABSTRACT

The European Railway Agency (ERA) has the challenging task of establishing common safety targets and common safety methods throughout Europe. In this context, the harmonization of risk analysis methods is also discussed. The purpose of this paper is to present a new semi-quantitative approach for the risk analysis of technical systems and the means by which compliance with legal and regulatory requirements can be demonstrated. As a particular reference, a new German pre-standard, which lays out requirements for semi-quantitative approaches, is taken into account.

INTRODUCTION

The European Railway Agency (http://www.era.europa.eu), established by European Regulation 881/2004, has the mission of reinforcing railway safety and interoperability throughout Europe in times of ongoing privatization. Central to its work on railway safety is the development of measures based on common safety targets (CSTs) and common safety methods (CSMs), common safety indicators and harmonized safety certification documents.

The common safety methods describe how safety levels, the achievement of safety targets and compliance with other safety requirements are assessed in the various member states. As a first step, EC Regulation 352/2009 will finally come into force for the complete railway sector by July 2012. In this regulation, a semi-quantitative risk acceptance criterion for technical systems (RAC-
Semi-Quantitative Risk Assessment of Technical Systems on European Railways

TS) similar to civil aviation has been introduced: For technical systems where a functional failure has 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.

This criterion is limited to those technical systems where failure can lead to catastrophic effects, e.g. accidents involving several fatalities, and for which there are no credible barriers or substantial mitigating factors that will prevent this consequence from materializing. The criterion can be used for the most critical functions performed by technical systems on railways such as speed supervision, control of the switch position, complete and permanent loss of the brake system, or loss of the traction cut-off function. This means that formally RAC-TS relates only to potentially catastrophic accidents. In order to apply it also to other severity categories, RAC-TS has to be embedded in a risk analysis method.

The chapter is organized as follows: after a description of problems with risk analyses, an applicable standard is reviewed, from which the requirements are taken. Then a new semi-quantitative risk analysis method is constructed and some arguments and examples concerning the validation of the method are presented. Finally directions for future research are given.

Problems with Risk Analyses in Railway Applications

Risk is a combination of accident severity and accident frequency. Accident frequency can be calculated by hazard frequency and the probability of a hazard developing into an accident. This probability is derived by taking into account the efficiency of barriers. Barriers can be of different origin, e.g. human interactions, operational barriers, technical barriers.

It is well known that risk acceptance is an intricate topic and that risk analyses may be quite time-consuming and tedious [Braband (2005)], in particular if they are performed quantitatively. There exist simpler semi-quantitative methods, e.g. risk matrix, risk graph or risk priority numbers, however they often lack justification and it is not clear whether the derived results are trustworthy. So, a major research challenge consists in constructing dependable semi-quantitative methods.

In particular, schemes based on risk priority numbers (RPN) are widely used in Failure Modes, Effects and Criticality Analyses (FMECA) although it is known that they have not been well constructed and that their use may lead to incorrect decisions:

- The risk of different scenarios that lead to the same RPN may differ by orders of magnitude
- Scenarios with similar risks lead to different RPN

This has already been observed by Bowles (2003) and has now also lead to cautionary advice in the standards.

Risk matrices are a well-known tool in risk assessment and risk classification, also in the railway domain (see for example EN 50126 (1999) or Braband (2005)). Table 1 gives a typical example. The major drawbacks of such risk matrices are:

- Risk matrices must be calibrated to their particular application.
- The results depend on the system level to which they are applied.
- The parameter classes must be concisely defined in order to avoid ambiguity and misjudgments.
- It must be defined which frequency is meant, e.g. accident or hazard frequency.
- It is not directly possible to take barriers or risk reduction factors into account in the risk matrix.

However, if these drawbacks can be overcome, risk matrices are a well-accepted and easy-to-