Chapter 10

Formal Assurance of Signaling Safety: A Railways Perspective

Pallab Dasgupta
Indian Institute of Technology Kharagpur, India

Mahesh Mangal
Indian Railways, India

ABSTRACT

The EN50128 guidelines recommend the use of formal methods for proving the correctness of railway signaling and interlocking systems. The potential benefit of formal safety assurance is of unquestionable importance, but the path towards implementing the recommendations is far from clear. The EN50128 document does not specify how formal assurance of railway interlocking may be achieved in practice. Moreover, the task of setting up an electronic interlocking (EI) equipment involves multiple parties, including the EI equipment vendor, the certification agency which certifies the resident EI software to be correct, and the end user (namely the railway service provider) who must configure the EI equipment. Considering the distributed nature of the development process, a feasible approach towards formal certification of the end product (post configuration) is not obvious. This chapter outlines the basics of formal verification technology and presents, from the perspective of the railways, a pragmatic roadmap for the use of formal methods in safety assurance of its signaling systems.

INTRODUCTION

Railway signaling has been one of the most well studied safety critical systems for nearly two centuries. During this period, the notion of railway signaling has evolved in various ways, including the protocol for signaling, the technology used for implementing the signaling system, and most importantly the way in which safety guarantees are assured. The very early form of signaling relied on temporal separation of trains, which was primarily implemented by setting up time tables that ensured that two trains never shared a track at the same time. With the increase in railway traffic, it became necessary to divide the DOI: 10.4018/978-1-5225-0084-1.ch010

Copyright © 2016, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
tracks into segments (or blocks), thereby giving birth to the notion of *block signaling*, where one or more trains can be on the same track, but on different blocks – which effectively means that the trains are *spatially separated*. Signals guard the entry of the block and implement the spatial separation.

Railway yards also have *points* where two tracks intersect. The *point setting* determines whether the train will continue to move on the same track or whether it will move into the intersecting track. A complex yard may contain many *points*, with the tracks crisscrossing each other, which significantly increases the complexity of ensuring that a train can safely move from one track to another possibly passing through several intermediate tracks. In signaling parlance such complex passages are called *routes*. A railway yard can have hundreds of routes, and the signaling system must ensure that conflicting routes are kept free when a train is passing through a route. This is achieved by a mechanism called *interlocking*.

In the past railway interlocking was primarily manual. The hand-operated point levers shown in Figure 1 are reminiscent of the times when point positions were changed manually using such levers. The interlocking system, implemented using electrical relays, would ensure that signal aspects change only when points are in proper position.

In recent times, railways use *electronic interlocking*, where the signals and point positions are controlled by software running on an electronic interlocking (EI) system. Such computer controlled systems are designed to adhere to the signaling standards. Once configured properly with respect to a specific railway yard, they continue to work reliably over time and are not subject to human errors.

The primary concern with EI equipment is in determining with absolute certainty that the system configuration is correct, and that given a correct system configuration, the software is guaranteed to never err in signaling decisions. In current practice this verification task is performed using a high level of certification of the software and through rigorous testing of the configured equipment.

In spite of the best practices followed in configuring and testing of EI equipment, there are known instances of failures resulting out of human errors in the design of the logic for the EI equipment. The following two incidents may be highlighted:

- [The Milton Keynes Incident, Dec 29, 2008] As reported in (Railway Accident Investigation Branch Report, 2010), on December 29, 2008, a serious signaling error was detected at the Milton Keynes Central station on the West Coast Main Line in UK. The driver of a train observed a signal change from red to green, although the track beyond the signal was occupied by another train.
Related Content

Ethics Is Not Enough: From Professionalism to the Political Philosophy of Engineering
www.igi-global.com/chapter/ethics-is-not-enough/144551?camid=4v1a

Selection of Renewable Energy Sources for Buildings
www.igi-global.com/chapter/selection-of-renewable-energy-sources-for-buildings/199586?camid=4v1a

A General Simulation Modelling Framework for Train Timetabling Problem
Özgür Yalçıkaya (2016). Handbook of Research on Emerging Innovations in Rail Transportation Engineering (pp. 335-386).
www.igi-global.com/chapter/a-general-simulation-modelling-framework-for-train-timetabling-problem/154423?camid=4v1a

Applying the Safety and Environmental Risk and Reliability Model (SERM) for Malaysian Langat River Collision Aversion