

# **Rail Optimisation Safety Analysis**

**Project ROSA – an Overview**

**18<sup>th</sup> Annual IRSC**

**Denver, October 5 – 10, 2008**



TECHNISCHE  
UNIVERSITÄT  
DRESDEN



**Reviewed by:**  
**Author(s):**  
**Document ID:**  
**Date:**

M. GEISLER, R. PUETTNER, K. A. KLINGE, DB AG  
080905\_ROSA\_IRSC2008\_DB  
05/09/2008

## **Abstract**

This paper gives a report about the project ROSA (Rail Optimization Safety Analysis), which is a complete and coherent analysis of a railway system at global level. It includes the aims and results of ROSA at the present status of the work, distinguished between the Working Packages. The model of ROSA with its parts Basic System Model, Starting Point Hazards, Risk Control Model and Barrier Quantification Model is explained. Finally the project state and the future work are presented.

## **Introduction**

Today, rail transport is considered as a safe land transport mode. The functional and procedural concepts of safety governing the member state's railways in Europe grew historically and complex sets of rules and regulations (in particular with respect to operations under degraded conditions) are implemented as well as specific railway technologies. However, never has a complete analysis been carried out on detailed level for this mode of transport which would have established a logical, causal and mathematical correlation between the safety of individual components and procedures and the safety indicators which take precedence.

On the basis of the recent European Safety Directive 2004/49/EC [1] the European Railway Agency (ERA) elaborates a scheme for Common Safety Methods (CSM) for railways as well as first definitions of Common Safety Targets (CST) and Common Safety Indicators (CSI) for railways. In order to support this work of ERA as well as to prepare for future more detailed analyses requirements, the cooperation partners endeavour for the first time to establish a global safety model for a complete railway system and to identify optimization potentials with respect to safety, quality and costs.

The two European railway undertakings and infrastructure managers (DB and SNCF/RFF) have taken this development as occasion to start the research project ROSA (Rail Optimization Safety Analysis) together with research institutions (Technical University of Dresden (D) and the French national institute for transport and safety research (INRETS) (F)).

The project serves three important objectives:

- Improvement in the understanding of railway safety in large major railway undertakings in Europe and its application to the growing cross-border traffic between the two countries
- Exploration of future optimisation potentials of railways through arbitration between safety requirements and, for instance, availability or maintainability requirements to ensure the profitability of investments.
- Support of DB AG and SNCF and above all of the European Railway Agency in assessing the impacts of safety target definitions

## **ROSA Work Package Structure**

"ROSA" stands for "Railway Optimization Safety Analysis" and is structured into four working packages to form for the first time a coherent safety analysis at global level, meaning that the complete safety behaviour of a complex railway network such as in Germany or in France can be better understood:

- WP 1: Railway Hazards Analysis, Functional Safety Structures, Consequence Analysis
- WP2: Generic Computer Based Quantification Tool for CST/CSI Impact Analysis
- WP3: Cost-Benefit-Analyses for CSTs/CSIs and Examples
- WP4: Conformity Validation/Verification of CSIs

The work packages had been organized in view of the bow-tie model, our representation of which is indicated in figure 2. Since the ROSA project difficulty is rather the enormous complexity of the safety model than the understanding of detailed entities, the project confines itself to large extent to the upper part of the double pyramid, i.e. starting with an agreed list of Hazards and neglecting detailed cause analyses at this time.

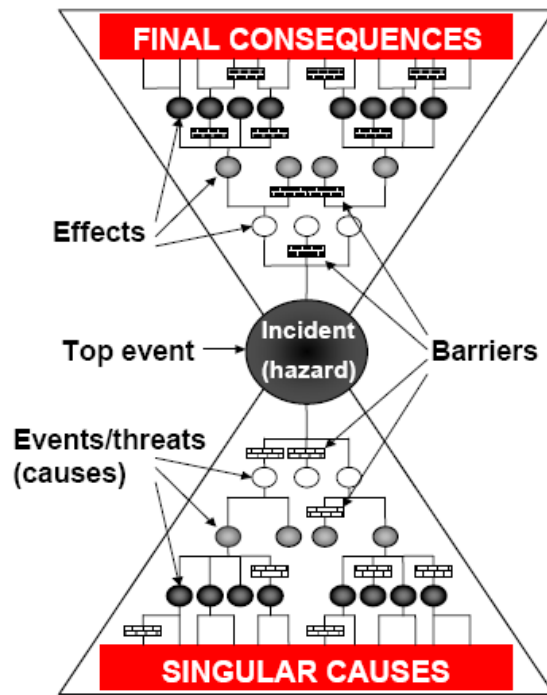


Figure 1: The ROSA Project is based on a Bow Tie Model Approach

The Work Packages 1 and 2 are closely linked and have the major task of providing a computer based tool that captures the safety characteristics of a complete network and permits to perform impact analysis if any parameter changes.

The work Packages 3 and 4 have deal with the question of how life cycle costs of a safety measure can be valued against safety performance increase and how future changes in the safety architecture may be integrated into a set of safety targets.

**The ROSA Safety Model (WP 1 and 2)**

The ROSA project started with the Working packages 1 and 2 adopting an implicit risk based approach as advocated by the Safety Directive. Parts of the model are based again on the bow tie model that is adapted in the modelling language as indicated in Figure 4:

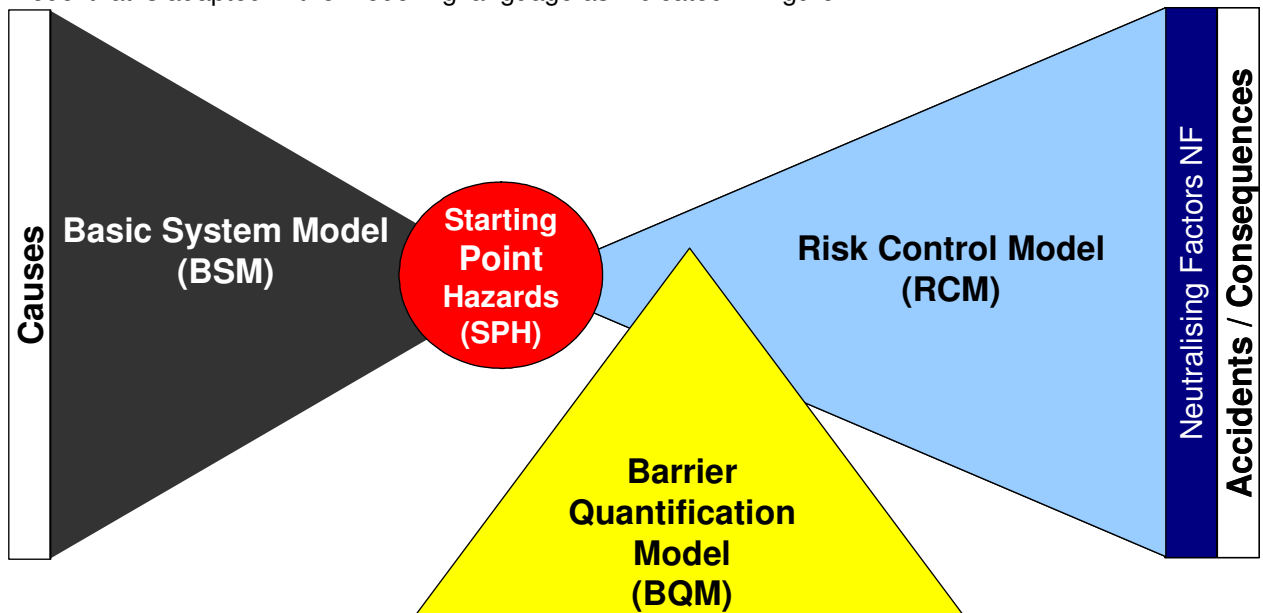


Figure 2: The ROSA Safety Model parts mirrored against the bow tie model

The reasoning of the ROSA model is the following:

1. A complete Railway Network is considered through its boundary definitions (what is part or the railway?) and actual traffic, operations and other features.
2. A complete list of potentially unsafe situations (hazards, e.g. train overspeed) is established at generic level, independently of the actually implemented safety measures and functions.
3. Each of the hazards is transferred by an Event Tree Analysis into possible consequences (e.g. overspeed → derailment). Since the efficiency of the already implemented safety functions is a crucial part of the ROSA model, possible implementations are introduced in the event tree step by step (following the historical evolution of the railway system).
4. The actual generic implementations enter into the ROSA model in the shape of a Barrier Quantification Model that reduces the consequences of the unprotected, more basic system
5. Other Neutralising Factors enter the model through an adequate Human Machine Interface

The quantification of the ROSA model requires a substantial analysis. As an analysis example consider the case of the Level Crossing Accidents. First the number and traffic situations of all level crossings of the network are estimated (e.g. 20.000). Secondly, the risk potential of totally unprotected level crossings (basic level crossing that do of course not exist in this form in the network) is estimated, e.g. by calculating the incident rate of trains and individual traffic members “meeting” at the unprotected level crossing. The Event Tree Analysis determines the likelihood of accident categories (e.g. collision). The resulting raw hazard rate may yield e.g. some hundred thousand of hazardous situations. Finally, the Barrier Quantification Model determines which safety measures or safety barriers with its certain efficiency rates and actual percentages of implementations are actually implemented (e.g. St. Andrew Crossings, Blinking Warning Sights, Half Barriers, Full Barriers). By introducing also neutralising factors (e.g. train runs through level crossing, car is in the level crossing boundary but not in the clearance envelope of the train) and employing the efficiency factors of the barriers, the number of possible unprotected crossings is consequently reduced (e.g. to approximately 200). If all estimations are correct to some level of accuracy, the ultimate number of accidents should reproduce the actual statistics, which serve therefore as a validation check of the model.

It becomes obvious, that the ROSA model shall not only permit to analyze the origins and details of possible future safety data bases but in addition shows the Barrier Quantification Model what kind of safety measure (barrier) contributes how to the very safe railway performances as of today. Reducing in the model a barrier implementation number (like full barriers at level crossings) the ROSA model should yield the increase of the associated number of accidents. Vice versa, increasing the number of full barriers at level crossings should result in an associated reduction of these types of accidents.

Since ROSA is an ambitious research project, the next year of work shall reveal to what extent the described endeavour is achievable and how actual safety data bases can support the analysis.

### **Starting Point Hazards Analysis**

The ROSA Safety Model is centred around a consistent list of so called Starting Point Hazards that shall capture all potential hazards associated with the operation of a network.

This list of Starting Point Hazards had been derived by a full Fault Tree Preliminary Hazards Analysis at generic level and also been reviewed for completeness against other Preliminary Hazards Analyses of the Railway Domain.

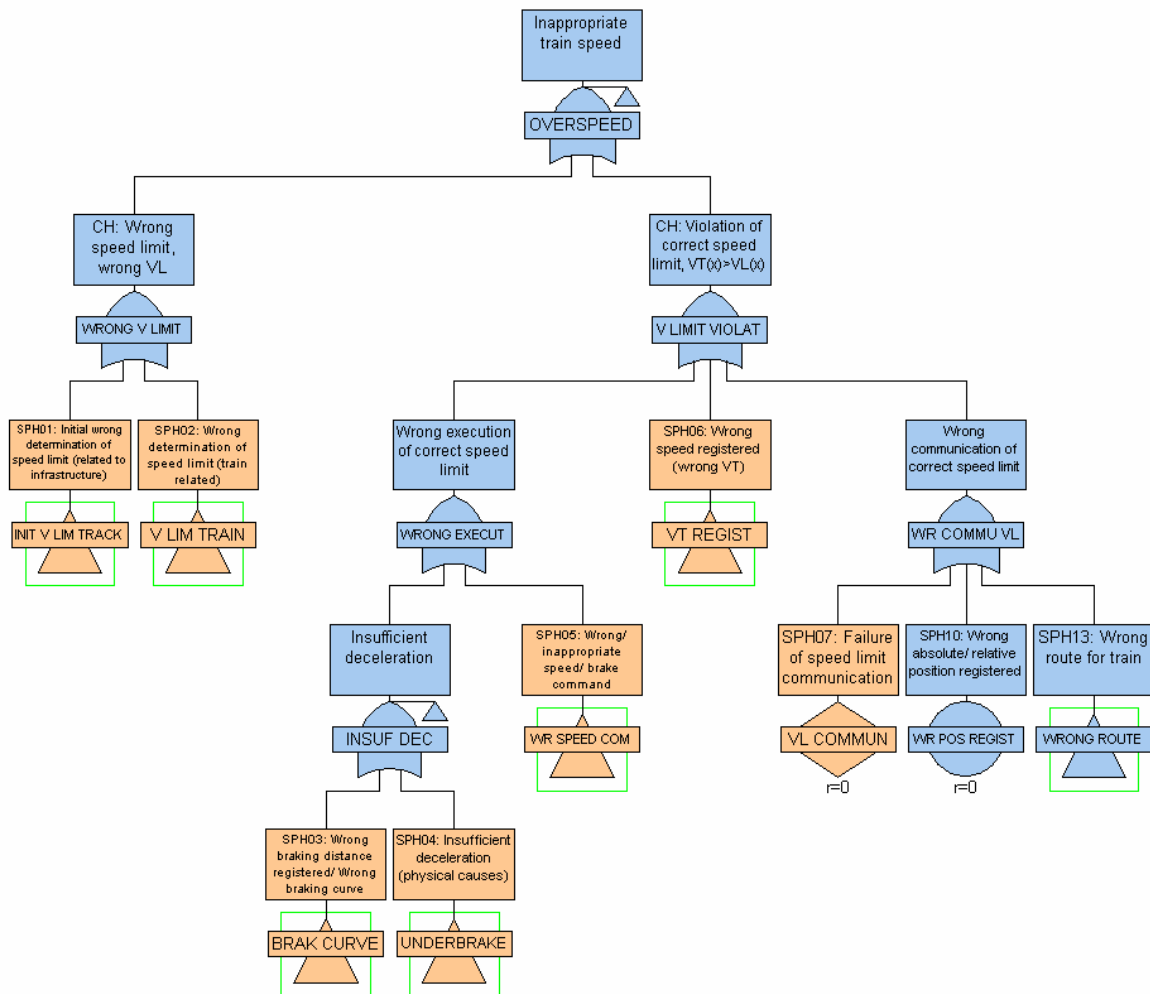


Figure 3: Snapshot example of the Preliminary Hazards Analysis Fault Tree. Starting Point Hazards are colour coded in orange.

Two criteria had been observed for the list of Starting Point Hazards:

1. The list shall be complete. This had been satisfied by assuring one complete cross section of the full Fault Tree and by review against other PHAs of the railway domain
2. The Starting Point Hazards shall be intermediate in the bow tie model, meaning that the selected hazards shall not be too close to the level of accidents nor be too close to the implementation level. This requirement had been assured by “cutting” the full fault tree at intermediate (however varying) level.

The resulting list of at the moment 60 Starting Point Hazards considers all parts of the railway with aspects of operation, signalling, rolling stock, infrastructure separated into track and station properties. It shall be noted, that the selection of a full “Cross Section” of Starting Point Hazards from the PHA is to some degree arbitrary, i.e. multiple possible lists could be selected. On the other hand, the completeness requirement fulfilment is on the first order independent of the selection, it has just to be assured that every branch of the PHA Fault Tree Analysis is taken into account.

### Event Tree Analysis

As mentioned further above, every Starting Point Hazard shall be developed further into possible consequences up until accident category probabilities are obtained. Crucial for the analysis is not so much any number of accidents as such but the fact that the initial raw hazard rates are determined from the operational and traffic patterns for a network not taking into account already at the beginning all protection measures and functions. Only those functions (e.g. traffic organization into block schemes) that are common for all European railways are considered from the beginning. Only after obtaining the raw hazard rate of the more or less unprotected system will the safety measures and functions be added as risk reducing filter functions (e.g. protecting the simple basic

block concept by signals, further by interlocking systems and with some percentage by virtual block protection systems).

Since some of the Starting Point Hazards evolve in particular operational settings and since the Safety Directive calls for differentiations of e.g. track and traffic categories it was felt necessary to describe in a context analysis each Starting Point Hazard before further analyzing the Event Tree developing from the Hazard.

After provision of the Context Analysis, the Event Tree Analyses are elaborated. The Event Tree Analyses shall be at a sufficiently generic level and ultimately transfer the 60 Starting Point Hazards into a relatively small number of accident categories defined in the European Railway Safety Directive and adopted for ROSA. In terms of structure of the tree analysis, a common scheme was developed that should encompass so diverse hazards as e.g. Wrong Movement Authority on the one hand and e.g. Persons falls from platform onto track on the other. Figure 8 shows an example of an Event Tree Analysis.

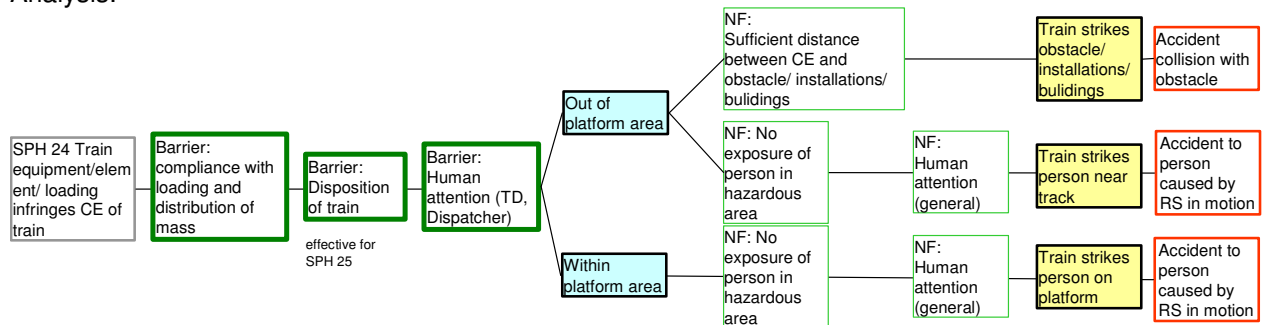


Figure 4: Event tree of SPH "Train equipment/element/loading infringes CE of train"

The hazards are further developed into sub-hazards for e.g. at different location if different parts of barriers or accidents would be likely to evolve. A next level of instances are the (sometimes multiple) barriers that protect with some likelihood the further development of the hazard. A next level of factors involves the likelihood of neutralizing factor (e.g. human attention of passenger). Before entering into the accident categories, the Event Tree Analysis may take into account other risk reducing factors (e.g. compliance with rules of loading and distribution of mass). Only when all possible barriers are either not existing or fail with residual rates, when no neutralizing factor applies and the train is likely to operate then the raw hazard protrudes into an entry in the accident categories data base.

As can be seen (and has been discussed before) the ROSA analysis focus is not only on prediction of ultimate rates, but rather has the objective to analyze the overall barrier structures that yield today an acceptable safe railway system. The barrier impact/efficiency analysis may be used, e.g. in order to determine which barrier in a network reduces unsafe situations the most, what is the impact of adding or increasing number or types of barriers and –linking in the future the barriers with their investment cost – also determine cost efficiencies.

Also the inverse analysis may be performed easily: Setting certain (Common Safety) Targets on certain kinds of accidents or requesting a certain degree of equipment may be input into the model and yield the impacts in terms of safety increases or equipment requirements. This feature was one of the original drivers of the project.

### State of the Safety Model and Further Proceedings

At this time, the ROSA project has accomplished the following tasks:

- System Boundary Definitions, Risk Group Definitions, Accident Categories Definitions
- Complete Preliminary Hazards Analysis and List of Starting Point Hazards
- Context Diagrams for Operational Schemes and per Track Categories
- Qualified Event Tree Analyses
- Data model and functional model of the calculation tool
- Method of calculation the barrier's efficiency

As a next step on the Safety Model the transforming of the Event Tree Analyses into a Fault Tree Plus Model and the definition of the interfaces to databases has to be done. By linking the computer based tools to the example case of Germany (accident and incident data bases) the quantification of the

model shall validate the approach by the early of 2009. First rapid prototype calculations showed already the feasibility of the approach. Also, upon validation of the model, a Human Machine Interface will be constructed by the end of 2008.

Within the work package 3 three case studies are elaborated concerning the aspects of LC, tunnel safety and SPAD. These case studies were done with existing CBA-method adopted from other application areas (e.g. road, air traffic). Based on the case studies a methodology is developed how the correlation between the costs for a safety measures and its benefit can be handled in the ROSA safety model. For optimization the method shall enable to balance safety measures even with different responsibilities considering the costs and safety benefit for the whole system.

The work package 4 deals with the methodology and guideline of introducing new or modified safety functions (barriers) to the model. Within this work package the ROSA model will be verified by considering two examples, which were chosen because data before and after the introduction / modification are available. The verification of the model is done by changing the model after modifying the 'hot axle detection system' and the introduction of an 'automatic train control system' to the model.

## References

- [1] Directive 2004/49/EC. *Railway Safety Directive*. Brussels : European Commission, 2004