ISA Transactions 53 (2014) 44–49

Contents lists available at ScienceDirect

ISA Transactions

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

Research Article

Safety analysis of discrete event systems using a simplified Petri net controller

Meysam Zareiee *, Abbas Dideban, Ali Asghar Orouji

Electrical Engineering Department, Semnan University, Semnan, Iran

A R T I C L E   I N F O

Article history:
Received 14 June 2013
Received in revised form
9 August 2013
Accepted 4 September 2013
Available online 24 September 2013

Keywords:
Discrete event system
Supervisory control
Controller synthesis
Petri net

A B S T R A C T

This paper deals with the problem of forbidden states in discrete event systems based on Petri net models. So, a method is presented to prevent the system from entering these states by constructing a small number of generalized mutual exclusion constraints. This goal is achieved by solving three types of Integer Linear Programming problems. The problems are designed to verify the constraints that some of them are related to verifying authorized states and the others are related to avoiding forbidden states. The obtained constraints can be enforced on the system using a small number of control places. Moreover, the number of arcs related to these places is small, and the controller after connecting them is maximally permissive.

1. Introduction

Discrete event systems (DESs) work based on changing states by occurring events [1]. Supervisory control is a theory which wants to restrict the behavior of the system for obtaining desired function [2,3]. The restriction can be performed by disabling some events in special conditions [4]. DESs can be modeled by Petri net (PN) where its compact structure, modeling power and mathematical properties have made it suitable for modeling this kind of systems [5,6]. Moreover, the PN can also model a large range of systems such as discrete, continuous and hybrid ones [7,8].

In DESs, there are some states which are called forbidden states and the system should be prevented from entering them. The reachable states without forbidden states are called authorized states. In recent years, a lot of researches have been accomplished for avoiding the forbidden states. Specifically, in flexible manufacturing systems (FMS) where deadlocks are major problems, a lot of methods based on PN models have been proposed to deal with deadlocks [9–16]. Some of them generate control places to prevent the system from entering the deadlock states. Particularly, many researchers construct generalized mutual exclusion constraints (GMEC) and enforce them on the system to satisfy a safety specification that specifies which evolutions of the system should not be allowed. However, achieving maximally permissive behavior after this enforcement is important. It means that all the authorized states should be reachable and all the forbidden states must be avoided. Giua et al., [17] have proposed a method for assigning GMECs to forbidden states in safe PNs which is developed in [18] and [19] for non safe PNs. Also, region theory is a useful method for generation of GMECs [20]. GMECs can be enforced on the system using control places [21]. When the number of GMECs is large, a large number of control places should be added to the system which leads to a complicated model. However, the number of control places can be reduced by considering PN structural properties [22–28]. In all the above methods, the conjunctions of the GMECs are enforced on the system, but, when the set of authorized states is nonconvex, the disjunctions of constraints can be enforced on the system [29].

In this paper, the aim is to develop the method in [25] for obtaining a small number of control places with small number of arcs in smaller time. For this reason, three types of Integer Linear Programming (ILP) problems are solved to classify the forbidden states in small number of sets where for each one of the sets, a GMEC is assigned. The first type problems try to classify the forbidden states in a small number of sets. For each one of these sets, a GMEC can be assigned but the number of arcs related to the control places may be large (in this step the number of control places is only reduced). So, the second type of ILP problems is designed to change the sets of forbidden states and obtain new sets. This leads to reducing the number of arcs of control places. At the end, by solving the third type of ILP problems, a GMEC is assigned to each one of the new sets. Enforcing these GMECs on the system leads to a maximally permissive controller with small numbers of control places and arcs. So, the structural complexity of the controller is reduced. Moreover, the hardware and software costs for implementing the controller

* Corresponding author. Tel.: +98 231 3354123; fax: +98 231 3366997.
E-mail addresses: mzareiee@semnan.ac.ir, meisamzareiee@gmail.com (M. Zareiee), adideban@semnan.ac.ir (A. Dideban), aliaorouji@ieee.org (A. Asghar Orouji).

0019-0578/$ - see front matter © 2013 ISA. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.isatra.2013.09.006

may be reduced. At the end, to show the advantages of the new method, some examples are introduced.

The rest of this paper is as follows. In Section 2, some important and basic concepts are introduced. The new method is explained in Section 3. In Section 4, experimental results are considered. Finally, conclusions are presented in Section 5.

2. Preliminary presentation

In this section, basic concepts and important definitions are presented which will be used later. It is supposed that the reader is familiar with the PNs basis [30], and the theory of supervisory control [2,3,31].

2.1. Petri nets

A PN is represented by a quadruplet $R=\{P, T, W, M_0\}$ where P is the set of places, T is the set of transitions, W is the incidence matrix and M_0 is the initial marking. Each marking of the PN can be shown by a vector as follows:

$$M^T=[m_1 m_2 m_3 \ldots m_n] \tag{1}$$

where, m_i is the number of tokens in place p_i and n is the number of places. M_R denotes the set of all reachable markings and is divided into two subsets: the set of authorized states M_A and the set of forbidden states M_F. M_F is separated into two groups: (1) the set of reachable states (M'_F) which either do not respect the specifications or are deadlock states. (2) The set of states for which the occurrence of uncontrollable events leads to the states in M'_F. The set of reachable states without forbidden states is the set of authorized states.

2.2. GMECs and enforcing them on the system using control places

GMECs are the constraints that restrict the weight sum of tokens in some places. The constraints can be assigned to forbidden states to prevent the system from entering these states [17–19]. Control places can be connected to the system for enforcing GMECs on the system. In this case, for each GMEC, a control place is added to the system. To explain how it is possible to calculate the control places, suppose that the incidence matrix and the initial marking of the system are W_P and M_{P0} respectively. The set of GMECs is considered as $L\times M_P \le b$ where M_P is the marking vector, L is a $n_c\times n$ matrix, b is a $n_c\times 1$ vector, n_c is the number of GMECs and n is the number of places. For each GMEC, a row is added to W_P. These rows are considered in matrix W_c and are calculated as follows [21]:

$$W_c=-LW_P \tag{2}$$

So, the incidence matrix of the system after connecting the control places is in the following form:

$$W=\begin{bmatrix} W_P \\ W_c \end{bmatrix} \tag{3}$$

The initial marking of the control places are calculated as follows:

$$M_{c0}=b-LM_{P0} \tag{4}$$

Therefore, the initial marking of the controlled system is in the following form:

$$M_0=\begin{bmatrix} M_{P0} \\ M_{c0} \end{bmatrix} \tag{5}$$

The set of places in a PN model of an FMS is classified into three groups: Idle, Operation and Resource places, respectively. To calculate the set of GMECs (control places), the markings of operation places should be only considered [13]. This concept leads to reducing the numbers of states that should be verified or forbidden by the controller [19] which simplifies the computations for constructing the GMECs. The reduced sets of authorized and forbidden states are denoted as M_{C-A} and M_{O-F}, respectively.

When the number of GMECs is large, a large number of control places should be added to the system which complicates the model. In the next section, a method is proposed for obtaining a small number of control places with small number of arcs which is maximally permissive.

3. New approach for obtaining a small number of control places with small number of arcs

In this section, the objective is to obtain a small number of simple GMECs which enforcing them on the system leads to obtaining a small number of control places and small number of related arcs. So, the objective is to modify the method in [25]. To do this, at first step we consider a set of safe constraints (with unknown variables) where each one of these constraints are for verifying an authorized state, and also a set of unsafe constraints (with unknown variables) at which each one of these constraints is for avoiding one of the forbidden states. Verifying all the safe constraints leads to verifying all the authorized states and verifying each one of the unsafe constraints leads to avoiding the related forbidden state. Then, we solve an ILP problem to obtain the unknown variables by verifying all the safe constraints and the largest number of unsafe constraints and we save the answer in a set like W_1. Next, the verified unsafe constraints should be eliminated from the set of unsafe constraints and should be saved in a new set (for example we call this set as R_1). If the set of unsafe constraints is not empty, we repeat this step again for the remaining unsafe constraints and save the answer in a set like W_2 that verify all the safe constraints and the largest number of remaining unsafe constraints. The new verified unsafe constraints should be eliminated from the set of unsafe constraints and must be considered in a new set (we call this set as R_2). Then, we solve another ILP problem which verifies all the safe constraints and all the unsafe constraints in the set R_2 and the largest number of unsafe constraints in R_1 and replace this answer by the answer in W_2 (in this ILP problem a constraint is added that do not permit the right side of the obtained GMEC increase more than before. For example suppose that the obtained GMEC in this step should be in this form: $k_1+k_2+\ldots+k_n\le x$, and the number in the right side of the obtained GMEC in the last step is 5. So, the constraints $x\le 5$ is added to the ILP problem. This constraint can be lead to reducing the number of arcs and their weighs). The verified unsafe constraints should be eliminated from R_1 and should be added to R_2. If the set of unsafe constraints is not empty, we do these steps for the remaining unsafe states (in this case, if we are in step t, we consider $R_1\cup R_2\cup\ldots\cup R_{t-1}$ instead of R_1). When the set of unsafe constraints is empty, for each one of the sets R_1, R_2, …, R_{t-1} (by considering that this is repeated t times), other ILP problems should be solved to verify all the safe constraints and all the constraints in R_e ($e=1, 2, \ldots, t-1$) and replace the answer in W_e ($e=1, 2, \ldots, t-1$). This concept is formalized and generalized in Algorithm 1.

Algorithm 1. Obtaining a small number of control places with small number of arcs

Input: The set of authorized states $M_A=\{[z_{11}\ z_{12}\ \ldots\ z_{1n}], \ldots, [z_{r1}\ z_{r2}\ \ldots\ z_{rn}]\}$ and the set of forbidden states $M_F=\{[B_{11}\ B_{12}\ \ldots\ B_{1n}], \ldots, [B_{t1}\ B_{t2}\ \ldots\ B_{yn}]\}$.

Output: The small number of control places with small number of arcs.