Applied Mathematical Modelling 38 (2014) 413–424

Contents lists available at SciVerse ScienceDirect

Applied Mathematical Modelling

journal homepage: www.elsevier.com/locate/apm

Extending Petri net to reduce control strategies of railway interlocking system

Sher Afzal Khan [a,*], Nazir Ahmad Zafar [b], Farooq Ahmad [c], Saeed Islam [d]

[a] Department of Computer Science, Abdul Wali khan University, Mardan, Pakistan
[b] Department of Computer Science, King Faisal University, Al Hassa, Saudi Arabia
[c] Faculty of Information Technology, University of Central Punjab, Lahore, Pakistan
[d] Department of Mathematics, Abdul Wali Khan University, Mardan, Pakistan

ARTICLE INFO

Article history:
Received 27 October 2012
Received in revised form 24 February 2013
Accepted 11 June 2013
Available online 10 July 2013

Keywords:
Software specification and verification
Petri net
Mobile Petri net
Railway interlocking system
Safety properties

ABSTRACT

In our previous articles we gave step by step refinement process towards the development of safety properties of moving block interlocking system (MBRIS). The refinement process started from abstraction to fuzzy based safety properties using *Z* and then fuzzy multi agent specification language. However, one dimensional control of train passing through a switch and level crossing were not discussed. This paper reduces the existing two dimensional controls along the switch and level crossing to one dimensional for shifting it to a train only. For example, in the existing model the train movement along components switches and level crossings depends on both the train and components control. Whereas, in one dimensional control train is the only authority to control a switch and level crossing required for its desired operation. For this reduction, concurrent and mobile agent concepts are required. Therefore, we integrate mobile agent concepts with Petri nets to develop the mobile Petri net (MPN) a new class of PNs. This supports both mobility and concurrency. Further, we prove that the collection of different MPNs in a connected network is a PN. This proof allowed us to use the properties of PN to verify the system. Finally, we use MPN to model the safety properties of MBRIS along the switch and level crossing. This provides one dimensional control to a train along a switch and level crossing which increases the safety of the railway interlocking system. Moreover, we use reachability graph (RG) to verify the switch and level crossing models.

Contents

1. Introduction . . . 414
2. Petri net . . . 415
3. Mobile Petri net . . . 415
4. Conceptual model using mobile agent net . . . 417
5. Modeling and verification using mobile Petri net . . . 418
   5.1. Switch model . . . 418
   5.2. Level crossing model . . . 421

* Corresponding author. Tel.: +92 3335128208.
E-mail addresses: sher.afzal@awkum.edu.pk (S.A. Khan), nazafar@kfu.edu.sa (N.A. Zafar), drfarooq@ucp.edu.pk (F. Ahmad), saeedislam@awkum.edu.pk (S. Islam).

0307-904X/$ - see front matter
http://dx.doi.org/10.1016/j.apm.2013.06.002

6. Conclusion 423
References 423

1. Introduction

The huge train's weight in tons, great length in hundreds of meters, iron track, distributed environment, multiple control and presence of critical tracks components, make the interlocking a high safety, monetary and environmentally critical system. Its malfunctioning can cause very serious consequences such as loss of human life, severe injuries, large scale of environmental damages and considerable economic penalties. For example Table 1 shows the number of human losses and injuries due to trains accidents and derailments from year 2005 to 2009 [1].

The use of computer in railway interlocking has increased concerns about its safety. This is because of the historical experience with the software systems that exhibit larger numbers of errors than their other counterparts. The software itself cannot cause safety problems. Safety problems occur due to loopholes which we leave in software development of potentially dangerous system. Formal methods, based on mathematical foundation, can be applied for modeling such systems to give an increased confidence. Use of formal methods requires all assumptions to be stated which avoid omission and expose inconsistencies that often exists in the natural language descriptions [2]. Further, formal methods use logic theory which is used to check consistency of logic formulas. It is evident that most of the software fails due to its incomplete and inconsistent requirements. As it is mentioned in [3], most software errors are introduced during the requirement phase. It is also documented that fixing errors is extremely costly when it comes later in the software life cycle. According to the European Committee of Electro Technical Standardization [4], use of formal methods in the development of safety-critical and computer-controlled systems for railways applications is recommended. Formal methods have also been used successfully in different industrial projects [5–8].

Railway safety is a system which prevents trains from collisions. Trains are always at risk for collision because, running at fixed track a train is not capable of steering away from another conflicting train as like road vehicle to avoid collision. Also in case of obstacle at railway track, the train cannot stop in time to avoid collision. This is because; the train cannot decelerate rapidly, when the driver sees the obstacle.

To avoid collision and other conflicts there is a mechanism in which the message transformed from a signalman of the rail network to the rail team either to pass or stop the train is called the signaling system. The interlocking is an arrangement of signals that prevents trains from collision along railway components: crossings, level crossings and switches. The signaling and track arrangements are collectively called interlocking system. In interlocking design it is impossible for a train to enter a route unless it is proved to be clear and safe.

There are two main existing technologies of railway interlocking: fixed block and moving block. The work carried out in [9,10] and a list [11] of 299 publications addressing various issues on this topic, proves its importance. Most of the research work is done on fixed block railway interlocking, while there is a little work on moving block interlocking system. The moving block is considered to be more important in railway industry because of some disadvantages in fixed block [12].

Uses of formal methods for specification of both the technologies have been documented. Work carried out by Simpson et al. [13] concerns geographic databases with logical representations of physical components, which describes fixed block interlocking. Further, Haxthausen et al. [14] use `RAISE` [15] to describe formal representation of distributed rail control. They do not describe in strict sense the approach of moving block in rail system. However, they describe its distributed rail system using both approaches of moving and fixed block. Moreover, Simpson [16] has further introduced the notation of "safe distance" (moving block) enhancing the existing work on fixed block interlocking systems. Zafar et al. [17] extends the existing approach of moving block and specify safety and control properties of railway interlocking systems using `VDM-SL` [18]. Khan et al. [19,20] specifies the moving block using a different strategy of promotion in *Z*-notations.

In our previous work [21], we improved the existing work to capture the inexact and continuous features like speed, weight and moving block. For this, we developed fuzzy multi-agent specification language (FMASL) using an integration of Object-*Z*, fuzzy logic and MAS approaches. It is then used to specify the movement of a train along the railway crossing which provides intelligent and human skilled operator capability to the train to pass through a crossing based on its priority.

Table 1
Fatalities and Injuries due to Accidents and Derailments.

Accident and Derailment	2005		2007		2009	
	killed	Injured	killed	Injured	killed	Injured
Level crossing accidents	122	370	85	130	35	26
Crossing accidents	40	70	30	120	60	330
Derailments	230	1100	245	340	120	250
Linear track accidents	180	200	74	125	40	100
Other	110	237	70	200	35	120