



(12)发明专利

(10)授权公告号 CN 101842773 B

(45)授权公告日 2016.11.09

(21)申请号 200880113905.2

(22)申请日 2008.11.26

(65)同一申请的已公布的文献号
申请公布号 CN 101842773 A

(43)申请公布日 2010.09.22

(30)优先权数据
60/990,539 2007.11.27 US
12/276,577 2008.11.24 US

(85)PCT国际申请进入国家阶段日
2010.04.29

(86)PCT国际申请的申请数据
PCT/US2008/084824 2008.11.26

(87)PCT国际申请的公布数据
W02009/070655 EN 2009.06.04

(73)专利权人 波音公司
地址 美国伊利诺伊州

(72)发明人 F·J·麦克莱恩 T·W·古尔德
L·费谢斯 B·克劳斯纳

(74)专利代理机构 北京纪凯知识产权代理有限公司 11245

代理人 赵蓉民

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

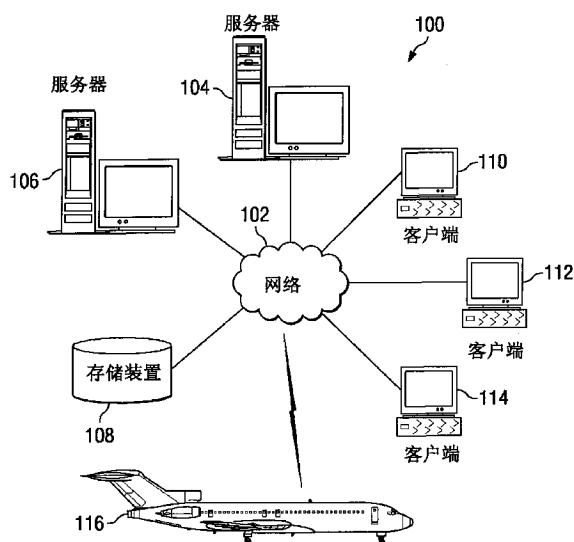
(56)对比文件
US 20030149670 A1,2003.08.07,
US 20030109973 A1,2003.06.12,
US 20070198513 A1,2007.08.23,
US 20060164261 A1,2006.06.27,
审查员 郑宁

权利要求书2页 说明书12页 附图8页

(54)发明名称
替换部件签名列表文件

(57)摘要

本发明公开了一种管理软件飞行器部件的计算机实现的方法、设备和计算机程序产品。在一个实施例中,计算机实现的方法创建替换部件签名列表部件,其具有存储的一组软件飞行器部件的一组签名。该替换部件签名列表部件被分配到飞行器数据处理系统。飞行器数据处理系统上存储的一组软件飞行器部件的每个签名使用替换部件签名列表部件中的对应签名来替换,从而在飞行器数据处理系统上形成一组当前签名。



1. 一种计算机实现的管理软件飞行器部件的方法,所述计算机实现的方法包括:
创建替换部件签名列表文件,该文件具有一组软件飞行器部件的一组签名;
签名所述替换部件签名列表文件;
将所述替换部件签名列表文件设置在文件箱中从而形成装箱的替换部件签名列表文件;
签名所述装箱的替换部件签名列表文件从而形成已签名文件箱;
将所述已签名文件箱作为软件飞行器部件发送到飞行器数据处理系统;以及
使用所述已签名文件箱中对应的签名替换所述飞行器数据处理系统上的软件飞行器部件的每个签名,从而在飞行器数据处理系统上形成一组当前签名。
2. 根据权利要求1所述的计算机实现的方法,其中所述发送步骤包括:
发送所述已签名文件箱到所述飞行器数据处理系统上的机载电子分配系统。
3. 根据权利要求1所述的计算机实现的方法,进一步包括:
在加载到外场可更换单元之前用该组当前签名的相应当前签名验证特定的软件飞行器部件。
4. 根据权利要求3所述的计算机实现的方法,其中所述加载步骤由操作人员启动。
5. 一种计算机实现的管理软件飞行器部件的方法,所述计算机实现的方法包括:
识别一组软件飞行器部件;
将与该组软件飞行器部件关联的一组签名设置在文件中;
将所述文件作为软件飞行器部件发送到飞行器数据处理系统,其中该组签名对应于具有相应的旧签名的现有软件飞行器部件;以及
用该组签名替换所述相应的旧签名。
6. 根据权利要求5所述的计算机实现的方法,进一步包括:
在所述飞行器数据处理系统中存储所述软件飞行器部件;
使用所述软件飞行器部件文件中该组签名的所选签名验证存储在所述飞行器数据处理系统中的该组软件飞行器部件中所选软件飞行器部件,从而形成已验证的软件飞行器部件;以及
加载所述已验证的软件部件到所述飞行器中的外场可更换单元上。
7. 根据权利要求6所述的计算机实现的方法,其中所述加载步骤由操作人员启动。
8. 根据权利要求5所述的计算机实现的方法,其中每个旧签名是过期签名。
9. 根据权利要求5所述的计算机实现的方法,其中所述设置步骤包括:
将与该组软件飞行器部件关联的该组签名设置在所述文件中;
自所述文件创建所述软件飞行器部件;
签名所述软件飞行器部件从而形成已签名软件飞行器部件;
将所述已签名软件飞行器部件设置在文件箱中从而形成装箱的软件飞行器部件。
10. 根据权利要求5所述的计算机实现的方法,其中所述软件飞行器部件存储在文件箱中。
11. 根据权利要求5所述的计算机实现的方法,其中该组签名是一组可扩展标记语言签名。
12. 一种计算机实现的管理软件飞行器部件的方法,所述计算机实现的方法包括:

接收软件飞行器部件,所述软件飞行器部件包含与飞行器上的一组软件飞行器部件关联的一组签名;以及

使用所述软件飞行器部件中的相应新签名替换和所述飞行器上的该组软件飞行器部件的每个软件飞行器部件关联的每个旧签名。

13.根据权利要求12所述的计算机实现的方法,进一步包括:

将与该组软件飞行器部件关联的该组签名设置在文件中;

使用所述文件形成所述软件飞行器部件;以及

将所述软件飞行器部件发送到飞行器数据处理系统。

14.根据权利要求12所述的计算机实现的方法,其中所述替换步骤包括:

响应加载所述飞行器上的该组软件飞行器部件中选择的软件飞行器部件的请求,使用来自所述软件飞行器部件的与所述选择的软件飞行器部件关联的新签名替代与所述选择的软件飞行器部件关联的旧签名来验证所述选择的软件飞行器部件;

响应所述选择的软件飞行器部件被成功验证,加载所述选择的软件飞行器部件到所述飞行器上的外场可更换单元。

15.根据权利要求14所述的计算机实现的方法,其中所述请求是由飞行器技术人员发出的。

16.一种管理软件飞行器部件的设备,其包括:

飞行器中的飞行器数据处理系统;以及

位于所述飞行器数据处理系统上的软件应用程序,其中所述软件应用程序能够:接收软件飞行器部件,该软件飞行器部件具有与所述飞行器数据处理系统中的一组软件飞行器部件关联的一组签名;使用文件中该组签名中选择的签名验证存储在所述飞行器数据处理系统上该组软件飞行器部件中选择的软件飞行器部件,从而形成验证的软件飞行器部件;加载所述验证的软件部件到所述飞行器中的外场可更换单元上;以及用该组签名替换所述外场可更换单元中的一组旧签名。

17.根据权利要求16所述的设备,进一步包括:

第二数据处理系统;以及

位于所述第二数据处理系统上的软件飞行器部件管理应用程序,其中所述软件飞行器部件管理应用程序能够:识别该组软件飞行器部件;将与该组软件飞行器部件关联的该组签名设置在所述文件中;以及将所述文件作为软件飞行器部件发送到所述飞行器数据处理系统。

替换部件签名列表文件

技术领域

[0001] 本发明一般涉及飞行器,且特别涉及管理飞行器上软件的方法和设备。更特别地,本公开涉及用于管理飞行器上的软件或飞行器部件的计算机实现方法、设备和计算机可用程序代码。

背景技术

[0002] 现代飞行器是极度复杂的。例如,飞行器可具有许多类型的机载电子系统。飞行器上的电子系统也可称为外场可更换单元(LRU)。每个外场可更换单元可进一步呈现出各种形式。外场可更换单元可以是,例如但不限于,飞行管理系统、自动驾驶仪、机上娱乐系统、通信系统、导航系统、飞行控制器、飞行记录器、防撞系统。

[0003] 诸如这些的外场可更换单元可使用软件或编程以为各种操作和功能提供逻辑或控制。这些外场可更换单元中使用的软件也通常被视为航空业的部分。特别地,飞行器上外场可更换单元中使用的软件应用程序也可被独立跟踪并被称为可加载软件飞行器部件(LSAP)或软件飞行器部件。

[0004] 当某个实体(如航空公司)接收飞行器时,软件飞行器部件通常已经安装在飞行器中的外场可更换单元上。在某些情形下,软件飞行器部件需要重新安装或重新加载到飞行器上的外场可更换单元上。安装或重新加载软件是费时并且单调沉闷的。

[0005] 飞行器软件部件开始被电子分配从而减少分配飞行器软件部件所需要的时间和人力。数字签名用来确保飞行器软件部件的安全。随着飞行器签名及其相应证书到期,有时需要更新飞行器上的签名有效性。

[0006] 因此,提供一种用于分配软件飞行器部件和更新其数字签名、解决上述和其他问题的改进的方法和设备是有利的。

发明内容

[0007] 有利实施例提供用于管理软件飞行器部件的计算机实现的方法、设备和计算机程序产品。在一个实施例中,计算机实现的方法创建替换部件签名列表文件,该签名列表文件具有一组软件飞行器部件的一组签名。替换部件签名文件列表被签名,且替换部件签名列表文件设置在文件箱(crate)内从而形成装箱的替换部件签名列表文件。装箱的替换部件签名列表文件被签名以形成签名的文件箱。签名的文件箱被发送到飞行器数据处理系统。飞行器数据处理系统上软件飞行器部件的每个签名被签名文件箱中的相应签名替代从而形成飞行器数据处理系统上的一组当前签名。

[0008] 在另一有利实施例中,一组软件飞行器部件被识别。与该组软件飞行器部件关联的一组签名设置在文件中,并且文件作为软件飞行器部件被送到飞行器数据处理系统。

[0009] 在又一有利实施例中,包含与一组软件飞行器部件关联的一组签名的软件飞行器部件被飞行器接收。与一组软件飞行器部件关联的每个旧签名被与飞行器上该组软件飞行器部件中的软件飞行器部件关联的替换部件签名列表中的相应新签名替代。

[0010] 在另一有利实施例中,设备包括飞行器中的飞行器数据处理系统和位于飞行器数据处理系统上的软件应用程序。软件应用程序能够接收软件飞行器部件,软件飞行器部件具有与飞行器数据处理系统中的一组软件飞行器部件关联的一组签名。软件应用程序也能够使用文件中该组签名中的所选签名验证存储在飞行器数据处理系统上该组软件飞行器部件中的所选软件飞行器部件,从而形成验证的软件飞行器部件,并且能够将验证的软件飞行器部件加载到飞行器数据处理系统中的外场可更换单元上。

[0011] 在又一有利实施例中,计算机程序产品包括计算机可读介质和存储在计算机可读介质上的程序代码。程序代码包括识别一组软件飞行器部件和将与该组软件飞行器部件关联的一组签名存入文件的代码。该程序代码还包括将文件作为软件飞行器部件发送到飞行器数据处理系统的代码。

[0012] 可在本公开的不同实施例中独立实现特征、功能和优点,或可在其他实施例中组合特征、功能和优点,其中进一步的细节可参考下面的说明和附图看出。

附图说明

[0013] 有利实施例中新型特征在权利要求中给出。然而,可参考本公开有利实施例的以下详细说明并结合附图最佳理解有利实施例和优选使用模式、及其进一步目的和优点,其中:

[0014] 图1是实现有利实施例的数据处理系统的网络的示意图;

[0015] 图2是根据示例性实施例的数据处理系统的示图;

[0016] 图3是根据有利实施例的重新签名飞行器部件机制的示意图;

[0017] 图4是根据有利实施例的软件飞行器部件管理系统的示意图;

[0018] 图5是根据有利实施例的外场可更换单元和飞行器数据处理系统的示图;

[0019] 图6是根据有利实施例的有效部件列表的示图;

[0020] 图7是根据有利实施例的替换部件签名列表文件的示图;

[0021] 图8是根据有利实施例的采用软件飞行器部件形式的替换部件签名列表文件的示意图;

[0022] 图9是根据有利实施例的替换部件签名列表文件结构的示意图;

[0023] 图10是根据有利实施例的管理软件飞行器部件过程的流程图;

[0024] 图11是根据有利实施例管理飞行器上软件飞行器部件过程的流程图;

[0025] 图12是根据有利实施例接收替换部件签名列表文件过程的流程图;

[0026] 图13是根据有利实施例加载软件飞行器部件过程的流程图;以及

[0027] 图14是根据有利实施例处理替换部件签名列表过程的流程图。

具体实施方式

[0028] 下面参考附图且具体参考图1-2,提供了可实现有利实施例的数据处理环境的示例图。应当理解图1-2仅是示例性的而不是为了断言或暗示关于可实现不同实施例的环境的任何限制。可对所述环境做出许多修改。

[0029] 图1示出数据处理系统网络的示意图,其中可实现本发明的有利实施例。网络数据处理系统100是实现实施例的计算机网络。网络数据处理系统100含网络102,其是用于在

网络数据处理系统100内连接在一起的各种装置和计算机之间提供通信链路的介质。网络102可包括连接,如有线、无线通信链路或光缆。

[0030] 在所示例子中,服务器104和服务器106与存储单元/装置108一起连接到网络102。此外,客户端110、112和114连接到网络102。这些客户端110、112和114可以是例如个人计算机或网络计算机。在所示例子中,服务器104向客户端110、112和114提供数据,如引导文件、操作系统映像和应用程序。

[0031] 在该例子中,客户端110、112和114是服务器104的客户端。飞行器116也是可与客户端110、112和114交换信息的客户端。飞行器116也可与服务器104和106交换信息。飞行器116在飞行时可与不同计算机通过无线通信链路交换数据,或者当在地面上时与不同计算机通过任何其他类型的通信链路交换数据。在这些例子中,可在网络数据处理系统100中实现有利实施例从而管理诸如飞行器116等飞行器上的软件飞行器部件。具体地,不同有利实施例提供用于管理签名的计算机实现的方法、设备和计算机程序产品,所述签名用来验证飞行器116上的软件飞行器部件。网络数据处理系统100可包括额外服务器、客户端和其他未显示的装置。

[0032] 在所示例子中,网络数据处理系统100是因特网,其中网络102表示使用传输控制协议/网际协议(TCP/IP)族彼此进行通信的网络和网关的全球集合。当然,网络数据处理系统100也可实现为多种不同类型的网络,如内联网、局域网(LAN)或广域网(WAN)。图1用作不同实施例的一个示例,而非对不同实施例的架构限制。

[0033] 现在参看图2,根据说明性实施例绘制了数据处理系统示图。数据处理系统200是可用于实现服务器和客户端(如服务器104和客户端110)的数据处理系统的例子。进一步,数据处理系统200是可在图1的飞行器116中找到的数据处理系统的例子。

[0034] 在该示例中,数据处理系统200包括通信光纤202,其提供处理器单元204、存储器206、永久存储装置208、通信单元210、输入/输出(I/O)单元212和显示器214之间的通信。

[0035] 处理器单元204用来执行可加载到存储器206中的软件指令。根据特定实施,处理器单元204可以是一个或更多处理器集合,或可以是多处理器核。进一步,处理器单元204可利用一个或更多异构处理器系统实现,在异构处理器系统中一个主处理器和多个副处理器同时存在于单个芯片上。作为另一个说明性例子,处理器单元204可以是含多个同类处理器的对称多处理器系统。

[0036] 在这些例子中,存储器206可以是例如随机存取存储器或任何其他合适的易失性或非易失性存储装置。根据特定实施,永久存储装置208可采用各种形式。例如,永久存储装置208可含一个或更多组件或装置。例如,永久存储装置208可以是硬驱、闪存、可重写光盘、可重写磁带或这些装置的某种组合。永久存储装置208使用的介质可以是可移除的。例如,可移除硬驱可用于永久存储装置208。

[0037] 在这些例子中,通信单元210提供与其他数据处理系统或装置的通信。在这些例子中,通信单元210是网络接口卡。通信单元210可利用物理或无线通信链路中的一种或两种提供通信。

[0038] 输入/输出单元212允许与连接到数据处理系统200的其他装置进行数据输入和输出。例如,输入/输出单元212可经键盘和鼠标为用户输入提供连接。进一步,输入/输出单元212可发送输出到打印机。显示器214提供向用户显示信息的装置。

[0039] 操作系统的指令和应用程序或程序位于永久存储装置208中。这些指令可加载到存储器206中以由处理器单元204执行。不同实施例的处理可由处理器单元204使用计算机实现的指令来执行,该计算机实现的指令可位于存储器中,如存储器206。这些指令被称为可由处理器单元204中的处理器读取和执行的程序代码、计算机可用程序代码或计算机可读程序代码。不同实施例中的程序代码可包含在不同物理或有形计算机可读介质上,如存储器206或永久存储装置208。

[0040] 程序代码216以功能形式位于可选择性地移除的计算机可读介质218上并可加载或传送到数据处理系统200上以便由处理器单元204执行。这些例子中,程序代码216和计算机可读介质218形成计算机程序产品220。在一个例子中,计算机可读介质218可以是有形的,如插入或置于硬驱或永久存储装置208的部件内以传送到存储装置的光盘或磁盘,存储装置如为作为永久存储装置208的部件的硬驱动。在有形的形式中,计算机可读介质218也可采用永久存储装置的形式,如硬驱动,拇指驱动(thumb drive)或连接到数据处理系统200的闪存。有形形式的计算机可读介质218也被称为计算机可读存储介质。在某些情形中,介质218是不可移除的。

[0041] 可替换地,程序代码216可自计算机可读介质218通过至通信单元210的通信链路和/或至输入/输出单元212的连接传送到数据处理系统200。在所示例子中,通信链路和/或连接可以是物理或无线的。计算机可读介质也可采用无形介质,如含程序代码的通信链接或无线传输。

[0042] 数据处理系统200中所示不同组件不是为了对实现不同实施例的方式提供架构限制。不同说明性实施例可以在包括除数据处理系统200所示组件之外或替换数据处理系统200所示组件的组件的数据处理系统中实现。图2中所示其他组件可与所示例子不同。

[0043] 例如,总线系统可用来实现通信结构(communication fabric)202并可包括一个或更多总线,如系统总线或输入/输出总线。当然,总线系统可用任何合适类型的架构实现,该架构提供连接到总线系统的不同组件或装置之间的数据传送。此外,通信单元可包括一个或更多用来发送和接收数据的装置,如调制解调器或网络适配器。进一步,存储器可以是例如存储器206或缓存,如可能在存在于通信结构202中的接口和内存控制中心(memory controller hub)找到的缓存。

[0044] 不同有利实施例可与用数字签名技术签名的软件飞行器部件一起使用。软件飞行器部件可以利用私钥签名。软件飞行器部件的公钥存储在飞行器中。私钥和公钥结合用来确定是否软件飞行器部件来自预定或授权来源。公钥用来验证发送方签名软件飞行器部件和软件飞行器部件没有被修改。修改可归因于软件飞行器部件的损坏或篡改。

[0045] 在不同的有利实施例中,公钥存储在飞行器数据处理系统上从而在软件飞行器部件被加载到飞行器内的外场可更换单元之前验证这些软件飞行器部件。该过程被称为验证过程。换句话说,私钥/公钥对可用来确定软件飞行器部件是可信的。

[0046] 在有利实施例中,当飞行器被航空公司接收时,公钥从制造商公钥改变为航空公司公钥。结果,当前位于飞行器上的软件飞行器部件不再是已鉴定的。在这些情形中,航空公司可使用已经以新私钥签名的软件飞行器部件重新加载软件飞行器部件。在后面某个时间点需要时,软件飞行器部件被重新加载到飞行器上的存储装置中。

[0047] 软件飞行器部件在被改变前有时可能存在于飞行器上十年或更多年。而密钥在到

期前通常仅有效约两年。在签名到期时可重新安装软件飞行器部件的一种方式是以新私钥签名每个软件飞行器部件并将所有软件飞行器部件传送到飞行器数据处理系统上进行存储。与新私钥对应的公钥被发送到飞行器数据处理系统。该类过程是昂贵和耗时的,并可引起飞行器维护的延迟。

[0048] 不同的有利实施例认识到飞行器上该类软件飞行器部件管理需要一种改进的管理签名的方法和设备以减少重新加载软件飞行器部件所需要的时间量和人力。换句话说,不同的有利实施例认识到,如果这些部件的签名到期,则避免向飞行器数据处理系统重新分配所有软件飞行器部件是有益的。

[0049] 如果软件飞行器部件的签名已经到期或由于某种其他原因而不再有效,则需要将软件飞行器部件重新加载到飞行器中的外场可更换单元上。对于这种情形,软件飞行器部件必须使用新的有效私钥重新签名或再次签名。如本文所使用的,术语重新签名(resign)、已重新签名的(resigned)或正重新签名(resigning)表示要传达提供新签名的动作。之后,具有新签名的软件飞行器部件被重新加载到飞行器上的存储器中。与该私钥对应的新公钥被加载到飞行器数据处理系统中。如果需要,之后软件飞行器部件可重新安装到飞行器中的外场可更换单元上。

[0050] 因此,提供一种用于分配飞行器部件、解决上述问题的改进的方法和设备是有利的。

[0051] 现在参考图3,其根据有利实施例示出了重新签名飞行器部件机制的示意图。在该例子中,软件飞行器部件管理系统300是用于实体的软件管理系统,实体诸如航空公司、维护修复和大修提供商(MRO)或军队航空中队。软件飞行器部件管理系统300可位于地面数据处理系统中,如图1中的服务器104,在该管理系统300上可管理和存储软件飞行器部件。

[0052] 在这些例子中,飞行器数据处理系统302是飞行器上的计算机组,如图1中飞行器116上的计算机组。如在不同示例性例子中所使用的,“组”指一个或更多项。例如,计算机组是一台或更多台计算机,签名组是一个或更多个签名。飞行器数据处理系统302包含具有签名的软件飞行器部件。

[0053] 不再对具有新签名的每个软件飞行器部件进行重新分配,不同的有利实施例发送新签名而不发送软件飞行器部件。签名自存储在地面上的软件飞行器部件产生,且签名用在飞行器数据处理系统上以验证飞行器上的软件飞行器部件。

[0054] 在这些例子中,软件飞行器部件是替换部件签名列表文件304。该文件包含飞行器数据处理系统302上的软件飞行器部件的签名。通过将飞行器数据处理系统302上每个飞行器部件的每个新签名列表设置在替换部件签名列表文件304中,将只有该文件而不是所有软件飞行器部件被加载到飞行器数据处理系统302中。例如,飞行器机队(aircraftfleet)可具有500个以上的软件飞行器部件,而一个飞行器可具有200个或更多个要求签名的软件飞行器部件。

[0055] 替换部件签名列表文件304包含每个软件飞行器部件的新签名。这些新签名可替换存储在飞行器数据处理系统302上每个软件飞行器部件的当前签名。结果,当软件飞行器部件要加载到飞行器上的外场可更换单元时,存在有效签名则允许软件飞行器部件在加载到外场可更换单元上之前被验证。如果签名太老或过了有效期,则签名可能过期。这种情形导致失效签名。例如,但不限于,如果飞行器所有权变化,则也可能存在失效签名。之前所有

者的签名变为失效,即使该签名没有过期。

[0056] 现在参考图4,其根据有利实施例示出了软件飞行器部件管理系统的示图。在该例子中,软件飞行器部件管理系统400是图3中软件飞行器部件管理系统300的一个实现示例。

[0057] 在该例子中,软件飞行器部件管理系统400包括软件飞行器部件库402、管理过程404和用户接口406。这些软件飞行器部件可以通过管理过程404进行管理。在这些例子中,用户可通过用户接口406操作管理过程404。管理过程404可用来向不同飞行器分配软件飞行器部件。

[0058] 管理过程可包括接收软件飞行器部件以便将其包括到软件飞行器部件库402中的过程。进一步,管理过程404包括用来验证软件飞行器部件库402内软件飞行器部件的过程或代码。进一步,管理过程404也可以在向软件飞行器部件管理系统400所管理的不同飞行器分配软件飞行器部件以前签名软件飞行器部件库402内的不同软件飞行器部件。

[0059] 在这些例子中,签名过程包括输入软件飞行器部件和私钥到签名算法中,该签名算法生成软件飞行器部件的签名作为输入结果。不同有利实施例可使用可用的任何签名算法或过程。所用的特定算法或过程取决于特定实现。

[0060] 此外,在有利实施例中,管理过程404可用来生成替换部件签名列表文件408。替换部件签名列表文件408可包含软件飞行器部件库402内一个以上的软件飞行器部件的签名。在所实施实施例中,这些签名是“分离的签名”,因为这些签名并未集成为软件飞行器部件的一部分。在这些例子中,该文件可采用软件飞行器部件的形式以加载到飞行器数据处理系统上。

[0061] 替换部件签名列表文件408也可具有数字签名以表明包含该文件的部件的真实性。在这些例子中,替换部件签名列表文件408可以是包含签名的可扩展标记语言(XML)数据结构。在这些例子中,扩展标记语言签名可用来签名数据源,如软件飞行器部件库402。

[0062] 当签名过期或由于某些原因不再有效,操作人员可从软件飞行器部件库402中选择一组软件飞行器部件用于生成替换部件签名列表文件408中的签名。在其他实施例中,软件飞行器部件库402中所有软件飞行器部件可生成签名并将其置于替换部件签名列表文件408中。有效的软件飞行器部件是具有有效签名的部件。替换部件签名列表文件408可被发送到飞行器以用来替换飞行器上软件飞行器部件的过期签名。在所例子中,替换部件签名列表文件408以软件飞行器部件的形式发送到飞行器数据处理系统。该形式用来使飞行器数据处理系统接收含这些签名的文件并将其存储为软件飞行器部件。该部件和其他软件飞行器部件一样也被签名。

[0063] 现在看图5,其根据有利实施例示出了飞行器数据处理系统和外场可更换单元的示图。在该例子中,飞行器数据处理系统500和外场可更换单元502位于飞行器上。外场可更换单元502是飞行器上执行不同功能的不同数据处理系统。例如,外场可更换单元502可包括,例如机上娱乐系统、自动驾驶仪、飞行管理系统、液压系统或空调单元。

[0064] 在该例子中,飞行器数据处理系统500包括504、存储装置506和数据加载功能装置510。机载电子分配系统504可存储公钥508。存储装置506存储软件飞行器部件516和签名518。在这些例子中,签名518与软件飞行器部件516是彼此分开的数据结构。在这些例子中,签名518采用可扩展标记语言(XML)签名的形式。

[0065] 在这些例子中,在部件被接收并且在加载到外场可更换单元502之前,机载电子分

配系统504执行软件飞行器的验证。在数据加载功能装置将软件飞行器部件加载到外场可更换单元502之前,机载电子分配系统504用来验证软件飞行器部件516中的软件飞行器部件。

[0066] 机载电子分配系统504对软件飞行器部件516中的软件部件执行验证过程,从而确定是否可以将软件通过数据加载功能装置510加载到外场可更换单元502中的外场可更换单元上。如果相应于要加载到外场可更换单元502的飞行器部件的签名过期或由于其他原因签名失效,则数据加载功能装置510不将软件飞行器部件加载到外场可更换单元502。

[0067] 在不同的有利实施例中,替换部件签名列表(APSL)文件520可通过机载电子分配系统504作为软件飞行器部件(如软件飞行器部件522)被加载并存储在存储装置506中。替换部件签名列表文件520中的签名可用来替换签名518内的失效签名。结果,具有过期签名的软件飞行器部件无需重新分配到飞行器数据处理系统500。

[0068] 当软件飞行器部件516内的多个软件飞行器部件的签名过期时,该类特征特别有利。进一步,当新飞行器交付时,通过使用替换部件签名列表文件520取代签名518中的失效签名,不需要将软件飞行器部件516全部重新分配。

[0069] 在其他有利实施例中,无需替换签名518,机载电子分配系统504可检查签名518内的当前签名。如果当前签名过期,则机载电子分配系统504可检查替换部件签名列表文件520从而查看该软件飞行器部件中是否存在相应的新签名。如果替换部件签名列表文件520中存在相应的新签名,则机载电子分配系统504可使用新签名执行验证。

[0070] 现在看图6,其根据有利实施例示出了有效部件列表文件的示图。有效部件编号(number)列表文件600包含要包括在替换部件签名列表文件中的部件列表。在该例子中,部件602、604、606和608出现在有效部件编号列表文件600中。可通过用户选择软件飞行器部件库中的部件创建这个文件。替换地,有效部件编号列表文件600可包括所有出现在该库中的部件编号。在其他实施例中,该文件可包含特定类型飞行器或特定种类飞行器中的所有部件编号。

[0071] 现在参考图7,示出了根据有利实施例的替换部件签名列表文件的示图。在该例子中,替换部件签名列表文件700包括图6中有效部件编号列表文件600的部件602、604、606和608的标识。该文件是图3中替换部件签名列表文件304、图4中替换部件签名列表文件408和图5中替换部件列表文件520的例子。此外,签名702、704、706和708是为这些不同部件生成的新的有效签名。

[0072] 现在参考图8,其根据有利实施例示出了采用软件飞行器部件形式的替换部件签名列表文件的示图。在该例子中,软件飞行器部件800包括替换部件签名列表文件802和头文件804。替换部件签名列表文件802是文件,诸如图7中的替换部件签名列表文件700。

[0073] 在这些例子中,头文件804是将替换部件签名列表文件802识别为可加载软件飞行器部件的头文件。在这些例子中,头文件通过Aeronautical Radio, Incorporated公司(ARINC)颁布的标准进行定义。这些例子中,所用标准是ARINC 665。具体地,软件飞行器部件是航空公司可修改信息(AMI)软件飞行器部件。该部件也包括将软件飞行器部件文件800作为可加载到飞行器数据处理系统的部件进行识别的信息。

[0074] 现在参考图9,其根据有利实施例示出了替换部件签名列表文件的结构的示图。在该例子中,替换部件签名列表文件900包括唯一标识符902、日期/时间904、源906、替换部件

签名列表文件部件编号908和签名910。签名910包括部件编号912和签名主体914。

[0075] 在这些例子中,唯一标识符902是从其他列表或软件飞行器部件中识别替换部件签名列表文件900的唯一标识符。日期/时间904是替换部件签名列表文件900创建的日期和时间。源906识别创建替换部件签名列表文件900的源。例如,在这些例子中,源可以是特定用户或系统。

[0076] 替换部件签名列表文件部件编号908识别作为特定飞行器部件的替换部件签名列表文件。部件编号912包含软件飞行器部件的部件编号。在这些例子中,签名主体914是编码的签名扩展标记语言文件。当然,签名主体914可使用扩展标记语言签名以外的其他类型的签名。

[0077] 接下来参看图10,其根据有利实施例示出了管理软件飞行器部件过程的流程图。图10中所示过程可在软件飞行器部件管理系统中执行,如示例中图4中的软件飞行器部件管理系统400。当然,根据特定实施,这些步骤可在其他数据处理系统或计算机设备中执行。

[0078] 该过程是从识别一组软件飞行器部件开始的(操作1000)。该组软件飞行器部件可以通过多种不同方式识别。例如,用户可从软件飞行器部件库中选择该组软件飞行器部件。可替换地,该组软件飞行器部件可由计算机实现的过程识别。例如,图4中的管理过程404可以不使用输入识别图4中软件飞行器部件库402中的部分或全部软件飞行器部件从而形成一组软件飞行器部件。这种识别可基于一组规则做出。例如,一规则可规定选择所述软件飞行器部件作为针对特定飞行器型号或飞行器制造商的任何软件飞行器部件。

[0079] 然后,将与该组软件飞行器部件关联的一组签名置于文件中(操作1002)。在这些例子中,与特定软件飞行器部件关联的文件中的每个签名是利用软件飞行器部件生成的签名。在这些例子中,数字签名是用私钥创建的。位于飞行器上的公钥用于验证签名。换句话说,公钥被用来确定与签名关联的软件飞行器部件是否实际来自记录的源和/或未被修改。

[0080] 之后,该过程使用包含签名的文件创建软件飞行器部件(操作1004)。在这些例子中,软件飞行器部件可通过添加或关联头或头文件(如图8中的头文件804)自包含软件飞行器部件签名的文件创建。通过自包含数字签名的文件创建软件飞行器部件,数字签名可发送到飞行器数据处理系统,该过程是传送软件飞行器部件的常规过程的一部分。结果,不必建立特别或不同的过程即可将签名引入飞行器数据处理系统。飞行器数据处理系统为了接收和存储数字签名的目的将这些数字签名识别为软件飞行器部件。

[0081] 该过程签名部件(操作1006)。在这些例子中,签名是用私钥执行的。之后,公钥可用于证明部件是否为真的验证中。然后,将签名的部件置于文件箱(crate)中(操作1008)。在这些例子中,文件箱是采用可存储文件组(如软件飞行器部件)的文件格式的文件。文件箱中的该组文件可压缩以减小其大小。换句话说,文件箱一个或更多项目的打包。文件箱系统的例子是ZIP文件格式。另一个例子是Java®档案文件格式。这些类型的文件也可用作不同有利实施例中的文件箱。

[0082] 然后,该过程签名文件箱(操作1010)。操作1004-1010是可选步骤,可能用于有些而不是所有的有利实施例中。此时,签名的文件箱准备发送到飞行器数据处理系统。该过程发送部件到飞行器上的飞行器数据处理系统(操作1012)。

[0083] 在操作1012中,该部件可以通过多种不同方式发送到飞行器数据处理系统。例如,无线通信链路可用于发送该部件到飞行器数据处理系统。借助该类通信链路,飞行器可位

于不同位置,如飞机跑道、登机候机楼、维护机构或空中。

[0084] 可替换地,文件可通过物理手段发送到飞行器数据处理系统。例如,操作人员可携带包含文件的存储装置并连接存储装置到飞行器数据处理系统以将文件传输到飞行器数据处理系统。该存储装置可以是,例如光盘、闪存或膝上型计算机的硬驱。

[0085] 接下来参看图11,其根据有利实施例示出了管理飞行器上软件飞行器部件的过程流程图。图11中所示过程可在飞行器数据处理系统中实现,如图5中的飞行器数据处理系统500。具体地,不同的示例性过程可在软件组件中实现,如图5中机载电子分配系统504和数据加载功能装置510。

[0086] 该过程从接收包含签名组的文件开始(操作1100)。在这些例子中,文件以软件飞行器部件的形式被接收。当然,在其他实施例中,根据具体实施,文件可以不同于软件飞行器部件的形式被接收。作为例子,在其他实施例中,文件可作为可扩展标记语言文件接收。

[0087] 存储文件(操作1102)。然后过程使用文件中与软件飞行器部件对应的签名加载该软件飞行器部件到飞行器上(操作1104)。然后过程结束。当存储在飞行器数据处理系统上的软件飞行器部件将要被加载到飞行器中的外场可更换单元时发生该操作。与软件飞行器部件对应的数字签名用于替换旧的数字签名,该旧的数字签名可能已经过期或由于其他原因已经失效。

[0088] 现在参考图12,其根据有利实施例示出了接收替换部件签名列表文件的过程流程图。图12中所示过程可在飞行器数据处理系统中实现,如图5中的飞行器数据处理系统500。具体地,不同过程可利用图5中的机载电子分配系统504实现。

[0089] 该过程从接收包含作为软件飞行器部件的替换部件签名列表文件的文件箱开始(操作1200)。该过程验证文件箱和软件飞行器部件上的签名(过程1202)。这些例子中,验证可通过发送请求到图5中控制器服务器模块508执行。响应该请求,图5中的控制器服务器模块508使用图5中的机载验证服务511和图5中的公钥512中的适当公钥确定文件箱和文件箱中的软件飞行器部件是否可信。

[0090] 可以通过签名效验算法来验证签名。该类算法使用签名或签名的文件以及与用于生成签名的私钥对应的公钥。所用算法将取决于特定实施。

[0091] 确定验证是否成功(操作1204)。如果验证成功,则该过程在飞行器上的存储器中存储替换部件签名列表文件(操作1204)。在该例子中,存储器可以是图5中的存储装置506。

[0092] 然后该过程处理替换部件签名列表文件以供使用(操作1206),然后过程结束。在操作1206中,替换部件签名列表文件中的签名可用来替换与软件飞行器部件对应的旧签名。

[0093] 在其他实施例中,可存储和维护替换部件签名列表文件而不用替换签名。在该类实施例中,如果对现有签名的验证过程失败,则参考替换部件签名列表文件确定是否存在针对验证失败的软件飞行器部件的签名。如果签名存在,则签名被用来执行验证。再参考操作1204,如果验证不成功,则过程结束。

[0094] 现在参考图13,其根据有利实施例示出了加载软件飞行器部件的过程流程图。图13所示过程可在飞行器数据处理系统中实现,如图5中的飞行器数据处理系统500。具体地,该过程可利用图5中的数据加载功能装置510执行。

[0095] 该过程从接收加载软件飞行器部件到外场可更换单元的请求开始(操作1300)。在

这些例子中,请求是由操作人员启动的。当然,在其他实施例中,请求可通过其他机制启动。例如,事件可用来启动该过程,如从航空公司服务器发送到飞行器数据处理系统的消息。

[0096] 定位软件飞行器部件的数字签名(操作1302)。利用定位的数字签名执行对软件飞行器部件的验证(操作1304)。确定验证是否成功(操作1306)。如果数字签名不再有效,则验证不成功。

[0097] 在这种情形中,定位替换部件签名列表文件(操作1308)。确定软件飞行器部件的签名是否存在于替换部件签名列表文件(操作1310)中。如果签名存在,则过程返回到操作1304从而利用该定位的签名执行验证。验证也可能由于其他原因失败。例如,在这些例子中,如果数字签名和/或软件飞行器部件损坏,则验证失败。否则,产生出错信号(操作1312),之后过程结束。

[0098] 再参考操作1306,如果软件飞行器部件的验证成功,则软件飞行器部件从存储器加载到外场可更换单元(操作1314),然后过程结束。

[0099] 下面参考图14,其根据有利实施例示出处理替换部件签名列表的过程流程图。在该例子中,图14中所示过程可在飞行器数据处理系统中执行,如图5中的飞行器数据处理系统500。具体地,可利用图5中的机载电子分配系统504执行该过程。

[0100] 该过程从接收处理替换部件签名列表的请求开始(操作1400)。确定替换部件签名列表是否可用以进行处理(操作1402)。如果替换部件签名列表可用,则确定通用标识符(UID)文件是否可用(操作1404)。

[0101] 如果通用标识符文件可用,则确定通用标识符文件中的通用标识符值是否与替换部件签名列表中的通用标识符值匹配(操作1406)。如果文件中的通用标识符值与替换部件签名列表中的通用标识符值不匹配,则过程读取替换部件签名列表文件中的部件编号(操作1408)。

[0102] 确定部件是否存在于飞行器数据处理系统中的机载存储装置中(操作1410)。在该例子中,使用替换部件签名列表文件中的部件编号并比较该编号和飞行器数据处理系统上的额外部件来做出确定。如果部件存在于飞行器数据处理系统上,则过程使用替换部件签名列表中与部件编号对应的签名替换部件签名(操作1412)。

[0103] 然后,过程确定替换部件签名列表文件中的部件编号是否是文件中的最后的部件编号(操作1414)。如果部件编号是最后的部件编号,则过程将替换部件签名列表中的通用标识符值写入通用标识符文件(操作1416),然后过程结束。

[0104] 再参考操作1414,如果部件编号不是替换部件签名列表文件中的最后部件编号,则过程返回到操作1408以从替换部件签名列表文件中读取另一个部件编号。参考操作1410,如果部件不存在于飞行器数据处理系统中,则过程继续操作1414,如上所述。

[0105] 回到操作1406,如果文件中的通用标识符值与替换部件签名列表中的通用标识符值匹配,则过程结束。再参考操作1404,如果通用标识符文件可用,则过程继续操作1408,如上所述。再参考操作1402,如果替换部件签名列表不可用,则过程结束。

[0106] 不同所示实施例中的流程图和方框图示出设备、方法和计算机程序产品的某些可能实施的架构、功能和操作。在这一点上,流程图或方框图中的每个方框可代表计算机可用或可读取程序代码的模块、段(segment)或部分,其包括一个或更多执行规定功能(一种或多种)的可执行指令。在某些可替换实施中,方框中标注的功能可不以图中给出的顺序发

生。例如,在某些情形中,两个连续示出的方框可基本同时执行,或方框有时可以逆序执行,这取决于所涉及的功能。

[0107] 因此,不同有利实施例提供计算机实现的方法、设备和计算机可用代码以便管理软件飞行器部件。在不同有利实施例中,一组软件飞行器部件被识别,与该组软件飞行器部件关联的一组签名被置于文件中。然后文件被发送到飞行器数据处理系统。文件中的签名可用来验证位于飞行器上的该组软件飞行器部件。通过这种方式,避免重新安装数字签名过期的每个软件飞行器部件。

[0108] 实际上,借助某些或所有不同有利实施例,只有数字签名需要被发送给飞行器。发送到飞行器的信息量的减少节省了网络带宽以及使用新数字签名重新安装每个软件飞行器部件当前所需的时间和开销。

[0109] 不同有利实施例可采用全部硬件实施例、全部软件实施例或含硬件和软件元素的实施例的形式。一些实施例是以软件执行的,其包括但不限于诸如固件、常驻软件和微代码的形式。

[0110] 而且,不同实施例可采用自计算机可用或计算机可读介质可存取的计算机程序产品的形式,该介质提供计算机或执行指令的任何装置或系统使用的程序代码或者与其结合使用的程序代码。为了公开的目的,计算机可用或计算机可读介质通常是可包含、存储、通信、传播、或传输程序以供指令执行系统、设备或装置使用或与其结合使用的任何有形设备。

[0111] 计算机可用或计算机可读介质可以是例如但不限于电子、磁性、光学、电磁、红外或半导体系统或传播介质。非限制的计算机可读介质的例子包括半导体或固态存储器、磁带、可移除计算机磁盘、随机存取存储器(RAM)、只读存储器(ROM)、硬磁盘(rigid magnetic disk)和光盘。光盘可包括只读光盘(CD-ROM)、可读/写光盘(CD-R/W)和DVD。

[0112] 进一步,计算机可用或计算机可读介质可含或存储计算机可读或可用程序代码,以便当计算机可读或可用程序代码在计算机上执行时,该计算机可读或可用程序代码的执行引起计算机在通信链路上发送另一个计算机可读或可用程序代码。该通信链路可使用例如但不限于实体或无线介质。

[0113] 适于存储和/或执行计算机可读或计算机可用程序代码的数据处理系统包括一个或更多处理器,所述处理器通过诸如系统总线等通信结构直接或间接耦合到存储器元件。存储器元件可包括在实际执行程序代码过程中采用的本地存储器、大容量存储器和为至少某些计算机可读或计算机可用程序代码提供临时存储从而减少在代码执行过程中从大容量存储器中检索代码的时间量的高速缓冲存储器。

[0114] 输入/输出或I/O装置可直接或通过中间I/O控制器耦合到系统。这些装置可包括,例如但不限于,键盘、触摸屏显示器和指向装置。不同通信适配器也可耦合到系统,从而使数据系统经中间私有或公共网络耦合到其他数据处理系统或远程打印机或存储装置。非限制性的例子是调制解调器和网络适配器,其仅是当前可用的几种类型的通信适配器。

[0115] 为了例示和说明的目的提供了不同有利实施例的说明,这些说明并不是为了穷举或限制实施例于公开的形式内。许多修改和变化对本领域技术人员来说是显然的。例如,虽然在这些例子中,替换部件签名列表文件中的新签名转化为飞行器部件的形式或者以飞行

器部件的形式创建以分配到飞行器上,但是也可以使用其他形式。例如,签名可作为数据文件的部分发送,而非软件飞行器部件,这取决于特定实施。进一步,有利实施例中所示的这些过程可应用于其他类型的交通工具或设备。例如不同有利实施例可用于诸如潜水艇、水面船只、汽车、太空船等交通工具,但不限于此,其中软件部件可从交通工具上的存储器重新加载到不同的数据处理系统。进一步,不同有利实施例可应用于存储软件部件的任何装置,这些软件部件可重新加载到重新加载需要验证的不同系统上。

[0116] 而且,不同有利实施例可提供与其他有利实施例相比不同的优点。实施例或者被选择的实施例之所以被选择和说明是为了最佳地解释实施例原理、实际应用,并使得本领域其他普通技术人员能够理解具有修改的实施例的公开同样适合预期的特定使用。

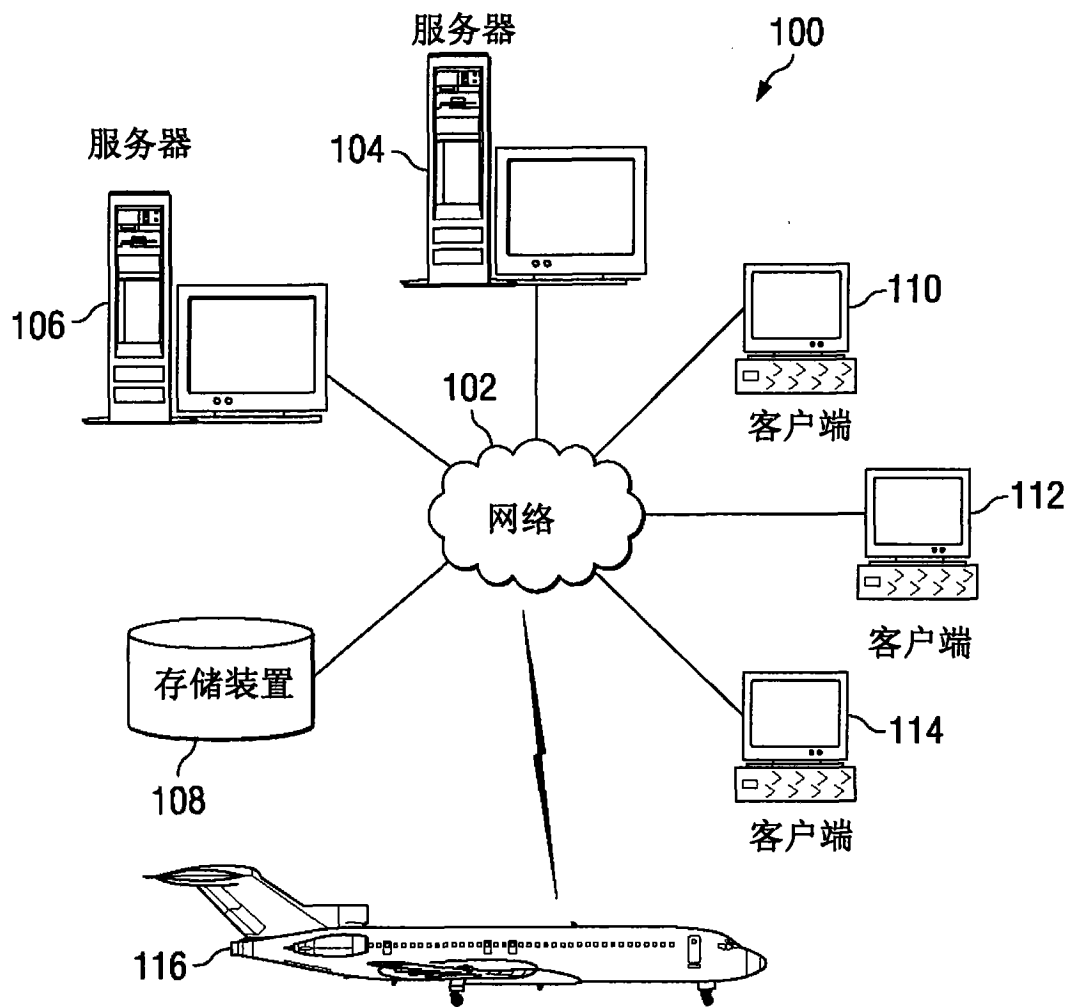


图1

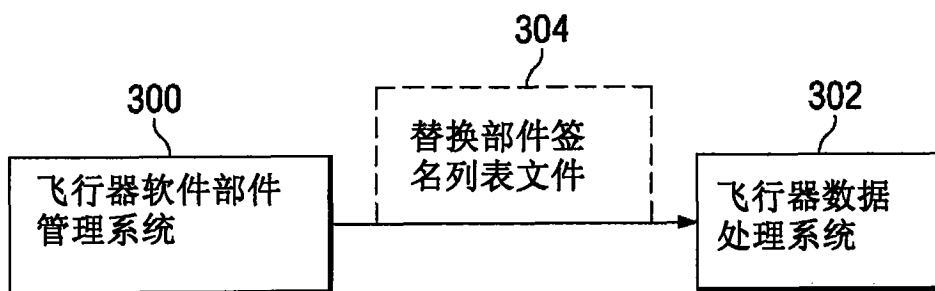


图3

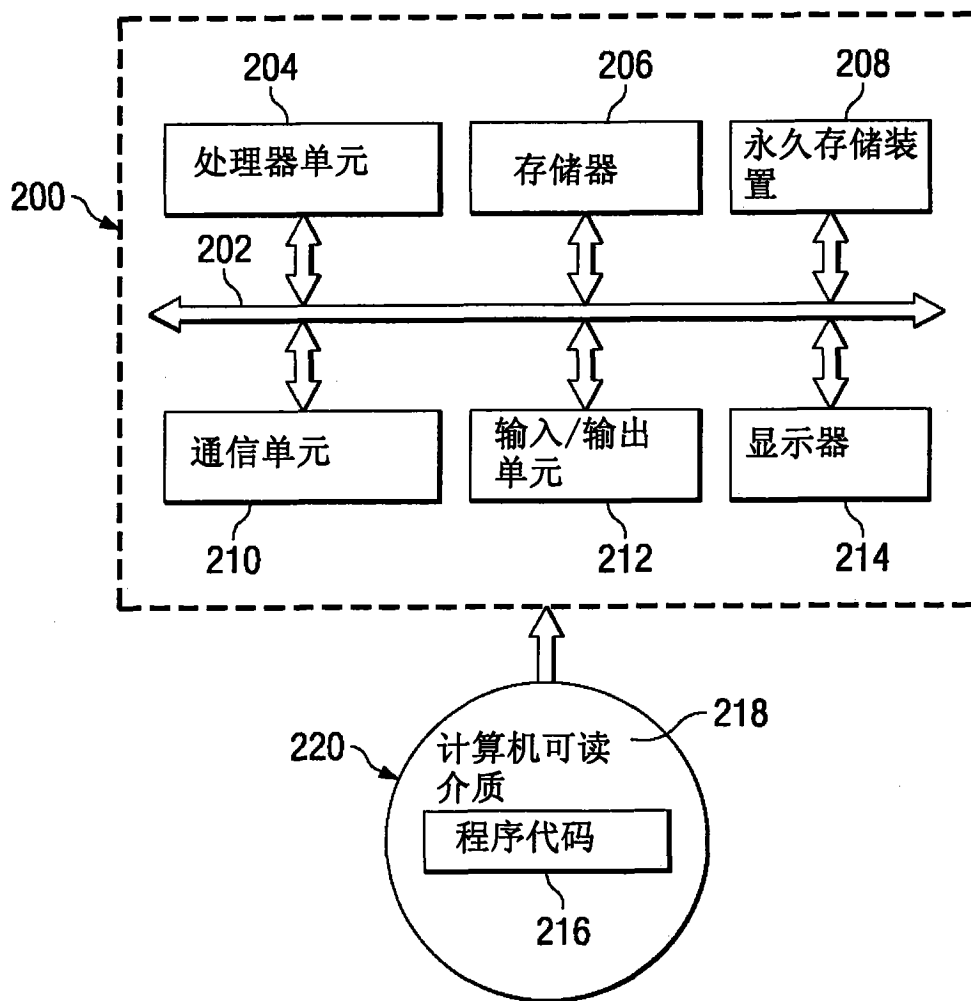


图2

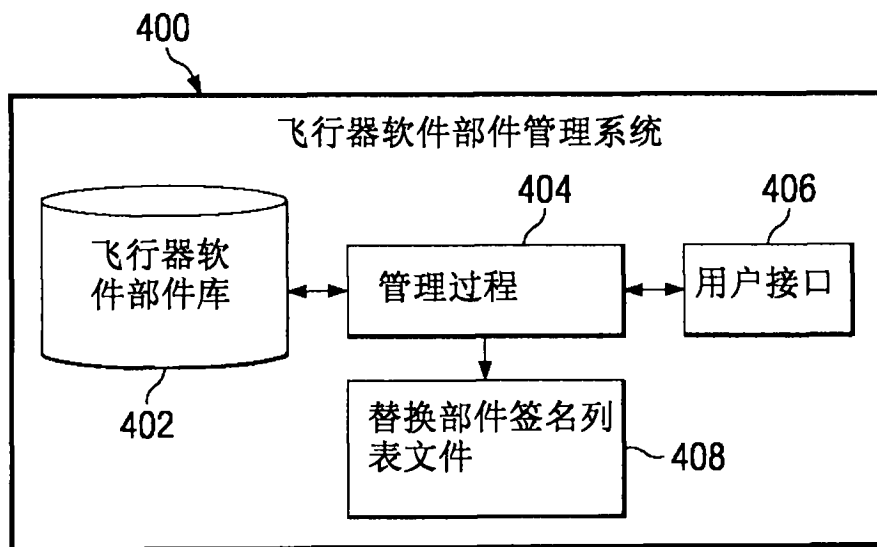


图4

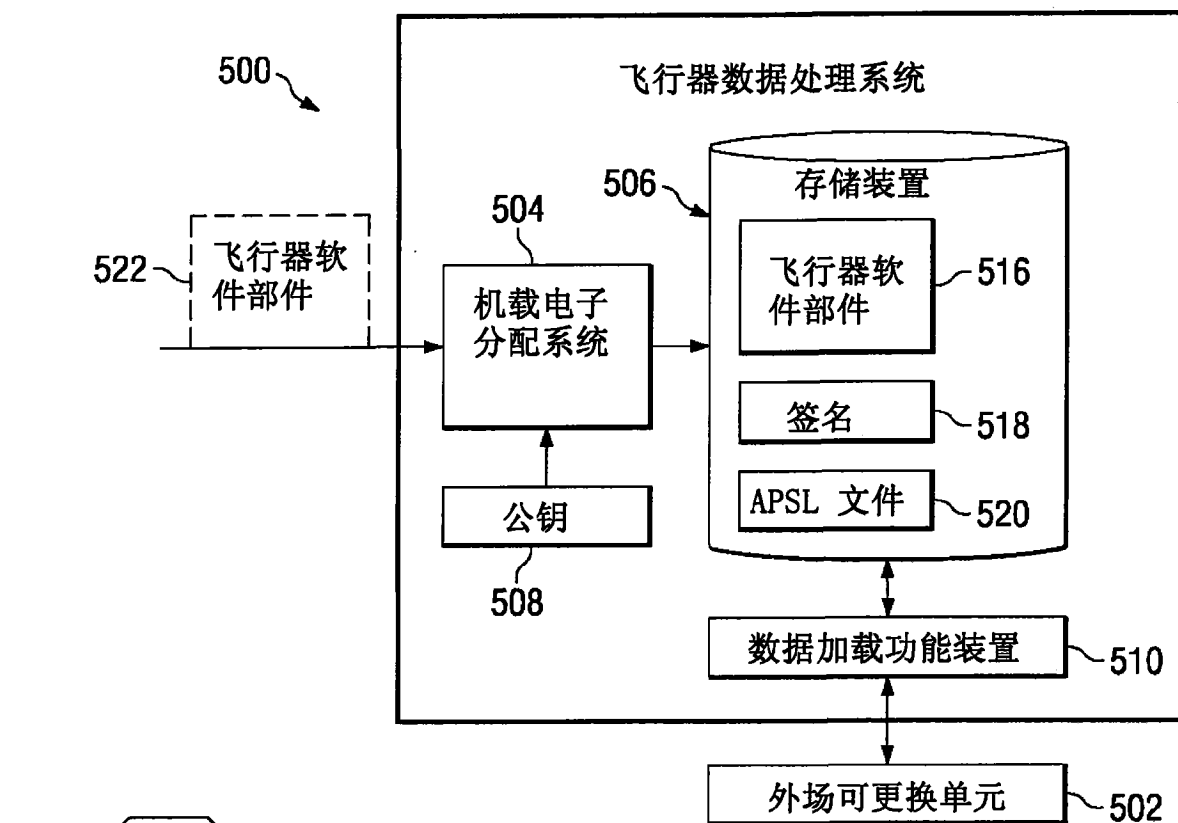


图5

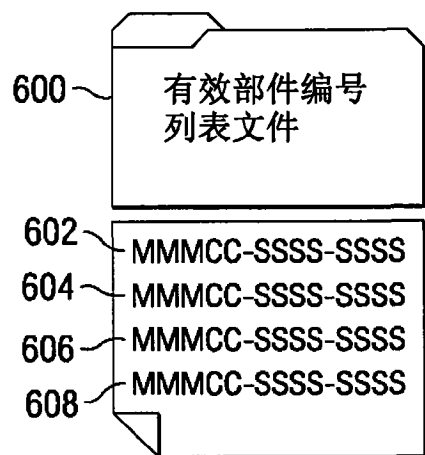


图6

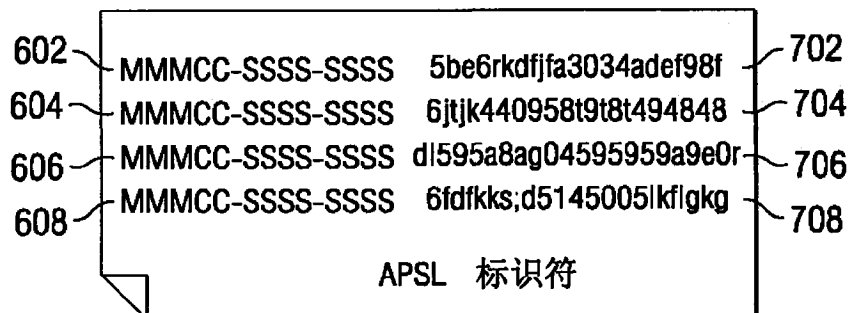
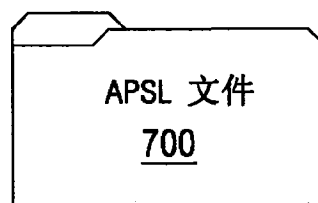


图7

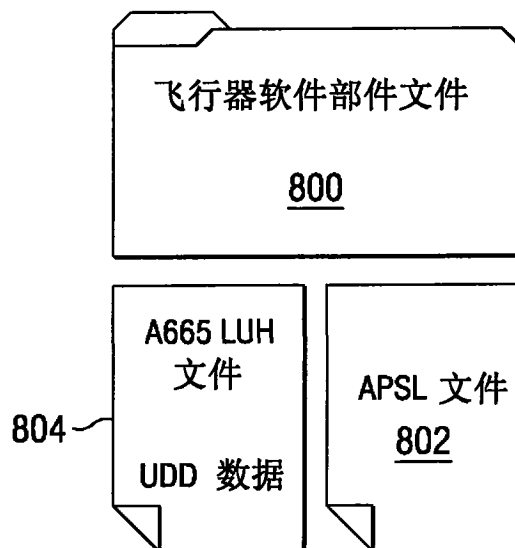


图8

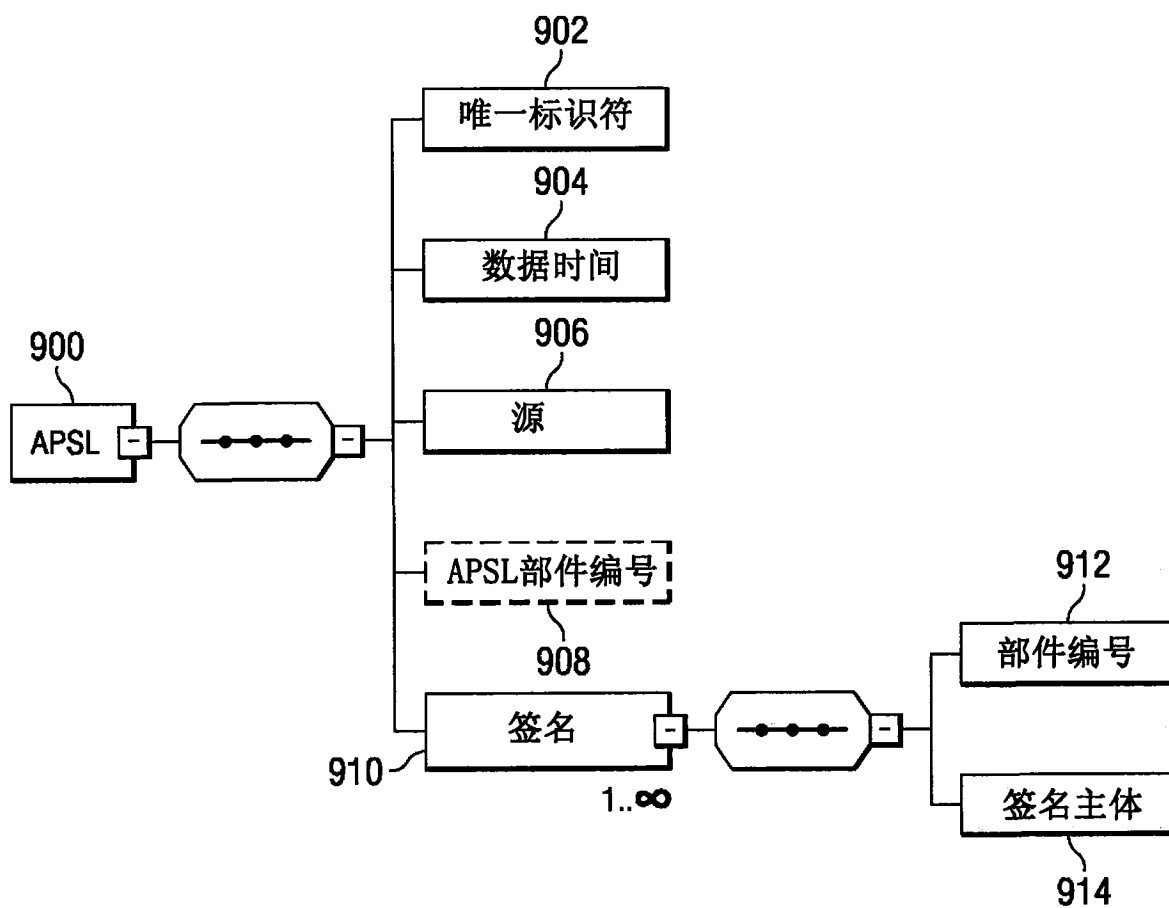


图9

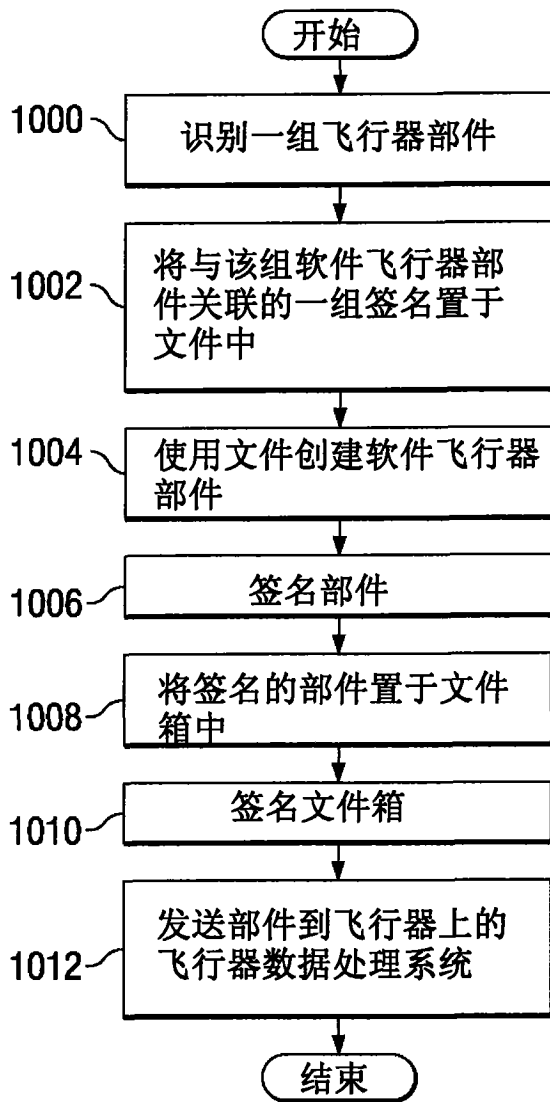


图10

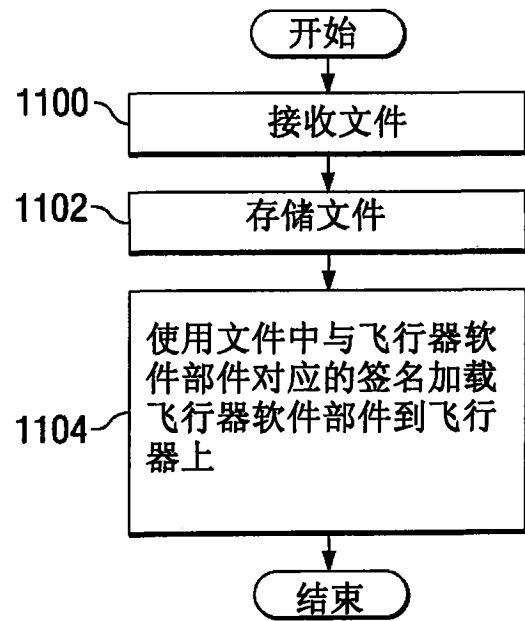


图11

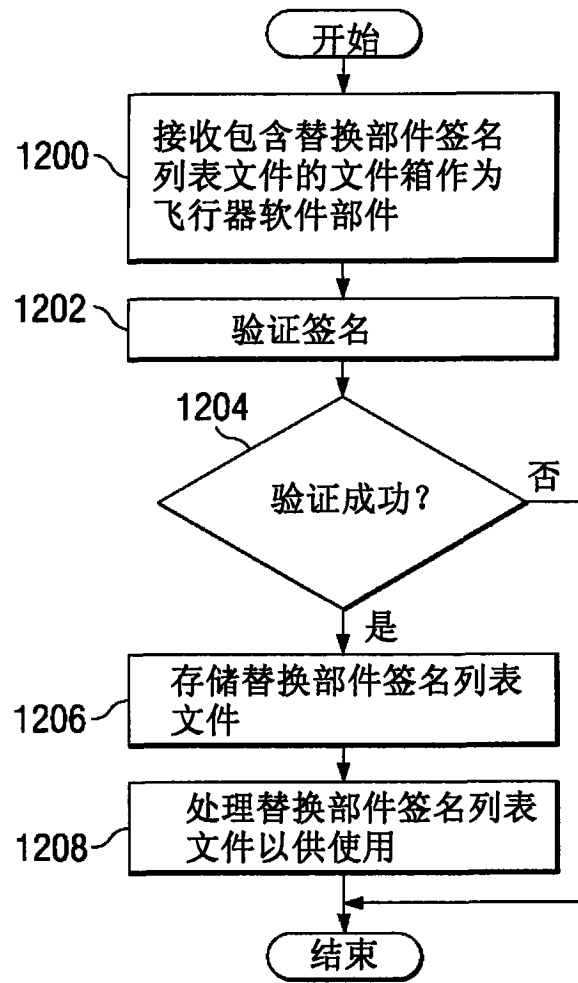


图12

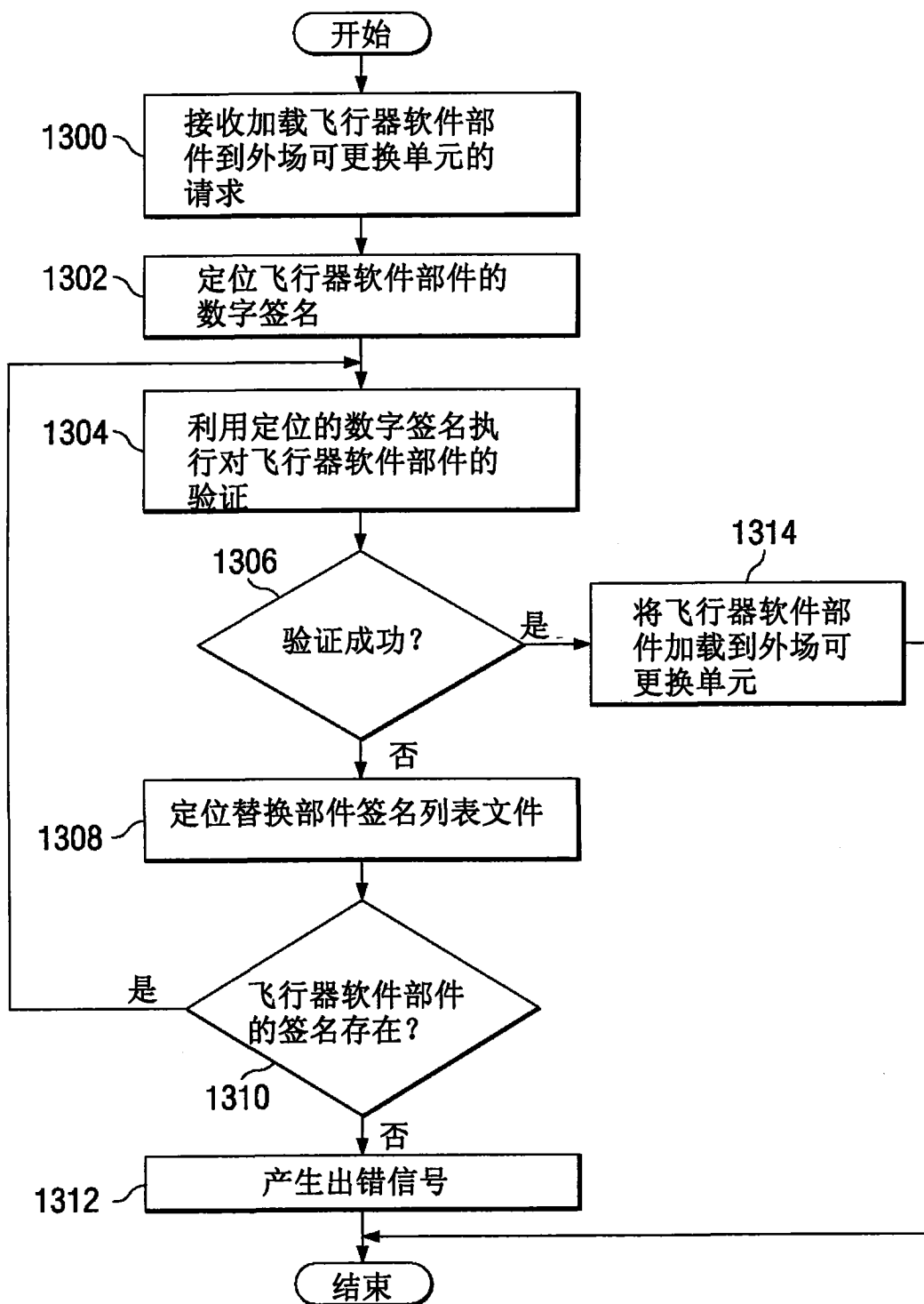


图13

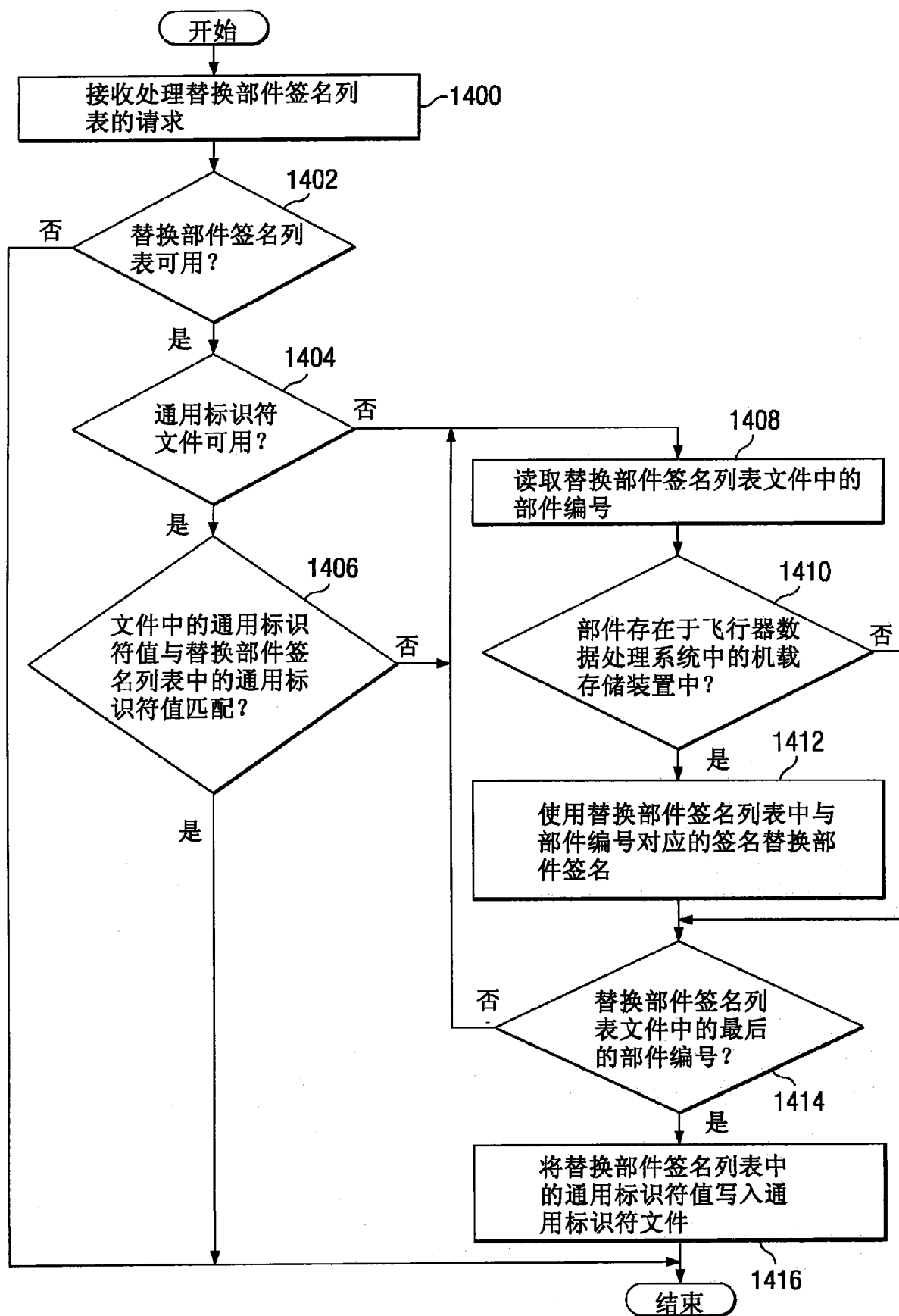


图14