ROSA – a computer based safety model for European railways

J. Schütte[1] & M. Geisler[2]
[1]*Dresden University of Technology, Germany*
[2]*Deutsche Bahn AG, Frankfurt, Germany*

Abstract

On the basis of the European Safety Directive 2004/49/EC, the recently created European Railway Agency (ERA) elaborates currently amongst others a scheme for Common Safety Methods (CSM) for European Railways, as well as first definitions of Common Safety Targets (CST) and Common Safety Indicators (CSI).

In order to support this work of the ERA, the German and French Ministries for Research supported a larger project, involving Deutsche Bahn AG (German Railways), SNCF (French Railways), INRETS (French National Institute for Transport Research) and the TUD (Dresden University of Technology), to develop a computer based environment to analyse and optimize Safety Characteristics and Safety Indicators of railways. This ROSA (Rail Optimization Safety Analysis) has concluded at the end of 2009 after three years of research with a first complex ROSA toolset and analysis results.

The ROSA model and toolset, as well as first applications and an outlook, will be presented in this paper.

Keywords: railway safety, hazards analyses, barrier model, safety UML model, computer based quantified safety analysis, common safety targets, common safety indicators.

1 Background to and outline of the ROSA model

After several harmonization activities in the European railway domain (Technical Specifications of Interoperability, High Speed and Conventional Railway Packages, ERTMS) the European Commission had published the so-called European Safety Directive for Railways [1, 2] in 2004 with the ultimate

WIT Transactions on The Built Environment, Vol 114, © 2010 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR100701

objective of defining safety characteristics of railways and streamlining (harmonizing) safety key features amongst the European member states' railways [6]. In order to pursue this and other tasks, a European Railway Agency (ERA) was founded in Valenciennes in France in 2007.

A set of first tasks of the ERA was the definition of common key elements: Common Safety Methods (agreed and published in the meantime), Common Safety Targets (currently elaborated) and Common Safety Indicators (currently defined). In particular, the questions related to the Common Safety Targets and Indicators were debated in Europe under diverse aspects, such as

- Metric (safety measured per train kilometre? train hours? passenger hours? safety measured in number of safety equipments or only by accident database entries? etc.)
- System and operations (separate targets for high speed systems, conventional systems, low speed regional trains, etc?)
- Safety measures/indicators (may investments in staff training be considered alternatives to technical investments? should only global targets/indicators be considered? per accident category? etc.)
- Should the targets/indicators be mandatory? What if they are not respected?
- Should even best in class railways improve permanently?

In order to support the debate and to prepare larger railway networks, the French and German research ministries decided to support a larger project (ROSA – Rail Optimization Safety Analysis) conducted by the Deutsche Bahn AG, French Railways (SNCF), the French National Institute for Transport Research and the Technical University of Dresden, Germany.

While for components and subsystems have clear standards that had evolved over the recent decades [3–5], no clear prescription had been found for complex complete railway networks. Therefore, the intention of the ROSA-project was to analyse for the first time, for a complete large network (like in Germany, about 35.000 km of track) at a higher level, where safety is actually coming from, what mechanisms, processes and subsystems are sensitive to safety, and how the global safety features would be impacted by modifications. It relatively quickly became clear that such a complex enterprise can only adequately be approached by means of computer based models and tools that support large amounts of diverse data. Two models turned out critical in this respect. The establishment and modelling of a complete list of Starting Point Hazards (SPH), including their development into consequences by an Event Tree Analysis, and the establishment of a Barrier Quantification Model (BQM) that limits the potential hazards.

2 Approach of the ROSA model

In order to remain independent from national particularities, but being still able to draw some conclusions from the analysis, the elements below had been found to be adequate:

1. A complete Railway System is first described through parameter lists (e.g. track kilometres, number of switches, trips, signals passenger flows, operating modes, civil structures, level crossings, etc.).
2. In further analysis, the "unprotected" system is considered in order to estimate where possible hazards can lead to without any safety measure and then to see how today's and future safety elements ("barriers") limit the dangerous development of the hazards into accidents. As starting points of these analyses, so called Starting Point Hazards had been derived from a complete Preliminary Hazards Analysis. It shall be noted that the "unprotected" system (sometimes called "basic system") represents for a certain mode of operation today's operation, including correct train densities, etc.
3. For every Starting Point Hazard, the development of further consequences is modelled through Event Tree Analyses.
4. The chain of these events in the trees is then reduced stepwise by the "barriers", where barriers may be of technical or procedural nature. In addition to these barriers, other risk neutralizing factors ("lucky circumstances") and reduced exposure to the risk (e.g. empty train) had been taken into account to correctly reproduce reality.
5. The modelling and quantification of the barriers had been performed in a separate tool. The resulting reduction factors are transferred into the Event Trees after their calculation.
6. As for other tools of this nature, statistical and other assumptions have to be made. It has been checked, however, that reasonable assumptions lead to plausible results.

Figure 1 below shows the overall described logic of the model elements.

3 System definition, system hazards analysis and event tree analyses

The ROSA analysis was intended as a global analysis for a complete national railway, remaining applicable, however, to any national railway (the model

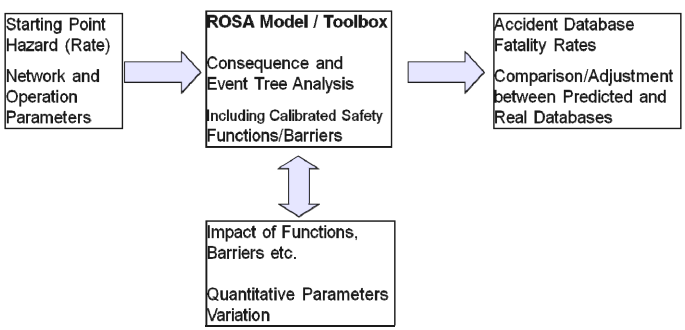

Figure 1: Overall flow chart of the ROSA model.

toolset is generic). Before application of the ROSA model to a network, first some definitions are (were) required:

3.1 Accident Categories

Accident Categories had been used similar to respective definitions of the ERA.

- Rear End, Head On and Flank Collisions, Shunting Collisions, Collisions with other railway/non-railway objects on the track.
- Derailments (derailments as a consequence of collisions not in this category, re-railments are taken into account).
- Level Crossing Accidents (collisions with individuals, vehicles, objects).
- Personal Damages inside of moving vehicles).
- Fire, others.

Suicides had not been taken into account.

3.2 System boundary

While for most typical railway subsystems, such as overhead lines, tracks or signals, it is intuitively clear that they form part of the considered system, it is less clear for some civil structures and interfaces. Therefore, the following structures had been taken out of the scope in the ROSA project:

- (Non-railway) Bridges under/over railway line. In addition, pedestrian bridges are excluded, except track change bridges for passengers as common in some countries.
- Interlocking Building and other civil structures that contain railway equipments but are not accessible for passengers.
- Yards.
- Station Areas not directly adjacent to railway tracks (e.g. shopping area).

Figure 2 shows an example of the system boundary definition.

3.3 Risk groups

For the risk groups in ROSA, the ERA definition of passenger group had been precised due to differences in the passenger definitions in Germany and in France.

- Passengers in the train and passenger exchange areas with low risk control (platform)
- Passengers in areas with higher risk control (e.g. crossing station tracks for train change)
- Staff (wayside/onboard)
- Persons on level crossings
- Unauthorized trespassers in the track area.
- Others (accompanying/escort persons, sales personnel in station, etc.)

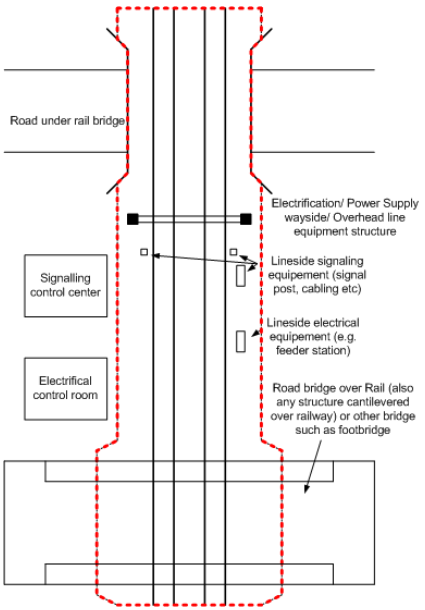

Figure 2: Example of the system boundary definitions.

3.4 Operations

With respect to operations, the ROSA project had tried to organize the different operational concepts (or, in Germany, "track categories"), such that the complete national traffic flow can be configured as easily as possible by respective weighting of the categories. Since every individual operational category/track category is not only reflected by particular equipments, but requires also different consequence analyses, every operational category fixes the respective barrier model, as well as the Event Tree Analysis.

It turns out, however, that for example categories like "Main" and "Secondary" Tracks, Category "P160", etc., as used in Germany, are not (even) compatible whatsoever with the categories used in France. The model had therefore been structured in one overcomplete tree and barrier model, such that by activating (or not) the individual elements of the tree a certain configuration of the operational/track category is generated. This shall assure usability by different diverse networks.

3.5 Hazards analysis

Critical for the ROSA model is a complete, but still generic, identification of all hazards that members of the above risk groups may be exposed to within the system boundary. Several available hazards analyses of the partners had therefore to be combined into a fault tree structure within a total of

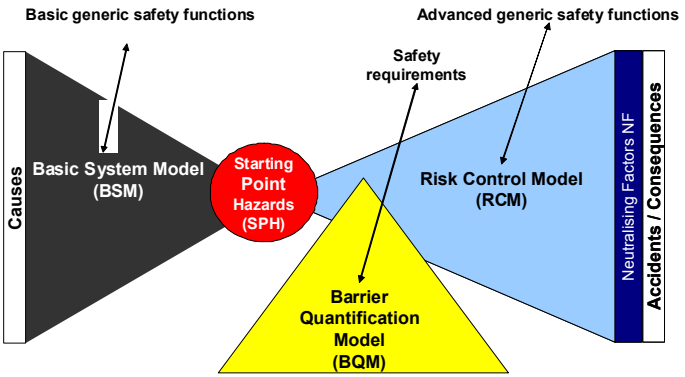

Figure 3: Double pyramid representation.

approximately 1.000 hazards, which is considered complete at this time. Since proceeding further at too low a level (e.g. "Measured distance between too low due to odometry failure") turned out to be impractical and hazards at too a high level ("vehicles too close") appeared too close to the Accident Categories, an intermediate level of hazards was selected as "Starting Point Hazards". The intermediate character of the hazard also offered the possibility to remain within the double pyramid model that is often used to define "Tolerable Hazard Rates" (see Fig. 3).

The list of the approximately 60 selected Starting Point Hazards (see Fig. 4) had been checked for completeness and mutual exclusivity (as much as possible), meaning that there is no hazard in the overall fault tree that does not lead to any of the SPH ("cause") or is not a later consequence of any SPH and that the SPHs do not follow from each other in the tree.

3.6 Event Tree Analysis

As previously mentioned, an event tree at the generic level has been developed in ROSA from each of the Starting Point Hazards. The tool FaultTree+ (Isograph Ltd) was utilized to formally store the trees. In order to show a more complete image of the typical tree content, Figure 5 shows another (PowerPoint) representation of an example tree of less complexity; larger trees, such as SPH13 (Wrong Route), are difficult to read in paper presentations.

The typical quantitative estimation to calculate the event trees includes the Starting Point Hazards rate, split factors into different branches of the tree, reduction factors and the barrier efficiencies that are imported from another part of the model (Barrier Quantification Model). By quantification, every tree leads into some contributions to a vector of accidents; compiling all accident contributions shall lead to a reproduction of an accident database.

	STARTING POINT HAZARDS
Number	Name
SPH01	Wrong speed limit, wrong VL
SPH03	Insufficient deceleration
SPH05	Wrong/ inappropriate speed/ brake command
SPH06	Wrong speed registered (wrong v_train)
SPH07	Failure of speed limit communication
SPH08	Possibility of train rolls away
SPH10	Wrong absolute/ relative position registered
SPH11	Train detection failure
SPH12	Loss of train integrity
SPH13	Possible wrong route for train
SPH14	Failure in transmission/ communication of timetable/ MA
SPH15	Guideway structural failure
SPH16	Broken switch component
SPH17	Wrong switch command
SPH18	Wrong switch status
SPH19	Object on guideway/ within CE
SPH21	Road traffic user on LC
SPH22	Slipstream effects on ballast
SPH23	Aerodynamic forces impact on train
SPH24	Train equipment/ element/ loading infringes CE of train
SPH25	Inappropriate CE dimension for train (wayside)
SPH26	Wrong distribution of loading
SPH27	Broken wheel, broken axle
SPH28	Hot axle/ wheel/ bearing
SPH29	Failure of bogie/ suspension/ damping
SPH30	Failure of vehicle frame/ car body

Number	Name
SPH31	Trespassing (security aspect)
SPH32	Authorised person crosses track
SPH33	Staff working on / near track
SPH34	Unauthorised person intrudes track (negligences)
SPH35	Possibility of person falls from platform edge onto track
SPH36	Slipstream/ person too close to platform edge
SPH38	Possibility of person leaves train intentionally (excl. PXCH)
SPH39	Possibility of person falls out of door
SPH41	Train leaves/ rolls with open doors after PXCH (uninfringed CE)
SPH42	Possibility of person falls in gangway area between two cars
SPH43	Possibility of passenger leans out of door/ window
SPH45	Staff/ train attendant leans out of door/ window
SPH47	Staff on vehicle leaning out from step
SPH48	Possibility of person falls/climbs from PLF into gap between vehicle and PLF
SPH49	Possibility of person falls out of/ leaves train without presence of platform
SPH50	Possibility of person falls in door area at PXCH
SPH51	Possibility of train doors close with person in door area
SPH52	Possibility of train moves during passenger exchange
SPH53	Possibility of person hurt in train
SPH55	Inappropriate temperature (in train)
SPH56	Toxication/ asphyxiation (in/ at train)
SPH57	Electrocution (in/ at train)
SPH58	Person falls on platform (excl. PXCH)
SPH59	Inappropriate temperature (on platform)
SPH60	Toxication/ asphyxiation (on platform)
SPH61	Electrocution (on platform)

Figure 4: List of ROSA starting point hazards.

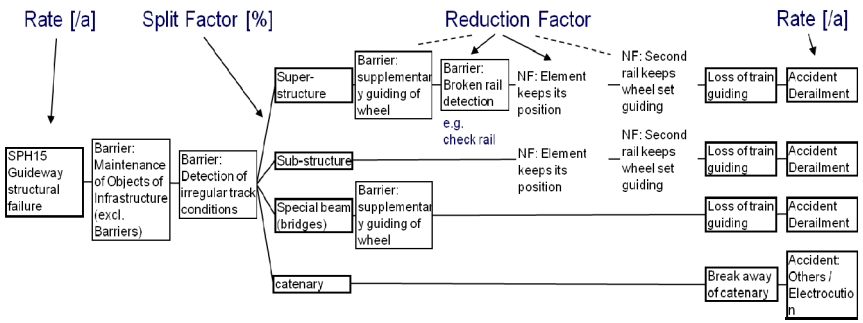

Figure 5: Lower complexity event tree example, here in a PowerPoint representation.

4 Barrier quantification model

Besides the FaultTree+ Event Tree Model, the Barrier Quantification Model (BQM) is the second major model part. Since for every generic barrier of the event trees a variety of technical or operational realizations may be used and in turn for every individual realization multiple types may exist, the BQM is organized into several levels as indicated by the example "Track Vacancy Detection" in figure 6.

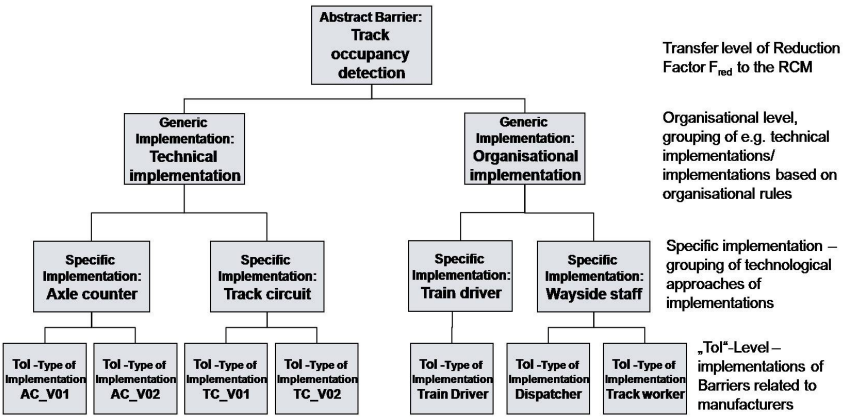

Figure 6: Example of the BQM (here track vacancy detection).

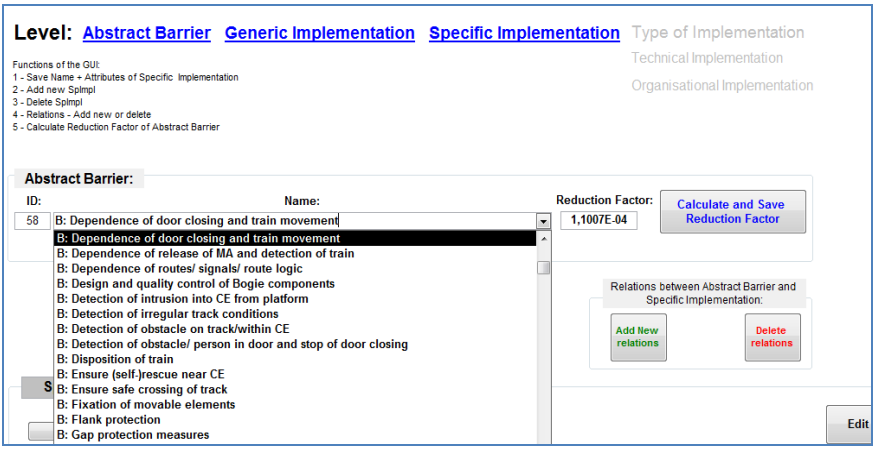

Figure 7: Example screenshot of the BQM input mask.

In order to characterize a full network, the analyst is requested by particular Graphical User Interfaces (GUI) to input with what percentages what specific Barriers are implemented on the network. In addition, new barriers or implementations may be added, as well as dependencies between barriers, procedural or human barriers and the safety efficiency of each barrier type. Other features, such as maintenance state impacts or costs, are prepared but had not been fully implemented into this first model. Fig. 7 shows a screenshot of the GUI of the BQM.

Once the input has been completed, the MS ACCESS based BQM can calculate the resulting rates for each barrier at the appropriate level, which is in turn transferred to the FaultTree+ Event Trees.

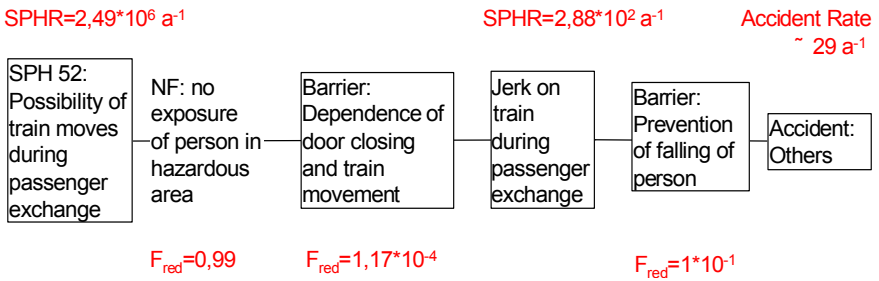

Figure 8: Quantitative estimation example.

(1)	Name	Unit	Calculation rule	Example
A	Average number of stations where a train run stops	-		13
B	Number of train runs – long distance trains	per day		2.500
C	Number of train runs – local trains	per day		50.000
D	Number of station stops	per year	365·A·(B+C)	249.112.500
E	Probability, that train moves during passenger exchange	-		0,01-0,001
F	**Number of train runs that moves during passenger exchange**	**per year**	**D·E**	**2.491.125-249.113**

Figure 9: Starting Point Hazard Rate estimation example.

5 Example: "train moves during passenger exchange"

In order to illustrate the above texts, figure 8 shows the summary numbers of the examples, where a passenger train starts to jerk/move during passenger exchange.

The ROSA tool requires the quantified estimations for the various elements, such as the Starting Point Hazard Rate, Neutralizing Factors and Barriers.

5.1 Starting Point Hazard Rate "Moving Train at Passenger Exchange"

Based on statistical data of operated trains, stations and network parameters, the total number of raw Starting Point Hazards was estimated for the reference system to approximately 2,5 million per year. It shall be noted that this rate is based on the estimation, which without any further reducing elements every 100th to 1000th train may show any move during passenger exchange in the "basic" unprotected system.

5.2 Neutralizing factors and barriers estimation

The generic event tree of the respective hazard shows two Barriers and one Neutralizing Factor. For the Neutralizing Factor "No Passenger Exposed to Hazard", a percentage of approximately 99% was assumed. For the first Barrier "Dependency between Door Closing and Train Movement" different weighted implementations of the reference system and their safety efficiency are input to ROSA (see Fig. 10), including Manual Door Closing before Train Departure, Time Interval Controlled Door Locking, Speed Dependent Door Locking,

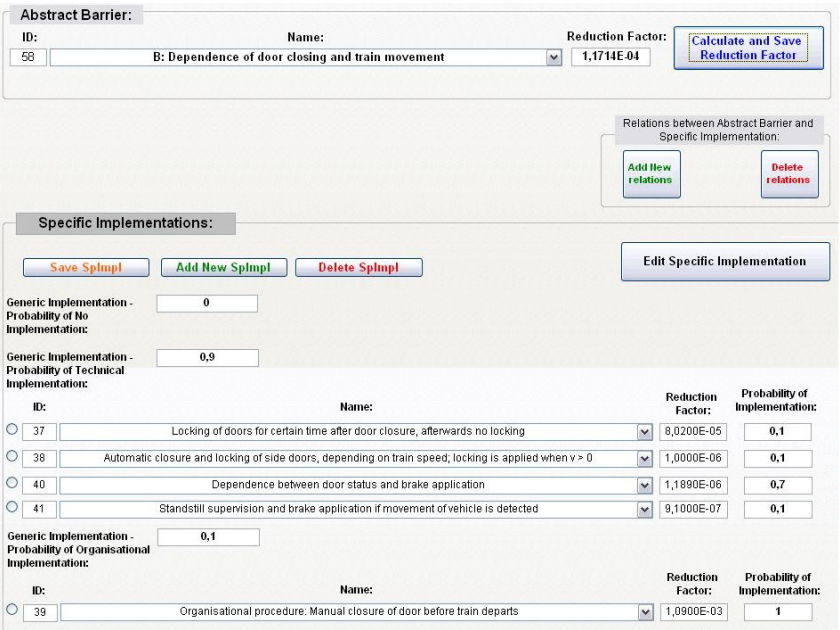

Figure 10: Barrier quantification example.

Dependency between Immobilization Brake and Door Lock Status, Zero Speed Detection (Brake Initiation). The properly weighted reduction factor is then correctly generated by the tool.

Similarly, the impact of a second barrier ("Mechanical Preventions from Falling Out of Open Doors") had been estimated and the rates were transferred to the FaultTree+ Model that resulted in the final accident number estimation.

Although the example is presented for illustration only, it shows, however, how a large estimated number of hazardous situations is ultimately reduced by independent estimations of the active barriers to a comparably low number (here 28) that are compatible with the field data of such a reference system.

6 Summary and future aspects

The ROSA project has established for the first time a consistent computer based Framework and Analysis Scheme that may permit the estimation of the safety characteristics of a complete railway network. The first utilization steps of ROSA show, as expected, that the objective requires confinement to a quite generic and higher level of detail and also the estimation of most of the rates requires separate analyses. The verification examples in the project show, however, that the tool delivers plausible results and that it remains "complete" in the sense that all relevant sources of safety (or respectively residual non-safety) even in a complex railway system (such as that of Germany).

One aspect for future work appeared early in the project, but has not been implemented due to time constraints. If approximate cost estimation for every barrier is input into the model, it should be possible to compare at a complete railway system level all relative "prices/costs for safety". Although agreement was found in the project that the objective of such an analysis cannot consist in pure Cost Efficiency aspects for Safety, it is still anticipated that such future work may contribute to high level cost benefit analyses, in particular for newly introduced safety systems.

References

[1] 2004/49/EG European Railway Safety Directive
[2] Progress report on the implementation of the Railway Safety Directive (Directive 2004/49/EC)and of the Railway Interoperability Directives (Directives 96/48/EC and 2001/16/EC), Brussels 2009
[3] IEC 61508-1 Functional safety of electrical / electronic / programmable electronic safety related systems – Part 1: General requirements, 1st ed. (1998)
[4] IEC 61508-1 Functional safety of electrical / electronic / programmable electronic safety related systems, Part 1: General requirements, Committee Draft For Vote (CDV) (2008)
[5] EN 50129 Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling (2003)
[6] "SAFE 2005", "Derivation of Common Safety Targets for European Railways", J. Schütte, TU Dresden, Rome, Italy 2005