PERFORMANCE VERIFICATION OF DISCRETE EVENT SYSTEMS USING HYBRID MODEL-CHECKING

Bruno Denis (1), **Jean-Jaques Lesage** (1), **Zulema Juárez-Orozco** (1), (2)

(1) LURPA-ENS de Cachan, France, {denis, lesage, juarez}@lurpa.ens-cachan.fr
(2) CIATEQ - Querétaro, Mexico, PhD grant financed by CONACYT (Mexico)

Abstract: The results generated over the past few years on the formal verification of both Discrete Event Systems (DES) and Hybrid Dynamic Systems (HDS) are quite substantial, especially as regards the controller's properties of liveness and safety. In this paper, we will study the range of possibilities offered using the model-checking techniques in order to evaluate DES performances (in terms of quality of service provided by the automated system). This task calls for proceeding with a model-based approach that couples a hybrid model of the plant with a timed discrete model of the controller. We will also show, using a basic example, that by parameterizing the hybrid process model, the model-checker may then be employed to evaluate the robustness of the discrete control to perturbations encountered by the plant. *Copyright © 2006 IFAC*

Keywords: DES controller, hybrid plant model, model-based verification, model-checking, linear hybrid automaton, HYTECH.

1. INTRODUCTION

A physical system is not, in most cases, intrinsically either purely discrete or purely continuous; instead, it's the abstraction the control engineer undertakes to ensure automation specification is being met that lends one distinction or the other. In the area of manufacturing systems for example, many processes have mobility axes that enable products to circulate, establish their position, etc.; consequently, some of the major physical variables controlled are either displacements or speeds. Depending not only on the level of quality to be guaranteed for these controlled variables, but also on the aggressiveness or variability in the external environment (e.g. type and importance of perturbations, parameter variation interval for the law of movement) and on the relative weight of economic constraints, the control engineer is required to choose between a servo control or a discrete control for each of these axes. Such automation-related choices will yield the physical variables to be observed and controlled by the controller, with either continuous or discrete control abstraction. Once the requisite displacement axis positioning quality has been achieved and provided that the perturbations encountered remain tolerable, the control engineer will then select a discrete control for obvious cost reduction reasons. This discrete displacement control, despite often being able to accommodate mobile positioning quality requirements, still constitutes an abstraction, and as such necessarily a simplification of the associated physical variables. The logic control of a linear displacement between two extreme positions, observed by means of two limit switch sensors, clearly does not enable ascertaining the precise position of the mobile, nor the time elapsed to complete this displacement.

Satisfying industrial system dependability requirements often necessitates conducting offline analyses, such as formal verification, before placing the automated system into operation (for further information on this topic, see the standard IEC 61508 entitled “ Functional safety of electrical / electronic / programmable electronic safety-related systems ”). These verifications, which are now frequently performed by means of model-checking (MacMillan, 1993), may be practiced by electing to incorporate or not a plant model.

In this paper, our efforts have focused on checking systems composed of a discrete controller coupled with a continuous (or partially-continuous) physical process whose entire set of observed and controlled variables constitute discrete abstractions of physical variables. To proceed, we will make use of model-checking techniques by coupling the discrete controller model with a hybrid plant model; this set-up will demonstrate that beyond the liveness and safety properties, it is indeed possible to check whether automated system performance is compatible with that stipulated in the specifications. We will also show that by parameterizing the hybrid process model, it becomes possible to use the model-checker to evaluate the robustness of discrete control to perturbations encountered by the plant.

This paper has been organized as follows. After having recalled the possibilities and limitations of both DES and HDS model-checking, we will introduce the expectations derived from a hybrid plant model for verifying a discrete controller. In order to illustrate our approach, the paper's second part will present the example of a positioning axis, which represents a component of a more complex assembly system. We will thus be able to show that use of a model-checker (such as HyTech), by implementation of a hybrid process model, makes it possible to verify the expected performance of this DES. Furthermore, a sensitivity study conducted on model parameters will allow evaluating the robustness of discrete control when confronted with perturbations.

2. ACQUIRED KNOWLEGE AND LIMITATIONS FROM AUTOMATED SYSTEM VERIFICATION

2.1 DES verification.

Formal verification techniques stem from the field of computer science. Only recently have they been adapted and applied to DES verification and, more specifically, to model-checking (Clarke E. M., *et al.*, 1986). The general principle behind model-checking may be expressed as follows (see Figure 1).

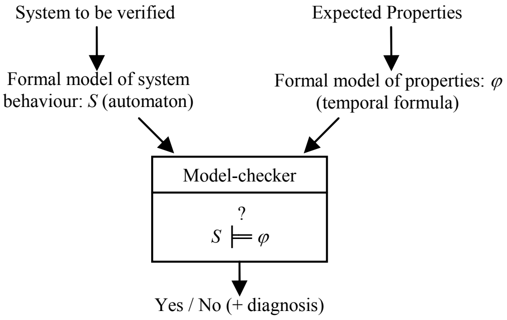
System to be verified
Expected Properties
Formal model of system behaviour: S (automaton)
Formal model of properties: φ (temporal formula)
Model-checker
$S \overset{?}{\models} \varphi$
Yes / No (+ diagnosis)

Fig. 1. Model-checking scheme.

Let's start with a system that has been designed to verify an entire array of properties (logical correctness, dependability, liveness, etc.). The first task of model-checking consists of formalizing system behavior in the form of a finite state automaton: S, plus the properties to be verified within a temporal algebra such as CTL (Emerson and Halpern, 1986): φ. The model-checker then conducts a thorough analysis of the state space reachable by S, which serves either to prove that $S \models \varphi$ (this algebraic statement denotes that "the system model satisfies the set of properties φ") or, when such is not the case, to propose a counterexample that revokes those properties not verified by S.

Moreover, a DES may be represented in a generic manner, as shown in Figure 2: a discrete controller acting in a closed loop on a plant. As part of a dependable controller design approach, the system being targeted for verification can thus be (according to Frey. and Litz, 2000) either the controller on its own, presumed to be operating within an open loop on the plant (a non "model-based" verification), or the {controller + plant} assembly set interacting within a closed loop ("model-based" verification).

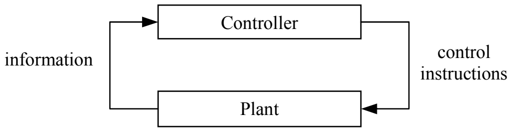

Fig. 2. A generic closed-loop DES.

The research work focusing on DES verification initially favored a non model-based approach (Moon I., 1994). The reachable state space of the controller model is thus to be built in the most permissive manner possible, i.e. such that the evolution of its inputs are in no way constrained by plant behavior. In this case, the safety properties capable of being demonstrated provide the basis for strong proof given that they can be demonstrated regardless of the evolution in controller inputs. On the other hand, a good number of liveness or accessibility properties cannot be demonstrated via a non model-based model-checking approach given the often fast-paced combinatory explosion of the reachable state space.

One means for reducing this combinatory explosion, using realistic constraints that depict the interaction of plant behavior with controller behavior, is to conduct a model-based verification. (Rausch and Krogh, 1998), (Machado, *et al.*, 2003).

Through reliance upon these results, we are now in a position to study the possibilities offered by the model-checking procedure in evaluating DES performance (in terms of quality of service provided by the automated system). To accomplish this task, it is necessary to undertake a model-based approach by selecting a hybrid plant model. The physical variables of the plant, and not their discrete abstraction by the controller, are what give the actual performance measures to be evaluated. The coupling of a hybrid plant model with a discrete controller model thus leads to a Hybrid Dynamic System (HDS) verification problem. We will now proceed by recalling the basic knowledge acquired and current limitations of HDS verification.

2.2 Hybrid systems verification.

While model design using hybrid automata is not exactly straightforward, their semantics is well-adapted to the analysis of HDS behavior. We will then assume that HDS verification is tantamount to exploring the reachable state space of a hybrid automaton. When framed as such, the fundamental