Available online at www.sciencedirect.com
ScienceDirect
Information Sciences 177 (2007) 1290–1308
INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL
www.elsevier.com/locate/ins

Fault diagnosis in discrete time hybrid systems – A case study

Prodip Bhowal [a], Dipankar Sarkar [b,*], Siddhartha Mukhopadhyay [c], Anupam Basu [b]

[a] *Investment Projects (Corporate Expert Group, Process Automation) Mittal Steel, Poland SA, Poland*
[b] *Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur 721 302, India*
[c] *Department of Electrical Engineering, Indian Institute of Technology, Kharagpur 721 302, India*

Received 21 December 2005; received in revised form 24 May 2006; accepted 1 August 2006

Abstract

A method of analysing diagnosability of discrete time hybrid systems (DTHS), which are similar to the simple *n*-rate timed automata [R. Alur, C. Courcoubetis, T.A. Henzinger, P. Ho, Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems, in: Hybrid Systems, LNCS 736, Springer Verlag, 1993, pp. 209–229], has been proposed. A state based fault modeling formalism is used. The properties of the DTHS model, under measurement limitations due to inadequacy or non-availability of sensors, are discussed. A definition of diagnosability for DTHS models has been adopted from the one proposed in [M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, D. Teneketzis, Diagnosability of discrete-event systems, IEEE Transactions on Automatic Control 40 (9) (1995) 1555–1575] for discrete-event system (DES) models. Based on the measurement limited DTHS models, an algorithm for construction of a diagnoser is presented. It is next demonstrated through an example of a chemical reaction chamber that the diagnosability condition (over the diagnoser), which has been shown to be necessary and sufficient for DES diagnosability, fails to hold for many systems. This is so because the abstraction employed in DES modeling obliterates an important feature of the transitions namely fairness. Exploiting the explicit continuous dynamics of the DTHS models, the fairness of transitions is identified and used to demonstrate diagnosability. The diagnosability condition over the diagnoser is suitably modified to encompass the situations typified by the example.

Keywords: Hybrid systems; Simple *n*-rate timed automata; Discrete time systems; Fault diagnosability; Diagnoser

1. Introduction

The analysis of fault diagnosability of a system comprises modeling its normal and faulty behaviours using a set of observable and unobservable events or a set of normal and fault states. The analysis consists in identifying whether the occurrence of faults can be inferred within a finite time of their occurrences based on observations of the system behaviour. The fault detection and diagnosis (FDD) problem for industrial processes has

* Corresponding author. Fax: +91 3222 55303/82700.
E-mail addresses: ds@cse.iitkgp.ernet.in (D. Sarkar), smukh@ee.iitkgp.ernet.in (S. Mukhopadhyay).

0020-0255/$ - see front matter
doi:10.1016/j.ins.2006.08.004

been studied using untimed and timed discrete-event system (DES) models [15,16,21,8,6,12,14,10,4,13], asynchronous DES [3], distributed diagnosis [17], stochastic automata [18], and hybrid dynamic system (HDS) models [7,19,11,2,9]. Usually industrial processes involve continuous variables which pure DES models cannot capture. DES modeling surmounts this problem by partitioning the continuous state space and capturing each subspace in the partition as a discrete state. It is, however, found through the example treated in this work that failure diagnosis using DES, with continuous dynamics completely abstracted out, leads to erroneous inferences. Hence, a discrete time hybrid system (DTHS) modeling framework is used in this work to develop a diagnosability analysis formalism. Decision problems for general hybrid system models are undecidable; simplifying restrictions are incorporated to achieve positive decidability results [1,5]. The framework adopted in this work is similar to the *simple n-rate timed automata* for which the emptiness problem is decidable [1].

Conventional design starts with constructing a detailed process model encompassing all the normal and faulty conditions by means of some hypothetical *status* variables; such variables obviously do not exist in reality. Moreover, in many real life situations, it may not be possible to provide sensors for even some process variables. Thus, the general problem of state estimation and the particular problem of FDD have to be addressed under some measurement limitation. The limitation can be captured either as a partition of variables into *measurables* and *unmeasurables* or a partition of events as *observables* and *unobservables*. In this work, the problem has been addressed using the partition of variables, which, in turn, induces a binary relation of *indistinguishability* of transitions. The diagnosability definition proposed in [15] for untimed DES models is adopted for DTHS models. A diagnoser construction algorithm using the indistinguishability relation over the transitions is then presented. The DES diagnosability condition (of absence of F_i-indeterminate cycles in the diagnoser), reported in the literature [15,20] as a necessary and sufficient condition for diagnosability, is then shown to fail for the diagnoser of a temperature and pressure controlled chemical reaction chamber. It is argued here that the failure is due to the fact that the abstraction employed in DES modeling obliterates the continuous dynamics. This, in turn, suppresses an important feature of some transitions called fairness. Specifically, transitions are said to be fair if they occur infinitely often in a model trace if the states they emanate from occur infinitely often in the trace.

The remedy suggested in [15] consists in associating *indicator events* to faults. The notion of indicator events is not formally defined. In the present work, a more intrinsic notion of *PF_i-diagnosability* is formulated. The method associates each fault F_i with some component process model P. Any F_i-uncertain diagnoser cycle is categorised as *PF_i-uncertain* if some state of the cycle changes any discrete variable of the component P. A continuous variable can change its mode (from a positive rate to a negative rate of change, or vice versa) only if there is a change in some (discrete) controller output fed as an input to the component. Now, in a cycle, which is not PF_i-uncertain, there is no change in any discrete (input) variables of P; hence, in such a cycle, some continuous variable changes unidirectionally and finally reaches a threshold whereupon the controller output changes forcing the diagnoser out of the cycle. Therefore, the presence of diagnoser cycles, which are not PF_i-uncertain, does not impair the model diagnosability, even if they are F_i-indeterminate. A suitable formalism including the diagnosability condition for PF_i-diagnosability is developed in this paper and demonstrated for the chemical reaction chamber example.

The paper is organized as follows. Section 2 presents the DTHS model. Section 3 discusses the characteristics of the process model under measurement restriction. Fault modeling and a formal definition of diagnosability, referred to in this work as *F_i-diagnosability*, are presented for such a model in Section 4. A diagnoser construction algorithm is discussed and the DES diagnosability condition involving F_i-indeterminate cycles over the diagnoser is reproduced in Section 5. In Section 6 an example of a chemical reaction chamber is introduced; the diagnoser is shown to violate the DES diagnosability condition. The notion of PF_i-diagnosability is introduced in Section 7 to alleviate the problem. It is finally shown how this new notion captures the diagnosability of the chemical reaction chamber of Section 6. The paper is concluded in Section 8.

2. Discrete time hybrid system model

The discrete time hybrid system (DTHS) *model M* is defined as $M = \langle V, X, t, \Im, \theta \rangle$, where $V = \{v_1, v_2, \ldots, v_n\}$ is a finite set of continuous and discrete data variables, X is a finite set of activity states similar to control locations of [1], t is a clock variable, $\Im$ is a finite set of transitions and θ is the initial condition.