MODEL OF SAFETY LAYERS IN THE RAILWAY SYSTEM - MoSiS

Markus Pelz[1], Stefanie Schwartz[2], Michael Meyer zu Hörste[3]

Summary: The Institute of Transportation Systems (IFS) of the German Aerospace Center (DLR) is engaged in research regarding technical as well as operational safety and human factors in railways. The aim is to develop a model of safety layers (MoSiS – Modell der Sicherheits-Schichten) in the railway system to make safety scaleable. With this model of safety layers it will be possible to look at the safety of a railway system in a modular way. This contribution presents the basic approach to achieve this aim using the example of a level crossing.

1. Introduction

The IFS researches new possibilities to improve efficiency and performance of railway lines while maintaining the existing high level of safety. These two aims are somehow contradictory. Observations show that high performance systems have more safety gaps than those with a high level of safety but low performance. The more restrictive safety is dealt with the more performance the system will loose. More permissive regulations give better performance but might decrease safety.

Increasing requirements for the development of new products (faster, cost-effective, more variants etc.) make it more and more difficult to comply with all safety constraints and to prove the safety of systems. On the other hand the railway system has reached a very high level of technical safety: Today less than 1 % of all accidents with damage to persons are caused by technical failures during normal operation [1]. In spite of that we still have a high number of accidents that occur at a particular part of the railway system: the level crossing (see fig. 1) [2].

Level crossings are often a cause of decreasing performance. They often imply a constraint on safety, too, particularly in degraded modes of operation. This is the source of motivation for developing a model that aids in showing that safety can be improved by using low cost technology, available at the market, together with appropriate process instructions.

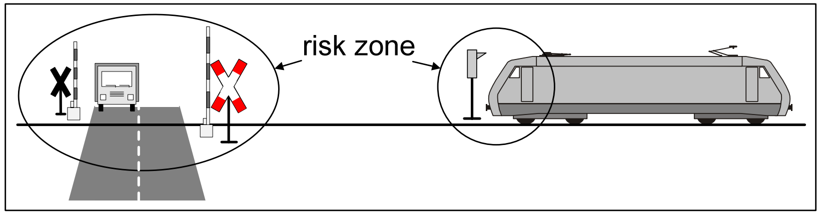

Fig.1. Level crossing with barriers

Improving safety usually means spending a lot of money. One of the reasons for this is the existing high level of safety – a lot of measures have already been taken. Another reason is the trend to use components suitable for SIL 4 applications regardless of the actually needed SIL (Safety Integrity Level [3]). There are attempts to get away from these very expensive components, to use components suitable only for SIL 2 or SIL 3 applications instead – without decreasing safety.

Regarding these components – in combination with rules and operating procedures – there are two problems that need to be solved: First, the gaps in the existing safety system need to be identified, so it becomes clear what needs to be done to improve safety. Second, it needs to be shown that the new solution really does ensure the required level of safety. The model of safety layers (MoSiS) shall help with both of these problems.

2. Terms and Definitions

To develop a model that shows the flaws of the existing safety system we need to know how it comes to accidents. Which are the critical situations, the component failures, the human errors, the unobserved rules? We need to do accident analysis. From the result of this analysis we build our model. Which methods and models we use for that will be explained in the next paragraphs.

2.1. Safety Layers

Safety layers are used in several areas. In computer science a safety layer describes a mechanism that aims at detecting errors in communication. The term is also used for a part of an application that checks the access authorisation of communicating processes [4]. Medical science uses the

[1] e-mail: markus.pelz@dlr.de, phone: +49 531 295 3483; fax: +49 531 295 3402;
German Aerospace Center, Institute of Transportation Systems, Lilienthalplatz 7,
38108 Braunschweig, Germany
[2] e-mail: stefanie.schwartz@dlr.de, phone: +49 531 295 3444; fax: +49 531 295 3402
[3] e-mail: michael.meyerzuhoerste@dlr.de, phone: +49 531 295 3440; fax: +49 531 295 3402

similar term “layers of defence”. These layers are often illustrated in form of the so-called Swiss cheese model (see chapter 2.2.).

For our purpose of building MoSiS a safety layer is a combination of technology and procedures, of components, rules and persons that are considered as an interrelated entity, represented by one layer. A combination of different safety layers leads to a safety concept for the system under consideration (see fig. 2).

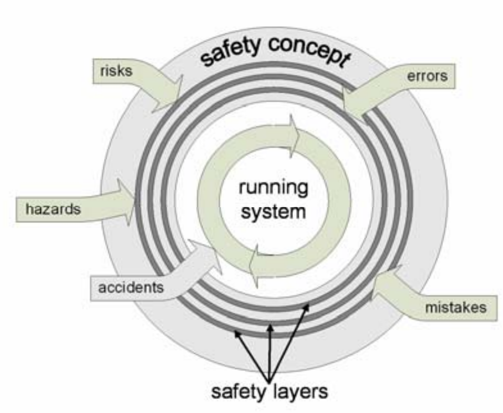

Fig.2. Safety concept built of safety layers with influencing factors

A system is considered to be safe as long as its safety layers block or at least weaken any errors or hazards that threaten the system. No accident should happen until every single safety layer of the system has been broken. If an accident happens this can have several reasons:

- The safety layer failed.
- The safety layer was circumvented or sabotaged.
- The system was used outside its operating parameters.
- A safety layer was missing.

There can be very good reasons for running a system without a specific safety layer. The layer could be far too expensive, even impossible to design and the remaining risk simply acceptable.

2.2. Swiss Cheese Model

Usually it takes more than one single failure to cause an accident. Especially where the existing level of safety is high a combination of several failures is needed so that it comes to an accident. To illustrate this James Reason developed the LOP-Model (LOP = “layers of protection”), also known as “Swiss cheese model” [5]. The name Swiss cheese model comes from the fact that every layer of protection has weaknesses, gaps, through which hazards can enter the system. These gaps can best be illustrated by holes in a slice of cheese (see fig. 3).

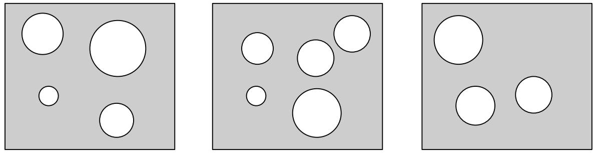

Fig.3. Layers of protection according to the Swiss cheese model

Reason’s Swiss cheese model is the starting point for the development of MoSiS. It is essential that the development of a model of safety layers starts with the identification of the flaws of the railway system.

2.3. Accident Analysis

First, it is necessary to find out why it comes to an accident, e. g. at a level crossing. This is done by accident analysis. The analysis gives us the reasons behind the accident, the relevant situations, involved components, involved persons and applicable operational rules. Accident analysis methods, for example from aviation, are applied to railway accidents and incidents. One analysis method already used in the railway sector is the Why-Because Analysis (WBA) of Peter Ladkin [6].

For a WBA one starts with the accident and then asks for the causal factors that contributed to that accident. An especially nice feature of this method is the graphical representation of the analysis. The accident and its contributing causal factors are illustrated by a Why-Because Graph (WBG). WBGs have an easy to understand format, suitable for discussion among different stakeholders. For an example of a WBG see fig. 4.

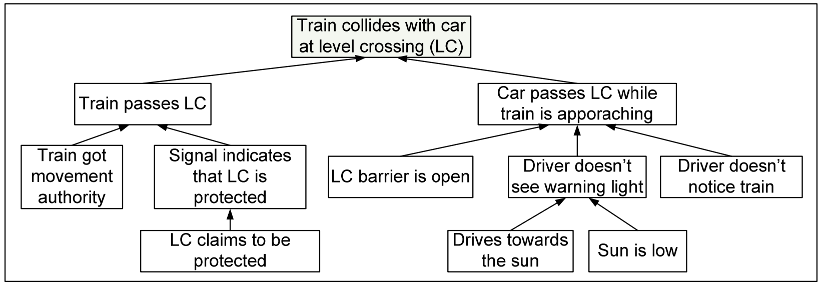
Train collides with car at level crossing (LC)
Train passes LC
Car passes LC while train is apporaching
Train got movement authority
Signal indicates that LC is protected
LC barrier is open
Driver doesn’t see warning light
Driver doesn’t notice train
LC claims to be protected
Drives towards the sun
Sun is low

Fig.4. Example of a Why-Because Graph

3. MoSiS: Model of Safety Layers in the Railway System

By means of MoSiS (the model of safety layers that is currently under development at IFS) it shall be possible to look at the safety of the railway system in a modular way. It shall assist in creating a custom-built, cost-effective safety concept. The aim is to reduce costs, compared to current status, and thus to increase the cost effectiveness of the railway system without neglecting safety. MoSiS is also expected to be helpful for building safety cases.

To build a model of safety layers a sufficiently large accident database is needed. When building this database it is important to take an appropriate sample of accidents. That means one should always investigate more than one accident of a type (e. g. level crossings accidents or derailments).

It is practically infeasible to build a model of safety layers of the whole railway system all at once. We need a starting point, a small, well-defined subsystem. It needs to be a subsystem where (in a statistical sense) a sufficiently large number of accidents occur. According to Eurostat [7] 17 % of all railway accidents in the EU in 2005 happened at level crossings. So, a level crossing could be a good subsystem to start with (see fig. 5).

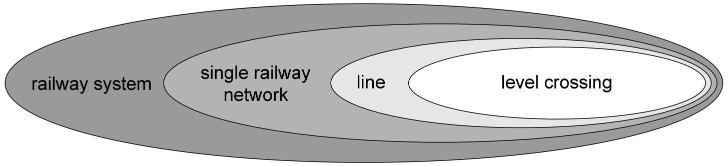

Fig.5. Expanding MoSiS from starting point level crossing

After choosing the starting point the following tasks have to be performed:

- Accident analysis (e. g. using WBA)
- Identification of flaws in the subsystem
- Construction of safety layers

From here we can build the model of safety layers for the chosen subsystem, using Reason’s Swiss cheese model as a basis. To get alternative safety concepts for the subsystem the next steps will be:

- Close the gaps in the safety layers
- Add new safety layers
- Exchange safety layers
- Recombination the existing safety layers.

3.1. Accident Analysis and Existing Safety Layers

The collected accident data need to be analysed in a structured way. To stick to the example: We will select a reasonable number of level crossing accidents from the database and perform WBAs for all of them. The WBAs will give us the causal factors that led to those accidents. Every causal factor provides an indication of a flaw in the level crossing subsystem. From these flaws we start to construct the existing safety layers. Every flaw is a gap in a safety layer. So, when we found a flaw, we know there has to exist a safety layer around it. Using the Swiss cheese model for illustration this approach can be described as shown in fig. 6.

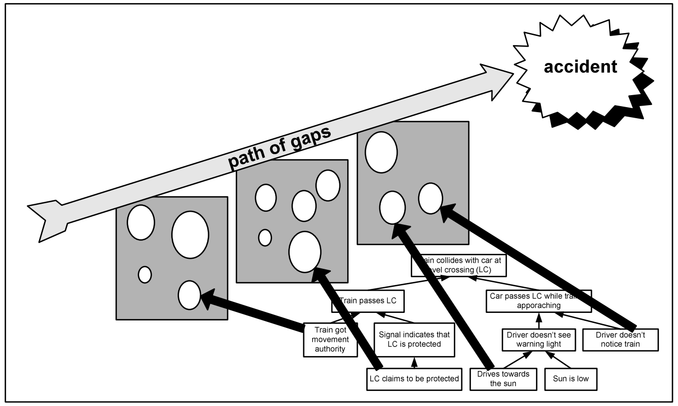
accident
path of gaps
Train collides with car at level crossing (LC)
Train passes LC
Car passes LC while train apporaching
Train got movement authority
Signal indicates that LC is protected
Driver doesn’t see warning light
Driver doesn’t notice train
LC claims to be protected
Drives towards the sun
Sun is low

Fig.6. Description of holes in the safety layers by means of WBA

It would be illusory to believe that we could find every gap and every safety layer just by looking at accidents. Accident analysis tells us about safety layers that have already failed in the past only. Safety layers that have never been broken don’t appear in this approach. We need to complete the results from accident analysis with a system analysis.

3.2. New Safety Layers and Recombination

Absolute safety is impossible to reach. Every concept, every layer will have gaps. Instead of spending a lot of effort, time and money on the attempt to close the existing gaps it can be much better to develop a new safety layer that itself has a lot of gaps, but elsewhere. The required level of safety is reached by combination of those layers.

New layers like these can be added to MoSiS. The more different layers we know the more comprehensive the portfolio of safety layers will become. A good portfolio offers a wide range of possibilities: New safety layers can be added to an existing safety concept in order to improve safety. Safety concepts can be optimised by exchanging some of the safety layers already in place with others that are more (cost) effective. This will be a great benefit especially for low-density railway lines. For completely new systems one can choose an optimal combination of safety layers right from the beginning. The better this portfolio the easier it will become to construct custom-built solutions by selecting the appropriate safety layers from the collection.

3.3. Expected Benefit and Problems

MoSiS is expected to provide the following benefits:

- Identification of flaws in the railway system
- Modelling of safety layers
- Possibility to add, to exchange and to recombine safety layers
- Possibility to optimise the safety concept in order to reduce costs
- Possibility to improve safety

Though the concept of safety layers will give us deep insight into the railway system and offers great possibilities it cannot offer perfect safety. Safety layers might be influenced from outside the system or simply wear out and thereby get new gaps. Common cause failures can weaken several safety layers at the same time or open new gaps all in a row.

There is evidence that the reliability of a safety layer depends on the protection by other layers in front of it. This effect is often observed in modes of degraded operation: A staff member, reliable during normal operation, can become overloaded when technical assistance is lost.

4. Perspective

In the full-scale state MoSiS will include the functions of its safety layers. It will be possible to compare existing and new safety concepts for the railway system. New cost-efficient safety systems, e. g. for level crossings, can be developed and compared with existing solutions. The advantage of MoSiS is the ability to show on a qualitative level, whether a new solution will eliminate only a specific safety flaw or improve the overall safety level. It can be used as a kind of “library” of safety layers as well as a kind of validation environment.

Used in the right way MoSiS can help to use new and existing safety layers in an efficient way or at least to identify precisely the required characteristics of a new safety layer.

5. Conclusion

The railway system is one of the safest transport systems we have. It usually takes more than one failure to cause an accident. Nevertheless we should improve the safety of the railway system where it is possible, reasonable and affordable. A systematic accident analysis is an adequate starting point for this task. Structured analysis methods like WBA help us finding causal factors of accidents instead of the culprit. Causal factors of accidents are flaws in the safety of a system. They lead us to gaps in safety layers and from there to the safety layers themselves which form the model of safety layers in the railway system (MoSiS). MoSiS reflects the fact that we usually have more than one causal factor of an accident: Before it comes to an accident several safety layers need to break.

The development of MoSiS starts with a subsystem (like a level crossing) and from there the model will be expanded until it covers the whole railway system. The main benefits of the model of safety layers are new possibilities for improving safety and reducing costs.

6. References

1. J. Braband: Risikoanalysen in der Eisenbahn-Automatisierung, Siemens AG, Eurailpress, Darmstadt 2005
2. D. Ellinghaus, J. Steinbrecher: Das Kreuz mit dem Andreaskreuz, Continental AG, Köln/Hannover 2006
3. EN 50129 Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling, 2003
4. S. Arnold et al.: Software Patent: Method for exchanging data between application processes in a secure computer network, EPO, 1999, http://gauss.ffii.org/patentview/EP913759
5. J. Reason: Human error: models and management, BMJ 2000, 320:768-770
6. P. B. Ladkin: A Quick Introduction to Why-Because Analysis, 1999, http://www.rvs.uni-bielefeld.de/research/WBA/
7. S. Pasi: Rail transport accidents in the European Union in 2004-2005, Statistics in focus, Transport, 34/2007, Eurostat