18th Annual International Railway Safety Conference
Denver, Colorado, October 5-10, 2008

Safety Analysis of Operational Rules and Specifications

Authors: Dipl.-Ing. Katrin Hartwig, Dr.-Ing. Michael Meyer zu Hörste (German Aerospace Center, Institute of Transportation Systems, Braunschweig, Germany)

Abstract

Since 2005 the Institute of Transportation Systems at DLR develops a method and a software tool for the examination of distributed technical systems, such as railway vehicles, with regard to the relation to safety of their elements.

The starting point of the analysis is the output of the system, i.e. the actions performed which influence the environment, e.g. acceleration, braking or signaling. 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 analyzed 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.

To bring the European Railways closer together and enable safe cross country rail traffic the European Train Control System (ETCS) has been developed as one technical component of the European Rail Traffic Management system (ERTMS). To run the ERTMS/ETCS in several countries, not only a common technology but also harmonized operational rules are needed. Hence, the national operational rules must be modified.

After the modification of the operational rules it has to be verified that the rules allow safe rail traffic, are not in conflict with the existing rules and have been formulated unambiguously.

As operational rules consist of instructions how to act, they are comparable to software and even to hardware logic, while the staff acting to the rules can be seen as systems performing actions and communication to each other, just like technical systems do. Therefore it seems plausible and possible to treat operational rules like software and hardware logic and use the same methods and tools for the analysis.

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.

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.

The knowledge about safety related and non-safety related tasks and information paths allows also using the most appropriate technology in system design and optimizing safety and life cycle costs. Tool and method allow also allocating various attributes to the elements. Therefore the systems information paths can also be analyzed regarding the characteristic of these paths, e.g. which kind of processors are involved in the generation of information or actions.

The paper discusses the principles of the software tool developed by DLR, its application and potential future developments.

Introduction

Railways are an important means of transport for passengers and goods all over the world. They link towns and also countries. But this link is not without complications. As the railways in the different countries have developed independently from each other the systems deployed and the rules for operation differ; in many cases they are not compatible – both systems and rules – and it can be dangerous (or just impossible) to drive a rail vehicle in another country without adapting the systems and rules of that country.

Since railways normally do not drive "on sight", as they are faster than their braking distance would allow, complex systems and rules are necessary to ensure a safe operation. In Europe there are many different train control systems applied in the different countries. To bring the European Railways closer together and enable safe cross country rail traffic the European Train Control System (ETCS) has been developed as one technical component of the European Rail Traffic Management system (ERTMS).

At the Institute of Transportation Systems at the German Aerospace Centre a method has been developed and is currently being extended to perform system-analyses regarding the relevance for safety of sub-systems and components. The method has been implemented in a software tool and for a feasibility study used for the analysis of several small systems.

The following chapters discuss the analysis method and the tool, and the results of the analyses performed will be presented.

Method and tool

For the development of the analysis method one question was in the front of interests: "Which sub-systems and components of a complex control system are safety-related?"

By the time the method was developed two more questions appeared: "Is it possible to analyze operational rules with this method?" and "Where is the human involved in safety-related tasks?"

And finally the question "Is it possible to develop safe, interoperable systems with the ETCS specifications provided?" came up.

For the development of the analysis method two challenges can be derived from these questions:

- find a possibility to assess the possible faults in a system regarding their effects to the system's environment;
- find a way to derive information flows functions and the involved systems from verbal descriptions of rules, such as operational rules, e.g. of Deutsche Bahn, and ETCS specifications of procedures.

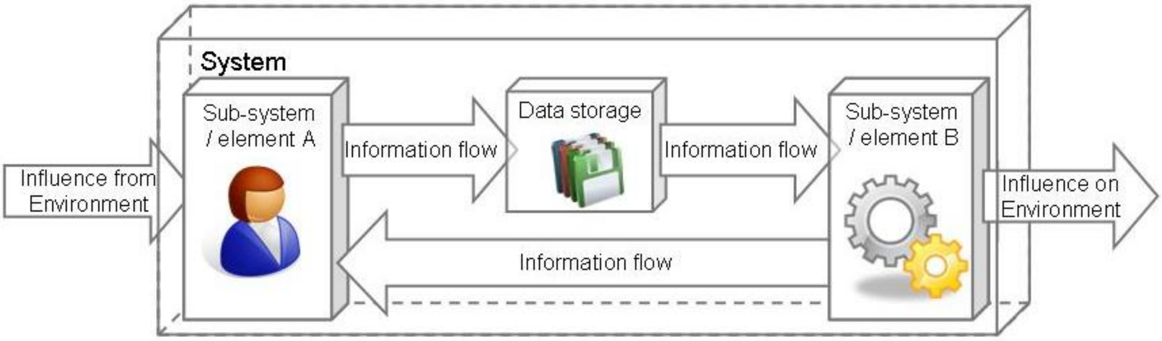

Fig. 1: Elements of a control system

Approach

System analysis[1]

For the assessment of possible faults in a system regarding their safety implication following assumptions have been made

- a safety related action is an action whose false performance can lead to a hazardous situation, while false performance can be too early, too late, too much, too few etc.
- a system / sub-system / component, performing a safety-related action, is safety-related
- a signal that influences safety-critical actions in a safety-related way is safety-related
- a sub-system generating safety-related signals is safety-related

This means that the relevance to safety is handed down from the safety-related action through the components generating the action and the signals influencing/triggering the action to the sub-systems and components generating the safety-related signals.

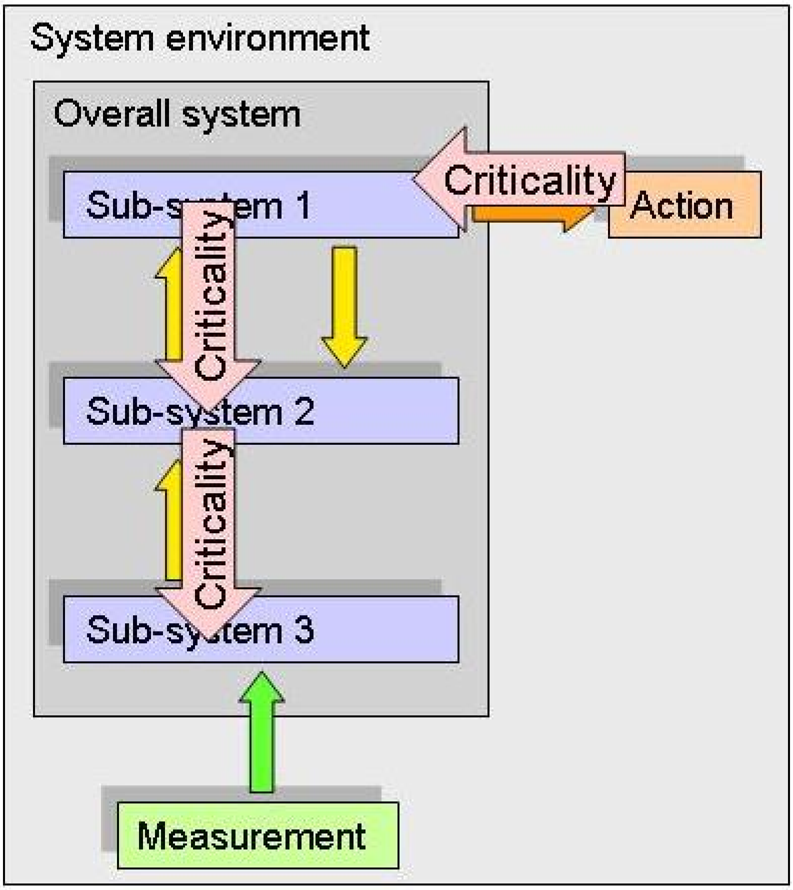

Fig. 2: hand down of criticality

Hence, the starting point of the analysis is the assessment of the criticality of the effects, i.e. the criticality of possible erratic behavior of actuators of the system, e.g. the consequence of brakes not applying with enough force, points moving mistimed (e.g. under a train), doors closing while people are between the door leafs or door leaf and frame, or the light at the St. Andrew’s Cross not flashing while a train is approaching.

[1] Patent pending

The second step is to identify the signals influencing the effects in a safety critical way, while here various situations must be considered. The unexpected opening of doors, for example, while the train is at standstill at a platform is not as dangerous as opening doors while the train is on the free track moving or at standstill at a red signal. Furthermore is the signal to close the doors not as safety-related as the signal from the anti-trap protection.

With the assumptions stated above the result of the analysis is an overview of the safety-related sub-systems of the system considered. With this knowledge it can be decided which sub-systems need to be developed according to safety standards. Beside this, the method also allows to analyze the system regarding other parameters, e.g. regarding the costs of a certain function by summing up the costs of the sub-systems involved in the realization of this function.

For this analysis it is necessary to know the sub-systems the overall system consists of and the functionality of the sub-systems, i.e. the logic of data processing in the sub-systems, to follow the information flows from the effects to the sensors through the system.

Transformation from written rule to information flow and functionality

To consider also the human and his tasks, e.g. a driver, within the analysis it is necessary to consider him as sub-system receiving and generating information. But is this feasible? Fig. 3 shows at a simple example for the transform from technical system to a written rule and vice versa.

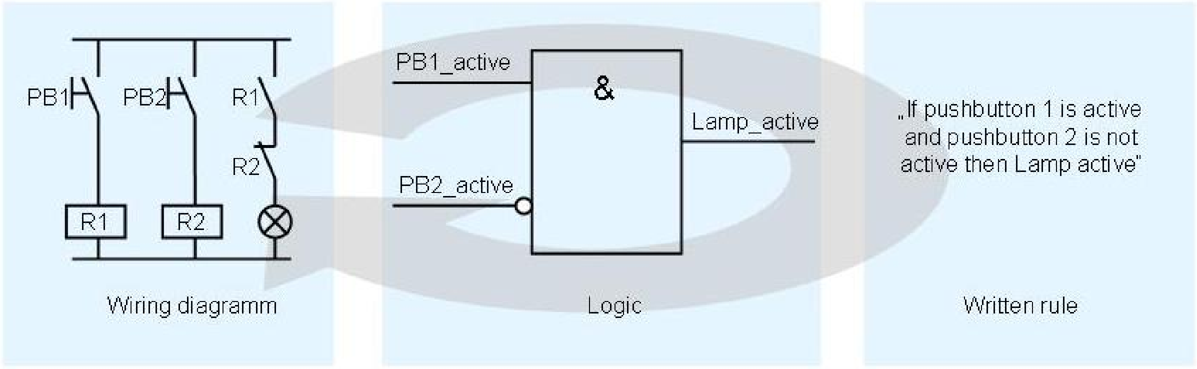

Fig. 3: Transformation of rules

If the functionality of the system is provided only verbally, and not by means of wiring diagrams and the graphical presentation of the software logic, the information flows and involved sub-systems / components have to be derived from the written rules. This can be rules for the human involved, e.g. operational rules, or specifications how the system should react, e.g. in the ETCS specifications.

For the transformation of a written rule into a set of signals and functionalities it is necessary to identify

- the involved sub-systems,
- the functions to be realized,
- the information exchanged between the sub-systems, and
- the conditions for the generation of information.

The results of this analysis can be documented by means of a table that contains for each signal its source and its destinations, the conditions for its generation, and, as far as possible, the way of data transmission. The latter is useful for the check if the transmission system inherits safety relevance from the transmitted signal.

For the analysis is has to be decided for which level of the system the knowledge of the relevance for safety is desired, e.g. ETCS overall system, only EVS[2], or for sub-system level only or also for the functional level. This level influences the depth of the system analysis.

If the signals generated by the various sub-systems are documented in a chronological order, it can be checked if all conditions necessary to generate a signal have been fulfilled already, or if signals that are a condition for a certain operation have not been generated yet. (see example of ETCS specification).

By means of a sequence of operation diagram the result of the transformation can be depicted. By means of the analysis method developed the operational rules for the signalers in the telephone block operation have been analyzed. The analysis showed that, although this procedure is in use since a very long time, there is still room for improvement.

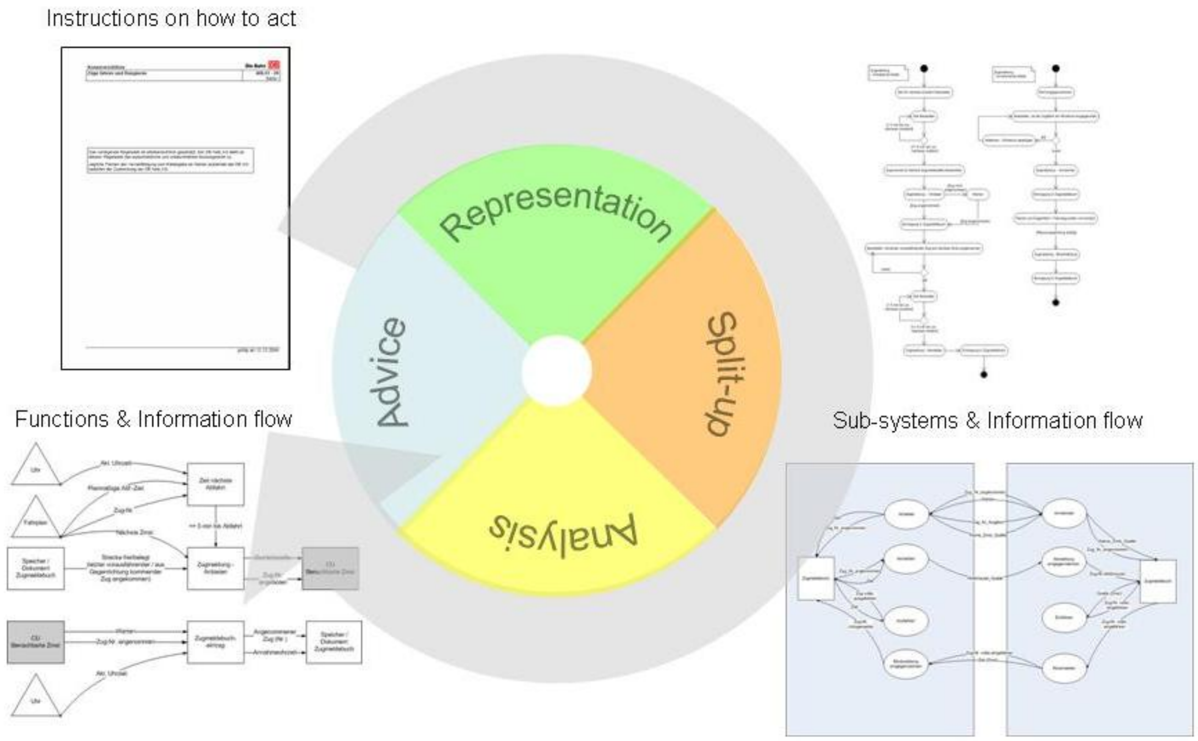
Instructions on how to act
Representation
Split-up
Analysis
Advice
Functions & Information flow
Sub-systems & Information flow

Fig. 4: Analysis of operational rules

The tool highlighted the information on the track occupancy as safety-related – as could be expected. A further analysis of the rules revealed, that the information about the track occupancy is stored twice (in the train report books in offering and accepting train reporting point) but according to the written rule it has to be checked only once (at the offering train reporting point just before a train is offered). Hence, this is a single point of failure, while the risk from this source of failure can be easily reduced if at the accepting train reporting point the occupancy of the track is checked as well and the train only accepted, if the track is free from vehicles. So far, for the signaler at the accepting post the rule is to accept the train “when no conflict exists”, while it is not written, which conflicts that can be.

During the transformation of the rules it should be checked if the rules are formulated in a way that it can be checked against compliance, i.e. they are unambiguously and do not

[2] EVS: European Vital Computer

contain fuzzy formulations. Furthermore they must use clearly defined, unambiguously input and output information.

The method for the system analysis has been implemented in a software tool and tested on various systems. To have the possibility to check the results manually only small systems, which are sub-systems of rail vehicles or fragments of operational rules, have been analyzed.

For the data input the tool provides two different possibilities – to enter the data by hand via the keyboard and to read the data from files. The data are stored in a database and can also be exported into files. Interfaces to development tools are planned but not realized yet. Before the analysis can be started, the effects have to be assessed and a value must be allocated to the effects. If the analysis has been started the tool checks, if all effects have been assessed, all signals are generated and have at least one target. If these conditions are fulfilled the value allocated to the effects is being allocated from each effect to the signals influencing the effect, then to the computing units generating the signals and so on. If one signal influences several effects and would get different values for its relevance to safety, then the higher value is authoritative. The tool also offers the possibility to stop the process of heredity in the processing units for each incoming signal.

Potential development

The application of the tool revealed the potential of a computer-supported analysis and the possibilities beyond the analysis for safety purposes. Once the structure of a system is stored in the database many more characteristics of the system can be analyzed, as long as the relevant parameters are available for all system components. So it is possible to analyze which data transmission modes are safety-related, where the human is involved, what a certain function costs, if all safety-related components can bear this responsibility etc. It might even be possible to support the generation of manuals for the system.

To tap the full potential of the tool currently further investigations in the possibilities to use the tools are being carried out and the possibilities to apply the tool are being tested at the institute of Transportation systems.

Analysis of ETCS specifications

For the safe operation of trains in Europe the ERTMS/ETCS has been developed. In a long process a group of system suppliers[3] have developed the system specification for ETCS. These specifications form the basis for the development of ETCS equipment, such as the European Vital Computer or Radio Block Centres. These specifications are binding for the development of train control systems (see DIRECTIVE 2008/57/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 June 2008 on the interoperability of the rail system within the Community, Official Journal of the European Union L 191, 18/07/2008 P. 0001 - 0045).

But are the systems developed according to the specifications safe and interoperable?

To answer this question two procedures have been analyzed: Override EoA[4] and Train Reversing (see [subset-026-5] version2.3.0, chapters 5.8 and 5.13). In the System Requirements Specification (SRS) for Procedures the requirements are noted in chronological order for each procedure. They describe the tasks of the entities (on-board

[3] UNISIG companies (ALSTOM, ANSALDO SIGNAL, BOMBARDIER, INVENSYS RAIL and SIEMENS, THALES)
[4] EoA: End of (Movement) Authority

equipment, trackside equipment and driver)[5] and the conditions under which the tasks have to be performed. These are the data that are used by the method and tool described above.

For the analysis the relevant systems and signals have been listed in chronological order as given in the SRS, together with the path of the signals from the generating to the receiving system, including the interfaces to be used, the kind of data transmission (hardware/wireless/software/verbally), and the conditions for the start of data transmission.

This first step of the analysis showed that, at least for these two procedures, the specifications leave room for interpretation and also misinterpretation. This can hinder the interoperability of the components developed under the application of the specifications. Following the findings from the example of the “Re-activation of the transition to train trip” in the “Procedure override EoA” shall be described. The override procedure can be used to prevent a forced brake at the end of movement authority in the modes “Staff Responsible” (SR) and “Shunting”(SH). The procedure is triggered by selection of override by the driver. In the introduction of this procedure is said: “... the procedure allows to avoid a train trip[6] when passing a balise group transmitting “stop in SR mode” or “stop in SH mode” information. But the section “Re-activation of the transition to train trip” lists as a condition for the end of the inhibition of the transition to Trip mode “the train passes a Balise group giving “stop in SR” or “Stop in SH” information. Obviously it is meant to end the inhibition of the transition to trip mode if a Balise group transmitting “stop in SR/SH” is passed by the train to avoid the passing of a second Balise group sending “stop in SR/SH”. However, the description of the procedure is not unambiguous and could be misinterpreted and lead to increased development effort.

The analysis of the procedure for “Train reversing” showed that information provided in other documents is necessary to understand the specification, while no reference to the relevant document is given, i.e. there is a gap in the specification that could lead to equipment not being interoperable with equipment from other system suppliers.

While in sentence 5.13.1.2 is written “The area where initiation of reversing shall be possible shall be announced to the ERTMS/ETCS on-board equipment, with a message, indicating its start and end and permitted distance to run and maximum speed, after switching to RV[7] mode.” In sentence 5.13.1.5 is written “If the driver confirms, the on-board equipment shall switch to RV mode”. Having in mind that the procedures are described in a chronological order, these two sentences leave room for (mis-)interpretation. The reason for this is that the information that the announcement for the RV area is transmitted by Balises at the beginning of this area is missing here. This information is given in another document but a reference to this document is not provided in the specification of Train Reversing.

These two examples show the necessity of an independent analysis of system specifications, especially for safety-critical systems such as ETCS. On the one hand ambiguous specifications can lead to the design of not interoperable safety-critical systems. In the better case the missing interoperability leads to an obstruction of the railway operation, in the worse case it leads to a dangerous situation. On the other hand it can lead to increased development costs for these systems when the interoperability problems are discovered late in the development process.

It cannot be expected that people involved in the system design and development know all documents of the ETCS specification by heart, recognize gaps in the descriptions and know where to find the missing information. It is only human to fill the gaps by supposed knowledge, not recognizing that important information is missing. As not only those companies that where involved in the specification of ERTMS/ETCS are developing ETCS system components but also companies that are new in the field of ETCS it is even more important to describe the functions clearly and completely.

[5] Correspond in method with „sub-systems”
[6] Penalty brake
[7] RV: Reversing

Summary and Future development

ETCS System Requirements Specifications and Operational Rules allow safe rail traffic. However, they must take into consideration the infrastructure and must not be in conflict with the existing (national) rules, e.g. it is not allowed to share responsibility. The rules and specifications must be formulated unambiguously and completely where needed. Parts, where freedom to choose different ways is given must be marked accordingly. All relevant references must be given to avoid guessing the circumstances of the applicability of rules and specifications and the right context. The chronology in the specification of messages must be clear and interfaces must be described clearly. Also the different languages of the people involved in system development, and hence the difficulties in translation, must be taken into consideration during the formulation of the rules and specifications.

The system developers must ensure that safety-related components are developed in an appropriate way and no component has more responsibility than it can bear. This is also valid for the human. Hence, an analysis of systems is necessary that shows where faults can lead to dangerous situations. The method and tool described above can be one building block in this analysis. For humans this analysis will be the task analysis, which can help to find the safety-critical tasks.

At the Institute of Transportation Systems at the German Aerospace Center the method will be further developed and implemented in a software tool, and further fields of the application of the method will be investigated. As the requirements of the certifying bodies regarding the differentiation of Safety Integrity Levels of the sub-systems increase, also the investigation and implementation of the allocation of SILs to redundant systems is planned.

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, Frankfurt am Main 28.04.2004 (in German)

[3] Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS) EN 50126

[4] Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems, EN 50128

[5] Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling, EN 50129

[6] UNISIG ETMS/ETCS subset 026: ETCS System Requirements Specifications (SRS), Issue 2.3.0, 2008