Tool-based Safety Analysis of Operational Rules

Katrin Hartwig[1], Georg Mandelka[2]

Summary: Operational rules are important for the safe operation of railway systems. By analysis of the operational rules and the identification of possibilities to support the staff in its task or even replace the staff by a more reliable electronic system the safety of railway operation can be increased and the costs for the various functions of the railway system can be optimized.

1. Background

Since 2005 the Institute of Transportation Systems at DLR develops a software tool for the examination of technical systems, such as railway vehicles, with regard to the relation to safety of their elements. The tool ist based on a method for safety analysis developed at the DLR (see [1]). The aim of the examination is to identify safety-related sub-systems and to describe the effects of errors in the system, i.e. if a certain error can lead to a dangerous situation. The documentation of the results of the examination can be included in the system documentation which is to submitted to the certification authority. The system supplier can use the results to decide which sub-systems need to be designed in a way that they fulfill the requirements of a certain Safety Integrity Levels.

2. Consideration of safety

The starting point of the analysis of a railway vehicle is the output of the system, i.e. the actions performed which influence the environment, e.g. acceleration, braking or signalling. The tool helps to identify the safety-related signals generated by the various subsystems or components. Knowing the critical paths of information transmission, actions can be taken to reduce error-proneness. It can be analysed to what extent the safety will improve when implementing appropriate products, such as signal relays, or adding redundant or fall-back elements or when changing the related safety levels.

[1] German Aerospace Center, Institute of Transportation Systems, Lilienthalplatz 7, 38108 Braunschweig, Germany, tel.: +49-531-295-3467, fax: +49-531-295-3402, katrin.hartwig@dlr.de

[2] Bombardier Transportation, Rail Control Solutions, Neustadter Str. 62, 68309 Mannheim, Germany, tel.: +49 621 7001-0540, fax: +49 621 7001-0505, georg.mandelka@de.transport.bombardier.com

2. Analysis of operational rules

However, a system does not only consist of hardware and software components and their interaction, but also, if not essentially, it consists of rules for operation and the staff operating the system. Therefore, it appears necessary to examine the operational rules as well.

A first approach to the analysis of operational rules shows, that it is possible to represent rules in a form that comprises all necessary information needed by the tool to perform the analysis.

For the validation of this approach a set of rules has been used which seemed simple enough to assess the results of the analysis by hand, and complex enough to test the applicability of the tool for such a purpose. The rules of Deutsche Bahn for the telephone block (Zugmeldeverfahren) as described in [2]. The rules contain instructions e.g. on how to act when a train shall run from one station to another both for the movements inspector of the sending station and for the movements inspector of the receiving station. The instructions describe what has to be checked, what has to be sain and written down to offer a train to the next station and to accept a train an offert train.

For the validation of the approach to analyse operational rules with the tool developed the rules have been transformed into an activity diagramm as shown in Fig.1.

Fig.1. Activity diagramm for phone block operation

Examples for activities identified in the instructions are:

- Find out time for next departure;
- Find out current time;
- Find out train number and next train reporting point;
- Train report – offer;
- Entry in train record book;
- ...

From the activity diagramm the functions and the information flow have been derived. These are:

At the offering train reporting point

- To offer a train;
- To give notice of departure;
- To prepare and observe train departure;
- To receive confirmation of train arrival.

At the accepting train reporting point

- To accept a train;
- To receive notice of departure;
- To prepare and observe train arrival;
- To give confirmation of train arrival.

The train report book, as a kind of data storage, is a function on both train reporting points.

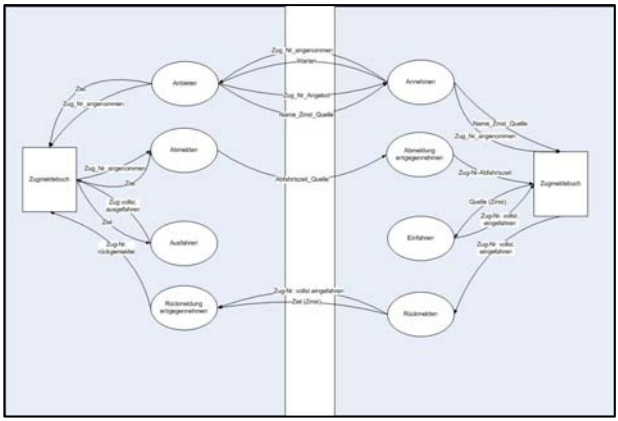

Fig.2. Activity diagramm for phone block operation

The data exchanged between the funtions contain information about the offer of the train, the train number, acceptance of train, departure of train, time of departure and so on.

Having identified the funktions and information flow between the functions the next step contains the identification of the sub-functions, i.e. the single steps and decision to be made. These can be documented by means of a sequence of operation diagram, as shown in figure [Fig.3]

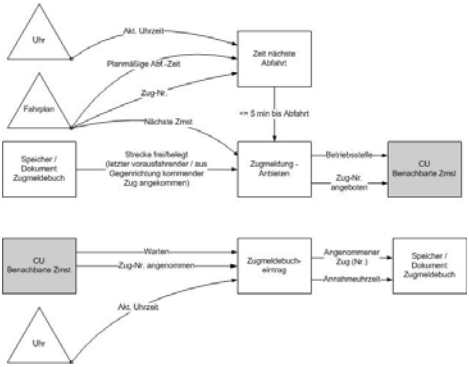

Fig.3. Sequence of operation diagram

In this diagramm also the sensors and actuators appear. Sensors in this sense are the watch, the timetable, the window to look through/the eyes of the signaller (to see if the train is complete / in standstill) and the sensors to detect the position of signals and points. Actuators are the signals, the points, and the train, i.e. all things that have an effect to the environment.

The data contained in the sequence diagramm can be fed into the tool for the safety analysis. For this purpose it is necessary to identify the links of information in each sub-funktion, i.e. link the input and output information of each subfunction, as one sub-function can generate more than only one output information.

If a failure in one of the actions of the system (e.g. acceleration, closing doors, switching light off) can lead to dangerous situations, the effects must be documented in the tool and a Safety Level must be given to the action.

During the analysis the tool allocates the Safety Level of the actions performed by the system to all information that is processed to

trigger each action of the system. However, it is possible to unlink the chain of information flow if an information is not used in a sefaty-related way. After the analysis of the data the tool generates lists of information flows from each measurement/sensor to the actuators/actions using the sensor information, and the information flows from the measurements to each action. Hence it is possible to see which measurement is linked with which action.

In the example used for the validation of the applicatbility of the tool and the method applied the result of the analysis showed that an important information flow is from the train report book the information on track occupancy to the signaller at the offering train reporting point and the offer of train to the signaller at the accepting train reporting point. The train must not be offered if the track is occupied. In case the first signaller makes a mistake and offers a train while the track is occupied the signaller at the accepting train reporting point has the chance to detect this mistake and prevent that the train is sent into the occupied track. However, in the instruction it is only mentioned that a train can only be accepted if there is no conflict. But contrary to the instructions for the offering train reporting point, which say that a train can only be offered if the last previous train has reached the next block post or the last train in the oppsite direction has arrived at the own train reporting point, the instructions for the accepting train reporting point do not state this clear rule (i.e. accept only when track is nbot occupied).

3. Conclusions

The output of the tool presents the components and information paths which are relevant to the safe operation of the system and where human involvement bears the risk of hazards. With this result it is possible to identify ways to support the staff in its task or even replace the staff by a more reliable electronic system. With those actions the system gets not only safer, but staff can be relieved from safety-related tasks or even deployed in other services.

Beside this, system integrators are also interested in the analysis of further characteristics of their systems in order to optimise the design. As the tool works with a data base it is possible to assign a number of attributes to the various components of a system, such as costs or availability. Further interesting attributes could be the kind of processing units of the various functions, e.g. computer, relay or human being, and the communication

channel between the functions of a system, e.g. LAN, GSM-R or public networks.

4. References

1. Hartwig, Katrin; Grimm, Matthias; Meyer zu Hörste, Michael (2006): Tool for the Allocation of Safety Integrity Levels. In: Symposium Proceedings, 9th International Level Crossing Safety and Trespass Prevention Symposium, Montréal (CND), 2006-09-10 - 2006-09-14

2. DB Netz AG: Konzernrichtlinie 408 – Züge fahren und rangieren, Frakfurt am Main 28.04.2004