Available online at www.sciencedirect.com
ScienceDirect
Computers in Industry 59 (2008) 41–54
COMPUTERS IN INDUSTRY
www.elsevier.com/locate/compind

Model-based system analysis using Chi and Uppaal: An industrial case study

N.C.W.M. Braspenning *, E.M. Bortnik, J.M. van de Mortel-Fronczak, J.E. Rooda

Department of Mechanical Engineering, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Received 10 October 2006; received in revised form 12 March 2007; accepted 4 June 2007
Available online 10 August 2007

Abstract

New methods and techniques are needed to reduce the integration and test effort (lead time, costs, resources) in the development of high-tech multi-disciplinary systems. To facilitate this effort reduction, a method called model-based integration and testing is being developed. The method allows to integrate formal and executable models of system components that are not yet physically realized with available realizations of other components. The combination of models and realizations is then used for early analysis of the integrated system by means of validation, verification, and testing. The analysis enables early detection and prevention of problems that would otherwise occur during real integration, resulting in a significant reduction of effort invested in the real integration and testing phases. This paper illustrates the application of the method to a realistic industrial case study, focusing on verification of the models obtained. We show how a system model has been developed for model-based integration and testing in the timed process algebra χ (Chi), and how certain behavioral properties of this model have been verified by the Uppaal model checker.
© 2007 Elsevier B.V. All rights reserved.

Keywords: Model-based integration and testing; Model checking; Chi; Uppaal translation; Industrial case study

1. Introduction

High-tech multi-disciplinary systems like wafer scanners, electronic microscopes and high-speed printers are becoming more complex every day. Growing system complexity also increases the effort (in terms of lead time, cost, resources) needed for the, so-called, *integration and testing phases*. During these phases, the system is integrated by combining component realizations and, subsequently, tested against the system requirements. Existing industrial practice shows that the main effort of system development is shifting from the design and implementation phases to the system integration and testing phases [1]. Furthermore, finding and fixing problems during integration and testing can be up to 100 times more expensive than finding and fixing the problems during the requirements and design phases [2].

Literature reports wealth of research proposing a *model-based* way of working to counter the increase of development effort, like requirements modeling [3], model-based design [4], model-based code generation [5], hardware–software co-simulation [6], and model-based testing [7]. In most cases, however, these model-based techniques are investigated in isolation, and little work is reported on combining these techniques into an overall method. Although model-based systems engineering [8] and OMG's model-driven architecture [9] (for software only systems) are such overall model-based methods, these methods are mainly focusing on the requirements, design, and implementation phases, rather than on the integration and test phases. Furthermore, literature barely mentions realistic industrial applications of such methods, at least not for high-tech multi-disciplinary systems.

Our research within the TANGRAM project [10] focusses on a method of *model-based integration and testing* (MBI&T), introduced in [11]. In this method, formal executable models of system components (e.g. software, mechanics, electronics) that are not yet realized are integrated with available realizations of other components, establishing a *model-based integrated system*. Such a model-based integrated system can be

* Corresponding author at: Eindhoven University of Technology, Room WH0.07A, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.
Tel.: +31 40 247 8325; fax: +31 40 245 2505.
E-mail address: n.c.w.m.braspenning@tue.nl (N.C.W.M. Braspenning).
URL: http://yp.wtb.tue.nl/showemp.php/3060

0166-3615/$ – see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.compind.2007.06.002

established much earlier compared to a real integrated system, and it can effectively be used for early model-based system analysis and system testing, which has three main advantages. First, the fact that it is earlier means that the integration and test effort is distributed over a wider time frame. This reduces the effort to be invested during the real integration and testing phases. Second, it allows earlier and thus cheaper detection and prevention of problems that would otherwise occur during real integration. Early problem detection and prevention also reduces the corresponding diagnostic and fix effort and increases the quality of the system at an earlier stage. Finally, the use of formal models enables the application of powerful model-based analysis techniques, like simulation and verification. These analysis techniques help to improve the insight in the system's behavior for the engineers, resulting in better system quality as well.

This paper illustrates the application of the MBI&T method to the development of a part of a realistic industrial system, namely the ASML [12] wafer scanner.

In the case study, a system is formally specified by means of a process algebraic language χ (Chi) [13]. The χ language is supported by a toolset that allows simulation of the obtained χ model, e.g. for the analysis of system performance and exceptional behavior handling. The formal semantics of χ enable functional analysis of χ models, e.g. verification of the correctness of a system model. Combining performance analysis and functional analysis in the χ environment is the objective of the TIPSy project [14]. As a part of this project, a translation scheme [15] from χ to Uppaal timed automata [16,17] has been developed and integrated into the χ toolset, allowing verification of the translated models by the Uppaal model checker. The Uppaal tool has been used in a number of industrial case studies. A complete overview can be found in [18]. Mostly, the case studies concerned verifying real-time controllers [19] and communication protocols [20–23]. In [24] the problem of synthesizing production schedules and control programs for the mock-up of the batch production plant was addressed. In [25] the throughput of an ASML wafer scanner was analyzed with Uppaal.

The case study described in this paper focuses on verification of system properties such as deadlock freeness, liveness, safety, and temporal properties using the χ to Uppaal translation scheme and the Uppaal model checker. The goal of the case study and this paper is threefold. We show the potential of the proposed MBI&T method (in which the verification techniques are used) to reduce the integration and test effort of industrial systems. We investigate the applicability and usability of the χ toolset as integrated tool support for all aspects of the MBI&T method, particularly focusing on the implementation of the χ to Uppaal translation scheme. Finally, we discuss the advantages, applicability, and scalability of verification techniques for realistic industrial systems.

The structure of the paper is as follows. Section 2 describes the MBI&T method in general with the focus on the use of verification within the method. Section 3 introduces the industrial case study to which the MBI&T method has been applied. The activities that have been performed in the case study are described in Sections 4 (modeling and simulation with χ) and 5 (translation to and verification with Uppaal). Although model-based and real system testing are not the focus of this paper, Section 6 gives a short summary of these steps. Finally, the conclusions are drawn and discussed in Section 7.

2. Model-based integration and testing method

In current industrial practice, the system development process is subdivided into multiple concurrent component development processes. Subsequently, the resulting components (e.g. mechanics, electronics, software) are integrated into the system.

The development process of a system S that consists of n components $C_{1,\ldots,n}$ (we denote a set $\{A_1,\ldots,A_i,\ldots,A_n\}$ by $A_{1,\ldots,n}$) starts with the system requirements R and system design D. After that each component is developed. The development process of a component C_i consists of three phases: requirements definition, design, and realization. Each of these phases results in a different representation form of the component, namely the requirements R_i, the design D_i, and the realization Z_i. The realization of system S is the result of the integration $\{Z_{1,\ldots,n}\}_I$ of realizations $Z_{1,\ldots,n}$ by means of the infrastructure I. Here, infrastructure I contains everything that is needed to connect the components in order to let them perform the system's function, e.g., nuts and bolts (mechanical infrastructure), cables (electronic infrastructure), communication network (software infrastructure).

Fig. 1 shows a graphical representation of the current development process of system S. The arrows depict the different development phases and the boxes depict the different representation forms of systems and components. The vertical double headed arrow depicts the infrastructure I that connects the components. For simplicity, the figure shows a 'sequential' development process, however in practice the development process will have an incremental and iterative nature. This involves multiple versions of the requirements, designs, and

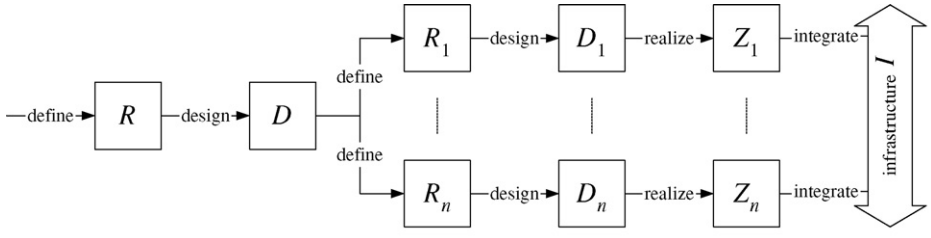

Fig. 1. Current system development process.

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات