(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107894894 A
(43)申请公布日 2018.04.10

(21)申请号 201710905349.3

(22)申请日 2017.09.29

(30)优先权数据
15/283,552 2016.10.03 US

(71)申请人 施耐德电气IT公司
地址 美国罗得岛州

(72)发明人 彭文春 林新晓

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 韩倩倩 杨明钊

(51)Int.Cl.
G06F 8/65(2018.01)
G06F 9/445(2018.01)

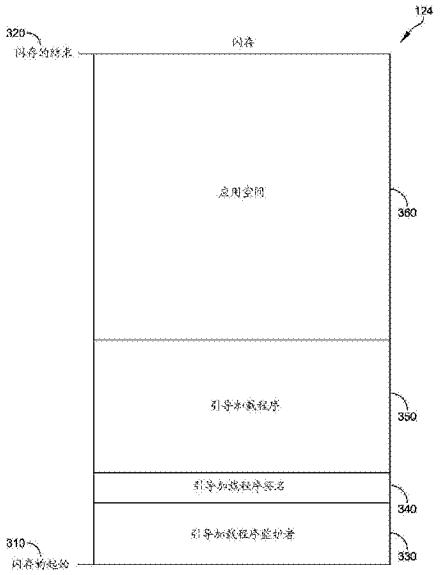
权利要求书2页 说明书8页 附图6页

(54)发明名称

用于更新设备软件的系统和方法

(57)摘要

本公开涉及用于更新设备软件的系统和方法。设备包括处理器和存储器。处理器被配置为确定引导加载程序区域是否不包含有效的引导加载程序指令集，定位引导加载程序指令集，以及将引导加载程序指令集复制到引导加载程序区域。然后，处理器执行来自引导加载程序区域的引导加载程序指令集。



CN 107894894 A

1.一种设备,包括:

存储器;以及

处理器,所述处理器耦合到所述存储器并被配置为执行以下操作:

确定引导加载程序区域不包含有效的引导加载程序指令集,

定位引导加载程序指令集,

将所述引导加载程序指令集复制到所述引导加载程序区域,以及

执行来自所述引导加载程序区域的所述引导加载程序指令集。

2.根据权利要求1所述的设备,其中,所述处理器还被配置为读取引导加载程序签名以确定所述引导加载程序区域不包含有效的引导加载程序指令集。

3.根据权利要求1所述的设备,其中,所述处理器还被配置为使用所述引导加载程序指令集的长度和存储器指针中的至少一个来定位所述引导加载程序指令集。

4.根据权利要求1所述的设备,其中,所述处理器还被配置为从所述存储器的预定位置读取值以定位所述引导加载程序指令集。

5.根据权利要求1所述的设备,其中,所述引导加载程序区域在所述存储器内。

6.根据权利要求1所述的设备,其中,所述处理器还被配置为缓冲所述引导加载程序指令集并且存储所述引导加载程序指令集的位置的指示符。

7.根据权利要求6所述的设备,其中,所述处理器还被配置为将所述指示符存储在所述存储器的预定位置处。

8.一种控制具有处理器和存储器的设备的方法,所述方法包括:

确定引导加载程序区域不包含有效的引导加载程序指令集;

定位引导加载程序指令集;

将所述引导加载程序指令集复制到所述引导加载程序区域;以及

执行来自所述引导加载程序区域的所述引导加载程序指令集。

9.根据权利要求8所述的方法,还包括读取引导加载程序签名以确定所述引导加载程序区域不包含有效的引导加载程序指令集。

10.根据权利要求8所述的方法,还包括使用所述引导加载程序指令集的长度和存储器指针中的至少一个来定位所述引导加载程序指令集。

11.根据权利要求8所述的方法,还包括从所述存储器的预定位置读取值以定位所述引导加载程序指令集。

12.根据权利要求8所述的方法,还包括缓冲所述引导加载程序指令集并且存储所述引导加载程序指令集的位置的指示符。

13.根据权利要求12所述的方法,其中,所述指示符被存储在所述存储器的预定位置处。

14.一种控制具有处理器和存储器的设备的方法,所述方法包括:

接收新的引导加载程序指令集的通知;

在所述存储器中存储所述新的引导加载程序指令集的位置的指示符;以及

在所述存储器中存储所述存储器的引导加载程序区域不包含有效的引导加载程序指令集的指示。

15.根据权利要求14所述的方法,还包括接收所述新的引导加载程序指令集并缓冲所

述新的引导加载程序指令集。

16.根据权利要求14所述的方法，还包括擦除所述引导加载程序区域。

17.根据权利要求14所述的方法，还包括将所述新的引导加载程序指令集复制到所述引导加载程序区域中。

18.根据权利要求14所述的方法，其中，所述新的引导加载程序指令集的位置的指示符包括存储器指针和所述新的引导加载程序指令集的长度中的至少一个。

19.根据权利要求14所述的方法，其中，所述新的引导加载程序指令集的位置的指示符被存储在所述存储器的预定位置处。

20.根据权利要求14所述的方法，其中，存储所述新的引导加载程序指令集的所述位置的指示符包括存储所述引导加载程序区域不包含有效的指令集的指示。

用于更新设备软件的系统和方法

[0001] 背景

[0002] 1.公开的领域

[0003] 本文中所描述的至少一些实施例通常涉及具有存储的(例如可存储在固件中的)指令集的设备,以及用于更新指令集的方法。

[0004] 2.相关技术的讨论

[0005] 许多设备利用执行软件指令的可编程组件并要求启动时的起始点。这样的设备包括处理器或微控制器,其经常将初始指令或者在某些情况下将所有指令和应用存储在耦合到控制器或被包含在控制器内的闪速存储器中。通常,存储在闪存中的引导加载程序(bootloader)包括初始指令,该初始指令可以在将控制传递到核心应用或操作系统之前建立起始变量或进行上电自检(POST)。这样的引导加载程序也可能负责处理对核心应用的更新,有时引导加载程序本身可能需要更新。

[0006] 概述

[0007] 本公开的各个方面涉及用于管理对引导加载程序的更新的方法和装置。

[0008] 根据一个方面,设备包括存储器和耦合至存储器的处理器。处理器被配置为确定引导加载程序区域不包含有效的引导加载程序指令集,定位引导加载程序指令集,将引导加载程序指令集复制到引导加载程序区域,以及执行来自引导加载程序区域的引导加载程序指令集。

[0009] 根据一些实施例,处理器还被配置为读取引导加载程序签名以确定引导加载程序区域不包含有效的引导加载程序指令集。在一些实施例中,处理器还被配置为使用引导加载程序指令集的长度和存储器指针中的至少一个来定位引导加载程序指令集。在一些实施例中,处理器还被配置为从存储器的预定位置读取值以定位引导加载程序指令集。在一些实施例中,引导加载程序区域在存储器内。在一些实施例中,处理器还被配置为缓冲引导加载程序指令集并且存储引导加载程序指令集的位置的指示符。处理器还可以被配置为将指示符存储在存储器的预定位置处。

[0010] 根据另一方面,一种控制具有处理器和存储器的设备的方法包括:确定引导加载程序区域不包含有效的引导加载程序指令集,定位引导加载程序指令集,将引导加载程序指令集复制到引导加载程序区域,以及执行来自引导加载程序区域的引导加载程序指令集。

[0011] 根据一些实施例,该方法包括读取引导加载程序签名以确定引导加载程序区域不包含有效的引导加载程序指令集。在一些实施例中,该方法包括使用引导加载程序指令集的长度和存储器指针中的至少一个来定位引导加载程序指令集。在一些实施例中,该方法包括从存储器的预定位置读取值以定位引导加载程序指令集。在一些实施例中,该方法包括缓冲引导加载程序指令集并存储引导加载程序指令集的位置的指示符。指示符可被存储在存储器的预定位置处。

[0012] 根据另一方面,一种控制具有处理器和存储器的设备的方法包括:接收新的引导加载程序指令集的通知,在存储器中存储新的引导加载程序指令集的位置的指示符,并在

存储器中存储存储器的引导加载程序区域不包含有效的引导加载程序指令集的指示。

[0013] 根据一些实施例，该方法包括接收新的引导加载程序指令集并缓冲新的引导加载程序指令集。在一些实施例中，该方法包括擦除引导加载程序区域。在一些实施例中，该方法包括将新的引导加载程序指令集复制到引导加载程序区域中。在一些实施例中，新的引导加载程序指令集的位置的指示符包括存储器指针和新的引导加载程序指令集的长度中的至少一个。在一些实施例中，新的引导加载程序指令集的位置的指示符被存储在存储器的预定位置处。在一些实施例中，存储新的引导加载程序指令集的位置的指示符包括存储引导加载程序区域不包含有效的指令集的指示。

[0014] 下面详细讨论了以及这些示例性方面和实施例的优点。此外，应理解，上述信息和下面的详细描述都仅仅是各个方面和实施例的说明性的示例，并且旨在提供用于理解所要求保护的方面和实施例的性质和特性的综述或者框架。本文公开的任何实施例可与任何其它实施例组合。对“实施例”、“示例”、“一些实施例”、“一些示例”、“可替代的实施例”、“各种实施例”、“一个实施例”、“至少一个实施例”、“这个和其它实施例”等的提及并不一定是相互排他的，且意欲指示关于实施例描述的特定特征、结构或特性可被包括在至少一个实施例中。本文中这类术语的出现不一定都指同一实施例。

附图说明

[0015] 以下参考附图讨论了至少一个实施例的各个方面，该附图并不旨在按比例绘制。附图中，在各个图中示出的每个相同的或者接近相同的组件用相似的数字表示。为了清楚起见，并非每个组件都可以在每个图中被标记。在附图中：

[0016] 图1是根据本公开的方面和实施例的设备的框图；

[0017] 图2是现有技术中闪速存储器对一组固件指令的常规分配的示意图；

[0018] 图3是根据本公开的方面的闪速存储器对一组固件指令的示例分配的示意图；

[0019] 图4是根据本公开的方面的用于更新引导加载程序的示例过程的流程图；

[0020] 图5是根据本公开的方面的闪速存储器对一组固件指令的另外的示例分配的示意图；以及

[0021] 图6是根据本公开的方面的用于引导(boot)设备的示例过程的流程图。

[0022] 详细描述

[0023] 许多设备在执行指令的处理器或控制器的帮助下操作，并且在初始启动(例如上电或启动)时，处理器或控制器具有固定位置，指令从该固定位置被存储和读取。然后，固定位置处的指令可以进一步控制或指示处理器或控制器，并且可以将控制传递给各种程序或应用，并且系统可以根据操作系统的方案运行，该操作系统的方案本身是一组指令或另一应用。通常，由处理器或控制器执行的第一组程序指令是引导加载程序。引导加载程序尤其可以在将控制传递给核心应用或操作系统之前建立操作参数或进行系统测试。引导加载程序可能涉及更新核心应用，有时引导加载程序本身需要更新。当引导加载程序更新时，存在有些事情可能会出错而使引导加载程序处于无效或破坏的状态的风险。由于引导加载程序是控制器试图执行的第一程序，因此破坏或无效的引导加载程序可使控制器无法做任何事情，从而导致设备发生故障。

[0024] 图1图示了根据本公开的设备100。设备100包括提供设备的特定功能操作和/或核

心操作的操作硬件110，其示例在下面进一步描述。设备100部分地由包括处理器122的控制器120控制。控制器120至少部分地通过处理器122执行保存在存储器124中的指令来控制硬件110。在一些实施例中，存储器124可被包括在控制器120之内，或者存储器124可以是被包括在控制器120中的内部存储器或耦合到控制器120的其他存储器的任何组合。控制器120还耦合到一个或更多个数据/通信接口130，诸如网络接口132和外围接口134。网络接口132可以耦合到网络140以提供与其他系统的通信并且接收外部数据或指令集。示例网络包括有线网络(例如，以太网、令牌环、FDDI、DOCSIS等)或无线网络(例如，Wi-Fi、IEEE 802.11、蜂窝等)。外围接口134允许各种外围设备的耦合，例如可用于在外部存储数据或指令集或提供外部数据或指令集的存储介质150。外围接口134的示例包括通用串行总线(USB)、安全数字(SD)、紧凑型闪存(CF)、IEEE 1394、火线，雷电(thunderbolt)等。另外，控制器120耦合到用户接口160，以允许用户控制和配置控制器120、操作硬件110、接口130以及设备100的其他方面。用户接口160可以包括诸如例如开关、鼠标、小键盘、键盘和/或触摸屏的输入设备或者可以供该输入设备之用，并且可以包括诸如例如可视指示器、可听指示器和/或显示器的输出设备或者可以供该输出设备之用。

[0025] 可具有操作硬件110和控制器120的设备100的示例包括但不限于诸如路由器和交换机的通信网络工具；环境控制装备，诸如供热、通风和空气调节(HVAC)系统、传感器和控制装置、计算机房空气处理装置(CRAH)、机架式空气调节器(RMAC)和计算机房空气调节器(CRAC)；计算设备；配电装备，诸如发电机、不间断电源(UPS)、受管的电源插座和各种控制装置；以及工业过程管理装备，诸如自动控制设备(ACD)、流量和温度传感器、致动器、加热器等。这些设备中的每一个可以具有操作硬件110以提供设备的有益操作。操作硬件110的示例例如在UPS中包括但不限于：电力输入端口、电力输出端口、传感器、监控器、电力转换硬件以及诸如电池的能量储存器。在另一示例中，HVAC系统可以包括诸如电动机、风扇、压缩机、冷凝器、线圈、加热元件、温度和气流传感器等的操作硬件110。可以是任何这样的设备100的一部分的控制器120的示例组件包括但不限于ARM®Cortex®-M处理器系列。

[0026] 在至少一些设备中，控制器120包括处理器122和诸如闪速存储器的固定存储器124，处理器122将在启动时从该固定存储器124获取第一指令。引导加载程序是由处理器122可执行的、存储在通常从存储器124的第一存储器位置开始的引导加载程序区域中的一组指令。

[0027] 在本文所描述的至少一些实施例中，存储器124的开始用被称为引导加载程序监护者(guardian)的新的指令集编程，该新的指令集有助于防止设备100由于对引导加载程序的中断的更新而变得不可操作。引导加载程序监护者允许确定有效的引导加载程序不存在，并允许通过找到新的引导加载程序并将其复制到引导加载程序区域中来完成引导加载程序更新。以这种方式，处理器122始终具有可用于执行的有效的初始指令，并且这些指令能够从失败的引导加载程序更新中恢复。因此，即使引导加载程序更新被意外地中断，设备100也将返回到可操作状态。

[0028] 本文所讨论的方法和系统的示例并不将其应用限于下面描述中阐述的或者在附图中示出的组件的结构和布置的细节。方法和系统能够在其他实施例中实施，并且能够以各种方式实践或执行。本文提供的特定实现的示例仅用于说明性目的而并不旨在限制。具体来说，结合任何一个或更多个示例论述的动作、组件、元件以及特征不旨在排除任何其他

的示例中的类似作用。

[0029] 另外，本文所用的措辞和术语是出于描述的目的，不应视为具有限制性。对于本文中以单数提及的系统和方法的示例、实施例、组件、元件或者动作的任何引用也可以包含包括复数的实施例，并且对于本文的任何实施例、组件、元件或者动作以复数的任何引用也可以包含仅包括单数的实施例。单数形式或者复数形式的引用并不旨在限制当前公开的系统或者方法、它们的组件、动作或者元件。本文使用的“包括”、“包含”、“含有”、“涉及”及其变型旨在包括其后列举的项目及其等价物以及额外的项目。“或”的引用可解释为包括性的，使得使用“或”所描述的任何术语可以指示所描述的术语的单个、多于一个以及全部中的任何一种。另外，在本文件和通过引用并入的文件之间术语的用法不一致的情况下，在并入的文件中的术语用法作为对本文件中的术语用法的补充；对于不可协调的不一致，以本文件中的术语用法为准。

[0030] 图2图示了存储器200(例如，闪速存储器)的常规布置，该存储器200包含要由设备中的控制器处理器执行的指令。存储器200具有在存储器200内的开始存储器位置或第一存储器位置处的起始210以及在结束存储器位置或最后存储器位置处的结束220。存储器200具有引导加载程序230和应用空间240。引导加载程序230在起始210处开始，并且包括供处理器在引导时运行的一组指令。通常，在处理器完成引导加载程序230指令之后，处理器(例如，通过引导加载程序指令)被指导以从应用空间240获取下一个指令，一个或更多个核心应用程序或操作系统被存储在该应用空间中。在不同的时间，任何应用或引导加载程序230可需要被更新以例如向设备添加功能或者修正在对设备编程中的缺陷或错误。

[0031] 当应用空间240中的一组指令要被更新时，引导加载程序230可被启动(即，处理器执行来自引导加载程序230的指令)以处理更新过程。执行引导加载程序230的指令的处理器可以例如经由网络接口从网络或耦合到物理接口的存储器卡或其他地方接收新的应用固件(即，新的指令集)。对于某些类型的存储器设备，例如与闪速存储器的典型情况一样，存储器空间需要在新的内容可被写入空间之前被擦除。因此，引导加载程序230可以指示处理器首先擦除应用空间240的部分或全部以容纳更新的应用指令。为了完成应用更新，引导加载程序230指示处理器将新的应用固件写入到应用空间240中。

[0032] 当引导加载程序230要被更新时，引导加载程序230指令可以以与当应用空间240中的指令需要更新时的方式大致相同的方式处理该过程。然而，引导加载程序230指令通常不应在引导加载程序230指令正在从存储器200活跃地运行时从存储器200中擦除，因此处理器通常将诸如引导加载程序230的一部分的某部分代码复制到另一存储器区域，例如存储器200的另一区域或复制到耦合到处理器的其他存储器，例如，随机存取存储器(RAM)。复制的部分代码然后控制处理器以继续以下过程：擦除存储器200的一部分(存储器200中的需要包含新的引导加载程序指令集的部分)，接收新的引导加载程序固件以及将新的引导加载程序写入到存储器200的被擦除部分中。

[0033] 上述引导加载程序更新过程具有固有的风险，一旦存储器200中的包含现有的引导加载程序230的部分开始被擦除，则存储器200将不再具有有效的引导加载程序230，直到该过程完全完成。如果在此期间例如由于电力中断而发生故障，则设备在下一次启动时将无法启动，因为处理器在其查找存储器200的起始210时将找不到有效的指令。

[0034] 图3图示了包含根据本文公开的方面和实施例的布置和指令的存储器124(例如，

闪存)。存储器124具有起始310和结束320,并且包含引导加载程序监护者330指令集和引导加载程序签名340,处理器122将在开始或启动序列期间很早执行或首先执行引导加载程序监护者330指令集,引导加载程序签名340将指示引导加载程序350是否有效。存储器124还包括应用空间360,其包含在成功开始或启动时要执行的一个或更多个应用。在图3中所示的示例实施例中,引导加载程序监护者330从存储器124的起始310开始,引导加载程序350通常可能已经驻留在其中。在其他实施例中,引导加载程序监护者330可以位于存储器124或耦合到处理器122的另一存储器中的其他地方,但位于处理器122将在开始或启动过程中执行的位置,例如引导加载程序监护者330将在开始或启动过程中首先执行或非常早地执行的位置中。

[0035] 如下面更详细地描述的,引导加载程序监护者330在引导加载程序更新失败时提供恢复机制,部分地通过依赖引导加载程序签名340指示这样的失败。引导加载程序监护者330可以是相对小的一组指令,如果引导加载程序更新失败,则其将恢复新的引导加载程序,否则的话,将使引导加载程序350照常执行。

[0036] 图4是图示由设备100中的处理器122执行的引导加载程序更新过程400的流程图。参照图5进一步描述引导加载程序更新过程400,图5图示了在引导加载程序更新过程400的部分期间存储器124的使用分配。在引导加载程序更新过程400的开端处,引导加载程序350指令集运行且是有效的,并且引导加载程序签名340指示引导加载程序350是有效的并且驻留在其在存储器124中的常用位置(例如,引导加载程序区域530)中。在块410处接收新的引导加载程序510并在块420处缓冲到闪存(例如,存储器124)中。为了在块420处将新的引导加载程序510缓冲到闪存中,可能需要过程400擦除闪存的区域以为新的引导加载程序510腾出空间,诸如图5中所示的区域。在块430处,过程400还存储新的引导加载程序510的位置的指示符520。在引导加载程序更新失败的情况下,新的引导加载程序510的位置的指示符520可以由引导加载程序监护者330使用以恢复并建立新的引导加载程序510作为引导加载程序350的替代。

[0037] 在一个实施例中,指示符520被写入到存储器124的预定位置处,诸如例如,靠近存储器124的结束320,并且新的引导加载程序510被缓冲为紧邻指示符520。指示符520可以是指向存储器124中的新的引导加载程序510的开始位置的存储器地址或存储器偏移的指针。结果是,引导加载程序监护者330可以在必要时根据指示符520知道或确定新的引导加载程序510的位置和长度。新的引导加载程序510的长度是以诸如例如字节、字、长字等的度量单位的新的引导加载程序510指令集的大小。在其他实施例中,新的引导加载程序510和/或指示符520中的任一个可以在其他地方被缓冲或写入,或者替代指针可以指示指示符520或新的引导加载程序510的位置。另外,在其他实施例中,指示符520可以仅包括新的引导加载程序510的长度,或者可以包括新的引导加载程序510的位置和长度两者。例如,利用图5的相同布置,其中指示符520正好在存储器124的结束320处并且新的引导加载程序510占据存储器124中的紧挨着指示符520、在指示符520前面的区域,指示符520可以指示新的引导加载程序510的长度而不是起始位置,并且根据新的引导加载程序510的长度可以容易地确定起始位置。

[0038] 在(块410)接收到新的引导加载程序510并将其进行缓冲(块420)并且存储新的引导加载程序510的位置的指示符520(块430)后,下一个主要操作将是将新的引导加载程序

510复制到其在存储器124中的预期位置(其是引导加载程序区域530)中。可能需要擦除引导加载程序区域530。引导加载程序区域530可以是当前引导加载程序350驻留的位置,因此开始擦除或复制到存储器124的引导加载程序区域530中将使当前引导加载程序350无效,并且如果新的引导加载程序510的复制出于任意原因而未能完成,则引导加载程序区域530中的指令集将有错误。因此,在块440处,引导加载程序更新过程400存储引导加载程序签名340,该引导加载程序签名340指示引导加载程序区域530在过程400在块450处擦除引导加载程序区域530并在块460处将新的引导加载程序510复制到引导加载程序区域530之前是不可信的(例如,有错误的或无效)。如果新的引导加载程序510到引导加载程序区域530中的复制(块460)成功完成,则过程400在块470处存储引导加载程序签名340,该引导加载程序签名340指示引导加载程序区域530包含有效的引导加载程序指令集。

[0039] 在实施例中,引导加载程序签名340可具有特定值以指示引导加载程序区域530包含有效的引导加载程序指令集,并且任何其他值可以指示引导加载程序区域530不包含有效的引导加载程序指令集。在其他实施例中,引导加载程序签名340可具有特定值以指示引导加载程序区域530不包含有效的引导加载程序指令集,并且任何其他值可以指示引导加载程序区域530确实包含有效的引导加载程序指令集。

[0040] 在一些实施例中,当前引导加载程序350可以包含使处理器122执行引导加载程序更新过程400的指令。因此,当前引导加载程序350可使处理器122在其擦除引导加载程序区域530(块450)之前将至少一部分代码复制到其他地方(例如,RAM),因为当前引导加载程序350驻留在引导加载程序区域530中,其将被擦除或以其他方式覆盖。复制到例如RAM的部分代码可以是对执行引导加载程序更新过程400的剩余部分必需的指令集。

[0041] 在实施例中,新的引导加载程序510可以被缓冲在除存储器124之外的不同的存储器中。在实施例中,新的引导加载程序510可以被提供在缓冲的位置中,因此进行接收(块410)和缓冲(块420)可以不是过程400的一部分。在实施例中,块430和块440可以通过使用引导加载程序签名340作为指示新的引导加载程序510的位置和/或长度的指示符520来组合成一个动作。例如,引导加载程序签名340的值为零可以指示引导加载程序区域530具有存储在其中的有效的引导加载程序指令集,以及除零之外的引导加载程序签名340的值可以是存储器124中的指向新的引导加载程序510的位置的指针。

[0042] 在实施例中,存储无效的引导加载程序的指示符(块440)可以通过擦除存储器124中的包含引导加载程序签名340的区域来实现。在实施例中,引导加载程序签名340可以是诸如引导加载程序350的引导加载程序的一部分,使得擦除引导加载程序区域(块450)也擦除引导加载程序签名340,从而完成存储无效的引导加载程序的指示符(块440)。类似地,将新的引导加载程序510复制到引导加载程序区域350中(块460)因此可以包括写入引导加载程序签名340,从而完成存储有效的引导加载程序的指示符(块470)。在替代实施例中,引导加载程序签名340(即,有效的引导加载程序的指示符)可以结合复制新的引导加载程序510(块460)被存储(块470),或者可以作为与复制新的引导加载程序510(块460)分离的步骤被存储(块470)。存储引导加载程序签名340(块470)的变化可以有利地适应各种类型的存储器,诸如那些需要整个块、页、扇区等被擦除以作为可用于在其任何部分中存储新信息的单元的存储器。

[0043] 引导加载程序更新过程400将如上所述完成,除非它被中断。例如,在过程400期间

的断电可能导致引导加载程序更新不能完成。如果在引导加载程序区域530已经开始被擦除(块450)或复制到其中(块460)之后发生这样的中断,则引导加载程序区域530将不具有存储在其中的有效的引导加载程序指令集,因此一旦电力恢复,该设备可能无法引导。然而,本文公开的方面和实施例提供了从这样的场景的恢复机制。

[0044] 图6是图示至少一个引导加载程序监护者过程600的流程图。引导加载程序监护者330包含指令集,每当设备100启动时,该指令集将使处理器122执行过程600。在实现过程600时,在判定块610处,引导加载程序监护者330指令集使处理器122针对引导加载程序区域530是否包含有效的引导加载程序指令集的指示来检查引导加载程序签名340。如果引导加载程序签名340指示有效的引导加载程序(是),则处理器122将通过例如在块660处将控制传递到引导加载程序来继续正常启动操作。

[0045] 如果引导加载程序签名340指示有效的引导加载程序并不驻留在引导加载程序区域530中(否),例如当如上所讨论的在引导加载程序更新过程400期间发生电力故障或其他中断时,过程600将试图通过找到新的引导加载程序510并将新的引导加载程序510复制到引导加载程序区域530中来完成引导加载程序更新。过程600在块620处通过读取指示符520(如上所述其也可以是引导加载程序签名340)来找到新的引导加载程序510,在块630处擦除引导加载程序区域530,并在块640处将新的引导加载程序510复制到引导加载程序区域530中。当复制(块640)成功完成时,过程600在块650处存储指示引导加载程序区域530包含有效的引导加载程序指令集的引导加载程序签名340。接下来,过程600在块660处将使处理器122通过例如将控制传递到引导加载程序指令集来继续正常操作。

[0046] 在实施例中,引导加载程序监护者330可以是仅执行图6中所示的过程600的一组指令,因此可以是可能本身永远不需要更新的相对小的一组指令。

[0047] 在实施例中,引导加载程序更新过程400的行为可以不同于图4中所示的行为。例如,不是擦除引导加载程序区域530(块450)和复制新的引导加载程序510(块460),而是引导加载程序更新过程400可以引起重新启动,这又将导致引导加载程序监护者过程600在启动时擦除引导加载程序区域530(块630)并复制新的引导加载程序510(块640)。

[0048] 另外,在实施例中,以上所描述的和在图4和图6中所示的一个或更多个过程块可以以与所描述或示出的方式或顺序不同的方式或顺序执行,或者可能根本不执行。在备选方案中,引导加载程序更新过程400可以通过替代的处理器而不是处理器122来执行,替代的处理器包括通过例如耦合到外围接口134或与控制器120结合的维护接口的暂时耦合的处理器。存储器124可以是嵌入在处理器122或嵌入在包括处理器122的微控制器中的板载存储器或闪速存储器,或者可以是诸如闪存、EEPROM或其它可重写非易失性存储器的外部存储器。对数据或指令集的缓冲或其他存储可以是针对其他形式的存储器,诸如光盘或磁盘、可编程ROM、RAM等。

[0049] 设备100可以是本地或远程设备,并且可以具有有限的资源,诸如存储器(例如,存储器124),并且引导加载程序监护者330和引导加载程序350可以各自符合由例如存储器124容纳的应用特定的大小参数。引导加载程序监护者330和引导加载程序350可以进一步符合更严格的大小要求,以使存储器124对应用空间360中的核心应用和/或操作系统具有足够的存储容量。存储器124可以包括各种存储介质类型、模式或配置,并且可以包括跨一个或更多个存储介质类型、模式或配置的多个存储器的组合。

[0050] 至此，已经描述了至少一个实施例的几个方面，应认识的是，各种变化、修改和改善对于本领域的技术人员来说将是很容易想到的。这种变化、修改和改善旨在成为本公开的一部分，并且旨在处于本发明的精神和范围内。因此，前文的描述和附图仅仅是示例性的。

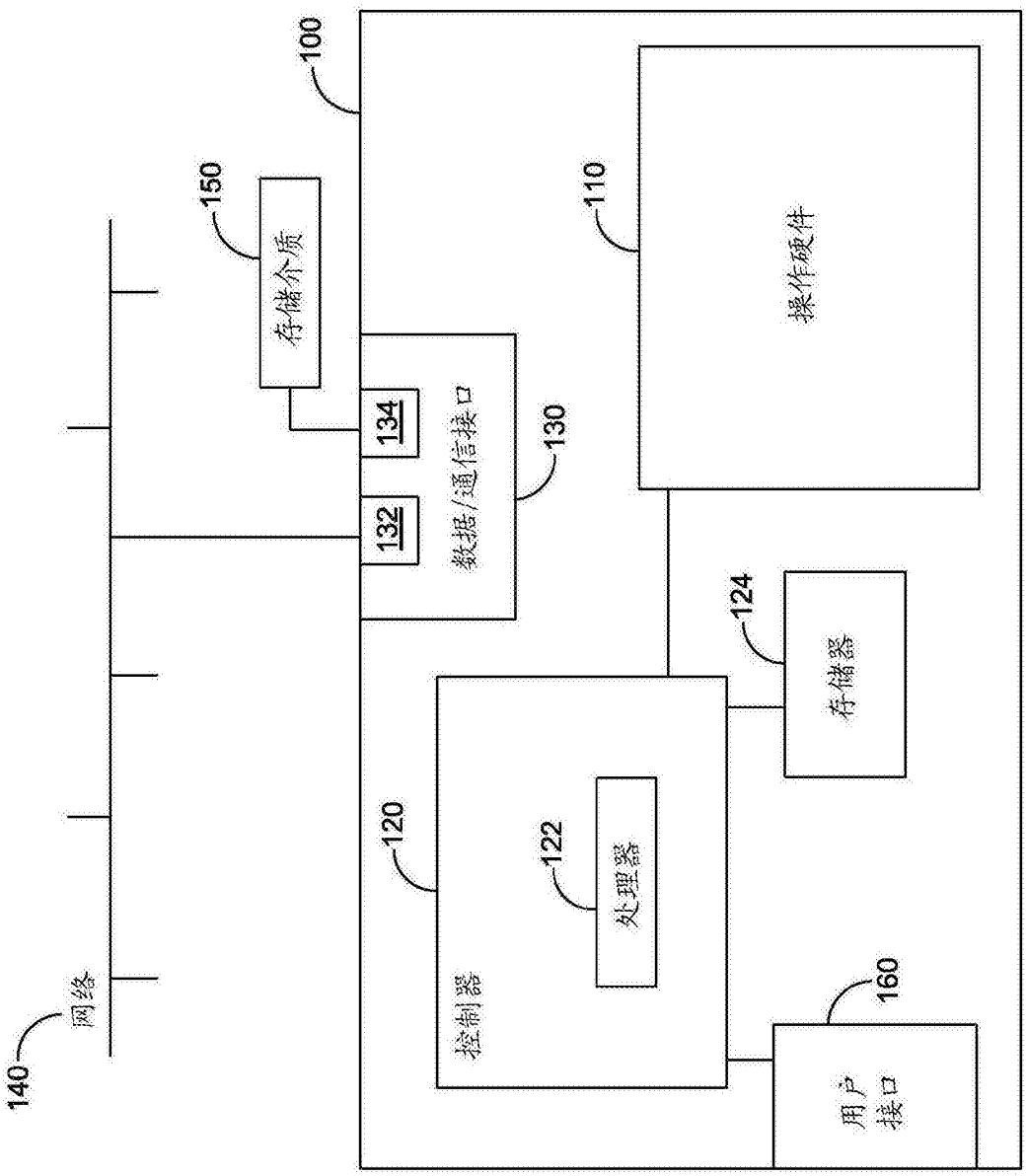

100
150
存储介质
110
操作硬件
134
132
数据/通信接口
130
124
存储器
120
122
处理器
控制器
160
用户接口
网络
140

图1

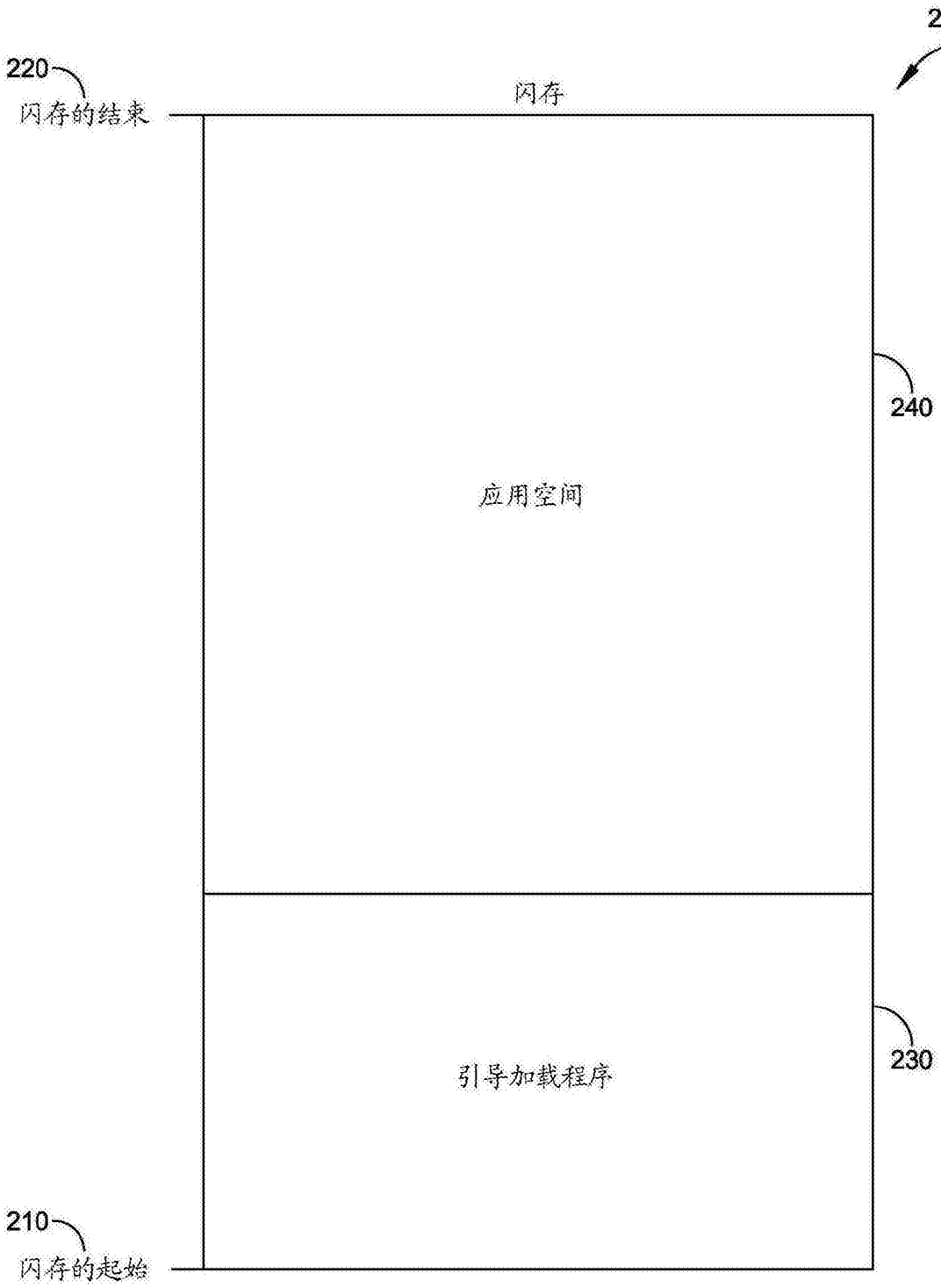


图2

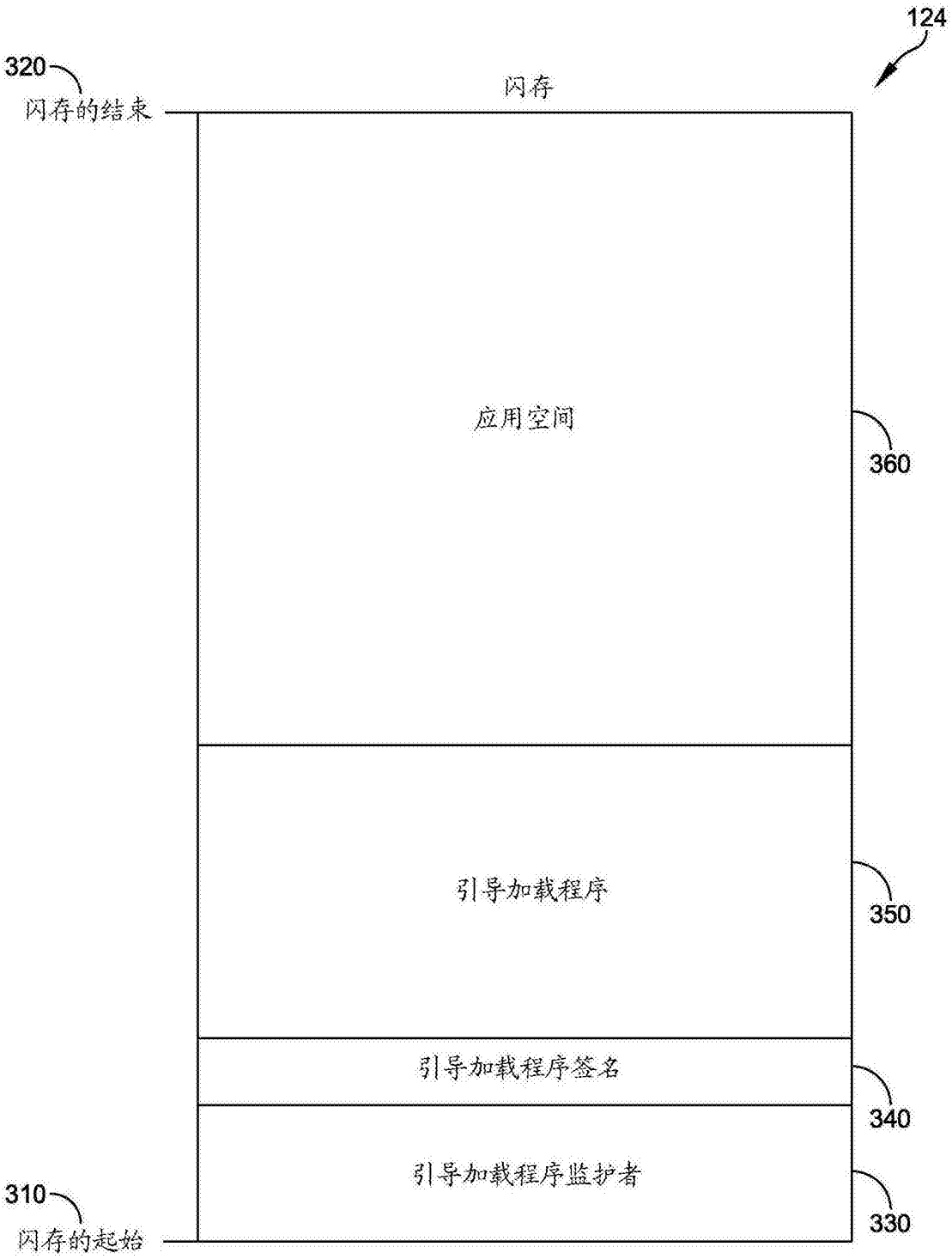

124
320
闪存的结束
闪存
应用空间
360
引导加载程序
350
引导加载程序签名
340
引导加载程序监护者
330
310
闪存的起始

图3

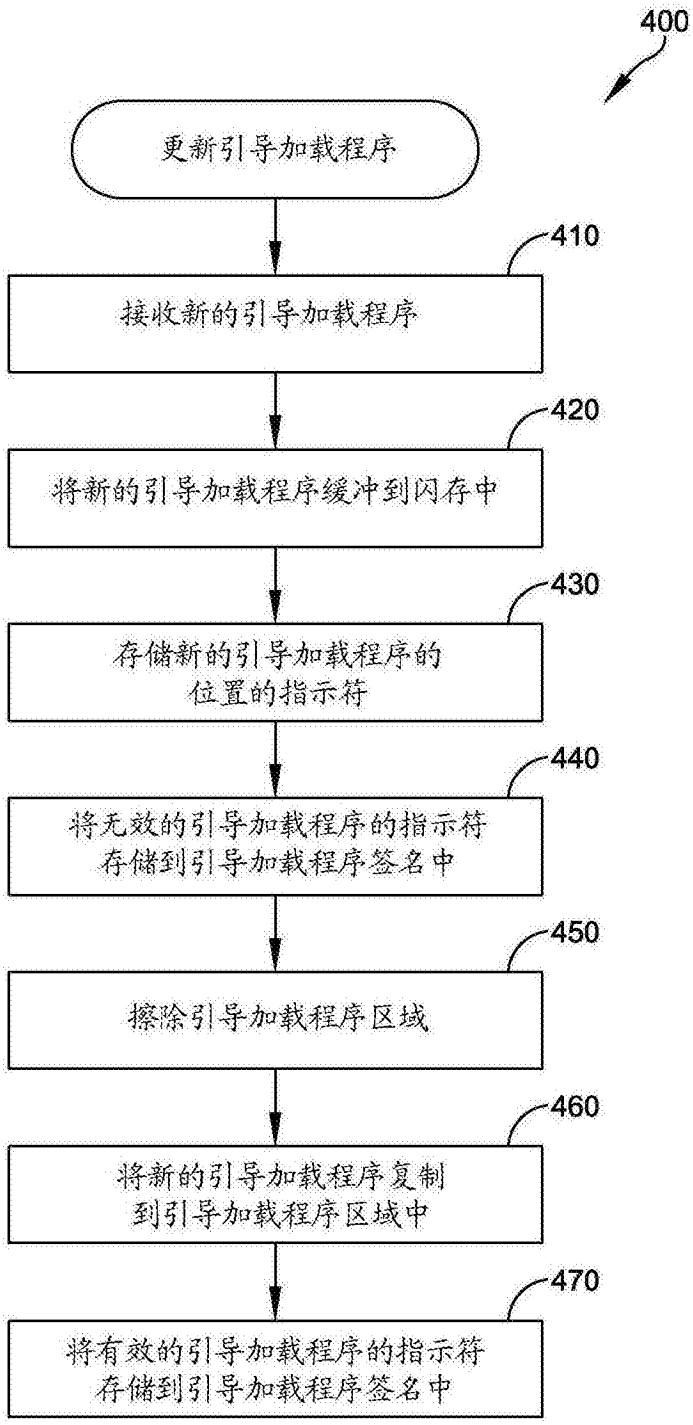

400
更新引导加载程序
410
接收新的引导加载程序
420
将新的引导加载程序缓冲到闪存中
430
存储新的引导加载程序的
位置的指示符
440
将无效的引导加载程序的指示符
存储到引导加载程序签名中
450
擦除引导加载程序区域
460
将新的引导加载程序复制
到引导加载程序区域中
470
将有效的引导加载程序的指示符
存储到引导加载程序签名中

图4

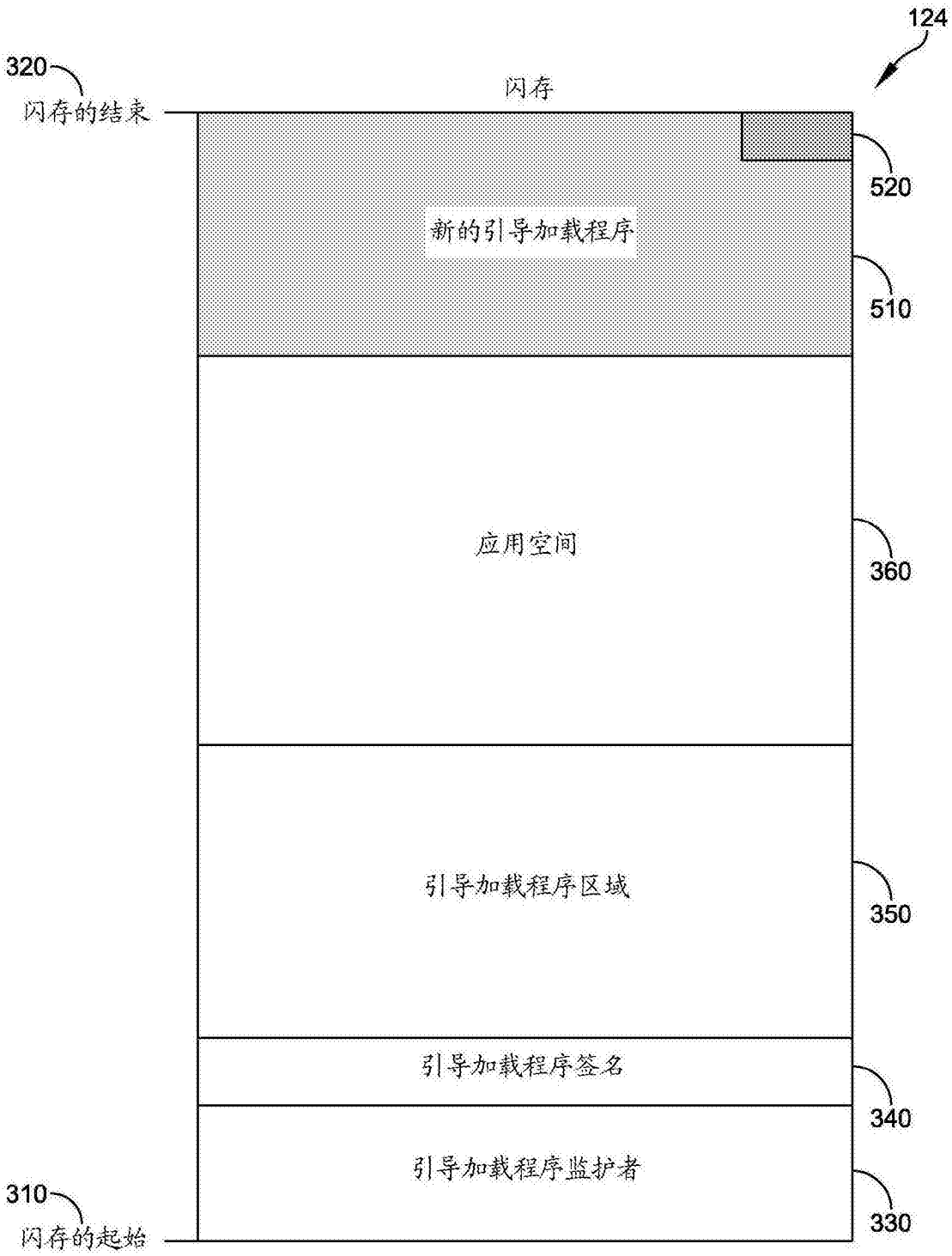

124
320
闪存的结束
闪存
520
新的引导加载程序
510
应用空间
360
引导加载程序区域
350
引导加载程序签名
340
引导加载程序监护者
330
310
闪存的起始

图5

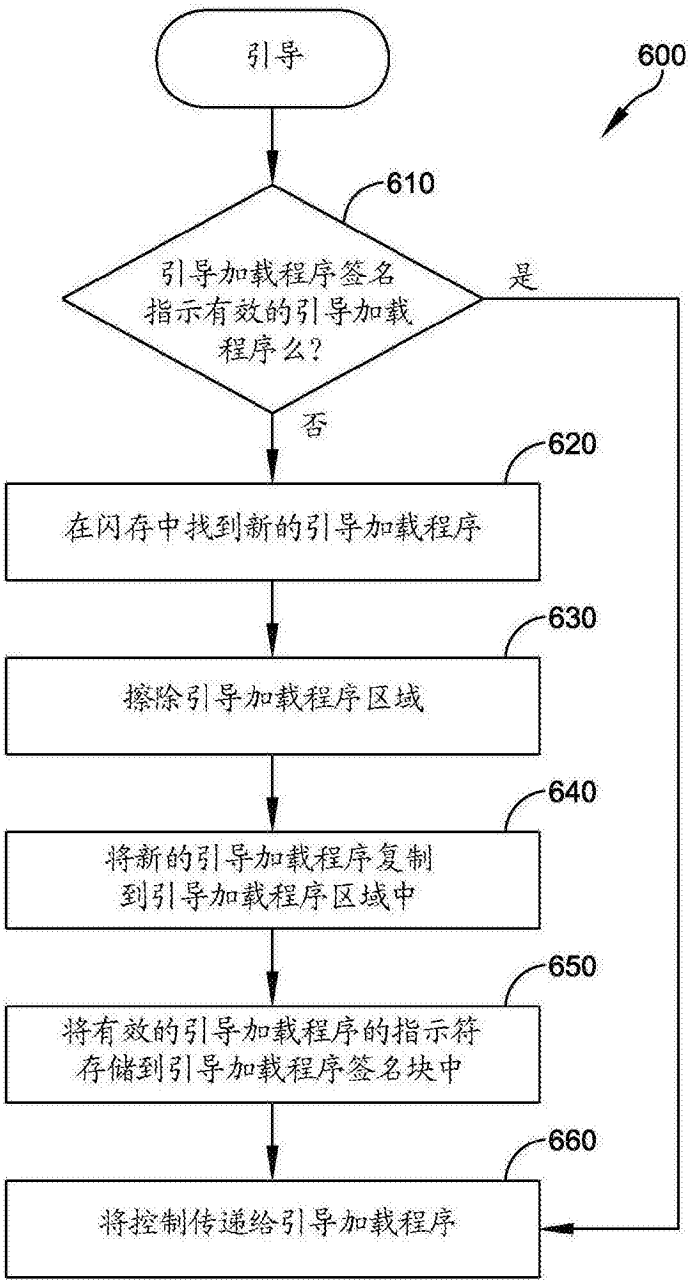

引导
600
610
引导加载程序签名指示有效的引导加载程序么?
是
否
620
在闪存中找到新的引导加载程序
630
擦除引导加载程序区域
640
将新的引导加载程序复制到引导加载程序区域中
650
将有效的引导加载程序的指示符存储到引导加载程序签名块中
660
将控制传递给引导加载程序

图6