(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 105009134 A
(43)申请公布日 2015.10.28

(21)申请号 201480009022.2
(22)申请日 2014.03.14
(30)优先权数据
13/838,038 2013.03.15 US
(85)PCT国际申请进入国家阶段日
2015.08.14
(86)PCT国际申请的申请数据
PCT/US2014/027684 2014.03.14
(87)PCT国际申请的公布数据
WO2014/143671 EN 2014.09.18
(71)申请人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 B·邢
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 高见
(51)Int.Cl.
G06F 21/12(2006.01)

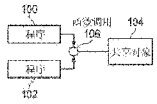
权利要求书3页 说明书17页 附图13页

(54)发明名称

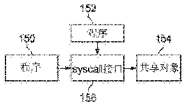
提供安全操作的方法、装置、系统和计算机可读介质

(57)摘要

在实施例中提供了以下技术，这些技术用于接收飞地程序以便在飞地中操作，标识该飞地程序的至少一个共享对象依赖性，确定该共享对象依赖性是否对应于至少一个飞地共享对象，在其中该共享对象依赖性对应于该飞地共享对象的环境中致使该共享对象依赖性和该飞地共享对象之间的关联性，以及在其中该共享对象依赖性不能对应于该飞地共享对象的环境中致使该共享对象依赖性与飞地可加载非飞地共享对象之间的关联性。



1A



1B

CN 105009134 A

1. 一种用于提供安全操作的装置，所述装置包括：

至少一个处理器；

至少一个存储器，所述至少一个存储器包括当由所述处理器执行时致使所述装置至少执行以下操作的指令：

接收飞地程序以便在飞地中操作；

标识所述飞地程序的至少一个共享对象依赖性；

确定所述共享对象依赖性是否对应于至少一个飞地共享对象；以及

飞地动态链接器，包括由所述处理器执行时致使所述装置至少执行以下操作的指令：

在其中所述共享对象依赖性对应于所述飞地共享对象的环境中导致所述共享对象依赖性和所述飞地共享对象之间的关联性；以及

在其中所述共享对象依赖性不对应于所述飞地共享对象的环境中导致所述共享对象依赖性和飞地可加载非飞地共享对象之间的关联性。

2. 如权利要求 1 所述的装置，其特征在于，所述飞地动态链接器包括当由所述处理器执行时致使所述装置至少部分地基于对所述共享对象依赖性的调用执行致使对所述飞地共享对象的调用的指令。

3. 如权利要求 2 所述的装置，其特征在于，对所述共享对象依赖性的调用涉及与所述共享对象依赖性相关联的函数调用的执行以及与所述飞地共享对象相关联的所述函数调用的执行。

4. 如权利要求 2 所述的装置，其特征在于，对所述共享对象依赖性的调用涉及对表示与所述共享对象依赖性相关联的 syscall 函数的 syscall 操作的调用以及所述飞地共享对象的函数调用的执行，所述函数调用对应于所述 syscall 函数。

5. 如权利要求 1-4 中任一项所述的装置，其特征在于，所述飞地共享对象是蹦床共享对象，并且进一步包括致使至少部分地基于对所述共享对象依赖性的调用来调用所述蹦床共享对象。

6. 如权利要求 5 所述的装置，其特征在于，所述蹦床共享对象的调用包括致使将操作转移到对应于所述蹦床共享对象的非飞地可加载共享对象。

7. 如权利要求 6 所述的装置，其特征在于，致使将操作转移到所述非飞地可加载共享对象包括发送标识所述非飞地可加载共享对象的指示。

8. 如权利要求 7 所述的装置，其特征在于，发送所述指示包括将所述指示发送到飞地加载器。

9. 如权利要求 8 所述的装置，其特征在于，致使将操作转移到所述非飞地可加载共享对象包括调用飞地代理，并且所述飞地代理将所述指示发送到所述飞地加载器。

10. 如权利要求 9 所述的装置，其特征在于，致使将操作转移到所述非飞地可加载共享对象包括由飞地加载器调用 syscall 操作。

11. 如权利要求 10 所述的装置，其特征在于，调用所述蹦床共享对象包括将与所述函数调用相关联的数据从至少一个飞地存储器复制到至少一个非飞地存储器，并且其中致使将操作转移到所述非飞地可加载共享对象包括发送标识所述非飞地存储器的指示。

12. 如权利要求 11 所述的装置，其特征在于，发送所述指示包括将所述指示发送到飞地加载器，并且其中致使将操作转移到所述非飞地可加载共享对象包括调用飞地代理，并

且所述飞地代理将所述指示发送到所述飞地加载器。

13. 至少一个用于提供安全操作的包括指令的计算机可读存储介质，当被处理器执行时，所述指令致使装置：

接收飞地程序以便在飞地中操作；

标识所述飞地程序的至少一个共享对象依赖性；

确定所述共享对象依赖性是否对应于至少一个飞地共享对象；

在其中所述共享对象依赖性对应于所述飞地共享对象的环境中导致所述共享对象依赖性和所述飞地共享对象之间的关联性；以及

在其中所述共享对象依赖性不对应于所述飞地共享对象的环境中导致所述共享对象依赖性和飞地可加载非飞地共享对象之间的关联性。

14. 如权利要求 13 所述的介质，其特征在于，标识所述共享对象依赖性包括评估所述飞地程序以便标识函数调用操作。

15. 如权利要求 14 所述的介质，其特征在于，飞地加载器标识所述函数调用操作。

16. 如权利要求 14 所述的介质，其特征在于，导致所述共享对象依赖性与所述飞地共享对象之间的关联性包括所述共享对象依赖性到所述飞地共享对象的链接，并且其中导致所述共享对象依赖性与所述飞地可加载非飞地共享对象之间的关联性包括所述共享对象依赖性到所述飞地可加载非飞地共享对象的链接。

17. 如权利要求 13 所述的介质，其特征在于，对所述共享对象依赖性的标识包括接收标识 syscall 操作的调用的异常的通知，所述 syscall 操作标识函数，并且其中导致所述共享对象依赖性与所述飞地共享对象之间的关联性包括标识提供所述函数的所述飞地共享对象。

18. 如权利要求 17 所述的介质，其特征在于，飞地数据链接器接收所述异常的所述通知。

19. 如权利要求 17 所述的介质，其特征在于，导致所述共享对象依赖性与所述飞地共享对象之间的关联性包括标识提供所述函数的所述飞地共享对象。

20. 如权利要求 13 至 19 中任一项所述的介质，其特征在于，所述飞地共享对象涉及与设备的飞地特权交互。

21. 如权利要求 20 所述的介质，其特征在于，与所述设备的所述交互在非飞地存储器中不存在指令并且非飞地存储器中不存在数据时发生，并且其中，所述设备与飞地存储器在相同的芯片上。

22. 如权利要求 20 所述的介质，其特征在于，所述设备涉及受保护音频视频通道启用设备中的至少一个。

23. 一种用于提供安全操作的方法，所述方法包括：

接收飞地程序以便在飞地中操作；

标识所述飞地程序的至少一个共享对象依赖性；

确定所述共享对象依赖性是否对应于至少一个飞地共享对象；

在其中所述共享对象依赖性对应于所述飞地共享对象的环境中导致所述共享对象依赖性和所述飞地共享对象之间的关联性；以及

在其中所述共享对象依赖性不对应于所述飞地共享对象的环境中导致所述共享对象

依赖性和飞地可加载非飞地共享对象之间的关联性。

24. 如权利要求 23 所述的方法，其特征在于，进一步包括致使至少部分地基于所述共享对象依赖性的调用而调用所述飞地共享对象。

25. 一种包括用于执行如权利要求 23 至 24 中任一项所述的方法的装置的设备。

提供安全操作的方法、装置、系统和计算机可读介质

技术领域

[0001] 本公开总体上涉及电子装置安全领域并且更具体地涉及提供安全操作。

[0002] 背景

[0003] 装置安全领域在当今社会已经变得日益重要。互联网已经允许全世界不同计算机网络的互连。然而，互联网同样已经为恶意行动者呈现利用这些网络而消极地影响装置的许多机会。某些类型的恶意软件（例如，bot（僵尸））可被配置成用于一旦软件感染主机计算机就从远程操作者接收命令。软件可被指令执行任何数量的恶意动作，诸如从主机计算机发送出垃圾邮件或恶意电子邮件、从与主机计算机相关联的商业或个人盗取敏感信息、传播到其他主机计算机、和/或协助服务攻击的分布式拒绝。此外，恶意行动者可销售或以其他方式给予其他恶意行动者访问，由此使主机计算机的利用恶化。因此，有效地保护和维护稳定的计算机和系统的能力继续为组件制造商、系统设计者和网络运营商提出显著的挑战。

[0004] 附图简要描述

[0005] 为了提供本公开及其特征和优点的更完整的理解，结合附图参照以下描述，其中相同的参考标号表示相同的部分，在附图中：

[0006] 图 1A 和图 1B 是根据至少一个实施例的程序和共享对象之间的关联性的框图；

[0007] 图 2A 和图 2B 是示出根据一个实施例的飞地 (enclave) 存储器的框图；

[0008] 图 3A-3C 是示出根据实施例的飞地的框图；

[0009] 图 4A-4E 是示出根据至少一个实施例的与飞地相关联的交互的交互图；

[0010] 图 5 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图；

[0011] 图 6 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图；

[0012] 图 7 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图；

[0013] 图 8 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图；

[0014] 图 9 是示出根据实施例的与处理器耦合的存储器的框图；以及

[0015] 图 10 是根据实施例的安排在点到点 (PtP) 配置中的计算系统的框图。

[0016] 实施方案的详细描述

[0017] 图 1A 和图 1B 是根据至少一个实施例的程序和共享对象之间的关联性的框图。图 1A 和图 1B 的示例仅仅是程序和共享对象之间的关联性的示例并且不限制权利要求书的范围。例如，归因于组件的操作可变化，组件数量可变化，组件的组成可变化等等。例如，在某些实施例中，可归因于图 1A 或图 1B 的示例的一个组件的操作可被分配给一个或多个其他组件。

[0018] 在计算系统中，可能令人期望的是多个程序能够利用同一组服务。例如，可能令人

期望的是多个程序能够向显示器提供信息、从输入设备接收信息、经由通信设备发送信息等等。

[0019] 在至少一个实施例中，多于一个程序利用共享对象访问同一组服务。在至少一个实施例中，共享对象涉及可用于多于一个程序的任何功能。例如，共享对象可以是由操作系统、内核、驱动程序等等提供的库、应用编程接口 (API)。在至少一个实施例中，利用共享对象的程序的一部分被称为共享对象依赖性 (shared object dependency)。例如，共享对象依赖性可以是与执行函数调用、从函数调用接收信息、从共享对象接收回调、向共享对象提供信息、从共享对象接收信息、通过共享对象调用操作等等相关联的程序的一部分。

[0020] 在至少一个实施例中，共享对象依赖性和共享对象之间存在关联性。例如，关联性可涉及与特定服务有关的共享对象依赖性到提供该特定服务的共享对象的映射。在至少一个实施例中，共享对象依赖性可以是共享对象的抽象，诸如句柄、名称、标识符等等。在这种示例中，抽象可用关联性补充以便允许程序与共享对象交互。例如，可通过提供与共享对象相关联的地址将抽象映射到共享对象，从而使得程序可通过抽象和映射地址访问共享对象。

[0021] 在至少一个实施例中，程序可通过调用共享对象依赖性导致对共享对象的调用。例如，如果共享对象依赖性涉及程序中的函数调用表示，则程序可通过执行与借助共享对象依赖性将控制转移到共享对象相关联的操作来调用共享对象依赖性，诸如通过执行函数调用。

[0022] 图 1A 是根据至少一个实施例的程序和共享对象之间的关联性的框图。在图 1A 的示例中，程序 100 和 102 具有对共享对象 104 的共享对象依赖性。在图 1A 的示例中，程序 100 的共享对象依赖性和程序 102 的共享对象依赖性与共享对象 104 的函数调用 106 相关联。在至少一个实施例中，共享对象依赖性的调用涉及执行与共享对象依赖性相关联的函数调用。例如，程序 102 可通过执行由程序 102 包括的代表性函数调用操作来调用其与函数调用 106 的关联性。在至少一个实施例中，共享对象的调用涉及执行与共享对象相关联的函数调用。例如，共享对象 104 可至少部分地基于程序 100 调用函数调用 106 来执行与函数调用 106 的实现相关联的操作。

[0023] 图 1B 是根据至少一个实施例的程序和共享对象之间的关联性的框图。在至少一个实施例中，通过 syscall（系统调用）操作执行共享对象的调用。在至少一个实施例中，syscall 操作涉及用于利用操作系统内核服务的机制。在至少一个示例实施例中，syscall 操作涉及通过软件中断（诸如“INT 80”）调用共享对象。例如，程序可执行触发软件中断的操作。在至少一个实施例中，syscall 操作涉及调用与共享对象的调用相关联的中断（诸如 syscall/sysenter 指令）。syscall 可涉及 ioctl 函数、fcntl 函数等等。在这种示例中，内核可接收 syscall 的通知并且调用共享对象来执行操作。在这种示例中，程序可在完成 syscall 之后接收控制。在至少一个实施例中，程序可访问可由共享对象访问的数据结构中的数据。以此方式，程序可通过在调用 syscall 操作之前写入这种数据结构来向共享对象发送信息。类似地，共享对象可通过在软件中断完成之前写入这种数据结构向程序发送信息。

[0024] 在图 1B 的示例中，程序 150 和 152 通过 syscall 接口 156 与共享对象 154 相关联。在至少一个实施例中，共享对象依赖性的调用涉及调用表示与共享对象依赖性相关联的函

数调用的 syscall 操作。例如，程序可执行调用 syscall 操作的操作。在至少一个实施例中，syscall 函数涉及程序期望通过 syscall 调用的函数。syscall 操作可通过标识函数、与函数相对应等等指示 syscall 函数。在至少一个实施例中，共享对象的调用涉及执行共享对象的函数调用。例如，中断处理器可接收指示函数的软件中断。在这种示例中，内核可执行共享对象的函数调用。在至少一个实施例中，函数调用与 syscall 函数相对应。

[0025] 图 2A 和图 2B 是示出根据一个实施例的飞地存储器的框图。图 2A 和图 2B 的示例仅仅是飞地存储器的示例并且不限制权利要求书的范围。例如，归因于组件的操作可变化，组件数量可变化，组件的组成可变化等等。例如，在某些实施例中，可归因于图 2A 或图 2B 的示例的一个组件的操作可被分配给一个或多个其他组件。

[0026] 在某些情况下，恶意程序可执行干扰非恶意程序的正常操作的动作。例如，恶意程序可修改由非恶意程序使用的数据。在另一个示例中，恶意程序可修改非恶意程序的操作存储在其中的存储器，从而使得恶意程序改变非恶意程序所执行的操作。以此方式，恶意程序可利用非恶意程序用于恶意目的。可能令人期望的是保护包括与程序相关联的数据和 / 或指令的存储器不受到这种修改。

[0027] 在至少一个实施例中，处理器提供用以预防对与程序相关联的指令和 / 或存储器的不适当修改的飞地。在至少一个实施例中，飞地是由处理器（诸如图 10 的处理器 1102）提供的安全措施。在至少一个实施例中，飞地涉及与程序相关联的存储器范围。在至少一个实施例中，与飞地程序相关联的存储器范围被称为飞地存储器。在至少一个实施例中，与飞地存储器相关联的存储器事务由处理器加密。在至少一个实施例中，处理器通过飞地密钥加密存储器事务。飞地密钥可在不同的飞地之间改变。例如，飞地可具有相关联的飞地密钥并且不同的飞地可具有不同的相关联的飞地密钥。在至少一个实施例中，处理器可阻止利用与飞地相关联的飞地密钥，除非处理器正在执行来自飞地存储器的指令。例如，如果处理器正在执行来自飞地外部的存储器的操作，则处理器可阻止利用飞地密钥。以此方式，如果飞地外部的程序从飞地存储器检索信息，处理器可不解密这种信息。

[0028] 在至少一个实施例中，飞地涉及安全飞地。

[0029] 安全飞地 (SE) 是英特尔的下一代处理器的革命性特征。简言之，安全飞地涉及到应用的虚拟地址空间中的孔径 (aperture)。朝向给定飞地范围的所有存储器事务可由处理器使用安全飞地特定的密钥加密，并且可在飞地由 EENTER 操作进入时变为可能。出于安全原因，飞地范围外部的任何代码可能不被允许执行，并且因此可能永远不具有机会访问安全飞地存储器。

[0030] 在至少一个实施例中，处理器在安全模式中操作。在至少一个实施例中，飞地模式涉及处理器处于处理器向信息应用飞地密钥的状态下。在至少一个实施例中，处理器在飞地模式下操作时阻止执行来自飞地外部的存储器的指令。例如，处理器可基于 EENTER 操作的调用进入飞地模式。在这种示例中，处理器可阻止执行来自飞地存储器外部的存储器的任何指令，直到处理器退出飞地模式。在至少一个实施例中，在飞地模式中操作的程序被称为飞地程序。

[0031] 图 2A 是示出根据至少一个实施例的涉及非飞地存储器 204 和 206 的飞地存储器 202 的框图。如前所述，飞地可通过从飞地存储器（诸如飞地存储器 202）读取和 / 或写入而阻止非飞地程序影响和 / 或检查飞地程序。

[0032] 图 2B 是示出根据至少一个实施例的飞地存储器的框图。在图 2B 的示例中，飞地存储器包括飞地程序 252、飞地共享对象 254、256 和 258、飞地动态链接器 (EDL) 260、共享对象信息 262、线程信息 264、266 和 268 以及未填充区域 270。在至少一个实施例中，飞地可被创建为包括静态分配的存储器区域。例如，飞地可被创建为具有指定的飞地存储器，并且可阻止分配给飞地存储器的存储器区域的修改。在至少一个实施例中，未填充区域 270 涉及不与飞地程序的任何模块的数据和 / 或指令相关联的飞地存储器的区域。在至少一个实施例中，线程信息涉及用于操作和管理一个或多个线程的信息。可能令人期望的是在飞地存储器中提供线程信息以便允许线程的安全管理。共享对象信息、EDL 和飞地共享对象可类似于参照图 3A-3C 所描述的。在至少一个实施例中，飞地程序涉及处理器执行以便执行飞地程序的操作的指令。

[0033] 图 3A-3C 是示出根据实施例的飞地的框图。图 3A 和图 3B 的示例仅仅是飞地的示例并且不限制权利要求书的范围。例如，归因于组件的操作可变化，组件数量可变化，组件的组成可变化等等。例如，在某些实施例中，可归因于图 2A 或图 2B 的示例的一个组件的操作可被分配给一个或多个其他组件。

[0034] 图 3A 是示出根据至少一个实施例的飞地的框图。在图 3A 的示例中，飞地动态链接器 (EDL) 303 和飞地程序 305 在飞地模式 301 下操作，并且飞地加载器 (ELoader) 304 在非飞地模式 302 下操作。

[0035] 在至少一个实施例中，ELoader 执行与可在飞地模式外部执行的飞地相关联的操作。例如，ELoader 可创建飞地、准备飞地程序用于加载、加载飞地程序、对来自飞地的向外调用做出响应、向飞地发送向内调用等等。在至少一个实施例中，来自飞地的向外调用涉及将控制从飞地模块转移到非飞地模块。例如，可存在可在飞地中执行以便退出飞地模式并且调用飞地模式外部的操作的 OCall 操作。在至少一个实施例中，到飞地的向内调用涉及将控制从非飞地模块转移到飞地模块。例如，可存在可在飞地外部执行以便进入飞地模式和 / 或致使执行飞地操作的 ECall 操作。在至少一个实施例中，ELoader 例如通过调用 ECreat 操作创建飞地。在图 3A 的示例中，ELoader 304 通过创建交互 311 创建飞地模式 301。

[0036] 在至少一个实施例中，EDL 执行与飞地内的飞地管理相关联的操作。例如，EDL 可在飞地内执行动态链接，准备飞地以便在加载之后进行操作，发送来自飞地的向外调用，对到飞地的向内调用做出响应等等。

[0037] 以此方式，ELoader 和 EDL 可例如通过 ECall 和 OCall 与彼此交互。在图 3A 的示例中，ELoader 304 和 EDL 303 通过 E/O 调用交互 312 与彼此交互。

[0038] 图 3B 是示出根据至少一个实施例的飞地的框图。在图 3B 的示例中，飞地动态链接器 (EDL) 326、飞地程序 327、飞地共享对象 326 和蹦床 (trampoline) 共享对象 327 在飞地模式 321 下操作，并且飞地加载器 (ELoader) 324 在非飞地模式 322 下操作。在图 3B 的示例中，ELoader 324 和 EDL 323 通过 E/O 调用交互 342 与彼此交互。在图 3B 的示例中，ELoader 324 通过创建交互 341 创建飞地模式 321。

[0039] 在至少一个实施例中，ELoader 可包括用于执行一个或多个操作的软件模块。例如，ELoader 可包括飞地创建器。在至少一个实施例中，飞地创建器执行与飞地创建相关联的操作，诸如创建、添加存储器页、初始化等等。在另一个示例中，ELoader 可包括飞地桥。

在至少一个实施例中，飞地桥与飞地内的模块交互，诸如通过接收 OCall、调用 ECall 等等。在图 3B 的示例中，ELoader 324 包括飞地创建器 333 和飞地桥 335。

[0040] 在至少一个实施例中，EDL 可包括用于执行一个或多个操作的软件模块。例如，EDL 可包括链接器。在至少一个实施例中，链接器执行操作，诸如将依赖性与函数调用相关联。例如，链接器可评估加载飞地程序以便解析程序的依赖性，从而使得依赖性映射到一个或多个函数调用。在另一个示例中，EDL 可包括飞地代理。在至少一个实施例中，飞地代理与飞地外部的模块交互，诸如通过接收 ECall、调用 OCall 等等。在图 3B 的示例中，EDL 323 包括飞地代理 332 和链接器 331。

[0041] 在某些情况下，可能令人期望的是飞地程序利用共享对象。在这种情况下，飞地可阻止直接使用共享对象。例如，共享对象可与非飞地存储器相关联。在这种情况下，飞地程序可不直接从飞地内调用共享对象。

[0042] 在某些情况下，共享对象可以是飞地可加载共享对象。在这种情况下，可能令人期望的是飞地可加载共享对象被加载到飞地以便允许飞地程序利用飞地内的飞地可加载共享对象。在至少一个实施例中，飞地可加载共享对象涉及能够与飞地操作的共享对象。飞地可加载共享对象可能不一定是为飞地内的操作而设计的，而是可以是适合于飞地内的操作的。例如，飞地可加载共享对象可避免利用非飞地存储器。在这种情况下，飞地可加载共享对象可被加载到飞地并且可在飞地内操作。在某些情况下，共享对象可以是非飞地可加载共享对象。非飞地可加载共享对象可以是与非飞地设备交互的共享对象（如参照图 3C 所描述的）、内核共享对象等等。

[0043] 在某些情况下，可能令人期望的是提供飞地共享对象。在至少一个实施例中，飞地共享对象涉及被创建以便在飞地模式下操作的共享对象。

[0044] 在至少一个实施例中，飞地共享对象涉及飞地专用共享对象。在至少一个实施例中，飞地专用共享对象涉及被涉及成用于在飞地内操作的共享对象。例如，飞地专用共享对象可执行可能不期望在飞地外部执行的特权操作，诸如加密或解密敏感信息。在不以任何方式限制权利要求书的范围的情况下，与提供飞地专用共享对象相关联的至少一个技术效果是允许飞地共享对象内的安全操作。例如，处理器可通过从飞地存储器读取和 / 或写入而阻止非飞地程序影响和 / 或检查飞地专用共享对象。在至少一个实施例中，飞地包括至少一个飞地专用共享对象。在至少一个实施例中，飞地专用共享对象涉及在非飞地存储器中不存在指令时以及非飞地存储器中不存在数据时的共享对象。

[0045] 在某些情况下，一个计算系统的飞地共享对象的可用性可不同于不同计算系统的飞地共享对象的可用性。例如，计算系统可提供飞地图形加速器驱动器，而不同计算系统可提供蹦床图形加速器驱动器。在这种情况下，可能期望允许程序不知道共享对象是涉及飞地共享对象还是蹦床共享对象。在至少一个实施例中，装置确定共享对象依赖性是否对应于飞地共享对象。在至少一个实施例中，共享对象依赖性和飞地共享对象之间的对应涉及身份、函数、句柄等等的对应。在至少一个实施例中，该装置在其中共享对象依赖性对应于飞地共享对象的环境中导致共享对象依赖性和飞地共享对象之间的关联性。在至少一个实施例中，该装置在其中共享对象依赖性不对应于飞地共享对象的环境中导致共享对象依赖性和蹦床共享对象之间的关联性。

[0046] 在某些情况下，一个或多个共享对象可能不是飞地可加载共享对象。在这种情况

下，可能期望在不存在提供与共享对象相关联的函数的飞地共享对象的情况下提供飞地程序利用该函数的方式。然而，如前所述，在飞地模式下，处理器可阻止非飞地共享对象从飞地存储器访问数据。这种阻止可阻止非飞地共享对象读取和/或写入与利用共享对象相关联的参数。例如，如果飞地程序调用共享对象并且将存储在飞地存储器中的参数传递到共享对象，处理器可阻止非飞地共享对象访问该参数。因此，至少出于此原因，可能期望提供蹦床共享对象。在至少一个实施例中，蹦床共享对象涉及致使调用与非飞地共享对象相关联的函数的飞地共享对象。蹦床共享对象可将与共享对象相关联的数据（诸如与函数调用相关联的数据）从飞地存储器复制到非飞地存储器。在至少一个实施例中，非飞地存储器中的复制数据可由非飞地共享对象接收，诸如非飞地可加载共享对象 328、非飞地可加载共享对象 329 等等。在至少一个实施例中，ELoader 可接收复制数据并且通过调用共享对象将复制数据提供给共享对象。在至少一个实施例中，调用非飞地可加载共享对象可类似于参照图 1A-1B 所描述的，诸如通过函数调用 343 和/或 syscall 344。

[0047] 在至少一个实施例中，蹦床共享对象致使将操作转移到对应于蹦床共享对象的非飞地可加载共享对象。例如，蹦床共享对象可例如通过函数调用 348 与飞地代理交互，以便导致调用非飞地共享对象，类似于参照图 4C-4D 所描述的。在至少一个实施例中，非飞地共享对象通过提供由蹦床共享对象所提供的服务的至少一部分对应于蹦床共享对象。在至少一个实施例中，将操作转移到非飞地模式可通过调用 OCall 操作来导致。

[0048] 在至少一个实施例中，飞地程序调用飞地可加载共享对象，诸如飞地可加载共享对象、飞地专用共享对象和/或蹦床共享对象。调用飞地可加载共享对象可类似于参照图 1A-1B 所描述的。例如，飞地程序可致使至少部分地基于共享对象依赖性的调用而调用飞地可加载共享对象。在另一个示例中，飞地程序可致使至少部分地基于共享对象依赖性的调用而调用蹦床共享对象。在图 3B 的示例中，飞地程序 325 通过调用 346 而调用飞地可加载共享对象 326 并且通过调用 347 而调用蹦床共享对象 327。飞地可加载共享对象 326 可以是飞地专用共享对象、飞地可加载非飞地享对象、蹦床共享对象等等。

[0049] 图 3C 是示出根据至少一个实施例的飞地的框图。在图 3C 的示例中，飞地动态链接器 (EDL) 353、飞地程序 355、飞地共享对象 356 和蹦床共享对象 357 在飞地模式 521 下操作，并且飞地加载器 (ELoader) 354 在非飞地模式 352 下操作。在图 3C 的示例中，ELoader 354 和 EDL 353 通过 E/O 调用交互 372 与彼此交互。在图 3C 的示例中，ELoader 354 通过创建交互 371 创建飞地模式 351。在图 3C 的示例中，飞地程序 355 通过调用 376 而调用飞地共享对象 356 并且通过调用 377 而调用蹦床共享对象 357。在图 3C 的示例中，EDL 353 包括飞地代理 362 和链接器 361。在图 3C 的示例中，蹦床共享对象 357 例如通过函数调用 378 调用飞地代理 362。在图 3C 的示例中，ELoader 354 包括飞地创建器 363 和飞地桥 365。在图 3C 的示例中，ELoader 354 通过函数调用 358 调用非飞地可加载共享对象 358 并且通过 syscall 374、syscall 接口 360 和函数调用 375 调用非飞地可加载共享对象 359。

[0050] 在至少一个实施例中，程序通过共享对象与设备交互。例如，共享对象可涉及用于设备的驱动器。在这种示例中，设备可以是图形加速器并且共享对象可以是图形加速器驱动器。

[0051] 在某些情况下，可能期望在程序和设备之间提供安全交互。例如，可能期望以不涉及非飞地存储器的方式与设备通信。例如，可能期望通过这种通信提供受保护音频视频通

道 (PAVP)。在另一个示例中，设备可涉及通信设备。在这种示例中，可能期望利用安全交互，诸如安全套接层 (SSL) 交互，其受益于飞地所提供的安全性。在这种示例中，可能期望提供与设备交互的飞地共享对象。

[0052] 在至少一个实施例中，飞地专用共享对象涉及与设备交互。在至少一个实施例中，飞地专用共享对象通过飞地特权交互与设备交互。在至少一个实施例中，设备知道交互是飞地特权交互。这种指示可允许执行安全操作、信任操作等等。在至少一个实施例中，飞地特权交互在非飞地存储器中不存在指令时以及非飞地存储器中不存在数据时发生。例如，飞地特权交互可阻止使用非飞地存储器。在至少一个实施例中，设备与飞地存储器位于相同的芯片上。在不以任何方式限制权利要求书的范围的情况下，设备与飞地存储器位于相同的芯片上的至少一个技术效果允许阻止访问共享飞地共享对象和设备之间的飞地特权交互。

[0053] 在至少一个实施例中，蹦床共享对象涉及设备。在至少一个实施例中，蹦床共享对象通过非飞地特权交互与设备交互。在至少一个实施例中，非飞地特权交互设备涉及与飞地存储器不相关联的交互。在图 3C 的示例中，蹦床共享对象 357 可通过非飞地特权交互 380 借助飞地代理 362 和飞地桥 365 来与设备 381 交互。

[0054] 图 4A-4E 是示出根据至少一个实施例的与飞地相关联的交互的交互图。图 4A-4E 的示例仅仅是交互的示例并且不限制权利要求书的范围。例如，模块的数量可变化，特定交互可变化，交互顺序可变化等等。

[0055] 图 4A 是示出根据至少一个实施例的与飞地相关联的交互的交互图。图 4A 的示例涉及 ELoader 401 和 EDL 402 之间的交互。

[0056] 在框 403，ELoader 接收飞地程序以便在飞地中操作。ELoader 可从操作系统、内核等等接收飞地程序。飞地程序可涉及任何程序，诸如被写为飞地程序的程序、在不考虑程序是飞地程序的情况下写入的程序等等。ELoader 可确定程序是飞地程序还是非飞地程序。可存在其中 ELoader 确定程序是飞地程序的某些情况以及其中 ELoader 确定相同的程序是非飞地程序的其他情况。例如，ELoader 可利用安全策略信息、配置文件信息、环境信息、命令行信息等等以便评估这种环境。

[0057] 在框 404，ELoader 准备飞地信息。在至少一个实施例中，飞地信息涉及与执行飞地程序相关联的信息。例如，飞地信息可涉及共享对象依赖性、飞地大小、飞地程序所使用的存储器量、与飞地程序指令相关联的存储器量、飞地程序是否利用线程、飞地程序指令等等。飞地信息的准备可包括确定飞地大小、确定共享对象依赖性、确定飞地共享对象的可用性、确定共享对象是否是飞地可加载共享对象、确定飞地专用共享对象的可用性、确定蹦床共享对象的可用性等等。

[0058] 在交互 405，ELoader 创建 EDL。EDL 的创建可以是飞地的创建的一部分。ELoader 可通过 ECreate 操作创建 EDL。

[0059] 在交互 406，ELoader 初始化 EDL。在至少一个实施例中，ELoader 通过初始化交互 406 向 EDL 发送飞地程序。在这种示例中，EDL 通过交互 406 接收飞地程序。

[0060] 在框 407，EDL 准备飞地。飞地准备可包括设置飞地栈、设置飞地堆、评估共享对象信息、链接飞地程序和共享对象信息等等。在至少一个实施例中，共享对象涉及共享对象列表。共享对象列表可包括与共享对象相关联的地址、共享对象的身份、与共享对象相关联的

句柄等等。在至少一个实施例中，共享对象信息是位置独立的，从而使得地址信息涉及从飞地存储器的基址的偏移。

[0061] 一旦接收到指示初始化完成的交互 408，在交互 409，Eloader 就可为 EDL 提供指示以便进入执行飞地程序。在至少一个实施例中，交互 409 涉及 EEnter 操作。

[0062] 在框 410，EDL 导致执行飞地程序。例如，EDL 可调用飞地程序的主可执行指令的进入点。当执行完成时，在交互 411，EDL 向 ELoader 发送指示飞地程序的执行终止的通知。当接收到交互 411 时，在交互 412，ELoader 可移除 EDL。在至少一个实施例中，ELoader 通过移除飞地（诸如通过 ERmove 操作）移除 EDL。

[0063] 图 4B 是示出根据至少一个实施例的与飞地相关联的交互的交互图。图 4B 的示例涉及 ELoader 421 和 EDL 422 之间的交互。

[0064] 在框 423，ELoader 接收飞地程序以便在飞地中操作，类似于参照图 4A 的框 403 所描述的。在框 424，ELoader 标识飞地程序的至少一个共享对象依赖性。标识共享对象依赖性可包括评估飞地程序以便确定共享对象依赖性。在至少一个实施例中，标识共享对象依赖性包括评估飞地程序以便标识函数调用操作。在至少一个实施例中，标识共享对象可包括确定共享对象依赖性是否对应于至少一个飞地共享对象。例如，ELoader 可利用可用飞地共享对象列表。在至少一个实施例中，标识共享对象包括标识蹦床共享对象。例如，如果 ELoader 确定共享对象依赖性不对应于至少一个飞地共享对象，则 ELoader 可标识对应于共享对象依赖性的蹦床共享对象。

[0065] 在框 425，ELoader 确定飞地大小。确定飞地大小可至少部分地基于由飞地程序利用线程、飞地程序所使用的数据结构、配置文件信息等等。在至少一个实施例中，飞地大小至少部分地基于所标识的共享对象。在框 426，ELoader 准备共享对象信息。准备共享对象信息可涉及评估所标识的共享对象依赖性以及任何所标识的共享对象。

[0066] 在交互 427，ELoader 创建 EDL，类似于参照图 4A 的交互 405 所描述的。在交互 428，ELoader 初始化 EDL，类似于参照图 4A 的交互 406 所描述的。在至少一个实施例中，在 428，ELoader 可向 EDL 发送共享对象信息。在至少一个实施例中，EDL 可通过交互 428 从 ELoader 接收共享对象信息。

[0067] 在框 429，EDL 设置飞地的堆和栈。堆和栈可至少部分地基于飞地信息、共享对象信息等等。在框 430，EDL 评估共享对象信息。评估共享对象信息可包括标识共享对象、解析共享对象信息、初始化堆等等。

[0068] 在框 431，EDL 导致飞地程序的共享对象依赖性和飞地共享对象之间的关联性。例如，在共享对象依赖性对应于飞地共享对象的情况下，EDL 导致飞地程序的共享对象依赖性和飞地共享对象之间的关联性。在另一个示例中，在共享对象依赖性不对应于飞地共享对象的情况下，EDL 导致飞地程序的共享对象依赖性和飞地可加载非飞地共享对象之间的关联性。在至少一个实施例中，导致共享对象依赖性和飞地共享对象之间的关联性包括共享对象依赖性到飞地共享对象的链接。例如，EDL 可链接飞地程序和飞地共享对象。在至少一个实施例中，导致共享对象依赖性和飞地可加载非飞地共享对象之间的关联性包括共享对象依赖性到飞地可加载非飞地共享对象的链接。例如，EDL 可链接飞地对象和蹦床共享对象。

[0069] 图 4C 是示出根据至少一个实施例的与飞地相关联的交互的交互图。图 4C 的示例

涉及飞地桥 441、飞地代理 442、飞地程序 443、蹦床共享对象 444 和非飞地可加载共享对象 445 之间的交互。

[0070] 在图 4C 的示例中，在框 446，飞地程序执行操作。在框 446 执行的操作可以是与飞地程序相关联的任何操作，诸如与飞地程序指令、线程管理指令等等相关联的操作。在至少一个实施例中，在交互 447，飞地程序导致调用蹦床共享对象。在至少一个实施例中，蹦床共享对象的调用导致将操作转移到对应于蹦床共享对象的非飞地共享对象。蹦床共享对象的调用可类似于参照图 1A-1B、图 3A-3C、图 7、图 8 等等所描述的。在至少一个实施例中，在框 448，蹦床共享对象的调用导致调用飞地代理。在至少一个实施例中，飞地代理的调用可与非飞地共享对象的数据相关联。在这种实施例中，蹦床共享对象的调用包括将与函数调用相关联的数据从至少一个飞地存储器复制到至少一个非飞地存储器，类似于参照图 2A-2B 和图 3B 所描述的。在图 4C 的示例中，在框 449，飞地代理 442 将数据复制到非飞地存储器。

[0071] 在至少一个实施例中，飞地代理导致将操作转移到非飞地模式。转移操作可涉及发送标识数据被复制到其上的非飞地共享对象和 / 或非飞地存储器的指示。在图 4C 的示例中，在交互 450，飞地代理 442 导致通过 OCall 操作将操作转移到飞地桥 441。OCall 操作可包括表示标识非飞地共享对象 445 的指示的信息。OCall 操作可包括表示在非飞地存储器中复制的数据的信息。在至少一个实施例中，接收包括标识非飞地共享对象的信息的 OCall 交互导致调用非飞地共享对象。调用可类似于参照图 1A-1B 和图 3A-3C 所描述的。在图 4C 的示例中，在交互 451，飞地桥调用非飞地可加载共享对象。

[0072] 在框 452，非飞地可加载共享对象执行操作。操作可涉及与完成与调用交互 451 相关联的服务的指令。当完成框 452 的操作时，在交互 453，非飞地可加载共享对象将控制返回到飞地桥。从非飞地可加载共享对象接收控制可导致飞地桥将控制转移到飞地代理。

[0073] 在至少一个实施例中，飞地桥导致将操作转移到飞地模式。转移操作可涉及发送标识数据由非飞地共享对象提供给其的非飞地共享对象、蹦床共享对象和 / 或任何非飞地存储器的指示。在图 4C 的示例中，在交互 454，飞地桥 441 导致通过 ECall 操作将操作转移到飞地代理 442。ECall 操作可包括指示非飞地存储器中的与非飞地共享对象的操作相关联的数据的信息。在至少一个实施例中，在框 445，飞地代理将从飞地桥接收的数据从非飞地存储器复制到飞地存储器。在交互 456，飞地代理 442 将控制返回到蹦床共享对象 444。在至少一个实施例中，交互 456 包括指示在框 456 被复制到飞地存储器的数据的信息。在至少一个实施例中，将控制返回到蹦床共享对象导致将控制返回在飞地程序和交互 457。在至少一个实施例中，交互 457 包括指示在框 456 被复制到飞地存储器的数据的信息。

[0074] 图 4D 是示出根据至少一个实施例的与飞地相关联的交互的交互图。图 4D 的示例涉及飞地桥 461、飞地代理 462、飞地程序 463、蹦床共享对象 464 和设备 466 之间的交互。

[0075] 在图 4D 的示例中，在框 467，飞地程序执行操作，类似于参照图 4C 的框 446 所描述的。飞地程序 463 通过交互 468 调用蹦床共享对象 464，类似于参照图 4C 的交互 447 所描述的。蹦床共享对象 464 通过交互 469 调用飞地代理 462，类似于参照图 4C 的交互 448 所描述的。飞地代理 462 通过交互 470 导致将控制转移到飞地桥 461，类似于参照图 4C 的交互 450 所描述的。飞地桥 461 通过交互 471 调用非飞地可加载共享对象 465，类似于参照图 4C 的交互 451 所描述的。

[0076] 在至少一个实施例中，调用非飞地可加载共享对象可包括非飞地共享对象和设备

之间的非飞地特权交互。非飞地特权交互可类似于参照图 3C 所描述的。非飞地可加载共享对象 465 通过非飞地特权交互 472 与设备 466 交互。非飞地可加载共享对象 465 通过交互 475 将控制返回到飞地桥 461，类似于参照图 4C 的交互 453 所描述的。飞地桥 462 通过交互 476 将控制转移到飞地代理 462，类似于参照图 4C 的交互 454 所描述的。飞地代理通过交互 477 将控制返回到蹦床共享对象 464，类似于参照图 4C 的交互 456 所描述的。蹦床共享对象 464 通过交互 478 将控制返回到飞地程序 463，类似于参照图 4C 的交互 457 所描述的。

[0077] 图 4E 是示出根据至少一个实施例的与飞地相关联的交互的交互图。图 4E 的示例涉及交互飞地程序 481、飞地专用共享对象 482 和设备 483。设备 483 可类似于参照图 3C 的设备 382 所描述的。

[0078] 在图 4E 的示例中，在框 484，飞地程序执行操作，类似于参照图 4C 的框 446 所描述的。在至少一个实施例中，在交互 485，飞地程序导致调用飞地专用共享对象。飞地共享对象的调用可类似于参照图 1A-1B、图 3A-3C、图 7、图 8 等等所描述的。在至少一个实施例中，在交互 486，飞地专用共享对象的调用导致与设备 483 的交互。在至少一个实施例中，飞地专用共享对象和设备之间的交互是飞地特权交互，类似于参照图 3C 所描述的。在交互 487，飞地专用共享对象将控制返回到飞地程序。

[0079] 图 5 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图。在至少一个实施例中，存在与图 5 的活动相对应的一组操作。装置（例如图 10 的计算系统 1100）可利用该组操作。该装置可包括用于执行这种操作的装置（包括例如图 9 的处理器 1000）。在实施例中，装置（例如图 10 的计算系统 1100）通过具有包括计算机代码的存储器（例如图 10 的存储器 1110）进行变换，该计算机代码被配置成用于与处理器（例如图 10 的处理器 1102）一起工作以便致使该装置执行图 5 的该组操作。

[0080] 在框 502，该装置接收飞地程序以便在飞地中操作。该接收可类似于参照图 4A 的框 403、图 4A 的交互 406 等等所描述的。飞地程序和飞地内的操作可类似于参照图 2A-2B 和图 3A-3C 所描述的。

[0081] 在框 504，该装置标识飞地程序的至少一个共享对象依赖性。共享对象、共享对象依赖性和标识可类似于参照图 1A-1B、图 2A-2B、图 3A-3C 和图 4A-4E 所描述的。在至少一个实施例中，共享对象依赖性的标识包括接收对标识调用 syscall 操作的异常的通知，类似于参照图 7 的所 704 所描述的。

[0082] 在框 506，该装置确定共享对象依赖性是否对应于至少一个飞地共享对象。飞地共享对象和与飞地共享对象的对应可类似于参照图 2A-2B 和图 3A-3C 所描述的。如果该装置确定共享对象依赖性对应于飞地共享对象，则流程进行到框 508。如果该装置确定共享对象依赖性不对应于飞地共享对象，则流程进行到框 510。

[0083] 在框 508，该装置导致飞地程序的共享对象依赖性和飞地共享对象之间的关联性。在至少一个实施例中，该装置在其中共享对象依赖性对应于飞地共享对象的环境中执行框 508 的动作。关联性和致使关联性可类似于参照图 1A-1B、图 3A-3C 等等所描述的。在至少一个实施例中，导致共享对象依赖性和飞地共享对象之间的关联性可包括共享对象依赖性到飞地共享对象的链接。

[0084] 在框 510，该装置导致共享对象依赖性和飞地可加载非飞地共享对象之间的关联

性。在至少一个实施例中，该装置在其中共享对象依赖性不能对应于飞地共享对象的环境中执行框 510 的动作。关联性和致使关联性可类似于参照图 1A-1B、图 3A-3C 等等所描述的。例如，导致共享对象依赖性和飞地可加载非飞地共享对象之间的关联性可包括共享对象依赖性到飞地可加载非飞地共享对象的链接。

[0085] 图 6 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图。在至少一个实施例中，存在与图 6 的活动相对应的一组操作。装置（例如图 10 的计算系统 1100）可利用该组操作。该装置可包括用于执行这种操作的装置（包括例如图 9 的处理器 1000）。在实施例中，装置（例如图 10 的计算系统 1100）通过具有包括计算机代码的存储器（例如图 10 的存储器 1110）进行变换，该计算机代码被配置成用于与处理器（例如图 10 的处理器 1102）一起工作以便致使该装置执行图 6 的该组操作。

[0086] 在框 602，该装置接收飞地程序以便在飞地中操作，类似于参照图 5 的框 502 所描述的。在框 604，该装置标识飞地程序的至少一个共享对象依赖性，类似于参照图 5 的框 504 所描述的。在框 606，该装置确定共享对象依赖性是否对应于至少一个飞地共享对象，如参照图 5 的框 506 所描述的。如果该装置确定共享对象依赖性对应于飞地共享对象，流程进行到框 608。如果该装置确定共享对象依赖性不对应于飞地共享对象，流程进行到框 612。

[0087] 在框 608，该装置准备与飞地共享对象相关联的共享对象信息，如参照图 4B 的框 426 所描述的。在框 610，该装置至少部分地基于共享对象信息链接飞地程序和飞地共享对象，类似于参照图 4B 的框 431 所描述的。

[0088] 在框 612，该装置准备与飞地可加载非飞地共享对象相关联的共享对象信息，如参照图 4B 的框 426 所描述的。在框 614，该装置至少部分地基于共享对象信息链接飞地可加载非飞地程序和飞地共享对象，类似于参照图 4B 的框 431 所描述的。

[0089] 图 7 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图。在至少一个实施例中，存在与图 7 的活动相对应的一组操作。装置（例如图 10 的计算系统 1100）可利用该组操作。该装置可包括用于执行这种操作的装置（包括例如图 9 的处理器 1000）。在实施例中，装置（例如图 10 的计算系统 1100）通过具有包括计算机代码的存储器（例如图 10 的存储器 1110）进行变换，该计算机代码被配置成用于与处理器（例如图 10 的处理器 1102）一起工作以便致使该装置执行图 7 的该组操作。

[0090] 在某些情况下，程序可具有至少部分地基于 syscall 操作的共享对象依赖性，类似于参照图 1B 所描述的。在这种情况下，可能期望通过 syscall 调用共享对象。例如，当发生由于在飞地内缺少适当的 syscall 接口的可用性而抛出异常时，飞地可捕获 syscall 操作。在这种情况下，该装置可接收由于调用 syscall 操作而发生异常的通知。例如，EDL 可捕获异常并且调用相应的飞地共享对象。在至少一个实施例中，标识共享对象依赖性包括接收异常标识调用 syscall 操作的通知。syscall 操作可标识函数。

[0091] 在框 702，该装置接收飞地程序以便在飞地中操作，类似于参照图 5 的框 502 所描述的。在框 704，该装置可接收异常标识调用 syscall 操作的通知。在至少一个实施例中，syscall 操作标识与软件中断相关联的函数，类似于参照图 1B 所描述的。在框 706，该装置确定该函数是否对应于至少一个飞地共享对象。飞地共享对象和与飞地共享对象的对应可类似于参照图 2A-2B 和图 3A-3C 所描述的。如果该装置确定该函数对应于飞地共享对象，则流程进行到框 708。如果该装置确定该函数不对应于飞地共享对象，则流程进行到框 710。

[0092] 在框 708，该装置导致调用飞地共享对象。飞地共享对象的调用可类似于参照图 1A-1B、图 3A-3C、图 4E 等等所描述的。在至少一个实施例中，该装置标识提供该函数的飞地共享对象，并且调用至少部分地基于标识。在至少一个实施例中，导致共享对象依赖性与飞地共享对象之间的关联性包括标识提供该函数的飞地共享对象。例如，组合图 5 的动作与图 7 的动作的实施例，框 508 可包括标识提供该函数的飞地共享对象。

[0093] 在框 710，该装置导致调用飞地可加载非飞地共享对象。飞地可加载非飞地共享对象的调用可类似于参照图 1A-1B、图 3A-3C、图 4C-4D 等等所描述的。在至少一个实施例中，该装置标识提供该函数的飞地可加载非飞地共享对象，并且调用至少部分地基于标识。在至少一个实施例中，致使共享对象依赖性与飞地可加载非飞地共享对象之间的关联性包括标识提供该函数的飞地可加载非飞地共享对象。例如，组合图 5 的动作与图 7 的动作的实施例，框 510 可包括标识提供该函数的飞地可加载非飞地共享对象。

[0094] 图 8 是示出根据至少一个实施例的与致使共享对象和飞地程序之间的关联性相关联的活动的流程图。在至少一个实施例中，存在与图 8 的活动相对应的一组操作。装置（例如图 10 的计算系统 1100）可利用该组操作。该装置可包括用于执行这种操作的装置（包括例如图 9 的处理器 1000）。在实施例中，装置（例如图 10 的计算系统 1100）通过具有包括计算机代码的存储器（例如图 10 的存储器 1110）进行变换，该计算机代码被配置成用于与处理器（例如图 10 的处理器 1102）一起工作以便致使该装置执行图 8 的该组操作。

[0095] 在框 802，该装置接收飞地程序以便在飞地中操作，类似于参照图 5 的框 502 所描述的。在框 804，该装置标识与 syscall 操作相关联的飞地程序的至少一个共享对象依赖性。共享对象、共享对象依赖性、与 syscall 操作的关联性和标识可类似于参照图 1A-1B、图 2A-2B、图 3A-3C 和图 4A-4E 所描述的。在框 806，该装置确定共享对象依赖性是否对应于至少一个飞地共享对象，如参照图 5 的框 506 所描述的。如果该装置确定共享对象依赖性对应于飞地共享对象，则流程进行到框 808。如果该装置确定共享对象依赖性不对应于飞地共享对象，则流程进行到框 812。

[0096] 在框 808，该装置准备与飞地共享对象相关联的共享对象信息，如参照图 6 的框 608 所描述的。在框 810，该装置指示 syscall 操作与飞地共享对象之间的关联性，如参照图 5 的框 508 所描述的。流程进行到框 816。

[0097] 在框 812，该装置准备与飞地可加载非飞地共享对象相关联的共享对象信息，如参照图 6 的框 612 所描述的。在框 810，该装置指示 syscall 操作与飞地可加载非飞地共享对象之间的关联性，如参照图 5 的框 510 所描述的。流程进行到框 816。

[0098] 在框 816，该装置接收异常标识调用 syscall 操作的通知，类似于参照图 7 的框 704 所描述的。在框 818，该装置调用与 syscall 操作相关联的共享对象。该调用可类似于参照图 7 的框 708、图 7 的框 710 等等所描述的。

[0099] 图 9 示出根据至少一个实施例与处理器 1000 耦合的存储器 1002。存储器 1002 可以是各种各样的存储器（包括存储器层级的各个层）中的任何一种。存储器 1002 可包括有待由处理器 1000 执行的代码 1004，该代码可以是一个或多个指令。处理器 1000 遵循代码 1004 所指示的指令程序序列。在至少一个实施例中，指令进入前端逻辑 1006 并且由一个或多个解码器 1008 处理。解码器可生成微操作（诸如处于预定义格式的固定宽度微操作），或者可生成表示该指令的其他指令、微指令、或控制信号等等。前端逻辑 1006 还包括

可分配资源并对微操作进行排队的寄存器重命名逻辑 1010 和调度逻辑 1012。

[0100] 处理器 1000 被示出为包括具有一组执行单元 1016-1 至 1016-N 的执行逻辑 1014。至少一个实施例可包括专用于特定功能或功能组的多个执行单元。至少一个实施例可包括仅一个执行单元或可执行具体功能的一个执行单元。执行逻辑 1014 执行微操作。

[0101] 在微操作执行完成之后，后端逻辑 1018 引退代码 1004 的指令。在一个实施例中，处理器 1000 允许乱序执行但实施指令的顺序引退。引退逻辑 1020 可采取各种形式（例如，重排序缓冲器等等）。以此方式，处理器 1000 在代码 1004 的执行期间被转换，至少在由解码生成的输出、寄存器重命名逻辑 1010 所利用的硬件寄存器和表和执行逻辑 1014 所修改的任何寄存器（未示出）方面。

[0102] 尽管未在图 9 中示出，处理元件可包括具有处理器 1000 的其他片上元件。例如，处理元件可包括存储器控制逻辑以及处理器 1000。处理元件可包括 I/O 控制逻辑和 / 或可包括集成有存储器控制逻辑器的 I/O 控制逻辑。处理元件还可包括一个或多个高速缓存。

[0103] 图 10 示出根据实施例的安排在点到点 (PtP) 配置中的计算系统 1100。具体而言，图 10 示出其中处理器、存储器和输入输出设备通过多个点到点接口互连的系统。

[0104] 如图 10 所示，系统 1100 可包括若干个处理器，为了清晰，仅示出了其中两个处理器，处理器 1102 和 1104。处理器 1102 和 1103 可各自包括可执行程序的多个进程的一组核 1103 和 1105。处理器 1102 和 1104 还可各自包括存储器控制器逻辑 (MC)1106 和 1108 以便与分别与存储器 1110 和 1112 通信。存储器 1110 和 / 或 1112 可存储各种数据，诸如参照存储器 1112 讨论的那些。在至少一个实施例中，存储器控制器逻辑 1106 和 1108 是与处理器 1102 和 1104 分离的离散逻辑。处理器 1102 和 1104 表示包括具有各种执行速度和功耗的单核或多核处理器的安排广泛范围的处理器和存储器安排以及各种架构（例如，具有一个或多个高速缓存级别）和各种类型（例如，动态随机存取、FLASH（闪存）等等）的存储器。

[0105] 处理器 1102 和 1104 可以是任何类型的处理器。处理器 1102 和 1104 可使用点到点接口电路 1116 和 1118 经由点到点 (PtP) 接口 1114 交换数据。处理器 1102 和 1104 可各自使用点到点接口电路 1126、1128、1130 和 1132 经由单独的点到点接口 1122 和 1124 与控制逻辑 1120 交换数据。控制逻辑 1120 可经由高性能图形接口 1136 使用接口电路 1137（其可以是 PtP 接口电路）与高性能图形电路 1134 交换数据。在至少一个实施例中，图 10 中示出的任何或全部 PtP 互连可被实现为多点总线而不是 PtP 链路。

[0106] 如在此所公开的，至少一个实施例被提供在处理器 1102 和 1104 中。然而，至少一个实施例存在与图 10 的系统 1100 内的其他电路、逻辑单元或设备中。此外，至少一个实施例分布通过图 10 中示出的若干电路、逻辑单元或设备。

[0107] 控制逻辑 1120 可经由接口电路 1141 与总线 1140 通信。总线 1140 具有通过其通信的一个或多个设备，诸如总线桥 1142 和 I/O 设备 1143。经由总线 1144，总线桥 1143 可与其他设备（诸如键盘 / 鼠标（或其他输入设备，诸如例如触摸屏）、通信设备 1146（诸如调制解调器、网络接口设备、或其他类型的可通过计算机网络通信的通信设备）、音频 I/O 设备 1147、数据存储设备 1148 等等）通信。数据存储设备 1148 可存储可由处理器 1102 和 / 或 1104 执行的代码 1149。在至少一个实施例中，总线架构的至少一部分用一个或多个 PtP 链路实现。

[0108] 在图10和图11中描绘的计算机系统是可根据各实施例利用的计算系统的实施例的示意说明。将认识到在图9和图10中描绘的系统的各个组件可组合在片上系统(SoC)架构中、可跨多个芯片或在任何其他合适的配置中分布。例如，在此公开的至少一个实施例可被结合到系统（诸如例如移动设备，诸如智能蜂窝电话、平板计算机、超极本计算机、个人数字助理、便携式游戏设备、桌上计算机、服务器、游戏控制台、互联网电器等等）中。将认识到在至少某些实施例中这些移动设备可提供有SoC架构。

[0109] 注意在至少一个实施例中，在此列出的至少一个操作、活动、功能等等可由在一个或多个有形介质（例如，在专用集成电路(ASIC)中提供的嵌入式逻辑、数字信号处理器(DSP)指令、有待由处理器或其他类似的机器执行的软件（可能包括对象代码和源代码）等等）中编码的逻辑实现。在至少一个实施例中，该逻辑可以是计算机程序指令，诸如图9的代码1004。在至少一个实施例中，存储器元件可存储用于在此描述的操作的数据。这包括存储器元件能够存储被执行以便实现在本说明书中描述的活动的软件、逻辑、代码或处理器指令。处理器可执行与数据相关联的任何类型的指令以便实现在本说明书中详细描述的操作。在至少一个实施例中，处理器通过指令将元件或物件（例如，数据）从一个状态或事物变换为另一种状态或事物。在另一个示例中，在此列出的活动可用固定逻辑或可编程逻辑（例如，由处理器执行的软件/计算机指令）实现，并且在此标识的元件可以是某种类型的可编程处理器、可编程数字逻辑（例如，现场可编程门阵列(FPGA)、EPROM或EEPROM)或可包括数字逻辑、软件、代码、电子指令或其任何合适的组合的ASIC。

[0110] 至少一个实施例包括软件以便实现在此列出的活动。与飞地相关联的模块（例如ELoader或EDL)可包括用于存储有待用于实现在此讨论的安全活动的信息的存储器元件。此外，与飞地相关联的模块可包括可执行软件以便执行在此公开的活动的处理器。当合适时并且基于特定需要，这些设备可进一步在任何合适的存储器元件（随机存取存储器(RAM)、ROM、EPROM、EEPROM、ASIC等等）、软件、硬件或在任何其他合适的组件、设备、元件或对象中保存信息。此外或可替代地，与飞地相关联的模块可以是软件、硬件、固件或其组合。在此讨论的任何存储器项目（例如，数据库、表、树、高速缓存等等）应当被解释为包含在广义术语“存储器元件”中。类似地，在本说明书中描述的任何可能的处理元件、模块和机器应当被解释为包含在广义术语“处理器”中。

[0111] 注意，结合以上提供的示例和在此提供的许多其他示例，可在两个、三个或四个元件方面描述交互。然而，已经仅为了清晰性和示例的目的完成了这一动作。在某些情况下，可能更容易的是仅通过引用有限数量的元件描述给定流程集合的功能中的一个或多个。应当认识到组件、模块等等（及其教导）是容易可扩展的并且可容纳大量的组件以及更复杂/精细的安排和配置。因此，所提供的示例不应当限制范围或抑制与飞地相关联的模块的广泛教导，因为其可能应用于非常大量的其他架构。

[0112] 还重要的是注意前述流程图中的操作仅示出可与致使有待结合安全异常执行的操作相关联地执行的可能的相关场景和模式中的一些。当合适时可删除或移除这些操作中的某些，或者可相当地修改或改变这些操作而不背离本公开的范围。此外，这些操作中的多个操作已经被描述为与一个或多个附加操作并发地或并行地执行。然而，可相当地更改这些操作的定时。已经为示例和讨论的目的提供了前述操作流。与飞地相关联的模块提供了大量的灵活性，因为可提供任何合适的安排、时序、配置和定时机制而不背离本公开的教

导。

[0113] 尽管已经详细地参照特定安排和配置描述了本公开，可显著地改变这些示例配置和安排而不背离本公开的范围。

[0114] 其他注释和示例

[0115] 示例 1 是一种提供安全操作的装置，该装置包括：至少一个处理器；至少一个存储器，该至少一个存储器包括当由该处理器执行时致使该装置至少执行以下内容的指令：接收飞地程序以便在飞地中操作；标识该飞地程序的至少一个共享对象依赖性；确定该共享对象依赖性是否对应于至少一个飞地共享对象；以及飞地动态链接器，包括由该处理器执行时致使该装置至少执行以下操作的指令：在其中该共享对象依赖性对应于该飞地共享对象的环境中导致该共享对象依赖性和该飞地共享对象之间的关联性；以及在其中该共享对象依赖性不能对应于该飞地共享对象的环境中导致该共享对象依赖性和飞地可加载非飞地共享对象之间的关联性。

[0116] 在示例 2 中，关于示例 1 所述的主题，该飞地动态链接器包括当由该处理器执行时致使该装置至少部分地基于该共享对象依赖性的调用执行致使该飞地共享对象的调用的指令。

[0117] 在示例 3 中，关于示例 2 所述的主题，对该共享对象依赖性的调用涉及与该共享对象依赖性相关联的函数调用的执行以及与该飞地共享对象相关联的该函数调用的执行。

[0118] 在示例 4 中，关于示例 2-3 所述的主题，对该共享对象依赖性的调用涉及对表示与该共享对象依赖性相关联的 syscall 函数的 syscall 操作的调用以及该飞地共享对象的函数调用的执行，该函数调用对应于该 syscall 函数。

[0119] 在示例 5 中，关于示例 1-4 所述的主题，该飞地共享对象是蹦床共享对象，并且进一步包括至少部分地基于对该共享对象依赖性的调用来调用该蹦床共享对象。

[0120] 在示例 6 中，关于示例 5 所述的主题，该蹦床共享对象的调用包括致使将操作转移到对应于该蹦床共享对象的非飞地可加载共享对象。

[0121] 在示例 7 中，关于示例 6 所述的主题，致使将操作转移到该非飞地可加载共享对象包括发送标识该非飞地可加载共享对象的指示。

[0122] 在示例 8 中，关于示例 7 所述的主题，其中，发送该指示包括将该指示发送到飞地加载器。

[0123] 在示例 9 中，关于示例 8 所述的主题，其中，致使将操作转移到该非飞地可加载共享对象包括调用飞地代理，并且该飞地代理将该指示发送到该飞地加载器。

[0124] 在示例 10 中，关于示例 9 所述的主题，其中，致使将操作转移到该非飞地可加载共享对象包括由飞地加载器调用系统调用操作。

[0125] 在示例 11 中，关于示例 10 所述的主题，其中，调用该蹦床共享对象包括将与该函数调用相关联的数据从至少一个飞地存储器复制到至少一个非飞地存储器，并且其中，致使将操作转移到该非飞地可加载共享对象包括发送标识该非飞地存储器的指示。

[0126] 在示例 12 中，关于示例 11 所述的主题，其中，发送该指示包括将该指示发送到飞地加载器，并且其中致使将操作转移到该非飞地可加载共享对象包括调用飞地代理，并且该飞地代理将该指示发送到该飞地加载器。

[0127] 示例 13 是至少一种用于提供安全操作的包括指令的计算机可读存储介质，当被

执行时，该指令致使装置：接收飞地程序以便在飞地中操作，标识该飞地程序的至少一个共享对象依赖性，确定该共享对象依赖性是否对应于至少一个飞地共享对象，在其中该共享对象依赖性对应于该飞地共享对象的环境中导致该共享对象依赖性和该飞地共享对象之间的关联性，以及在其中该共享对象依赖性不能对应于该飞地共享对象的环境中导致该共享对象依赖性与飞地可加载非飞地共享对象之间的关联性。

[0128] 在示例 14 中，关于示例 13 所述的主题，标识该共享对象依赖性包括评估该飞地程序以便标识函数调用操作。

[0129] 在示例 15 中，关于示例 14 所述的主题，飞地加载器标识该函数调用操作。

[0130] 在示例 16 中，关于示例 14-15 所述的主题，致使该共享对象依赖性与该飞地共享对象之间的关联性包括该共享对象依赖性到该飞地共享对象的链接，并且其中，致使该共享对象依赖性与该飞地可加载非飞地共享对象之间的关联性包括该共享对象依赖性到该飞地可加载非飞地共享对象的链接。

[0131] 在示例 17 中，关于示例 13-16 所述的主题，对该共享对象依赖性的标识包括接收标识 syscall 操作的调用的异常的通知，该 syscall 操作标识函数，并且其中，致使该共享对象依赖性与该飞地共享对象之间的关联性包括标识提供该函数的该飞地共享对象。

[0132] 在示例 18 中，关于示例 17 所述的主题，飞地数据链接器接收该异常的该通知。

[0133] 在示例 19 中，关于示例 17-18 所述的主题，致使该共享对象依赖性与该飞地共享对象之间的关联性包括标识提供该函数的该飞地共享对象。

[0134] 在示例 20 中，关于示例 13-19 所述的主题，该飞地共享对象涉及与设备的飞地特权交互。

[0135] 在示例 21 中，关于示例 20 所述的主题，与该设备的该交互在非飞地存储器中不存在指令并且非飞地存储器中不存在数据时发生，并且其中，该设备与飞地存储器在相同的芯片上。

[0136] 在示例 22 中，关于示例 20-21 所述的主题，该设备涉及受保护音频视频通道启用设备中的至少一个。

[0137] 在示例 23 中，关于示例 20-22 所述的主题，该设备涉及通信设备并且该交互涉及关于安全套接层的交互。

[0138] 示例 24 是一种方法，该方法包括：用于接收飞地程序以便在飞地中操作，标识该飞地程序的至少一个共享对象依赖性，确定该共享对象依赖性是否对应于至少一个飞地共享对象，在其中该共享对象依赖性对应于该飞地共享对象的环境中导致该共享对象依赖性和该飞地共享对象之间的关联性，以及在其中该共享对象依赖性不对应于该飞地共享对象的环境中导致该共享对象依赖性与飞地可加载非飞地共享对象之间的关联性。

[0139] 在示例 25 中，关于示例 24 所述的主题，标识该共享对象依赖性包括评估该飞地程序以便标识函数调用操作。

[0140] 在示例 26 中，关于示例 25 所述的主题，飞地加载器标识该函数调用操作。

[0141] 在示例 27 中，关于示例 25-26 所述的主题，致使该共享对象依赖性与该飞地共享对象之间的关联性包括该共享对象依赖性到该飞地共享对象的链接，并且其中，致使该共享对象依赖性与该飞地可加载非飞地共享对象之间的关联性包括该共享对象依赖性到该飞地可加载非飞地共享对象的链接。

[0142] 在示例 28 中，关于示例 24-27 所述的主题，该共享对象依赖性的标识包括接收标识 syscall 操作的调用的异常的通知，该系统调用操作标识函数，并且其中，致使该共享对象依赖性与该飞地共享对象之间的关联性包括标识提供该函数的该飞地共享对象。

[0143] 在示例 29 中，关于示例 28 所述的主题，飞地数据链接器接收该异常的该通知。

[0144] 在示例 30 中，关于示例 28-29 所述的主题，致使该共享对象依赖性与该飞地共享对象之间的关联性包括标识提供该函数的该飞地共享对象。

[0145] 在示例 31 中，关于示例 24-30 所述的主题，该飞地共享对象涉及与设备的飞地特权交互。

[0146] 在示例 32 中，关于示例 31 所述的主题，与该设备的该交互在非飞地存储器中不存在指令并且非飞地存储器中不存在数据时发生，并且其中，该设备与飞地存储器在相同的芯片上。

[0147] 在示例 33 中，关于示例 31-32 所述的主题，该设备涉及受保护音频视频通道启用设备中的至少一个。

[0148] 在示例 34 中，关于示例 31-33 所述的主题，该设备涉及通信设备并且该交互涉及关于安全套接层的交互。

[0149] 示例 35 是一种包括用于执行示例 24-34 所述的方法的装置的设备。

[0150] 在示例 36 中，关于示例 35 的主题，用于执行该方法的该装置包括处理器和存储器。

[0151] 在示例 37 中，关于示例 36 所述的主题，该存储器包括机器可读指令，当被执行时，该指令致使该设备执行示例 24-34 所述的方法。

[0152] 示例 38 是至少一个包括指令的计算机可读介质，当被执行时，该指令实现一种用于实现在前述示例中任一项中所描述的设备的方法。

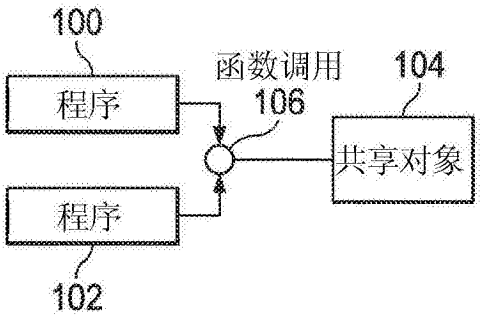


图 1A

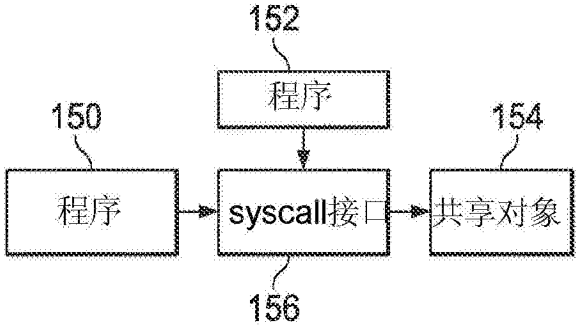


图 1B

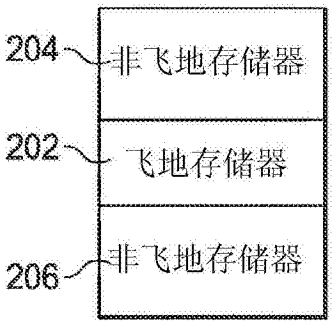


图 2A

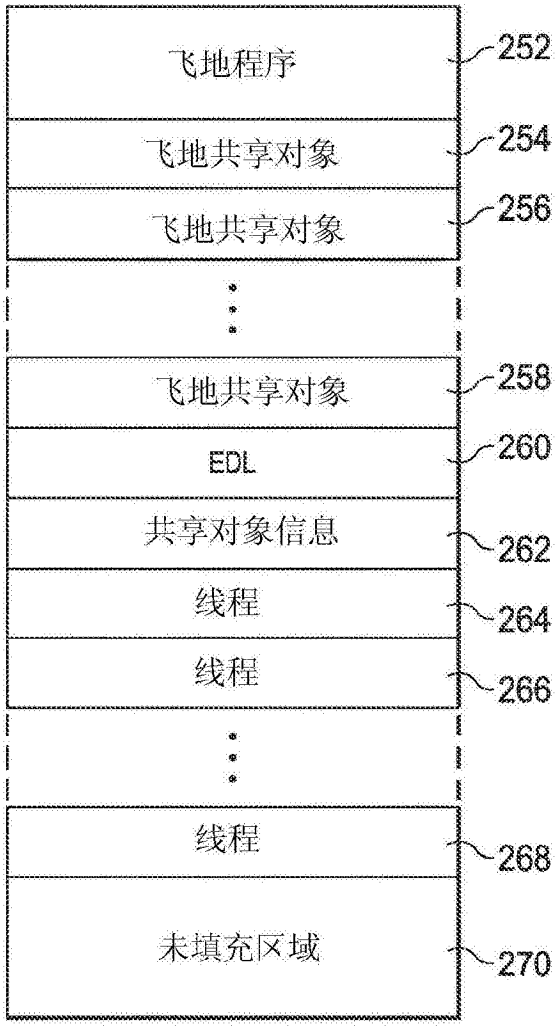


图 2B

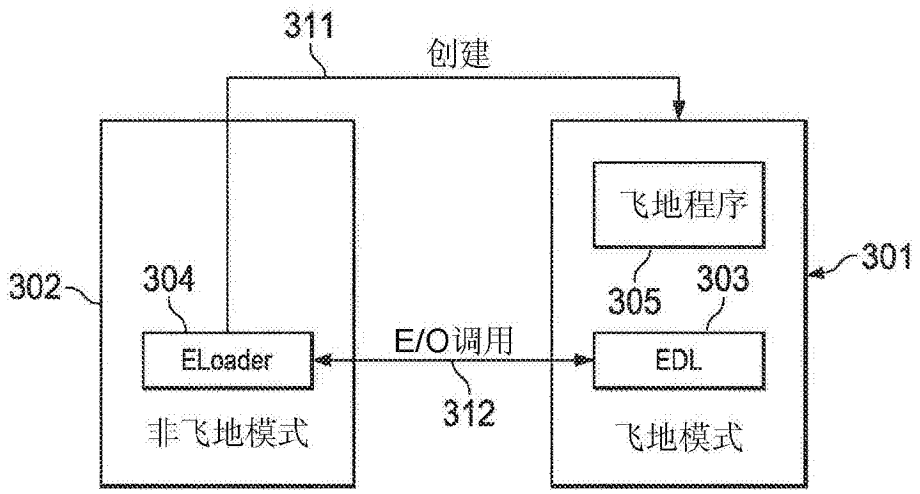

311
创建
飞地程序
301
302
304
305
303
ELoader
E/O调用
EDL
312
非飞地模式
飞地模式

图 3A

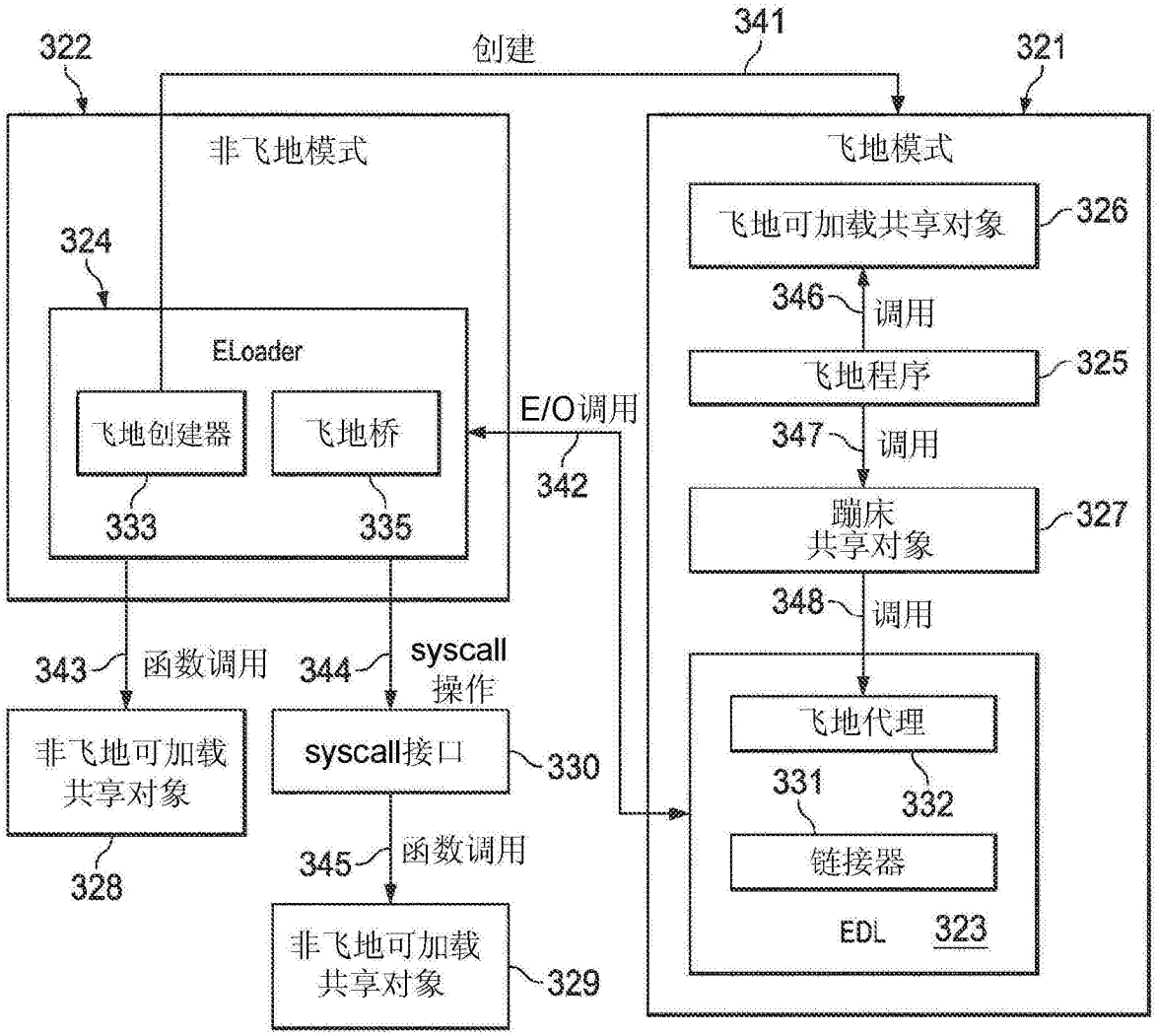

322
创建
341
321
非飞地模式
飞地模式
飞地可加载共享对象
326
324
346
调用
ELoader
飞地程序
325
飞地创建器
飞地桥
E/O调用
347
调用
342
333
335
蹦床
共享对象
327
348
调用
343
函数调用
344
syscall
操作
飞地代理
非飞地可加载
共享对象
syscall接口
330
331
332
链接器
345
函数调用
EDL
323
328
非飞地可加载
共享对象
329

图 3B

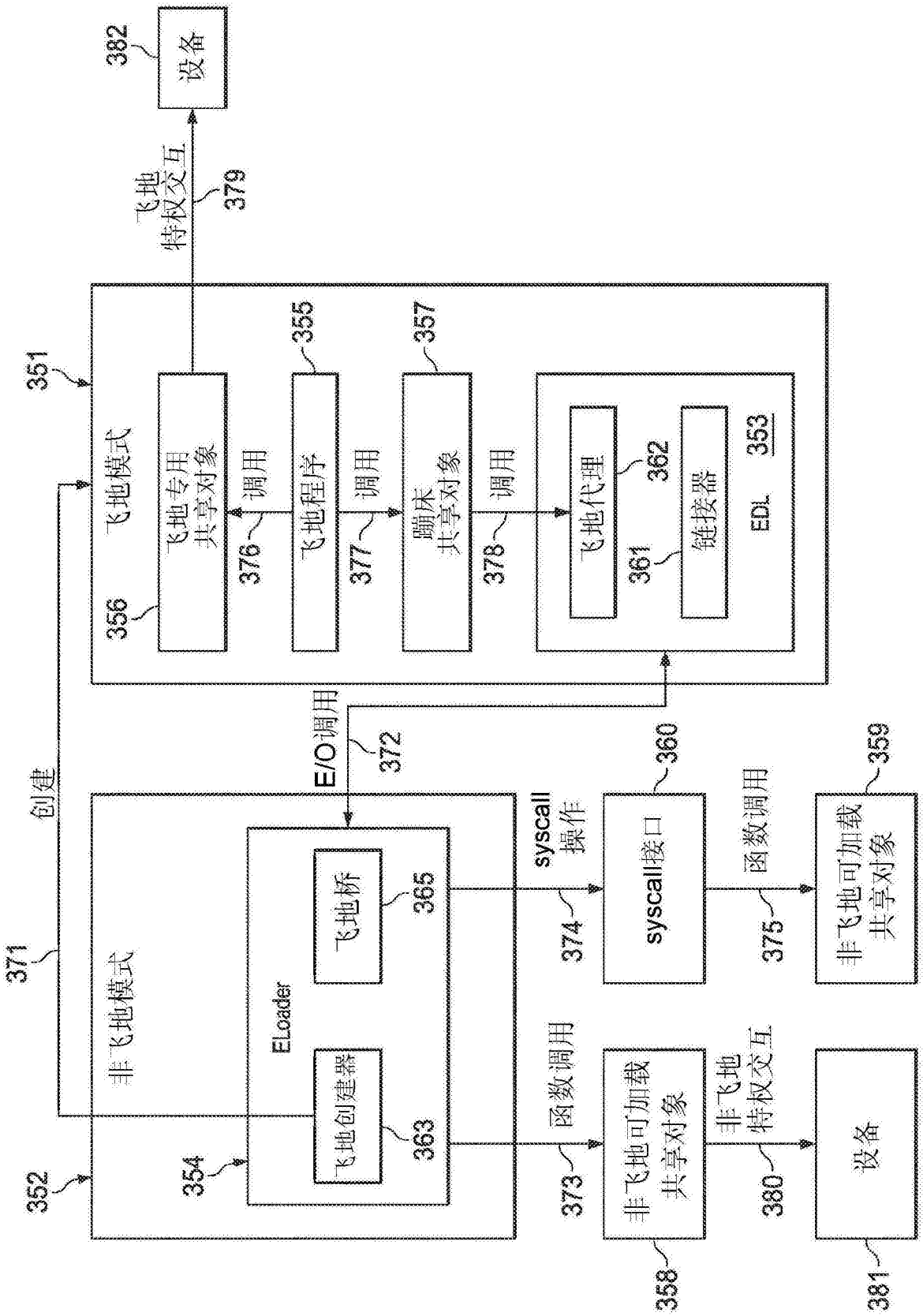

382
设备
飞地
特权交互
379
351
飞地模式
355
357
飞地专用
共享对象
调用
飞地程序
调用
蹦床
共享对象
调用
飞地代理
362
链接器
361
EDL
353
356
376
377
378
E/O调用
372
创建
371
非飞地模式
ELoader
飞地桥
365
飞地创建器
363
354
352
syscall
操作
374
360
syscall接口
函数调用
375
359
非飞地可加载
共享对象
函数调用
373
非飞地可加载
共享对象
358
非飞地
特权交互
380
设备
381

图 3C

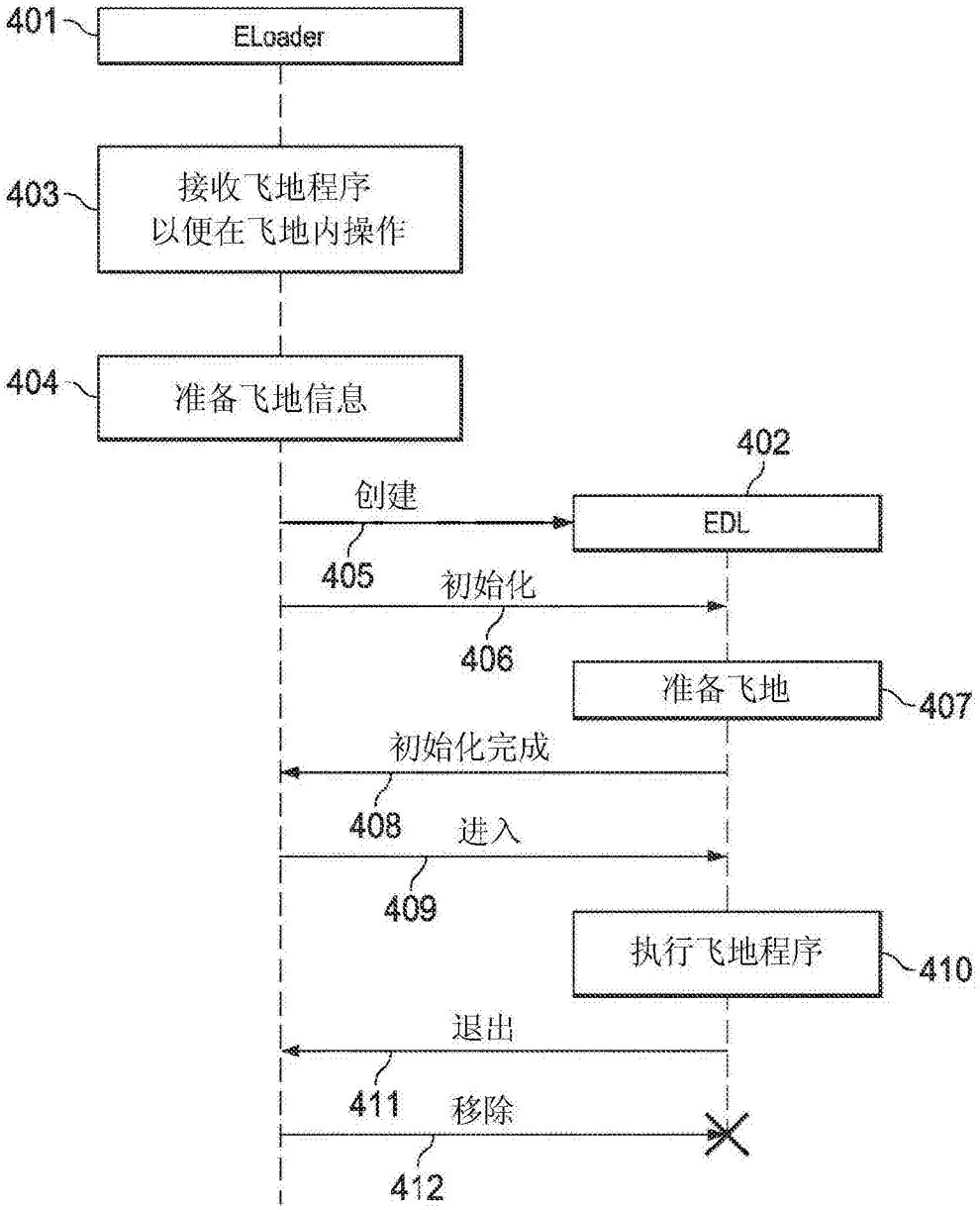

401
ELoader
403
接收飞地程序
以便在飞地内操作
404
准备飞地信息
402
创建
EDL
405
初始化
406
准备飞地
407
初始化完成
408
进入
409
执行飞地程序
410
退出
411
移除
412

图 4A

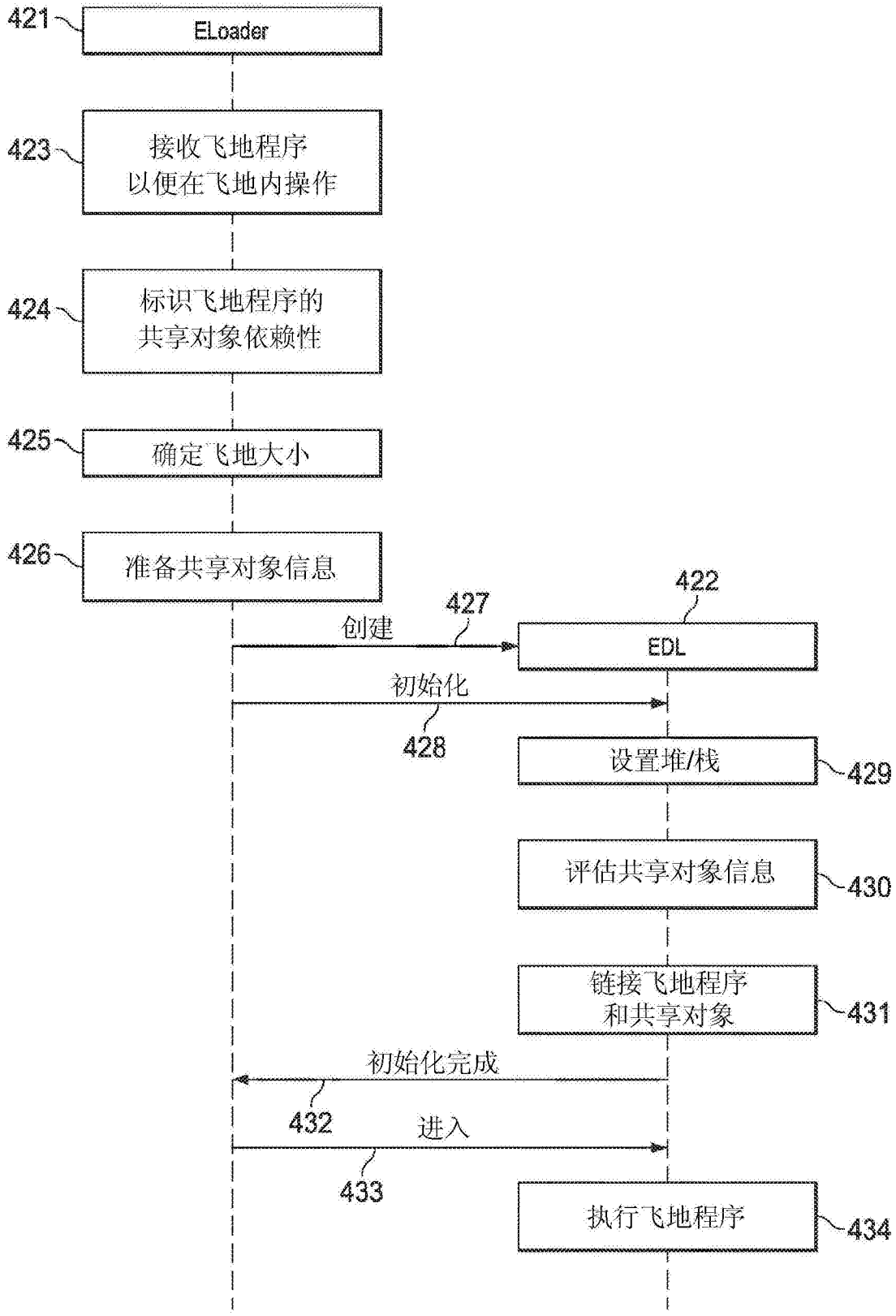

421
ELoader
423
接收飞地程序
以便在飞地内操作
424
标识飞地程序的
共享对象依赖性
425
确定飞地大小
426
准备共享对象信息
422
427
创建
EDL
初始化
428
设置堆/栈
429
评估共享对象信息
430
链接飞地程序
和共享对象
431
初始化完成
432
进入
433
执行飞地程序
434

图 4B

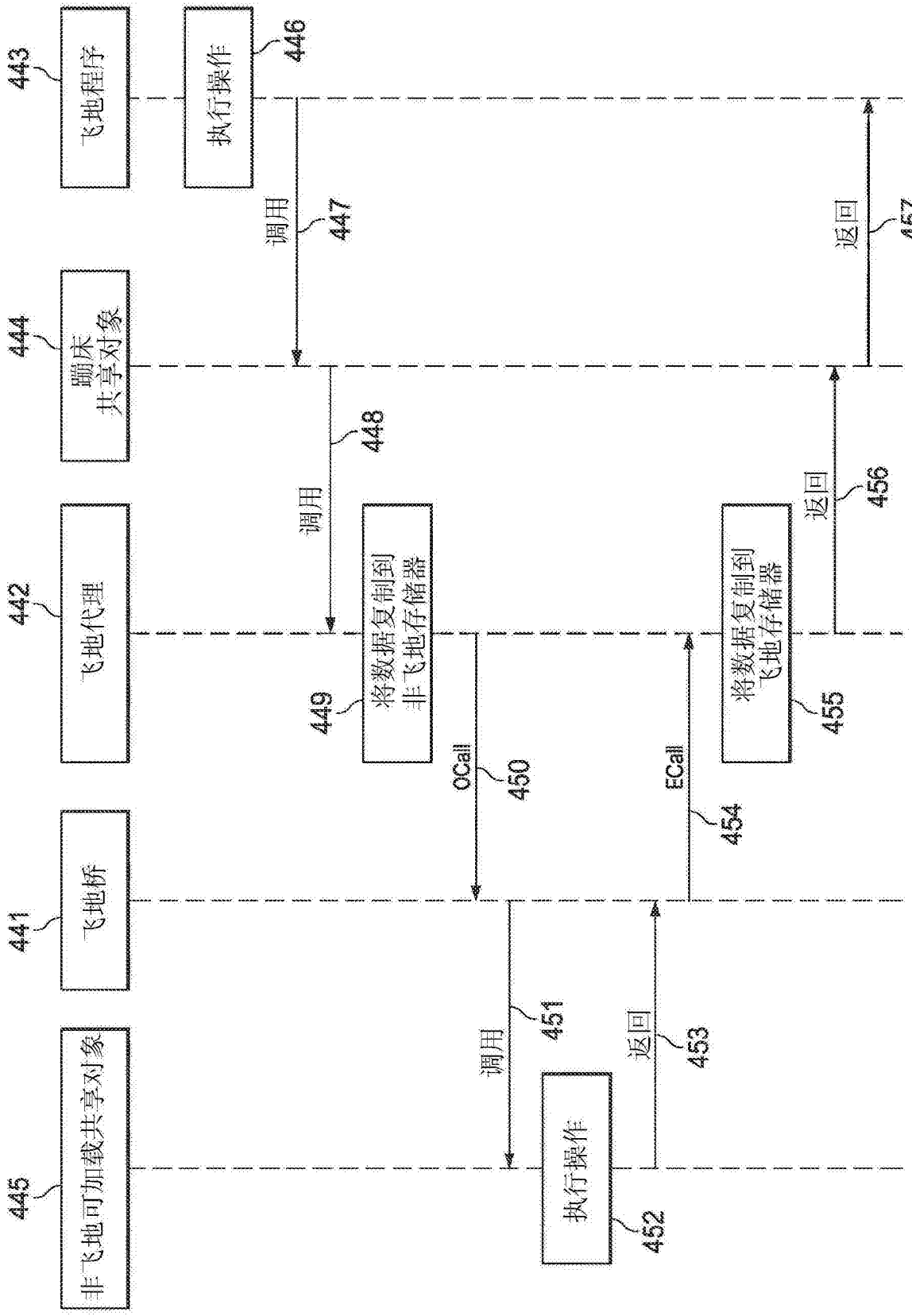

443
飞地程序
446
执行操作
调用
447
返回
457
444
蹦床
共享对象
448
调用
442
飞地代理
449
将数据复制到
非飞地存储器
返回
456
将数据复制到
飞地存储器
455
OCall
450
ECall
454
441
飞地桥
调用
451
返回
453
445
非飞地可加载共享对象
执行操作
452

图 4C

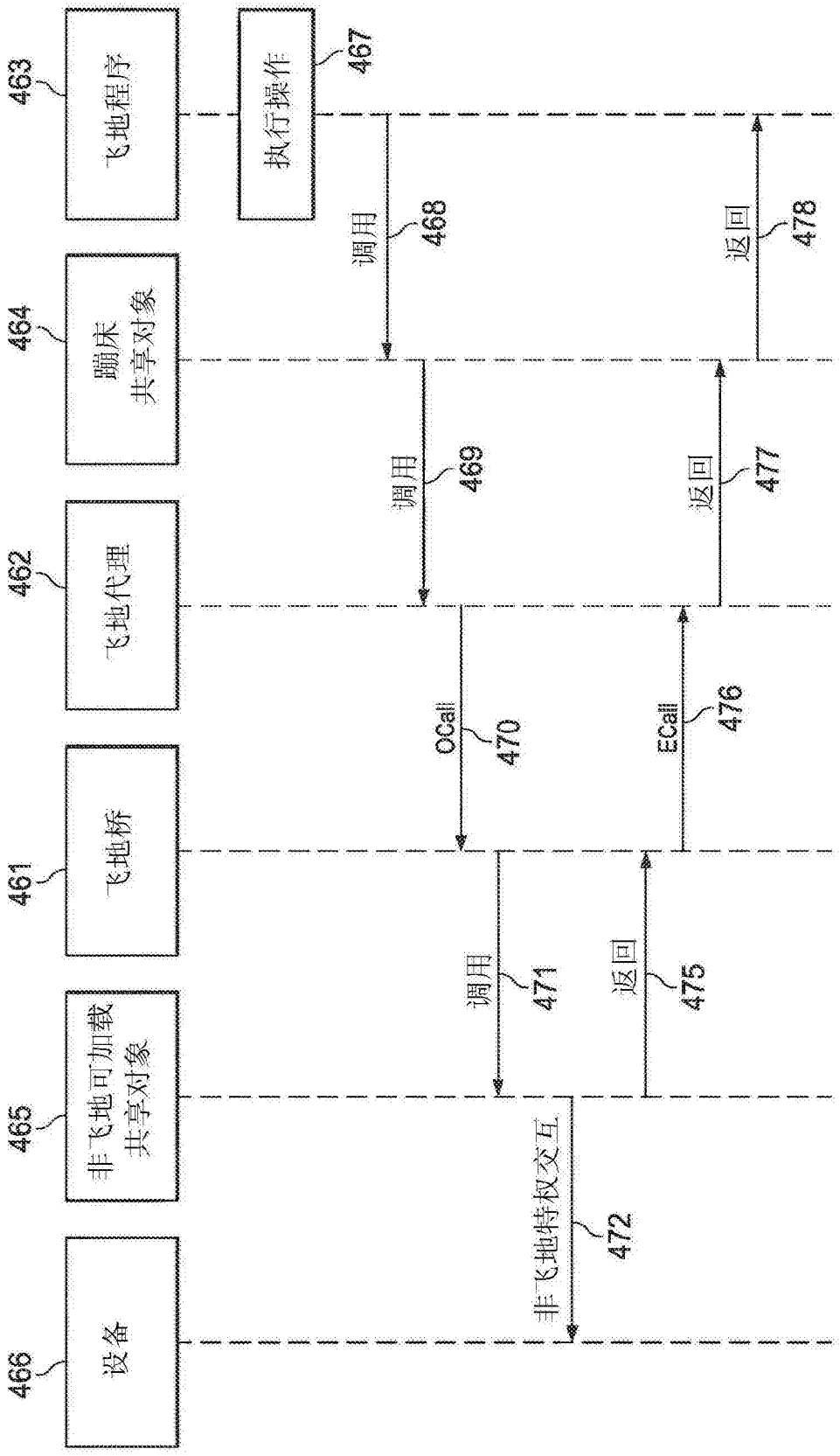

463
飞地程序
执行操作
467
调用
468
返回
478
464
蹦床
共享对象
调用
469
返回
477
462
飞地代理
OCall
470
ECall
476
461
飞地桥
调用
471
返回
475
465
非飞地可加载
共享对象
非飞地特权交互
472
466
设备

图 4D

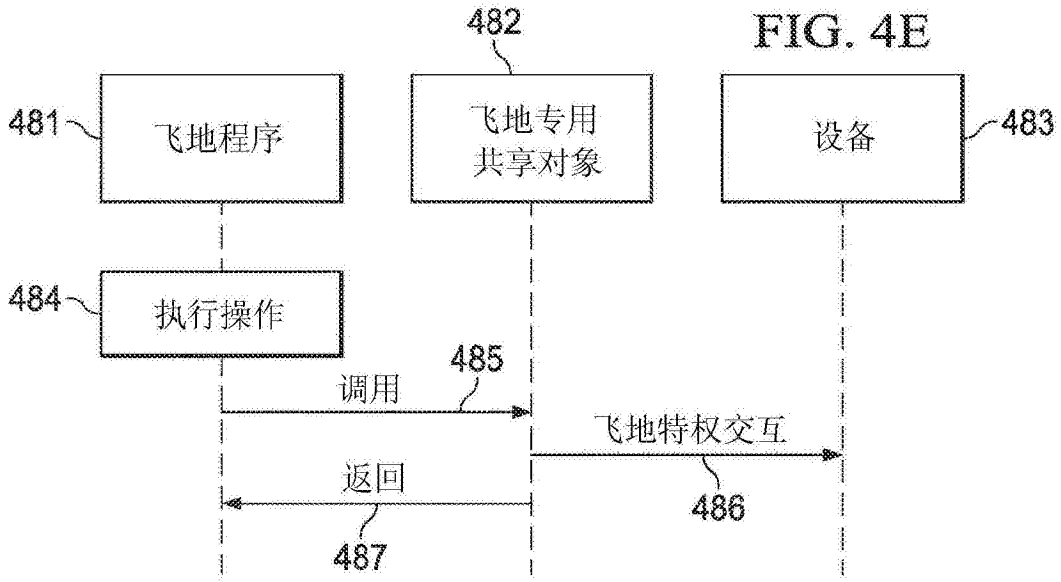


FIG. 4E
482
481
飞地程序
飞地专用
共享对象
设备
483
484
执行操作
485
调用
飞地特权交互
返回
486
487

图 4E

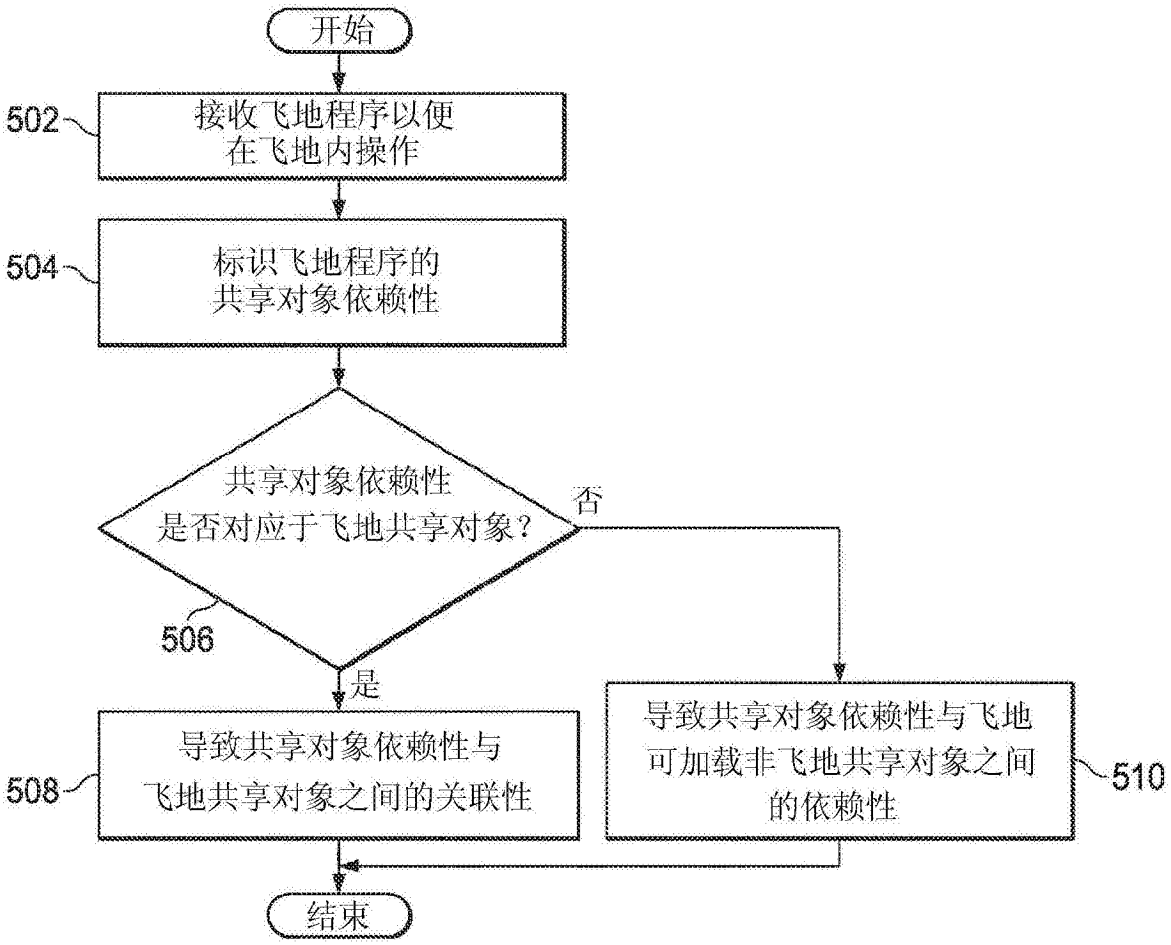

开始
502
接收飞地程序以便
在飞地内操作
504
标识飞地程序的
共享对象依赖性
共享对象依赖性
是否对应于飞地共享对象？
否
506
是
508
导致共享对象依赖性与
飞地共享对象之间的关联性
导致共享对象依赖性与飞地
可加载非飞地共享对象之间
的依赖性
510
结束

图 5

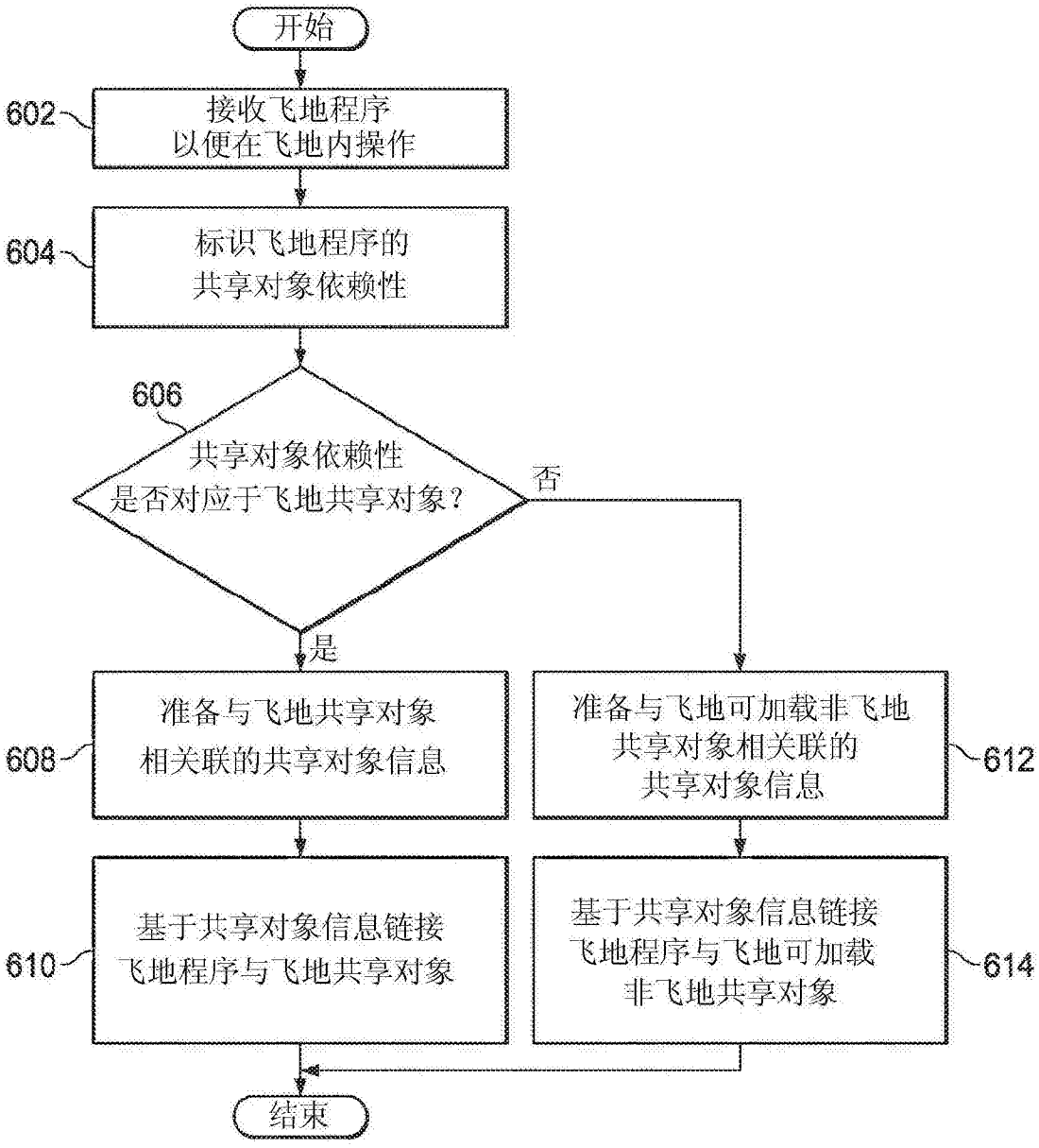

开始
602
接收飞地程序
以便在飞地内操作
604
标识飞地程序的
共享对象依赖性
606
共享对象依赖性
是否对应于飞地共享对象？
否
是
608
准备与飞地共享对象
相关联的共享对象信息
610
基于共享对象信息链接
飞地程序与飞地共享对象
612
准备与飞地可加载非飞地
共享对象相关联的
共享对象信息
614
基于共享对象信息链接
飞地程序与飞地可加载
非飞地共享对象
结束

图 6

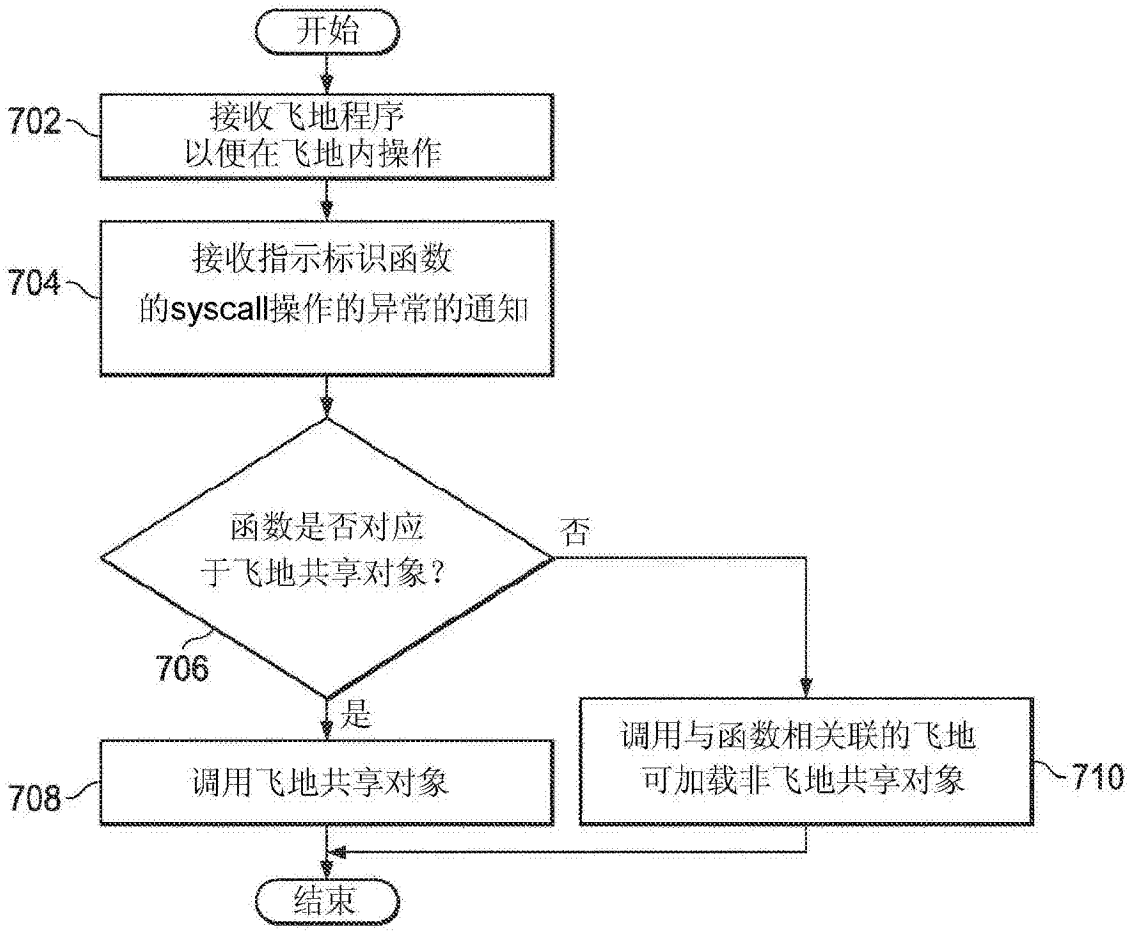

开始
702
接收飞地程序
以便在飞地内操作
704
接收指示标识函数
的syscall操作的异常的通知
函数是否对应
于飞地共享对象？
否
706
是
708
调用飞地共享对象
调用与函数相关联的飞地
可加载非飞地共享对象
710
结束

图 7

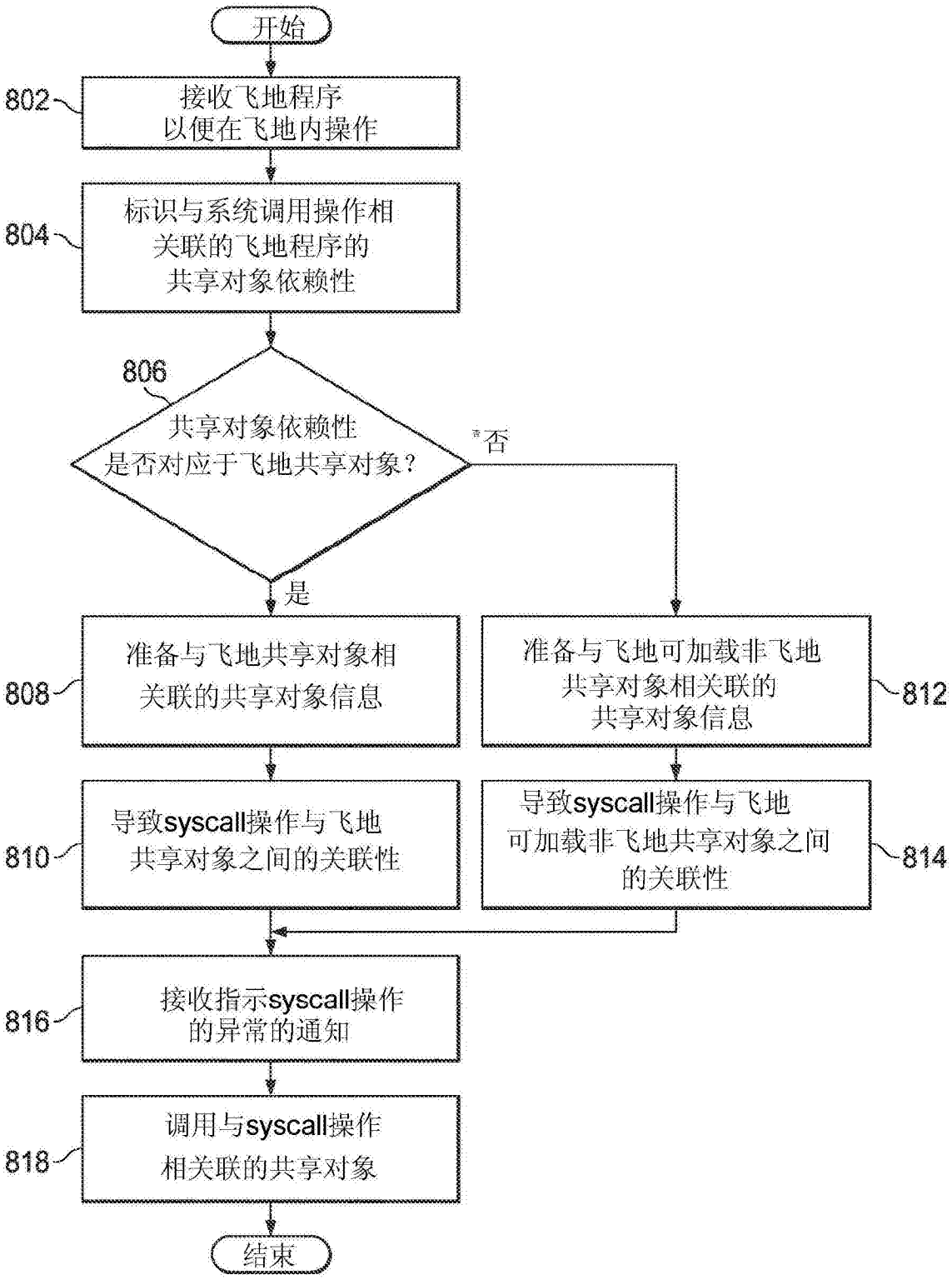

开始
802
接收飞地程序
以便在飞地内操作
804
标识与系统调用操作相
关联的飞地程序的
共享对象依赖性
806
共享对象依赖性
是否对应于飞地共享对象？
否
是
808
准备与飞地共享对象相
关联的共享对象信息
812
准备与飞地可加载非飞地
共享对象相关联的
共享对象信息
810
导致syscall操作与飞地
共享对象之间的关联性
814
导致syscall操作与飞地
可加载非飞地共享对象之间
的关联性
816
接收指示syscall操作
的异常的通知
818
调用与syscall操作
相关联的共享对象
结束

图 8

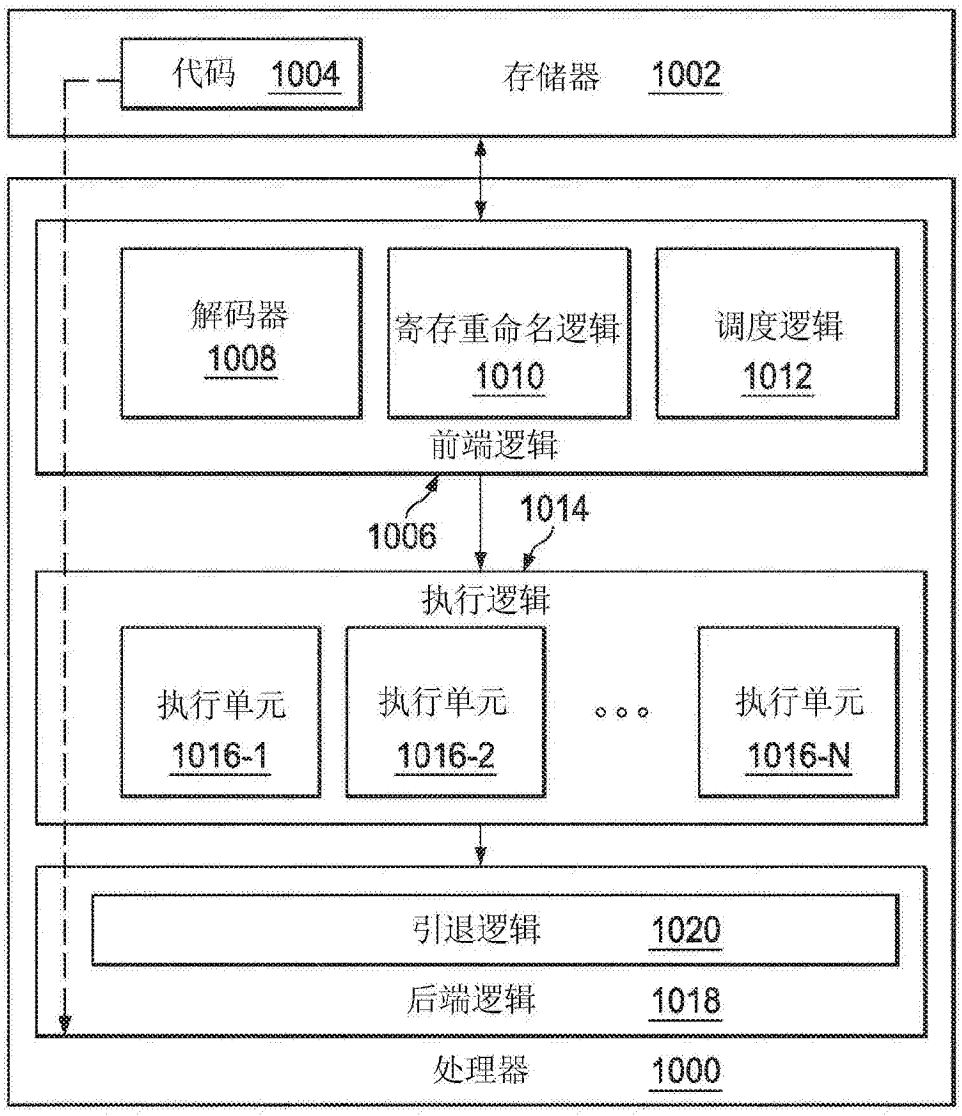

代码 1004
存储器 1002
解码器 1008
寄存重命名逻辑 1010
调度逻辑 1012
前端逻辑
1006
1014
执行逻辑
执行单元 1016-1
执行单元 1016-2
。。。
执行单元 1016-N
引退逻辑 1020
后端逻辑 1018
处理器 1000

图 9

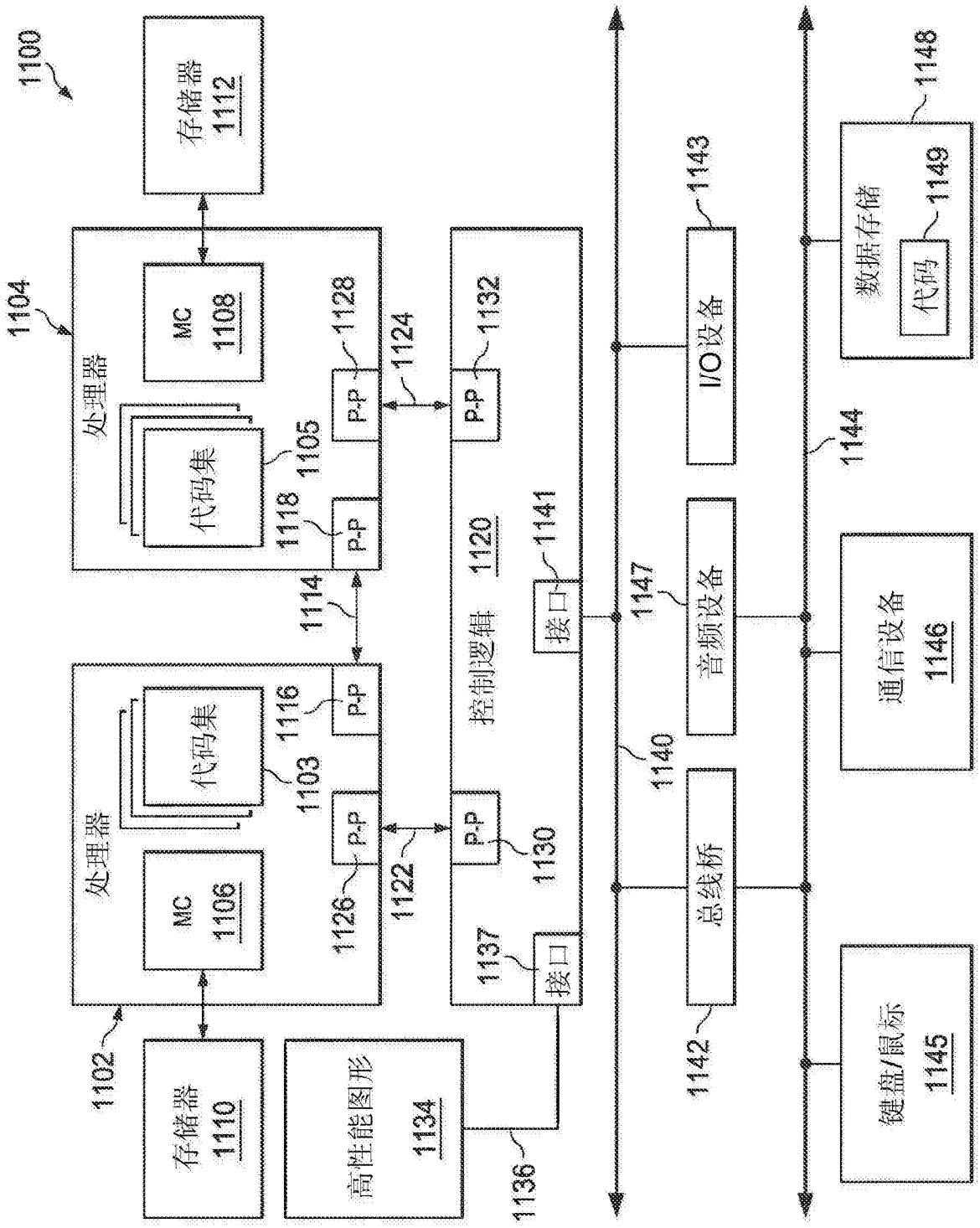

1100
存储器 1112
1104
处理器
MC 1108
代码集
1105
1128
1124
1132
P-P
1118
1120
控制逻辑
1141
接口
1114
1116
1103
1122
1130
1126
1137
1102
存储器 1110
高性能图形 1134
1136
1147
1140
1143
I/O设备
音频设备
总线桥
1142
1144
数据存储
1148
1149
代码
通信设备 1146
键盘/鼠标 1145

图 10