PERGAMON

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Automatica 39 (2003) 1695 – 1706

automatica

www.elsevier.com/locate/automatica

Robustness of deadlock avoidance algorithms for sequential processes☆

Fu-Shiung Hsieh

Overseas Chinese Institute of Technology, 100 Chiao-Kwang Road, Taichung, Taiwan

Received 13 June 2002; received in revised form 3 March 2003; accepted 2 May 2003

Abstract

Although deadlock avoidance issue has attracted much attention and has been extensively studied, most of the existing results assume reliable machines. This assumption makes it difficult to apply existing deadlock avoidance algorithms to real manufacturing systems with unreliable machines. This paper presents the results to apply an existing deadlock avoidance algorithm to systems with unreliable machines by analyzing the robustness of the deadlock avoidance algorithm. Sequential production processes are considered in this paper, and Petri Net is adopted as the tool for modeling and analysis of the sequential processes. Different types of tolerable machine failures under which liveness property can be preserved are characterized. Computational complexity of the proposed algorithm is analyzed.

Keywords: Deadlock; Flexible manufacturing systems; Algorithms; Robustness

1. Introduction

Deadlock is a highly undesirable situation in which a set of parts or jobs are requesting or waiting for resources held by other parts or jobs in the same set, with the set of parts or jobs in circular waiting. In the context of manufacturing systems, deadlock issue has attracted much attention in the last decade (Lawley & Sulistyono, 2002; Hsieh, 2000; Wu, 1999; Reveliotis, 1999; Lawley, 1998; Lawley, Spyros, Reveliotis, & Placid,1998; Reveliotis, Lawley, & Ferreira, 1997; Cho, Kumaran, & Wysk, 1995; Ezpeleta, Colom, & Martinez, 1995; Hsieh & Chang, 1994; Wysk, Yang, & Joshi, 1991; Banaszak & Krogh, 1990; Viswanadham, Narahari, & Johnson, 1990). Banaszak and Krogh (1990) proposed a production Petri net (PPN) model and developed a simple and low computational complexity deadlock avoidance restriction policy. Hsieh (Hsieh & Chang, 1994) overcame the drawbacks of the above approach by formulating a deadlock avoidance controller (DAC) synthesis problem for a class of Petri net called CPPN. Ezpeleta et al. (1995) formulated a policy that prevents deadlocks by establishing the equivalence between deadlocks and unmarked siphons in a class of Petri net called S^3PR. Wysk et al. (1991) and Cho et al. (1995) proposed graph-theoretic models for deadlock detection and avoidance of manufacturing systems.

Reveliotis, Lawley and Ferreira proposed polynomial complexity deadlock avoidance policies for sequential resource allocation systems (RAS) in Reveliotis et al. (1997).

The authors identified four significant classes of sequential manufacturing systems: (1) the single-unit RAS, where every process stage requires only one unit from a single resource for its successful execution; (2) the single-type RAS, where every process stage requires an arbitrary number of units, however, all of the same resource type, for its successful execution; (3) the conjunctive (AND) RAS, where every process stage, to be successfully executed, requires the simultaneous exclusive service of an arbitrary number of units of different resource types; and (4) the disjunctive/conjunctive (AND/OR) RAS, where every stage is associated with a set of conjunctive requests, the implication being that satisfaction of any of these request by the system is sufficient for the successful execution of the step. The authors showed that for a large subset of single-unit RAS, the optimal deadlock avoidance problem can be solved in polynomial time when all the resource types are available in more than one unit. Lawley (1998) and Lawley et al. (1998) addressed the scalability, configurability and routing flexibility design issues of deadlock avoidance algorithms for manufacturing systems.

☆ A shorter version of this paper was presented at the 15th IFAC World Congress b'02, Barcelona, June 21–26, 2002. This paper was recommended for publication in revised form by Associate Editor Tor Arne Johansen under the direction of Editor Frank Allgower.

E-mail address: shie1210@ocit.edu.tw (F.-S. Hsieh).

0005-1098/03/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/S0005-1098(03)00176-6

Finally, Fanti, Maione, Mascolo, and Turchiano (1997, 2000) proposed several restriction policies based on digraph approach. The authors first derived necessary and sufficient conditions for deadlock occurrence and also characterized undesirable situation, called second level deadlocks, which will inevitably evolve to circular waits in the next future. Based on these results, the authors proposed several restriction policies (Restriction Policy 1–5) and compared their performance with DAA by simulation.

Most of the existing results assume reliable machines. This assumption is an unrealistic for most real manufacturing systems. Unreliable machines pose challenges in control of production processes as machine failure may bring the system to a dead state or deadlock and has negative impacts on scheduled production activities. Feasibility to tailor or modify existing deadlock avoidance algorithms for manufacturing systems with failure prone machines requires further study.

An interesting question is whether existing deadlock avoidance algorithms posses desirable robust properties to cope with uncertainties. In control theory, a controller designed for a plant often exhibits some degree of robustness with respect to the nominal system state. That is, as long as the unmodeled dynamics is within some safety margin, the real system remains stable using the nominal controller. This motivates the research of this paper to study whether there exists any safety margin within which a nominal deadlock avoidance algorithm still works. Is it possible to characterize the safety margin quantitatively? There is a lack of research regarding evaluation of the impacts of unreliable machines on the manufacturing systems under the supervisory control of deadlock avoidance algorithms. The goal of this paper is to quantitatively characterize the tolerable margin of a nominal deadlock avoidance algorithm. It will provide us much insights on development of deadlock avoidance algorithms for manufacturing systems with unreliable machines.

Although there are many literatures on modelling and design of production shop floor controllers (Jeng, 1997; Jeng & DiCesare, 1993; Zhou, DiCesare, & Desrochers, 1992; Zhou & DiCesare, 1989, 1991; Narahari & Viswanadham, 1985), Petri Net is chosen in this paper owing to its modelling power as well as analysis capability. Given a state or a marking in the terminology of Petri Net theory, sufficient liveness conditions for tolerable perturbation of marking are established. Each liveness condition represents a condition under which the perturbed system can be kept live under the deadlock avoidance algorithm. For different types of machine failures, different safety margins that guarantee the preservation of liveness property of the perturbed system are established.

This paper considers a class of sequential processes where there are different types of products are concurrently processed. Each operation may require more than one type of resources. Different operations of the same production process or among distinct processes may share and contend for the same type of resources. Operations of a process must satisfy a set of precedence and resource capacity constraints. We first propose a nominal controlled Petri Net model for this class of manufacturing systems. The Petri Net model can be obtained by merging resource Petri Net models with job Petri Net models. For the purpose of DAC synthesis, we then add several control places into the Petri Net to obtain the controlled production Petri Net (CPPN) model. The CPPN model proposed in this paper is largely the same as that of (Hsieh & Chang, 1994). We analyze the properties of CPPN by exploiting its structure.

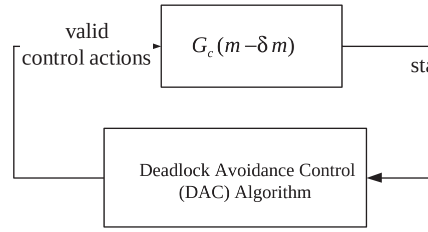

Fig. 1. A CPPN G_c with marking $m - \delta m$ under DAC algorithm, where δm denotes the set of tokens removed from nominal marking m due to machine failure and $0 \leqslant \delta m \leqslant m$.

The problem formulation is based on the nominal CPPN to avoid deadlocks under the deadlock avoidance control (DAC) algorithm proposed by Hsieh and Chang (1994). To model the unavailability of resources during the course of time-consuming (in comparison with processing times of operations) recovery procedures, a resource unavailability model is adopted. Resource unavailability models regard unavailability of resources as removal of tokens from nominal CPPN models. We define three types of token loss to model (1) resource failure at a single operational state, (2) resource failure at multiple operational states of a single type of production process and (3) resource failure at multiple operational states of multiple types of production processes. For each type of token loss, we establish sufficient condition that guarantees the liveness of the Petri Nets even if a subset of tokens are removed from the system. Our results include robustness analysis to characterize the tolerable uncertainties for CPPNs under DAC algorithm and computational complexity analysis. Fig. 1 is the block diagram of this formulation, where δm represents the set of unavailable resources that have been removed from the nominal state m of the CPPN model G_c under DAC algorithm.

The remainder of this paper is organized as follows. Section 2 formulates the deadlock avoidance problem for sequential production processes with unreliable machines based on Petri Nets. Section 3 presents the necessary and sufficient liveness conditions for sequential processes. Section 4 analyzes the robustness of the DAC algorithm with respect to resource failures at a single operational state. Section 5 analyzes the robustness of the DAC algorithm with respect to resource failures at multiple operational states. Appendix analyzes the computational complexity