Risk apportionment for railway systems using constraint programming

M. Rafrafi & E. M. El Koursi
ESTAS, INRETS, France

Abstract

The apportionment of railway safety targets is a key issue in developing common safety management in the European railway system. In this paper, we develop a generic approach based on the functional railway architecture, to analyse the safety of railway systems for a unified European network and to comply with the Common Safety Targets (CSTs) required by the European railway safety directive. We suggest using constraint programming with the functional railway architecture, developed by the AEIF, to allocate the safety targets to the railway functions.
Keywords: railway safety, common safety targets, risk apportionment, functional analysis, constraint programming.

1 Introduction

The railway system is composed of various subsystems such as energy, infrastructure, control command and signalisation, rolling stock, operation, telematics, etc. These subsystems are performed by various functions, which are implemented by a number of resources and programs. These elements constitute the representative architecture [1] of the rail system.

The interoperability of railway systems requires the clear definition of subsystems and their interaction to allow free movement of trains across Europe and to facilitate the opening of the European railway market. In order to maintain the safety level, a directive was set up by the European Commission (EC) to regulate the European railway system.

European directives impose a division in the chain of the operational and safety responsibilities between the *Infrastructure Manager* (IM) (the person in charge of the maintenance of the rails) [2] and one or more *Railway Undertakings* (RU) [2] (national companies or private operators) [3]. This shared responsibility may

WIT Transactions on Information and Communication, Vol 39, © 2008 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK080481

derive from the goal of the function – that involves both IM and RU – or from the way it is implemented.

Qualitative and quantitative safety targets can be allocated from a bottom-up approach as well as a top-down approach.

The first section of this paper provides the safety and interoperability requirements prescribed by the European directives and gives the risk apportionment strategies. The second section focuses on the approach of functional risk analysis.

2 Context

The reorganization of the European railroads undertaken by the directive 91/440/EC, relating to the development of the community railroads led to the separation of the functions of the infrastructure managers and the railway companies. This process currently continues to support the passage of the system of national rail networks towards a single European railway system. Although the level of safety of the rail-bound transports in Europe is very good, this development towards a single network will require many efforts to maintain the level of safety of the European rail-bound transports.

The EC has the task of contributing to the establishment and development of trans-European networks in the area of transport. In order to achieve these objectives, the EC must take the necessary measures to ensure the interoperability of the networks, particularly in the field of *technical standardisation*.

In this context, two European directives, 96/48/EC and 2001/16/EC, dealing with interoperability on railway system at high speed and conventional railway system were adopted on July 1996 and on March 2001. They introduce community procedures for the preparation and adoption of Technical Specifications for Interoperability (TSIs) [2] and common rules for assessing conformity to these specifications.

In order to achieve the objectives of that directives, TSIs are set up by the European Association for Railway Interoperability (AEIF), which acts as the joint representative body defined in the directive, bringing together representatives of the infrastructure managers and railway companies. During the last four years, AEIF has been engaged in the development of the TSIs required by the directive 96/48/EC (Interoperability of the trans-European high speed railway system). The AEIF has also the task of setting up the TSIs for conventional rail according to the approved directive on interoperability of conventional rail.

The safety directive 2004/49/EC [4], published in April 2004, comes to supplement this process by reinforcing safety from the European railway system. It adopts a *progressive* approach for the harmonization and the development of the *common approaches of safety*, by taking into account the differences which exist between the Member States. It specifies that "each manager of the infrastructure and each railway company is responsible for the safety of exploitation related to his activity".

2.1 Railway functional architecture

The AEIF has elaborated a group of TSIs. That was very important and innovative work, applied to the whole transeuropean railway system. It was made possible by the large coverage of the fields of expertise necessary for its realisation [5]. The AEIF has produced starting functions for generic railway architecture. These functions contain most of the Basic Parameters (BP) for interoperability. The BP are the basic constituents of the railway system.

Moreover, it has set up a functional system analysis of the conventional railway system covering the full chain of railway transport. This analysis represents also a systematic and coherent decomposition of functions (functional breakdown) up to four levels of decomposition fulfilling the above mentioned requirements of a functional breakdown. Due to the enormous scope of the overall European conventional rail system, AEIF selected specific functions relevant for interoperability for in-depth analysis. The functions of the first level are listed in Table 1.

The method of system analysis is based on a matrix consisted of two perspectives: functional, and structural [1].

- The *functional aspects*. This analysis aims to identify the functions of the system and their definitions, specifications and relations. It does not take into account any notion of time. Invariants and safety properties of the system are linked to this point of view. The use of inputs, under certain conditions, and the generation of outputs, which have to respect a number of requirements, are the main issues at this stage of analysis.
- The *structural aspects* are mainly related to tasks, resources and devices that are allocated to perform the functions of the system. The network

Table 1: Functions according to AEIF.

Function	Description
F1	Support and guide the train
F2	Supply the train
F3	Load freight
F4	Load passengers
F5	Move rolling stock
F6	Maintain and provide data on rolling stock, infratsructure and time table
F7	Prepare operation of train
F8	Operate a train
F9	Evaluate transport quality
F15	Provide service for passengers
F16	Provide service for freight
F17	Manage human resources

of resources constitutes the railway architecture. All constituents of the architecture must operate under a set of constraints like safety and interoperability. It is throughout these structural points of view that the interfaces requirements are addressed.

A railway system can also be divided into partial systems, subsystems and components. Each *level* demands for another approach in risk identification and risk control. In order to put on most suitable methods and to obtain most reliable results, these levels should be taken into account during the whole process of risk management [6].

Due to his advantage to allow the identification of duty holders (institutions or enterprises responsible to fulfill a defined target) as well as a generic approach applicable on different kinds of railway operations, a functional breakdown approach has been chosen for the apportionment of CSTs to a more detailed level.

The functional breakdown remains universally valid when stopping at a sufficiently high level. If an allocation of a function to the duty holders is not possible at a specific (high) level, it is necessary to breakdown a function into more detailed level until a further precise assignment of responsibility for this function between duty holders such as IM, RU is possible. It is important in this process that the independence of specific technical realisation remains maintained. It does not make sense to define CSTs on a level where this independence is not guaranteed. Finally the generic approach and the independence of specific technical and/or operational realization is a more important criteria than the allocation of duty holders.

The railway system is embedded within its physical environment. This means that interactions with the environment are possible. In example, it is possible that trains collide with road traffic at level crossings. Level crossings are places where there is an interaction between road and railway traffic. Beside that the physical environment can interfere with the railway system and vice versa. A good system description as well as the description of the system boundaries and the possible interaction of the system with its environment are essential for the identification of risks and the adequate strategy for their apportionment.

2.2 Risk apportionment strategies

Risk apportionment strategies are based on CENELEC standard EN50126 [7] which has defined risk as in eqn 1.

$$Risk = Damage * Probability \tag{1}$$

2.2.1 System breakdown approach

This approach consists of decomposing the whole railway system into its major components (organizational and/or physical) parts and assigning a risk portion of the overall risk to each part [8], depending on the estimated or required contribution of each part to the global risk.

2.2.2 Breakdown by categories of hazard causes

This breakdown was proposed by the International Union of Railways (UIC) Safety Platform. It recommends setting specific CSTs related to causes of hazardous situations, based on the following classification: – technical faults; – human errors; – Organizational failures (e.g. wrong rules or procedures); – External causes.

2.2.3 Functional approach

The functional approach looks at all the phases, functions and processes taking place in the operation of a railway system. It identifies the hazards that may occur in each of these functions before evaluating the potential resulting risks associated with each function, process and subsequently the phase of operation (bottom-up). Alternatively, it allows apportioning the global risk to each phase, functions and process (top-down).

2.2.4 Breakdown by hazard types

By this approach, the global residual risk is apportioned between all possible hazards [6]. By hazards, it is meant here generic system level hazards which can lead to accidents.

2.2.5 Breakdown by accident types

This is the simplest approach of all. First a list of typical railway accidents has to be agreed on, then the global residual risk (per group categories) is apportioned to the different accident types, using statistics.

It is necessary to bear in mind some general considerations about CSTs. A global CST is expressed as a risk (e.g. a combination of frequency and severity of harmful events). This implies that the specific CST should also be expressed as a risk, as a portion of the global residual risk [8]. What is however eventually useful for operators and suppliers is to know what should be the acceptable frequency rate of events such as an accident, a hazard, and more importantly, a function fault, a constituent dangerous failure, etc., so as to determine specific safety requirements on parts of the railway system, particularly for new systems. Thus, it is important to stress that whichever way the risks might be apportioned for defining CSTs, there will still be some rather complicated safety allocation process necessary behind, in order to derive safety requirements.

Following the analysis of existing risk, it is essential to comply with the safety level required by each function of the railway system as below.

3 An operational functional approach

The methodology used to apportion Safety Integrity Level (SIL)'s to safety functions/ sub-systems is derived from the CENELEC standards and should been performed according to the following steps:

1. Functional Analysis of the railway system to identify all safety related functions.

2. Identification of the required level of safety/SIL assignment to safety related functions.
3. Assignment of each safety related function to safety systems.
4. Identification, where applicable, of external risk reduction facilities. Redundant or back up risk reduction measures can be a combination of system design, procedures and external facilities.

Based on these steps, functions required to avoid the occurrence of the hazard, or its evolution into an accident, are identified.

3.1 Functional risk apportionment

The proposed risk apportionment methodology is specifically focused on identifying an optimum safety level for each safety function while keeping the following objectives in mind:

- Individual functional packages should be as independent as possible with a minimum of interactive effects on other packages;
- In breaking down a system into (sub)functions at low level where the communication between the (sub)functions is minimized.

It can be assumed that when this approach is useful in allocating the risk, it should be possible to modify it to perform the system functionality [9]. Thus, it allows the technical components needed to achieve the allocated functionality.

The idea of the method is to provide each IM or RU with a reliability level for each function.

Based on the functional breakdown of railway system, a five-steps approach (Fig. 1) has thus been conducted [10]:

1. Given the functional railway architecture breakdown proposed by the AEIF, build the corresponding hierarchical model;

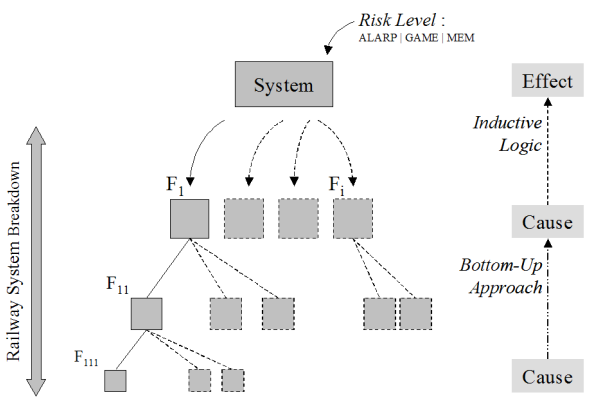

Figure 1: Functional risk apportionment.

2. Choose the safety acceptance criteria (global safety target) to be adopted in the European Community in order to comply with European Safety Directive;
3. Transform the safety acceptance criteria into specific safety target (qualitative and quantitative);
4. Propagate the specific safety target through the functional breakdown;
5. Check the consistency with the Safety Integrity Levels (SILs) and other safety requirements of constituents and subsystem levels.

In order to achieve a system breakdown method, the following objective has been formulated: develop a system breakdown method that provides risk apportionment insight the system functionality in terms of system effectiveness.

Moreover, the extension of this approach to make it applicable in practice needs to establish certain quantitative considerations and breakdown rules.

One of the main disadvantages of this single model approach is represented by the lack of reusability of the model. A new model needs to be built if the behavior of the system in any phase is changed or if the phase order is changed. Moreover, a substantial effort may be needed to define and solve, using automatic tools, the overall model of the system, which is often of large size. To this end, we examined the contribution of the constraint programming.

3.2 Constraint programming

This method is particularly adapted to our approach of functional decomposition since it is a question, to each stage, of considering the safety requirements in the rail-bound transport. Generally, Constraints Satisfaction Problem (CSP) are used to tackle the problem of ressources' allocation, which is similar to our problem of Common Safety Targets' allocation.

One of the major interests of this technique is that the constraints are used in a deductive process in the sense that the propagation can make it possible to detect an inconsistency quickly and thus to accelerate the treatment of the problem [11].

Our CSP is thus the triplet (X,D,C) such as:

- $X = X_1, X_2, \ldots, X_n$ is a whole of N risks
- D is the function which associates each variable X_i its $D(X_i)$ field, the whole of the values which a risk X_i can take
- $C = C_1, C_2, \ldots, C_m$ is a whole of constraints. Each C_j constraint is a relation between the risks which can take of the functions.

Constraint programming is an embedding of constraints in a host language. The first host languages used were logic programming languages, so the field was initially called constraint logic programming. The two paradigms share many important features, like logical variables and backtracking. Today most Prolog implementations include one or more libraries for constraint logic programming [12]. The difference between the two is largely in their styles and approaches to modeling the world. Some problems are more natural (and thus, simpler) to write as logic programs, while some are more natural to write as constraint programs.

The constraints used in constraint programming are typically over some specific domains. Some popular domains for constraint programming are boolean domains, where only true/false constraints apply (SAT problem: Boolean SATisfaibility problem (SAT)). The combination of constraint programming to SAT problem decides whether a given propositional formula is satisfiable and is of central importance in automation and verification [13].

What makes this railway use case really tricky is the omnipresent dependencies between components, and between the functions.

Another criticism is that this use case could suffer from is the fact that all distributions are exponential. This assumption is very common about the times to failures of components, but what may seem strange is the fact that the phases durations are exponentially distributed. We have deliberately chosen this assumption in order to be able to use the Monte-Carlo solving method.

4 Conclusion

The paper highlights the use of the functional railway architecture for risk apportionment in railways.

The suggested approach is based on functional breakdown of railway systems and the use of the constraints to the apportionment of the global safety targets. The qualitative approach of this analysis is examined in this paper using an example of railway function. The set up of the Constraints Satisfaction Problem for risk apportionment is under development within a PhD research.

However, several allocation solutions may be simultaneously eligible. In other terms, one could have several spreads of the risk on the basic functions of the railway system which lead to the same total level of safety, while checking the local constraints.

References

[1] Chatel, V., El-Koursi, E.M., Feliot, C. & Huismann, U., Functional analysis of the sub-system of energy and infrastructure of conventional rail. *Systems, Man and Cybernetics, 2002 IEEE International Conference on*, **3**, 2002.

[2] El-Koursi, E.M. & Duquenne, N., Assessment of the safety management system in railway sectors. *WCRR*, Montreal, 2006.

[3] El-Koursi, E.M., Mitra, S. & G., B., Harmonising safety management systems in the european railway sector. *Safety Science Monitor*, **11(2)**, 2007.

[4] Directive 2004/49/ec of 29 april 2004 on safety on the community's railways and amending council directive 95/18/ec on the licensing of railway undertakings and directive 2001/14/ec on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (railway safety directive). *Official Journal of the European Union*, **L220**, pp. 16–39, 2004.

[5] Gigantino, A., Report on the representative architecture. Technical report, AEIF, 2002.
[6] Kuijlen, H. & VanDerBerg, P., D.2.3.0: Common safety methods. Technical report, 2004.
[7] En50126 : The specification and demonstration of reliability, availability, maintainability and safety. Technical report, 1999.
[8] Mihm, P. & Eckel, A., D.2.4.0: Acceptable risk level. Technical report, 2004.
[9] Rafrafi, M., Bourdeaud'Huy, T. & El-Koursi, E.M., Risk apportionment methodology based on functional analysis. pp. 1103–1109, 2006.
[10] Rafrafi, M. & El-Koursi, E.M., Functional hazard analysis for railway safety. *Formal Methods for Automation and Safety in Railway and Automotive Systems "FORMS/FORMAT2007"*, ed. E.S.G.T. (Eds.), pp. 164–73, 2007.
[11] Ouis, S., Jussien, N. & Lhomme, O., Explications conviviales pour la programmation par contraintes. *Journées Francophones de Progammation en Logique et avec Contraintes (JFPLC'02)*, Hermès, pp. 105–118, 2002.
[12] Van Hentenryck, P., Constraint satisfaction in logic programming, 1989.
[13] Piechowiak, S. & Rodriguez, J., The localization and correction of errors in models: A constraint-based approach. *Applied Intelligence*, **23(3)**, pp. 153–164, 2005.