Preprint version of Harms-Ringdahl L. and Kecklund, L. *Safety Functions in Railways - a Structural Analysis of Safety Rules*. In Spitzer, U., Schmocker, U., and Dang, V.N. (eds.) *Probabilistic Safety Assessment and Management.* Springer (pp 2751 –2757) 2004. Proceedings of ESREL 2004.

# Safety Functions in Railways - a Structural Analysis of Safety Rules

*Lars Harms-Ringdah*l [1]
Royal Institute of Technology, Stockholm, and
Institute for Risk Management and Safety Analysis,
Stockholm, Sweden

*Lena Kecklund* [2]
MTO Psychology,
Huddinge, Sweden

## Abstract

There are several ways to describe and structure safety rules for railways, and a few examples are given in the report. A tentative holistic framework for describing safety features in relation to safety rules is presented. The approach has been applied on rules needed to regulate the communication between different railway organisations and other parties.

# 1 Introduction

Rules for safety control of railways have a long history and have been developed over several years. An important driving force for safety rules has been the operating experiences – new rules has been devised as a result of railway accidents, incidents and problems. The introduction of more actors in the railway field adds to the complexity by the increasing number of interfaces between people and organisations.

In general, the observed safety problems have been solved by adding more barriers and rules to an existing structure, which often increases complexity. The number of safety rules has therefore increased, while the rule system structure has been less developed. Problems have occurred with usability as well as in the communication of the safety content of the rules to train drivers and dispatchers.

The aim of this study was to look at different ways of describing and structuring safety rules for railways. Furthermore, the intention was to develop a tentative holistic framework for describing safety features in relation to safety rules in the railway area. One potential use of this analysis was to provide background information for the ongoing revision of the railway safety rules in Sweden.

The approach in the study has been to direct interest towards human and organisational factors, as contrasted with more formal rule oriented thinking. In the rule revision work, there had been ideas for testing the possibilities of working with functional demands instead of detailed prescriptions. Accordingly, the concept of safety functions was found to be a potential framework to apply in the analysis.

[1] e-mail LHR@irisk.se
[2] e-mail Lena.Kecklund@mtop.nu

# 2 Some Aspects on Rule Systems

## 2.1 European examples

A quick survey was made of some approaches to structuring rules in a few European countries, e.g. Germany, Sweden and the United Kingdom [1]. A common approach is to base the structure on different types of traffic and activities, such as passenger traffic, shunting, and maintenance. Also, the different groups of staff concerned are used for structuring. This is more explicit in the German system [2] than in the Swedish [3] system.

The United Kingdom structure [4, 5] for the rule books is based on general safety responsibilities, train operation in normal conditions and incidents as well as infrastructure activities. In addition a "Top controls framework" has been developed to include the organisational level and the safety rules as a part of the safety management system. The "Top controls framework" classification scheme sets out three broad areas for control:

- Controls for management and operations of railway activities
- Controls for physical assets
- Controls for interactions between physical assets

## 2.2 A User perspective

*General*

The gradual development of the safety rule system and the increased automation has in some cases given better support to the users, but it has also made the system more difficult to use. One explanation of the problems is that the users have been left with an arbitrary collection of tasks which cannot be solved by technical means. Also, system complexity has increased as a result of the different technical systems being used, and of the increased number of operators involved. This increased complexity puts great demands on the operators´ mental capacity (memory, attention and vigilance), and creates higher workload. Some examples are presented below.

*Dispatchers*

A study of train dispatchers' work [6] showed that many concurrent work tasks had to be performed on different signalling systems. This created a high mental (short-term memory) workload. Also, forgetting subtasks or performing them in the wrong sequence occurred quite frequently and was most probably related to the high workload. However, the dispatchers were quite successful in coping with these high work demands by use of extra effort

*Drivers*

The rules are probably more difficult to grasp and follow when complexity increases, if they are not supported by a well developed structure. One example can be taken from a questionnaire to train drivers [7]. This revealed that many drivers considered the operational safety rules to be too extensive, making them almost incomprehensible. Also, many drivers reported problems with the understanding and design of some functions in the Automatic Train Control system (ATC), in particular the supervision of release speed. The results of the questionnaire study showed that many drivers did not have a complete understanding of how the ATC system, signals and rulebook interact. The conclusion was that some drivers held a number of potentially dangerous misconceptions.

*Management*
The complexity and the involvement of several organisations might create problems also for managers at different levels. Especially with several organisations involved in operations, responsibility issues are complex to handle, which is illustrated by example in Section 3.4. Also, for managers to provide background information to “sharp end” users is essential, because if a user does not understand a rule he is less motivated to apply it.

# 3 Structuring of Rules

## 3.1 A Cube Model

One way of describing the types of parameters related to a bottom-up perspective can be represented by a "Cube Model". It was proposed by Pålsson [8] as a way to illustrate the common thinking. The "safety space" is at first divided in three "dimensions".

1. Type of traffic and activity, e.g. normal train running and shunting. (Between 4 - 8 examples of categories can be anticipated.)
2. Type of employee task, e.g. train driving, dispatching (5-10 categories).
3. Type of railway system, e.g. Track Circuit Block System, Telephone Block System (3-8).

These three parameters can be described as a cube in three dimensions, containing a number of sub-blocks. This can be illustrated as a "cube" in five dimensions as shown in Figure 1. Each of these can be divided in further dimensions, which can be:

4. Degree of normality, which can be normal, planned deviations and irregular situations (3 categories).
5. Stage of activity, e.g. preparation and planning, starting conditions, operations, and termination (4 categories).

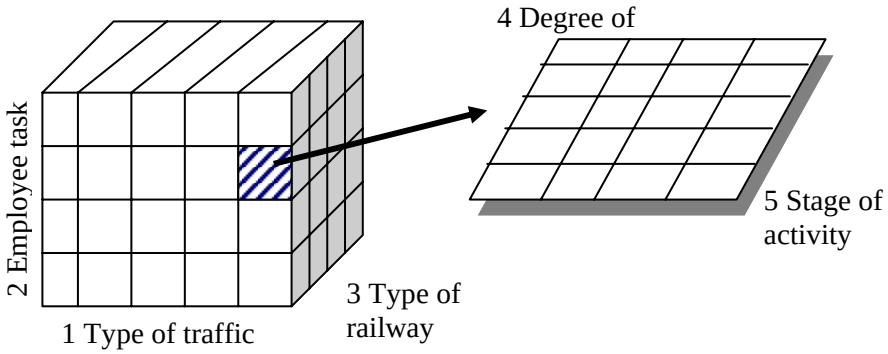


*Figure 1. Parameters in railway safety illustrated as a super cube.*

After each parameter in the list above, the numbers indicate how many different "values" the parameter may take. These values can be used to estimate the number of elements in the model.

The basic cube can have between 60 (4 x 5 x 3) and 640 (8 x 10 x 8) sub-blocks. Each sub-block can have 12 (3 x 3) elements. Totally, the number of elements can fall somewhere between 700 and 7 700. The number of elements is large, but several elements will be irrelevant (empty). Each element can be seen as a state or situation, for which safety considerations are needed.

### 3.2 Safety Functions

One approach was to focus on the functions needed to obtain a state of safety and the requirements needed for the functions to obtain this state. One keyword was "functional demands", which implied a fairly abstract description of how a certain safety feature could be achieved. These ideas come close the general concept of safety functions, which were applied on this case. A general definition of safety function has been proposed in [9]. The definition is:

> *"A safety function is a technical, organisational or combined function that can reduce the probability and/or consequences of accidents and other unwanted events in a system."*

Human actions are here regarded as part of the organisational component. Safety function is a broad concept and, in specific applications, requires more concrete characterisation. This can be achieved using a set of "parameters" to characterize important features of the safety function. For example, the same reference proposes the following: a) Level of abstraction, b) System level, c) Type of safety function, d) Type of object.

The safety function concept was adapted to the railway system and the rule writing procedure [10]. A logical chain from abstract to more concrete safety functions is illustrated in Figure 2, which illustrates the following components:

- In the system, a number of hazards should be controlled.
- The Safety Functions on a general level shall reduce probability and/or consequences of accidents.
- To obtain this, a number of different "functional resources" (technique, organisation, people) are needed.
- Some of these resources can be put in operation and formalised as a set of safety rules.
- Finally, there are technical solutions and organisational actions, which will transform the demands to a practical reality.

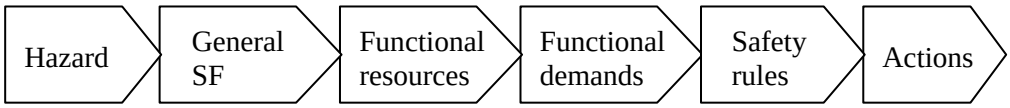


*Figure 2. Model of safety functions adapted to railway rules, going from an abstract to a more concrete function.*

This chain has many similarities with the model from UK Railway Safety [4] which includes the steps: Hazards ⇨ Controls ⇨ Measures ⇨ Rules & Standards.

### 3.3 A general structure

There are numerous ways of describing the railway safety system. In this exercise, three main parameters were selected, which are related to dependence, solution, and system state.

1) *Dependence*. This concerns if the safety function (or action) is shared between two or more organisations or if it is internal to one organisation. Two alternatives:
   a) A system used by several organisations requires an organised cooperation.
   b) An independent system is probably easier to control.
2) *Solution* of the safety function, which can be divided in:
   a) Technical solution
   b) Combination of technical and administrative solution, e.g. maintenance of communication equipment
   c) Administrative solution, e.g. rule about a specific action

3) The *system state* can be classified in:
   a) Normal state, working as planned, usually stable over time.
   b) Planned deviation, which can be between hours to e.g. a month.
   c) Disturbance, unplanned, occurring quickly

One ground for the approach was to test a top-down approach. It was also considered as a fairly simple way of comprising all types of situations for which safety actions were needed. A combination of the parameters and variables gives a matrix with 18 basic blocks.

In a specialists group, the matrix boxes were filled in with more specific cases of safety features. Between three to eight subheadings might be relevant in each box, resulting in about 100 subheadings.

### 3.4 Example of safety functions in communications

As an example, the subheading "Communications between actors" was chosen (with a focus on the parameters 1a, 2c, and 3a). This theme is interesting as communication relates to most types of situations with several actors involved.

The subheading was analysed and divided into six basic elements, as shown in Table 1. This division is not unique and can be done in many ways. Based on this structure, safety functions on a more detailed level were identified.

This was done along two routes in parallel as an iterative process. One way was to take the safety function, and then go from an abstract to a more concrete function or from a high system level to a lower one. This is in accordance with principles described in section 3.2 above.

| Safety function | Aim |
|---|---|
| ***Communication between actors*** | Avoid risks due to errors in communication between actors in different organisations |
| 1) General procedures for communication | Coordination between organisations |
| 2) Communication across legislative boarders | Avoid risk due to administrative problems |
| 3) Terminology and methods | Give standardisation and good reliability regarding signals, vocabulary etc |
| 4) General conventions | Define good praxis and procedures |
| 5) Special conventions | Define situations when communication is crucial, and how to handle this. |
| 6) Responsibilities and decisions | Improve reliability by clarifying responsibilities in communication. |

*Table 1. Example of structuring "Communication between actors" seen as a Safety Function.*

The other way was to focus on requirements and problems which needed solutions. A number of problems were identified through a coarse deviation analysis [9] of scenarios related to communication. This procedure resulted in the identification of around 60 safety functions related to communication.

# 4 Discussion and conclusions

There are obviously many ways of structuring and describing safety features and safety rules. There are top-down as well bottom-up approaches. In this paper, focus has been on applying the concept of safety functions to analyse a control structure.

The exercise presented here shows that the concept of safety functions can work, and that it gives a clear top-down approach. A general experience was that the concept was easily understood and accepted in the practically oriented group, in which these structuring models were discussed.

One general dilemma within the whole area is the large number of different types of elements, e.g. rules, safety features or safety functions. Consequently, this increases the complexity, which is difficult to handle on most levels, from authorities to train drivers. It indicates the importance of a good structure of rules, and a need of tools for analysing and describing safety control. Top-down approaches might therefore be necessary.

The large number of rules and safety elements is common to several rule systems. A comparison between different approaches can be made. In Section 3.3, the safety function exercise suggested 16 main areas in a matrix format. It was estimated to be around 100 subheadings. This can be compared with the structure proposed by Railway Safety [4]. There you have 16 "top-controls" divided in 103 subheadings. So when comparing the basic headings you end up with similar numbers.

A comparison can also be made on the ideas of structure for communication (in Section 3.4). The European directives for interoperability [11]emphasize communication as an important aspect. The main headings in this area are:

- Safety-related communications between subsystems
- Nature and structure of the messages
- Communication methodology

After trying to apply the concept of safety function on rule structures, some clear advantages can be identified. The first advantage is the emphasis on organisational aspects. Traditionally, rules are often directed only to the sharp end, for example to drivers train and dispatchers. The approach presented in this paper shows a potential for a integration between rules and safety management aspects.

A second potential advantage is that the concept can support functional aspects and efficiency, through a more clear definition of goals.

A third advantage is that this approach provides means for motivating rule users by giving a clear “map” of how the rules relate to the safety management system – and thus it can be easier comprehended. A good structure will probably make it easier for users to develop adequate mental models. Better motivation and comprehension can also contribute to an improved safety culture.

## References

1. Harms-Ringdahl L., Kecklund, L. Strukturer för TRI-projektet. (Structures for the rule book project). Banverket, Borlänge, Sweden, 2001.
2. Züge fahren und Rangieren –Fahrdientvorsschrift (FV), DS/DV 408. Germany.
3. Säkerhetsordning - Trafiksäkerhetsinstruktion (Swedish rule book), BVF 900. Banverket, Borlänge, Sweden, 2001.
4. Railway Safety, Railway Group Standards Unit. Top Controls framework. Railway Safety, UK, Version 1.4. March 2001.
5. Railway Safety, Railway Group Standards Unit. Documentation from a conference, Railway Safety, Heathrow, London, 11th September 2001.

6. Kecklund L. Utvärdering av driftledningscentralen i Hallsberg. Slutrapport. (Evaluation of a train dispatching centre – final report.). Prepared for Banverket by MTO Psychology. MTO Psychology, Stockholm, 2003.
7. Kecklund L. Final report on the TRAIN-project. Risks and proposals for safety enhancing measures in the train driver system. Banverket, Borlänge, Sweden, 2001.
8. Pålsson, U., SJ AB, Sweden. Notes and private communication, 2001.
9. Harms-Ringdahl, L. Safety analysis - Principles and practice in occupational safety (2nd edition). Taylor & Francis, London, 2001.
10. Harms-Ringdahl, L., Hedlund, E., Kecklund, L., Lövgren, M. Struktur för Trafiksäkerhet och Funktionella Krav (Structures for railway safety and functional demands). Banverket, Borlänge, Sweden, 2001
11. European commission. Directive 96/48. Interoperability of trans-European high-speed rail system. Draft Technical Specification for Interoperability, Subsystem ”Operation”, 2001.