Simulation Modelling Practice and Theory 66 (2016) 1–15

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

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

A new specification-based qualitative metric for simulation model validity

D. Foures[a,b], V. Albert[a,b], A. Nketsa[a,b,*]

[a] CNRS; LAAS; 7 avenue du colonel Roche, F-31077 Toulouse, France
[b] Université de Toulouse, UPS, INSA, INP, ISAE, LAAS, F-31077 Toulouse, France

ARTICLE INFO

Article history:
Received 14 May 2014
Revised 25 February 2016
Accepted 7 March 2016
Available online 26 March 2016

Keywords:
Experimental frame
Abstraction
Input/Output Automata
Compatibility

ABSTRACT

Informal validation techniques such as simulation are extensively used in the development of embedded systems. Formal approaches such as model-checking and testing are important means to carry out Verification and Validation (V&V) activities. Model-checking consists in exploring all possible behaviors of a model in order to perform a qualitative and quantitative analysis. However, this method remains of limited use as it runs into the problem of combinatorial explosion. Testing and model-checking do not take into account the context of use objectives of the model. Simulation overcomes these problems but it is not exhaustive. Submitted to simulation scenarios which are an operational formulation of the V&V activity considered, simulation consists in exploring a subset of the state space of the model. This paper proposes a formal approach to assess simulation scenarios. The formal specification of a model and the simulation scenarios applied to that model serve to compute the effective evolutions taken by the simulation. It is then possible to check whether a simulation fulfills its intended purpose. To illustrate this approach, the application study of an intelligent cruise controller is presented. The main contribution of this paper is that combining simulation objectives and formal methods leads to define a qualitative metric for a simulation evaluation without running a simulation.

1. Introduction

1.1. Context

In [1] it is stated that a model abstraction is valid if it maintains the validity of the simulation results with respect to the questions the simulation is supposed to address. Hence, the validity of a model should never be assessed in isolation but should always be envisaged in relation to the context in which the model is experimented, i.e. the purpose of the simulation. Traditional Modeling and Simulation (M&S) practices describe abstraction choices when building up a model to provide documentation of its “domain of use” as suggested in [1–3]. These practices do not follow the same process for the intended purpose of the simulation. However, simultaneously conducting the same process for the model and its context would make it possible to define a priori the sufficient and necessary model required to reach an intended purpose and to check a posteriori whether a model can be used in various contexts. Thus, challenging issues in M&S are mostly related to

* Corresponding author at: CNRS, LAAS, 7 avenue du colonel Roche, F-31077 Toulouse, France. Tel.: +33 562258208.
E-mail addresses: dfoures@laas.fr (D. Foures), valbert@laas.fr (V. Albert), alex@laas.fr (A. Nketsa).

http://dx.doi.org/10.1016/j.simpat.2016.03.002
S1569-190X(16)00041-1/

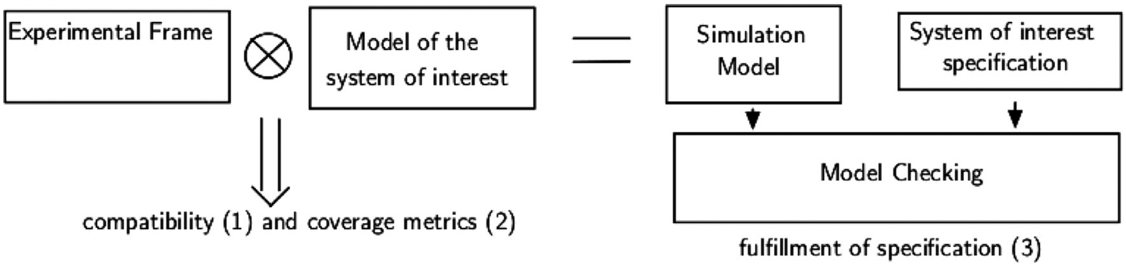

Fig. 1. Novelty of the concept.

their specification/documentation, the capabilities of the model and the properties expected from this model to achieve the simulation purpose.

1.2. Framework

We retained the Theory of Modeling and Simulation (TMS) developed in [4]. Zeigler established a framework which provides a precise definition of the entities involved in the process of modeling and simulation. We consider this framework as an excellent base for structuring modeling and simulation applications. It highlights relationships between the intended purpose of the simulation, the system which is represented and the simulations themselves. TMS is not the only existing framework available to describe dynamic system modeling. It can be compared with other work which has been published concerning the community of Verification, Validation and Accreditation (VV&A) of simulations as in [5,6]. The experimental frame is one of the entities that have been introduced in the TMS to make a distinction between the model and the experiment. The experimental frame can be viewed as a system which interacts with the model in order to answer the questions raised by the simulation purpose. Then it consists in stimuli injected into the model inputs, observation of the model outputs and constraints to determine whether the model outputs “fit” some acceptance conditions. The experimental frame concept has been used for the simulation of embedded systems engineering in [7], for ecology systems in [8,9] and for environmental processes in [10]. In [8], Traoré and Muzy pioneered a formal definition of the experimental frame. Our approach relies on this definition. However, this definition does not allow formal verification of the behavioral compatibility analysis between an experimental frame and a model. Such an issue is of paramount importance in order to know whether a model within an experimental frame can address the questions raised by the simulation purpose. Our approach is model-based. Therefore the experimental frame and the studied system are represented by their models. In this paper to avoid repeating the model word for both the system and the experimental frame, we are going to use a model for the system under test and experimental frame for its model.

1.3. Novel concept and its benefits

The novel concept relies on building a simulation model which specifies the model behavior under the conditions of the experiment. This model is obtained by *composition* of the system model of interest and the model of the context within which that system is studied, i.e. its experimental frame. In a simulation-based development methodology, the intended purpose of the simulation would usually be to check that some requirements on the real system are met. The simulation model and the simulation intended purpose can then be input into a model checker for quantitative analysis. This idea is illustrated in Fig. 1.

A simulation scenario consists of a trajectory injected into the model inputs and a path of interest observed on the model outputs. Typically a simulation is not comprehensive in the sense that it does not explore all possible trajectories of the model. A simulation scenario restricts the model to a subset of evolutions the model may produce. Then the simulation requires metrics which capture (1) the applicability of a scenario to a model, i.e. a set of stimuli can be accepted by the model and the model produces expected outputs, (2) the reliability of the simulation results, i.e. to what extent the state space of the model has been explored by the simulation, and (3) whether certain requirements of the real system are met by the simulation model.

Metrics (1) and (2) can be measured by composition of the system model of interest and the model of the experimental frame, and metric (3) can be measured by checking the simulation model against the specification of the system of interest.

1.4. Formal specification languages

TMS also offers a specification language for models called Discrete Event System Specification (DEVS) using precise operational semantics thanks to an abstract simulator which establishes formal rules for executing a DEVS model. It is important to highlight that TMS is based on a general system theory. In this way, many types of systems can be modeled within TMS. TMS has given rise to many subclasses such as Cell-DEVS for cellular automata, DTSS for discrete-time systems and DESS