Partial Plant Models in Formal Verification of Industrial Automation Discrete Systems

José Machado
Departamento de Engª Mecânica/CT2M
Universidade do Minho
jmachado@dem.uminho.pt

José Creissac Campos
Departamento de Informática/CCTC
Universidade do Minho
jose.campos@di.uminho.pt

Abstract

The use of a plant model for formal verification of Industrial Automation systems controllers must be used in order to improve the obtained results. However, if there are some cases where the use of a plant model makes the formal verification results more realistic and robust, there are other cases where this does not always happen. The discussion presented in this paper is related with the need of using a Plant Model considering, not all of the Plant Model, but Partial Plant models in order to facilitate formal verification tasks of Industrial Automation Discrete Event Systems.

1. Introduction

Formal verification techniques stem from the field of computer science and are currently being applied to other fields like, for instance, Automation [1]. With formal verification approaches, the designers of automation systems controllers are able to guarantee more accuracy for their programs and they are also surer about the desired behavior for those systems. One of the most common techniques used in this field is model-checking [2].

When using model-checking the first task 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 [3]: φ. The model-checker then conducts a thorough analysis of the state space reachable by S, which serves either to prove that S $\models$ φ "the system model satisfies the set of properties φ ".

A DES may be represented in a generic manner, as shown in Figure 1: a discrete controller acting in a closed loop on a plant.

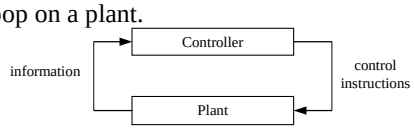

Figure 1. A generic closed-loop DES.

As part of a dependable controller design approach, the system being targeted for verification can thus be [4] 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).

One problem with model-cheking is related to the state explosion problem. The state of the model may become too big for verification to be feasible with reasonable resources. In this paper we report on results of work on mode-based verification resorting to partial models of the Plant. This enables the use of smaller models, thus making it possible to verify larger systems.

This solution allow us, also, the stronger proof of safety properties that will be as stronger as much as the plant model is reduced [5].

2. Example

The chosen system for this case study lies in the well-known category of "pick-and-place" systems (Figure 2); its function is to take parts, fed by gravity into three feed chutes, for placement in a single unloading chute. Sensors pp1, pp2 and pp3 indicate the presence of a part in one of the feed chutes, while sensor pp0 signals the presence of a part in the unloading chute. The device that enables picking and placing a part is composed of a group of three pneumatic cylinders plus a vacuum suction cup system. The vertical cylinder (VC) places the suction cup in contact with a part. Longitudinal cylinders L1C and L2C are arranged in series to allow positioning the vertical cylinder VC in front of the four chutes (L2C stroke is twice as long as than L1C stroke). The four reached positions are thereby detected by position sensors s0, s1, s2 and s3. The depression in the suction cup is obtained by virtue of a venturi and detected by a vacuum sensor.

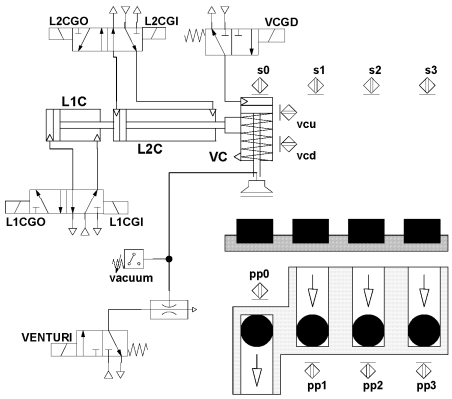

Figure 2. A generic closed-loop DES.

3. Formal verification step

Considering the approach proposed at [6] the formal verification tasks can be performed with the assumption of a closed loop behavior of the controller model and the plant model. Also, in the same work, it is proposed that a possible solution for obtaining the plant model for this system is considering a set of plant modules, and the solution proposed is the combination of twelve plant modules in order to obtain a modular solution for the entire system plant model.

In [5] a set of behavior properties for the exposed system is considered, to be proven using verification by Model-checking. This set of properties is composed by *safety properties* and *liveness properties*. The same work proposes a systematic approach to prove the set of properties using, or not, the plant model of the system, depending on the specific type of property under consideration. It was observed that some safety properties were not proved without a plant model, but were proved when the entire plant model was used.

Hence, in this paper, we analyze what happens if only a part of the plant model is used. For instance, consider the following behavior property:

- "*While the vertical cylinder is moving down, all the other cylinders stay in deployed or retracted position*".

This property cannot be proved without a model of the plant. With all the model of the plant, the property takes 109 minutes to prove [5], using the NuSMV model-checker, and a machine with a Pentium III processor at 1 GHz and 1 GB of RAM.

When we intend to prove the property, the use of the entire plant model is not a good solution, for both reasons: first, because the proof of safety properties will be as stronger as much the plant model is reduced [5] and, second, the global model is bigger and more difficult to analyze by the model-checker.

Considering this property, which deals only with the three cylinders of the system, it seems enough to use only the models of these three cylinders.

Using the same machine for calculations, the same Model-checker NuSMV and, now, considering a partial plant model - composed by the models of the three cylinders of the system - the property can be proved only in 12 minutes (about 10% of the time needed if the entire plant model is considered).

In fact, only these plant modules are enough to prove the property. However, it cannot be adopted as a systematic rule. The ongoing work is showing us that, for some properties, this rule cannot be applied.

4. Conclusions

In this paper it is illustrated that the consideration of partial plant models (instead of a global plant model) can be useful for formal verification of Industrial Automation Discrete Event Systems Controllers.

However, this is an ongoing work. Even if we can directly see the importance of this approach, we have not developed, yet, a systematic approach to finding out, quickly, which models must be considered in order to verify a specific behavior property of the system.

References

[1] I. Moon I. Modeling programmable logic controllers for logic verification. *IEEE Control Systems*, 14, 2, 1994, p. 53-59, 1994.

[2] B. Bérard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, and P. Schnoebelen. *Systems and software verification: model-Checking techniques and tools.* Springer, 190 pages, 1999.

[3] E.A. Emerson and J.Y. Halpern. Sometimes and Not Never revisited : on branching versus linear time temporal logic. *Journal of the ACM*, 33, 1, p. 151-178, 1986.

[4] G. Frey and L. Litz. Formal methods in PLC programming. Proceedings of the *IEEE Conference on Systems, Man and Cybernetics*, SMC 2000. Nashville, USA, 2000.

[5] J.Machado, B.Denis, and J.-J. Lesage. Formal Verification of Industrial Controllers: with or without a plant model? In *7th Portuguese Conference on Automatic Control (CONTROLO'06)*, pages 341-346, September 2006.

[6] J.Machado, B.Denis, and J.-J. Lesage. A generic approach to build plant models for DES verification purposes. In *8th International Workshop On Discrete Event Systems (WODES'06)*, pages 407–412, July 2006.