基于抗辐照龙芯的星载计算机容错启动研究

黄 超[1,2] 陈 勇[1] 林宝军[1]
(中国科学院光电研究院 北京 100190)[1] (中国科学院大学 北京 100190)[2]

摘 要 将硬件冗余、检错纠错和刷新技术相结合,设计了一种以龙芯 1E 处理器为核心且使用 FLASH 存储引导程序的新型容错星载计算机结构。在对存储器进行冗余备份的基础上,采用硬件 EDAC 和刷新技术提高了存储器数据的可靠性。基于这种新型硬件结构设计,分析了星载计算机的可靠性,并提出了一种星载计算机高可靠容错启动方案。该方案通过利用硬件冗余资源和软件备份屏蔽了存在故障的存储芯片及出错软件,从而引导星载计算机正常启动。实验结果表明,该方案有效地屏蔽了常见的星载计算机启动故障,提高了星载计算机的可靠性。

关键词 星载计算机,龙芯,可靠性,容错启动
中图法分类号 TP302 **文献标识码** A

Research of Fault-tolerant Booting for On-board Computer Based on Anti-radiation Loongson

HUANG Chao[1,2] CHEN Yong[1] LIN Bao-jun[1]
(Academy of Opto-Electronics, Chinese Academy of Sciences, Beijing 100190, China)[1]
(University of Chinese Academy of Sciences, Beijing 100190, China)[2]

Abstract To protect on-board computer (OBC) against negative impact brought by space environment, a new architecture of OBC which takes a Loongson processor as its core and uses FLASH memory to store the boot program was proposed. Hardware redundancy was combined with error detection and correction (EDAC) and scrubbing technology in fault-tolerant design. Memory data reliability can be improved obviously by EDAC and scrubbing technology. The OBC reliability was analyzed and a fault-tolerant boot method was described on the basis of the new hardware design. The method shields faulty memory chip and software error by hardware redundancy and software backup. The experimental results show that the solution protects OBC against the common fault of the boot process and improves OBC reliability effectively.

Keywords On-board computer, Loongson, Reliability, Fault-tolerant booting

1 引言

由于发达国家对高性能宇航级器件的出口限制,国内能购买到的宇航级 CPU 都是国外航天应用的低端产品。同时,现在航天应用电子设备有更新换代和国产化的需求。因此,本文选用面向航天应用进行抗辐射加固的龙芯 1E 处理器。龙芯 1E 是以龙芯 1 号处理器为运算核心的高性能应用处理器 SOC,其性能参数为外频 50 MHz,内频 100 MHz,定点 300 MIPS,浮点 50 MIPS[1]。龙芯 1E 抗辐照总剂量为 168KradSi,单粒子锁定阈值不低于 74MeV/mg/cm^2,且 CPU 采用三模设计避免了单粒子翻转效应的危害。

在复杂空间环境中,存储器受单粒子效应的影响会出现存储单元逻辑状态的改变和硬件的临时故障。由此产生的故障会导致星载计算机不能正常启动及运行。故在设计过程中需要采用故障容错技术以提高系统可靠性,从而保证星载计算机能够长期可靠地在轨运行。Bentoutou Y[2] 提出了一种由四片 FPGA 构成的可变两级三模冗余 EDAC 结构,能屏蔽 SRAM 和 EDAC 的故障,实现了 CPU 与 SRAM 之间高可靠数据交换。Saleh A M 等对[3-5] 采用 EDAC 技术和刷新技术的存储器可靠性进行了建模和分析。支天[6] 在模型的基础上进行实验测试,他们的研究结果证明使用 EDAC 和刷新技术可有效地提高存储数据的可靠性。辛宁等[7] 提出了一种利用 SPARC V8 芯片 EDAC 功能与操作系统冗余备份的容错引导算法,在有效降低硬件成本和软件开销的同时,实现了对操作系统文件的纠错检错及错误屏蔽功能,提高了操作系统数据的可靠性。

基于上述研究的结果和设计思想,本文根据实际应用需求和器件特性,应用容错技术设计了一种新型星载计算机结构。该方案使用可多次编程的 NOR FLASH 存储引导程序,并通过热备份、EDAC 和刷新技术提高该部分的可靠性。针对星载计算机启动过程中可能会出现的问题,本文提出了一种星载计算机容错启动方案,能在存储器临时故障和存储数据出错的情况下引导系统进行容错启动。

2 星载计算机结构设计

由于宇航级 PROM 对单粒子效应免疫,且具有很高的可靠性,航天应用中经常使用宇航级 PROM 存储可靠性要求高且代码量小的星载计算机引导程序。但是其有存储空间小、

黄 超(1992-),男,硕士,主要研究方向为计算机应用技术、嵌入式设计,E-mail:huangchao566@126.com;陈 勇(1978-),男,副研究员,主要研究方向为计算机应用技术;林宝军(1963-),男,研究员,主要研究方向为计算机应用技术、空间飞行器总体设计。

价格昂贵和一次性编程等缺点。虽然引导程序会经过地面的严格测试，但还是可能存在软件缺陷。并且在轨运行时可能需要通过更改引导程序扩展星载计算机应用功能。故本文提出一种使用可多次编程的存储器存储引导程序的方案。

根据实际应用需求并比较各种存储器性能，本文选择 NOR FLASH 存储引导程序，选择 NAND FLASH 存储操作系统和应用程序，选择 SDRAM 作为数据存储器。因为 NOR FLASH 的单器件可靠性较 PROM 低，会导致系统可靠性降低，所以需要采用容错技术以提高系统整体的可靠性。从硬件冗余的角度，可以采用冷备份、热备份和三模冗余的方式进行存储器容错。其中，三模冗余不需要进行芯片切换，可直接通过表决器电路输出，但是这种方式功耗最大。由于 CPU 不需要经常读取引导程序，本文综合考虑功耗和实时性选择双片热备份的方式对 NOR FLASH 进行容错；而对于 CPU 需要经常进行读写操作的 NAND FLASH，则采用三模冗余设计。可靠性方面，采用 NOR FLASH 和 PROM 组成异构热备份的可靠性要优于 NOR FLASH 同构热备份的方案。但考虑到仍有一片不可重复编程的 PROM 和实验本身的经济原因，本文选择后者。

本文在硬件冗余的基础上对存储器采用 EDAC 技术及定期刷新存储数据进行数据容错。因为空间应用使用宇航级存储器件并采用硬件抗辐照保护措施，所以存储器中单个存储字出现多位错误的可能性很低。综合考虑纠错码的纠错能力及资源开销，选用可纠正一位错误和检测两位错误的汉明码作为 EDAC 的纠检错编码方式。EDAC 只能检测及纠正存储器输出数据中在其检错和纠错能力范围内的错误，并不能对存储器数据中存在的错误进行纠正。如果不及时对存储数据的错误进行处理，那么随着错误的积累会导致超出 EDAC 能力范围的错误。定期刷新技术能减少错误的累积，有效地解决这个问题。

根据文献[3-5]，同时采用 EDAC 技术和刷新技术存储数据的可靠性如式(1)：

$$R(t)=[r^n(T)r(t-nT)]^M \tag{1}$$

其中，T 刷新周期，M 是存储器中存储字个数，$r(t)$为$[0,T]$时间内单个存储字的可靠性。

$$r(t)=e^{-\lambda_b(w+c)t}[1+(w+c)(e^{\lambda_b t}-1)] \tag{2}$$

其中，λ_b 是所在轨道存储器单个存储位的翻转率，w 是单个存储字信息位位数，c 是单个存储字校验位位数。

针对以上文献未涉及的刷新周期 T 的取值，本文提出刷新周期 T 的选取需要满足限制条件 $T_0<T\leqslant T_m$。T_0 是星载计算机刷新一次程序所需的最短时间，T_m 是存储器发生一次存储位逻辑翻转平均时间，可由式(3)计算：

$$T_m=\frac{1}{N}=\frac{1}{\lambda_b(w+c)M} \tag{3}$$

其中，N 是单位时间内存储器发生翻转存储位位数。

星载计算机结构框图如图 1 所示，通过 FPGA 实现对 FLASH 存储器的 EDAC 并周期刷新存储数据。龙芯 1E 芯片内有 SDRAM 控制器且支持 EDAC 功能。在使能 ECC 的情况下，如果某个 SDRAM 存储单元由于 SEU 发生一位翻转，龙芯 CPU 对该地址单元进行读操作时，可以自动纠正发生一位翻转的数据，并回写至该地址单元。图 1 中 NOR FLASH B 为 NOR FLASH A 的备份，通过图 2 所示由逻辑门、边沿 JK 触发器和看门狗芯片组成的控制电路实现两片 NOR FLASH 的切换，RST 和 DOG 都表示负脉冲信号有效。切换电路逻辑如表 1 所列，表中 RST＝0 和 DOG＝0 都表示负脉冲信号。当只有复位信号 RST 作用时，星载计算机从 A 片中引导程序引导启动；当只有看门狗信号 DOG 作用时，星载计算机从 B 片中引导程序引导启动；当复位信号和看门狗信号同时作用时，触发器输出状态与前一输出状态反相，即从另一片 NOR FLASH 引导启动；当复位信号和看门狗信号都不作用时，触发器输出状态保持，即保持原片选状态。

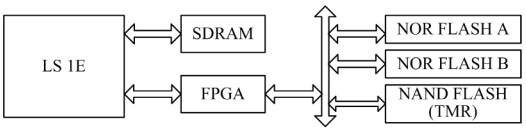

图 1　星载计算机结构框图

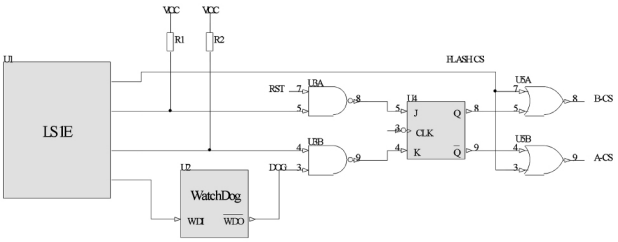

图 2　切换电路原理图

表 1　切换电路逻辑

RST	DOG	Q(n)	Q(n+1)	A-CS	B-CS
0	0	0	1	0	1
0	0	1	0	1	0
0	1	0	1	0	1
0	1	1	1	0	1
1	0	0	0	1	0
1	0	1	0	1	0
1	1	0	0	1	0
1	1	1	1	0	1

3　星载计算机可靠性分析

由星载计算机结构框图可绘制系统可靠性框图，如图 3 所示。根据器件生产厂商提供的数据和器件的失效模式可计算器件失效率。NOR FLASH 的失效率为 $\lambda_1=0.01\times10^{-6}/h$，NAND FLASH 的失效率为 $\lambda_2=0.01\times10^{-6}/h$，FPGA 的失效率为 $\lambda_f=0.0005865\times10^{-6}/h$，SDRAM 的失效率为 $\lambda_s=0.0199\times10^{-6}/h$，CPU 的失效率为 $\lambda_c=0.0292\times10^{-6}/h$，NOR FLASH 切换电路的失效率为 $\lambda_k=0.002\times10^{-6}/h$。它们的可靠性可以用电子器件可靠性通用公式(4)计算，式中 λ 为电子器件的失效率[8,9]。

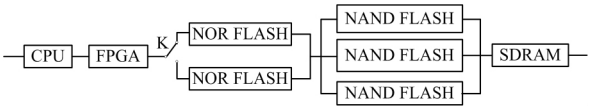

图 3　系统可靠性框图

$$R(t)=e^{-\lambda t} \tag{4}$$

根据热备份系统开关寿命指数型模型，切换电路与 NOR FLASH 组成的子系统的可靠性为：

$$R_k(t)=e^{-\lambda_1 t}-\frac{\lambda_1}{\lambda_k+\mu}[e^{-\lambda_1 t}-e^{-(\lambda_1+\lambda_k+\mu)t}] \tag{5}$$

NAND FLASH 构成 2/3(G)系统的可靠性为：

$$R_{TMR}(t)=3e^{-2\lambda_2 t}-2e^{-3\lambda_2 t} \quad (6)$$

根据系统可靠性框图，系统的硬件可靠性可由式(7)计算。

$$R(t)=R_c(t)R_f(t)R_s(t)R_k(t)R_{TMR}(t) \quad (7)$$

其中，$R_c(t)$为 CPU 的可靠性，$R_f(t)$为 FPGA 的可靠性，$R_s(t)$为 SDRAM 的可靠性。系统硬件可靠性仿真曲线如图 4 所示，星载计算机在轨工作 15 年的硬件可靠度为 0.9955。

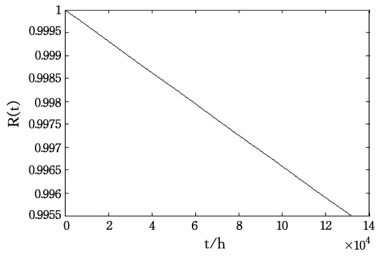

图 4　系统硬件可靠性

4　容错启动方案

星载计算机存储器受空间环境的影响会出现存储器文件数据损坏和存储器硬件临时故障等问题。在这种情况下，如果星载计算机引导软件没有容错引导的功能，星载计算机直接引导错误的操作系统文件或者通过错误的引导软件进行启动会导致星载计算机无法正常启动[7]。同时，地面测控站也不能及时通过星地链路获取星载计算机的最新状态并进行故障的分析和定位。

针对上述问题，本文提出一种基于前文所述新型硬件结构的容错启动方案。该方案将星载计算机引导程序和安全模式程序存储于 NOR FLASH 中。操作系统及应用程序采用软件冗余，将 3 份相同的代码分别存储在同一片 NAND FLASH 特定的存储空间中。当主份操作系统出现 EDAC 不可纠正错误时，可以引导备份操作系统启动。根据 3 份操作系统校验启动的顺序，依次记作操作系统＃1、＃2 和＃3。NAND FLASH 采用三模冗余，通过硬件方式屏蔽了单个故障芯片，处理器能从两个正常工作的芯片中获得所需数据。这种硬件冗余与软件备份相结合的方式可使星载计算机在 2 片或 3 片存储芯片在同一位置出现 EDAC 不可纠正错误的情况下引导备份正确的操作系统进行启动。

容错启动流程图如图 5 所示。系统上电后从启动地址即 NOR FLASH 逻辑地址(0xBFC00000)开始执行引导程序的第一条指令。引导程序先初始化启动所需的硬件环境，完成清缓存、初始化寄存器、配置协处理器 0 等工作[10]，再开始引导操作系统。本文星载计算机选用高可靠、高实时的 VxWorks 嵌入式操作系统。引导操作系统具体流程如图 6 所示。首先，引导程序校验主份操作系统＃1。在操作系统压缩映像数据正确或只存在 EDAC 可纠正错误的情况下，操作系统数据可以通过引导程序校验。若＃1 未通过校验，则依次校验备份操作系统。其中一份操作系统代码校验通过后，不再继续校验优先级较低的代码。然后，将校验通过的操作系统压缩映像解压缩并复制到 SDRAM 中。再以校验和的方式校验 SDRAM 中操作系统代码是否正确。若校验和错误，则校验备份操作系统；若校验和正确，则记录引导操作系统过程中的状态数据。接着，设置系统启动标志。最后，加载并运行应用程序。如果未能正确引导操作系统，引导程序就会停止喂狗。看门狗芯片计数器溢出后会输出信号，切换电路输出使 NOR FLASH B 片选有效，A 片选无效。此时，星载计算机通过 B 片中引导程序引导启动。当 A 片出现硬件故障或者其存储的引导程序出错导致引导程序无法正常执行时，看门狗芯片不会收到喂狗信号，溢出后切换电路会进行切换操作。

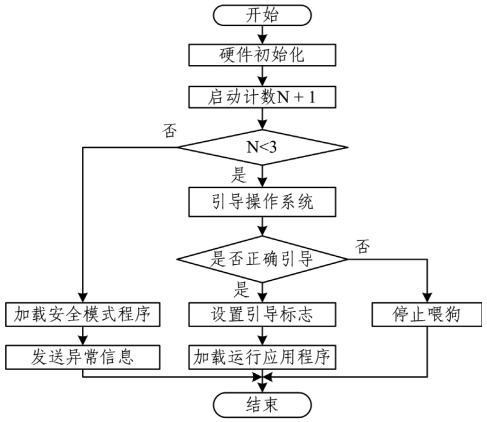

图 5　容错启动流程图

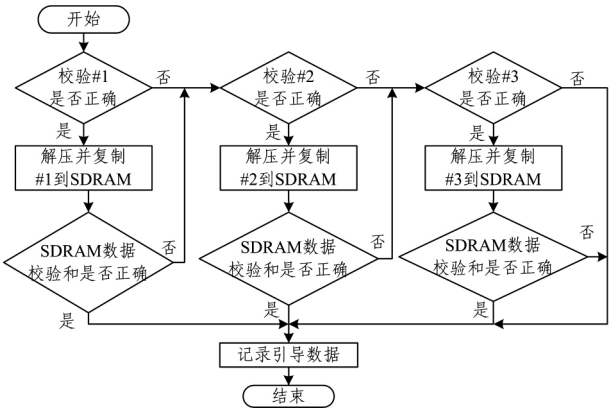

图 6　引导操作系统流程

如果在一定时间内星载计算机的启动次数达到 3 次，那么认为星载计算机出现不可恢复故障。此时，系统不能容错启动，将会加载安全模式程序。在安全模式状态下，可通过星地链路与地面站进行数据交互。安全模式程序将引导启动过程中记录的信息和星载计算机状态发送给地面站。地面站可根据收到的异常信息对星载计算机存在的故障进行分析。若地面分析异常信息后判定其是可恢复软件故障，则可通过上注重构数据的方式实现软件在轨重构；若判定是不可恢复硬件故障，则可通过发送指令切换备份机到工作状态。

本文基于可重构龙芯处理板进行容错启动方案测试实验，实验结果如表 2 所列。实验通过修改处理板存储数据的方式模拟星载计算机受单粒子效应影响而出现在轨故障。当对 NAND FLASH 中存储程序进行注入故障时会同时对 3 片 NAND FLASH 注入相同的故障。表中 Bootflag 为引导程序标志，表示从 A 片或 B 片 NOR FLASH 进行启动；OSflag 为操作系统标志，表示引导的操作系统编号，0xFF 代表未能正确引导操作系统；N 为启动计数值；Status 为状态标志，0x01 表示正常启动，0x0F 表示进入安全模式。在表 2 所列情况下，星载计算机在引导程序或操作系统程序出现错误时能够进行高可靠的容错启动。

表 2　实验结果

故障原因	Bootflag	OSflag	Status	N
A 片引导程序故障	0x0B	0x01	0x01	1
B 片引导程序故障	0x0B	0xFF	0x0F	3
存储器单字单比特错误	0x0A	0x01	0x01	1
#1 单字多比特错误	0x0A	0x02	0x01	1
#1#2 单字多比特错误	0x0A	0x03	0x01	1
#1#2#3 单字多比特错误	0x0B	0xFF	0x0F	3

结束语　本文基于抗辐照龙芯设计了一种新型高可靠星载计算机结构，可靠性仿真结果满足星载计算机在轨工作 10 到 15 年的可靠性要求。为减小单粒子效应的影响，采用 EDAC 技术及通过定期刷新存储数据提高了星载计算机存储数据的可靠性。针对星载计算机因受空间环境的影响而在启动过程中可能会出现的问题，容错启动方案利用硬件冗余资源并且结合软件冗余和编码技术，保证星载计算机能够可靠地引导启动。图 2 所示切换电路使系统能够在引导程序出错或存储器故障时从备份 NOR FLASH 引导星载计算机启动。并通过对 NAND FLASH 采用硬件三模冗余及对操作系统和应用程序代码进行软件备份，确保能引导正确的操作系统及加载正确的应用程序。如何将在轨软件重构和容错启动有效地结合是进一步研究的方向。

参 考 文 献

[1] 龙芯中科技术有限公司. 龙芯 1E 处理器用户手册 [R]. 北京：龙芯中科技术有限公司，2011

[2] Bentoutou Y. A Real Time EDAC System for Applications On-board Earth Observation Small Satellites [J]. IEEE Transactions on Aerospace and Electronic Systems，2012，48(48)：648-657

[3] Saleh A M，Serrano J J，Patel J H. Reliability of Scrubbing Recovery-techniques for Memory Systems [J]. IEEE Transactions on Reliability，1990，39(1)：114-122

[4] Maestro J A，Reviriego P. Reliability of Single-error Correction Protected Memories [J]. IEEE Transactions on Reliability，2009，58(1)：193-201

[5] Li Y，Nelson B，Wirthlin M. Reliability Models for SEC/DED Memory with Scrubbing in FPGA-based Designs [J]. IEEE Transactions on Nuclear Science，2013，60(4)：2720-2727

[6] 支天，杨海刚，蔡刚，等. 嵌入式存储器容错方案可靠性评估 [J]. 微电子学，2015，45(2)：275-280

[7] 辛宁，邱乐德，张立华，等. 一种星载计算机操作系统容错引导算法研究 [J]. 宇航学报，2013，34(6)：818-823

[8] Koren I，Krishana C M. 容错系统 [M]. 杨志，唐宏，王海龙，等，译. 北京：国防工业出版社，2015：10-25

[9] 邹逢兴，张湘平，龙志强，等. 计算机应用系统的故障诊断与可靠性技术基础 [M]. 北京：中国水利水电出版社，2012：166-184

[10] Sweetman D. MIPS 体系结构透视 [M]. 李鹏，鲍峥，石洋，等译. 北京：机械工业出版社，2007：38-89

(上接第 528 页)

中，将致力于如下研究：

(1)并发系统中是否有其它的元素影响调度策略；

(2)当调度控制的条件给定后能够自动产生调度策略；

(3)在不同的层级上获取能够满足限制条件的最优化调度策略。

参 考 文 献

[1] Wing J，et al. Cyber-Physical Systems Summit summary report [R]. the April 2008 CPS Summit，St. Louis，MO，2008

[2] Alur R，Courcoubetis C，et al. The algorithmic analysis of hybrid systems[J]. Theoretical Computer Science，1995，138：3-34

[3] Bliudze S，Sifakis J. The algebra of connectors：structuring interaction in BIP[C]// EMSOFT. ACM，2007：11-20

[4] Eidson J C，Lee E A，Matic S，et al. Distributed Real-Time Software for Cyber-Physical Systems[J]. Proceedings of the IEEE，2012，100(1)：45-59

[5] Jiang J，Zhang S，et al. Configuring business process models[J]. ACM SIGSOFT Software Engineering Notes，2013，38(4)：1-10

[6] Jiang J，Zhu H，et al. Configuration of Services based on Virtualization[C]// TASE. 2014：178-184

[7] Tan Y，Vuran M C，Goddard S，et al. A concept lattice-based event model for cyber-physical systems[C]// ICCPS. 2010：50-60

[8] Talcott C. Cyber-Physical Systems and Events[M]. Software-Intensive Systems and New Computing Paradigms. Berlin，Heidelberg：Springer-Verlag，2008：101-115

[9] Bornot S，Ga G，Sifakis G J. On the construction of live timed systems[M]. Graf S，Schwartzbach M. eds. ，2000：109-126

[10] Altisen K，Gössler G，Sifakis J. Scheduler modeling based on the controller synthesis paradigm [J]. Journal of Real-Time Systems，Special Issue on Control Theoretical Approaches to Real-time Computing，2002，23(1/2)：55-84

[11] Zhang F，Szwaykowska K，Wolf W，et al. Task scheduling for control oriented requirements for cyber physical systems[C]// Real-Time Systems Symposium. 2008：47-56

[12] Li Q. Scheduling in Cyber-Physical Systems[J]. Dissertations，2012：91

[13] Li Q，Negi R. Maximal scheduling in wireless ad hoc networks with hypergraph interference models[J]. IEEE Transactions on Vehicular Technology，2012，61(1)：297-310

[14] Tang Q，Gupta S K S，Varsamopoulos G. A Unified Methodology for Scheduling in Distributed Cyber-Physical Systems. ACM Trans[J]. Embedded Comput. Syst. ，2012，11(S2)：57

[15] Hennessy M，Lin H. Symbolic Bisimulations[J]. Theor. Comput. Sci. ，1995，138(2)：353-389

[16] Jiang J，Zhang S，et al. Modeling and analyzing mixed communications in service-oriented trustworthy software[J]. Science China Information Science，2012，55(12)：2738-2756

[17] Lanese I，Bedogni L，Di Felice M. Internet of things：a process calculus approach[J]. SAC，2013：1339-1346

[18] Winskel G，Nielsen M. Models for Concurrency，Handbook of Logic in Computer Science，Semantic Modelling[J]. Oxford Science Publications，Oxford，1995，4：1-148

[19] Jiang J，Zhang S，et al. Configuring business process models[J]. ACM SIGSOFT Software Engineering Notes，2013，38(4)：1-10

[20] Jiang J，Zhang S，et al. Message Dependency-Based Adaptation of Services[J]. APSCC，2011：442-449

[21] Finkel A，Leroux J. Recent and simple algorithms for Petri nets [J]. Software & Systems Modeling，2015，14(2)：719-7251

[22] Folschette M，Paulevé L，Magnin M，et al. Sufficient Conditions for Reachability in Automata Networks with Priorities[J]. Theoretical Computer Science，2015，608：66-83