[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G06F 11/14 (2006.01)*

# [12] 发明专利申请公布说明书

[21] 申请号 200610083033.2

[43] 公开日 2007 年 6 月 20 日

[11] 公开号 CN 1983206A

[22] 申请日 2006.5.29

[21] 申请号 200610083033.2

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

[72] 发明人 詹东华

[74] 专利代理机构 北京凯特来知识产权代理有限公司

代理人 郑立明

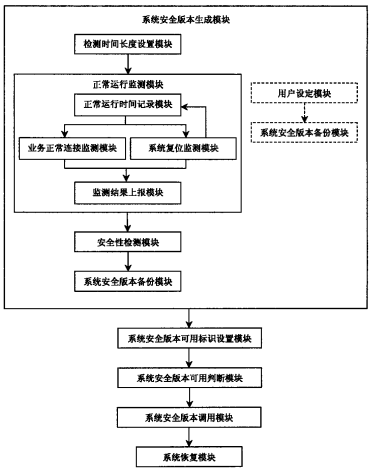
权利要求书 5 页 说明书 13 页 附图 3 页

[54] 发明名称

软件系统自动恢复的方法及装置

[57] 摘要

本发明涉及一种软件系统自动恢复的方法及装置，本发明主要包括：首先生成系统安全版本；然后，当软件系统需要恢复时，则调用所述的系统安全版本，并利用所述的系统安全版本对软件系统进行自动恢复处理。 本发明能够在尽可能短的时间内，恢复软件系统，最大程度的保障系统运行的可靠性。 同时，本发明能够有效简化用户恢复软件系统时操作的复杂性，并降低用户误操作的可能性。相应地，本发明能够帮助运营商有效降低利益损失与业务流失，并有助于提高用户对运行商的信任度。



1、一种软件系统自动恢复的方法，其特征在于，包括:

A、生成系统安全版本;

B、当软件系统需要恢复时，则调用所述的系统安全版本，并利用所述的系统安全版本对软件系统进行自动恢复处理。

2、根据权利要求1所述的方法，其特征在于，所述步骤A包括:

A1、检测当前运行系统，如果被检测系统正常运行的时间达到或超过预先设定的检测时间长度，则该被检测系统通过安全性检测，由该通过安全性检测的系统生成所述的系统安全版本;

或者，

A2、用户主动将当前运行系统设定为系统安全版本。

3、根据权利要求2所述的方法，其特征在于，所述的正常运行为:

所述被检测系统业务连接正常，且未出现断电或异常的系统复位现象;

当出现正常的系统复位现象时，所述的被检测系统对自身已运行的时间清零，并在运行后对自身运行时间重新开始计时。

4、根据权利要求2所述的方法，其特征在于，所述步骤A还包括:

将通过安全性检测的系统或用户设定为系统安全版本的系统设置为处于安全状态，并对处于安全状态的系统的数据区与程序区的文件进行备份，生成所述的系统安全版本;

保存所述系统安全版本，并为其设定可用标识，所述的可用标识用于表示存在可用的系统安全版本。

5、根据权利要求4所述的方法，其特征在于，所述步骤B具体包括:

B1、当用户主动要求恢复当前运行系统或当前运行系统发生异常，需要自行恢复时，则用户或当前运行系统根据所述系统安全版本的可用标识判断

出当前存在可用的所述系统安全版本，并激活所述的系统安全版本;

B2、所述的系统安全版本的数据区与程序区自动覆盖当前运行系统的数据区与程序区，并复位系统。

6、根据权利要求1所述的方法，其特征在于，所述的方法还包括:

系统所处的安全状态包括：当前运行系统为初次被激活的所述系统安全版本，或当前运行系统通过安全性检测，或用户主动将当前运行版本设定为系统安全版本;

系统所处的不安全状态包括：当前运行系统初次被加载或重新被激活或数据被破坏。

7、根据权利要求1所述的方法，其特征在于，所述的方法还包括:

当系统运行异常且无法调用系统安全版本时，记录此时系统的状态数据，捕获异常中断信息，并将寄存器、堆栈和/或函数调用栈信息记录在高端内存或保留内存中；当系统再次出现非断电复位时，将记录的相关信息导入死机信息日志。

8、一种软件系统自动恢复的装置，其特征在于，包括:

系统安全版本生成模块，用于生成系统恢复需要的系统安全版本;

系统安全版本调用模块，用于激活生成的所述系统安全版本，并触发系统恢复模块;

系统恢复模块，用于利用所述激活的系统安全版本对需要恢复的系统进行恢复操作。

9、根据权利要求8所述的装置，其特征在于，

所述的系统安全版本生成模块具体包括:

检测时间长度设置模块，用于设置对被检测系统进行安全性检测的时间长度值，并将该时间长度值提供给正常运行监测模块;

正常运行监测模块，用于对被检测系统的正常运行进行监测，并将监测

结果上报给安全性检测模块;

安全性检测模块，用于接收正常运行监测模块的监测结果，并在接收到所述监测结果后确认所述被检测系统通过安全性检测，之后触发系统安全版本备份模块;

系统安全版本备份模块，用于对通过安全性检测的系统的数据区与程序区进行备份，生成所述的系统安全版本;

或者，所述的系统安全版本生成模块具体包括:

用户设定模块，用于将当前运行系统直接设定为系统安全版本，并触发系统安全版本备份模块;

系统安全版本备份模块，用于对由所述用户设定模块设定为系统安全版本的当前运行系统的数据区与程序区进行备份，生成所述的系统安全版本。

10、根据权利要求9所述的装置，其特征在于，所述正常运行监测模块具体包括:

正常运行时间记录模块，用于对系统运行时间进行计时，并在系统正常复位后，对系统的运行时间重新计时，当系统运行至由检测时间长度设置模块提供的检测时间长度后，触发业务正常连接监测模块和系统复位监测模块上报监测结果给监测结果上报模块;

业务正常连接监测模块，在正常运行时间记录模块开始计时后被触发，用于监测被检测系统在所述安全性检测的时间长度内业务的连接是否正常，并在系统业务能够正常连接时将该监测结果提供给监测结果上报模块；否则，等待正常运行时间记录模块的下一次计时被触发;

系统复位监测模块，在正常运行时间记录模块开始计时后被触发，用于监测被检测系统在所述安全性检测的时间长度运行是否出现异常断电或异常复位情况，如果出现所述异常情况，则，等待正常运行时间记录模块的下一

次计时被触发，否则，将系统正常复位或未出现异常断电的监测结果提供给监测结果上报模块，并在系统正常复位时，触发正常运行时间记录模块;

监测结果上报模块，用于接收所述业务正常连接监测模块和系统异常监测模块的监测结果，并在接收到该两个模块的监测结果后，将系统正常运行的监测结果上报给所述安全检测模块，否则，继续等待下一次安全性检测的时间长度内上述两个模块的监测结果。

11、根据权利要求9所述的装置，其特征在于，所述的装置还包括:

系统安全版本可用标识设置模块，用于为所述的系统安全版本设置可用标识。

系统安全版本可用判断模块，用于判断当前是否存在系统安全版本的可用标识，并在存在可用标识时触发系统安全版本调用模块。

12、根据权利要求8所述的装置，其特征在于，所述装置还包括:

故障信息记录模块，当系统数据被严重破坏，并导致无法调用系统安全版本时，自动触发，用于记录此时系统的状态数据，捕获异常中断信息，并将寄存器、堆栈和/或函数调用栈信息记录在高端内存或保留内存中;

故障信息导入模块，当系统下次出现非断电复位时，自动触发，用于将故障信息记录模块所记录的信息导入死机信息日志。

13、根据权利要求8所述的装置，其特征在于，所述的装置还包括:

系统运行状态标识模块，用于根据预先设定的规则标识系统的运行状态。

14、根据权利要求13所述的装置，其特征在于，所述的预先设定的规则包括:

若当前运行系统初次被加载或重新被激活或数据被破坏，则标识该系统处于不安全状态;

若当前运行系统为初次被激活的所述系统安全版本，则标识该系统处于

安全状态；

若当前运行系统通过安全性检测，则标识该系统处于安全状态；

若用户主动将当前运行的系统的状态设定为安全状态，则标识该系统处于安全状态。

# 软件系统自动恢复的方法及装置

## 技术领域

本发明涉及通信技术领域，尤其涉及一种软件系统自动恢复的技术。

## 背景技术

基站（或其他类似通信设备，如中继站等）在通信系统中担任着非常重要的角色，以作为业务接入点或者业务接入的汇聚点的基站为例，它作为通信技术的基础设施，为实现业务连接提供必要保障。通常，运营商常需要投入大量的人力物力以保证基站软硬件设施的可靠运行。

在现阶段，当基站软件系统发生故障，如关键信息丢失，文件、数据被破坏或系统无法正常启动时，基站软件系统的维护人员往往需要对出错的软件系统进行一系列的人工查询，并通过对一系列的告警和日志等信息进行分析，来获取基站系统的运行情况，以判断并确认所述的软件系统中哪些数据信息被破坏。然后维护人员通过执行一系列的人工文件操作，对所述软件系统的数据区和程序区进行恢复。

上述分析确认过程往往需要专业人士的参与才能完成，而通常事故发生的最前方的系统维护人员未必是相关技术的专家，并且通常采用上述分析确认过程必然会消耗较长的恢复时间，种种实际情形就与要求系统尽快恢复的需求形成矛盾。

并且，系统运行的可靠性与系统恢复过程的耗费时长不仅与运营商的利益相关，更关系用户对运营商的信任度，即如果系统恢复过程耗时过长，不仅会造成运营商的利益损失，还会降低用户对运营商的信任度。

## 发明内容

本发明提供一种软件系统自动恢复的方法及装置，从而使所述的软件系统在发生故障时能够自动恢复，以尽快进入正常运行状态。

本发明技术方案通过以下过程实现:

本发明提供一种软件系统自动恢复的方法，包括:

A、生成系统安全版本;

B、当软件系统需要恢复时，则调用所述的系统安全版本，并利用所述的系统安全版本对软件系统进行自动恢复处理。

所述步骤A包括:

A1、检测当前运行系统，如果被检测系统正常运行的时间达到或超过预先设定的检测时间长度，则该被检测系统通过安全性检测，由该通过安全性检测的系统生成所述的系统安全版本;

或者，

A2、用户主动将当前运行系统设定为系统安全版本。

所述的正常运行为:

所述的被检测系统业务连接正常，并且未出现断电或异常的系统复位现象;

当出现正常的系统复位现象时，所述的被检测系统对自身已运行的时间清零，并在运行后对自身运行时间重新开始计时。

所述步骤A还包括:

将通过安全性检测的系统或用户设定为系统安全版本的系统设置为处于安全状态，并对处于安全状态的系统的数据区与程序区的文件进行备份，生成所述的系统安全版本;

保存所述系统安全版本，并为其设定可用标识，所述的可用标识用于表示存在可用的系统安全版本。

所述步骤B具体包括:

B1、当用户主动要求恢复当前运行系统或当前运行系统发生异常，需要自行恢复时，则用户或当前运行系统根据所述系统安全版本的可用标识判断出当前存在可用的所述系统安全版本，并激活所述的系统安全版本；

B2、所述的系统安全版本的数据区与程序区自动覆盖当前运行系统的数据区与程序区，并复位系统。

所述的方法还包括：

系统所处的安全状态包括：当前运行系统为初次被激活的所述系统安全版本，或当前运行系统通过安全性检测，或用户主动将当前运行版本设定为系统安全版本；

系统所处的不安全状态包括：当前运行系统初次被加载或重新被激活或数据被破坏。

所述的方法还包括：

当系统运行异常且无法调用系统安全版本时，记录此时系统的状态数据，捕获异常中断信息，并将寄存器、堆栈和/或函数调用栈信息记录在高端内存或保留内存中；当系统再次出现非断电复位时，将记录的相关信息导入死机信息日志。

本发明还提供一种软件系统自动恢复的装置，包括：

系统安全版本生成模块，用于生成系统恢复需要的系统安全版本；

系统安全版本调用模块，用于激活生成的所述系统安全版本，并触发系统恢复模块；

系统恢复模块，用于利用所述激活的系统安全版本对需要恢复的系统进行恢复操作。

所述的系统安全版本生成模块具体包括：

检测时间长度设置模块，用于设置对被检测系统进行安全性检测的时间长度值，并将该时间长度值提供给正常运行监测模块；

正常运行监测模块，用于对被检测系统的正常运行进行监测，并将监测结果上报给安全性检测模块；

安全性检测模块，用于接收正常运行监测模块的监测结果，并在接收到所述监测结果后确认所述被检测系统通过安全性检测，之后触发系统安全版本备份模块；

系统安全版本备份模块，用于对通过安全性检测的系统的数据区与程序区进行备份，生成所述的系统安全版本；

或者，所述的系统安全版本生成模块具体包括：

用户设定模块，用于将当前运行系统直接设定为系统安全版本，并触发系统安全版本备份模块；

系统安全版本备份模块，用于对由所述用户设定模块设定为系统安全版本的当前运行系统的数据区与程序区进行备份，生成所述的系统安全版本。

所述正常运行监测模块具体包括：

正常运行时间记录模块，用于对系统运行时间进行计时，并在系统正常复位后，对系统的运行时间重新计时，当系统运行至由检测时间长度设置模块提供的检测时间长度后，触发业务正常连接监测模块和系统复位监测模块上报监测结果给监测结果上报模块；

业务正常连接监测模块，在正常运行时间记录模块开始计时后被触发，用于监测被检测系统在所述安全性检测的时间长度内业务的连接是否正常，并在系统业务能够正常连接时将该监测结果提供给监测结果上报模块；否则，等待正常运行时间记录模块的下一次计时被触发；

系统复位监测模块，在正常运行时间记录模块开始计时后被触发，用于监测被检测系统在所述安全性检测的时间长度运行是否出现异常断电或异常复位情况，如果出现所述异常情况，则等待正常运行时间记录模块的下一次

计时被触发，否则，将系统正常复位或未出现异常断电的监测结果提供给监测结果上报模块，并在系统正常复位时，触发正常运行时间记录模块。

监测结果上报模块，用于接收所述业务正常连接监测模块和系统异常监测模块的监测结果，并在接收到该两个模块的监测结果后，将系统正常运行的监测结果上报给所述安全检测模块，否则，继续等待下一次安全性检测的时间长度内上述两个模块的监测结果。

所述的装置还包括:

系统安全版本可用标识设置模块，用于为所述的系统安全版本设置可用标识。

系统安全版本可用判断模块，用于判断当前是否存在系统安全版本的可用标识，并在存在可用标识时触发系统安全版本调用模块。

所述装置还包括:

故障信息记录模块，当系统数据被严重破坏，并导致无法调用系统安全版本时，自动触发，用于记录此时系统的状态数据，捕获异常中断信息，并将寄存器、堆栈和/或函数调用栈信息记录在高端内存或保留内存中;

故障信息导入模块，当系统下次出现非断电复位时，自动触发，用于将故障信息记录模块所记录的信息导入死机信息日志。

所述的装置还包括:

系统运行状态标识模块，用于根据预先设定的规则标识系统的运行状态。

所述的预先设定的规则包括:

若当前运行系统初次被加载或重新被激活或数据被破坏，则标识该系统处于不安全状态;

若当前运行系统为被激活的所述系统安全版本，则标识该系统处于安全状态;

若当前运行系统通过安全性检测，则标识该系统处于安全状态；

若用户主动将当前运行的系统的状态设定为安全状态，则标识该系统处于安全状态。

由上述本发明给出的技术方案可见，本发明能够在尽可能短的时间内，恢复软件系统，重新建立业务，最大程度的保障系统运行的可靠性。同时，本发明能够有效简化用户恢复软件系统时操作的复杂性，并降低用户误操作的可能性，因此，本发明的实现也能够降低对用户，如基站维护人员能力的要求。相应地，本发明能够帮助运营商有效降低利益损失与业务流失，并有助于提高用户对运行商的信任度。

## 附图说明

图1是本发明具体实施提供的系统安全版本生成流程图；

图2是本发明具体实施提供的系统运行状态转换示意图；

图3是本发明具体实施提供的用户主动触发系统恢复流程图；

图4是本发明具体实施提供的软件系统自动恢复的装置示意图。

## 具体实施方式

本发明在实施过程中主要基于以下做法以实现对软件系统的自动恢复，即先生成系统安全版本；当软件系统需要恢复时，则调用所述的系统安全版本，并利用所述的系统安全版本对软件系统进行自动恢复处理。

首先具体说明所述的系统安全版本。

本发明中，所述系统安全版本可通过以下两种方法生成：

方法一、通过对当前运行的系统进行安全性检测，由通过该安全性检测的系统生成；

方法二、由用户主动将当前运行系统设定为所述的系统安全版本。

结合图1，具体说明所述方法一中所述系统安全版本的生成过程。

步骤11、加载被检测系统，即基站（或其他类似设备，如中继站）软件系统初次加载当前运行系统，或者用户重新激活新的软件系统为当前运行系统，并将该当前运行系统作为所述的被检测系统；

步骤12、系统自动对被检测系统的运行时间清零；

步骤13、之后启动被检测系统的运行时间定时器；

所述的定时器的时间长度由用户根据需要自行设定。

步骤14、当被检测系统运行到定时器设定的时间长度后，检查系统的正常运行时间是否已达到或超过预先设定的用于检测被检测系统安全性的时间长度，即检测时间长度，如果达到或超过，则该被检测系统通过安全性检测，并设定该通过安全性检测的系统为系统安全版本；否则，执行步骤12；

其中，定时器中设定的时间长度需要至少为所述的预先设定的检测时间长度。

所述预先设定的检测时间长度可以由用户根据自身要求或经验自行设定。

并且，所述的正常运行需要满足的条件是：

被检测系统的业务能够正常连接，其中，业务连接是否正常的分析过程可通过对基站的呼叫日志得出；

并且所述的被检测系统在所述的检测时间长度内未出现断电或异常复位现象；

并且当出现正常的系统复位现象时，所述的被检测系统对已运行的时间清零，并在其运行后对运行时间重新开始计时。

步骤15、对通过安全性检测的被检测系统的数据区与程序区的文件进行备份，生成系统安全版本；

步骤16、设置存放区，并将所述的系统安全版本存放于该存放区备用；

步骤17、为存放的所述系统安全版本设置可用标识，过程结束。

对于所述方法二中所述系统安全版本的生成主要是由用户根据自身经验或根据当前运行系统的运行状况等来决定，当用户认为当前运行系统可以作为所述的系统安全版本后，即可对该当前运行系统的数据区与程序区的文件进行备份，生成系统安全版本；之后步骤同上述步骤16和步骤17，即为该生成的所述系统安全版本设置存放区和可用标识。

本发明中，如在上述关于被检测系统通过检测生成系统安全版本的过程中，涉及当前运行系统处于安全运行状态或不安全运行状态的情况，即当前运行系统可从其中一个状态转变为另一个状态，并且，当前运行系统的运行状态信息有助于用户或当前运行系统及时了解系统的运行情况。下面结合如图2，具体描述所述的系统软件版本的状态变迁过程：

a、如果当前运行系统初次被加载，或者系统软件是在重新下载后被激活的版本，此时该系统状态为不安全状态；当当前运行系统通过上述安全性检测后，该系统状态由不安全状态转为安全状态；

b、如果当前运行系统即为初次被激活的系统安全版本，即此时该系统处于安全状态，之后若该系统被重新激活或出现数据被破坏状况，则此时该系统状态由安全状态转为不安全状态；

c、如果用户主动将当前运行的系统的状态从不安全状态设定为安全状态，则此时该系统状态发生相应的转变。

可见，上述通过安全性检测的系统或用户设定为系统安全版本的当前运行系统均处于安全状态。

另外，如果系统在运行时出现崩溃的状态，如CPU运行出现严重故障，或某任务长时间运行导致“看门狗”叫，或发生单板死机的情况，此时系统无法再调用系统安全版本对当前运行系统进行恢复，本发明针对该种情况给

出的解决方案是，记录此时系统状态数据，捕获异常中断信息，同时将此时一些相关信息，如寄存器、堆栈和/或函数调用栈等信息记录到高端内存或保留内存中，当下次设备出现非断电复位时，将上述相关信息导入到死机信息日志中，以便为后续针对所发生的问题的定位和分析提供一种手段。

上述生成的所述系统安全版本在基站等设备的软件系统需要恢复时作备用。所述系统安全版本对需要恢复的系统所进行的恢复处理可在两种情况下被触发，一种是用户主动要求恢复系统，如用户根据当前运行系统的运行状态为不安全状态，但为确保基站软件系统的稳定运行，用户在当前运行系统未出现异常时，即要求调用可能存在的系统安全版本。此时用户自行触发系统恢复流程；一种为当前运行系统运行出现异常，自动触发系统恢复流程。

下面结合附图3，以用户的主动触发为例具体说明本发明对所述软件系统自动恢复的过程:

步骤31、用户（如基站软件系统维护人员）在客户端发起恢复系统的指令;

步骤32、用户通过系统安全版本可用标识判断当前是否存在系统安全版本，如果不存在，执行步骤33，否则，执行步骤34;

步骤33、系统构造寻找系统安全版本失败的响应，回复用户，即当前无可用的系统安全版本，过程结束;

步骤34、系统判断出当前存在可用的系统安全版本后，向用户发出要求确认加载系统安全版本操作的消息;

步骤35、用户确认加载系统安全版本的操作;

步骤36、当前运行系统取出所述的系统安全版本，覆盖当前运行系统的程序区和数据区，完成加载操作;

步骤37、当前运行系统向用户回复加载成功的消息，并复位基站（或其

他类似设备）以待运行，过程结束。

上述为本发明中用户主动触发恢复系统的过程，系统自动触发的恢复过程与由用户主动触发的恢复过程的实质相同，即当系统在运行中发生故障或者在复位后无法正常启动（如任务挂死导致基站复位、其他异常复位等）时，自动检测是否存在可用的系统安全版本，如果存在，则自动加载系统安全版本，由所述系统安全版本的数据区与程序区覆盖当前运行系统的数据区与程序区，复位基站；如果不存在，则系统将无法实现加载所述系统安全版本的操作。

本发明还提供一种如图4所示的软件系统自动恢复的装置，主要包括以下功能的模块：

（1）系统安全版本生成模块

用于生成所述的系统安全版本。

当由被检测系统通过安全性检测生成系统安全版本时，所述的系统安全版本生成模块具体包括：

检测时间长度设置模块，用于设置对被检测系统进行安全性检测的时间长度值，并将该时间长度值提供给正常运行监测模块；

正常运行监测模块，用于对被检测系统的正常运行进行监测，并将监测结果上报给安全性检测模块；

所述正常运行监测模块具体包括：

正常运行时间记录模块，用于对系统运行时间进行计时，并在系统正常复位后，对系统的运行时间重新计时，当系统运行至由检测时间长度设置模块提供的检测时间长度后，触发业务正常连接监测模块和系统复位监测模块上报监测结果给监测结果上报模块；

业务正常连接监测模块，在正常运行时间记录模块开始计时后被触发，用于监测被检测系统在所述安全性检测的时间长度内业务的连接是否正常，

并在系统业务能够正常连接时将该监测结果提供给监测结果上报模块；否则，等待正常运行时间记录模块的下一次计时被触发；

系统复位监测模块，在正常运行时间记录模块开始计时后被触发，用于监测被检测系统在所述安全性检测的时间长度运行是否出现异常断电或异常复位情况，如果出现所述异常情况，则，等待正常运行时间记录模块的下一次计时被触发，否则，将系统正常复位或未出现异常断电的监测结果提供给监测结果上报模块，并在系统正常复位时，触发正常运行时间记录模块。

监测结果上报模块，用于接收所述业务正常连接监测模块和系统异常监测模块的监测结果，并在接收到该两个模块的监测结果后，将系统正常运行的监测结果上报给所述安全检测模块，否则，继续等待下一次安全性检测的时间长度内上述两个模块的监测结果。

安全性检测模块，用于接收正常运行监测模块的监测结果，并在接收到所述监测结果后确认所述被检测系统通过安全性检测，之后触发系统安全版本备份模块；

系统安全版本备份模块，用于对通过安全性检测的系统的数据区与程序区进行备份，生成所述的系统安全版本；

当由用户主动设定系统安全版本时，所述的系统安全版本生成模块具体包括：

用户设定模块，用于将当前运行系统直接设定为系统安全版本，并触发系统安全版本备份模块；

系统安全版本备份模块，用于对由所述用户设定模块设定为系统安全版本的当前运行系统的数据区与程序区进行备份，生成所述的系统安全版本。

（2）系统安全版本可用标识设置模块

由系统安全版本存放模块触发，用于为所述的系统安全版本设置可用标识。

（3）系统安全版本可用判断模块

用于判断当前是否存在由所述系统安全版本可用标识设置模块设置的系统安全版本的可用标识，如果存在，则触发系统安全版本调用模块。

（4）系统安全版本调用模块

用于激活所述的系统安全版本，并触发系统恢复模块。

（5）系统恢复模块

用于由所述系统安全版本对需要恢复的系统进行恢复。

所述的系统恢复模块具体用于将所述的系统安全版本的数据区与程序区覆盖需要恢复的系统的数据区与程序区，并复位所述的软件系统。

本发明中除提供上述用于对需要恢复的系统进行恢复的各模块之外，还提供下列各模块:

（6）故障信息记录模块

当系统数据被严重破坏，并导致无法调用系统安全版本时，自动触发，用于记录此时系统的状态数据，捕获异常中断信息，同时将寄存器、堆栈和/或函数调用栈信息记录在高端内存或保留内存中;

（7）故障信息导入模块

当系统下次出现非断电复位时，自动触发，用于将故障信息记录模块所记录的信息导入死机信息日志。

（8）系统运行状态标识模块

用于标识系统的运行状态为安全状态或不安全状态，用户或当前运行系统可通过该标识查看当前运行系统的运行状况。

所述系统运行状态标识模块根据相应的规则来标识系统运行状态，所述的相应的规则包括:

如果当前运行的系统初次被加载或者重新被激活，则触发系统状态自动标识模块标识此时该系统状态为不安全状态;

当当前运行的系统通过所述的安全性检测后，该系统状态由不安全状态转为安全状态，触发系统状态自动标识模块标识该系统状态为安全状态；

如果当前运行的系统即为被激活的所述的系统安全版本，此时该系统处于安全状态；之后若该系统重新被激活或出现数据被破坏的状况，则该系统状态由安全状态转为不安全状态，触发系统状态自动标识模块标识该系统状态为不安全状态；

如果用户主动将当前运行的系统的状态从不安全状态设定为安全状态，则此时该系统状态从不安全状态转变为安全状态，触发系统状态自动标识模块标识该系统状态为安全状态。

综上所述，本发明提供的技术方案能够在尽可能短的时间内，恢复软件系统，重新建立业务，最大程度的保障系统运行的可靠性。同时，本发明能够有效简化用户恢复软件系统时操作的复杂性，并降低用户误操作的可能性，因此，本发明的实现也能够降低对用户，如基站维护人员能力的要求。相应地，本发明能够帮助运营商有效降低利益损失与业务流失，并有助于提高用户对运行商的信任度。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，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该以权利要求书的保护范围为准。

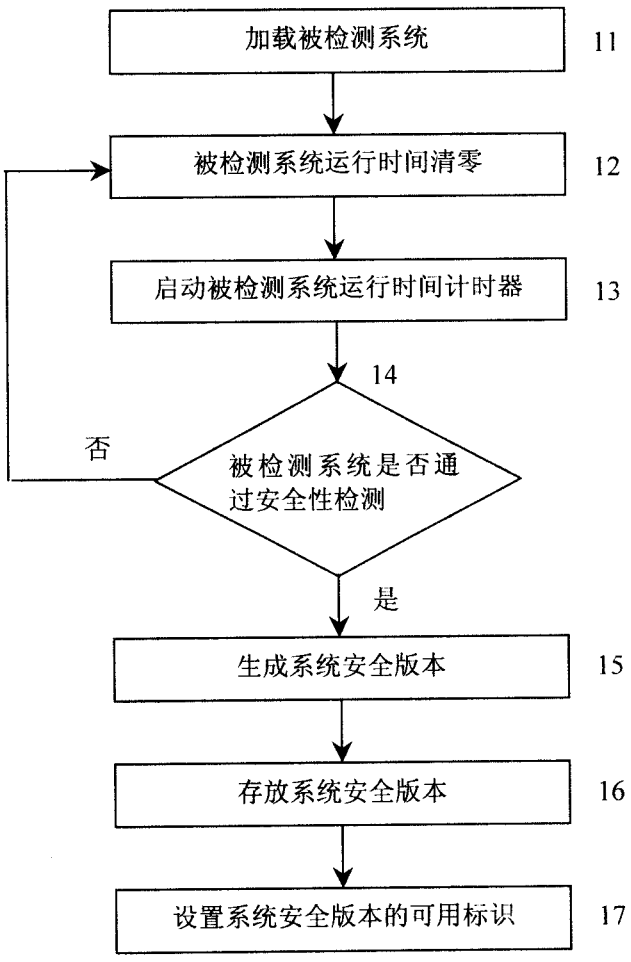

加载被检测系统
11
被检测系统运行时间清零
12
启动被检测系统运行时间计时器
13
14
被检测系统是否通过安全性检测
否
是
生成系统安全版本
15
存放系统安全版本
16
设置系统安全版本的可用标识
17

图1

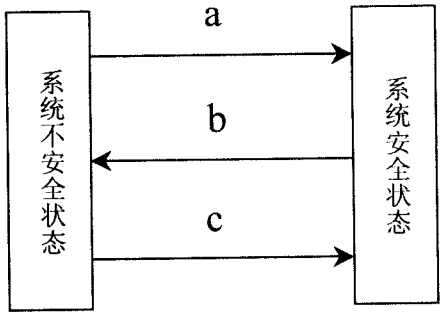

a
b
c
系统不安全状态
系统安全状态

图2

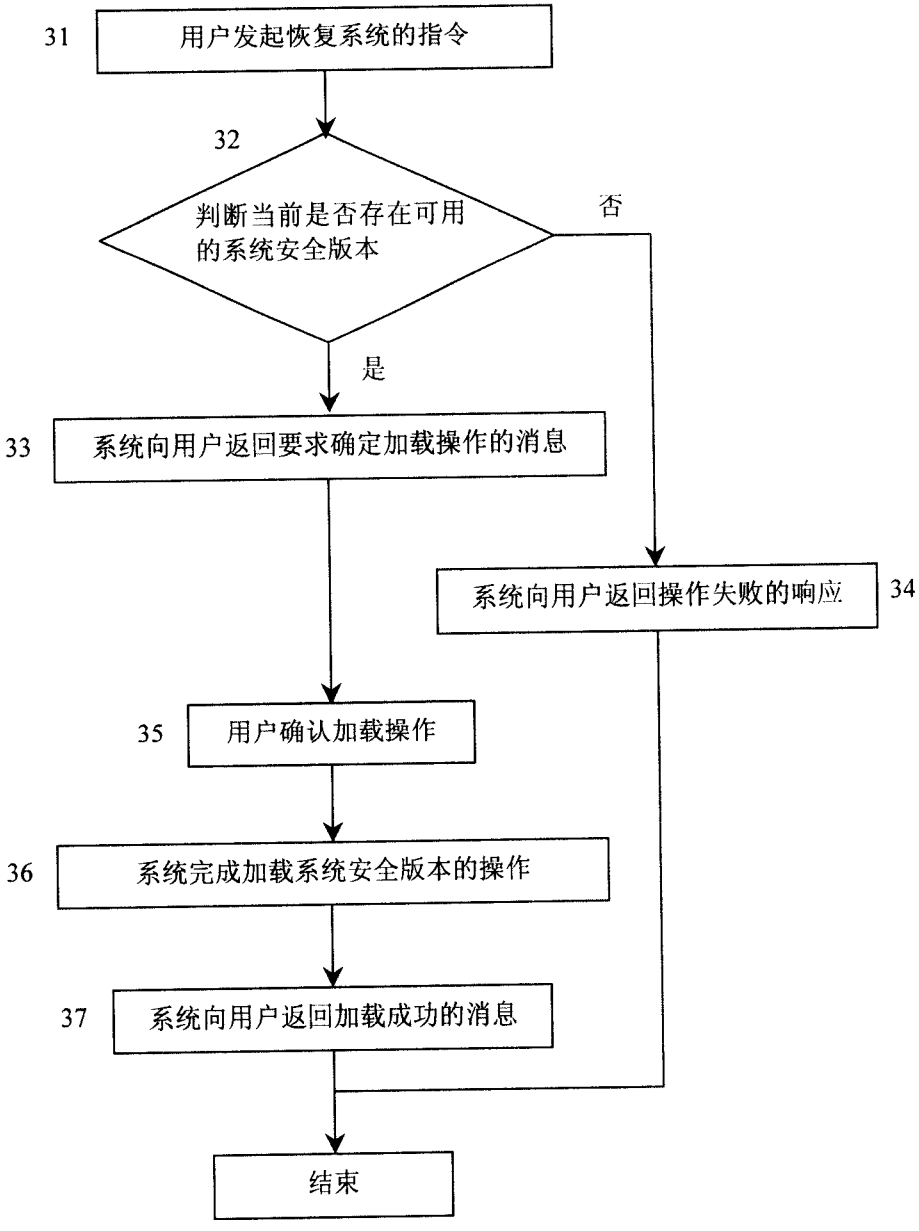

31
用户发起恢复系统的指令
32
判断当前是否存在可用的系统安全版本
否
是
33
系统向用户返回要求确定加载操作的消息
系统向用户返回操作失败的响应
34
35
用户确认加载操作
36
系统完成加载系统安全版本的操作
37
系统向用户返回加载成功的消息
结束

图3

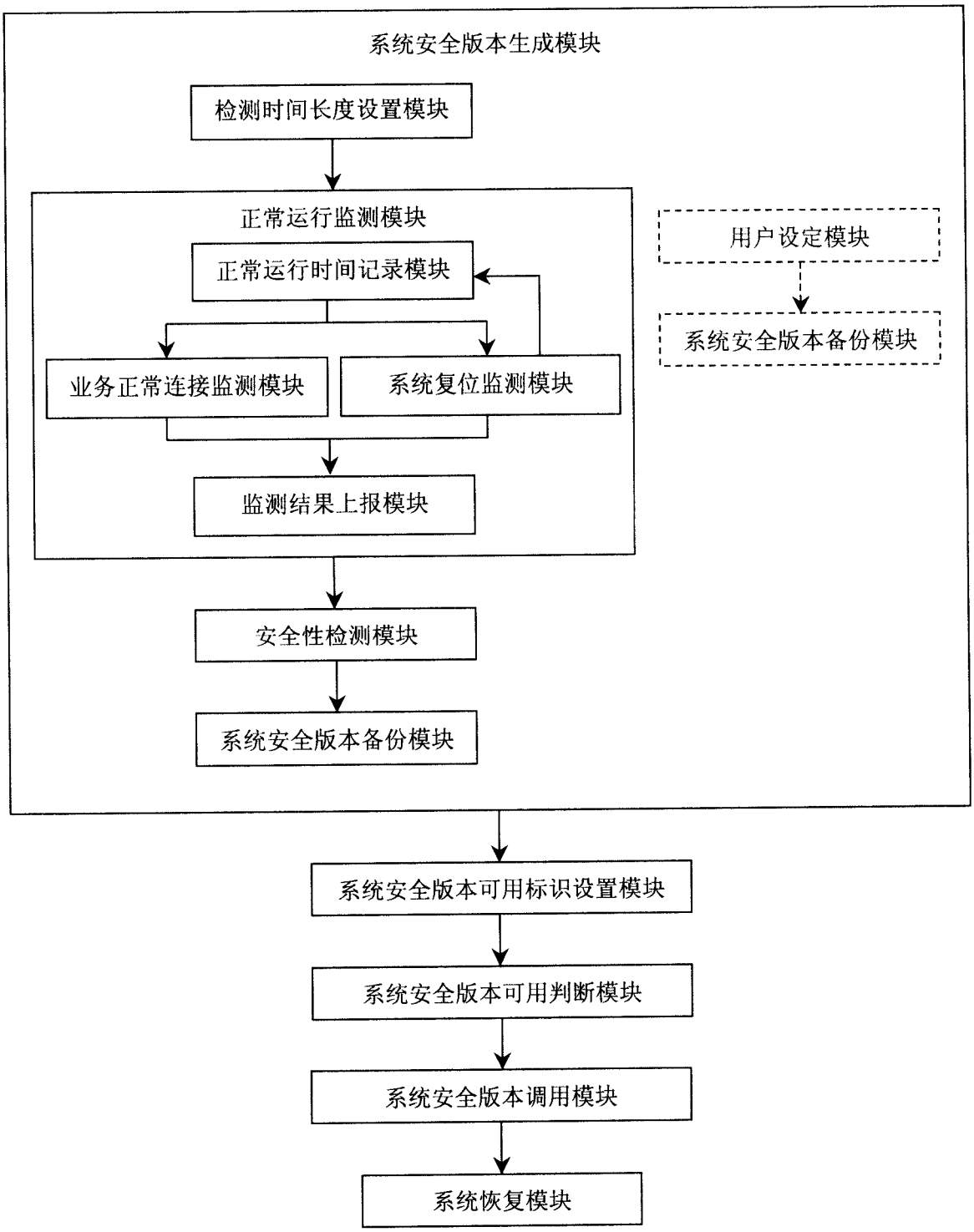

系统安全版本生成模块
检测时间长度设置模块
正常运行监测模块
正常运行时间记录模块
业务正常连接监测模块
系统复位监测模块
监测结果上报模块
用户设定模块
系统安全版本备份模块
安全性检测模块
系统安全版本备份模块
系统安全版本可用标识设置模块
系统安全版本可用判断模块
系统安全版本调用模块
系统恢复模块

图4