DOI:10.19695/j.cnki.cn12-1369.2012.08.037

处理器 Lockstep 技术研究

陈浩[1]
(中航工业西安飞行自动控制研究所 陕西西安 710065)

摘要:文章介绍了处理器Lockstep技术的概念和包含的内容,分析了该技术对计算机系统的故障检测、隔离、以及余度管理的影响,最后对三种Lockstep实现方式的差异进行了分析和研究。

关键词:Lockstep(锁步) Byzantine Fault(拜占庭故障) 故障检测与隔离 余度管理
中图分类号:TP2 **文献标识码**:A **文章编号**:1007-9416(2012)08-0056-03

Research on Processor Lockstep Technique

Chen Hao1
(AVIC Xi ' an Flight Automatic Control Research Institute, Xi ' an,710065,China)

Abstract:The conception of processor lockstep and architecture are introduced in the paper.Error detection、fault isolation、and redundance arrangement are analyzed regarding on lockstep technique application for computer systems.Three methods of processor lockstep design for computer are analyzed and researched finally.

Key Words:Lockstep Byzantine Fault Error detection and fault isolation Redundance arrangement

处理器Lockstep技术作为一项安全关键计算机技术,国外八十年代已经提出相关理论,经过三十年的发展,已经日趋成熟,并形成产品,被应用于波音777、波音787等民机项目的IMA(综合化航电),该技术的应用对提升了目标飞行器的安全性和可靠性,对计算机余度管理技术的发展,也产生了重要影响。目前国内还未见相关资料和产品,作为一项安全关键计算机技术,有必要对处理器Lockstep技术进行跟踪、研究和实践。

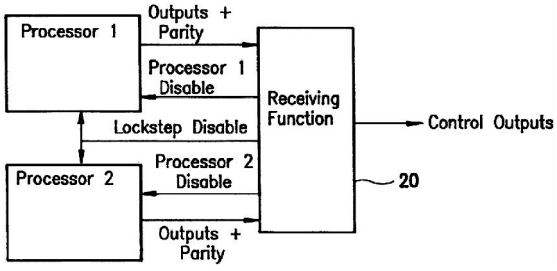

图 2-1 典型 Lockstep 处理器系统框图

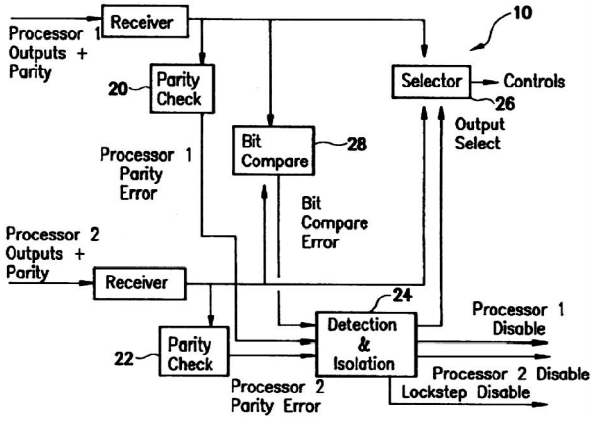

图 2-2 处理器输出面结构框图

1、处理器 Lockstep 概念

Lockstep中文译为锁步,即由两个处理器构成的自监控对,不间断地检查其操作功能的正确性,并且能诊断出故障处理器(支路),以及建立故障抑制区,防止故障蔓延到系统[1]。

2、处理器 Lockstep 包含的内容

典型的Lockstep处理器系统[2](以下简称系统),如图2-1所示,包括两个独立处理器,通常设计为一个MASTER,允许其结果输出,另一个为SLAVE,只负责监测MASTER的工作情况,不允许其结果输出,在Lockstep状态下,两个完成相同的任务,两个处理器的输出面综合在一起,两个处理结果逐条进行比对,当发现有不一致的情况出现时,表明出现故障,系统停止工作。然而,这种策略仍然是不完善的,原因是缺乏代码检测功能,无法判断是MASTER还是SLAVE出现了故障,该策略难以实现故障隔离,也不能实现系统降级或部分故障的恢复[3][4]。

一个完整的Lockstep处理器系统应该包括错误检查、隔离和恢复逻辑,能够恢复一个或两个处理器功能,简言之,处理器的输入面、控制输出面、I/O总线、存储器的地址/数据总线应该具有瞬态故障自诊断和修复的能力。

现以处理器的输出逻辑为例,如图2-2所示,进行说明:如果比

表 3-1 拜占庭故障条件

Required Fault Tolerance	Self Test Coverage	Cross Channel Trust	Number of Redundant Channels
0 Faults	N/A	N/A	≥1
1 Fault	100%	Truthful	≥2
	<100%	Truthful	≥3
	<100%	Lies*	≥4
2 Sequential Faults**	100%	Truthful	≥3
	<100%	Truthful	≥4
	<100%	Lies*	≥5
2 Simultaneous Faults***	100%	Truthful	≥3
	<100%	Truthful	≥5
	<100%	Lies*	≥7

* Classic Byzantine Fault: number of required channels is established by a formal proof
** 1st failure removed before second failure occurs
*** 1st failure not removed before second failure occurs

1作者简介:陈浩(1970-),男,四川旺苍人,汉,工学硕士,高级工程师,研究方向为计算机技术。

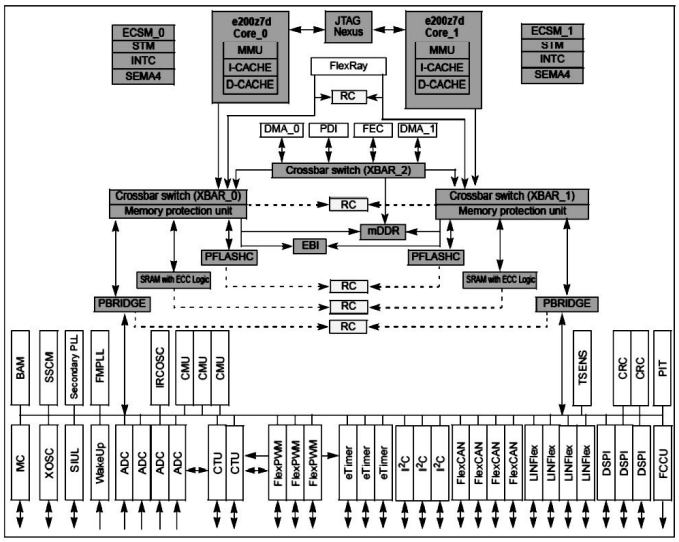

图 4-1 双核 lockstep 结构框图

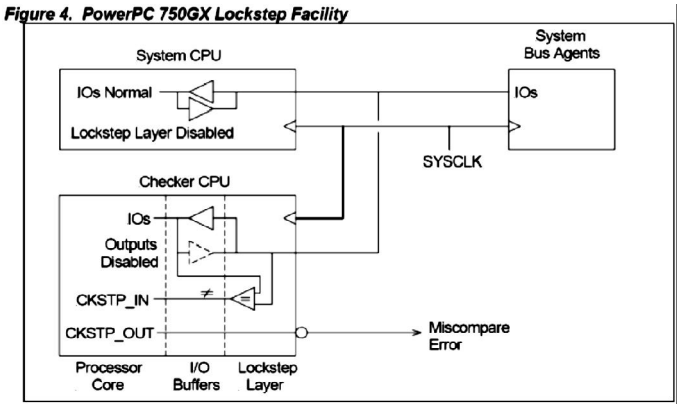

图 4-2 双处理器 lockstep 结构框图

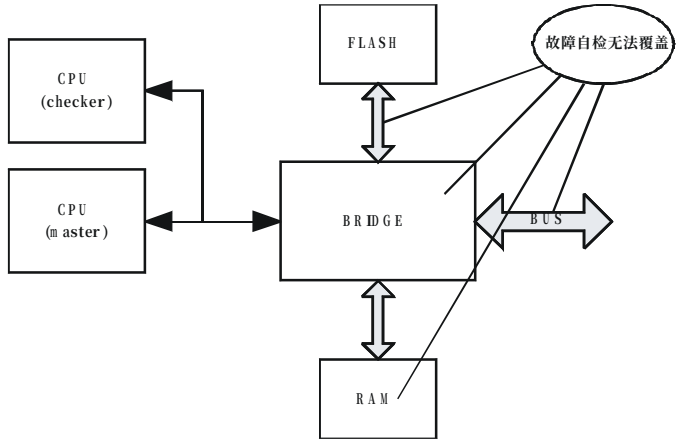

图 4-3 双处理器 lockstep 故障自检覆盖率示意图

较对,但一路校验错,说明这路的校验逻辑出错,可以禁止其的CPU和解除lockstep,只让另一路的CPU工作(如果系统没有其它CPU资源) 如果比较有一位不对,且其中一路校验错,说明这路的校验逻辑或接收模块出错,恢复到上一个状态 如果比较不对,但两边校验正常,说明两边失步,系统停止工作 如果发生两边校验错,说明两个CPU或接收模块故障,系统停止工作。

综上,处理器lockstep技术可以归纳为以下三方面内容 :第一、故障发现,即通过数据、地址、控制总线等的交叉比对,发现是否有故障 ;第二、故障容忍和隔离,即通过检纠错模块(EDC),纠正瞬态故障,增强系统鲁棒性 ;第三、故障恢复,即根据故障情况,尝试恢复部分故障,考虑降级使用。

3、Lockstep 对余度管理的影响

对于高可靠计算机系统,无论是从理论计算还是从工程实践,以现有的技术水平,单个余度是达不到设计要求的,以有人机的飞控计算机为例,要求不可检测故障发生概率 <10-9,要达到这样的指标,至少需要四个余度,这就是典型的三代机余度配置,然而这是飞机系统付出代价换来得,四个余度带来了成本的提高、重量的增加和余度管理的复杂,高起的成本,对即便是世界头号强国的美国也对也难以承受,对飞机战术性能的追求与发动功率提升之间的矛盾,要求航电设备减重减重再减重,随着世界各国新一代战机研制的展开,对成本、重量指标越来越敏感。随着余度技术和电子技术的发展,以三个余度来实现传统四余度的可靠性指标,已经成为现实,之所以会出现这种情况,正是由于这个三余度采用了不同与以前四余度的一些新技术,其中就包括处理器Lockstep技术。

根据Honeywell公司对拜占庭故障条件的研究[5],见表3-1,可以得出以下结论 如果故障自检覆盖率达到100%,并且交叉通道可信,即不存在拜占庭故障,则只需三个余度,就可实现对一次故障、二次顺序故障和二次同时故障的容忍。结合健壮性BIT技术,处理器Lockstep可以实现100%故障自检覆盖率(不含共摸故障)。Honeywell公司称其提出的Lockstep架构已经达到FAA(美国联邦航空管理局)的要求,即不可检测故障发生概率<10-9[6]。以上结论,为三余度配置替代传统四余度配置的构想提供了理论依据。

4、处理器 Lockstep 实现方式及分析

4.1 双核间 lockstep

实现方式 :以Freescale的微控制器MPC5675K为例,如图4-1所示,微控制器的双核间/存储器/桥间采用指令级lockstep,结构对称,双核并行工作,内嵌的存储器FLASH/RAM具有ECC检纠错功能,满足IEC61508 SIL3标准,故障概率(10-8～10-7/H),内嵌BIST,时钟/电源监控。

主要特点 :采用指令级lockstep技术,比对颗粒度小,单芯片实现方案,简化了应用设计 ;但由于芯片规模小,速度不高,存储器容量小,所以不适合作为高性能安全关键领域计算机的核心处理器。

面向对象 :主要面向汽车发动机控制应用。

4.2 双处理器间 Lockstep

实现方式 :如图4-2所示,1个为MASTER,1个为CHECKER。CHECKER负责接收MASTER的输出指令并比对,但自身结果不输出到总线。以IBM的PPC750GX Lockstep处理器应用为例[7],两个PPC750GX共享60X总线,一个被设置为MASTER,另一个被设置为CHECKER,其中CHECKER的总线只具有接收功能,外设来的信息分发到两个CPU,MASTER发出的总线信息被CHECKER接收后,CHECKER进行比对,并将结果输出到故障处理逻辑。

主要特点 :硬件容易实现,但Lockstep只限于两个CPU间,如图4-3所示,CPU外围的MEMORY、BUS、BRIDGE由于缺乏比较监控机制而无法实现比对,不能发现故障,整个处理器系统故障自检覆盖率达不到100%。

面向对象 :高端服务器,网络关键节点。

4.3 双处理器模块间 lockstep

实现方式 :以B777飞控计算机为例,如图4-4所示[8],CPU采用AMD的29050,两CPU松耦合,同源时钟,时钟监控,两CPU模块的输入/输出面(Addr、Data、Ctrl)交叉互比,并带校验和检纠错功能,能及时发现故障,并纠正瞬态错误,增强计算机系统的鲁棒性。如图4-5是Honeywell面向宇航级应用的lockstep方案,采用PowerPC处理器,指令和监控支路的总线位对位比较,且带CRC校验,SDRAM采用三模冗余(TMR)设计,处理器桥片采用半定制ASIC,

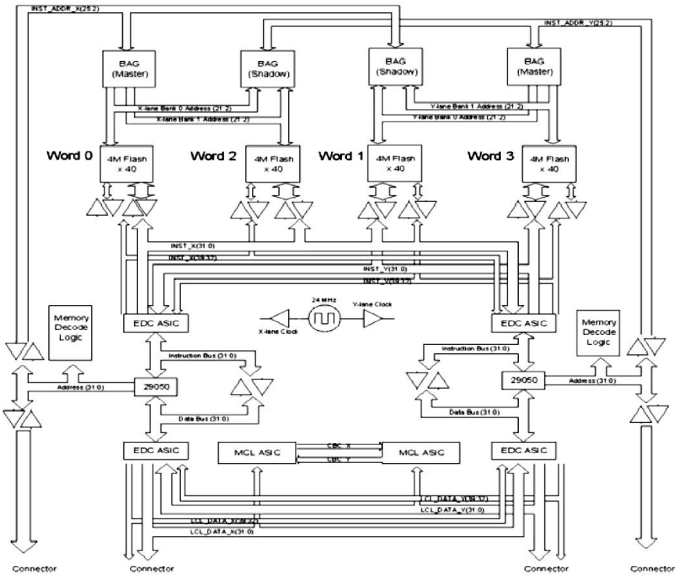

图 4-4 B777 处理器 lockstep 原理框图

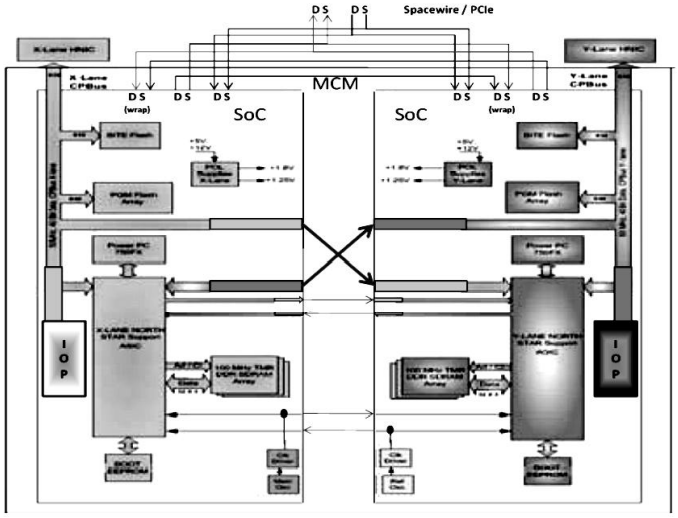

图 4-5 宇航级 Lockstep 模块结构框图

桥片集成了CPU桥、总线比较、CRC校验码以及TMR逻辑等功能(由于处理器lockstep是“小众”用途,所以采用定制ASIC 可以理解),同时采用SOC+MCM(Multi-Chip Module)工艺,实现抗辐射和小型化的目标。

主要特点 输入/输出面实时Bit to Bit比对,具有完备的故障检纠错、隔离和容忍措施,输出故障隔离,只有当指令和监控支路输出结果差异小于门限,且指令支路数据传输正确的情况下,结果才能放到总线上,但实现复杂,对硬件设计要求高。

面向对象 :飞行安全关键计算机系统(影响人的生命或任务的成功)。

5、结语

以上三种实现方式,各有其优缺点,需要根据不同应用对象选择。由于计算机具有复杂度高、可靠性低的特点,为满足其在安全关键领域应用的可靠度指标,传统的做法是采用冗余设计,即多个余度,但冗余设计也带来了不利因素,处理器Lockstep技术的出现,为提高计算机的可靠性、削减冗余数提供了新思路。处理器Lockstep技术本质上是故障自检、隔离和容忍,随着计算机和微电子技术的发展,特别是ASIC设计制造技术的日趋成熟,为Lockstep技术的实现提供了手段,然而,Lockstep技术对硬件设计的要求很高,如何平衡期望值与代价之间的关系,仍然需要进一步研究和实践。

参考文献

[1]《Multi-Modal Digital Avionics for Commercial Applications》. NASA.
[2]《Error detection and fault isolation for lockstep processor systems》,United States Patent, US5915082.
[3]《Dual-dual lockstep processor assembles and modules》,United States Patent, US7979746B2.
[4]《Functional lockstep arrangement for redundant processors》, United States Patent,US5226152.
[5]《Progression of an Open Architecture:from Orion to Altair and LSS》,Honeywell.
[6]《Using Proven Aircraft Avionics Principles to Support a Responsive Space Infrastructure》,AIAA.
[7]《PowerPC 750GX Lockstep Facility》,IBM.
[8]《Integrated Modular Avionic(IMA) Requirements and Development》, Kevin Driscoll.

……上接第55页

```
Ucharcode tab[]={0x3f,0x06,0x5b,0x4f,0x66,0x6d,0x7d,0x07,0x7f,0x6f}; //0到9字符表
void display(uchar x,uchar y); //显示子程序
void delay(uint z);  //定义延时子程序
void main(){ TMOD=0x01;
TH0=(65536-5000)/256;
TL0=(65536-5000)%256;  //定时器置初值
EA=1;ET0=1;    //中断初始化
TR0=0; P1=0xff;i=0;a=0;
display(0,0);  //初始显示00
while(1)  {if(i==200){i=0;a++;  if(a>59) a=0;
//60秒到,秒清零
ge=a%10;shi=a/10;    display(ge,shi);}}} //显示时间
Void display(uchar x,uchar y)
{P1=0xfe;P2=tab[y];delay(10);      P1=0xfd;P2=tab[x];delay(10);}
```

3.3 仿真效果图

运行Proteus,在原理图中的AT89C52上加载上面编译好的.hex文件,数码管开始显示00,按下开始脉冲触发器,秒表开始计时,按下停止脉冲触发器,秒表停止计时,图3.1是按下3秒后的仿真效果图。

4、结语

将PROTEUS虚拟实验技术应用于单片机实验,弥补了传统实验的不足,提供了利于学生创新能力、实践能力培养的虚拟实验教学模式。当然要让学生真正掌握单片机系统开发,仅有虚拟实验系统还是不够的,它必须和单片机真实的实验结合起来。

参考文献

[1] 江世明.基于Proteus的单片机应用技术[M].电子工业出版社,2009.
[2] 蒋辉平.基于PROTEUS的单片机系统设计与仿真实例[M].机械工业出版社,2009.
[3] 张文涛.PROTEUS仿真软件应用[M].华中科技大学出版社,2010.