(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 103403672 A
(43)申请公布日 2013.11.20

(21)申请号 201180067653.6

(22)申请日 2011.04.29

(85)PCT申请进入国家阶段日
2013.08.15

(86)PCT申请的申请数据
PCT/US2011/034673 2011.04.29

(87)PCT申请的公布数据
WO2012/148426 EN 2012.11.01

(71)申请人 惠普发展公司,有限责任合伙企业
地址 美国德克萨斯州

(72)发明人 爱德华·D·纳普顿

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 康泉 宋志强

(51)Int.Cl.
G06F 9/06(2006.01)
G06F 9/44(2006.01)

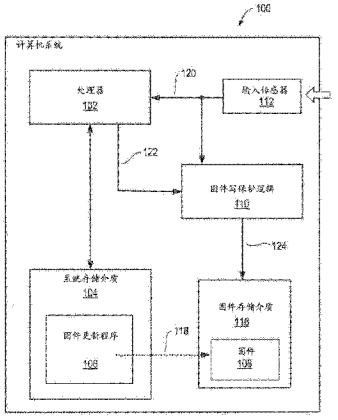
权利要求书2页 说明书6页 附图4页

(54)发明名称

计算机系统固件更新

(57)摘要

更新固件的技术包括输入传感器和处理器,该输入传感器提供信号,如果该信号是从输入传感器提供的,则处理器运行更新程序来发起固件的更新,并且处理器不从更新程序的指令的运行中提供该信号。



CN 103403672 A

1. 一种计算机系统，包括：

输入传感器，提供信号；

固件存储介质；以及

处理器，如果从所述输入传感器提供所述信号则所述处理器运行更新程序的指令，以发起所述固件存储介质上的固件的更新，其中所述处理器不从所述更新程序的所述指令的运行中提供所述信号。

2. 如权利要求 1 所述的计算机系统，其中所述处理器被配置为运行所述更新程序的指令，以在所述处理器发起所述固件存储介质上的所述固件的更新以前检查所述信号是否是由所述输入传感器提供的。

3. 如权利要求 1 所述的计算机系统，其中所述处理器被配置为运行所述更新程序的指令，以在不检查所述信号是否是由所述输入传感器提供的情况下发起所述固件存储介质上的所述固件的更新。

4. 如权利要求 1 所述的计算机系统，其中所述处理器被配置为运行所述更新程序的指令，以在所述处理器发起所述固件存储介质上的所述固件的更新以后验证所述固件存储介质上的所述固件的至少一部分是否被更新。

5. 如权利要求 1 所述的计算机系统，进一步包括显示构件，所述显示构件联接至基座构件，以使所述显示构件能相对于所述基座构件可变定位，并且其中所述输入传感器被配置为基于所述显示构件相对于所述基座构件的位置生成输入信号。

6. 如权利要求 1 所述的计算机系统，其中所述处理器被配置为运行所述更新程序的指令，来为所述输入传感器的触发提供用户提示。

7. 如权利要求 1 所述的计算机系统，其中所述固件存储介质包括非易失性存储器。

8. 如权利要求 1 所述的计算机系统，其中所述固件包括包含基本输入输出系统（BIOS）的指令。

9. 一种由处理器运行更新程序的指令来更新计算机系统的固件存储介质上的固件的方法，所述方法包括：

从输入传感器接收输入信号；

确定所述输入信号是否来自所述输入传感器并且不来自所述计算机系统的所述处理器运行所述更新程序的指令；以及

如果确定所述输入信号来自所述输入传感器并且不来自运行所述更新程序的指令，则所述处理器运行所述更新程序的指令，以发起所述计算机系统的固件存储上的所述固件的更新。

10. 如权利要求 9 所述的方法，进一步包括：

所述处理器运行所述更新程序的指令，来为触发所述输入传感器提供提示。

11. 如权利要求 9 所述的方法，进一步包括：

所述处理器运行所述更新程序的指令，以在所述处理器发起固件存储上的所述固件的更新以前检查所述信号是否是由所述输入传感器提供的。

12. 如权利要求 9 所述的方法，进一步包括：

所述处理器运行所述更新程序的指令，以在不检查所述信号是否是由所述输入传感器提供的情况下发起固件存储上的所述固件的更新。

13. 一种物品，包括至少一个计算机可读存储介质，所述计算机可读存储介质存储更新程序的指令，所述更新程序的指令在由处理器运行时促使计算机系统：

确定来自输入传感器的信号是否是由所述处理器运行所述更新程序的指令生成的；以及

如果确定所述输入信号来自所述输入传感器，而不来自所述更新程序的指令的运行，则发起所述计算机系统的固件存储介质上的固件的更新。

14. 如权利要求 13 所述的物品，进一步包括：

运行所述更新程序的指令，该指令促使所述计算机系统为触发所述输入传感器提供提示。

15. 如权利要求 13 所述的物品，进一步包括：

运行所述更新程序的指令，该指令促使所述计算机系统在所述处理器发起固件存储上的所述固件的更新以前检查所述信号是否是由所述输入传感器提供的。

计算机系统固件更新

背景技术

[0001] 一些计算机系统，例如膝上型计算机或笔记本计算机，可以包含固件，固件指用于控制与计算机系统关联的硬件组件的操作的软件指令。例如，一些计算机系统可以包括用于存储基本输入／输出系统(BIOS)的非易失性存储介质，基本输入／输出系统包括检查计算机系统内的硬件组件正在正常工作的软件指令。存在可能想要更新固件的时候，例如当发布固件的新版本来更正问题或改善操作时。

附图说明

[0002] 图 1 是更新固件的示例计算机系统的框图。

[0003] 图 2 是更新固件的示例计算机系统的立体图。

[0004] 图 3 是更新固件的另一示例计算机系统的立体图。

[0005] 图 4 是图示更新计算机系统上的固件的方法的流程图的示例。

具体实施方式

[0006] 如上所述，一些计算机系统，例如膝上型计算机或笔记本计算机，可以包含固件。这样的固件能够被称为用于控制与计算机系统关联的硬件组件的操作的软件指令。例如，一些计算机系统可以包括用于存储基本输入／输出系统(BIOS)的非易失性存储介质，基本输入／输出系统能够包括检查计算机系统内的硬件组件正在正常工作的软件指令。存在可能想要更新固件的时候，例如当发布固件的新版本来更正问题或改善操作时。

[0007] 然而，在更新计算机系统上的固件时可能遇到问题。例如，用户可能接收固件更新程序，以更新计算机系统上的固件。然而，可能难以验证更新程序的源的可靠性，并且即使未授权该程序执行更新，该程序也可能继续更新固件。该更新程序可能是未经授权的程序，并且可能将像病毒这样的不期望的代码引入固件中，病毒可能破坏计算机系统上的数据或以别的方式导致计算机系统不可操作。因此，可能想要开发用于对更新计算机系统上的固件的鉴权和验证过程进行改善的技术。

[0008] 在一些示例中，本申请可以提供帮助解决与更新计算机系统上的固件的鉴权和验证有关的问题的技术。例如，本申请描述具有一种计算机系统，该计算机系统具有需要用户输入以使固件更新程序能继续更新计算机系统上的固件的装置。在一个示例中，计算机系统能够配置有运行固件更新程序的处理器，如果从输入传感器提供信号，则发起固件更新，其中处理器不从更新程序的运行中提供该信号。换言之，如果用户因用户触发输入传感器而促使该传感器生成信号，则更新固件。输入信号由硬件生成，而不通过运行软件指令的处理器由软件生成，因为由软件的运行生成的信号可能由未经授权的软件生成。输入传感器能够检测用户的存在，计算机能够在其继续更新固件以前检查该信号。

[0009] 在一个示例中，计算机系统能够是具有显示构件的膝上型计算机，该显示构件可旋转地联接至基座构件。该计算机系统能够包括输入传感器，该输入传感器能够检测显示构件与基座构件的相对位置，并且能够检测计算机系统何时处于闭合位置，也就是计算机

显示构件和基座构件何时彼此邻近或彼此处于预定位置。该计算机系统能够提示用户将计算机系统置于闭合位置，该闭合位置能够允许该计算机系统继续更新固件。当计算机系统处于打开位置时，该计算机系统将不更新固件，需要用户将该计算机系统置于闭合位置。也就是说，需要用户在该计算机系统能够继续更新固件以前采取某一动作。因此，这些技术在更新固件以前需要来自用户的输入，这可以帮助减少未经授权的固件更新的可能性。

[0010] 图 1 是在来自输入传感器 112 的输入基础上更新计算机系统上的固件 108 的示例计算机系统 100 的框图。计算机系统 100 包括固件存储介质 116，固件存储介质 116 能够存储固件 108，固件 108 可以包括可由处理器 102 运行以管理计算机系统的硬件组件的软件指令。计算机系统 100 包括存储固件更新程序 106 的系统存储介质 104，固件更新程序 106 能够包括可由处理器 102 运行的软件指令，以利用来自更新程序的固件更新固件 108，如虚线箭头 118 所示。

[0011] 输入传感器 112 能够是能响应于用户的实体存在的检测而生成输入信号 120 的任何传感器装置。例如，输入传感器能够是需要用户采取某一动作来触发传感器的任何传感器装置。在一个示例中，计算机系统 100 能够是具有显示构件的膝上型计算机，该显示构件可旋转地联接至基座构件。在这种情况下，输入传感器 112 能够是开关，其能够检测显示构件相对于基座构件的位置。输入传感器 112 能够生成输入信号 120，输入信号 120 表示用户何时已将该膝上型计算机置于闭合位置(或预定的相对位置)。如下面更详细地解释的，计算机系统能够配置为在用户将计算机系统 100 置于闭合位置时更新固件 108。当计算机系统处于打开位置时，能够防止计算机系统 100 更新固件 108。

[0012] 将输入信号 120 示出为馈送至处理器 120 和固件写保护逻辑 110。处理器 102 生成被送往写保护逻辑 110 的写信号 122，写信号 122 表示处理器想要对固件存储介质 116 和固件 108 进行写。固件写保护逻辑 110 生成被送往固件存储介质 116 的写使能信号 124，以使处理器 102 能发起固件 108 的更新。写使能信号 124 能够基于输入信号 120 (其表示用户的存在或由用户触发传感器)和写信号 122 (其表示处理器 102 希望对固件存储介质 116 进行写) 生成。

[0013] 如下面进一步详细地解释的，如果输入传感器 112 基于该输入传感器的用户触发而生成输入信号 120，则处理器 102 能够运行更新程序 106 的指令，以发起固件 108 的更新。也就是说，输入信号 120 能够因用户的实体存在而生成，而不由处理器运行程序的指令而生成。更新程序 106 能够在继续发起固件 108 的更新以前检查输入信号 120 的存在。换言之，如下面进一步详细地解释的，当用户促使根据输入传感器生成信号而不因处理器运行更新程序的指令生成信号时，计算机系统 100 发起固件 108 的更新。这些技术需要在固件更新发生以前的用户输入，这可以降低未经授权的固件更新的可能性。

[0014] 如上所述，更新程序 106 能够在继续发起固件 108 的更新以前检查输入信号 120 的存在。在另一示例中，更新程序 106 能够在不检查输入信号 120 的存在情况下发起固件更新。在这种情况下，更新程序 106 能够通过开始将新固件的一部分从更新程序 106 拷贝或写至固件 108 来发起固件 108 的更新。通过读回被写的那一部分来验证固件 108 是否被更新，更新程序 106 能够检查更新是否成功。本示例依赖于使用写保护逻辑 110 和是否已生成输入信号 120。如果未生成输入信号 120，那么写使能信号 124 不被使能，这防止计算机系统 100 对固件 108 执行写操作，因此防止对固件 108 的更新。另一方面，如果生成输入

信号 120，那么写使能信号 124 被使能，这允许计算机系统 100 对固件 108 执行写操作，因此更新固件 108。

[0015] 尽管未示出，但计算机系统 100 能够包括其它硬件组件，例如键盘、硬盘驱动器、图形视频控制器、音频控制器、显示装置、通信系统和用于操作计算机系统的操作的其它组件。

[0016] 尽管未示出，但系统存储介质 104 可以包括其它程序或应用，该其它程序或应用具有可由处理器 102 运行以控制计算机系统 100 的操作的指令。例如，系统存储器 104 可以存储能够包括指令的操作系统（OS），该指令在由处理器运行时控制计算机系统 100 的操作。OS（未示出）可以包括软件（程序和数据），该软件（程序和数据）能够管理计算机硬件组件并且为各种应用程序的运行提供公共服务。在一个示例中，能够将 OS 存储在硬盘驱动器上或其它存储装置上，然后在完成固件 108 的运行后将 OS 加载到系统存储器 104 中。尽管示出单个存储介质组件 104，但应当理解，计算机系统 100 可以采用一个以上的存储器组件。

[0017] 固件 108 能够包括用于控制与计算机系统 100 关联的硬件组件（例如显示装置）的操作的软件指令。例如，固件 108 能够是基本输入 / 输出系统（BIOS），该基本输入 / 输出系统能够包括检查计算机系统内的硬件组件正在正常工作的软件指令。同样，尽管示出单个固件存储介质组件 116，但应当理解，计算机系统 100 可以采用一个以上的存储器组件。存储器组件 104 和存储器组件 116 能够包括计算机可读介质，例如易失性存储器（例如随机存取存储器等）、非易失性存储器（例如只读存储器、闪存、CD ROM 等）及二者的组合。

[0018] 处理器 102 能够是被配置为运行软件指令的任何硬件或逻辑。尽管示出单个处理器 102，但应当理解，计算机系统 100 可以采用一个以上的处理器。例如，计算机系统 100 可以包括用于控制装置的总体操作的处理器以及用于控制键盘的操作的键盘控制器。键盘控制器能够是使键盘与计算机系统接合的装置。

[0019] 图 2 示出图 1 的示例计算机系统 100 的立体图。在图 2 图示的示例中，计算机系统 100 包括膝上型计算机或笔记本计算机。然而，应当理解，计算机系统 100 可以包括其它类型的计算机装置，例如但不限于：平板个人电脑、移动电话和其它类型的便携式和 / 或手持式计算装置。在图 1 图示的示例中，计算机系统 100 包括显示构件 130，显示构件 130 通过铰接件 128 可旋转地联接至基座构件 132。图 1 所示的计算机系统 100 的组件能够布置在基座构件 132、显示构件 130 或二者的组合中。

[0020] 在图 2 图示的示例中，计算机系统 100 示出输入传感器 112，输入传感器 112 能够用于检测用户的存在且响应于用户的存在而生成输入信号 120（图 1）。输入传感器 112 需要用户采取某一动作来触发传感器，以使传感器生成信号 120。如下面说明的，为了允许计算机系统 100 更新固件，用户能够相对于基座构件 132 旋转显示构件 130，以触发输入传感器 112。输入传感器 112 包括开关 140，开关 140 用于检测显示构件 130 相对于基座构件 132 的位置。开关 140 包括可压下的按钮 142，将可压下的按钮 142 偏置为至少部分地向上延伸通过基座构件 132 的工作面 144 上的开口 138，并且偏置为响应于基座构件 132 与显示构件 130 的接触而至少部分地缩回至基座构件 132 中（例如由显示构件 130 从如图 2 所示的打开位置如通常由箭头 136 所示向相对于基座构件 132 的闭合位置移动或移动至相对于基座构件 132 的闭合位置中引起的接触）。然而，应当理解，按钮 142 可以位于其它位置，例

如在工作面 144 上的其它位置，按钮 142 位于在显示构件 130 上的反转位置，等等。此外，应当理解，可以使用其它装置和 / 或机制取代按钮 142（例如接触元件、机械触发器等）。

[0021] 计算机系统 100 能够采用输入传感器 112 来检测用户的存在，并且作为响应允许更新固件。例如，在操作中，计算机系统 100 能够运行固件更新程序 106 的指令，这能够向显示构件 130 的显示器提供提示，以请求用户是否需要更新固件 108。如下面说明的，该提示可以指导用户将膝上型计算机置于闭合位置。图 2 示出处于打开位置的计算机系统 100。用户能够通过将显示构件 130 朝箭头 136 指示的方向向基座构件 132 旋转至相对于基座构件的闭合和 / 或预定位置或者布置来对提示做出响应，显示构件 130 接近基座构件 132 并与按钮 142 搭合，从而致动开关 140。开关 140 的致动导致生成输入信号 120，计算机系统 100 利用该输入信号 120 来使能或允许固件 108 的更新。在其它示例中，开关 140 的致动能够导致通过计算机系统 100 的硬件、软件和 / 或硬件和软件的结合而生成和 / 或以其它方式处理中断和 / 或其它类型信号

[0022] 因此，在操作中，一旦计算机系统 100 闭合（例如将显示构件 130 带入相对于基座构件 132 的预定布置、距离和 / 或位置），计算机系统 100 就能够允许进行固件 108 的更新。在固件 108 已完成更新时，计算机系统 100 能够生成警报或提示。此时，用户能够通过将显示构件 130 朝箭头 134 指示的方向离开基座构件 132 旋转至相对于基座构件的打开和 / 或预定位置或者布置来将计算机系统 100 恢复至打开位置，显示构件 130 离开基座构件 132 移动并且脱离按钮 140。

[0023] 图 3 示出图 1 的计算机系统 100 的另一示例的立体图。在图 3 图示的示例中，计算机系统 100 包括另一示例输入传感器 112。将输入传感器 112 示出为包括开关 164，开关 164 具有布置在基座构件 132 中的传感器元件 166 和布置在显示构件 130 中的传感器元件 168。在操作时，输入传感器 112 能够生成输入信号 120（图 1）以允许计算机系统 100 更新固件 108。在其它示例中，输入传感器 112 能够生成中断和 / 或传输通过计算机系统 100 的硬件、软件和 / 或硬件和软件的结合生成和 / 或以别的方式处理的信号，以允许响应于传感器元件 166 和传感器元件 168 彼此被放置在预定距离内和 / 或彼此邻近的固件更新更新。计算机系统 100 在处于如图 1 所示的打开位置时不生成输入信号 120。计算机系统 100 在计算机系统处于闭合位置时生成输入信号 120。相应地，计算机系统 100 能够处于闭合位置，也就是说，当显示构件 130 处于相对于基座构件 132 的闭合布置或位置和 / 或另一预定布置或位置时，计算机系统 100 能够允许在计算机系统上进行固件更新。

[0024] 在图 3 图示的示例中，传感器元件 166 包括舌簧开关 160，传感器元件 168 包括磁体 162，使得响应于磁体 162 生成的磁场致动舌簧开关 160。相应地，舌簧开关 160 的致动导致生成输入信号 120，以允许计算机系统更新固件 108。还应当理解，舌簧开关 160 和磁体 162 的设置和 / 或位置可以是不同地互换的（例如舌簧开关 160 位于显示构件 130 中，磁体 162 位于基座构件 132 中）。此外，应当理解，在输入传感器 112 中可以使用其它类型的非机械传感器元件，以检测显示构件 130 相对于基座构件 132 的定位。

[0025] 尽管上文已在能够检测显示构件相对于基座构件的位置的传感器的背景下描述了输入传感器 112，但应当理解，输入传感器 112 能够采取其它形式和功能。例如，输入传感器 112 能够是生物计量传感器，其能够从用户接收生物计量信息并在允许计算机系统 100 更新固件 108 之前验证用户身份。

[0026] 图 4 是图示更新计算机系统 100 上的固件 108 的方法的流程图 400 的实施例。计算机系统 100 能够在框 402 处通过对用户生成提示来询问用户是否希望更新固件 108，开始该方法。例如，计算机系统 100 能够运行更新程序 106 的指令，以在计算机系统的显示器上生成提示，该提示询问用户是否希望更新固件 102。然而，应当理解，可以采用提示用户的其它手段，例如音频指示器（例如声音图案）、可视指示器（例如光图案）等等。

[0027] 在框 404 处，计算机系统 100 能够检查用户响应于提示是否希望更新固件 108。用户能够利用任何输入方式（例如通过计算机系统的键盘敲入输入）对提示做出响应。如果用户不希望对固件 108 进行更新，则能够通过继续至退出框而终止处理。另一方面，如果用户希望继续固件 108 的更新，则处理继续至框 406。

[0028] 在框 406 处，计算机系统 100 能够对用户生成提示，该提示要求用户触发输入传感器 112 来继续固件 108 的更新。例如，计算机系统 100 能够运行更新程序 106 的指令来在显示器上生成提示，该提示指示用户通过将显示构件 130 朝基座构件 132 旋转来将计算机系统 100 置于闭合位置。

[0029] 处理继续至框 408，这可以包括使计算机系统 100 检查用户是否已触发输入传感器 112。例如，更新程序 106 能够通过检查输入信号 120 的发生，检查用户是否将计算机系统置于闭合位置。如果未生成输入信号 120，则处理能够返回至框 406，以保持检查输入信号的生成。能够采用超时时间段来解决在超时时间段内未生成信号的情况。另一方面，如果已经生成输入信号 120，则处理能够继续至框 410。

[0030] 在另一示例中，计算机系统 100 能够在不检查输入信号的情况下发起固件更新。在这种情况下，计算机系统 100 能够运行更新程序 106 的指令，以通过开始将新固件的一部分从更新程序拷贝或写至固件 108 来发起固件 108 的更新。通过读回被写的那一部分来验证固件 108 是否被更新，更新程序 106 能够检查更新是否成功。该示例依赖于使用写保护逻辑 110 和是否已生成输入信号 120。如果未生成输入信号 120，那么写使能信号 124 不被使能，这防止计算机系统 100 对固件 108 执行写操作。另一方面，如果生成输入信号 120，那么写使能信号 124 被使能，这允许计算机系统 100 对固件 108 执行写操作。

[0031] 在框 410 处，计算机系统 100 能够继续发起固件 108 的更新。例如，更新程序 106 能够通过按需更新固件 108 的一个或多个部分，开始发起固件 108 的更新。在一些示例中，更新程序 106 能够通过读回被写的部分并将这两个部分相互比较，验证固件 108 的更新是否成功。

[0032] 计算机系统 100 的组件能够利用被加载以供在处理器上运行的机器可读指令实现。处理器能够包括微处理器、微控制器、处理器模块或子系统、可编程集成电路、可编程门阵列或另一控制或计算装置。

[0033] 数据和指令能够存储在被实现为一个或多个计算机可读存储介质或机器可读存储介质的各种存储装置中。存储介质包括不同形式的存储器，该不同形式的存储器包括：半导体存储器设备，例如动态随机存取存储器或静态随机存取存储器（DRAM 或 SRAM）、可擦写可编程只读存储器（EPROM）、电可擦写只读存储器（EEPROM）和闪存；磁盘，例如硬盘、软盘和可移动磁盘；包括磁带的其它磁性介质；光学介质，例如光盘（CD）或数字视频光盘（DVD）；或其它类型的存储装置。注意，上述介绍的指令能够设置在一个计算机可读存储介质或机器可读存储介质上，或者可替代地能够设置在分布在具有可能多个节点的大型系统

中的多个计算机可读存储介质或机器可读存储介质上。这样的计算机可读存储介质或存储媒介或者机器可读存储介质或存储媒介被认为是物品的一部分(或者制品的一部分)。物品或制品能够指任何被制造出的单个组件或多个组件。

[0034] 此外,本申请中示出和描述的组件还可以被实现在程序代码(例如固件和/或软件和/或其它逻辑指令)中,该程序代码被存储在一个或多个计算机可读介质中且可由一个或多个处理器运行,以执行本申请中描述的操作。这些组件仅仅是可以提供的各种功能的示例,而非旨在作为限制。所示出和所描述的实施例用于图示目的,而非旨在作为限制。

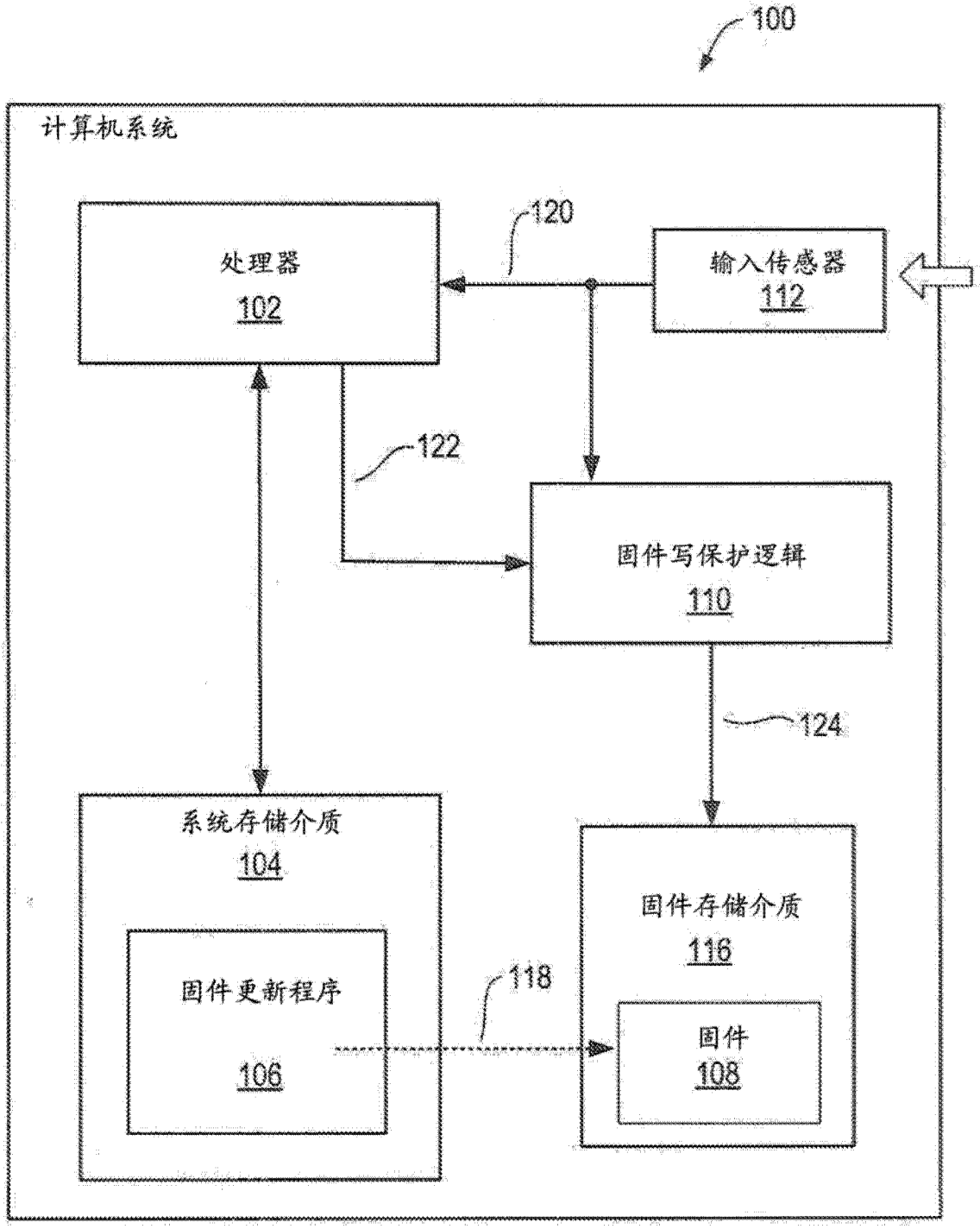

100
计算机系统
处理器
102
120
输入传感器
112
122
固件写保护逻辑
110
124
系统存储介质
104
固件更新程序
106
118
固件存储介质
116
固件
108

图 1

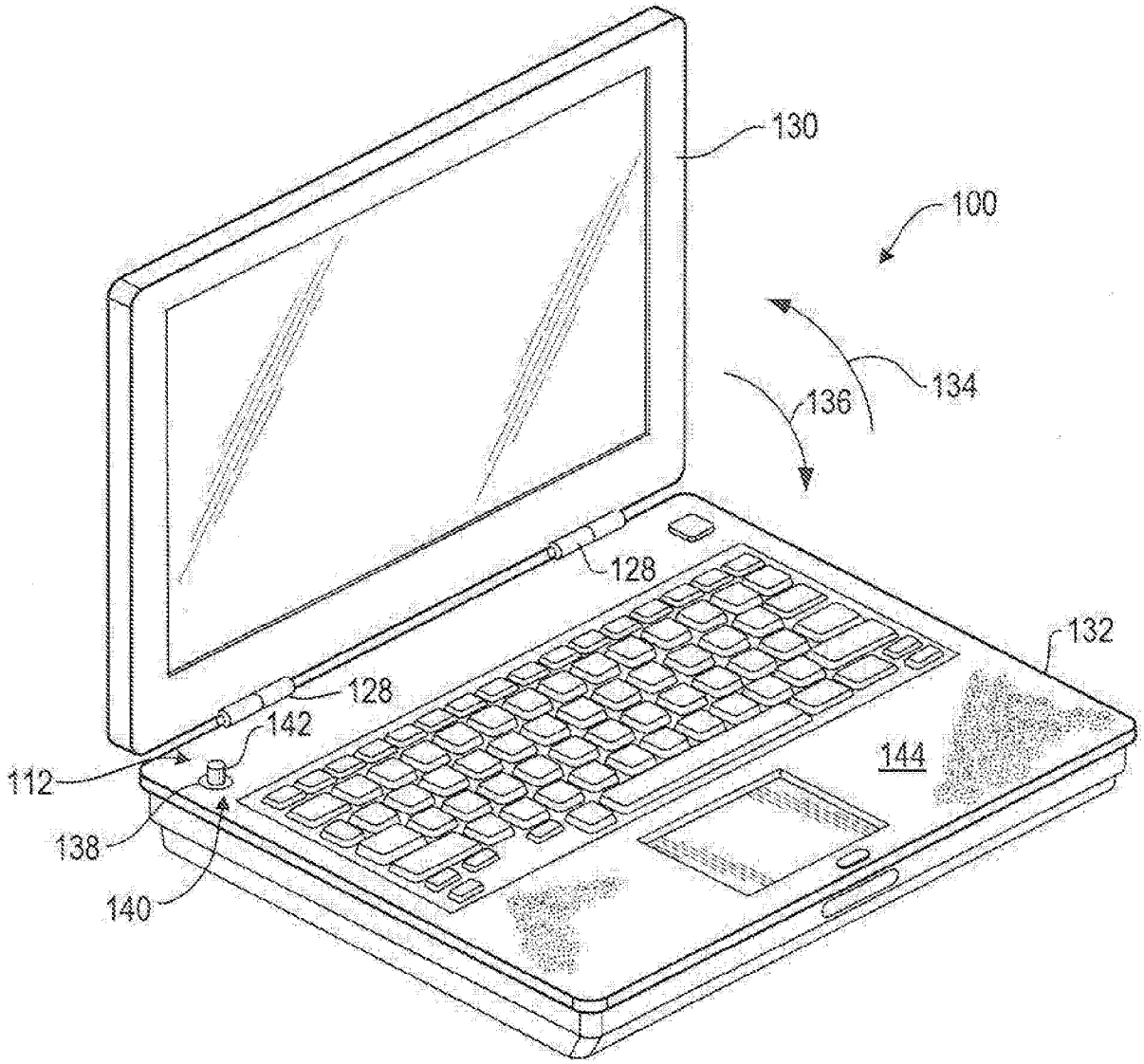


图 2

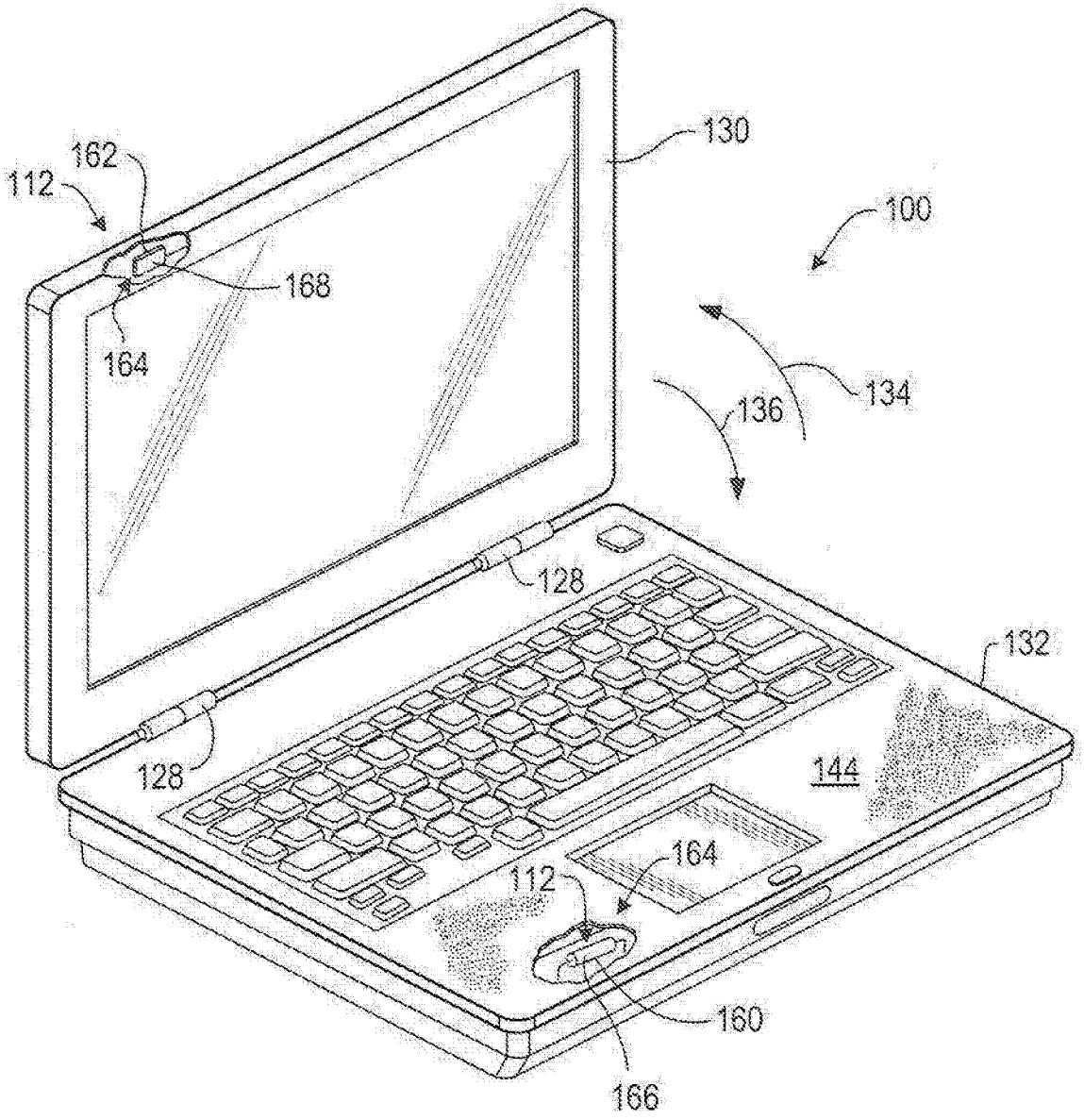


图 3

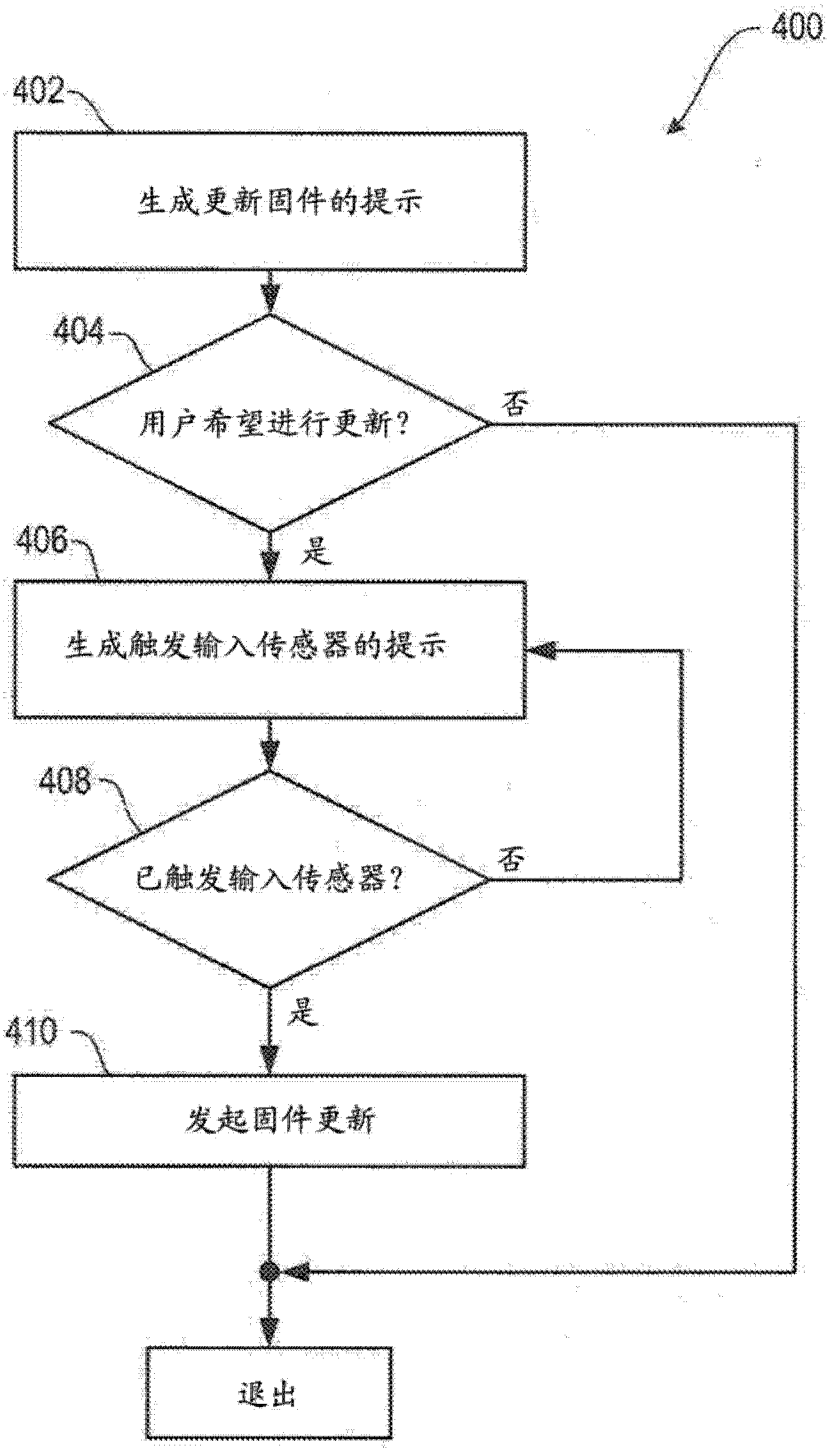

400
402
生成更新固件的提示
404
用户希望进行更新?
否
是
406
生成触发输入传感器的提示
408
已触发输入传感器?
否
是
410
发起固件更新
退出

图 4