Specification of Communication Based Train Control System Using AADL

Lichen Zhang\textsuperscript{1} and Bingqing Xu\textsuperscript{2,*}

\textsuperscript{1} Faculty of Software Engineering Institute, East China Normal University, Shanghai 200062, Shanghai, China
zhanglichen1962@163.com
\textsuperscript{2} Software Engineering Institute, East China Normal University, 200062 Shanghai, China
xbqjoya@gmail.com

Abstract. The development of railway cyber physical systems is a challenging process. In this paper we present our current effort to extend AADL to include new features for separation of concerns of railway cyber physical systems, we extend AADL in spatial aspect, dynamic continuous aspect, physical world modeling aspect. Finally, we illustrate the proposed method via an example of specification of communication based train control system.

Keywords: AADL Railroad system, Train control system, component, OSATE.

1 Introduction

The problems that must be addressed in operating a railway are numerous in quantity, complex in nature, and highly inter-related [1-3]. Because of the timeliness constraints, safety and availability of train systems, the design principles and implementation techniques adopted must ensure to a reasonable extent avoidance of design errors both in hardware and software. Thus a specific methodology relevant, to design should be applied for train control systems development. The dependability of the railway cyber physical system should arouse more attention [4-5].

In this paper, we propose a specification for communication based train control system (CBTC) using AADL. We use the AADL to specifying each subsystem, and make an effective integration of all subsystems together to form a complete CBTC system.

2 The Proposed Specification Method for Communication Based Train Control Systems

AADL [6-7] is an architecture description language developed to describe embedded systems is shown in Fig.3. AADL (Architecture Analysis and Design Language),

* Corresponding author.
which is a modeling language that supports text and graphics, was approved as the industrial standard AS5506 in November 2004. Component is the most important concept in AADL. The main components in AADL are divided into three parts: software components, hardware components and composite components. Software components include data, thread, thread group, process and subprogram. Hardware components include processor, memory, bus and device. Composite components include system.

In its conformity to the ADL definition, AADL provides support for various kinds of non-functional analyses along with conventional modeling [8]:

- **Flow Latency Analysis**: Understand the amount of time consumed for information flows within a system, particularly the end-to-end time consumed from a starting point to a destination.
- **Resource Consumption Analysis**: Allows system architects to perform resource allocation for processors, memory, and network bandwidth and analyze the requirements against the available resources.
- **Real-Time Schedulability Analysis**: AADL models bind software elements such as threads to hardware elements like processors. Schedulability analysis helps in examining such bindings and scheduling policies.
- **Safety Analysis**: Checks the safety criticality level of system components and highlights potential safety hazards that may occur because of communication among components with different safety levels.
- **Security Analysis**: Like safety levels, AADL components can be assigned various security levels.

AADL defines two main extension mechanisms: property sets and sublanguages (known as annexes). It is possible to extend the AADL concepts either by introducing new properties to the modeling elements, by addition of new modeling notations, or by developing a sublanguage as annex to the AADL [9-10].

- **Physical World Aspect**: Railway cyber physical systems are often complex and span multiple physical domains. Modelica [11-12] is a new language for hierarchical object oriented physical modeling which is developed through an international effort. The language allows the user to specify mathematical models of complex physical systems.

- **Dynamic Continuous Dynamics Aspect**: Railway cyber physical systems are mixtures of continuous dynamic and discrete events. These continuous and discrete dynamics not only coexist, but interact and changes occur both in response to discrete, instantaneous, events and in response to dynamics as described differential or difference equations in time.

- **Spatial Aspect**: The analysis and understanding of railway cyber physical systems spatial behavior – such as guiding, approaching, departing, or coordinating movements is very important.