QUESTIONING HUMAN ERROR PROBABILITIES IN RAILWAYS

F. Feldmann*, M. Hammerl*, S. Schwartz*

*Institute of Transportation Systems, German Aerospace Center (DLR), Lilienthalplatz 7, 38108 Braunschweig, Germany.
E-Mail: frederike.feldmann@dlr.de, malte.hammerl@dlr.de, stefanie.schwartz@dlr.de, fax: +49 531 295 3402

Abstract

Human errors are regarded as one of the main causes for railway accidents these days. In spite of this fact, the consideration of human error probabilities in quantified risk analyses has been very rudimentary up to now. A lack of comprehensive data and analyses in literature lead to the use of estimations and values from other industries. This paper discusses the transferability of human error probabilities for railways and identifies problems in handling methods and values. A model of working systems is used to demonstrate the particularities of railway work places and to derive a structure for performance shaping factors that influence the human error probability. A holistic approach is proposed to support the determination of appropriate human error probabilities for railways.

1 Introduction

The railway system is one of the safest transport systems available. Many safety measures have been introduced as a response to accidents. By learning from accidents much effort has been spent on the development of highly reliable technical safety systems. Because of the high safety of the technical parts of the railway system it is widely assumed that human error is the main cause for accidents nowadays. Thus, the awareness to integrate human factors into the design process grows. However, the application of human reliability assessment (HRA) is not yet common in railway engineering practice. There is a need to estimate the probability of human errors in railway risk analysis. On the following pages the usage of human error probabilities in the railway domain is discussed as well as occurring problems and solutions.

1.1 Current situation

The railway system's safety is on a very high level and is increased continuously. Over a long period of time the railway system developers have tried to design the human, regarded as the weakest part, out of the system. The proportion of human actions has been reduced, especially those that are safety-related. Among other things this has been done by introducing technical safety systems that serve as a fallback level in case of a human error. But human errors and their involvement in accidents persist. This is particularly the case in degraded modes of operation where the operator becomes a fallback level of the technical system. If in this case the operator fails, too, accidents are a likely consequence. However, the operator might be able to cope with the situation, thus reducing the risk emanating from the failure of the technical system.

Currently, many German risk analyses do not consider human actions to a satisfactory extent. They focus on the technical part of the system, not modeling the driver, the signaler and other human operators carefully. Some analyses simply stop as soon as they reach the human-machine-interface. Other risk analyses assume that the operator performs his tasks perfectly, never making any mistakes. Another common practice is to write thick operator's handbooks to cope with the technical deficiencies of the system. These handbooks do not consider whether the operator is able to fulfill the assigned task or how many errors he might make.

1.2 The need for numbers

The CENELEC standard EN 50129 [4] for railway applications requires quantitative risk analysis and the determination of tolerable hazard rates (THR). The actual hazard rate of a safety-related function must not be higher than the associated THR. The reliability of functions implemented by technical components can in most cases be estimated sufficiently. It is usually characterized by a failure rate λ from which the hazard rate λ^* can be derived. The human reliability is usually characterized by the human error probability (HEP) which is estimated by the ratio of the number n of the observed erroneous actions and the total number N of actions to be performed: HEP = n/N.

Because most safety-related functions are implemented by a combination of technical systems and human actions, most risk analyses have to consider both: the hazard rates of the technical components and the probability of human error.

The probability of human error is relevant for risk analyses in all situations where a human operator performs a safety-related task in co-operation with a technical system. The co-operation can be of various kinds: The technical system might be the tool to perform the task, e.g. a lever to set the train speed. The technical system might be a fallback system intervening only if the operator makes a mistake, e.g. an automatic braking system to prevent overspeed. The human operator can act as a fallback system for a technical system,

too, e. g. driving on sight because of a failure of a track clear detection device. In all these cases the probability of human error is needed to determine the overall system risk.

1.3 Human error probabilities in risk analysis methods

There are several methods available for risk analysis: Fault Tree Analysis (FTA), Failure Mode, Effects and Criticality Analysis (FMECA), Best Practice Risk (BP-Risk) [2], risk graph (IEC 61508-5), Braband's risk formula [2], etc. Some methods are quantitative, some are qualitative while others are somewhere in between. For a distinction between the terms qualitative and quantitative see [9].

BP-Risk considers human actions as a fallback level. The other methods are mostly used for technical systems only, but some of the methods can be expanded to include human error.
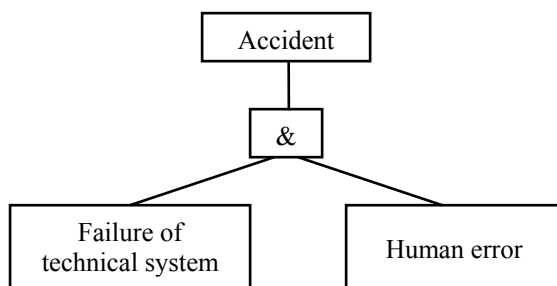

Figure 1: Schematic fault tree including human error

Human error probabilities can be applied in quantitative methods such as FTA, see figure 1 for a schematic fault tree of a system with human / machine redundancy. If the human error probability is converted into a hazard rate, it can be used in Braband's risk formula [2], another quantitative method. But human error probabilities are useful for qualitative methods, too: The common 10 categories of the probability of occurrence in a FMECA are often intervals of failure rates. A human error probability can be used to select the right category.

The knowledge of human error probabilities is of great value for risk analyses. There are situations where numbers are needed and there are methods available to process these numbers.

2 Existing human error probabilities and quantification techniques

2.1 Status quo

In the German railway domain, most risk analyses do not take human reliability into account. One of the reasons is a lack of available data. The German Federal Railway Authority, the Eisenbahn-Bundesamt (EBA) and the Deutsche Bahn AG maintain statistics on hazardous events; however, these statistics are not publicly available.

In the UK there are public statistics, e.g. on employee errors. The Office of Rail Regulation (ORR) publishes annual reports including statistics concerning signals passed at danger (SPAD). In spite of the great value of these numbers for British risk analyses these statistics cannot be simply transferred to other countries. Working conditions of German train drivers and signalers differ significantly in signaling and train protection systems and safety philosophies.

Railway incidents and accidents are rare, fortunately. Beside that, erroneous actions without any unwanted result for the overall system are often not recorded. Consequently, the collection of comprehensive data to derive statistically reliable information on human error probabilities is difficult.

In spite of these circumstances, there are a few attempts to integrate human reliability in risk analyses for German railways, see e. g. [3] and [16]. These analyses try to compensate the lack of objective data by the use of generic estimations for human error probabilities. For example, there is a kind of non written agreement to assign the probability of 10^{-3} to any human error. This number was for example used in a risk assessment of the German electronic timetable book and list of sections with temporary speed restrictions (EBuLa). But, instead of being the outcome of an objective measurement of human unreliability, the value 10^{-3} is just a hypothetical value used in an example calculation. This was revealed by Hinzen in his thesis [8], pp. 44-46. Moreover, there is no rationale for assigning the same probability to all kinds of human errors. Human beings show a much higher variability and complexity than technical components. Furthermore, the human error probability depends on several influencing factors (so called performance shaping factors, PSF) e.g. the quality of training for the task.

More sophisticated German railway risk assessments refer to the probabilities published by Hinzen [8]. His thesis provides different values for human error probabilities in railway applications depending on the stress level and the environmental conditions. Hinzen compares human error probabilities from the literature to a table provided by the Electric Power Research Institute. As the values correspond well, Hinzen assumes that the validity of the human error probabilities is verified. It is however questionable whether a pure comparison sufficiently proves the validity of the values. A deeper analysis of the origin of the numbers used in the comparison reveals that most of the HEPs date back to workplaces in the nuclear power plant sector. Hinzen also states that the transfer is not unrestrained possible because the working conditions vary reasonably between the two industries.

It can be concluded that appropriate human error data for railways are not publicly available, in Germany. In addition, the validity of values currently used in German railway risk assessments should be questioned. To obtain valid values, a common approach is the application of human error quantification (HEQ) methods, discussed in the next section.

2.2 Human error quantification techniques

Instead of giving an overview over the long list of techniques available to assess human reliability, this section starts with a description of the HEQ-process in risk analysis. Then, the methodology of two of the most common techniques is described, followed by a summary of some problems with these techniques.

In risk analysis, the analysis of possible causes of hazardous events specifies those human actions where a corresponding error probability is needed. An example of such a human action is a train driver closing the doors although a passenger stands between the open doors. The goal of the HEQ is then to provide a numerical value for that human error.

One method to provide that value is the *Technique of Human Error Rate Prediction* (THERP) [15]. The first step within THERP is to decompose the task (e.g. closing the door) into several individual tasks (like: checking visual scene, pushing a button). Then a list of HEPs and their respective task descriptions in the THERP-handbook is examined and the item that corresponds best to the action to be assessed is selected. The assessor will normally adjust this so called basic probability, depending on the effect of several listed performance shaping factors. The desired final value can then be calculated on the basis of the individual probabilities using prescribed combination rules.

The process within the *Human Error Assessment and Reduction Technique* (HEART) [18] is similar: The assessor compares the task under analysis with generic task types for which basic probabilities are provided by the technique. PSFs are used to adjust this basic value. The difference between these two techniques is the depth of decomposition: While THERP is characterized by a high degree of detail in modeling, HEART is less detailed.

Even though it is possible to generate a value for the human error probability through the application of HEART or THERP, it is important to keep in mind the drawbacks of HEQ-techniques in general. Their validity for railways is influenced by the lack of objective data (e.g. statistics) and the fact that human behavior shows a much higher variation than technical components. Different assessors can end up assessing different probabilities for the same event using the same technique. Or they determine equal probabilities although they considered different performance shaping factors. In fact, the process how to integrate performance shaping factors is not well structured in the methods. Often, the influence factors are numerous and interdependent from one another. In practice, many assessors only use the PSFs rarely [11].

Moreover, the application of different techniques can lead to the assessment of different HEPs for the same event, as revealed e.g. by Kim et al. [10] who assessed the probability of the event "Driver fails to check signal" with two different HEQ-techniques as being either 0.286 or $1.59 \cdot 10^{-3}$.

Another problem concerning the application of HEQ-techniques is mentioned by Pasquini et al. in [12]. In their study, it is found that the assumptions prior to the introduction of the Italian Signal Repetition System did not match the operative usage by train drivers. In order to assess human reliability for interaction with technical components, it is thus vital to perform a qualitative analysis, first.

Furthermore, traditional risk analysis lacks a way to model certain *errors of commission* [14]. In a fault tree, usually only *errors of omission* are modeled. Only interventions of operators that are required from the system point of view are considered – and modeled as success or failure. Interventions of operators that are not required at that time are not considered. In doing so, there is a risk to underestimate the probability of human errors using traditional risk analysis techniques.

A complete understanding of human actions, working conditions, and influence factors is the essential foundation for valid human error identification and quantification.

2.3 HEQ techniques in railways

In order to assess human error probabilities in a certain domain, an appropriate method has to be selected and thoroughly applied to the particular conditions. Traditional HEQ-techniques have been adapted to the railway domain; this section gives a brief overview.

In general, the railway industry is yet in progress to integrate human factors into system design. The awareness to include human reliability into risk analyses grows, however different opinions concerning HEQ in the railway can be found in literature. On the one hand, Hickling et al., who applied HEART for railway signaling tasks conclude that the method "was entirely applicable to all the human reliability assessment needed to be undertaken to populate the fault tree models with quantified human errors" [7]. On the other hand, Traub [13] found that the generic tasks within HEART did not map well onto railway worker's job conditions. An inspection of the generic tasks within HEART illustrates the problem: one of the task types reads: "Completely familiar, well-designed, highly practiced, routine task occurring several times per hour, performed to highest possible standards by highly-motivated, highly-trained, and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids" [18]. It is hard to find a task in the railway system where all these conditions are fulfilled. Similar problems arise with the application of THERP when task elements of a railway working environment need to be assessed, but are not represented in any of the HEP tables [11].

This was one main reason for the British Rail Safety and Standards Board to develop the so called *rail HEQ tool* which was meant to facilitate the assessment of human reliability particularly in the rail context [5]. This quantification technique is based on HEART and involves

a) Replacement of HEART generic task types by a list of generic error types

b) Proposal of rail specific probability values

c) Revision of PSFs provided by HEART to rail-specific PSFs.

According to a case study for the selection of a railway HRA-method [10], the rail-HEQ tool provided the most appropriate framework for railway tasks and environment. But: in rail-HEQ train drivers of different rolling stock were taken as experts in absolute probability judgment workshops. The following questions arise: Is it appropriate to use the mean value of responses of train drivers of different rolling stock? Do train drivers in local traffic and conventional drivers' cabs face the same working conditions as employees driving long distance trains? Was taken into account that humans have difficulties estimating error probabilities? Did the drivers intentionally overestimate their reliability due to social

desirability? Besides, it is questionable weather these HEPs can be transferred to German railway applications due to differences between national railway systems, train cabs, wayside equipment, and train protection systems.

Finally, it is to resume that the need for human error probabilities can actually not be met comprehensively.

3 Model of Working Systems

A profound analysis of actual procedures and the human-machine-interaction represents the starting point for the estimation of human error probabilities. Therefore, a model of working systems and a detailed task analysis are tools to understand railway work places and differences to other domains. They contribute to the discussion whether and how human error quantification techniques can be transferred to the railway domain.

3.1 Basic model

In this chapter, a model covering a wide range of ergonomics and human factors issues is presented. The model was first published in [6] and is applied to the railway domain. The visualization supports the sound analysis of railway work places and the identification of relevant PSFs.
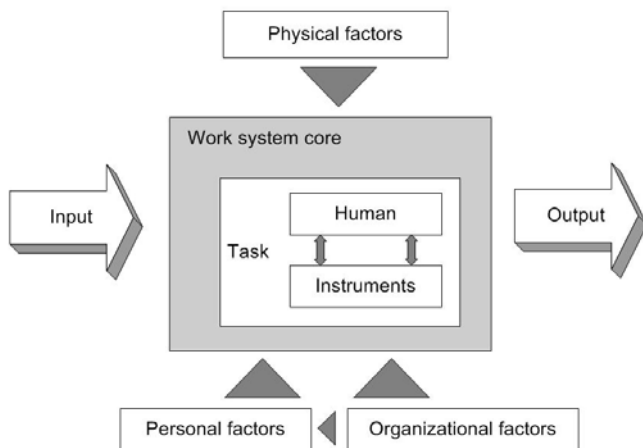

Figure 2: Model of working systems, basis

The model of working systems starts by defining the work system core as an interaction of a human, his task, and his instruments. These three items are presented in the center of figure 2. In the model, physical as well as organizational factors are regarded as influencing factors on the work system core. Additionally, the work depends on personal factors of the human. Physical factors not only represent the set of classic ergonomics, such as anthropometric design, light, and climate conditions etc. The design of the human-machine-interface and its usability belong to physical influencing factors as well. Age, health, motivation, and experience can be regarded as examples for personal factors. The organization also has an influence on the work system core through managing working conditions with roster planning, employee education and training, social programs, and its safety culture. Standards and guidelines also belong to

organizational influencing factors. It is clear that some of the organizational measures have an impact on personal factors, see the small arrow at the bottom of figure 2. For example the roster planning has an influence on the fatigue. These influencing factors have a continuous influence on the work system core and are less dynamic. In contrary, the horizontal axis represents the work system in the moment of operation: inputs can change dynamically. Via the work system core, influencing factors as well as input factors have an impact on the work output on the right hand side.

3.2 Human representation in the model

For the application of this model to railway work places, a second layer was added to the core of the work system. This is due to the high mental part of the train driver's and the signaler's work. How the influencing factors take effect on the human cognition can either be interpreted as a second layer of cognitive reaction behind the work system core or as a zoom on the human in the work system (figure 3 as the new center of figure 2). In either way, there is a tight interaction between the psychological issues and the work system basic representation. Phenomena like workload, stress, vigilance, and situation awareness shall here be understood as dependent from the influencing factors. For example, vigilance depends on the fatigue (personal factor), the roster planning (organizational factor), and in a certain way on the design of the human-machine-interaction as well – think of the dead-man's device for train drivers.
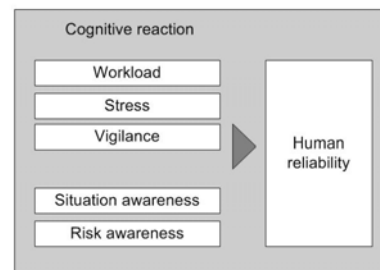

Figure 3: Model of working systems, layer of cognitive reaction

The modular setting of the model enables to add other human representations, for example as further layers in the center of the model (not depicted). Wickens' model of resources [17] can be interpreted as a third layer or a deeper zoom into human cognition.

In the model, the perspective of ergonomists and engineers is merged with psychological approaches. The integration of the two axes, the work process (horizontal axis) and the influencing factors (from the top and the bottom), helps to visualize and to separate independent (influencing and input factors) and dependent variables. With the influencing factors, functional chains between modifications and corresponding results for railway operation and safety can be set up (see [6]). They support the analysis of where the highest potentials for the reduction of human error can be found.

3.3 Railway application

In this section, the working system of train drivers is considered. Performance shaping factors are presented according to the structure of the model. The new six classes offer a better overview compared to existing HEQ-techniques:

- Input
- Physical factors
- Personal factors, influenced by organizational factors
- Personal factors, not-influenced by organizational factors
- Organizational factors, with impact on personal factors
- Organizational factors, without impact on personal factors

In an analysis of the scope of the classes, performance shaping factors were identified – some from existing human reliability assessment techniques were assorted and realigned. Concurrently, an example is given by the application to the train driver working system:

Input:
- Track observation
- Information obtained by signals (signal aspects)
- Information obtained by cab instruments
- Radio communication
- Weather conditions
- Delay
- Degraded modes of operation (e.g. due to signal failure, construction work etc.)

Physical factors:
- Design of human-machine-interface on board: usability of instruments (consistency, compatibility, dependability, correctness, directness, clarity)
- Design of wayside infrastructure: usability of signaling system; positioning of signals
- Physical working conditions
- Design of documents

For space reasons, the last four classes are not listed comprehensively as their characteristics are less railway-specific. For train drivers, work and vehicle experience, rule and route knowledge, risk perception and awareness, trust, fatigue, and motivation can be mentioned as personal factors that may be influenced by the organization. The output of a train driver's working system represents control of the train movement, additionally communication to staff and passengers.

While applying performance shaping factors to the train drivers' task, a list of particularities becomes apparent. The following set should not be understood as a complete list, but as an explanation of differences. Of course, the train driver has a mobile work environment and a single person job. Consider input and physical factors: driving a vehicle instead of working in a control center implicates input from trackside

and onboard devices. Additionally, sight conditions and vehicle control differ due to high influence of weather and time of day. Unless a continuous train control system with cab signaling is installed, trackside signals only offer a short time window to perceive the signal aspect – in spite of their high importance. In several cases, information is displayed far before the operator has to perform an action, e. g. the application of brakes must be started at a certain period of time after the restrictive signal aspect of the distant signal. Concerning organizational factors, it is to state that a large set of rulebooks and a complex composite of degraded modes, corresponding operations and procedures are particular for German the train driver working system. Nowadays, the task involves a high mental and supervisory part. The driver has a high degree of responsibility, but a low degree of movement control; movement authorities are given by the signaler. The task is characterized by modern automation mechanisms, monotony in normal operation and a sudden involvement in degraded modes. Bainbridge's well known ironies of automation [1] are apparent and train drivers are susceptible to the out-of-the-loop-syndrome and loss of skills. Finally, train drivers face high and continuous risk awareness due to their own driving and the fear and a psychological impact of suicide victims.

Obviously, the workplace of the train driver includes some very particular working conditions. We argue that some of them can hardly be modeled by methods developed for the nuclear domain.

3.3 Holistic approach

This paper proposes a holistic approach to analyze the actual working conditions and the interaction between the operator and his instruments and wayside equipment. A hierarchical task analysis is one of the tools that can support this systematic analysis of the interaction and the interfaces.

Often, a certain action of the human operator is isolated to estimate the human reliability during interaction with a technical component. This represents the point of view of the safety engineer calculating the reliability of an element in the fault tree. This method lacks an analysis of tasks the operator has to perform in parallel at that point of time, and therefore lacks an understanding of the cognitive demands in that moment. The task analysis should not only focus on certain tasks but on the entire task scope of the operator.

As a following step, cognitive demands can be derived. This step supports the analysis of the work load for concrete scenarios. By dint of this analysis, in a following step, failure types can be identified. Here, errors of commission are integrated into the considerations. This analysis of the tasks, connected cognitive demands, and possible human errors is the sound basis to quantify human error probabilities as a next step.

4 Conclusion and outlook

In the first chapter, the need for probabilities was outlined. The following section showed that current practice for human error estimation in the German railway domain does not

represent a sound approach. Fixed values, used in the railways, do not suit the complexity of human error. The empirical foundation of some values is also arguable (e.g. the number of 10^{-3}) or date back to different industries. Even Hinzen's discussion of probabilities does not answer the question of transferability to the railway domain satisfactorily. Human error quantification techniques exist and support the calculation; however some drawbacks concerning their validity for railway work places were shown. In section 3, a model for working systems was presented and the working conditions for German train drivers were briefly analyzed. Especially the train driver's task differs significantly from control center work stations, for example in the electric power industry. The great differences support doubts whether classic human reliability assessment methods like THERP are fully applicable to the railway domain.

The model and the performance shaping factors were not only presented to outline the differences of railway work places to other domains, but also as an approach to another way to understand human factors in railways. The modular layout enables an easy interpretation of human-machine-interaction for work system designers, reliability assessors, and psychologists. A new division of performance shaping factors was presented and applied to the railway domain. The determination of independent and dependent variables supports the identification of potentials for human error reduction.

For a new, holistic approach, this paper tried to outline the first steps: start with a profound qualitative analysis of the working system to understand the human-machine-interaction. Then, a cognitive analysis and workload assessment for the entire task scope represent the following steps on the way to human error probabilities. Here, the new understanding of performance shaping factors may help to reorganize basic human error probabilities and corresponding impacts. Existing techniques for quantification of human error can serve as a basis and can be adapted to future needs in railway systems in a next step.

The items on the most promising and one of the most important functional chain are design of human-machine-interaction, cognitive demands, workload, human error, and their impact on railway operation performance and safety. In order to consider this line, the Institute of Transportation Systems operates a laboratory where subject studies will support railway human factors research.

References

[1] L. Bainbridge. "Ironies of automation - Increasing levels of automation can increase, rather than decrease, the problems of supporting the human operator", *Automatica*, **19**, pp. 775-779, (1983).

[2] J. Braband. "Risikoanalysen in der Eisenbahn-Automatisierung", Hamburg: Eurailpress (2005).

[3] D. Brünenberg, D. H. Enders, J. Gullasch, J. Hartmann, J. Six.: "Risikoanalyse FFB – Ursachen- und Folgen-analyse anhand von Beispielen" *SIGNAL + DRAHT*, **93** (10), pp. 18–25, (2001).

[4] CENELEC. "EN 50129 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling" (2003).

[5] J. Gilroy, E. Grimes. "The development and application of a rail human reliability assessment tool", *People and rail systems – Human factors at the heart of the railway;* pp. 455-463, (2007).

[6] M. Hammerl, B. Jäger, K. Lemmer. "An integrated model for working environments and rail human factors". *D. de Waard et al. (Eds.): Human Factors for assistance and automation*, pp. 415 - 427, (2008).

[7] N. Hickling, L. Gaskell, T. Clarke. "Generic Human Reliability Assessment for Railways: Results", *People and rail systems – Human factors at the heart of the railway;* pp. 447-454, (2007).

[8] A. Hinzen. "Der Einfluss des menschlichen Fehlers auf die Sicherheit der Eisenbahn". Aachen (1993).

[9] B. Milius. "A New Classification for Risk Assessment Methods", *E. Schnieder, G. Tarnai (Eds.): Proceedings of Symposium FORMS/FORMAT 2007*, pp. 258–267, (2007).

[10] J. Kim, W. Jung, S.-C. Jang, J.-B. Wang. "A Case Study for the Selection of a Railway Human Reliability Analysis Method" *International Railway Safety Conference: Dublin*, (2006).

[11] B. Kirwan. "The validation of three Human Reliability Quantification techniques – THERP, HEART and JHEDI. Part 1 – technique descriptions and validation issues", *Applied Ergonomics*, **27** (6), pp. 359-373, (1996).

[12] A. Pasquini, A. Rizzo, L. Save, M. A. Suja. "Quantitative Evaluation and Operative Usage of Interactive Systems", *Proceedings of the 12th International Symposium on Software Reliability Engineering*, pp. 356-361, (2001).

[13] P. Traub. "Human Error Analysis in Railway Safety Cases; Panacea Or Poison", *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting*, pp. 2065-2069, (2004).

[14] O. Sträter, B. Reer, V. Dang, S. Hirschberg. "Methoden zur Analyse von kognitiven Fehlern: Ergebnisse einer ersten Anwendung von Methoden und Ausblicke auf zukünftige Arbeiten", *Viertes Expertengespräch Mensch-Maschine-Wechselwirkung in Kernkraftwerken*, pp. 54-73, (1999).

[15] A. Swain, H. Guttmann. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", Sandia National Labs, US Nuclear Regulatory Commission: Washington D.C., (1985).

[16] Wegel, Hansen. "Sichere Bahn trotz hoher menschlicher Fehlermöglichkeiten. Analyse zur Robustheit des System Eisenbahn am Beispiel der Zugdateneingabe", presentation on *7th Bieleschweig Workshop*, (2006)

[17] C. D. Wickens. "Multiple resources and performance prediction" *Theoretical Issues in Ergonomics Science*, **3** (2), pp. 159-177, (2002).

[18] J. C. Williams. "HEART – a proposed method for assessing and reducing human error", *9th Advances in Reliability Technology Symposium*, (1986).