



(12)发明专利申请

(10)申请公布号 CN 113220492 A
(43)申请公布日 2021.08.06

(21)申请号 202010070159.6

(22)申请日 2020.01.21

(71)申请人 上海晨鑫信息科技有限公司
地址 201100 上海市闵行区广通路66弄4号
楼308室

(72)发明人 不公告发明人

(51)Int.Cl.
G06F 11/07(2006.01)
G06F 11/14(2006.01)

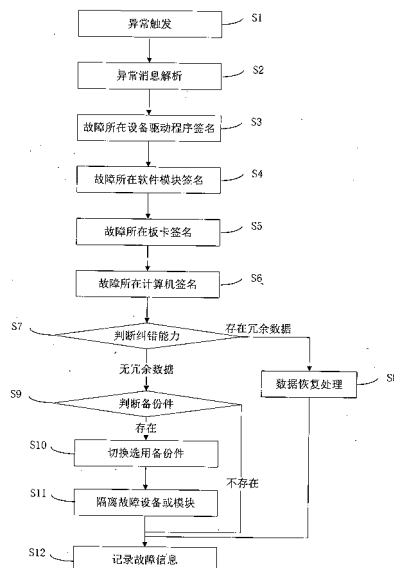
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种支持即插即用的全球卫星导航系统定位软件容错方法

(57)摘要

本发明涉及多平台环境全球卫星导航系统定位软件容错的方法,公开了一种支持即插即用的全球卫星导航系统定位软件容错方法,采取的步骤包括:异常触发、异常消息解析、故障所在设备驱动程序签名、故障所在软件模块签名、故障所在板卡签名、故障所在全球卫星导航系统定位计算机签名、判断纠错能力、数据恢复处理、判断备份件、切换选用备份件、隔离故障设备或模块、记录故障信息。本发明解决了复杂应用环境下对多处理器及硬件设备的全球卫星导航系统定位软件采取容错设计时不易扩展和兼容的问题,取得了提升软件快速开发能力、可靠性和支持设备即插即用等有益效果。



1. 一种支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,包括以下步骤:

S1:异常触发,并获取异常消息;

S2:进行异常消息解析,获得异常类型、异常前的程序地址、异常前的系统寄存器组的数据、异常前访问的设备标识及引发异常的内存物理地址;

S3:进行故障所在设备驱动程序签名;

S4:进行故障所在软件模块签名;

S5:进行故障所在板卡签名;

S6:进行故障所在全球卫星导航系统定位计算机签名;

S7:根据引发异常的内存物理地址是否存在冗余数据来判断是否具有纠错能力,如存在冗余数据,进入步骤S8,如无冗余数据,进入步骤S9;

S8:进行数据恢复处理,然后进入步骤S12;

S9:根据异常前的程序地址、异常前访问的设备标识检查是否存在具有相同功能的软件模块或硬件设备,判断是否存在备份件,如存在,进入步骤S10,如不存在,进入步骤S12;

S10:切换选用备份件;

S11:隔离故障设备或模块;

S12:记录故障信息。

2. 根据权利要求1所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,所述的异常触发采用处理器陷阱中断的方式触发。

3. 根据权利要求1所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,所述步骤S3中,故障所在设备驱动程序签名是根据异常前访问的设备标识确定的,用8位整形数表示;所述步骤S4中,故障所在软件模块签名是由全球卫星导航系统定位软件对各子程序入口分别进行编码签名,用8位整形数表示;所述步骤S5中,故障所在板卡签名是根据异常前访问的设备标识所属的硬件板卡进行编码签名,用8位整形数表示;所述步骤S6中,故障所在全球卫星导航系统定位计算机签名用8位整形数表示。

4. 根据权利要求1所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,所述步骤S8具体为:若引发异常的内存物理地址所在的硬件存储器芯片支持汉明校验(EDAC)纠错功能,则采用汉明校验(EDAC)一位错中断纠错的方式进行数据恢复处理。

5. 根据权利要求4所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,所述的汉明校验(EDAC)一位错中断纠错方式具体为:通过在全球卫星导航系统定位软件背景任务中按照地址顺序循环读所有内存单元,如果读取的内存单元出现一位错,由处理器触发可纠正存储器错误中断,在可纠正存储器错误中断服务程序中读取出错内存单元地址,通过硬件汉明校验(EDAC)纠错,将正确的数据写回出错内存单元地址。

6. 根据权利要求1所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,所述步骤S8具体为:若引发异常的内存物理地址所在的硬件存储器芯片不支持汉明校验(EDAC)纠错功能,则采用数据三取二表决的方式进行数据恢复。

7. 根据权利要求1所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,所述步骤S10具体包括:判断当前故障的软件模块或硬件设备是否发生不可纠正的故障,如果发生故障且不可纠正,则在程序中设置变量标志,通过判断变量标志,使备份件

执行并替代发生故障的软件模块或硬件设备,并不再执行已发生故障的软件模块或硬件设备。

8. 根据权利要求7所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,判断是否发生不可纠正的故障的方法为:通过监视定时器记录程序模块死锁的时间,计数达到指定阈值后,则发生了不可纠正的故障。

9. 根据权利要求7所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,判断是否发生不可纠正的故障的方法为:通过对硬件设备周期性自检,错误计数达到指定阈值后,则发生了不可纠正的故障。

10. 根据权利要求1所述的支持即插即用的全球卫星导航系统定位软件容错方法,其特征在于,所述故障信息包括:故障发生时间、故障所在设备、故障所在软件模块、故障所在板卡、故障所在全球卫星导航系统定位计算机、异常类型、异常前的程序地址、异常前的系统寄存器组的数据、异常前访问的设备标识和引发异常的内存物理地址。

一种支持即插即用的全球卫星导航系统定位软件容错方法

技术领域

[0001] 本发明涉及卫星全球卫星导航系统定位软件容错设计以及软件容硬件容硬件错的设计技术领域,特别涉及一种支持对多处理器、硬件设备及多种软件组件即插即用的全球卫星导航系统定位软件容错方法。

背景技术

[0002] 通过过去几十年中对全球卫星导航系统定位软件可靠性的研究,发现软件错误仍然是影响系统可靠性的最关键因素。高精度导航设备设计要求系统即使出现故障时仍能保持运转而提供相应服务,因此要求高精度导航设备具有超强的容错能力,保证系统的高可靠性。直接开发容错应用是比较困难的,因为开发者不仅要处理复杂的应用逻辑,如星上多种异构的硬件设备、不同架构的软件模块、单机和分系统,还要面对复杂的容错逻辑,开发者很难将整个系统的应用逻辑和容错逻辑考虑全面,致使系统的可靠性得不到全面的保障。在全球卫星导航系统定位软件设计基础上,针对高精度导航设备系统的容错模型,设计支持即插即用的容错管理方法,可屏蔽容错实现和管理困难,降低了容错处理的难度,实现容错管理的精细化。

[0003] 全球卫星导航系统定位软件容错体系架构,不仅要考虑软件本身的容错,还需要考虑对硬件及上层系统的容错,通过软件对硬件容错的技术称为软件实现容错性(SIFT, Software-Implemented Fault Tolerance),全球卫星导航系统定位软件容错领域对此加以扩充,并结合软件自身的容错技术,采取分层方式实现,根据容错对象的业务特点及影响范围可以自上而下划分成:系统级、板卡级、模块级及部件级四个层次。为实现快速响应和在轨维护,支持即插即用的全球卫星导航系统定位软件容错方法不仅要考虑软件本身的容错,还需要考虑对硬件及上层系统的容错,通过软件对硬件容错的技术称为软件实现容错性(SIFT, Software-Implemented Fault Tolerance),采取分层方式实现,根据容错对象的业务特点及影响范围可以自上而下划分成:系统级、板卡级、模块级及部件级四个层次。针对全球卫星导航系统定位软件中间件的数据流、控制流特点,设计多级容错管理软件中间件框架,采用层次化的软件构件化设计技术和分级签名技术,分别在系统、板卡、模块和部件等四个层面建立标准化容错业务及协议。

[0004] 为此,一种支持即插即用的全球卫星导航系统定位软件容错方法可以弥补传统全球卫星导航系统定位软件设计模式下容错设计不支持多处理器和不同硬件设备的兼容的不足,实现全球卫星导航系统定位软件容错设计的通用化和产品化,并可以支持全球卫星导航系统定位软件中间件分层体系架构,这种方法提高了全球卫星导航系统定位软件开发的效率以及全球卫星导航系统定位软件可靠性。

[0005] 目前没有发现同本发明类似技术的说明或报道,也尚未收集到国内外类似的资料。

发明内容

[0006] 本发明的目的在于提供一种支持即插即用的全球卫星导航系统定位软件容错方法,以解决传统的全球卫星导航系统定位软件设计模式下容错设计不支持多处理器和不同硬件设备兼容的问题,并实现全球卫星导航系统定位软件容错设计的通用化和产品化。

[0007] 为实现上述目的,本发明提供了一种支持即插即用的全球卫星导航系统定位软件容错方法,包括以下步骤:

[0008] S1:异常触发,并获取异常消息;

[0009] S2:进行异常消息解析,获得异常类型、异常前的程序地址、异常前的系统寄存器组的数据、异常前访问的设备标识及引发异常的内存物理地址;

[0010] S3:进行故障所在设备驱动程序签名;

[0011] S4:进行故障所在软件模块签名;

[0012] S5:进行故障所在板卡签名;

[0013] S6:进行故障所在全球卫星导航系统定位计算机签名;

[0014] S7:根据引发异常的内存物理地址是否存在冗余数据来判断是否具有纠错能力,如存在冗余数据,进入步骤S8,如无冗余数据,进入步骤S9;

[0015] S8:进行数据恢复处理,然后进入步骤S12;

[0016] S9:根据异常前的程序地址、异常前访问的设备标识检查是否存在具有相同功能的软件模块或硬件设备,判断是否存在备份件,如存在,进入步骤S10,如不存在,进入步骤S12;

[0017] S10:切换选用备份件;

[0018] S11:隔离故障设备或模块;

[0019] S12:记录故障信息。

[0020] 较佳地,所述的异常触发采用处理器陷阱中断的方式触发。

[0021] 较佳地,所述步骤S3中,故障所在设备驱动程序签名是根据异常前访问的设备标识确定的,用8位整形数表示;所述步骤S4中,故障所在软件模块签名是由全球卫星导航系统定位软件对各子程序入口分别进行编码签名,用8位整形数表示;所述步骤S5中,故障所在板卡签名是根据异常前访问的设备标识所属的硬件板卡进行编码签名,用8位整形数表示;所述步骤S6中,故障所在全球卫星导航系统定位计算机签名用8位整形数表示。

[0022] 较佳地,所述步骤S8具体为:若引发异常的内存物理地址所在的硬件存储器芯片支持汉明校验(EDAC)纠错功能,则采用汉明校验(EDAC)一位错中断纠错的方式进行数据恢复处理。

[0023] 较佳地,所述的汉明校验(EDAC)一位错中断纠错方式具体为:通过在全球卫星导航系统定位软件背景任务中按照地址顺序循环读所有内存单元,如果读取的内存单元出现一位错,由处理器触发可纠正存储器错误中断,在可纠正存储器错误中断服务程序中读取出错内存单元地址,通过硬件汉明校验(EDAC)纠错,将正确的数据写回出错内存单元地址。

[0024] 较佳地,所述步骤S8具体为:若引发异常的内存物理地址所在的硬件存储器芯片不支持汉明校验(EDAC)纠错功能,则采用数据三取二表决的方式进行数据恢复。

[0025] 较佳地,所述步骤S10具体包括:判断当前故障的软件模块或硬件设备是否发生不可纠正的故障,如果发生故障且不可纠正,则在程序中设置变量标志,通过判断变量标志,

使备份件执行并替代发生故障的软件模块或硬件设备,并不再执行已发生故障的软件模块或硬件设备。

[0026] 较佳地,判断是否发生不可纠正的故障的方法为:通过监视定时器记录程序模块死锁的时间,计数达到指定阈值后,则发生了不可纠正的故障。

[0027] 较佳地,判断是否发生不可纠正的故障的方法为:通过对硬件设备周期性自检,错误计数达到指定阈值后,则发生了不可纠正的故障。

[0028] 较佳地,所述故障信息包括:故障发生时间、故障所在设备、故障所在软件模块、故障所在板卡、故障所在全球卫星导航系统定位计算机、异常类型、异常前的程序地址、异常前的系统寄存器组的数据、异常前访问的设备标识和引发异常的内存物理地址。

[0029] 本发明提供一种支持即插即用的全球卫星导航系统定位软件容错方法,由于采取上述的技术方案,采取了系统级、板卡级、模块级及部件级四个层次的软件签名流程设计,将故障检测、故障隔离和故障恢复的各类容错设计有机统一在软件架构中。本发明解决了传统全球卫星导航系统定位软件容错设计零碎化,难以兼容不同处理器、硬件设备和不同应用环境下软件中间件复用的问题,取得了提高全球卫星导航系统定位软件开发效率和可靠性的有益效果。

附图说明

[0030] 图1为本发明提供的支持即插即用的全球卫星导航系统定位软件容错方法流程图;

[0031] 图2为优选实施例的判断故障所在模块自主恢复能力的程序流程图;

[0032] 图3为优选实施例的三取二数据恢复的程序流程图。

具体实施方式

[0033] 为更好地说明本发明,兹以一优选实施例,并配合附图对本发明作详细说明,具体如下:

[0034] 如图1所示,本实施例提供的支持即插即用的全球卫星导航系统定位软件容错方法,包括以下步骤:

[0035] S1:进行异常触发,并获取异常消息;

[0036] 其中,这里的异常触发采用处理器陷阱中断的方式触发。

[0037] S2:进行异常消息解析;获得异常类型、异常前的程序地址、异常前的系统寄存器组的数据、异常前访问的设备标识及引发异常的内存物理地址;

[0038] S3:进行故障所在设备驱动程序签名;

[0039] S4:进行故障所在软件模块签名;

[0040] S5:进行故障所在板卡签名;

[0041] S6:进行故障所在全球卫星导航系统定位计算机签名;

[0042] S7:判断是否具有纠错能力,如存在冗余数据,进入步骤S8,如无冗余数据,进入步骤S9;

[0043] 其中,根据引发异常的内存物理地址是否存在冗余数据来判断是否具有纠错能力。

[0044] S8:进行数据恢复处理,然后进入步骤S12;

[0045] S9:判断是否存在备份件,如存在,进入步骤S10,如不存在,进入步骤S12;

[0046] 其中,根据异常前的程序地址、异常前访问的设备标识检查是否存在具有相同功能的软件模块或硬件设备,判断是否存在备份件。

[0047] S10:切换选用备份件;

[0048] S11:隔离故障设备或模块;

[0049] S12:记录故障信息。

[0050] 所记录的故障信息包括:故障发生时间、故障所在设备、故障所在软件模块、故障所在板卡、故障在全球卫星导航系统定位计算机、异常类型、异常前的程序地址、异常前的系统寄存器组的数据、异常前访问的设备标识和引发异常的内存物理地址。

[0051] 上述的步骤S3中,故障所在设备驱动程序签名是根据异常前访问的设备标识确定的,用8位整形数表示;上述的步骤S4中,故障所在软件模块签名是由全球卫星导航系统定位软件对各子程序入口分别进行编码签名,用8位整形数表示;

[0052] 上述的步骤S5中,故障所在板卡签名是根据异常前访问的设备标识所属的硬件板卡进行编码签名,用8位整形数表示;

[0053] 上述的步骤S6中,故障在全球卫星导航系统定位计算机签名用8位整形数表示。

[0054] 上述的步骤S8具体为:若引发异常的内存物理地址所在的硬件存储器芯片支持汉明校验汉明校验(EDAC)纠错功能,则采用汉明校验(EDAC)一位错中断纠错的方式进行数据恢复处理。其中,汉明校验(EDAC)一位错中断纠错方式具体为:通过在全球卫星导航系统定位软件背景任务中按照地址顺序循环读所有内存单元,如果读取的内存单元出现一位错,由处理器触发可纠正存储器错误中断,在可纠正存储器错误中断服务程序中读取出错内存单元地址,通过硬件汉明校验(汉明校验(EDAC))纠错,将正确的数据写回出错内存单元地址。

[0055] 步骤S10具体包括:判断当前故障的软件模块或硬件设备是否发生不可纠正的故障,如果发生故障且不可纠正,则在程序中设置变量标志,通过判断变量标志,使备份件执行并替代发生故障的软件模块或硬件设备,并不再执行已发生故障的软件模块或硬件设备。其中,所述的变量标志用8位整型数表示,按三模冗余保存在三个内存单元中。具体地,所述的切换选用备份件是在确认系统中存在实现相同功能的软件模块或硬件设备后,判断模块或硬件设备是否发生不可纠正的故障,如果发生故障且不可纠正,则在程序中设置变量标志,通过判断变量标志,使程序能够执行替代发生故障的软件模块或硬件设备。而在判断备份件时,确认系统中存在实现相同功能的软件模块或硬件设备后,通过判断程序中的变量标志,不执行已发生故障的软件模块或硬件设备。

[0056] 判断是否发生不可纠正的故障(也即是否具有自主恢复能力)的方法为:通过监视定时器记录程序模块死锁的时间,计数达到指定阈值后,则发生了不可纠正的故障。参见图2,本实施例中的阈值设为预设的最大时间值(MAX_TIMEOUT),则判断过程包括:监视定时器计数加1;判断所述监视定时器计数是否大于最大时间值(MAX_TIMEOUT),如是,则降低任务优先级后进行监视定时器清理,如否,则结束。

[0057] 在另一优选实施例中,步骤S8具体为:若引发异常的内存物理地址所在的硬件存储器芯片不支持汉明校验(EDAC)纠错功能,则采用数据三取二表决的方式进行数据恢复。

具体地,所述的数据三取二表决是指同一个变量或程序分别存储在三个固定地址间隔的内存数据块A、B、C中,使用时将A、B、C转换为二进制,并进行位运算,用公式 $R = (A \& B) | (A \& C) | (B \& C)$ 计算输出结果R。参见图3,本实施例中的数据三取二表决包括:开始并输入参数A、B、C;对数据块A、B、C位宽对齐处理;禁止中断(避免表决过程中数据块被其他正在运行的任务所修改);计算 $R = (A \& B) | (A \& C) | (B \& C)$;开放中断;返回R。其中,符号“&”表示位与运算,符号“|”表示位或运算。

[0058] 在另一优选实施例中,判断是否发生不可纠正的故障的方法为:通过对硬件设备周期性自检,错误计数达到指定阈值后,则发生了不可纠正的故障。

[0059] 本发明解决了复杂应用环境下对多处理器及硬件设备的全球卫星导航系统定位软件采取容错设计时不易扩展和兼容的问题,取得了提升软件快速开发能力、可靠性和支持设备即插即用等有益效果。

[0060] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何本领域的技术人员在本发明揭露的技术范围内,对本发明所做的变形或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以所述的权利要求的保护范围为准。

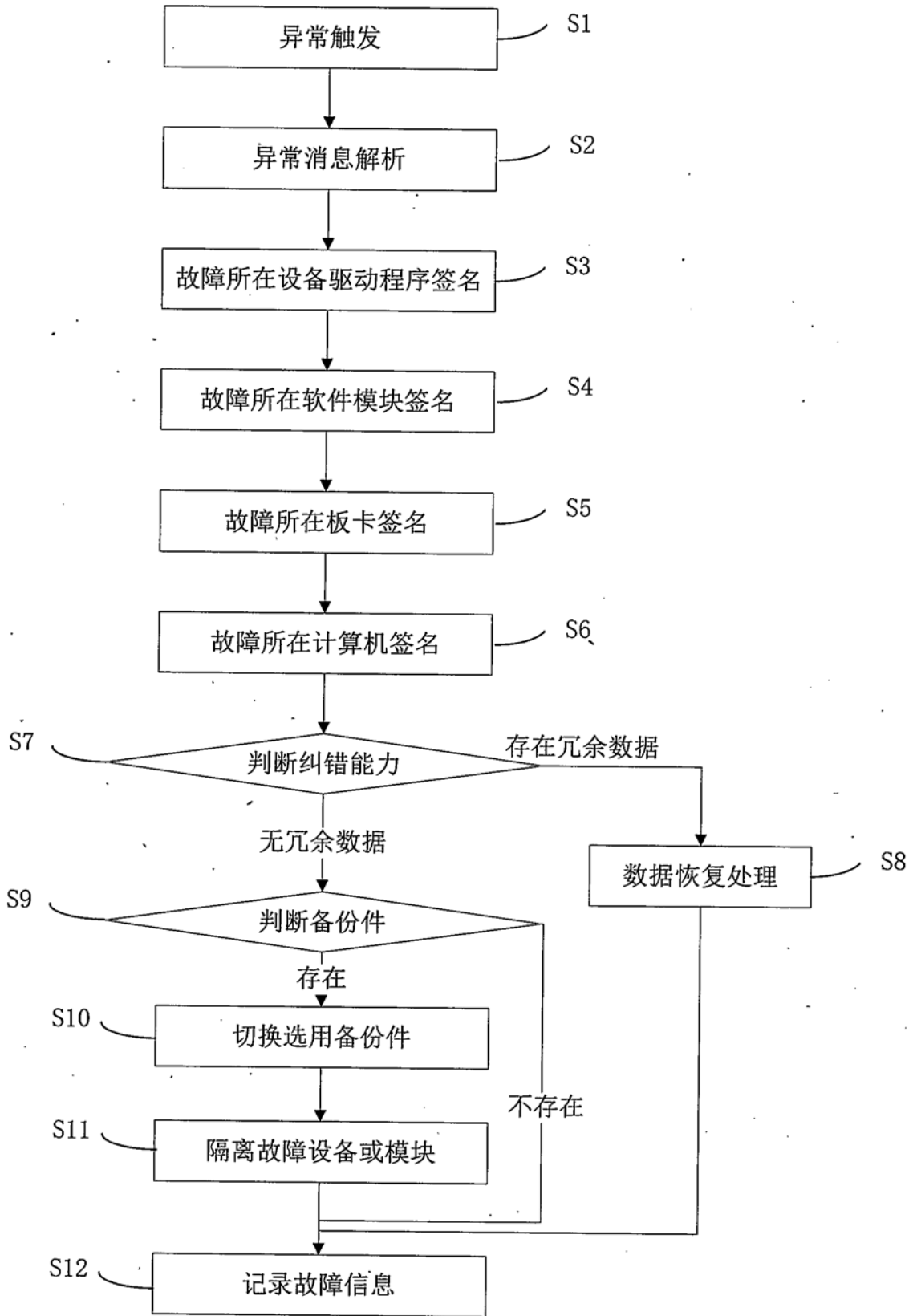


图1

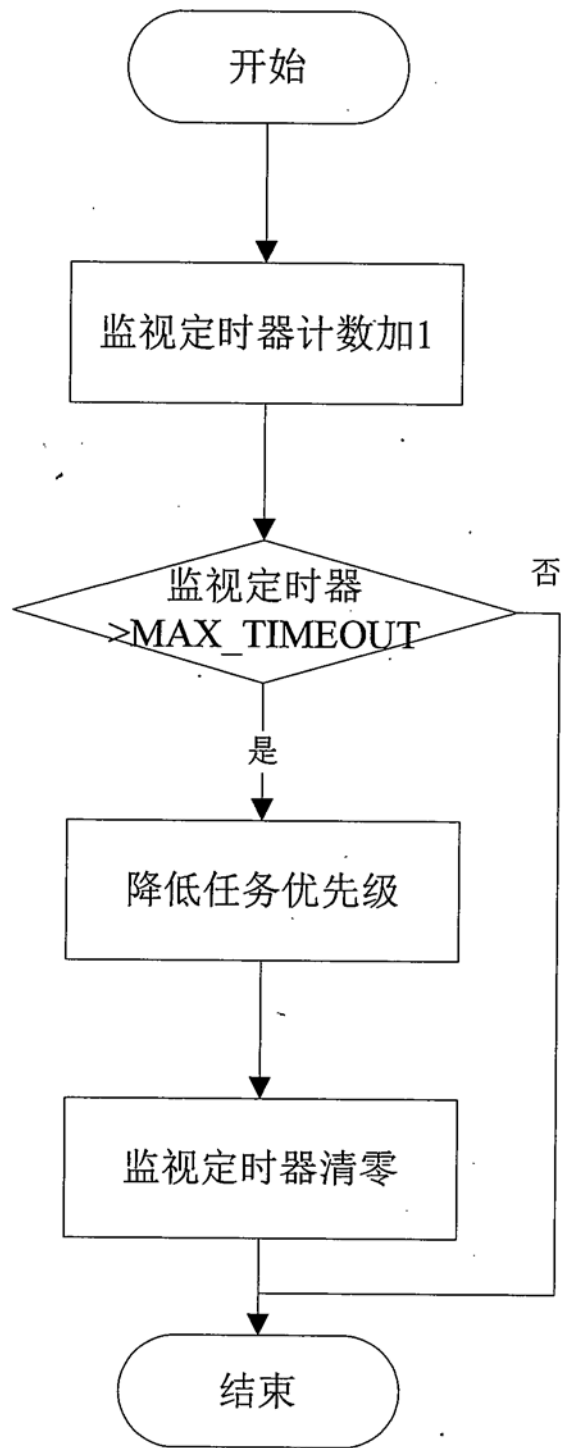


图2

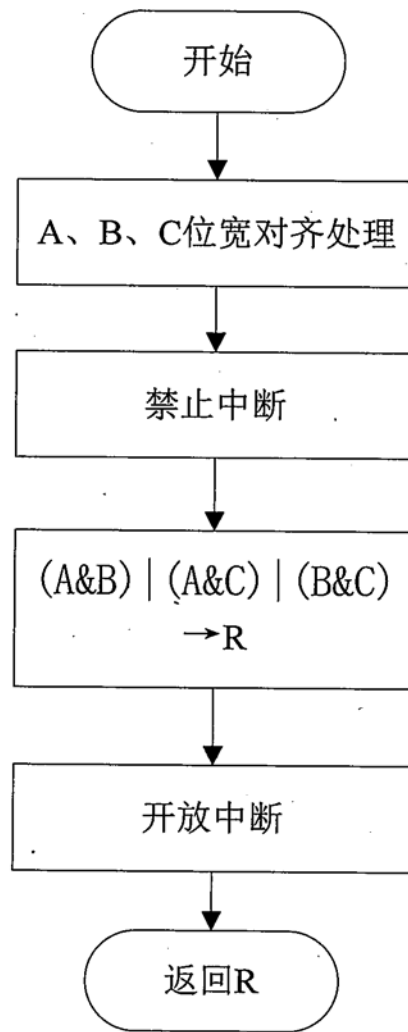


图3