DOI: 10.7641/CTA.2017.60929

逻辑控制器设计与离散事件系统监控理论

罗继亮[1,2†], 邵　辉[1,2], 吴维敏[3], 苏宏业[3]

(1. 华侨大学 信息科学与工程学院, 福建 厦门 361021; 2. 福建省电机控制与系统优化调度工程技术研究中心, 福建 厦门 361021;
3. 浙江大学 工业控制技术国家重点实验室 智能系统与控制研究所, 浙江 杭州 310027)

摘要: 物联网等通信技术将越来越多的控制元件集成起来, 导致系统规模快速增长, 逻辑控制规范也日益复杂, 任何逻辑错误都可能造成重大事故和人身灾难, 再加上“维数灾”问题, 安全可靠的逻辑控制程序的设计和调试面临巨大的计算复杂性难题. 而离散事件系统监控理论旨在研究复杂控制规范的设计和实现问题, 将连锁、互斥、字符串语言等复杂控制逻辑描述为自动机或Petri网, 然后转换为可编程逻辑控制器或现场可编程门阵列上执行的程序代码. 本文综述了现有的逻辑控制器的形式化设计方法, 主要涉及如何利用监控理论(自动机或Petri网)来缩短程序开发周期、提高程序可重用性和确保程序可靠性和安全性等问题.

关键词: 可编程逻辑控制器; 离散事件系统; 现场可编程门阵列; 监控理论

引用格式: 罗继亮, 邵辉, 吴维敏, 等. 逻辑控制器设计与离散事件系统监控理论. 控制理论与应用, 2018, 35(1): 86 – 91

中图分类号: TP273　　**文献标识码**: A

Synthesis of logical controllers and discrete-event systems supervisory control theory

LUO Ji-liang[1,2†], SHAO Hui[1,2], WU Wei-min[3], SU Hong-ye[3]

(1. College of Information Science and Engineering, Huaqiao University, Xiamen Fujian 361021, China;
2. Fujian Engineering Research Center of Motor Control and System Optimal Schedule, Xiamen Fujian 361021, China;
3. State Key Laboratory of Industrial Control, Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou Zhejiang 310027, China)

Abstract: More and more control elements are incorporated into a single system by the information technology such as internet of things. Consequently, the scale of a control system increases quickly, and the control specification becomes more and more complicated. Any logic mistake that violates a given control specification may lead to a serious industrial failure and even security issue. Besides, there is a “state space explosion” for discrete event systems. These make a challenge for designing and debugging programs running in programmable logic controllers (PLCs) or field programmable gate arrays (FPGAs). The supervisory control theory of discrete event systems is to implement a given complicated logic specification by formal methods. The specification such as interlock, sequence, mutual exclusion, and language is expressed by a Petri net or automata. It is in turn translated into codes that can be executed by a PLC or FPGA. This paper surveys these formal methods for synthesis of logical controller, which are to shorten the costed time for control programs, to ease the reuse of them, and to increase the safety and reliability of them.

Key words: programmable logic controller; discrete event systems; field programmable gate array; supervisory control

Citation: LUO Jiliang, SHAO Hui, WU Weimin, et al. Synthesis of logical controllers and discrete-event systems supervisory control theory. *Control Theory & Applications*, 2018, 35(1): 86 – 91

1　引言(Introduction)

工业4.0代表着未来工业生产的发展趋势, 越来越多的仪表、传感器、执行机构、现场设备、机器和产品将被连接到一个通讯网络, 使得我们能够获得更多的状态数据, 并且有更丰富的控制手段来操纵生产过程, 使得制造系统具有更好的稳定性、鲁棒性、柔性和效

收稿日期: 2016−12−07; 录用日期: 2017−06−06.
†通信作者. E-mail: jlluo@hqu.edu.cn; Tel.: +86 13110595996.
本文责任编委: 胡核算.
国家自然科学基金项目(61573158, 61374066, 61621002, 61773343), 浙江大学工业控制国家重点实验室自主课题(ICT 1607), 福建省科技计划项目(2015H0026), 福建省自然科学基金项目(2017J01117)资助.
Supported by the National Natural Science Foundation of China (61573158, 61374066, 61621002, 61773343), the Project State Key Laboratory of Industrial Control of Zhejiang University (ICT 1607), the Fujian Provincial Science and Technology Plan Project (2015H0026) and the Fujian Provincial Natural Science Project (2017J01117).

率. 从工业控制的角度, 两大挑战也随之而来, 一是控制规范更为复杂, 如何判断和描述好的和差的系统行为变得非常困难; 二是“维数灾”难题, 随着系统单元数的增加, 其状态空间将指数级地增长. 而且它们又在互相叠加彼此的复杂性, 这为工业逻辑控制程序的设计带来了巨大的挑战, 表现在可编程逻辑控制器的程序设计面临的诸多问题.

执行逻辑程序的控制单元主要分为两类: 一类基于微处理器, 包括可编程逻辑控制器(programmable logic controller, PLC)、工控机、单片机和嵌入式系统等等, 它们都具有同步行为特征, 逻辑事件的执行由微处理器的时钟同步驱动; 另一类基于异步逻辑电路, 比如现场可编程门阵列 (field programmable gate array, FPGA), 能够实现逻辑事件的异步执行. 他们的程序设计语言包括指令表、梯形图、C、汇编和标准硬件描述语言: VHDL等, 但这些语言相对接近自然语言, 语法语义相对灵活, 缺乏形式化程序设计方法, 其程序代码难于重复利用[1], 容易出现逻辑错误, “状态空间爆炸”使得中、大型工程不可能排除全部逻辑错误, 程序调试工作量巨大而繁琐, 工程开发周期过长, 与工业4.0对控制程序设计的敏捷和柔性要求严重不符. 而这些问题的本质在于, 在逻辑控制器设计领域, 主要依靠人工编程和程序员经验, 缺乏经典和现代控制理论中的形式化模型–传递函数和状态空间方程, 更缺乏它们的严谨的控制方法, 比如稳定性判据等等.

离散事件动态系统最早由何毓琦教授定义[2], 由事件序列驱动, 其状态离散变化, 大多数工程对象都涵盖在其范畴之内, 比如制造系统是由工序、车床的启停等事件驱动, PLC是由指令的执行、传感器的上升或下降沿信号、继电器动作等事件驱动. 实际上通过对系统施加影响, 使得系统产生的事件序列满足我们的期望, 就是离散事件系统的控制问题, 为了和连续动态系统相区别, 通常称其为监控问题. 20世纪80年代早期, Ramadge和Wonham[3]在监控理论方面给出了开创性的工作, 采用自动机为形式化模型, 来描述控制规范和设计控制器. 针对广义互斥约束或线性约束, Giua[4]和Moody等人 [5]分别给出了将离散事件系统控制器描述为Petri网的方法. 随后, 借助自动机和Petri网等形式化模型, 离散事件系统监控理论研究获得了长足的进展, 关于可控性、可观性、无阻塞、活性、最大允许性等问题的研究方面, 都取得了重要的成果. 这使得我们可以重新考虑逻辑控制程序的设计问题, 不必先人工设计后试错调试, 而是以监控理论为工具, 直接设计正确、可靠的Petri网或自动机控制器, 然后再将它们转换为控制代码. 这样就可以节省大量的程序调试时间, 从理论上避免程序中的逻辑错误, 而且Petri网或自动机形象直观, 工程对象或控制规范更改时, 易于迭代改进和重复利用.

近年来, 随着离散事件系统监控理论的发展, 大量的研究开始寻求一种形式化的设计工具来代替梯形图、VHDL等编程语言, 比如法国的David和Allen提出了GRAFCET作为一种顺序控制器的规范标准[6], 其对应国际标准为顺序功能图[7]. 目前的研究工作大致可以分为以下两类: 1) 如何将自动机或Petri网转换为程序代码, 比如梯形图、指令表或VHDL语言等等; 2) 如何设计符合PLC和FPGA等硬件特性的自动机或Petri网控制器. 本文将综述这些工作, 并展望未来的研究方向.

2　基于微处理器的逻辑控制程序的形式化设计 (Formal design of logical control programs executed in microprocessors)

基于微处理器的控制单元的执行过程分3个阶段, 即输入扫描、指令执行和输出更新, 如图1所示.

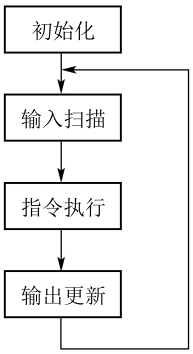

图 1　基于微处理器的控制单元执行过程

Fig. 1　Executing process of a microprocessor control-unit

在工程应用中, PLC是基于微处理器的控制单元的典型代表, 在工业控制领域占据着举足轻重的地位, 它也是工业3.0出现的象征. 2003年国际电工组织颁布了国际标准IEC 61131–3, 它描述了PLC的5种程序设计语言: 梯形图、指令表、结构文本、功能框图和顺序功能图.

2.1　Petri网和PLC编程语言的转换方法 (Method transforming Petri-net or automata into PLC programming language)

当给定一个PLC控制问题, 可以利用监控理论来设计形式化的控制器, 但最终还是要将其转换为PLC的标准化编程语言, 这样才能利用各种PLC厂家提供的编译器, 获得可以执行的机器代码, 因此需要研究Petri网与PLC编程语言之间的翻译方法.

现有的研究大致可以分为两类, 一类侧重于具体指令的形式化描述, 追求将程序变量和他们间的逻辑关系描述为Petri网结构. 文献[8]将触点描述为一对补库所, 分别对应“On”和“Off”; 将梯形图抽象为图模型(图论), 将从左母线到线圈结点的路径描述为从表示该线圈的“Off”库所指向“On”库所的变迁, 路径中结点对应的库所共同指向该变迁; 将它们之间的割集描述为该线圈的“On”库所指向“Off”库所的

变迁, 割集对应的库所共同指向该变迁; 从而利用继电器电路原理将梯形图描述为普通Petri网. 因为该方法获得的是普通Petri网, 有利于将监控理论获得的Petri网模型, 转换为梯形图代码, 但是该方法不适用于计数器和定时器等复杂模块. 文献[9]给出一种模块化的转换方法, 通过在Petri网内引入使能弧、抑止弧、加权使能弧、复位弧和赋时变迁, 将梯形图中各类触点、线圈、计数器和定时器描述为相应的网模块, 并定义网模块的连接规则, 从而能够将梯形图转换为Petri网. 该方法的适用范围较广, 但是因为引入了多种弧, 使得网模型语义变得非常复杂, 不利用于性能分析和评价. 文献[10]给出“与”、“或”、“置位复位”等基本指令转换为Petri网的规则, 然后利用该规则可以将梯形图转换为Petri网, 便于图形化、直观地描述梯形图逻辑, 但是网中包含抑止弧, 语义比较复杂.

另一类则重点关注指令之间的执行顺序, 具体变量的赋值运算则仍然采用代数表达式. 如图2所示, 文献[11]给出了一个PLC程序设计、验证、评价和仿真的工具箱, 它是由C#语言编写的集成开发环境, 包括可以绘制信号注释Petri网(signal interpreted petri net, SIPN)的图形编辑器, 还具有将SIPN转换为指令表、计算树逻辑和Petri网标记语言的多个接口, 能够进一步生成PLC可执行代码, 在NuSMV[12]中进行模型验证, 在Modelica中进行仿真, 还可以在GraphViz中显示状态可达图. 这是一个结合了设计和验证的相对比较完善的工具软件, 同时为控制器的形式化设计搭建了一个较为完整的框架, 但是在Petri网控制器设计上需要引入监控理论进一步完善.

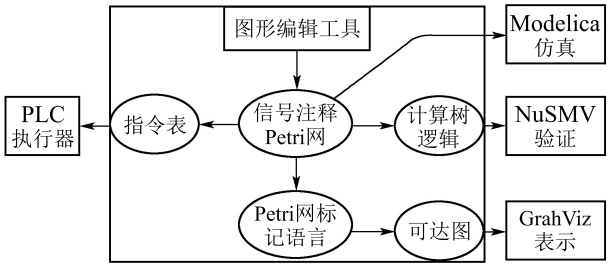

图 2 工具箱的功能结构

Fig. 2 Functional structure of the toolbox

文献[7]认为梯形图难于表现程序中的顺序和状态输出关系的逻辑, 使得程序设计和调试非常困难, 给出了将梯形图转换为顺序功能图的方法, 并说明顺序功能图比梯形图更容易设计、调试、更新、重用和维护. 文献[13]将顺序功能图中的步骤描述为库所, 变迁激发条件描述为控制库所, 并采用与顺序功能图一致的拓扑结构, 得到了顺序功能图的受控Petri网建模方法. 并用该方法的多轴高速机床的顺序功能图的Petri网模型, 分析和验证了程序的活性和安全性. 对于包含定时功能的顺序功能图, 文献[14]利用两对互补库所来分别描述步骤的活性和延时, 从而能够在延时库所对之间引入了赋时变迁, 来描述步骤执行的时效行为, 扩展了文献[13]中的方法, 能够将很多实际工程中的控制程序转换为赋时Petri网, 使能利用Petri网进行性能分析和验证成为可能.

前者对PLC程序的形式化更为彻底, 但是难于描述复杂代数等运算指令. 后者模型简洁, 但是无法描述指令逻辑和程序整体逻辑之间的相互影响. 总地来说, 两者都遵从了如图3所示的基本思路和原理: 从上到下依次给出了梯形图的“与”、“或”和“顺序”逻辑, 以及它们分别对应的Petri网的前向同步、后向冲突和顺序结构.

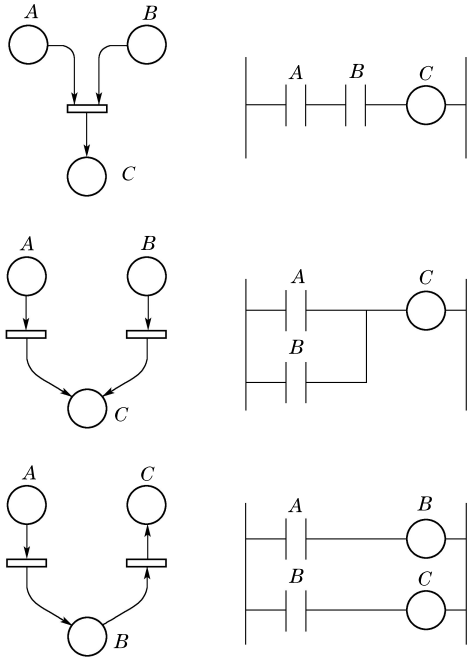

图 3 梯形图与Petri网的转换原理

Fig. 3 Principle transforming Petri-nets into ladder diagrams

类似于Petri网, 自动机具有严格的语法和语义, 便于采用模型验证方法进行自动化验证, 并且能够直观动态地执行, 文献[15]通过在自动机中引入输入、输出、延时和变迁之间的优先级, 定义了安全自动机: 用结点表示输出, 弧表示为输入信号的谓词函数, 从而能够严格描述控制规范. 并给出了将安全自动机翻译为顺序功能图程序的方法. 该方法的局限在于如何将控制规范描述为自动机, 要知道自动机模型相对于工程实施人员来说, 还是过于抽象了.

这些转换方法搭建了形式化模型与PLC指令之间的桥梁, 而且可以借以开发软件工具, 实现Petri网或自动机控制器到PLC程序的自动转换, 不仅可以利用Petri网形象直观的优势, 便于帮助程序员更加清晰地描述控制逻辑; 而且能够在控制器设计中引入Petri网和离散事件系统监控理论, 确保控制器满足期望性能, 从而减少或避免PLC系统的“维数灾”导致的程序测试和调试阶段的巨大工作量.

2.2 基于Petri网或自动机的控制程序设计方法 (Methods for synthesis of control programs via Petri nets or automata)

近年来, 学者们对如何利用形式化工具设计控制程序进行了大量探索, 特别是在典型工业装置或系统上进行了应用, 在系统建模和程序设计方面取得很多有价值的成果, 同时也遇到新的问题和挑战: 为了描述传感器、执行机构和PLC的特性行为, 对Petri网或自动机进行了扩展, 而这样的扩展虽然便于对象建模, 但是也对现有离散事件系统监控理论提出了新的挑战, 需要对现有理论做相应的扩展.

文献[16]利用实时Petri网来设计顺序控制器, 在Petri网内引入了输入、输出和赋时, 即在变迁上关联传感器、按钮或开关输入信号和延时, 在库所上关联线圈、螺线杆等输出信号, 这样实时Petri网由外部输入信号驱动, 并计算和执行输出控制动作; 结果显示, 实时Petri网能够等价描述梯形图, 分析和定位程序中的死锁和错误逻辑, 更易于控制规范时的修改和维护, 缩减工程开发周期和成本. 对于高速连续生产线, 文献[17]给出一种形式化的逻辑控制器设计方法, 首先将生产线上的各个加工单元描述为环状的Petri网模块, 再根据加工规范将各环状网的变迁同步起来, 获得整个系统的Petri网模型, 有趣的是, 利用网简化规则该网可以等价转换为环状事件图, 这样就可以利用环状事件图的性质, 来保证系统的活性、安全性和可重复性, 并给出了将该事件图转换为顺序功能图的方法. 该方法能够将工程人员从编写和调试程序代码的繁琐工作中解放出来, 致力于各个环状模块以及它们之间的逻辑关系, 更易于系统维护和修改.

文献[18]给出一种基于自动机监控理论的PLC程序设计方法: 在Petri网中引入抑止弧和使能弧, 并将谓词(激发条件)与变迁关联, 执行动作与库所关联, 得到自动化Petri 网; 建立被控对象的自动化Petri网模型, 计算其可达图, 逐一检验每个状态结点, 删除违反控制规范的结点, 从而获得满足控制规范的有限自动解, 最后将他转换为梯形图. 该方法通过利用监控理论, 能够确保控制逻辑严格正确, 从而能够避免程序的试错调试.

如图4所示, 文献[19]给出了离散事件监控系统的整体框架, 根据监控理论设计满足被控对象的逻辑控制规范的监控器, 监控器将观测到的事件序列映射到需要禁止的事件序列, 禁止事件序列由控制器(连续动态子系统的控制器)和执行元件具体完成, 从而使得整个系统满足规范要求. 并讨论了监控器实现中的3个问题: 1) 一个传感器信号(上升沿或下降沿)可能触发多个事件; 2) 在一个扫描周期中, 可能同时发生多个事件, 它们的发生顺序存在不确定性; 3) 监控器为了保证系统的最大允许性, 只禁止那些必须被禁止的事件, 这样可能存在两个事件发生冲突的问题; 4) 在一个扫描周期中的指令计算阶段, 可能发生一些事件, 这会使得该周期的输出不是根据最新的状态计算而来的, 导致系统紊乱或违反规范. 这给监控理论提出了一些新的挑战, 如果采用基于微处理器的控制硬件来实现, 需要对现有监控器设计方法进行改进. 该文也探讨了如何利用有色Petri网来设计控制器, 以及将它翻译成指令列表的方法.

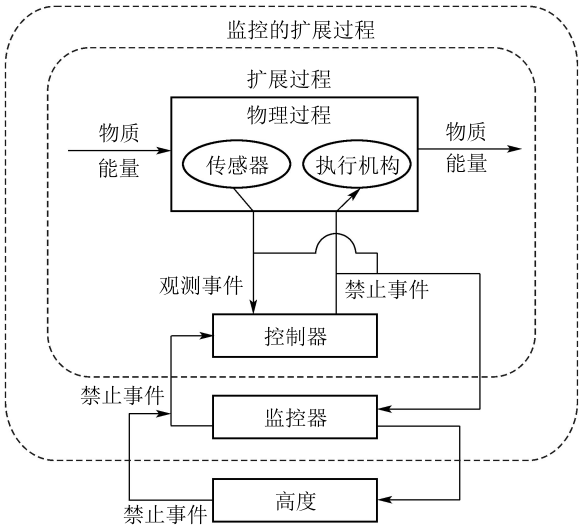

图 4 监控系统结构

Fig. 4 Architecture of a supervisory system

针对大规模和远距离分布式系统, 文献[20]先将控制规范描述为统一建模语言(unified modeling language, UML), 然后将其转换为Petri网, 利用Petri网理论和方法进行性能分析和评价, 从而迭代修正系统中的错误, 最后利用该Petri网设计Java和PLC程序. 该方法成功地应用于开发中国台湾移动电话公司的移动电话切换中心, 该系统包括温度、湿度、电源和安全等316个传感器和140个执行元件.

针对电磁导引的自动导航车辆系统, 文献[21]将传感器和执行机构描述为一个受控网, 然后根据交叉路口的交通规则, 给出了在受控网上实现该规则的控制变迁的设计方法, 从而获得闭环网, 最后给出将闭环网自动转换为梯形图程序的方法. 通过Petri网监控理论, 来保证闭环网控制逻辑的正确性, 从而可以大幅节省程序的开发和调试时间.

文献[22]定义了一种控制注释 Petri 网 (control interpreted Petri net, CIPN), 在Petri网中引入了抑制弧、变迁时延、变迁标签、库所标签、事件标签集合、控制动作集合和谓词条件集合, 极大地扩展了Petri网的建模能力, 对于复杂控制对象能够建立相应的CIPN控制器, 而且值得关注的是, 该文给出了利用梯形图描述了CIPN执行过程的方法, 而且这种将CIPN转换为梯形图的方法是严格根据Petri网的激发规则建立起来的, 具有很好的通用性. 但是, 该方法在Petri网内

引入了太多的扩展元素, 现在基本没有可供使用的网分析和监控方法作为理论支持, 后期仍然需要大量试错来调试程序.

3 FPGA的逻辑控制程序形式化设计方法 (Methods for designing logical programs running in FPGAs)

相对于微处理器等全局时钟同步的硬件电路, FPGA电路可以实现异步驱动, 具有更好的鲁棒、可检测和重用性、更低的成本和更小的电磁辐射[23], 更适合于描述离散事件系统固有的异步和并行等复杂动态行为, 因此FPGA是实现离散事件系统控制器的理想硬件选择.

文献[24]将库所、变迁和典型网结构描述VHDL代码模块, 并将其封装, 添加到Lattice公司的ispDesign Expert中元件库中, 从而使它们能够和“与”、“或”等门电路混合连接, 按照Petri网(控制器)的结构进行连接, 图形化地绘制Petri网逻辑电路, 获得VHDL程序. 该方法在一个液位控制系统中得到了验证, 能够正确根据液位传感器信息控制系统中的阀门开关动作.

为了将离散事件系统控制器实现为一个异步FPGA电路, 文献[25]定义了安全自动化Petri网(safe automation Petri net, SAPN), 其中引入了抑制弧、使能弧、谓词标签和变迁延时, 并给出了使能弧、抑制弧、分结构、合结构、冲突、选择、执行动作和延时变迁转换为逻辑电路的规则, 利用这套规则可以将一个表示离散事件系统控制器的SAPN转换为相应的FPGA电路. 并在一个装配制造系统上进行了实验, 采用了Xilinx公司的Spartan 2 XC2S200型号的FPGA, 实验结果能够验证方法的正确性和有效性.

翻译规则无法涵盖复杂的网结构, 文献[26]给出了一种基于状态演化方程的Petri网到VHDL的转换方法, 采用CIPN来描述离散事件系统控制器, 借助前置关联矩阵、后置关联矩阵、标识矩阵、变迁谓词矩阵等一系列矩阵数据来描述CIPN, 然后根据网演化规则将这些矩阵信息描述为VHDL, 还给出了CIPN中定时器和计数器的VHDL描述方法, 并开发了包括CIPN设计和VHDL转换的工具软件HPetriNets, 使得工程人员不必深入研究硬件就可以设计FPGA控制器.

核反应堆保护系统负责核电站的安全运行, 为了保证其FPGA控制程序的正确可靠性, 文献[27]给出了状态图和Petri网的程序设计方法, 将系统每个单元描述为状态图, 然后将全部状态图组合为Petri网, 从而得到控制系统的Petri网模型, 根据Petri网理论确保系统是无死锁、安全和可重复的, 最后将其转换为VHDL程序, 并利用该方法设计地震自动停堆控制系统的FPGA控制程序, 演示和验证了该方法. 以注释Petri网为工具, 文献[28]研究了双FPGA的安全控制器的设计方法, 通过比较两个执行相同控制算法FPGA的输出, 来检测控制器是否正常工作, 从而提高控制系统的安全可靠性.

4 总结与展望(Conclusions and prospects)

4.1 总结(Conclusions)

逻辑控制器的形式化设计和验证研究本质上是要解决离散事件系统控制的高计算复杂性问题, 目前着重于如何提高代码的可重用性和程序的自动化设计和验证, 已获得了一系列重要的研究成果:

1) 梯形图、有序功能图和指令表的Petri网和自动机的建模方法, 这解决了PLC程序设计长期缺乏形式化模型的问题, 可以利用形式化模型研究控制算法, 为工程实施提供理论依据, 也使得程序的自动化设计和验证成为可能;

2) VHDL语言的Petri网建模方法, 这建立起了异步电路与离散事件系统之间的桥梁, 能够用电路实现离散事件系统固有的异步和并行结构;

3) 基于禁止状态监控理论设计PLC 程序的方法, 由此获得的控制器必然严格遵守给定的控制规范, 大量降低项目开发周期和成本;

4) 逻辑控制程序形式设计和验证的工具软件, 比如 Frey 等人开发的 PLC 设计和验证软件和 Silva 等人[26]开发的FPGA设计软件HPetriNets等.

4.2 展望(Prospects)

微处理器或异步电路的逻辑控制器设计方法将越来越受到离散事件系统监控理论影响, 控制程序的设计也会越来越依靠Petri网和自动机等形式化模型, 而不是人工经验, PLC、FPGA和单片机等控制系统的开发将越来越自动化、敏捷化和柔性化, 其中很多有价值的工作有待开展:

1) 微处理器控制系统是一类特殊的离散事件系统, 现有的监控理论并没有考虑到它的特殊性, 比如周期扫描执行、明确的输入单元(传感器)和输出单元(执行机构)、不允许冲突等行为特征, 因此需要对现有的监控理论做相应的修改和扩展, 建立PLC等微处理器控制系统设计的监控理论基础.

2) 为了建立PLC或FPGA控制系统的形式化模型, 研究者们对自动机和Petri网做了不同程度的扩展, 包括抑制弧、使能弧、逻辑谓词标签、赋时变迁和变迁的优先级等元素, 这固然有力地扩展了Petri网的建模能力, 甚至减小了网规模, 但是也使得模型的语法和语义发生了改变, 脱离了现有的Petri网理论体系, 使得系统分析和评价缺乏理论工具支持, 因此在不做扩展或尽可能少地扩展Petri网的情况下, 如何建立PLC或FPGA控制系统的恰当的形式化模型是一个非常重要的问题.

3) 在核电、轨道列车、医疗等安全关键领域, 其逻辑控制程序不允许任何逻辑错误, 因此亟需发展形式

化的设计方法, 借助离散事件系统监控理论保证系统严格满足控制规范, 并开发设计软件工具, 实现逻辑控制程序的自动化设计, 避免人工疏忽导致逻辑错误.

4) 对于制造系统而言, 最优加工序列随着订单和生产装备改变也会改变, 那么就需要实时优化求解最优工序, 并快速生成执行该工序的控制代码, 因此需要着重研究如何建立兼顾优化调度和逻辑控制的离散事件系统模型[29], 以及基于该模型的优化调度理论和逻辑控制器设计方法.

5) 为了提高逻辑控制器的可靠性, 除了利用监控理论来保证控制程序的正确逻辑, 还可以设计故障诊断器, 比如Cabral等人[30]利用自动机来描述控制系统的状态空间, 进而构建了标签Petri网来进行故障推理, 并编写了梯形图程序来实现该Petri网故障诊断器.

参考文献(References):

[1] FELDMANN K, COLOMBO A W, SCHNUR C, et al. Specification, desgin, and implementation of logic controllers based on colored Petri net models and the IEC 1131.1 part I: specification and design [J]. *IEEE Transactions on Control Systems Techonology*, 1999, 7(6): 657 – 665.

[2] CAO X, COHEN G, GIUA A, et al. Unity in diversity, diversity in unity: retrospective and prospective views on control of discrete eventy systems [J]. *Discrete Event Dynamic Systems: Theory and Applications*, 2002, 12(3): 253 – 264.

[3] RAMADGE P, WONHAM W M, Supervisory control of a class of discrete event processes[J]. *SIAM Journal on Control and Optimization*, 1987, 25(1): 253 – 264.

[4] GIUA A, DICESARE F, SILVA M. Generalized mutual exclusions on nets with uncontrollable transitions [C] //*Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*. Chicago, USA: IEEE, 1992: 129 – 134.

[5] MOODY J O, ANTSAKLIS P J, Petri net supervisor for DES with uncontrollable and unobservable transitions [J]. *IEEE Transactions on Automatic Control*, 2000, 45(3): 462 – 476.

[6] DAVID R, ALLAN H. *Petri Net and Grafcet* [M]. Englewood Cliffs, NJ: Prentice Hall, 1992.

[7] FALCIONE A, KROGH B H. Design recovery for relay ladder logic [J]. *IEEE Control Systems*, 1993, 13(3): 90 – 98.

[8] CHEN X K, LUO J L, QI P F. Method for translating ladder diagrams to ordinary Petri net [C] //*Proceedings of IEEE International Conference on Decision and Control*. Maui, Hawaii, USA: IEEE, 2012: 6716 – 6721.

[9] LEE J, LEE J S. Conversion of ladder deagram to Petri net using module synthesis technique [J]. *International Journal of Modeling and Simulation*, 2009, 29(1): 79 – 88.

[10] QUEZADA J C, MEDINA, FLORES E, et al. Formal design methodology for transforming ladder diagram to Petri nets [J]. *International Journal of Advanced Manufacturing Technology*, 2014, 73(5): 821 – 836.

[11] FREY G, WAGNER F. A toolbox for the development of logic controllers using Petri nets [C] //*Proceedings of the 8th International Workshop on Discrete Event Systems*. New York, USA: IEEE, 2006: 473 – 474.

[12] CIMATTI A, ROERI M, CAVADA R, et al. *NuSMV* [EB/OL]. http://www.nusmv.org.

[13] JIANG J, AZZOPARDI D, HOLDING D J, et al. Real-time synchronisation of multiaxis high-speed machines, from SFC specification to Petri net verification [J]. *IEE Proceading–Control Theory Application*, 1996, 143(2): 164 – 170.

[14] WIGHTKIN N, BUY U, DARABI H. Formal modeling of sequential charts with timed Petri nets [J]. *IEEE Transactions on Control Systems Techonology*, 2011, 19(2): 455 – 464.

[15] FREY G, GRATH R, SCHLICH B, et al. “Safty automata”–a new specification language for the development of PLC saty applications [C] //*Proceedings of 17th IEEE International Conference on Emerging Technologies & Factory Automation*. [S.l.]: [s.n.], 2012: 1 – 8.x

[16] VENKATESH K, ZHOU M, CAUDILL R J. Comparing ladder logic diagrams and Petri nets for sequence controller design through a discrete manufacturing system [J]. *IEEE Transactions on Industrial Electronics*, 1994, 41(6): 611 – 619.

[17] PARK E, TIBURY D M, KHARGONEKAR P. Modular logic controllers for machine systems: formal representation and performance analysis using Petri nets [J]. *IEEE Transactions on Robotics and Automation*, 1999, 15(6): 1046 – 1061.

[18] UZAM M, JONE H, YUCEL I. Using a Petri-net-based approach for the real-time supervisory control of an experimental manufacturing system [J]. *International Journal of Advanced Manufacturing Technology*, 2000, 16(7): 498 – 515.

[19] BASILE F, CHIACCHIO P. On the implementation of supervised control of discrete event systems [J]. *IEEE Transactions on Control Systems Techonology*, 2007, 15(4): 725 – 739.

[20] LEE J, HSU P. Designing and implemention of the SNMP agents for remote monitoring and control via UML and Petri nets [J]. *IEEE Transactions on Control Systems Techonology*, 2004, 12(2): 293 – 302.

[21] LUO J, NI H, ZHOU M. Control program design for automated guided vehicle systems via Petri nets [J]. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2015, 45(1): 44 – 55.

[22] MOREIRA M V, BASILIO J C. Bridging the gap between design and implementation of discrete-event controllers [J]. *IEEE Transactions on Automation Science and Engineering*, 2014, 11(1): 48 – 65.

[23] YAKOVLEV A V, KOELMANS A B. Petri nets and digital hardware design [M] //Reisig W, Rozenberg G. *Lecture Notes in Computer Science*. Heidelberg: Springer, 1998.

[24] ZHAO Buhui, YAN Yangguang, Lu Jiyuan, et al. Study on control circuit's graphical design and simulation based on Petri net componets [J]. *Journal of Circuits and Systems*, 2005, 10(5): 54 – 58.
(赵不贿, 严仰光, 陆继远, 等. 控制电路基于 Petri 网元件的图形化设计和仿真研究 [J]. 电路与系统学报, 2005, 10(5): 54 – 58.)

[25] UZAM M, BURAK K I, GELEN G. Asynchronous implementation of discrete event controller based on safe automation Petri nets [J]. *International Journal of Advanced Manufacturing Technology*, 2009, 41(5): 595 – 612.

[26] SILVA C F, QUINTANS C, COLMENAR A, et al. A method based on Petri nets and a matrix model to implement reconfigurable logic controllers [J]. *IEEE Tansactions on Industrial Electronics*, 2010, 57(10): 3544 – 3556.

[27] CHEN C. A Petri net design of FPGA-based controller for a class of nuclear I&C systems [J]. *Nuclear Engineering and Design*, 2011, 241(7): 2597 – 2603.

[28] TKACZ J, BUKOWIEC A, ADAMSKI M. Dual synthesis of Petri net based application specific logic controllers with increased safety [J]. *Bulletin of the Polish Academy of Sciences-Technical Sciences*, 2016, 64(3): 467 – 478.

[29] ZHOU Jiazhong, LUO Jiliang, ZHAN Yukun. Optimal scheduling and control of batch chemical processes with Petri nets [J]. *Control Theory & Applications*, 2016, 33(6): 809 – 815.
(周家忠, 罗继亮, 詹瑜坤. 间歇式化工系统的 Petri 网优化调度与控制方法 [J]. 控制理论与应用, 2016, 33(6): 809 – 815.)

[30] CABRAL F G, MOREIRA M V, DIENE O, et al. A Petri net diagnoser for discrete event systems modeled by finite state automata [J]. *IEEE Tansactions on Automatic Control*, 2015, 60(1): 59 – 71.

作者简介:

罗继亮　(1977–), 男, 教授, 博士, 主要从事离散事件系统、Petri网监控和智能制造等研究, E-mail: jlluo@hqu.edu.cn;

邵　辉　(1973–), 女, 副教授, 博士, 主要从事机械运动控制、智能控制等研究, E-mail: shaohuihu11@163.com;

吴维敏　(1970–), 男, 副教授, 博士, 主要从事离散事件系统、Petri网监控和智能制造等研究, E-mail: wmwu@zju.edu.cn;

苏宏业　(1969–), 男, 教授, 博士, 主要从事时滞系统与非线性控制理论、鲁棒控制理论、离散事件系统等研究, E-mail: hysu69@zju.edu.cn.