How to Verify and Exploit a Refinement of Component-Based Systems*

Olga Kouchnarenko[1] and Arnaud Lanoix[1,2]

[1] LIFC, FRE 2661 CNRS, Besançon, France
{kouchna,lanoix}@lifc.univ-fcomte.fr
[2] LORIA, INRIA Lorraine & CNRS, Nancy, France
Arnaud.Lanoix@loria.fr

Abstract. In order to deal with the verification of large systems, compositional approaches postpone in part the problem of combinatorial explosion during model exploration. The purpose of the work we present in this paper is to establish a compositional framework in which the verification may proceed through a refinement-based specification and a component-based verification approaches.

First, a constraint synchronised product operator enables us an automated compositional verification of a component-based system refinement relation. Secondly, safety LTL properties of the whole system are checked from local safety LTL properties of its components. The main advantage of our specification and verification approaches is that LTL properties are preserved through composition and refinement.

Keywords: component-based systems, modules, refinement, LTL properties, composition, verification.

1 Introduction

Nowadays, formal methods are used in various areas, from avionics and automatic systems to telecommunication, transportation and manufacturing systems. However, the increasing size and complexity of these systems make their specification and verification difficult. Compositional reasoning is a way to master this problem.

The purpose of the work we present in this paper is to establish a compositional framework in which an algorithmic verification of a refinement of component-based systems by model exploration of components can be associated with the verification of LTL properties. In our compositional framework, we give ways (see Fig. 1) to preserve LTL properties through:

1. The composition operator for preserving safety LTL properties, meaning that a property satisfied by a separate component is also satisfied by a whole component-based system.

* Work partially funded by the French Research ACI *Geccoo*.

I. Virbitskaite and A. Voronkov (Eds.): PSI 2006, LNCS 4378, pp. 297–309, 2007.

2. The refinement relation for preserving both safety and liveness LTL properties, meaning that a property established for an abstract system model is ensured when the system is refined to a richer level of details.

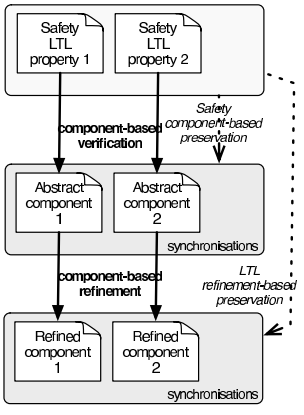

Fig. 1. Verification Principle

To achieve the goal of compositional verification and to model synchronous and asynchronous behaviours of components, we define two operators: a composition of the modules and a constraint synchronised product of transition systems.

We show that the modules [12,13,2] – subsystems sharing variables – whose composition is often used in a concurrent setting, are suitable to compositionally verify a kind of τ-simulation, called the weak refinement. Unfortunately, this model does not allow analysing the strict refinement – a divergence-sensitive completed τ-simulation – from the separate refinements of its modules. That is why we introduce a constraint synchronised product operator. Moreover, the semantics of the component-based systems using this operator makes it possible to verify the strict refinement more efficiently.

The main result of this paper is the theorem claiming that the strict refinement of a component-based system can be established by checking the weak refinement of its expanded components viewed as the modules. The main advantage of the component-based refinement we have been developing is that it allows us to master the complexity of specifications and verifications with a step by step development process without building the whole system. All steps of our compositional approach have been implemented in an analysis tool called SynCo [9].

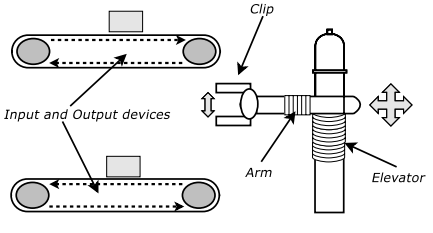

Fig. 2. Production Cell

The main concepts of the paper are illustrated on an example of a simple controller of a production cell moving pieces from an input device to an output device. A pictorial representation of this running example is given in Fig.2. The cell is composed of an arm having horizontal moves, a clip, and an elevator moving vertically. Sensors notify the controller about the production cell changes.

This paper is organised as follows. After giving preliminary notions, we recall in Section 2, the semantics of our refinement relation and its properties. Then Section 3 presents the modules, their composition and the weak refinement of the composition of the modules, called modular refinement. In Section 4, the constraint synchronised product is