DOI: 10.7641/CTA.2017.60910

自动制造系统的稳健控制方法的综述

杜 楠[1], 胡核算[1,2†]

(1. 西安电子科技大学 机电工程学院, 陕西 西安 710071;

2. 西安交通大学 机械制造系统工程国家重点实验室, 陕西 西安 710049)

摘要: 随着科学技术的快速发展, 制造自动化在制造工厂已经成为一个主流方向. 在过去的几十年中, 研究人员已经对自动制造系统的死锁问题做了大量的研究. 但是大多数解决方案总是假设分配的资源不会故障. 然而, 任何一个制造研究者都知道, 资源故障来自各种各样的原因, 包括工件破损、传感器故障、零件缺失和电器失灵等. 显然, 一旦资源发生故障, 后续加工路径中需要使用这个故障资源的进程将停滞, 不能完成其加工生产, 直到故障资源被修复. 那些不使用故障资源的支路也会被发生停滞的进程所阻塞. 最坏的情况就是一个简单的资源故障可能会导致整个系统的崩溃. 因此, 制造系统中的资源故障问题急需解决. 通过分析大量的文献资料, 本文对解决死锁和阻塞问题的控制方法做了系统的总结研究. 同时, 对本文提出的稳健无死锁控制策略以及亟待开展的研究工作做了详细的介绍.

关键词: 自动制造系统; 死锁预防; 资源故障; 稳健控制

引用格式: 杜楠, 胡核算. 自动制造系统的稳健控制方法的综述. 控制理论与应用, 2018, 35(1): 79 – 85

中图分类号: TP273 **文献标识码**: A

Review of robust control policies for automated manufacturing systems

DU Nan[1], HU He-suan[1,2†]

(1. College of Mechanical and Electrical Engineering, Xidian University, Xi'an Shannxi 710071, China;

2. State Key Laboratory for Manufacturing Systems Engineering, Xi'an Jiaotong University, Xi'an Shannxi 710049, China)

Abstract: With the quick development of science and technology, manufacturing automation plays a role of mainstay for the construction of manufacturing industries. Over the past decades, researchers have made tremendous achievements in understanding deadlock issues in automated manufacturing systems (AMSs); nevertheless, most of the deadlock avoidance or prevention methods have assumed that allocated resources never fail. In reality, as any practicing manufacturing researcher knows, resource failures derive from all kinds of causes, including tool breakages, sensor faults, part defects, component malfunctions, etc. Obviously, in case a resource fails undesirably, a process requiring the failed resource in its remaining route definitely cannot be accomplished unless the resource recovers. Moreover, a process not necessarily requiring the failed resource can be blocked innocently by this process. In the worst case, a single resource failure may paralyze the entire system. Therefore, resource failures in automated manufacturing systems need to be resolved forwardly. By surveying a large number of literatures, this paper summarizes the existing control approaches to resolving deadlock and blocking issues. Moreover, based on the reviews, our current and future research trends are pointed out in detail.

Key words: automated manufacturing system; deadlock prevention; resource failure; robust control

Citation: DU Nan, HU Hesuan. Review of robust control policies for automated manufacturing systems. *Control Theory & Applications*, 2018, 35(1): 79 – 85

1 引言(Introduction)

自动制造系统(automated manufacturing systems, AMSs)是指在较少的人工直接或间接干预下, 将原材料加工成零件或将零件组装成产品, 并在加工过程中实现管理过程和工艺过程自动化. 为了迎合激励的市场竞争和频繁的产品变化, 自动制造系统已经在增加生产效率、优化产品质量和降低成本等方面取得了巨大的发展. 自动制造系统往往是由许多小规模的、局

收稿日期: 2016−11−30; 录用日期: 2017−04−19.

†通信作者. E-mail: huhesuan@gmail.com; Tel.: +86 15291862950.

本文责任编委: 赵千川.

国家自然科学基金项目(61573265, 61203037, 51305321), 新世纪优秀人才支持计划项目(NCET–12–0921), 新加坡教育部Tier1科研基金项目(2014–T1–001–147), 新加坡教育部Tier2科研基金项目(MOE2015–T2–2–049)资助.

Supported by the National Natural Science Foundation of China (61573265, 61203037, 51305321), New Century Excellent Talents in University (NCET–12–0921), the Academic Research Fund Tier 1 by Ministry of Education in Singapore (2014–T1–001–147) and the Academic Research Fund Tier 2 by Ministry of Education in Singapore (MOE2015–T2–2–049).

部的、交互的、异步的以及事件驱动的并发子系统和一系列的资源(数控机床、机器人和自动处理设备等)构成. 考虑到系统的体积和资源的成本, 资源不会具备无限的供应. 因而高度的资源共享在自动制造系统中变得非常普遍. 由于子系统之间竞争有限的共享资源, 导致并不期望的情况发生, 如死锁和阻塞. 因此, 促使了监督控制理论的产生与发展.

绝大多数自动制造系统可以归类为离散事件系统, 对于自动制造系统的控制问题属于离散事件系统监督控制理论, 是自动化学科的重要分支, 一个相对年轻的学科, 并且有着广泛的应用前景. 在过去的几十年中, 学术研究者已经研究了大量的解决系统死锁的问题, 并形成了很多解决方案. 大多数的解决方法总是假设分配的资源不会发生故障, 然而事实并非如此. 在实际生产中, 资源故障是十分常见的现象, 比如信号丢失、传感器故障、电器失灵和工件损坏等. 因此, 根据资源是否会发生故障, 将它们分为可靠和不可靠的. 显然, 一旦资源发生故障, 后续加工路径中需要使用这个故障资源的进程将停滞, 不能完成其加工生产, 直到故障资源被修复. 同时, 那些不使用该故障资源的支路也会被发生停滞的进程所阻塞. 在最坏的情况下, 一个简单的资源故障, 可能会导致整个系统的崩溃. 因此, 排除行为上较低水平的控制问题, 稳健性是控制问题中另一个重要的因素. 对于一个可能发生资源故障的系统, 即使在不可靠资源发生了故障的情况下, 不使用故障资源的支路仍然可以进行加工生产, 那么称这个系统是稳健的.

本文首先通过一个简单自动制造系统实例阐述由资源故障引起的阻塞问题. 然后, 在分析大量文献资料的基础上, 对自动制造系统的稳健无死锁控制方法进行了总结和分析. 最后, 着重对本文提出的一种稳健无死锁控制策略做了详细的说明, 分析了其优势和不足, 并指出了未来将会在哪些方面做进一步的研究.

2 一个典型的自动制造系统 (A typical automated manufacturing system)

通常, 自动制造系统中包含了许多个加工进程, 每一个加工进程负责生产不同的工件. 当一个进程由于系统资源受到损坏而不得不中断时, 人们总是希望其他进程不被中断影响而继续顺畅地进行加工任务. 然而, 在现实生产中, 情况并非如此.

图1是一个带有不可靠资源的自动制造系统[1]. 在该系统中, 每一种产品由一个进程加工完成. 这个系统拥有以下几个特征: 每一个工作站代表一种资源, 它拥有若干存储单元(或缓冲器)和一个处理器(或服务器), 分别用来存放和加工工件. 如果资源发生故障, 意味着那台工作站的服务器不能使用而缓冲器仍然可以放置待加工的工件, 待加工的工件不会被破坏. 进一步讲, 可以继续往这个缓冲器中放置待加工的工件直到达到容量的上限. 被故障资源加工完成的工件可以离开工作站进行下一阶段的加工, 而待加工的工件却不能被当前服务器加工, 更不能被后续资源加工, 直到这个资源的服务器被修复. 不失一般性地, 假设只有在服务器正在加工的时候故障才可能发生.

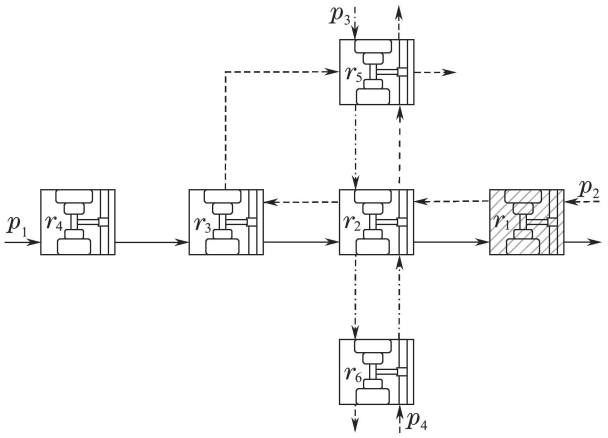

图 1 带有不可靠资源的自动制造系统

Fig. 1 An automated manufacturing system with unreliable resources

在该自动制造系统中, 根据是否使用不可靠资源, 将所有的加工进程区分为两类, 一类是需要使用不可靠资源的进程, 一类是只使用可靠资源的进程. 当前者发生了中断, 后者的加工不应该受到负面的影响. 然而, 事实并非如此. 图1可以模拟一个具有不可靠资源的自动制造系统的加工情况. 该系统中有4 种加工类型, 即P_1, P_2, P_3和P_4, 它们在该自动制造系统中同时被加工, 分别对应有序的加工阶段为: $P_1 = \langle P_{11}, P_{12}, P_{13}, P_{14}\rangle$, $P_2=\langle P_{21}, P_{22}, P_{23}, P_{24}\rangle$, $P_3=\langle P_{31}, P_{32}, P_{33}\rangle$和$P_4=\langle P_{41}, P_{42}, P_{43}\rangle$, 这里$P_{ik}$代表第$i$个加工类型的第 k 个加工阶段. 该系统有6种类型的资源r_1, r_2, r_3, r_4, r_5和r_6, 其中r_1是不可靠资源而其他都是可靠资源. 这些资源中, 除了r_2的缓冲器存储单元为2, 其余都为1. 用T_i表示第i个加工类型的加工路径, 这4种加工类型的加工路径分别为: $T_1=\langle r_4, r_3, r_2, r_1\rangle$, $T_2=\langle r_1, r_2, r_3, r_5\rangle$, $T_3=\langle r_5, r_2, r_6\rangle$和$T_4=\langle r_6, r_2, r_5\rangle$. 假设系统加工到某一状态, 资源$r_1$中拥有加工阶段$P_{14}$, 资源$r_2$中拥有加工阶段$P_{13}$和$P_{22}$, 资源中$r_3$拥有加工阶段$P_{23}$, 资源$r_5$中拥有加工阶段$P_{31}$. 明显地, 本文并不希望系统到达这个状态. 一旦r_1在此刻发生故障, 首当其冲的是P_1和P_2, 因为它使用了故障资源r_1而不得不被终止. 然而不使用故障资源的P_3和P_4也被迫中断加工, 这是因为加工阶段P_{14}停滞在故障资源r_1处, 从而导致P_{13}不能前进到r_1中, 并因此不能释放资源r_2, r_2中没有多余的存储单元, 致使P_{31}停滞在资源r_5中, 也因此导致P_{23}停滞在资源r_3中. 尽管这个例子很简单, 却为阐明故障资源问题的重要性提供了科学证据. 在现实的系统中, 上百台机器同时生

产大量的不同类型的工件, 完全可能因为某一个资源的故障导致全部生产停滞, 引发不可预想的后果. 由此, 自动制造系统中需要一个稳健的控制器, 用以保证系统安全地运行.

3 稳健无死锁控制的回顾(Review of robust deadlock-free control)

自动制造系统可以归类为离散事件系统, 对于自动制造系统的控制属于离散事件系统监督控制理论. 相比较连续系统的控制理论, 离散事件系统的控制理论既有相类似的基础, 又有诸多不同. 通过将事件区分为可控事件、不可控事件、可观事件和不可观事件, 监督控制器可以禁止某些事件的发生来实现控制目标. 监督控制器不会强迫特定事件发生, 而是通过观测事件发生序列, 禁止一些不安全事件的发生, 从而确保系统的安全运行.

尽管这个领域已经有大量的研究, 但是很少有研究者讨论资源故障的问题, 而资源故障的发生又是难以预测的. 如果对资源状态没有精确的预测, 控制器很难以最优的方式进行中断风险的管理. 根据资源是否会发生故障, 资源将被分为可靠和不可靠的. 这将有助于控制器在资源发生故障的时间段内做出最优的调度决策. 下面在总结现有文献的基础上分别讨论各种稳健无死锁控制方法.

3.1 基于自动机的稳健无死锁控制(Robust deadlock-free control based on automata)

在监督控制理论范畴, Ramadge和Wonham应用形式语言和自动机为数学工具, 率先提出了诸多基本的控制理论和方法[2]. 基于自动机, 一个自动制造系统被表示为一个有限状态自动机, 其中的节点代表了状态, 而弧线代表了事件, 事件的发生表示了工件在不同状态之间的转移. 通过遍历所有的系统状态, 导致死锁和阻塞状态的事件总是被提前检测并禁止.

将自动机作为数学工具, 文献[3]研究了一种容错的稳健控制器, 它是由一系列的事件序列构成的. 该控制器存在的合理性通过一个充分必要条件来说明. 文献[4]研究了具有单一不可靠资源的自动制造系统. 通过结合升级的资源顺序策略(resource order policy)和邻近限制策略(neighbourhood constraint policy), 确保系统中不需要故障资源的进程可以继续加工. 文献[5]同样针对具有单一不可靠资源的自动制造系统, 研究了两种稳健监督控制器. 一种是结合升级的银行家算法和邻近限制策略; 另一种是结合单步向前预测策略(single-step look-ahead policy)和邻近限制策略. 通过合理地分配资源, 确保系统遇到资源故障时, 不需要故障资源的进程能够继续地加工. 文献[6]放松了限制, 假设系统中有多个不可靠资源, 但是每条加工路径中有且仅有一个. 使用与文献[5]中类似的两种监督控制器, 通过合理地分配资源, 达到控制的目的. 文献[1]研究了一种新的控制无阻塞的方法. 通过使用共享资源缓存空间, 一旦资源发生故障, 需要使用故障资源的工件就会暂时进入到缓存空间中储存起来, 从而确保不需要故障资源的工件继续加工. 在同一时间内, 该方法只允许一个不可靠资源发生故障. 文献[7]针对一条路径中可以使用多个不可靠资源的系统研究稳健控制器. 利用路径分割算法(route partitioning algorithm), 使每条分割后的子路径只使用一个不可靠资源. 通过引入中央缓冲器, 并和文献[5]的两个控制器分别结合, 研究出两种新的控制器. 当多个不可靠资源同时故障时, 需要使用故障资源的工件就会进入到中央缓冲器中, 被占用可靠资源就会被释放, 从而确保不需要故障资源的进程继续加工. 文献[8]中应用与文献[3]中相类似的方法, 解决控制系统中同时出现多个不可靠资源的情况. 文献[9]研究了容错控制问题. 首先, 对于具有故障模式的离散事件系统, 提出了一种新的建模结构; 然后, 分别对完全事件可观测和部分事件可观测的系统, 提出了充分必要条件, 当故障发生时, 可确保系统避免不安全的状态; 最后, 针对具有多个故障的系统进行建模并控制. 文献[10]为具有不可靠资源的自动制造系统提出了一种死锁避免方针. 通过使用改进的银行家算法和预测有用资源的缓冲空间, 合理地分配资源以确保系统无死锁无阻塞的加工. 该方法对于系统的许可性有一定的改善. 文献[11]使用了一种类似于文献[3]中的制造系统结构, 研究出两种升级的银行家算法, 利用分布式的方式解决多个资源同时故障的问题. 文献[12]研究了由具有非确定性输出函数的Mealy 状态机建模的离散事件系统的非阻塞监督控制问题. 基于反许可方针 (anti-permissive policy), 作者研究了一种反许可监督控制器, 只要满足所提出了充分必要条件, 该控制器就能实现对系统的稳健无阻塞控制. 文献[13]提出了一种迭代的计算方法, 针对完全事件可观测的离散事件系统, 研究了稳健无阻塞控制策略. 该方法可以实现系统的最大许可性. 文献[14]分别针对具有相同和不同控制规格要求的离散事件系统, 提出了稳健控制的条件, 从而成功地解决了稳健控制问题.

3.2 基于Petri网的稳健无死锁控制(Robust deadlock-free control based on Petri nets)

由于Petri网的并发性和简约性, 被广泛地应用于自动制造系统的建模、分析和控制. 在过去几十年中, 研究者提出了许多基于Petri网的自动制造系统的死锁控制策略[15–21], 然而, 他们总是假设分配的资源不会故障, 很少有研究者考虑资源故障的问题. 接下来, 将回顾基于Petri网的稳健无死锁控制策略.

以Petri网为数学工具, 在文献[22–28]中, 作者对

一系列具有不可靠资源的Petri网结构做了详尽的分析与研究. 通过将使用故障资源的工件移出加工路径, 从而确保系统顺利地运行. 在这些文献中, 系统网的活性条件和稳健性分析是基于一些预定的限制条件. 最后通过一种结构分解的方法来验证系统运行的合理性. 文献[29]使用分而治之策略(divided-and-conquer strategy)提出一种基于Petri网的稳健无死锁控制方法. 通过给所有的不可靠资源以及使用不可靠资源的库所引入修复子网, 结合已经存在的控制信标非空的死锁避免方法, 实现稳健无死锁控制. 为了保证控制策略的可用性, 所有资源的缓冲空间必须大于1. 然而, 要执行该方法, 首先要遍历整个系统Petri网结构, 找到所有的信标. 事实上, 随着系统规模的增加, 信标数目将会以指数的方式增长. 文献[30]针对一种具有不可靠资源的复杂制造系统, 基于改进的银行家算法, 研究了一种稳健死锁避免策略. 文献[31]设计了一种稳健无死锁控制器. 首先, 引入资源故障和修复子网来描述资源的故障和修复; 然后, 给每一个严格极小信标引入限制集; 最后, 通过控制限制集中托肯的数量, 实现对系统的稳健无死锁控制. 相比较文献[30], 该控制器的结构复杂性简化了. 文献[32]中提出了一种稳健死锁避免控制器. 该控制器是由3种体系结构的控制器组成: 第1种是通过避免最大资源变迁回路(maximal resource transition-circuit) 饱和, 确保在没有资源故障时, 系统能够保持活性; 第2种控制器是针对使用不可靠资源的子网. 当资源故障时, 资源尽可能地被释放, 从而保证不需要故障资源的进程继续加工; 第3种控制器是阻止由第2种控制器所造成的死锁问题. 通过结合3种控制器, 确保系统稳健无死锁运行. 该控制器是以离线方式实现的. 文献[33]中提出了一种新颖的稳健无死锁控制策略. 通过预测剩余路径的资源需求和资源的状态, 判断是否有足够的资源支持相应的工件到达一个关键位置, 从而实现稳健无死锁控制. 该文献研究了一种带有资源的简单有序进程系统. 文献[34]在文献[33]的基础上, 研究了一种更复杂的系统结构, 即具有组合操作和灵活路径的自动制造系统. 通过实时地判断资源分配状态和预测剩余路径对资源需求, 确保系统进行稳健无死锁操作.

4 应用关键库所的稳健无死锁控制策略(Robust deadlock-free control policy using critical places)

事实上, 监督控制理论趋于完善的最大障碍就在于指数规模的计算复杂度. 基于以上文献分析可知, 许多监督控制方法严重地依赖于系统预定的、静态的进程路线以及资源分配方案. 它们禁止许多系统参数的变化, 如工件的加工要求、系统的加工能力或者系统运行期间的工作负荷. 很明显, 对于大规模的自动制造系统, 由于状态组合(可达图)爆炸和结构组合(信标)爆炸问题, 控制器的计算复杂度将变得无法想象. 当然, 研究人员在简化计算复杂度方面做了大量的研究, 但是大多数是以离线的和中心化的方式实现的. 因此, 这些方法几乎都没有能力处理具有动态路径和实时资源分配的系统, 从而不能应用到现实世界中去. 为了能更好地应用到实际生产中, 本文提出了一种新颖的稳健无死锁控制策略. 该控制策略适用于具有多个不可靠资源的自动制造系统, 相比较控制具有单个不可靠资源的系统[3–4], 本文提出的控制策略更具有普适性. 系统的大小和资源的成本一直是制造研究者考虑的主要因素, 尽管额外地增加缓冲器能够简化控制策略, 但是会给生产厂家带来一定的资源浪费, 不像文献[6–7]中提出的控制策略, 本文的策略不需要使用额外的中央缓冲器暂存工件, 而是通过实时地判断资源的状态和剩余路径中资源的数量, 在局部范围内, 判断工件能否安全地到达目标位置. 结构组合(信标)是最为经典的控制死锁的方法, 最近几年, 许多研究者对其进行深入地研究, 并形成了很多死锁控制策略[17]. 基于信标控制, 文献 [29,31]分别对具有不可靠资源的自动制造系统进行研究, 并提出相应的稳健无死锁控制策略. 事实上, 要执行该策略, 需要在离线的方式下遍历整个系统网, 从而找到所有的信标, 合成稳健无死锁控制器. 同时, 为了保证文献[29]中控制策略的合理性, 所有的资源缓存空间必须大于1. 相比较文献[29,31]中的控制策略, 本文提出的策略放松了假设(所有的资源缓存空间大于1), 在在线的方式下, 利用分布式的思想对系统进行实时的控制. 每一步的执行都是在局部范围内实现的, 不需要检索系统的全局信息. 因此, 系统的计算复杂度也大大地降低了. 相较于已经存在的稳健无死锁控制方法, 本文的控制策略具有限制条件少、实施成本低、适用性广泛等特点. 同时, 本文的控制策略能够适用于具有并发特性的复杂系统. 文献[33–34]对该策略做了初步的说明. 下面, 将对本文研究的稳健无死锁控制策略做进一步详细的介绍.

应用Petri网为数学工具, 本文的稳健无死锁控制策略将致力于避免遍历所有的系统状态, 从而有效地实现大规模系统的无阻塞控制问题. 该策略是一种在线的而非离线的、动态的而非静态的、柔性的而非刚性的、稳健的而非脆弱的监督控制策略, 使得它能适用于可能发生资源故障和(或)路径改变的系统. 用本文的方法, 资源故障和恢复没有给监督控制策略的执行或者控制系统的运行带来不利的影响. 不期望的资源故障和修复不受该控制方法约束, 因为它们被认为是正常的资源分配. 因而, 最终的控制系统是容错的, 而非故障敏感的. 同时, 去除和添加一些资源也不会影响该策略的运行. 这里所指的“ 故障”, 通常指资源

损坏, 需要从系统中移除进行修复和恢复. 一旦修复好之后, 就可以继续进行原来的加工.

传统的方法需要对所有结构的和行为的对象(如信标, 可达图)进行监督控制, 从而合成控制器. 由于结构和行为的对象是随着系统规模的增大以指数方式增长的, 所以不适用于高速发展的现代化大规模自动制造系统. 然而, 本文提出的策略在控制子系统或者执行单元时, 在没有必须要求达到最大许可行为的情况下, 将致力于避免指数级规模的运算和控制. 该策略使用一种预测分布式控制技术, 从而替代已有的中心式控制方法. 不失一般性地, 可以假设当任意进程正在进行特定操作时, 其他进程都暂时处于停止状态直到该操作执行完毕. 该控制器关注的是一条任意的或者刻意挑选的进程. 针对该进程, 控制器需要对其中一个托肯进行预测评估, 看其是否能够从当前位置到达一个特定的目标库所. 如果可以, 该托肯可以前进到下一个加工阶段; 否则, 它保持原有位置不变, 即使它能够向前移动一步. 由于这些特定的目标库所对控制策略的实现起到关键的作用, 所以它们被称为关键库所, 只要有足够资源支撑相应的托肯到达最近的关键库所, 该托肯才可以向前移动一步. 下面将会给出关键库所的详细说明.

在一个Petri网系统中, 根据所使用的资源的类型以及数量的多少, 将关键库所分成3种类型. 第1种是不使用任何资源的闲置库所. 对于该库所, 在拥有最小资源占有量的位置之后, 必然有着足够的资源支撑其他进程的加工; 第2种是在同一进程中使用资源最多的操作库所. 对于该库所, 在拥有最大资源占有量的位置之后, 必然不再需要更多的资源, 任何的活动只会是释放资源而不是占有更多的资源. 第3种是使用至少一种不可靠资源的操作库所. 对于该库所, 不可靠资源会突然地故障, 从而导致需要故障资源的进程停止加工. 本文提出的稳健控制策略是实时地判断是否有足够的资源支撑相应的托肯到达其最近的关键库所, 从而避免死锁和阻塞问题的出现. 因此, 在每一个可达状态下, 控制器需要确定哪一个变迁是可以被安全地发射并且哪一个状态是可以安全抵达的. 通过局部的仿真, 可以预测相关的托肯是否可以从当前库所前进到其最近的关键库所. 如果该仿真结果为真, 则该托肯前进一步, 且只能前进一步; 否则, 就必须暂停在当前位置, 进而对剩余托肯进行仿真, 直到存在一个托肯可以前进一步. 当托肯完成向前一步运动以后, 同样地, 控制器对其他进程中的托肯也需要进行仿真、筛选和决策, 使其中一个托肯完成向前一步运动. 这样的过程一步一步地迭代进行, 使系统从一个状态到达另一个新的状态. 从长远的角度看, 这些托肯并行交替地从初始位置前进至目标位置. 详细的实现方法如下所述.

为了方便说明, 将前两类关键库所称为无死锁关键库所, 第3类关键库所称为稳健关键库所.

首先, 不考虑资源故障, 那么稳健关键库所就不存在. 在任何一个可达状态下, 根据使能规则, 可以得到一系列使能变迁$T_{\rm EN}$. 在所有的使能变迁$T_{\rm EN}$中, 根据是否有足够资源支持相应的托肯到达其最近的无死锁关键库所, 可以得到一系列无死锁变迁$T_{\rm DF}$, 其中任何一个变迁的发射都不会造成系统死锁. 紧接着, 为了实现稳健无死锁控制, 从一系列保证系统无死锁的变迁$T_{\rm DF}$中, 挑选出一组可规避故障阻塞的变迁$T_{\rm RB}$. 这个过程是动态的和局部仿真的. 当一个变迁发射后, 导致托肯前进到只使用可靠资源的支路时, 该变迁将被归类到$T_{\rm RB}$中. 当一个变迁发射后, 导致托肯前进到需要使用不可靠资源的支路时, 这里分两个情况: a) 当前资源足够支持该托肯前进到使用该不可靠资源的稳健关键库所, 那么该变迁将被归类到$T_{\rm RB}$中; b) 当前资源不足够支持该托肯前进到使用该不可靠资源的稳健关键库所, 那么该变迁不能被归类到$T_{\rm RB}$中. 当该托肯正在使用不可靠资源, 该变迁发射后, 会导致托肯释放该资源. 这里又分两个情况: a) 该资源不可靠, 并且此时处于故障状态, 很明显, 这个变迁不能归类到$T_{\rm RB}$中; b) 该资源不可靠, 但是此时处于正常工作状态, 需要进一步分析. 假设在后续的加工路径中, 只使用可靠资源, 那么该变迁属于$T_{\rm RB}$; 假设后续加工路径中依然需要使用不可靠资源, 当前的资源也足够支持该托肯到达最近的稳健关键库所, 那么该变迁属于$T_{\rm RB}$; 相反地, 该变迁不能被归类到$T_{\rm RB}$中. 由此, 可以得到一系列稳健无死锁变迁$T_{\rm RB}$, 其中任意一个发射都不会造成死锁和阻塞问题的出现. 最后, 在所有的稳健无死锁变迁$T_{\rm RB}$中选择一个变迁并发射.

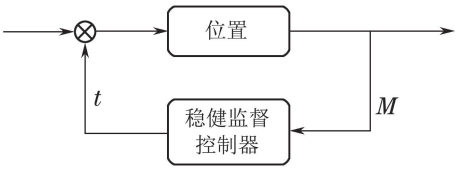

图 2　反馈闭环回路

Fig. 2　Feedback closed loop circuit

按照以上步骤所述, 本文的稳健无死锁控制策略可以用一个反馈闭环回路表示, 如图2所示. 在任何一个可达状态M下, 通过稳健监督控制器控制, 从一系列变迁中筛选出一个稳健无死锁变迁t并发射, 到达一个新的可达状态. 在新的状态下, 按照上述步骤, 继续执行. 就这样一步一步地迭代, 从一个状态到另一个状态. 最终, 这些托肯并行交替地从初始位置前进至目标位置. 在运行过程中, 一旦资源发生故障, 使用该故障资源的进程需要被停滞, 不使用该故障资源的进程可以继续地加工; 同时, 如果资源分配合理, 并且

故障资源还有空闲的缓冲存储空间, 需要该故障资源的工件仍然可以继续前进到这个故障资源的缓冲存储空间中进行临时存储, 目的是尽可能地释放占用的资源以便其他进程可以继续顺利地操作. 一旦故障资源恢复使用, 只要当前加工工件既可以前进到最近的无死锁关键库所, 又可以前进到最近的稳健关键库所, 那么该工件就可以加工到下一个位置.

不难看出, 本文提出的控制策略将对意外的中断和恢复进行稳健控制. 为了使系统具有容错能力, 该方法需具有足够的柔性和动态特性, 才能使得系统不受意外紧急事故的影响. 即在资源发生故障的情况下, 该方法不是为了诊断和(或)预测故障, 也不是为了修复故障资源; 相反, 该策略将不可靠资源的故障和修复看作是正常的资源分配, 资源的故障和修复不会给该控制策略带来不利的影响. 最终目标是使系统在任何时候都能保持顺利的运行. 因此, 本文的稳健无死锁控制策略满足:

1) 当不考虑资源故障时, 系统中不会出现任何死锁问题;

2) 一旦资源发生故障, 不需要故障资源的进程会继续顺利地运行;

3) 当故障资源被修复, 它会继续正常的运行, 不会给系统带来干扰.

由于自动制造系统中资源分配和占有的特殊性, 关键库所的存在是必然的. 在最坏的情况下, 只有每个进程的起始和终止位置是关键库所. 因为在这些位置, 资源占有量必然是最少的, 事实上为零, 也就是没有资源被占有. 虽然应用关键库所的控制方法在执行中的每一步仅仅关心局部结构和状态, 但是关键库所的存在必然性间接地确保了该方法的全局有效性. 换句话说, 在线控制解总是存在的, 不会出现系统运行几步后必然出现死锁的情况. 采用反证方法, 假设应用关键库所的控制方法出现了死锁, 意味着当前关心的托肯不能够前进到其所在进程的关键库所. 首先, 这种现象不符合应用关键库所进行控制的基本规则. 按照该规则, 当前关心的托肯既然不能到达最近的关键库所, 本身就不应该被选择并且往前推进的. 其次, 在当前状态下, 除了该托肯, 必然存在其他托肯, 可以使用当前资源, 前进到相应的关键库所. 在最坏的情况下, 就是导致系统运行到当前状态的那个托肯. 1) 如果该托肯的前进也会导致死锁, 则上述类似的反演推理可以迭代进行, 直到返回系统初始状态; 显然地, 在初始状态下, 必然存在托肯可以前进到其相应的关键库所包括终止位置, 而不会导致死锁. 2) 如果该托肯的前进不会导致死锁, 则该托肯可以前进一步, 引导系统进入一个新的状态; 最不理想的情况就是在新的状态下, 只有该托肯可以继续前进, 直到进入其相应的关键库所包括终止位置. 因此, 应用本文的稳健无死锁控制策略不会导致系统出现死锁和阻塞问题.

在上述文献中, 大多数都是以序列的线性系统结构作为例子(S^3PR[29,31], S^*PR[30], PPN[33]), 研究相应的稳健无死锁控制策略. 然而, 本文提出的控制策略的实现是基于系统中的关键库所, 无论是线性的系统, 还是非线性的系统(AMG[35], RCN[36], PNR[37]), 只要找到系统中的所有关键库所, 按照该控制策略, 合理地分配资源, 就能确保系统安全地运行[33–34].

对于基于结构和行为的中心化稳健无死锁控制方法, 大多数是在离线状态下, 通过遍历所有的系统状态, 禁止某些事件的发生, 从而确定相应的控制策略. 显然, 由于状态爆炸问题, 这些方法很难具有普适性和实用性. 相反, 本文提出的控制策略是以在线的、分布式的方式实现的, 不需要检索任何关于状态的或者结构的信息. 每一步的执行都在一个局部范围内实现. 相比较中心化的方法, 计算复杂度明显降低了. 然而, 任何事物都具有两面性, 本文提出的稳健无死锁控制策略也不例外. 根据该控制策略, 一个变迁的发射基于是否有足够的资源支撑相应的托肯进入到最近的关键库所. 由于一个进程上关键库所的数量是严格结构相关而状态无关的, 所以一些好的可达状态可能会被意外规避了, 从而系统的最大许可性得不到保证. 尽管算法复杂度大大地降低了, 但是系统的许可行为受到一定限制. 因此, 下一步的研究工作将致力于实现受控系统的最大行为许可性. 同时, 给库所和变迁引入确定的或者随机的时间变量, 对系统的性能进行评估并优化.

5 总结与展望(Conclusion and future work)

在监督控制领域, 对于自动制造系统的死锁问题, 研究者已经做了大量的工作. 然而, 他们总是假设分配的资源不会故障. 事实上, 制造系统中资源故障很容易发生. 本文在系统地分析与总结相关文献的基础上, 对本文提出的稳健无死锁控制策略做了详细的介绍. 通过引入关键库所的概念, 该策略以一种分布式的、在线的方式实现对系统的稳健无死锁控制. 与传统的方法相比, 控制器的计算复杂度有效地降低了. 下一步的研究工作将该方法推广到更具有普适性和实用性的Petri网模型中, 并致力于实现受控系统的最大行为许可性.

参考文献(References):

[1] WANG S Y, CHEW S F, LAWLEY M. Using shared-resource capacity for robust control of failure-prone manufacturing systems [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 2008, 38(3): 605 – 627.

[2] RAMADGE P, WONHAM W. Supervisory control of a class of discrete event processes [J]. *SIAM Journal Control Optimization*, 1987, 25(1): 206 – 230.

[3] PARK S, LIM J. Fault-tolerant robust supervisor for discrete event

systems with model uncertainty and its application to a work cell [J]. *IEEE Transactions on Robotics and Automation*, 1999, 15(2): 386 –391.

[4] LAWLEY M. Control of deadlock and blocking for production systems with unreliable resources [J]. *International Journal of Production Research*, 2002, 40(17): 4563 – 4582.

[5] LAWLEY M, SULISTYONO W. Robust supervisory control policies for manufacturing systems with unreliable resources [J]. *IEEE Transactions on Robotics and Automation*, 2002, 18(3): 346 – 359.

[6] CHEW S F, LAWLEY M. Robust supervisory control for production systems with multiple resource failures [J]. *IEEE Transactions on Automation Science and Engineering*, 2006, 3(3): 309 – 323.

[7] CHEW S F, WANG S Y, LAWLEY M A. Robust supervisor control for product routings with multiple unreliable resources [J]. *IEEE Transactions on Automation Science and Engineering*, 2009, 6(1): 195 – 200.

[8] CHEW S F, WANG S Y, LAWLEY M A. Resource failure and blockage control for production systems [J]. *International Journal of Computer Integrated Manufacturing*, 2011, 24(3): 229 – 241.

[9] SHU S L, LIN F. Fault-tolerant control for safety of discrete event systems [J]. *IEEE Transactions on Automation Science and Engineering*, 2014, 11(1): 78 – 89.

[10] YUE H, XING K Y, HU Z. Robust supervisory control policy for avoiding deadlock in automated manufacturing systems with unreliable resources [J]. *International Journal of Production Research*, 2014, 52(6): 1573 – 1591.

[11] YUE H, XING K Y, HU H S, et al. Robust supervision using shared-buffers in automated manufacturing systems with unreliable resource [J]. *Computers and Industrial Engineering*, 2015, 83: 139 – 150.

[12] USHIO T, TAKAI S. Nonblocking supervisory control of discrete event systems modeled by mealy automata with nondeterministic output functions [J]. *IEEE Transactions on Automatic Control*, 2016, 61(3): 799 – 804.

[13] YARI F, HASHTRUDI-ZAD S. Computational procedures for robust nonblocking supervisory control [C] //*Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering*. Vancouver: IEEE, 2016, 10: 15 – 18.

[14] WANG F, SHU S L, LIN F. Robust networked control of discrete event systems [J]. *IEEE Transactions on Automation Science and Engineering*, 2016, 13(4): 1528 – 1540.

[15] WU N Q, ZHOU M C. Avoiding deadlock and reducing starvation and blocking in automated manufacturing systems [J]. *IEEE Transactions on Robotics and Automation*, 2001, 17(5): 658 – 669.

[16] LI Z W, ZHOU M C. Elementary siphons of Petri nets and their application to deadlock prevention in flexible manufacturing systems [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 2004, 34(1): 38 – 51.

[17] LI Z W, WU N Q, ZHOU M C. Deadlock control of automated manufacturing systems based on Petri nets — A literature review [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Review*, 2012, 42(4): 437 – 462.

[18] WU N Q, ZHOU M C, HU G. Petri net modeling and one-step look-ahead maximally permissive deadlock control of automated manufacturing systems [J]. *ACM Transactions on Embedded Computing Systems*, 2013, 12(1): 1 – 23.

[19] HU H S, ZHOU M C, LI Z W, et al. Deadlock-free control of automated manufacturing systems with flexible routes and assembly operations using Petri nets [J]. *IEEE Transactions on Industrial Informatics*, 2013, 9(1): 109 – 121.

[20] HU H S, SU R, ZHOU M C, et al. Polynomially complex synthesis of distributed supervisors for large-scale AMSs using Petri nets [J]. *IEEE Transactions on Control Systems Technology*, 2016, 24(5): 1610 – 1622.

[21] HU H S, ZHOU M C. A Petri net-based discrete-event control of automated manufacturing systems with assembly operations [J]. *IEEE Transactions on Control Systems Technology*, 2015, 23(2): 513 – 524.

[22] HSIEH F S. Robustness of deadlock avoidance algorithms for sequential processes [J]. *Automatica*, 2003, 39(10): 1695 – 1706.

[23] HSIEH F S. Fault-tolerant deadlock avoidance algorithm for assembly processes [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 2004, 34(1): 65 – 79.

[24] HSIEH F S. Robustness analysis of Petri nets for assembly/disassembly processes with unreliable resources [J]. *Automatica*, 2006, 42(7): 1159 – 1166.

[25] HSIEH F S. Analysis of flexible assembly processes based on structural decomposition of Petri nets [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 2007, 37(5): 792 – 803.

[26] HSIEH F S. Robustness analysis of holonic assembly/disassembly processes with Petri nets [J]. *Automatica*, 2008, 44(10): 2538 – 2548.

[27] HSIEH F S. Collaborative reconfiguration mechanism for holonic manufacturing systems [J]. *Automatica*, 2009, 45(11): 2563 – 2569.

[28] HSIEH F S. Robustness analysis of non-ordinary Petri nets for flexible assembly systems [J]. *International Journal of Control*, 2010, 83(5): 928 – 939.

[29] LIU G Y, LI Z W, BARKAOUI K, et al. Robustness of deadlock control for a class of Petri nets with unreliable resources [J]. *Information Sciences*, 2013, 235(20): 259 – 279.

[30] YUE H, XING K Y, HU H S, et al. Petri-net-based robust supervisory control of automated manufacturing systems [J]. *Control Engineering Practice*, 2016, 54: 176 – 189.

[31] WU Y C, XING K Y, LUO J C, et al. Robust deadlock control for automated manufacturing systems with an unreliable resource [J]. *Information Sciences*, 2016, 346(c): 17 – 28.

[32] WANG F, XING K Y, HAN L B. A robust deadlock prevention control for automated manufacturing systems with unreliable resources [J]. *Information Sciences*, 2016, 345(1): 243 – 256.

[33] CHENG Y, HU H S, LIU Y. Robust supervisor synthesis for automated manufacturing systems using Petri nets [C] //*Proceedings of IEEE International Conference on Automation Science and Engineering*. Gothenburg: IEEE, 2015, 10: 1029 – 1035.

[34] DU N, HU H S. Robust control of backward conflict free systems with resources using Petri nets [C] //*Proceedings of IEEE International Conference on Automation Science and Engineering*. Fort Worth: IEEE, 2016, 11: 1034 – 1041.

[35] CHU F, XIE X L. Deadlock analysis of Petri nets using siphons and mathematical programming [J]. *IEEE Transactions on Robotics and Automation*, 1997, 13(6): 793 – 804.

[36] XIE X L, JENG M D. ERCN-merged nets and their analysis using siphons [J]. *IEEE Transactions on Robotics and Automation*, 1999, 15(4): 692 – 703.

[37] JENG M D, XIE X L, PENG M Y. Process nets with resources for manufacturing modeling and their analysis [J]. *IEEE Transactions on Robotics and Automation*, 2002, 18(6): 875 – 889.

作者简介:

杜　楠　(1991–), 男, 博士研究生, 主要研究离散事件系统的监督控制及应用, E-mail: dun@stu.xidian.edu.cn;

胡核算　(1977–), 男, 教授, 主要研究离散事件系统的监督控制及应用, E-mail: huhesuan@gmail.com.