(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112311552 B
(45)授权公告日 2024.12.24

(21)申请号 202010742604.9

(22)申请日 2020.07.29

(65)同一申请的已公布的文献号
申请公布号 CN 112311552 A

(43)申请公布日 2021.02.02

(30)优先权数据
1908696 2019.07.30 FR

(73)专利权人 意法半导体(大西部)公司
地址 法国勒芒

(72)发明人 F·阿里夫

(74)专利代理机构 北京市金杜律师事务所 11256
专利代理师 董莘

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
G06F 9/4401(2018.01)

(56)对比文件
US 2017220404 A1,2017.08.03
CN 104995629 A,2015.10.21
US 2014331033 A1,2014.11.06

审查员 刘慧敏

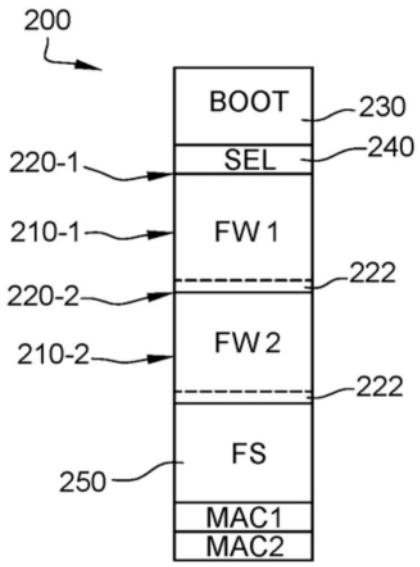
权利要求书2页 说明书8页 附图4页

(54)发明名称

具有固件的电子设备及其操作方法

(57)摘要

本公开的实施例涉及具有固件的电子设备及其操作方法。实施例电子设备包括存储器,存储器包含设备的固件的多个副本。



CN 112311552 B

1.一种电子设备,包括:

存储器,存储:

所述电子设备的相同固件的至少一个版本的多个副本;以及

针对所述副本中的每个副本的签名,所述签名用于检查所述副本的有效性;

中央处理单元,通信地耦合到所述存储器,其中所述相同固件的每个副本被配置为引起所述中央处理单元执行所述电子设备的根据可信平台模块TPM标准的操作,其中所述中央处理单元被配置为:

接收所述相同固件的附加副本,其中取决于在所述存储器中的所述附加副本的未来位置的值,利用相同的预定义值来被代替;

接收在所述存储器中的、所述副本的每个位置的相关值;

利用所述附加副本代替所述副本中的至少一个副本;以及

恢复与附加副本的所述位置相对应的所述相关值。

2.根据权利要求1所述的电子设备,其中所述存储器还包括用于启动所述电子设备的程序,在由所述电子设备执行时,所述程序能够引起所述副本中的至少一个副本的有效性验证和执行。

3.根据权利要求1所述的电子设备,其中所述存储器包括指示从所述副本之中选择的副本的值。

4.根据权利要求3所述的电子设备,其中所选择的副本对应于在所述固件的版本之中的最新版本。

5.根据权利要求1所述的电子设备,其中所述存储器还包括对所述副本中的每个副本均可访问的共用文件系统。

6.一种操作具有存储器的电子设备的方法,所述电子设备包括具有外部导电引脚的封装,被设置在所述封装中的第一集成电路芯片上的中央处理单元,以及被设置在所述封装中不同于所述第一集成电路芯片的第二集成电路芯片上的非易失性存储器,所述非易失性存储器包含所述电子设备的相同固件的至少一个版本的多个副本,所述方法包括:

通过在所述封装中的所述中央处理单元在所述封装中的所述非易失性存储器中存储针对相同固件的至少一个版本的每个副本的完整性签名,所述完整性签名用于检查所述副本的有效性;

由所述电子设备接收所述相同固件的附加副本,其中取决于在所述存储器中的所述附加副本的未来位置的值,利用相同的预定义值来被代替;

由所述电子设备接收在所述存储器中的、所述副本的每个位置的相关值;

利用所述附加副本代替所述副本中的至少一个副本;

恢复与所述附加副本的所述位置相对应的所述相关值;

由所述封装中的所述中央处理单元确定所述相同固件的所述副本中的第一副本是有效副本并且对应于有效副本的最新版本;以及

执行所述副本的所述第一副本,以引起所述电子设备的根据可信平台模块TPM标准的操作。

7.根据权利要求6所述的方法,其中当由所述电子设备执行时,所述有效副本中的每个有效副本能够引起所述电子设备的根据所述TPM标准的操作。

8.根据权利要求6所述的方法,包括:利用在所述副本之中有效的另一副本代替在所述副本之中无效的副本。

9.根据权利要求6所述的方法,包括:利用所述副本中的另一个副本代替所述副本中的一个副本,所述另一个副本对应于比被代替的所述一个副本更新的版本。

10.根据权利要求6所述的方法,还包括:

以压缩形式接收所述附加副本和/或所述相关值;以及

解压缩所述附加副本和/或所述相关值。

11.根据权利要求6所述的方法,其中所述预定义值具有的所有比特等于存储器擦除值。

12.一种电子部件,包括:

封装;

中央处理单元,被布置在所述封装中;

存储器,被布置在所述封装中,并且通信地耦合到所述中央处理单元;以及

所述电子部件的相同固件的至少一个版本的多个副本,被存储在所述存储器中,其中所述副本中的每个副本在由所述中央处理单元执行时,能够引起所述电子部件的根据可信平台模块TPM标准的操作;

针对所述副本中的每个副本的签名,所述签名用于检查所述副本的有效性;以及

其中所述中央处理单元被配置为:

接收所述相同固件的附加副本,其中取决于在所述存储器中的所述附加副本的未来位置的值,利用相同的预定义值来被代替;

接收在所述存储器中的、所述副本的每个位置的相关值;

利用所述附加副本代替所述副本中的至少一个副本;以及

恢复与附加副本的所述位置相对应的所述相关值。

13.根据权利要求12所述的电子部件,其中所述存储器还包括用于启动所述电子部件的程序,在由所述中央处理单元执行时,所述程序能够引起所述副本中的至少一个副本的有效性验证和执行。

14.根据权利要求12所述的电子部件,其中所述存储器包括指示从所述副本之中选择的副本的值。

15.根据权利要求12所述的电子部件,其中所选择的副本对应于所述固件的版本之中的最新版本。

16.根据权利要求12所述的电子部件,其中所述存储器还包括对所述副本中的每个副本均可访问的共用文件系统。

具有固件的电子设备及其操作方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2019年7月30日提交的申请号为No.1908696的法国专利申请的权益,该申请通过引用并入此。

技术领域

[0003] 本公开一般地涉及电子设备和方法,并且更具体地涉及包括固件的电子设备及其操作方法。

背景技术

[0004] 某些电子设备包括能够执行程序的数据处理单元。例如,包括一个或多个微处理器的处理单元。

[0005] 这样的设备通常地包括固件。固件意味着必须由处理单元执行以便设备操作的程序,该程序被存储在设备中,亦即,被包含在设备的存储器中。

发明内容

[0006] 实施例克服了包括处理单元的、特别是包括固件的已知电子设备的全部或部分缺点。

[0007] 实施例克服了已知固件的全部或部分缺点。

[0008] 实施例克服了已知固件更新方法的全部或部分缺点。

[0009] 实施例提供了电子设备,其中存储器包含设备的固件的多个副本。

[0010] 根据实施例,在由设备执行时,所述副本的每个副本能够使设备根据可信平台模块(TPM)标准操作。

[0011] 根据实施例,存储器还包含针对副本中的每个所述副本的签名,用于检查所述副本的有效性。

[0012] 根据实施例,存储器还包括用于启动设备的程序,当由设备执行时,该程序能够引起副本中的至少一个所述副本的有效性检查和执行。

[0013] 根据实施例,存储器包括指示从所述副本之中选择的副本的值。

[0014] 根据实施例,所选择的副本对应于固件版本之中的最新版本。

[0015] 根据实施例,存储器还包括对所述副本中的每个副本均可访问的共用文件系统。

[0016] 实施例提供了操作上文所述的设备的方法。

[0017] 根据实施例,方法包括执行所述副本的一个副本,被执行的副本有效、并且对应于有效副本版本之中的最新副本版本。

[0018] 根据实施例,方法包括用在所述副本之中有效的另一副本代替在所述副本之中无效的副本。

[0019] 根据实施例,方法包括用在所述副本中的另一个副本代替所述副本中的一个副本,该另一个副本对应于比所代替副本的版本更新的版本。

[0020] 根据实施例,方法包括由所述设备接收:固件的附加副本,其中取决于在存储器上的所述附加副本的未来位置的值,利用相同的预定义值来被代替,所述预先定义值优选地使其全部比特等于存储器擦除值;以及所述相关值,所述相关值针对在存储器中的、所述副本的位置的每个位置。

[0021] 根据实施例,方法还包括用附加副本代替所述副本中的至少一个副本,以及恢复与所代替副本的位置相对应的相关值。

[0022] 根据实施例,以压缩形式接收附加副本和/或所述相关值,并且然后解压缩附加副本和/或所述相关值。

[0023] 实施例提供电子部件,优选地包括封装,包括诸如上文所定义的设备或能够实施如上文所述的方法的设备。

[0024] 在下面结合附图对具体实施例进行的非限制性描述中,将详细讨论前述和其他特征与优点。

附图说明

[0025] 为了更全面地理解本发明以及其优点,现在结合附图对以下描述进行参考,其中:

[0026] 图1示出下文所描述的实施例适用的设备的示例;

[0027] 图2示意性地示出包括固件的设备的存储器的实施例;

[0028] 图3以块的形式示意性地示出由包括固件的设备实现的方法的实施例;

[0029] 图4示意性地示出固件更新方法的实施例的步骤;

[0030] 图5示意性地示出方法的另一个步骤;并且

[0031] 图6示意性地示出方法的另一个步骤。

具体实施方式

[0032] 在不同的附图中,相同元件被指定为相同附图标记。特别地,不同实施例共有的结构和/或功能元件可以用相同附图标记来指定,并且可以具有相同的结构、尺寸和材料特性。

[0033] 为了清楚起见,只示出以及详细说明了对理解所描述的实施例有用的步骤和元素。特别地,不详细说明固件,所描述的实施例与通常的固件兼容。

[0034] 在下面的描述中,当参考绝对位置限定的术语时(诸如术语“前”、“后”、“顶”、“底”、“左”、“右”等),或相对位置(诸如术语“在……上方”、“在……下方”、“上”、“下”等)时,或限定方向的术语(诸如术语“水平”、“竖直”等)时,除非另有规定,否则指图纸的取向。

[0035] 本文中使用术语“将近”、“近似地”、“基本上”和“大约”来表示所述值的正负10%、优选地正负5%的公差。

[0036] 图1示出了所描述的实施例适用于设备的示例。更特别地,设备是包括固件的设备。

[0037] 在该示例中,设备包括电子部件100。电子部件包括一个或多个电子集成电路芯片110。电子芯片或每个电子芯片110由半导体晶片部分和位于晶片内部和晶片上的电子电路定义。作为示例,电子部件100还包括了包括(多个)电子芯片的封装120,通常,紧密封装具有从其突出的导电引脚122。引脚122旨在被电耦合到其他部件,优选地焊接到印刷电路板

PCB。

[0038] 固件被存储在存储器130(MEM)中。优选地,存储器130是非易失性的、更优选地可重写的。例如,存储器130是电可擦可编程只读存储器EEPROM类型的存储器,诸如被称为“闪存”的存储器。这样的闪存存储器由包括晶体管的存储器定义,每个晶体管具有能够存储电荷的浮动栅极。优选地,存储器130位于封装120内部,更优选地被包括在(多个)芯片110内。

[0039] 电子部件100还包括数据处理单元140。优选地,处理单元位于封装120中。例如,数据处理单元位于与存储器130相同的电子芯片110上。

[0040] 优选地,在固件由设备(更精确地说,由处理单元140)执行期间,固件引起设备根据标准ISO/IEC11889-1(例如,ISO/IEC11889-1:2015或更新版本)的可信平台模块(TPM)标准操作。然后,设备可以形成TPM加密部件。TPM加密部件通常用于电子和/或计算机装备(诸如计算机、平板计算机、蜂窝电话等),或者也用于各种被称为已连接(亦即,可连接到互联网)的对象或系统,(例如机动车或摄像头)。这样的部件通常用于存储加密密钥。

[0041] 所描述实施例的应用不限于图1的设备的示例。所描述的实施例适用于包括固件的任何设备。特别地,存储器和处理单元可以位于不同的封装中,或者也可以将设备包括在部件内,例如,包括其他电子设备的片上系统。

[0042] 图2示意性地示出了包括固件的设备的存储器的实施例。更特别地,存储器200的内容在图2中示出。在实施例中,存储器200代替图1中的类型的设备的存储器130。

[0043] 存储器200例如与图1的设备的存储器130的类型相同(亦即,优选地非易失性可重写存储器(例如,闪存型存储器)。存储器200可以对应于一个或多个存储器库,存储器库位于相同部件、或多个不同部件的相同芯片、或多个芯片中。根据实施例,存储器中包含的元件在所示出位置的顺序中,亦即,在存储器中增加的地址的顺序中,这些地址是物理地址、或优选地逻辑地址。然而,所描述的实施例与在存储器中包含的不同元件的所有位置兼容。

[0044] 存储器130包括固件的多个副本FWi或实例(其中i是副本的从1到N的整数个数目)。在所示出的优选实施例中,存储器130包括固件的两个副本FW1、FW2(N=2)。在其它实施例中,存储器130可以包括固件的多于两个的副本。固件的副本在能够由设备在副本位于存储器中的位置处直接执行的方式中被存储,即,在由设备执行副本之前,副本不需要被移动、修改或解密。

[0045] 固件的副本中的一个副本可以出现缺陷或无效,例如,这归因于在存储器位置发生错误、或在尝试更新该固件副本失败后。然后,设备可以执行另一个副本(或其他副本的一个副本)。针对该目的,设备可以实现如下文所描述的关于图3的方法。

[0046] 相比之下,在存在单一固件副本的情况下,在存储器位置发生错误或更新失败的情况下(例如仅将副本的一部分放置在存储器中),设备无法正确地操作。因此,尽管在存储器中发生了错误或尝试更新失败,但是固件的多个副本FWi的存在使得设备能够操作。这使得设备的可用率和/或可靠性能够增加。在优选地只提供两个副本FWi的情况下,可以使得副本FWi在存储器中占用的空间和可靠性/可用率之间的权衡能够最优化。

[0047] 每个副本FWi从一个位置,或从副本的起始地址220-i(220-1,220-2)占用存储器200的区域210-i(210-1,210-2)的至少一部分。优选地,每个副本FWi留下空闲的,即不占用相关区域210-i的部分222,优选地位于区域中最高逻辑地址的一侧。在不改变位置220-i的情况下,部分222使得所考虑的副本FWi能够通过用更长的副本来更新该副本FWi。区域210-

i是优选地连续的,然而,作为变型,区域210-i可以具有任何位置。每个区域210-i由连续的存储器位置集定义,然而,作为变型,每个区域210-i可以被位于不同存储器位置的多个分隔的区域代替。

[0048] 优选地,副本FWi对应于固件的相同版本,亦即,当它们有效(无缺陷)、并且由处理单元140执行时,副本FWi引起设备的相同操作。然而,如关于图3所描述的,副本可以至少暂时地对应于固件的不同版本。

[0049] 优选地,提供相同版本固件的副本FWi,以引起相同的操作序列,每个操作对应于所执行的副本FWi的指令。在示例中,副本FWi可以包括取决于在存储器200中的副本FWi的位置220-i的指令,并且然后副本FWi优选地只相差其取决于位置220-i的指令。更精确地,有效副本FWi只相差其位置相关指示的操作数。因此,指令的操作符在有效副本中是相同的。在另一示例中,副本FWi从位置220-i完全独立,并且然后优选地相同。

[0050] 作为变型,相同版本固件的副本FWi可以对应于不同的指令,例如,从相同源代码和从被不同地实现的编译产生的指令。

[0051] 优选地,对于所述副本FWi中的每个副本,存储器还包含用于检查所考虑副本的有效性的签名MACi(MAC1,MAC2),亦即,完整性测量。签名MACi可以是任何类型的签名,使得能够检测在对应的副本FWi中的错误。这样的错误对应于:所提供的对应于固件的、并且被存储在所考虑的位置的副本与通过读取该位置的内容而获得的副本FWi之间的至少一比特的差异。优选地,签名MACi是消息认证码MAC类型的签名。作为示例,签名MACi是循环冗余校验或CRC类型、或校验和类型的签名。作为变型,可以用用于检查所考虑副本的有效性的任何方法来代替签名,诸如存储器和/或副本操作测试,或者更新失败指示。然而,与这些变型相比,签名MACi使得对副本FWi有效性的检查能够简化。签名MACi例如位于存储器200的末端的位置(它们的逻辑地址是存储器位置中最高的)。

[0052] 优选地,存储器还包括设备引导程序230(BOOT)。在设备启动时,通过执行设备引导程序230来启动处理单元(图1中的140)。设备引导程序230的执行随着固件副本FWi的一个副本的开始结束。优选地,存储器位置240包含值SEL。值SEL指示,在副本FWi之中,所选择的副本FW-SEL或有源副本将作为相对于其他副本FWi的优先级启动。优选地,设备引导程序230检查所选择的副本FW-SEL的有效性,并且如果该副本有效,则启动该副本。优选地,所选择的副本是例如在其安装期间、在前一步骤中检查了其有效性的副本。下文关于图3描述了在执行设备引导程序230期间实现的方法的示例。

[0053] 优选地,所选择的副本FW-SEL是在所述副本FWi之中对应于固件的最新版本的副本。这有利地导致对应于固件的最新版本的副本启动。

[0054] 作为变型,省略指示所选择的副本的值SEL。在该变型中,为了启动固件的最新版本,设备测试所有副本FWi的有效性,比较所有副本FWi的版本,并且然后选择和启动与最新版本相对应的有效副本。与这种变型相比,在所选择的副本有效的情况下,指示所选副本的值使得能够执行单个有效性测试,这使得设备引导程序230能够简化并且加速其执行。

[0055] 优选地,存储器还包括所述每个副本均可访问的共用文件系统250(FS)。共用文件系统250通常包括由固件使用以操作设备的数据。共用文件系统250的优点是所使用的数据与所启动的副本FWi相同。例如,文件系统在存储器中的副本FWi和签名MACi之间扩展。

[0056] 图3以块的形式示意性地示出包括了包括图2的存储器的固件设备的操作方法的

实施例。更特别地,对应于在执行以下项期间由设备实施的步骤的块:设备引导程序230、所选择的副本FW-SEL以及与所选择的副本不同的副本FWi,分别在框230'、210-SEL和210-BU中表示。

[0057] 在步骤302(START),设备引导程序230的执行启动,并且方法进行到步骤304。

[0058] 在步骤304(SEL OK?),设备测试所选择的副本FW-SEL的有效性。如果副本有效(Y),则该方法进行到启动执行所选择的副本FW-SEL的步骤306(START SEL)。如果副本无效(N),方法进行到步骤308。

[0059] 在步骤308(SEEK BU OK),如果该步骤从开始就未被执行,则设备在除了所选择的副本FW-SEL之外的有效副本FWi之中寻找备份副本FW-BU。然后方法继续进行到步骤310。

[0060] 在步骤310(LAST VERSION?),设备测试备份副本FW-BU的版本是否为最新版本。为了实现这点,在最新版本是所选择的副本FW-SEL的优选情况下,比较所选择的副本FW-SEL和备份副本FW-BU的版本是足够的。如果版本相同(Y),则方法进行到步骤312。否则,该方法返回到步骤308,或者,在存储器仅包含两个副本的情况下,方法继续进行到步骤314(虚线313)。

[0061] 在步骤308的新执行中,设备在除了所选择的副本FW-SEL和先前的副本或多个副本FW-BU的有效副本FWi之中寻找新的备份副本FW-BU。如果找到新的副本FW-BU(Y),则方法进行到步骤310。否则,方法进行到步骤314。

[0062] 在步骤312(NEW SEL),方法修改位置240的值SEL。有效的、并且对应于最新的值的副本FW-BU,成为将要优先执行的、新的所选择的副本FW-SEL。然后方法进行到上文所描述的步骤306。

[0063] 在步骤314(START BU),方法启动备份副本FW-BU。

[0064] 在步骤306之后,方法优选地经过步骤316(REPLACE?)。在执行所选择的副本FW-SEL期间,实现步骤316和步骤316之后的步骤。

[0065] 当由设备接收到请求时,执行步骤316。为了实现这点,设备经由平台与诸如服务器的系统进行通信。通信例如在诸如因特网的远程通信网络上执行,并且也可以通过适合于经由平台在设备与服务器之间的通信的任何通信模式来执行。在步骤316,设备发送指示在步骤304之前所选择的副本是否有效的信息。如果在此之后,设备接收到代替一个或多个无效副本的请求(Y),方法进行到步骤318。如果设备没有接收到代替请求(N),方法进行到步骤320。

[0066] 在步骤318(REPLACE BU),设备代替无效和/或对应于不同于最新版本的副本。更精确地,优选地,设备从服务器接收旨在代替无效副本的新副本。作为变型,在所选择的副本FW-SEL不依赖于其在存储器中的位置的情况下,在将被代替的副本的位置处提供所选择的副本FW-SEL的相同副本。优选地,然后设备用所选择的副本FW-SEL的检查签名代替被代替的副本的检查签名。在这种变型中,并且在所选择的副本FW-SEL包括位置相关指示的情况下,通过修改这些指示来实现副本。设备计算被代替副本FWi的新检查签名MACi,并且将签名存储在其存储器中的位置。方法的实施例与根据来自程序的另一副本的位置而将副本、实例或程序写入存储器的通常步骤兼容。步骤318使得副本能够有效,并且对应于最新版本。

[0067] 步骤320(UPDATE?)优选地在由设备接收到执行该步骤的请求时被实现。在该步

骤,设备测试是否应当执行固件更新。为此目的,设备经由平台与服务器通信。如果将要执行更新(Y),方法进行到步骤322(UPDATE BU)。否则(N),方法进行到步骤324。

[0068] 在步骤322,设备更新除了所选择的副本FW-SEL以外的副本。换言之,设备用对应于比所选择的副本FW-SEL的版本更新的版本的副本代替除了所选择的副本FW-SEL以外的副本。随后关于图4到图6描述了该步骤的实现模式的示例。在步骤322之后,例如,设备进行到步骤326,在此处设备检查经更新的副本是否有效。如果副本是有效的(Y),方法进行到步骤328(NEW-SEL)。否则,作为示例,方法可以返回到步骤322以尝试再次执行更新。作为变型,该方法可以进行到步骤318,以恢复更新失败的副本。

[0069] 在步骤328,该方法修改值SEL(图2)以指示在步骤322更新的副本将必须在设备下一次启动时优先启动。因此,经更新的副本将在下一次启动时成为新的被选择的副本FW-SEL,新副本对应于固件的最新版本。然后,在该下一次启动之后,步骤316将使得固件的所有副本能够更新。方法在步骤328之后进行到步骤324。

[0070] 步骤324(TPM)对应于在设备启动、副本FWi的外部更新和代替之后的操作。如所提到的,该操作优选地符合TPM标准。

[0071] 尽管在执行所选择的副本(框210-SEL)期间实施的步骤已按特定顺序示出,步骤的其他步骤是可能的。特别地,步骤316、318、320、322、326和328可以与步骤324的部分(虚线325)并行地执行、和/或在该步骤的部分(未示出)之后执行。另外,步骤316和318可以被省略,特别是在不存在请求的情况下,方法直接从步骤306传递到步骤320。类似地,步骤320、322、326和328可以被省略,特别地在没有请求的情况下,方法直接从步骤306或316通过到步骤324。

[0072] 在步骤314(START BU)之后,方法优选地经过步骤330(RELOAD SEL)。在该步骤,设备更新所选择的副本FW-SEL。换言之,设备用新版本的固件代替在本例中无效的所选择的副本。该步骤优选地与更新步骤322的步骤相同或类似地执行,亦即,通过优选地使用与服务器的通信执行该步骤。在步骤330之后,设备重新启动(方法返回到步骤302)。步骤330可以与步骤332(TPM)并行执行,在其中,设备确保步骤324(TPM)的功能的至少部分(优选地仅一部分)。

[0073] 图4、图5和图6示意性地示出了固件更新方法的实施例的步骤。更精确地,方法可以在上文关于图3所描述的步骤322和/或330被实现,以更新存储在包括固件的设备的存储器200(图2)中的固件的副本。

[0074] 图4的步骤优选地由在包括将被更新的固件的设备外部的系统来实现。这样的系统优选地是计算机信息系统,例如包括计算机,旨在与设备通信以执行更新。

[0075] 在图4的步骤中,固件的副本FWi被形成,优选地两个副本FW1和WF2。两个副本优选地对应于固件的相同最新版本。副本FWi能够从相应的位置220-i(220-1和220-2)被存储在设备的存储器200(图2)中。副本可以相差位置相关指示。然后副本FW1和FW2相差M数目个值FWiVj,诸如字(字由给定数目的比特定义,优选地32比特)。这些值位于从位置220-i偏移POSj的位置,j是在1到M的变化范围中整数。在示出的示例中,副本FW1和FW2的值相差FW1V1和FW2V1、FW1V2和FW2V2、FW1V3和FW2V3所对应的偏移POS1、POS2和POS3。每个偏移位置对副本FWi是共用的。可以通过比较副本FW1和FW2获得位置POSj。作为变型,通过定位位置相关值来形成单个副本并且获得偏移POSj。

[0076] 在图5的步骤,附加副本FW在对应于偏移位置POSj的位置形成,值被代替为相同的预定义值。优选地,当存储器200是闪存存储器时,预定义值的所有比特等于存储器200的擦除值,亦即,在存储器200被擦除之后,包含在存储器200的位置处的值,例如值1。预定义值因此,在例如32比特字的情况下,等于值0xFFFFFFFF(其中"0x"指示符号为十六进制)。

[0077] 优选地,以表格形式组织的值集合510被额外形成。集合510包括至少一个将被更新的副本FWi的值FWiVj,优选地对应于在表格中的另一列。优选地,集合510包括所有值FWiVj,其中整数i的每个值对应于列(整数j的每个值对应于行)。集合510优选地包括偏移POSj,更优选地对应于在表格中的列。表格中的列和行可以交换。

[0078] 在图6的步骤,附加副本FW被压缩。该步骤与通常的数据压缩步骤兼容。优选地,压缩使得从附加副本FW能够获得相对于附加副本的更小的尺寸的数据的集合610(而不丢失信息)。作为示例,集合610的尺寸比附加副本FW的尺寸小85%。作为示例,附加副本FW具有的尺寸大于或等于310千字节,并且压缩的集合610具有的尺寸小于260千字节。

[0079] 优选地,集合510不被压缩,然而,压缩集合510是可能的。

[0080] 在未示出的下一步骤中,集合510和610被发送到具有将被更新的固件的设备。优选地,设备在接收到集合610时对其进行解压缩,并将解压缩的结果(即,附加副本FW)直接存储在将被代替的副本FWi的位置。作为变型,图6的步骤被省略,并且由设备以非压缩形式接收附加副本FW。

[0081] 在变型中,设备在解压缩集合610之前,将集合610放入存储器200或另一个存储器中。然而,与该变型相比,在接收集合610时对集合610进行解压缩的事实使得所使用的存储器空间能够减少。在另一变型中,设备将解压缩后的副本存储在另一个存储器中,或者存储在存储器200中与将被代替的副本不同的位置。然而,与该另一变型相比,将压缩结果直接存储在将被代替的副本的位置的事实也使得所使用的存储器空间能够减少。

[0082] 然后,设备用由设备接收到的集合510的相对应的值代替替换至位置相关值FWiVj的预定义值。因此,在图4步骤中获得的值FWiVj已恢复到相关副本FWi中,并且因此更新了副本。

[0083] 在闪存类型存储器的情况下,被解压缩副本的部分被连续地存储。对于这些部分中的每个部分,存储器位置被同时擦除,之后,被考虑的部分被同时重新写入到所有位置中。

[0084] 在另一变型中,经解压的副本可以存储在另一个存储器中,例如RAM,并且当副本在RAM中时,可以用值FWiVj代替预定义值,然后可以将副本重写到闪存存储器中。与该变型相比,使用等于闪存存储器擦除值的比特将预定义值写入存储器,随后用值FWiVj代替它们,使得能够避免在不向闪存存储器添加写入/擦除周期的情况下使用在RAM中的空间。这使得能够减小RAM的尺寸,并且限制闪存存储器老化的风险和/或更新时间。

[0085] 图4至6的方法使得设备能够接收更新具有包含在集合510中的位置相关值FWiVj的任何副本FWi所需要的所有数据。特别地,在集合510包括所有值FWiVj的优选情况下,设备接收用于更新任何副本FWi所需要的所有值。更精确地,可以在不知道要更新哪个副本、或在不需要设备必须通信将被更新的副本的指示的情况下,有利地预先获得集合510和610。

[0086] 为了在不有利地知道将要更新哪个副本的情况下,向设备传送更新任何副本所需

要的数据,可以设计的是,传送在图4的步骤处获得的所有副本FWi。然而,通过比较,图4至图6的方法具有减少针对更新而传输的数据数目的优点。因此,可以更快地和/或通过具有较窄带宽的通信装置来执行更新。

[0087] 各种实施例和变化已被描述。本领域技术人员将理解,这些不同实施例和变型的某些特征可以组合,并且本领域技术人员将想到其他变型。

[0088] 最后,基于上文给出的功能指示,所描述实施例和变型的实际实现方式在本领域技术人员的能力范围内。

[0089] 这类变更、修改和改善旨在成为本公开的一部分,并在本发明的精神和范围内。因此,前文的描述仅作为示例,而不旨在限制。本发明仅限于以下权利要求书及其等同物中的限定。

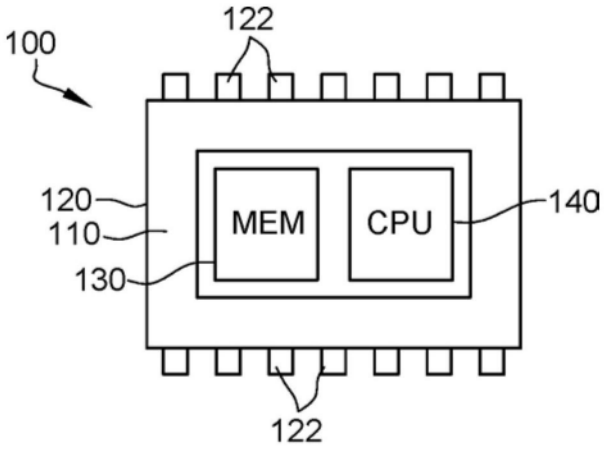

100
122
120
110
130
MEM
CPU
140
122

图1

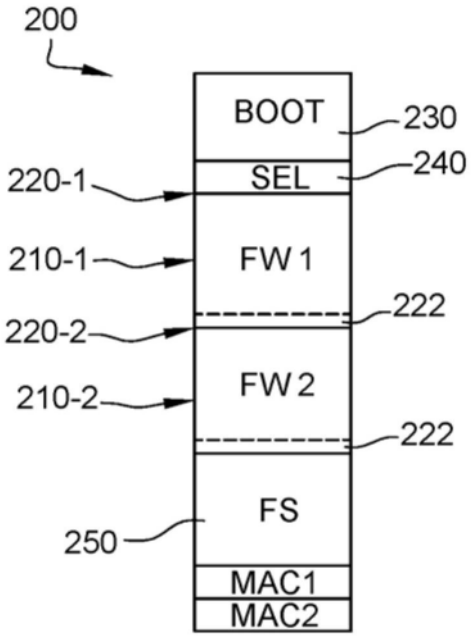

200
BOOT
230
220-1
SEL
240
210-1
FW 1
222
220-2
FW 2
210-2
222
FS
250
MAC1
MAC2

图2

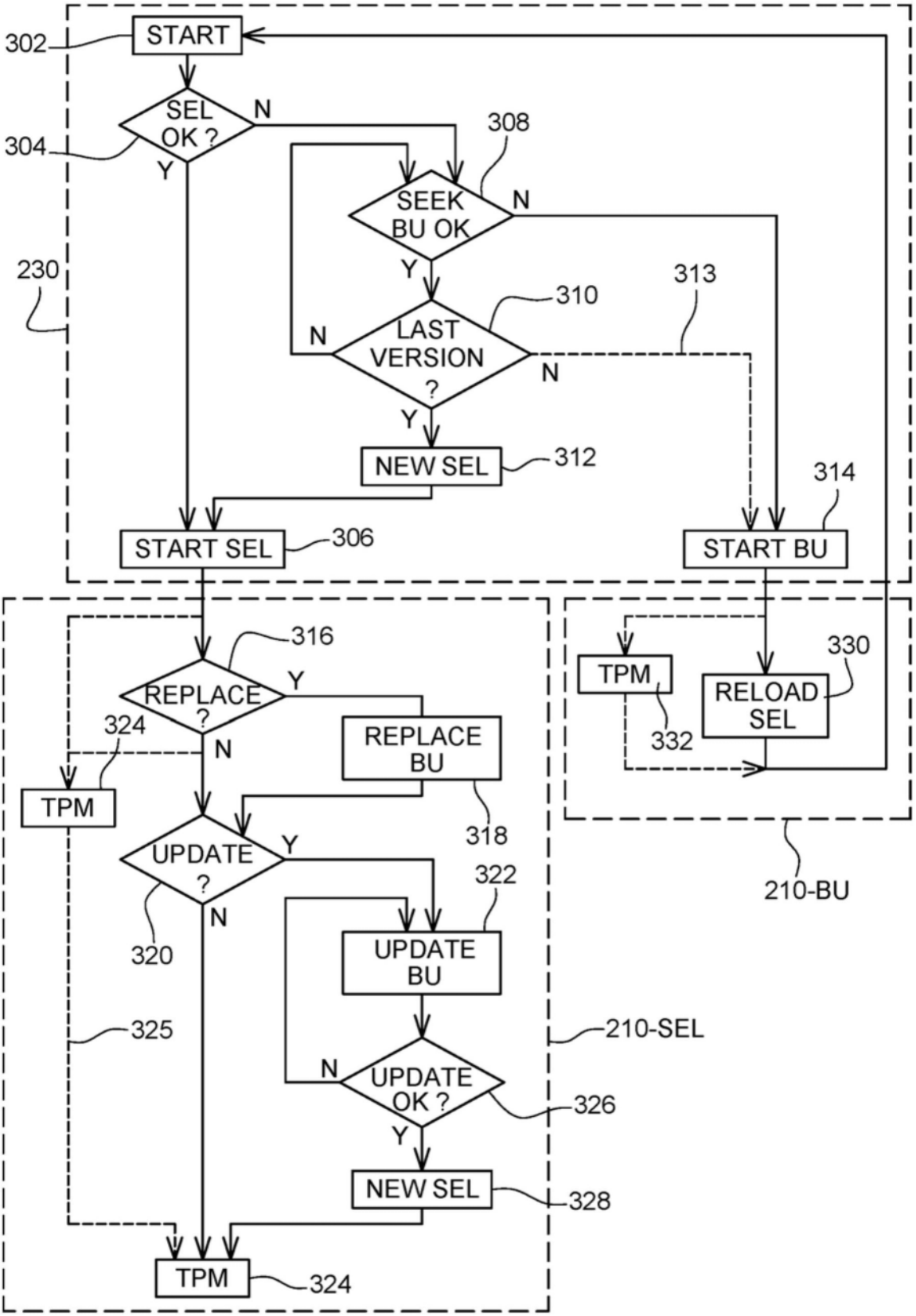

302
START
SEL OK ?
304
N
Y
308
SEEK BU OK
N
Y
230
310
313
LAST VERSION ?
N
N
Y
NEW SEL
312
314
START SEL
306
START BU
316
REPLACE ?
Y
N
324
REPLACE BU
318
TPM
UPDATE ?
Y
N
320
322
UPDATE BU
325
210-SEL
N
UPDATE OK ?
326
Y
NEW SEL
328
TPM
324
TPM
RELOAD SEL
330
332
210-BU

图3

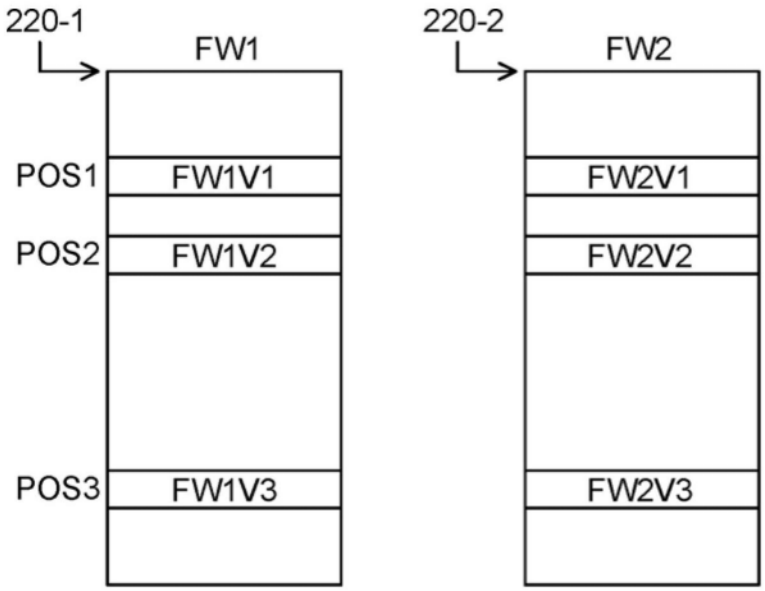

220-1
FW1
POS1
FW1V1
POS2
FW1V2
POS3
FW1V3
220-2
FW2
FW2V1
FW2V2
FW2V3

图4

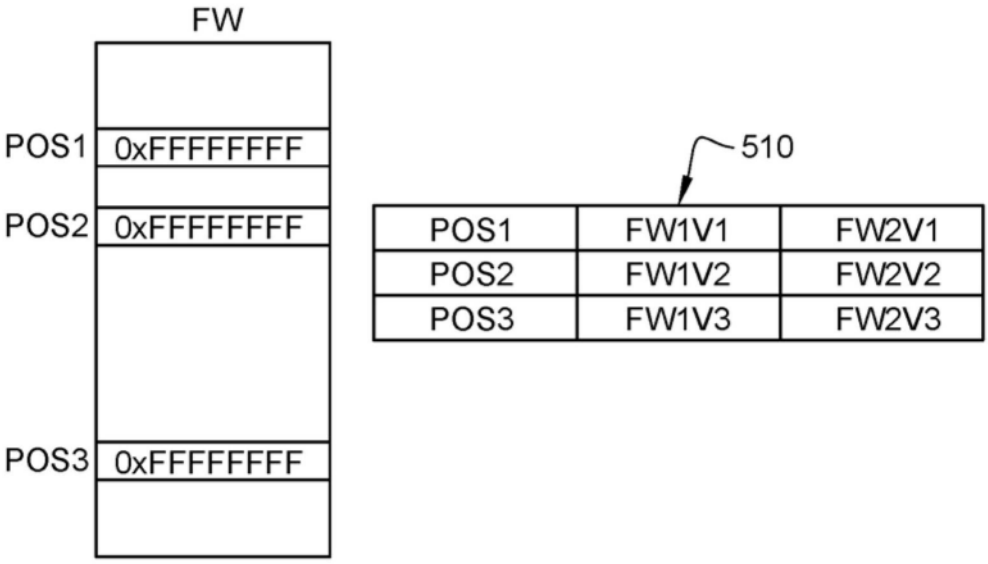

FW
POS1
0xFFFFFFFF
POS2
0xFFFFFFFF
POS3
0xFFFFFFFF
510
POS1 FW1V1 FW2V1
POS2 FW1V2 FW2V2
POS3 FW1V3 FW2V3

图5

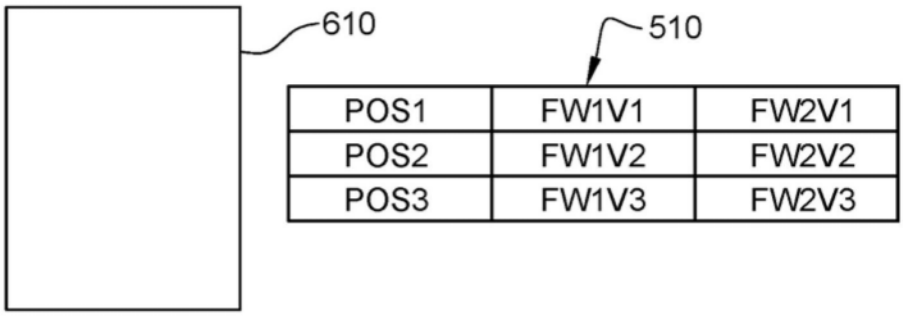


图6