Chapter 54
The Role of Formal Methods in Software Development for Railway Applications

Alessandro Fantechi
Università degli Studi di Firenze, Italy

ABSTRACT

Formal methods for thirty years have promised to be the solution for the safety certification headaches of railway software designers. This chapter looks at the current industrial application of formal methods in the railway domain. After a recall of the dawning of formal methods in this domain, recent trends are presented that focus in particular on formal verification by means of model checking engines, with its potential and limitations. The paper ends with a perspective into the next future, in which formal methods will be expected to pervade in more respects the production of railway software and systems.

INTRODUCTION

The challenges posed by the new scenarios of railway transportation (liberalization, distinction between infrastructure and operation, high speed, European interoperability,...) have a dramatic impact on the safety issues. This impact is counterbalanced by a growing adoption of innovative signaling equipments (most notable example is ERTMS/ETCS) and monitoring systems (such as on board and wayside diagnosis systems). Each one of these devices include some software, which in the end makes up the major part of their design costs; the malleability of software is paramount for the innovation of solutions. On the other hand, it is notorious how software is often plagued by bugs that may threaten its correct functioning: how can the high safety standards assumed as normal practice in railway operation be compatible with such threats?

The employment of very stable technology and the quest for the highest possible guarantees have been key aspects in the adoption of computer-controlled equipment in railway applications. Formal proof, or verification, of safety is therefore seen as a necessity.

DOI: 10.4018/978-1-4666-4301-7.ch054

This chapter reviews current experiences and future trends in the application of formal methods in the railway area: after a recall of the first steps of formal methods in this domain, recent trends are presented, both from the point of view of safety guidelines, and from that of the practical applications, pointing to the most adopted techniques, in particular related to formal verification by model checking. The specific application to railway signaling equipment is dealt with some detail, and future trends will emerge from such discussion.

BACKGROUND

Early Applications of Formal Methods

Nowadays, the necessity of formal methods as an essential step in the design process of industrial safety-critical systems is widely recognized.

In its more general definition, the term formal methods encompasses all notations having a precise mathematical semantics, together with their associated analysis and development methods, that allow to describe and reason about the behaviour and functionality of a system in a formal manner, with the aim to produce an implementation of the system that is provably free from defects.

Railway signaling has been traditionally considered as one of the most fruitful areas of intervention for formal methods (Fantechi, Fokkink, & Morzenti, 2011). Already in the early nineties, a series of railway signaling products have benefited from the application of the B formal method in the design process.

The B method (Abrial, 1996) targets software development from specification through refinement, down to implementation and automatic code generation, with formal verification at each refinement step: writing and refining a specification produces a series of *proof obligations* that need to be discharged by formal proofs. The B method is accompanied by support tools, which include tools for the derivation of proof obligations, theorem provers, and code generation tools.

The B method has been successfully applied to several railway signalingsignaling systems. The SACEM system for the control of a line of Paris RER (DaSilva, Dehbonei, & Mejia, 1993) is the first acclaimed industrial application of B. B has been adopted for many later designs of similar systems by Matra (now absorbed by Siemens). One of the most striking application has been the Paris automatic metro line 14. The paper (Behm, Benoit, Faivre, & Meynadier, 1999) on this application of B reports that several errors were found and corrected during proof activities conducted at the specification and refinement stages. By contrast, no further bugs were detected by the various testing activities that followed the B development.

CENELEC Guidelines

The success of B has had a major impact in the sector of railway signaling by influencing the definition of the EN50128 guidelines (CENELEC, 2001), issued by the European Committee for Electrotechnical Standardization (CENELEC). These guidelines address the development of ”Software for Railway Control and Protection Systems”, and constitute the main reference for railway signaling equipment manufacturers in Europe, with their use spreading to the other continents and to other sectors of the railway (and other safety-related) industry.

The EN50128 document is part of a group of documents regarding the safety of railway control and protection systems, in which the key concept of Safety Integrity Level (SIL) is defined, a number ranging from 0 to 4, where 4 indicates a high criticality, 0 gives no safety concern. The SIL is actually a property of the system, related to the damage a failure of the system can produce, and is usually apportioned to subsystems and functions at system level in the preliminary risk assessment process. Also software functions are associated a level (Software SIL); assigning different SILs