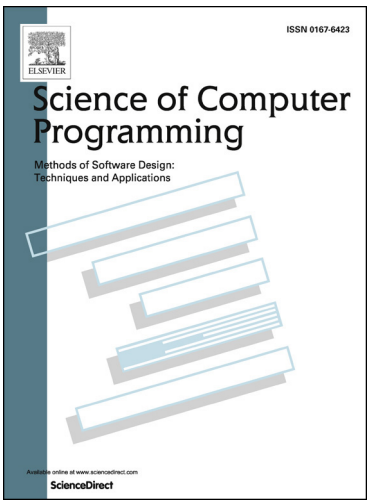
Accepted Manuscript



Dynamic state machines for modelling railway control systems

M. Benerecetti, R. De Guglielmo, U. Gentile, S. Marrone, N. Mazzocca et al.

PII: S0167-6423(16)30133-2
DOI: http://dx.doi.org/10.1016/j.scico.2016.09.002
Reference: SCICO 2050

To appear in: *Science of Computer Programming*

Received date: 21 December 2015
Revised date: 12 September 2016
Accepted date: 15 September 2016

Please cite this article in press as: M. Benerecetti et al., Dynamic state machines for modelling railway control systems, *Sci. Comput. Program.* (2016), http://dx.doi.org/10.1016/j.scico.2016.09.002

Dynamic State Machines for Modelling Railway Control Systems

M. Benerecetti[a], R. De Guglielmo[c], U. Gentile[a], S. Marrone[b], N. Mazzocca[a], R. Nardone[a,*], A. Peron[a], L. Velardi[c], V. Vittorini[a]

[a] *Department of Electrical Engineering and Information Technology, University of Naples Federico II, Naples, Italy*
[b] *Department of Mathematics and Physics, Second University of Naples, Naples, Italy*
[c] *Ansaldo STS, Naples, Italy*

Abstract

Verification and Validation of railway controllers is the most critical and time-consuming phase in a system development life-cycle. It is regulated by international standards, which explicitly recommend the usage of state machines to model the specification of the system under test. Despite the great deal of works addressing the usage of state machines and their extensions, model-based verification and validation processes still lack concise and expressive-enough notations able to easily capture peculiar features of the specific domain of multi-process control systems, on which proper tool chains can be implemented in order to realize effective and automated environments.

This paper introduces a novel class of hierarchical state machines, called Dynamic STate Machines (DSTMs), and proposes an approach for modelling and validating railway control systems, based on the new specification language. Key features of DSTM are recursive execution, parallelism, parameter passing, abortion transition, and communication through global variables and channels, but its main peculiarity resides in the semantics of fork and join operators which allows for dynamic instantiation of machines (processes). The formal semantics of DSTM allows for the definition of verification and validation methodologies supported by automated tools. The paper also describes how DSTM specifications may be mapped to Promela models in order to achieve automated generation of test cases by model checking and Spin.

The work presented in this paper was carried out in the context of an European project and is strongly driven by the industrial necessity of tackling issues concerning the automation of functional system-level testing of modern railway signalling systems. Hence, the language and the proposed approach are illustrated and motivated by applying them to a specific functionality of the Radio Block Centre, the vital core of the ERTMS/ETCS Control System.

Keywords: Formal Methods, Dynamic STate Machines, Promela model, ERTMS, ETCS, Control System, Verification and Validation

1. Introduction

Verification and Validation (V&V) of critical control systems is partly conducted accorKim Phucding to model-based approaches. International standards in the railway domain explicitly recommend the usage of Finite State Machines (for example in the CENELEC norms EN50128 [12] and EN50129 [11]), since the dynamics of critical control systems based on a sequential computation can be abstracted as a state-transition system. An upward trend is to automate the V&V processes by providing toolchains for effective model-based approaches and integrating well-known and assessed tools for quality and architecture management [36, 34, 3]. As the V&V activities often amount to more than fifty percent of the total development costs, automated solutions are very appealing in industrial settings [33]: they can enhance abstraction and reuse, enable

*Contact Author
Email address: roberto.nardone@unina.it (R. Nardone)