文章编号：1000-5013(2013)03-0241-06 **DOI**：10.11830/ISSN.1000-5013.2013.03.0241

PLC 程序形式化的设计与验证

齐鹏飞，罗继亮，陈雪琨

（华侨大学 信息科学与工程学院，福建 厦门 361021）

摘要： 从形式化方法的角度出发，阐述可编程逻辑控制器(PLC)程序的形式化设计和验证方法的相关研究. 在形式化设计方面，分析了根据 Petri 网和自动机模型判断程序正确性和可靠性的研究成果；在形式化验证方面，分析了 PLC 语言与形式化模型的转换和基于 NuSMV 或 UPPAAL 的验证方法 . 最后，比较将两种形式化方法应用到 PLC 程序的特点，探讨现有成果中存在的问题及研究发展方向.

关键词： 可编程逻辑控制器；形式化设计；Petri 网；自动机；定理证明；模型验证

中图分类号： TP 273 **文献标志码**： A

可编程逻辑控制器(PLC)是一种以微处理器为核心，在计算机技术、电气自动控制技术和网络通信技术基础上，开发出来的工业控制装置[1]. 传统设计方法存在程序设计和调试的工作量繁琐巨大，以及程序开发周期和开发成本难于控制等问题[2-4]. 一般来说，传统的 PLC 程序设计过程是一个开环控制过程，无法准确指出错误发生在哪一段程序. 也就是说，整个检测过程没有一个准确的反馈信息，这类似于开环控制存在的缺陷. 设计人员只能按照程序设计的顺序从上到下逐条检测，这样不但严重影响程序开发周期，浪费人力、物力，更重要的是人为检测并不能保证识别全部逻辑错误. 此外，编程软件主要针对语法、语义上的检测，并不能发现整个程序中逻辑性质上的错误，如竞态[5]和死锁等. 形式化方法是一种用于规范、设计和验证计算机系统的基本数学方法. 引入形式化方法的目的，在于希望能使系统具有较高的可信度和正确性，并能使系统具有良好的结构、易于维护、较好地满足客户的要求. 目前，形式化方法已在不同领域的主流产品开发中得到了成功应用，如 Multos 信用卡认证系统、Eurocopter 公司民用直升机自动导航系统和 AMD Athlon™芯片浮点运算部件验证等. 这都说明了形式化方法在工业界的应用条件已经成熟，开始逐渐被工业界所接受. 本文从形式化方法的角度出发，探讨将形式化方法应用到 PLC 程序设计中的理论成果.

1 形式化设计 PLC 程序

形式化设计 PLC 程序是以形式规范方法为核心，首先将被控对象的行为特性、时间特性、性能特性和内部结构用一种规范语言来描述，即构建形式化模型 . 最后，通过等价转换，将形式化语言翻译为工程人员熟知的 PLC 程序，并应用于实际生产. 整个设计过程，如图 1 所示.

1.1 构建系统的形式化模型

最近几年，形式化方法的应用已经渗入到现代工业各个领域. 然而，由于每个领域内系统的工作流程和特点不尽相同，所以在利用形式化方法对系统建模时也采用了不同的形式化语言 .

在核工业领域，韩赞东等[6]提出了基于可控 Petri 网(CPN)的复杂系统设计方法，通过赋予库所和变迁实际的控制属性，引入宏库所和宏操作，实现了对燃料元件装卸系统的分层设计，很好地满足了球

收稿日期： 2012-06-15

通信作者： 罗继亮(1977-)，男，副教授，主要从事离散事件动态系统与混杂系统的研究. E-mail：jlluo@hqu.edu.cn.

基金项目： 国家青年自然科学基金资助项目(60904018)；福建省高等学校新世纪优秀人才支持计划项目(11FJRC01)；福建省自然科学基金资助项目(2010J01339，2011J01352)；福建省高校杰出青年科研人才培育计划项目(JA10004)；中央高校基本科研业务费专项基金资助项目(JB-SJ1006)

床式高温气冷堆的设计要求.

在铁路交通领域,Giua 等[7]利用 Petri 网设计出了包含车站和轨道的铁路交通系统模型,在设计过程中,模型的控制器的加载是在离散事件系统监控理论的基础上自动完成的.这一方法能够有效降低复杂系统建模工作量,而且免去了对复杂逻辑关系的分析,确保了系统的准确性. Durmus 等[8]利用自动化 Petri 网(APN)实现了对一个简易铁路站场的信号与联锁系统的设计,通过使用抑制弧和附有激发条件的变迁等元素,动态地表示出了铁路站场内的列车调度流程,实现了对列车的联锁控制.

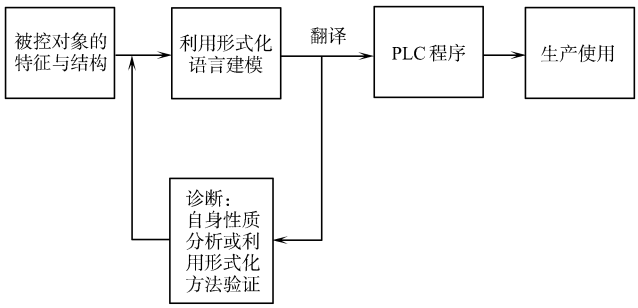

图1 PLC程序的形式化设计

Fig. 1 Design of PLC programs using formal methods

在化工领域,贾洋等[9]提出了基于赋时 Petri 网(TPN)的设计方法,实现了对间歇过程换热网络的设计,所采用时间库表示间歇过程的时间,适合于优化设计间歇过程换热网络.

在军事工业领域,胡昌华等[10]提出了基于普通 Petri 网(Ordinary PN)模型[11]的导弹控制系统故障诊断方法,充分利用了 Petri 网在描述系统动态迁移上的能力,通过观察托肯的最终走向来确定系统是否会达到故障状态,简单而直观地表示了整个诊断过程.

在处理商务流程方面,Du 等[12]也提出了以 TPN 为基础设计国际股票交易系统形式化模型的方法,很好地刻画了系统的动态行为,并利用时态公式描述了各事件之间的因果关系,确保了系统模型的准确性.

在离散制造业,Venkatesh 等[13]提出了基于 Petri 网的离散事件控制器的设计方法,利用实时 Petri 网结构去描述各单元之间的逻辑关系,并通过一个实例比较了 Petri 网模型与梯形图之间的优势与不足,最终指出此方法更简单高效.

虽然用来构建目标系统的形式化模型的语言有很多种,但是它们都遵循了一个共同的规则. 首先,要对目标系统进行透彻的分析,找出其重要的组成单元;然后,将这些组成单元用形式化语言来描述;最后,根据目标系统的工作流程将上述形式化的组成单元连接起来,这样就得到了目标系统的初步形式化模型.除了上文提到的几种形式化语言之外,还有很多人利用不同的语言进行着研究工作.如 Hanisch 等[14]应用 Timed C/E system 语言描述系统行为;Kotini 等[15]通过混杂自动机设计混合系统,等等.

1.2 形式化建模性质分析

当完成了对系统的形式化建模后,首先要考虑的问题就是这个模型是否正确. 即模型是否满足实际系统运行所需的活性、无死锁、无阻塞、有界、可重复性等性质,而这些性质的判断又可以借助模型本身的结构属性.

Frey 等[16-17]利用信号解释 Petri 网(SIPN)构建了一个简易的水箱加热控制器模型,通过托肯在库所中的流动动态地表示出了系统的动态行为.为了保证系统模型的正确性,他们针对 SIPN 这种语言具有的结构属性进行了诊断.由于 SIPN 属于普通 Petri 网的一种延伸,所以它也具有活性、可逆性、可达性和安全性等普通 Petri 网的性质.除此之外,SIPN 还有决定性、终止性、输出正确性、输入依赖性等特殊性质.因此,在利用普通 Petri 网建模后,实际上可以抛开模型的物理意义,单纯从数学角度去诊断整个模型是否存在错误.

由于在建模时是严格按照规则执行的,所以整个模型与实际系统是一一对应的,发现的错误可以直接还原到实际系统中.此外,可以使用 PIPE,TINA 等一些软件工具来帮助诊断.当软件中不再显示模型有错误时,就完成了对系统的形式化建模工作.两者相比较,不难看出:虽然 SIPN 在建模能力上超过了普通 Petri 网,但是在分析的时候却增加了不小的难度.

1.3 将系统的形式化模型翻译成 PLC 程序

Frey 等[18]给出了将 SIPN 翻译成 PLC 程序的转换方法.他们将每一个库所和变迁都对应转换成一条梯形图程序.以库所为例,如果当前要转换的库所已经被标识,那么在梯形图中,除了利用常开触点表示库所对应的地址外,还要利用复位和置位指令将库所对应的输出函数表示出来.当把网结构中的每

一个变迁和库所都转换成一条梯形图程序时，也就得到了整个系统对应的梯形图程序. 在后续的工作中，Frey 等[18]还开发出了相关的软件 SIPN-editor，可以在软件中自动实现上述整个过程.

除此之外，Wang 等[19]给出了将时间自动机[20]转换成梯形图的方法，也给出了相应的算法，并通过软件实现了自动转换. Perme 等[21]提出了一种将扩展 Petri 网（附带有抑制弧、赋时变迁等元素）转换成梯形图程序的方法，并在 PLC 程序软件上进行了仿真. 同样是以 Petri 网为模型，Dideban 等[22]通过将 Petri 网转换成顺序功能图表（SFC），解决了在资源分配时出现的互斥现象. Taholakian 等[23]，Jones 等[24]，琚长江等[25]，LEE 等[26]也都分别提出了将 Petri 网转换成梯形图的不同方法. 然而，在现有的方法中，更多的是针对 PLC 程序的单一指令，而没有考虑指令与指令之间的逻辑关系.

2　形式化验证 PLC 程序

与形式化设计 PLC 程序不同，形式化验证 PLC 程序是以形式化验证技术为核心，将已经编辑好的 PLC 程序转换成验证工具所能够识别的语言，然后利用验证工具对其进行验证. 如果出现错误，验证工具会给出相应的反例，这样就可以有针对性地对原始程序进行修改，从而得到正确的程序，保证了程序的可靠性. 整个形式化验证 PLC 程序的过程，如图 2 所示.

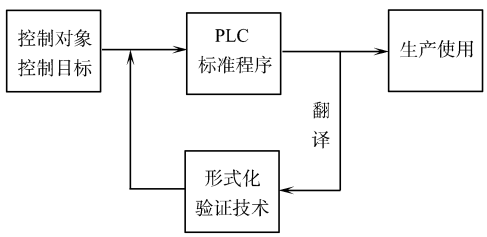

图 2　形式化验证 PLC 程序过程

Fig. 2　Verification of PLC programs using formal methods

2.1　将已存在的 PLC 程序翻译成形式化语言

现有的验证技术包括模型验证和定理证明两大类. 以此为标准，也把由 PLC 程序转换成形式化语言的方法分为两类.

1）适用于模型验证的形式化语言. Wightkin 等[27]提出了一种将 SFC 语言转换成 Petri 网的方法. 相比较前人的方法，Wightkin 在建模时考虑了时间参数，很好地描述了 PLC 的继电特性. 当然，赋时 Petri 网并不是唯一能够融合时间参数的形式化语言. Mokadem 等[28]利用时间自动机也实现了对 SFC 程序的转换，并且在 UPPAAL[29]中进行验证.

虽然两种语言都达到了最初的目的，但是赋时 Petri 网模型要远小于赋时自动机模型，建模效率更高. Oliveira 等[30]完成了从梯形图程序到有色 Petri 网的自动转换过程，Tsai 等[31]则采用布尔 Petri 网完成了从梯形图到形式化模型的翻译.

2）适用于定理证明的形式化语言. 陈钢等[32]提出借助 COQ 定理证明器，去验证 PLC 程序是否存在错误. 在翻译阶段，他们首先建立好相关的基本定义，包括类型定义、变量定义和程序定义等；然后通过用 COQ 中的谓词逻辑公式定义来描述每一段梯形图程序的语义，实现了从 PLC 程序到数学逻辑语言的转换.

相对来说，利用定理证明器来验证 PLC 程序的工作还是比较少见的. 目前，只有 Kramer 等[33]利用 HOL 系统做了同样的工作.

2.2　形式化描述 PLC 程序的控制规范

PLC 程序的控制规范与系统的控制规范相似，它们描述了整个程序要实现什么功能，以及在这个实现过程中可以达到的某些状态. 常见的规范有顺序、联锁和“无竞态”控制等. 实际上，在利用形式化语言进行系统建模时，也是要考虑到系统控制规范的. 能否清晰地表征出系统的控制规范是在利用形式化语言建模时的一个基本要求.

在这一步中，依然可以根据验证技术的不同，来选择不同的形式化语言来描述控制规范. 顾明等所使用的仍然是 COQ 特有的谓词逻辑公式来描述. 这把要验证的 PLC 程序和要实现的控制目标都转换成了同一种语言，方便于下一步的推理证明. 时态逻辑语言是另外一种可以用来描述 PLC 程序控制规范的形式化语言，可以根据对时间认识的不同将其分为线性时态逻辑（LTL）和计算树逻辑（CTL）[34]，广泛应用于模型验证技术.

2.3　利用形式化验证工具验证 PLC 程序

在定理证明中，经常被提到的验证工具除了 COQ 定理证明器外，还有 HOL 和 ACL2 等. 定理证明

实际上是利用逻辑公式来描述系统及其性质,通过一些公理或推理规则来证明系统满足某些性质.而且,可以利用归纳法来处理无限状态的验证问题.

与之相对的是模型检测技术.模型检验是最近十几年经常被学者们采用的一类形式化验证方法.它的基本思想是通过对状态空间的搜索来确认系统是否具有某些性质.其中,状态空间指的是利用形式语言并且在严格遵循被控对象性质的前提下,设计的系统模型中的所涵盖的全部状态.

NuSMV 是目前最为广泛应用的一种模型检测工具,它是由 Carnegie Mellon University 的 McMillan 博士在 SMV 基础上重新构造和实现的.虽然从输入语言的角度来讲,NuSMV 和 SMV 都是针对有限状态机来进行搜索的.但是,NuSMV 在融合了 BDD[35] 技术后,更有效地解决了状态空间爆炸的问题.相对来说更适用于更复杂的程序验证.

NuSMV 可以验证工业设计的可靠性,也作为一个定制的检测工具的核心,还可以作为一个验证技术的试验平台应用于其他领域.因此,在形式化验证 PLC 程序的研究领域内,NuSMV 都得到了很多学者的肯定,如 Pavlovic 等[36] 和 Gourcuffc 等[37].除此之外,SPIN[38],UPPAAL 等验证工具也被应用于 PLC 程序验证.

3 研究展望

PLC 程序可靠性的首要内容是 PLC 系统的形式化描述(形式化建模),它又分为硬件(传感器和执行机构)系统建模和控制规范的形式化描述,现有的方法在这两方面还没有出现系统的理论成果,还需要大量研究工作.

在硬件系统的建模方面,主要是通过 PLC 程序的识别来获得形式化模型(Petri 网或自动机).然而,现有的成果只是给出了某类指令到某类 Petri 网结构或自动机之间的一一对应关系,没有描述指令之间的逻辑语义,因此无法将一个完整的 PLC 程序自动描述为 Petri 网或自动机.在得到硬件系统的模型和控制规范的形式化模型之后,如何添加控制库所才能获得可靠、最优的闭环系统的研究还属空白.基于上述分析,以下几个问题是 PLC 形式化设计和验证的最具价值的研究方向.

1) 基于 Petri 网监控理论的形式化设计.包括受控 PLC 系统(传感器和执行机构)的系统建模方法、一般 PLC 控制规范(顺序、联锁和无竞态等)描述为线性约束[39] 的方法,以及根据控制规范设计闭环 Petri 网和从 Petri 网到 PLC 语言的等价转换方法.

2) PLC 程序的系统的形式化建模方法.目前,虽然学术界在针对 PLC 程序中简单指令的建模工作取得了一定的成绩,但现有的成果更多地局限于单一指令的建模,而没有考虑到指令之间逻辑组合后的建模方法.而且,定时器、计数器器等复杂指令或功能模块的建模问题还没有取得明显的进展.

3) 基于 Petri 网结构特征的定理证明方法.当构建一个系统的 Petri 网模型后,可以基于 Petri 网的结构特征对模型进行性质分析,如根据虹吸结构[40-41] 判断系统是否死锁(适用于普通 Petri 网).这样就可以避免模型检测遍历系统的每个状态,大大降低程序验证时的计算复杂性.

4) 定理证明技术和模型验证技术相融合的验证方法.模型验证的原理是在有穷状态上进行遍历搜索,无法处理系统状态无限多的情况和状态空间爆炸时模型检测的工作效率低下问题.显然,在利用定理证明的过程中,是可以通过推导来验证无穷状态的.

定理证明技术降低了计算量,而模型验证技术又保证了要被检测的系统中没有状态遗失.如何将两者完美地结合在一起,可以获得一种高效率、高质量的 PLC 程序验证方法,这将会是未来一个重要的研究方向.

参考文献:

[1] 吕卫阳.PLC 技术综述[J].自动化博览,2008(增刊 1):16-19.

[2] FREY G,LITZ L. Formal methods in PLC programming[C]// International Conference on Systems, Man and Cybernetics, Tennessee. Nashville:IEEE Press,2000:2431-2436.

[3] HOLLOWAY L E,KROGH B H. Synthesis of feedback logic for a class of controlled petri nets[J]. IEEE Transaction on Automatic Control,1990,35(5):514-523.

[4] PELED D A. Software reliability methods[M]. New York:Springer-Verlag,2001:1-9.

[5] BENDER D F,COMBEMALE B,CREGUT X,et al. Ladder metamodeling and PLC program validation through timed Petri nets[C]// 4th European Conference on Model Driven Architecture-Foundations and Applications. Berlin: Springer,2008:121-136.

[6] 韩赞东,刘继国,罗晟. 基于控制 Petri 网的高温气冷堆燃料装卸过程控制系统设计方法[J]. 核动力工程,2008,29(1):14-18.

[7] GIUA A,SEATZU C. Modeling and supervisory control of railway networks using Petri nets[J]. IEEE Transaction on Automation Science and Engineering,2008,5(3):431-445.

[8] DURMUS M S,SOYLEMEZ M T. Railway signalization and interlocking design via automation Petri nets[C]// Proceedings of the 7th Asian Control Conference. Hong Kong:[s. n.],2009:1558-1569.

[9] 贾洋,肖武,董宏光. 基于自组织 Petri Net 的间歇过程换热网络优化设计[J]. 化工学报,2010,61(12):3167-3171.

[10] 胡昌华,王青,陈新海. 基于 Petri 网的导弹控制系统故障诊断梯形图求解法[J]. 宇航学报,2001,22(1):37-42.

[11] 大卫 R,奥兰 H. 佩特利网和逻辑控制器图形表示工具(GRAFCET)[M]. 北京:机械工业出版社,1995:5-6.

[12] DU Yu-yue,JIANG Chang-jun,ZHOU Meng-chu. A Petri-net-based correctness analysis of internet stock trading systems[J]. IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews,2008,38(1):93-99.

[13] VENKATESH K,ZHOU Meng-chu,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):611-618.

[14] HANISCH H M,THIEME J,LIIDER A,et al. Modeling of PLC behavior by means of timed net condition/event systems[C]// Proceedings of the 6th International Conference on Emerging Technologies and Factory Automation. Los Angeles:[s. n.],1997:391-396.

[15] KOTINI I, HASSAPIS, MODELING G. Performance evaluation of hybrid systems[C]// Proceedings of the 1st South-East European Workshop on Formal Methods. Thessaloniki:[s. n.],2003:21-35.

[16] FREY G,LITZ L. Correctness analysis of Petri net based logic controllers[C]// Proceedings of American Control Conference. Chicago:[s. n.],2000:3165-3166.

[17] FREY G,LITZ L. Analysis of Petri-net based control algorithms-based properties[C]// Proceedings of American Control Conference. Chicago:[s. n.],2000:3172-3176.

[18] FREY G,LITZ L. Automatic implementation of Petri net based control algorithms on PLC[C]// Proceedings of American Control Conference. Chicago:[s. n.],2000:2819-2823.

[19] WANG Rui,SONG Xiao-yu,ZHU Jian-zhong,et al. Formal modeling and synthesis of programmable logic controllers[J]. Computer in Industry,2010,61(1):23-31.

[20] ALUR R,DILL D L. A theory of timed automata[J]. Theoretical Computer Science,1994,26(2):183-235.

[21] PERME T. Translation of extended Petri net model into ladder diagram and simulation with PLC[J]. Strojniski vestnik-Journal of Mechanical Engineering,2009,55(10):608-622.

[22] DIDEBAN A, KIANI M, ALLA H. Implementing PN-based controller with mutually exclusive transitions by SFC [C]// Proceedings of the 35th IEEE Annual Conference of Industrial Electronics. Porto:[s. n.],2009:4353-4358.

[23] TAHOLAKIAN A, HALES W M M. PNP↔PLC: A methodology for designing, simulating and coding PLC based control systems using Petri nets[J]. International Journal of Production Research,1997,35(6):1743-1762.

[24] JONES A H,UZAM M,KHAN A H,et al. A general methodology for converting Petri nets into ladder logic: The TPLL methodology[C]// Proceedings of the 5th Internatioal Conference on Computer Integrated Manufacturing and Automation Technology. Grenoble:[s. n.],1996:357-362.

[25] 琚长江,杨根科. Petri 网在模块化制造系统 PLC 程序设计中的应用[J]. 低压电器,2006(4):20-23.

[26] LEE G B,HAN Z D,LEE J S. Automatic generation of ladder diagram with control Petri net[J]. Journal of Intelligent Manufacturing,2004,15(2):245-252.

[27] WIGHTKIN N,BUY U,DARABI H. Formal modeling of sequential function charts with time Petri nets[J]. IEEE Transactions on Control System Technology,2011,19(2):455-464.

[28] BEHRMANN G,DAVID A,LARSEN K G. A tutorial on uppaal[J]. Lecture Notes in Computer Science,2004,3185:33-35.

[29] MOKADEM H B, BÉRARD B, GOURCUFF V, et al. Verification of a timed multitask system with UPPAAL[J]. IEEE Transactions on Automation Science and Engineering, 2010, 7(4): 921-932.

[30] DA SILVA O E A, DA SILVA L D, GORGONIO K, et al. Obtaining formal models from ladder diagrams[C]// Proceedings 9th IEEE International Conference on Industrial Informatics. Arapiraca: [s. n.], 2011: 796-801.

[31] TSAI J I, TENG C C. Constructing an abstract model for ladder diagram diagnosis using Petri nets[J]. Asian Journal of Control, 2010, 12(3): 309-322.

[32] 陈钢,宋晓宇,顾明. COQ定理证明器辅助PLC程序验证和分析[J]. 北京大学学报:自然科学版, 2010, 46(1): 30-34.

[33] KRAMER B J, VAOLKER N. A highly dependable computing architecture for safety-critical control application [J]. Real-Time Systems, 1997, 13(3): 237-251.

[34] HUTH M, RYAN M. Logic in computer science[M]. Cambridge: Cambridge Univercity Press, 2004: 172-254.

[35] 古天龙,徐周波. 有序二叉决策图及应用[M]. 北京:科学出版社, 2009: 18-19.

[36] PAVLOVIC O, EHRICH H D. Model checking PLC software written in function block diagram[C]// Proceedings of the 3rd International Conference on Software Testing, Verification and Validation. Braunschweig: [s. n.], 2010: 439-448.

[37] GOURCUFF V, DE SMET O, FAURE J M. Efficient representation for formal verification of PLC programs[C]// Proceedings of the 8th International Workshop on Discrete Event Systems. Michigan: [s. n.], 2006: 182-187.

[38] HOLZMANN G J. The SIPN Model Checker[EB/OL]. [2012-06-15]. http://spinroot.com/spin/whatispin.html.

[39] LUO Ji-liang, NONAMI K. Approach for transforming linear constraints on Petri nets[J]. IEEE Transactions on Automatic Control, 2011, 56(12): 2751-2765.

[40] XING Ke-yi, HU Bao-sheng, CHEN Hao-xun. Deadlock avoidance policy for Petri-net modeling of flexible manufacturing systems with shared resources[J]. IEEE Transactions on Automatic Control, 1996, 41(2): 289-295.

[41] LI Zhi-wu, ZHOU Meng-chu. Control of elementary and dependent siphons of Petri nets and their application[J]. IEEE Trans Systems, Man, Cybernetics, Part A: Syst Humans, 2008, 38(1): 133-148.

Design and Verification on the PLC Program Based on Formal Methods

QI Peng-fei, LUO Ji-liang, CHEN Xue-kun

(College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China)

Abstract: From the perspective of formal methods, this paper states lots of researches on the formal design and verification of programmable logic controllers (PLC) programs. As for formal design, the proposed methods, which are to judge whether PLC programs are correct and reliable based on Petri nets or automata, are depicted. As for formal verification, it is summarized that how to model PLC programs as Petri nets, and how to verify PLC programs using NuSMV or UPPAAL. At last, the advantages and disadvantages of these reported approaches are stated, and the research directions which are expected to breakthrough, are pointed out.

Keywords: programmable logic controllers; formal design; Petri nets; automata; theorem proving; model checking

(**责任编辑**: 钱筠 **英文审校**: 吴逢铁)