Foto: Max Lautenschläger

Concept

# Report
# Engineering competence maintains safety in a changing railway world

DB Systemtechnik GmbH

Minden, Germany

R. Puettner, M. Geisler

# Contents

# 1 Introduction

Human beings are always exposed to hazards caused by the application of technical systems wherever the system is used. This is also true for the use of railways. Railway operation is recognized as a safety mode of transport today. Long experience of operation, comprehensive rules, high quality of technical systems, well trained and reliable staff contribute to that recognition. Nevertheless absolute safety is not achievable.

The frequency of unwanted events and accidents within the railway system in comparison to other modes of transport is very low. In case of such a rare accident the consequences could easily be enormous – which we have seen in the past already.

The remaining risks arise from not identified hazards caused through changed condition and occur in unwanted events. To identify these causes and to take measure in advance is one task of the engineering risk assessment.

## 2 Traditional Approach

Until today after the occurrence of an unwanted event the railways reacted with additional or amended measures which focus on the elimination of the specific causes of that event to improve safety at that specific situation. These measures and knowledge were considered for changes and improvements of the system consequently. Risk could be controlled.

The approach was successful: The level of safety of the railway system increased continuously year by year towards that high degree. Nevertheless there are disadvantages :

The occurrence of an unwanted event or even an accident was the trigger for the identification of the causes of their hazards and the related risk. An event with harm to people or the environment raised discussions about the acceptance of risk and lowered the reputation of the system although the frequency has always been low.

A verification of the suitability of the new or amended measures was only partly possible due to the low frequency of the occurrence of these causes. It was not possible to demonstrate whether the non-occurrence of the unwanted event was the result of the improved safety measures or just due to the low frequency of occurrence.

Another weakness of the traditional approach is that it is difficult to assess whether on-going changes and improvements of the railway system lead to hazards which are not covered by existing safety measures. The structured identification of gaps in safety was hardly possible.

The assessment of the appropriateness of additional or improved safety measures for the control of risk was not in focus which could lead to over engineered or even counterproductive solutions.

To avoid these shortcomings  and to ensure that the complexity of the today's railway system can be handled in a safe manner in future as well the pro-active risk assessment has been implemented in the railway domain through the safety management systems.

# 3 State-of-the-art Approach

Even today absolute safety does not exist, absolute safety is not achievable, but a predictive approach supports to maintain and improve safety continuously. The pro-active kinds of risk assessments combined with structured methods and tools support the analysis of hazards within a specific part of the railway system and at its interfaces. It enables to assess the existing level of safety by taking into account implemented measures for risk control. Not adequately controlled risks are lowered by the implementation of new of improved safety barriers – before an unwanted event occurs. This pro-active approach leads to a map of the safety level of the analyzed sub-system of the railway.

## 3.1 Methodology

The methodology is based on a structure which can be applied in the same way and which leads – based on experience – to the best results of the assessment of the risk and of safety requirements for safety related functions. The methodology comprises the modules

- Aim and purpose of the intention (e.g. change)
- Definition and description of the (new or changed) system under assessment incl. conditions to be considered
- Identification of hazards
- Assessment of hazards, if appropriate focusing on relevant hazards
- Risk evaluation against risk acceptance principle.
- Development of additional measures to maintain the level of safety.

The structured way of working ensures a high degree of completeness of the analysis. Nevertheless a proof of completeness is not possible.

Experts for technical, maintenance or operational aspects are required next to experts for risk assessment: an engineering approach. It is essential that all contributors for the risk assessment are informed about the current status of the concept, developments, construction of the system under assessment – therefore the system definition needs specific awareness.

The depth of analysis is related to the significance of the project. Especially for innovative and complex projects it is necessary to go into all details.

## 3.2 Application Conditions

To apply the existing and appropriate methods and tools sufficiently competence and understanding for analysis techniques and the system under assessment itself are necessary. Next to the required technical competence of the system under assessment the experienced consulting and moderation of the analysis process is recommended.

The risk assessment should ideally start with the first draft of the technical concept of the system intended to be assembled or changed. The risk assessment accompanies the whole process including the design freeze, the technical design until the realization / construction of the system or component. If and only if the risk assessment is done in parallel to the technical specification it can provide its best affectivity and effects. Even after the system is in operation the pro-active risk assessment continues to renew safety measures if e.g. operating situations occur which had not been covered or the system is intended to be changed.

## 3.3 Challenges

The biggest challenge for the realization of this state-of-the-art approach is that traditional engineering approaches must be amended. Many applicants are familiar with the well-known rule-

based approach and have difficulties to apply new methods as the existing system is highly safe and the necessity of the change is not acknowledged.

The application of the risk assessment is difficult if the lifecycle model is not followed or if ongoing changes of the concept or technique of the system under assessment are done. The system definition and the hazard identification require continuous amendments to be up to date which leads to additional checks of the integrity of the already done assessments.

The results of the application of the risk assessment are always to be updated if changes of the concept and/or the technique of the system under assessment are introduced by the engineering. Ongoing changes on the concept lead at least to an increasing effort in documentation. Even more additional effort must be considered if interfaces are influenced in their safety behavior and additional measure for hazard control and risk mitigation are necessary to maintain at least the level of safety.

## 3.4 Benefit

The benefit of the pro-active risk assessment is obvious: Hazards and risk are identified and assessed without any exposure of people or environment to the risk. Furthermore such an approach reduces cost and time during the development of engineering projects. Requirements for safety-related function of substantial changes of sub-systems are known on time and are designed before construction which is always cheaper than additional amendments after the implementation was finished.

## 3.5 Example

An example illustrates the influences of weaknesses in engineering concepts.

### 3.5.1 Example – Description

Let's have a look on a modification project where a shunting locomotive is change to a locomotive for special needs.

For specific high-speed routes in Germany it is necessary to operate special rescue and emergency trains (R&E Trains) to meet the requirements of the rescue and emergency concept. These R&E Trains are built with container carriages and special containers on it, in which fire brigade equipment, firefighting water and other rescue equipment is carried to the place of the accident. As the relevant high-speed lines have a high number of tunnels the containers must be gas proof to protect the staff of the R&E Train and the rescue team and to allow that people involved in the accident can be secured and moved away from the hazardous area.

Two special diesel powered locomotives are necessary to operate each R&E Train. These locomotives are built out of modified existing shunting locomotives. The actual project contains the renovation, modernization and partly new design of the existing locos.

In addition to the requirements for a shunting locomotive special aspects must be considered:

1. Operation of the locomotives on high-speed lines in parallel to oncoming high-speed trains
2. Emergency pull back operation of the locomotive if the accident's surrounding becomes too dangerous for the rescue team (e.g. increase of toxic gases or temperature) – escape functionality overruns protection function of the locomotive.
3. Remote control of the locomotive by the train driver  located in the gas proof container (e.g. if the place of the accident is in a tunnel filled with smoke only by camera view (e.g. optical and infrared)

Out of these requirements specific conditions must be considered for the systems of the R&E Train. Next we will consider the locomotives.

Requirement 1: For operation on high-speed lines the driver's cabin must be designed to protect the staff against air-pressure waves resulting from oncoming other trains running with high speed. Especially the windows, the doors and the air-conditioning system must be designed for these specific needs.

Requirement 2: If the R&E Trains must escape from the location of the accident due to an uncontrolled hazardous situation, it must be ensured that failures of functions do not block the running of the train. Systems must be implemented which deactivate supervision and protection functions fast and efficient. The risk of damages to the motor of the locomotive due to overheating is less important than a reliable escape possibility. Even in case of a brake failure it must be possible to operate the train in an emergency case. The safe state of a train in normal operation that in case of a brake failure braking must designed as a fail-safe reaction is in contradiction to the escape operation where a deactivation of the brakes must be possible.

Requirement 3: All the functions of the locomotive must operate in the same manner and with the same failure reaction compared to normal operation if the locomotive is controlled by remote.

### 3.5.2 Example – Hazard Identification and Safety Measures

We limit the example now on the functions for requirement 1 and 2.

The following hazards were identified, if a task or function is conducted not or wrongly (examples are not comprehensive):

Hazard 1.1: In case of air pressure waves the entrance door of the driver's cabin opens: the driver could fall out of the door. This hazard is to be rated as safety relevant, because a human could be harmed.
Measure 1.1: The door locking system is designed with sufficient stability and function.

Hazard 1.2: In case of air pressure waves the window of the driver's cabin fails: bits of broken glass enter driver's cabin. This hazard is to be rated as safety relevant, because a human could be harmed.
Measure 1.2: The window is designed with sufficient stability and function.

Hazard 2.1: The escape from the location of accident is not possible, because the supervision and protection function locks the locomotive's traction control. Driver and rescue team cannot leave the location of accident and could be harmed (e.g. because of high temperature or toxic gas). This hazard is to be rated as safety relevant, because several humans could be harmed.
Measure 2.1: The monitoring system should to be deactivated before the rescue operation, but must be reactivated for regular operations. It must not be deactivated by mistake.

Hazard 2.2: The escape from the location of the accident is not possible because the braking system failed and the brakes cannot be released. Driver and rescue team cannot leave the location of accident and could be harmed (e.g. because of high temperature or toxic gas). This hazard is to be rated as safety relevant, because several humans could be harmed.
Measure 2.2: The braking system in case of its failure has to be released quickly without affecting the intact parts of the braking system. It must be ensured, that a subsequent regular operation of the locomotive is possible only with a regular safe condition of the braking system.

### 3.5.3 Example – Influences on design and construction

During the the work progress of concept and design it becomes clear that the replacement of old technique by modern solutions cannot be made without consequences to gain safe operations.

The consequences of the newly defined requirements after the application of the pro-active risk assessment were new concepts and surveys; for example:

Hazards 1.1 and 1.2: It had to be checked if the doors locking system and the windows in the driver's cabin meet the new requirements.

Hazard 2.1: The vehicle control concept has to be modified. The contradictory requirements for regular and for rescue operation still can be met only by manual action of the driver and by operational rules.

Hazard 2.2: The pneumatic brake concept has to be modified. The contradictory requirements for regular and for rescue operation still can be met only by manual action of the driver and by operational rules.

### 3.5.4 Example – Effort and Results

The practice of this reengineering project shows that the application of the pro-active risk assessment started much too late. Main concepts and requirements were already fixed. As the old locomotives which “only” have to be modernised, fulfilled their tasks since many years and there are no changes in the general requirements of their regular and rescue operations, no need of risk assessment was seen in the very beginning.

The effort for pro-active risk assessment has often been under determined and increased additionally because components and sub-systems had been ordered by many different suppliers. Only one major sub-system was under the responsibility of one partner.

Due to this diverse situation many interfaces had to be handled with huge effort of alignment as some suppliers had to be convinced to take over their safety responsibility. Finally the necessity of the safety cases resulting from the safety requirements was understood.

The integration and approval of the first locomotive will start shortly. At that phase it will be clear which requirements could be considered on time in design and construction and which of these functions contribute to a safe system in operation.

A number of requirements as results of the risk assessment were on-time that changes during construction could be avoided. E.g. the specification of the locomotive’s frame, the overall control system and the brake design were in a phase where the amendments could be done easily.

Some requirements have not been considered during design. Later amendments are expected as the overall separation of the vehicle structure was already finalized.

# 4 Conclusion

The state-of-the art pro-active risk assessment in comparison to the traditional approach has the advantage that hazards and risks can be identified well in advance. Their control can be considered and implemented already in the concepts. This leads to products of the today highly complex system from the beginning to a high level of safety in operation and in addition to a high degree of availability.

The pro-active risk assessment requires a higher amount of time and effort at the beginning of a project compared to traditional approaches. This amount of effort reduces during integration and operation the activities of re-engineering. Re-engineering during integration and operation costs a lot more as changes are more complex if they even can be implemented.

A structured project management takes time for risk assessment at the beginning of a project which will be re-earned during construction and integration.

Nevertheless to convince all players of the advantages of pro-active risk assessments is still a long way to go.