(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 105393258 A
(43)申请公布日 2016.03.09

(21)申请号 201480037591.8

(22)申请日 2014.06.30

(30)优先权数据
61/841,881 2013.07.01 US
14/014,032 2013.08.29 US

(85)PCT国际申请进入国家阶段日
2015.12.30

(86)PCT国际申请的申请数据
PCT/US2014/044776 2014.06.30

(87)PCT国际申请的公布数据
WO2015/002851 EN 2015.01.08

(71)申请人 高通股份有限公司
地址 美国加利福尼亚

(72)发明人 T·曾 A·托兹尼
W·托尔泽乌斯基

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英

(51)Int.Cl.
G06F 21/71(2006.01)
G06F 21/74(2006.01)
G06T 1/20(2006.01)
G06T 1/60(2006.01)

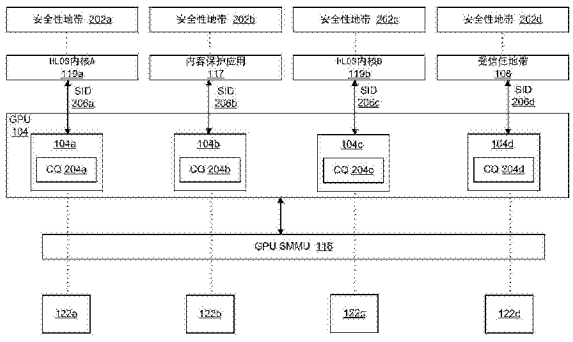
权利要求书4页 说明书7页 附图4页

(54)发明名称

用于提供对图形处理单元的安全访问控制的系统和方法

(57)摘要

公开了用于提供对图形处理单元(GPU)的安全访问控制的系统、方法和计算机程序。一个系统包括GPU、多个GPU编程接口和命令处理器。每个GPU编程接口被动态指派给多个安全性地带中的不同的一个安全性地带。每个GPU编程接口被配置为接收由与对应的安全性地带相关联的一个或多个应用发出的工作命令。所述工作命令包括将要由所述GPU来执行的指令。所述命令处理器与所述多个GPU编程接口相通信。所述命令处理器被配置为使用单独的安全存储器区域来控制对由所述多个GPU编程接口所接收的所述工作命令的执行。每个安全存储器区域被分配给所述多个安全性地带中的一个安全性地带。



CN 105393258 A

1. 一种用于提供对图形处理单元的安全访问控制的方法，所述方法包括：

定义用于控制对图形处理单元的访问的多个安全性地带；

将所述安全性地带中的每个安全性地带指派给由GPU提供的多个GPU编程接口中的对应的一个GPU编程接口，所述GPU编程接口中的每个GPU编程接口用于接收由与对应的安全性地带相关联的一个或多个应用发出的工作命令，所述工作命令包括将要由所述GPU来执行的指令；以及

使用单独的安全存储器区域来控制对由所述多个GPU编程接口所接收的所述工作命令的执行，每个安全存储器区域被分配给所述多个安全性地带中的一个安全性地带。

2. 根据权利要求1所述的方法，其中，所述GPU编程接口包括各自的命令队列，所述命令队列用于存储由对应的GPU编程接口所接收的工作命令。

3. 根据权利要求1所述的方法，其中，所述工作命令是由中央处理单元(CPU)根据所述安全性地带注入到对应的GPU编程接口中的。

4. 根据权利要求3所述的方法，其中，所述工作命令被使用流标识符来注入，所述流标识符标识对应的GPU编程接口。

5. 根据权利要求1所述的方法，其中，单独的存储器区域是由安全存储器管理单元来分配的。

6. 根据权利要求5所述的方法，其中，所述单独的存储器区域中的一个或多个单独的存储器区域包括具有硬件实施的保护的隔离的地址空间，所述硬件实施的保护是在所述安全存储器管理单元中使用相关联的上下文库来进行的。

7. 根据权利要求6所述的方法，其中，所述隔离的地址空间是经由以下各项中的一项或多项来实现的：管理两个或更多个操作系统的超级监督者软件层；以及受信任的硬件与不受信任的硬件之间的分离。

8. 根据权利要求1所述的方法，其中，所述安全性地带中的两个或更多个安全性地带是被并行地管理的。

9. 根据权利要求1所述的方法，其中，所述安全性地带中的一个或多个安全性地带包括不安全的地带或者安全的地带。

10. 根据权利要求1所述的方法，其中，发出所述工作命令的所述一个或多个应用包括以下各项中的一项或多项：内容保护地带应用、与操作系统相关联的内容保护地带内核、高级操作系统内核和受信任地带安全性监控器。

11. 一种用于提供对图形处理单元的安全访问控制的系统，所述方法包括：

用于定义用于控制对图形处理单元(GPU)的访问的多个安全性地带的单元；

用于将所述安全性地带中的每个安全性地带指派给由所述GPU提供的多个GPU编程接口中的对应的一个GPU编程接口的单元，所述GPU编程接口中的每个GPU编程接口用于接收由与对应的安全性地带相关联的一个或多个应用发出的工作命令，所述工作命令包括将要由所述GPU来执行的指令；以及

用于使用单独的安全存储器区域来控制对由所述多个GPU编程接口所接收的所述工作命令的执行的单元，每个安全存储器区域被分配给所述多个安全性地带中的一个安全性地带。

12. 根据权利要求11所述的系统，其中，所述GPU编程接口包括各自的用于存储由对应

的 GPU 编程接口所接收的工作命令的单元。

13. 根据权利要求 11 所述的系统，其中，所述工作命令是由中央处理单元 (CPU) 根据所述安全性地带注入到对应的 GPU 编程接口中的。

14. 根据权利要求 13 所述的系统，其中，所述工作命令被使用流标识符来注入，所述流标识符标识对应的 GPU 编程接口。

15. 根据权利要求 11 所述的系统，其中，单独的存储器区域是由安全存储器管理单元来分配的。

16. 根据权利要求 15 所述的系统，其中，所述单独的存储器区域中的一个或多个单独的存储器区域包括具有硬件实施的保护的隔离的地址空间，所述硬件实施的保护是在所述安全存储器管理单元中使用相关联的上下文库来进行的。

17. 根据权利要求 16 所述的系统，其中，所述隔离的地址空间是经由以下各项中的一项或多项来实现的：管理两个或更多个操作系统的超级监督者软件层；以及受信任的硬件与不受信任的硬件之间的分离。

18. 根据权利要求 11 所述的系统，其中，所述安全性地带中的两个或更多个安全性地带是被并行地管理的。

19. 根据权利要求 11 所述的系统，其中，所述安全性地带中的一个或多个安全性地带包括不安全的地带或者安全的地带。

20. 根据权利要求 11 所述的系统，其中，发出所述工作命令的所述一个或多个应用包括以下各项中的一项或多项：内容保护地带应用、与操作系统相关联的内容保护地带内核、高级操作系统内核和受信任地带安全性监控器。

21. 一种用于提供对图形处理单元的安全访问控制的计算机程序，所述计算机程序被包含在计算机可读介质中用于由处理器来执行，所述计算机程序包括被配置为进行以下操作的逻辑单元：

定义用于控制对图形处理单元 (GPU) 的访问的多个安全性地带；

将所述安全性地带中的每个安全性地带指派给由所述 GPU 提供的多个 GPU 编程接口中的对应的一个 GPU 编程接口，所述 GPU 编程接口中的每个 GPU 编程接口用于接收由与对应的安全性地带相关联的一个或多个应用发出的工作命令，所述工作命令包括将要由所述 GPU 来执行的指令；以及

使用单独的安全存储器区域来控制对由所述多个 GPU 编程接口所接收的所述工作命令的执行，每个安全存储器区域被分配给所述多个安全性地带中的一个安全性地带。

22. 根据权利要求 21 所述的计算机程序，其中，所述 GPU 编程接口包括各自的命令队列，所述命令队列用于存储由对应的 GPU 编程接口所接收的工作命令。

23. 根据权利要求 21 所述的计算机程序，其中，所述工作命令是由中央处理单元 (CPU) 根据所述安全性地带注入到对应的 GPU 编程接口中的。

24. 根据权利要求 23 所述的计算机程序，其中，所述工作命令被使用流标识符来注入，所述流标识符标识对应的 GPU 编程接口。

25. 根据权利要求 21 所述的计算机程序，其中，单独的存储器区域是由安全存储器管理单元来分配的。

26. 根据权利要求 25 所述的计算机程序，其中，所述单独的存储器区域中的一个或多

个单独的存储器区域包括具有硬件实施的保护的隔离的地址空间，所述硬件实施的保护是在所述安全存储器管理单元中使用相关联的上下文库来进行的。

27. 根据权利要求 26 所述的计算机程序，其中，所述隔离的地址空间是经由以下各项中的一项或多项来实现的：管理两个或更多个操作系统的超级监督者软件层；以及受信任的硬件与不受信任的硬件之间的分离。

28. 根据权利要求 21 所述的计算机程序，其中，所述安全性地带中的两个或更多个安全性地带是被并行地管理的。

29. 根据权利要求 21 所述的计算机程序，其中，所述安全性地带中的一个或多个安全性地带包括不安全的地带或者安全的地带。

30. 根据权利要求 21 所述的计算机程序，其中，发出所述工作命令的所述一个或多个应用包括以下各项中的一项或多项：内容保护地带应用、与操作系统相关联的内容保护地带内核、高级操作系统内核和受信任地带安全性监控器。

31. 一种用于提供对图形处理单元的安全访问控制的系统，所述系统包括：

图形处理单元 (GPU)；

多个 GPU 编程接口，其由所述 GPU 来提供，每个 GPU 编程接口被动态指派给多个安全性地带中的不同的一个安全性地带，并且被配置为接收由与对应的安全性地带相关联的一个或多个应用发出的工作命令，所述工作命令包括将由所述 GPU 来执行的指令；以及

命令处理器，其与所述多个 GPU 编程接口相通信，所述命令处理器被配置为使用单独的安全存储器区域来控制对由所述多个 GPU 编程接口所接收的所述工作命令的执行，每个安全存储器区域被分配给所述多个安全性地带中的一个安全性地带。

32. 根据权利要求 31 所述的系统，其中，所述 GPU 编程接口包括各自的命令队列，所述命令队列用于存储由对应 GPU 编程接口所接收的工作命令。

33. 根据权利要求 31 所述的系统，其中，所述工作命令是由中央处理单元 (CPU) 根据所述安全性地带注入到对应的 GPU 编程接口中的。

34. 根据权利要求 33 所述的系统，其中，所述工作命令被使用流标识符来注入，所述流标识符标识对应的 GPU 编程接口。

35. 根据权利要求 31 所述的系统，其中，单独的存储器区域是由安全存储器管理单元来分配的。

36. 根据权利要求 35 所述的系统，其中，所述单独的存储器区域中的一个或多个单独的存储器区域包括具有硬件实施的保护的隔离的地址空间，所述硬件实施的保护是在所述安全存储器管理单元中使用相关联的上下文库来进行的。

37. 根据权利要求 36 所述的系统，其中，所述隔离的地址空间是经由以下各项中的一项或多项来实现的：管理两个或更多个操作系统的超级监督者软件层；以及受信任的硬件与不受信任的硬件之间的分离。

38. 根据权利要求 31 所述的系统，其中，所述安全性地带中的两个或更多个安全性地带是被并行地管理的。

39. 根据权利要求 31 所述的系统，其中，所述安全性地带中的一个或多个安全性地带包括不安全的地带或者安全的地带。

40. 根据权利要求 31 所述的系统，其中，发出所述工作命令的所述一个或多个应用包

括以下各项中的一项或多项：内容保护地带应用、与操作系统相关联的内容保护地带内核、高级操作系统内核和受信任地带安全性监控器。

用于提供对图形处理单元的安全访问控制的系统和方法

[0001] 优先权与相关申请声明

[0002] 本申请基于 35U.S.C.119(e) 要求于 2013 年 7 月 1 日递交的、被指派了临时申请序列号 61/841,881、并且名称为“System and Method for Providing Secure Access Control to a Graphics Processing Unit”的美国临时专利申请的优先权，以引用方式将该临时申请的全部内容并入本文。

背景技术

[0003] 诸如移动电话之类的便携式计算设备 (“PCD”) 正在变得更加复杂。现有 PCD 时常具有多个处理器 (例如，中央处理单元 (CPU)、图形处理单元 (GPU)、数字信号处理器 (DSP) 等) 以执行不同的功能并且满足针对这样的设备的增长的需求。现有的 PCD 还可以支持内容保护架构，所述内容保护架构通常支持针对例如以下使用案例的访问控制需求 ：数字版权管理 (DRM)、控制对用于包括银行、病历、指纹等的应用的保密数据的访问。内容保护架构通常将存储器区域分离为不同的安全性地带，以用于控制通过应用对敏感内容进行的访问。然而，现有的 PCD 和内容保护架构被限制为 CPU 级的访问控制。

[0004] 因此，本领域中存在对用于提供对 GPU 的安全访问控制的改进的机制的需求。

发明内容

[0005] 公开了用于提供对图形处理单元 (GPU) 的安全访问控制的系统、方法和计算机程序。一种方法包括 ：定义用于控制对图形处理单元 (GPU) 的访问的多个安全性地带 ；将所述安全性地带中的每个安全性地带指派给由所述 GPU 提供的多个 GPU 编程接口中的对应的一个 GPU 编程接口，所述 GPU 编程接口中的每个 GPU 编程接口用于接收由与对应的安全性地带相关联的一个或多个应用发出的工作命令，所述工作命令包括将要由所述 GPU 来执行的指令 ；以及使用单独的安全存储器区域来控制对由所述多个 GPU 编程接口所接收的所述工作命令的执行，每个安全存储器区域被分配给所述多个安全性地带中的一个安全性地带。

[0006] 另一个实施例是用于提供对图形处理单元的安全访问控制的计算机程序。所述计算机程序被包含在计算机可读介质中，以用于由处理器来执行。所述计算机程序包括被配置为进行以下操作的逻辑单元 ：定义用于控制对图形处理单元 (GPU) 的访问的多个安全性地带 ；将所述安全性地带中的每个安全性地带指派给由所述 GPU 提供的多个 GPU 编程接口中的对应的一个 GPU 编程接口，所述 GPU 编程接口中的每个 GPU 编程接口用于接收由与对应的安全性地带相关联的一个或多个应用发出的工作命令，所述工作命令包括将要由所述 GPU 来执行的指令 ；以及使用单独的安全存储器区域来控制对由所述多个 GPU 编程接口所接收的所述工作命令的执行，每个安全存储器区域被分配给所述多个安全性地带中的一个安全性地带。

[0007] 另一个实施例是用于提供对图形处理单元 (GPU) 的安全访问控制的系统。所述系统包括具有多个 GPU 编程接口的 GPU 和命令处理器。每个 GPU 编程接口被动态指派给多个安全性地带中的不同的一个安全性地带，并且被配置为接收由与对应的安全性地带相关联

的一个或多个应用发出的工作命令。所述工作命令包括将要由所述 GPU 来执行的指令。所述命令处理器与所述多个 GPU 编程接口相通信，并且被配置为使用单独的安全存储器区域来控制对由所述多个 GPU 编程接口所接收的所述工作命令的执行。将每个安全存储器区域分配给所述多个安全性地带中的一个安全性地带。

附图说明

[0008] 在附图中，除非另外指出，否则相似的附图标记贯穿各种视图指代相似的部分。对于诸如“102A”或者“102B”之类的带有字母字符名称的附图标记，字母字符名称可以区分出现在同一幅图中的两个相似的部分或者元件。当旨在使附图标记包含全部图中的具有相同附图标记的全部部分时，可以省略针对附图标记的字母字符名称。

[0009] 图 1 是示出了用于提供对图形处理单元 (GPU) 的安全访问控制的系统的实施例的框图。

[0010] 图 2 是示出了图 1 的系统的实施例的框图，所述图 1 中的系统配置有四个安全性地带以及对应的 GPU 编程接口和分配的存储器区域。

[0011] 图 3 是示出了在图 1 中的系统中实现的方法的实施例的流程图，所述在图 1 的系统中实现的方法用于提供对 GPU 的安全访问控制。

[0012] 图 4 是示出了用于并入图 1 中的系统的示例性的便携式计算设备的框图。

具体实施方式

[0013] 本文使用词语“示例性的”来表示“用作示例、实例或者图示”。任何在本文中被描述为“示例性的”方面不必然将要被理解为比其它的方面优选或者有利。

[0014] 在本说明书中，术语“应用”还可以包括具有可执行内容的文件，例如：目标代码、脚本、字节码、标记语言文件和补丁。另外，本文提到的“应用”还可以包括本质上不可执行的文件，例如，可能需要被打开的文档或者需要被存取的其它数据文件。

[0015] 术语“内容”也可以包括具有可执行内容的文件，例如：目标代码、脚本、字节码、标记语言文件和补丁。另外，本文提到的“内容”还可以包括本质上不可执行的文件，例如，可能需要被打开的文档或者需要被存取的其它数据文件。

[0016] 当用在本说明书中时，术语“部件”、“数据库”、“模块”、“系统”等旨在指与计算机相关的实体，要么是硬件、固件、硬件和软件的组合、软件，要么是执行中的软件。例如，部件可以是但是不限于是运行在处理器上的过程、处理器、对象、可执行文件、执行线程、程序和 / 或计算机。作为图示，运行在计算设备上的应用或者模块和所述计算设备两者都可以是部件。一个或多个部件可以存在于过程和 / 或执行线程内，并且，部件可以被本地化在一台计算机上和 / 或分布在两台或多台计算机当中。另外，可以从其上存储有各种数据结构的各种计算机可读介质来执行这些部件。部件可以例如根据具有一个或多个数据分组（例如，来自一个部件的数据，所述一个部件通过信号的方式与本地系统、分布式系统中的另一个部件进行交互，和 / 或跨诸如互联网之类的网络与其它系统进行交互）的信号经由本地和 / 或远程过程来进行通信。

[0017] “便携式计算设备”（“PCD”）例如可以包括蜂窝电话、卫星电话、寻呼机、个人数字助理、智能电话、导航设备、智能本或者电子阅读器、媒体播放器、平板型计算机、膝上型计

算机或者其它这样的设备。

[0018] 图 1 是可以被并入到例如用于提供对图形处理单元 (GPU)102 的安全访问控制的 PCD(图 4) 中的系统 100。系统 100 包括一个或多个中央处理单元 (CPU)402 以及一个或多个 GPU 102,所述 GPU 102 用于执行与一个或多个应用 118 和 / 或一个或多个操作系统 120 相关联的图形和 / 或计算指令。CPU 402 和 GPU 102 可以通过硬件总线、连接或者其它接口连接起来。系统 100 为 GPU 访问控制提供多个安全性和 / 或内容保护地带 (“安全性地带”)。

[0019] GPU 硬件和 / 或软件向 CPU 402 提供多个 GPU 编程接口 104。GPU 编程接口 104 中的每个 GPU 编程接口与不同的安全性地带相关联,以用于接收由存在于不同安全性地带中的一个或多个应用 118 和操作系统 120 发出的工作命令。安全性地带可以由安全性策略管理器 106 基于任何可取的安全性使用案例来定义。每个安全性地带被指派给单独的 GPU 编程接口 104,并且被分配给单独的存储器区域。在图 1 的实施例中,系统 100 包括四个 GPU 编程接口 104a、104b、104c 和 104d,它们具有对应的安全存储器区域。上下文库 122a、122b、122c 和 122d 可以被分配作为用于执行对应的安全性地带中的工作命令的存储器资源。就这一点而言,安全存储器区域可以包括具有硬件实施的保护的隔离的地址空间,所述硬件实施的保护是在系统存储器管理单元 (SMMU)116 中使用上下文库 122a、122b、122c 和 122d 来进行的。每个上下文库 122 可以包括用于实施特定的安全的和隔离的地址空间的硬件资源。

[0020] 工作命令包括将要由 GPU 102 来执行的图形指令。应当领会的是,应用 118 可以包括从 GPU 102 请求资源的任何合适的应用。操作系统 120 可以包括一个或多个操作系统,例如,高级操作系统 (HLOS)。在一个实施例中,GPU 102 可以从被特别配置的内容保护应用 (例如,内容保护应用 117 或者与操作系统 120 相关联的内容保护内核 119) 接收工作命令。

[0021] 本领域的技术人员将领会,GPU 编程接口 104 包括控制资源。在一个实施例中,控制资源可以包括寄存器资源,以用于接受来自对应的安全性地带中的应用的工作命令,以及一个或多个中断资源,以指示工作命令执行的完成或者失败状态。可以基于例如虚拟机的大小以及安全性策略管理器 106 或者受信任地带部件 108(即,系统 100 中的“信任的根”) 是否需要对 GPU 402 的访问,来由虚拟机管理器 (VMM)110 配置 GPU 编程接口 104。系统 100 中的“信任的根”基于安全性策略管理器 106 的系统安全性策略来动态地将 GPU 编程接口 104 指派给所指定的安全性地带,这可以在安全性使用案例的启动时刻发生。

[0022] 如上文所提到的,每个 GPU 编程接口 104 可以是取决于特定使用场景被映射到对应的上下文库 122 的存储器,在该情况下,它们可以包括存储器映射的输入 / 输出 (MIMO) 寄存器。GPU 编程接口 104 可以直接地可被指派给一个或多个虚拟机或者 VMM 110。应当进一步认识到,可以由硬件实施的访问控制使用系统存储器管理单元 (SMMU)116 来保护每个 GPU 编程接口 104。以这种方式,在特定的使用案例已经启动之后,每个安全性地带对与 GPU 编程接口 104 相关联的寄存器和中断资源可以具有完全的控制。

[0023] 如图 1 中进一步示出的,GPU 102 可以包括与多个 GPU 编程接口 104 相通信的命令处理器 114。命令处理器 114 可以被配置为从与 GPU 编程接口 104 相关联的内容队列 204(图 2) 中选择工作命令。就这一点而言,命令处理器 114 可以基于例如 GPU 调度策略来

确定处理哪些工作命令，并且然后使用被分配给安全性地带的合适的上下文库来控制对所述工作命令的执行。

[0024] 应当认识到，在一个实施例中，可以由并发地运行在 CPU 402 上的应用 118 并行地管理多个安全性地带。每个应用 118 可以直接地管理相关联的命令队列。安全性地带中的一个或多个安全性地带还可以是安全的和 / 或不安全的。应用 118（以及其相关联的存储器）是安全的和 / 或不安全的所基于的安全性策略可以由控制 GPU 102 的处理器（例如，CPU 408）来确定。应当进一步领会到，由 CPU 402 来执行和 / 或管理的分段可以通过包括例如以下示例性方式的各种方式来实现：(1) 与超级监督者 (hypervisor) 层（例如，管理多个访客操作系统 120 的软件层）的隔离；和 / 或 (2) 定义了硬件安全域（例如，ARM 架构中所使用的“信任地带”安全性扩展）的硬件过程构造，其可以经由对指令的额外的硬件标记来控制受信任的和不受信任的硬件之间的分离，以跟踪存储器访问和 GPU 命令，以及隔离请求的来源。超级监督者层可以包括硬件上的软件抽象，所述硬件上的软件抽象可以被限制为控制单元的存储器访问隔离。

[0025] 系统 101 可以支持任何可取的、与 GPU 访问控制相关的安全性使用案例。例如，系统 101 可以支持诸如（举几个例子来说）数字版权管理 (DRM) 和控制对用于包括银行、病历、指纹等的应用的保密数据的访问之类的使用案例。在一个实施例中，系统 101 可以提供与各自的安全性地带相关联的四个异常级别，其中每个级别具有不同的或者经排序的安全性特权。第一异常级别 (EL0) 可以不严格地对应于用户模式。第二异常级别 (EL1) 可以对应于内核模式。第三异常级别 (EL2) 可以对应于超级监督者。第四异常级别 (EL3) 可以对应于包括享有最大特权的安全性地带的受信任地带部件 108。

[0026] 图 2 示出了涉及四个安全性地带 202a、202b、202c 和 202d 的示例性的使用案例。安全性地带 202a 被指派给 GPU 编程接口 104a，所述 GPU 编程接口 104a 被配置用于第一 HLOS 内核 119a，并且具有内容队列 204a。内容库 122a 被分配给安全性地带 202a。安全性地带 202b 被指派给 GPU 编程接口 104b，所述 GPU 编程接口 104b 被配置用于内容保护应用 117，并且具有内容队列 204b。上下文库 122b 被分配给安全性地带 202b。安全性地带 202c 被指派给 GPU 编程接口 104c，所述 GPU 编程接口 104c 被配置用于第二 HLOS 内核 119b，并且具有内容队列 204c。上下文库 122c 被分配给安全性地带 202c。安全性地带 202d 被指派给 GPU 编程接口 104c，所述 GPU 编程接口 104c 与受信任地带部件 108 相关联，并且具有内容队列 204d。受信任地带部件 108 拥有受信任的上下文库 122d，所述受信任的上下文库 122d 包括仅对受信任地带部件 108 可见的隔离的地址空间。

[0027] 应当领会的是，安全性地带 202 可以支持具有合适的应用 118 的任何可取的使用案例。例如，在一个实施例中，安全性地带 202a 可以与游戏应用和相关联的虚拟存储器空间相关联。安全性地带 202b 可以与视频应用和相关联的优质的视频虚拟存储器空间相关联。安全性地带 202c 可以与浏览器应用和相关联的虚拟存储器空间相关联。安全性地带 202d 可以与银行应用和相关联的虚拟存储器空间相关联。

[0028] 如图 2 中进一步示出的，每个 GPU 编程接口 104a、104b、104c 和 104d 可以通过单独的数据流标识符（分别为 SID 206a、SID 206b、SID 206c 和 SID 206d）来标识。应当领会的是，流标识符可以被 CPU 402 用于例如将工作命令注入到合适的 GPU 编程接口。命令处理器 114 可以根据流标识符来选择工作命令，并且 SMMU 116 可以根据流标识符来管理存

储器资源。

[0029] 图 3 示出了用于在系统 100 中提供 GPU 访问控制的方法 300 的实施例。在框 301 处，针对将要由 GPU 104 执行的指令定义多个安全性地带 202。可以由安全性策略管理器 106、受信任地带部件 108 或者与系统 101 相关联的其它软件和 / 或硬件来定义安全性地带 202。在一个实施例中，可以并行地管理安全性地带 202 中的两个或更多个安全性地带。此外，应当领会的是，在一些实施例中，可以实现安全的地带和不安全的地带两者。在框 303 处，每个安全性地带 202 被指派给单独的 GPU 编程接口，并且被分配给单独的存储器区域（例如，上下文库 122a、122b、122c 和 122d）。如上文提到的，可以由 VMM 110 基于例如虚拟机的大小以及安全性策略管理器 106 或者受信任地带部件 108 是否需要对 GPU 104 的访问，来配置 GPU 编程接口 104。在一个实施例中，系统 100 中的“信任的根”基于安全性策略管理器 106 的系统安全性策略来动态地将 GPU 编程接口 104 指派给所指定的安全性地带，这可以在安全性使用案例启动时刻发生。在框 305 处，存在于安全性地带 202 中的一个安全性地带中的应用 118 可以向合适的 GPU 编程接口 104 发出工作命令。CPU 402 可以使用流标识符 206 来注入工作命令。在框 307 处，可以基于对应的安全性地带 202 向合适的 GPU 编程接口 105 提供工作命令。在框 309 处，命令处理器 114 和 / 或 SMMU 116 可以使用分配给对应的安全性地带 202 和 GPU 编程接口 104 的单独的存储器区域（例如，上下文库 122a、122b、122c 和 122d）来控制对工作命令的执行。

[0030] 本领域的技术人员将领会的是，可以实现替代的使用案例。将描述涉及受信任地带部件 108 的示例性的“受信任地带”使用案例，以进一步示出 GPU 访问控制功能的特定方面。受信任地带部件 108 可以声明对受信任的上下文库 122d（图 2）的所有权。可以配置与 SMMU 上下文库相关联的页表。所述页表可以是利用由受信任地带（即，安全性地带 202d）拥有的缓冲器来填充的，并且所述缓冲器对任何其它部件（除了与另一个安全性地带 202a、202b 或者 202c 共享的缓冲器之外）而言是不可见的。安全性策略可以指定受信任地带部件 108 声明对 GPU 编程接口 104d 的所有权。SID 206d 可以被配置为映射到受信任的上下文库 122d 的安全的 SID。在操作中，受信任地带部件 108 通过向命令队列 204d 中注入请求来发出 GPU 工作命令。

[0031] 当工作命令被注入到命令队列 204 中时，可以（例如，通过“门铃”寄存器）提示命令处理器 114 开始处理。命令处理器 114 扫描 GPU 编程接口 104d 以选择对哪个 GPU 编程接口进行工作。当根据 GPU 编程接口 104d 设置了 SID 206d 时，可以处理工作命令。SID 206d 选择建立了合适的存储器保护的特定上下文库。当成功地完成了工作时或者在错误的情况下，命令处理器 144 使 CPU 402 中断，和 / 或受信任地带部件 108 接收该中断。在完成工作命令之后，受信任地带部件 108 可以发出进一步的工作命令。如果中断指示错误，则受信任地带部件 108 可以停止进一步的处理，并且根据错误处理策略来处理错误。

[0032] 图 4 示出了被并入到示例性的便携式计算设备 (PCD) 400 中的、上文所描述的系统 100。应当领会的是，系统 100 中的一些部件被包括在 SoC 322 中，而其它的部件可以位于芯片之外。SoC 322 可以包括任何可以被单独地制造并且并入到便携式计算设备 400 的设计中的嵌入式系统。

[0033] 如所示出的，PCD 400 包括 SoC 322，所述 SoC 322 包括多核 CPU 402A。多核 CPU 402A 可以包括第零核 410、第一核 412 和第 N 核 414。显示控制器 328 和触摸屏控制器 330

可以耦合到GPU 104，所述GPU 104可以存在于CPU 402上或者连接到CPU 402。继而，在SoC 322外部的触摸屏显示器108可以耦合到显示控制器328和触摸屏控制器330。

[0034] 图4进一步示出了视频编码器334（例如，逐行倒相(PAL)编码器、按顺序传送彩色与存储(SECAM)编码器或者国家电视系统委员会(NTSC)编码器）耦合到多核CPU 402A。进一步，视频放大器336耦合到视频编码器334和触摸屏显示器108。此外，视频端口338耦合到视频放大器336。如图4中所示，通用串行总线(USB)控制器340和其它跟踪宿109和跟踪转储110可以耦合到多核CPU 402A。此外，USB端口342耦合到USB控制器340。存储器404A和用户身份模块(SIM)卡346也可以耦合到多核CPU 402A。

[0035] 进一步，如图4中所示，数字照相机348可以耦合到多核CPU 402A。在示例性的方面中，数字照相机348是电荷耦合设备(CCD)照相机或者互补金属氧化物半导体(CMOS)照相机。

[0036] 如图4中进一步示出的，立体声音频编码解码器(CODEC)350可以耦合到多核CPU 402A。此外，音频放大器352可以耦合到立体声音频CODEC 350。在示例性的方面中，第一立体声扬声器354和第二立体声扬声器356耦合到音频放大器352。图4示出了麦克风放大器358也可以耦合到立体声音频CODEC 350。此外，麦克风360可以耦合到麦克风放大器358。在特定的方面中，频率调制(FM)无线电调谐器362可以耦合到立体声音频CODEC 350。此外，FM天线364耦合到FM无线电调谐器362。进一步，立体声耳机366可以耦合到立体声音频CODEC 350。

[0037] 图4进一步示出了，射频(RF)收发机368可以耦合到多核CPU 402A。RF开关370可以耦合到RF收发机368和RF天线372。如图4中所示，键区204可以耦合到多核CPU 402A。此外，具有麦克风的单声道耳机376可以耦合到多核CPU 402A。进一步，振动器设备378可以耦合到多核CPU 402A。

[0038] 图4还示出了电源380，其可以耦合到SoC 322。在特定的方面中，电源380是向PCD 400的需要功率的各种部件提供功率的直流(DC)电源。进一步，在特定的方面中，电源是可再充电的DC电池或者从连接到AC功率源的交流(AC)到DC变压器得到的DC电源。

[0039] 图4进一步指示PCD 400，其还可以包括网卡388，网卡388可以被用于访问数据网络（例如，局域网、个域网或者任何其它网络）。网卡388可以是蓝牙网卡、WiFi网卡、个域网(PAN)卡、个域网超低功率技术(PeANUT)网卡或者本领域中公知的任何其它网卡。进一步，可以将网卡388并入芯片中，即，网卡388可以是芯片中的完全解决方案，并且可以不是单独的网卡388。

[0040] 如图4中所描绘的，触摸屏显示器108、视频端口338、USB端口342、照相机348、第一立体声扬声器354、第二立体声扬声器356、麦克风360、FM天线364、立体声耳机366、RF开关370、RF天线372、键区374、单声道耳机376、振动器378和电源380可以在片上系统322的外部。

[0041] 在特定的方面中，可以将本文所描述的方法步骤中的一个或多个方法步骤作为计算机程序指令存储在存储器404A中，例如上文结合如图1中示出的系统100所描述的模块。

[0042] 可以由多核CPU 402A和/或GPU 102来执行这些指令，以执行本文所描述的方法。进一步，PCD 400中的多核CPU 402A、GPU 102、存储器404A或者其组合可以充当用于

执行本文所描述的方法步骤中的一个或多个方法步骤的单元。

[0043] 为了本发明如所描述的那样起作用，本说明书中所描述的过程或者过程流中的特定步骤自然地先于其它步骤。然而，如果所描述的步骤的次序或者顺序不改变本发明的功能，那么本发明不限于所描述的步骤的次序。也就是说，应当认识到，在不脱离本发明的范围和精神的情况下，一些步骤可以在其它步骤之前、之后或者与之并行地（与之大体上同时地）执行。在一些实例中，在不脱离本发明的情况下，可以省略或者不执行某些步骤。进一步，诸如“其后”、“然后”、“继而”等之类的词语不旨在限制步骤的次序。这些词语仅仅用于引导读者遍历对示例性的方法的描述。

[0044] 额外地，例如，编程领域的普通技术人员能够没有困难地基于本说明书中的流程图和相关联的描述来编写计算机代码或者识别实现所公开的发明的合适的硬件和/或电路。

[0045] 因此，不认为对程序代码指令的特定集合或者详细的硬件设备的公开对于充分地理解如何做出和使用本发明是必要的。在上面的描述中详细地并且结合附图来解释了所要求保护的计算机实现的过程的创造性的功能，所述附图可能示出了各种过程流。

[0046] 在一个或多个示例性的方面中，所描述的功能可以用硬件、软件、固件或者其任意组合来实现。如果用软件来实现，则所述功能可以作为一个或多个指令或者代码被存储在计算机可读介质上或者被发送。计算机可读介质包括计算机存储介质和通信介质两者，所述通信介质包括促进计算机程序从一个地方到另一地方的传送的任何介质。存储介质可以是可以通过计算机来访问的任何可用的介质。作为示例而非限制，这样的计算机可读介质可以包括 RAM、ROM、EEPROM、CD-ROM 或者其它光盘存储器，磁盘存储器或者其它磁存储设备，或者可以用于以指令或者数据结构的形式携带或者存储期望的程序代码并且可以通过计算机来访问的任何其它介质。

[0047] 此外，任何连接都被合适地称为计算机可读介质。例如，如果软件是使用同轴电缆、光缆、双绞线、数字用户线（“DSL”）或者诸如红外线、无线和微波之类的无线技术从网站、服务器或者其它远程源发送的，则同轴电缆、光缆、双绞线、DSL 或者诸如红外线、无线和微波之类的无线技术包括在介质的定义中。

[0048] 如本文所使用的，磁盘（disk）或者光盘（disc）包括压缩光盘（“CD”）、激光光盘、光盘、数字多功能光盘（“DVD”）、软盘和蓝光光盘，其中，磁盘通常磁性地复制数据，而光盘则利用激光光学地复制数据。以上的组合也应当被包括在计算机可读介质的范围之内。

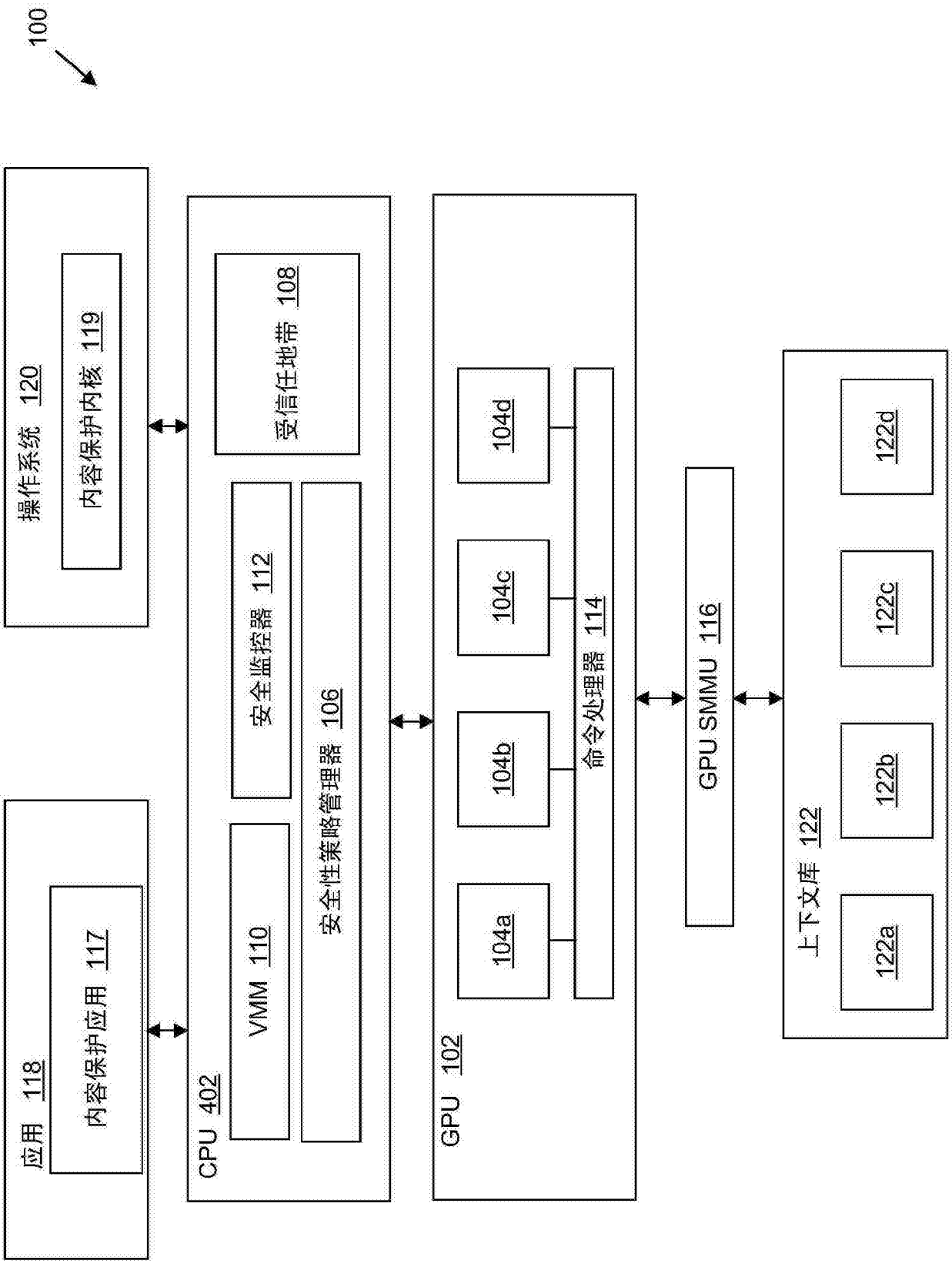

100
操作系统 120
内容保护内核 119
应用 118
内容保护应用 117
CPU 402
VMM 110
安全监控器 112
安全性策略管理器 106
受信任地带 108
GPU 102
104a
104b
104c
104d
命令处理器 114
GPU SMMU 116
上下文库 122
122a
122b
122c
122d

图 1

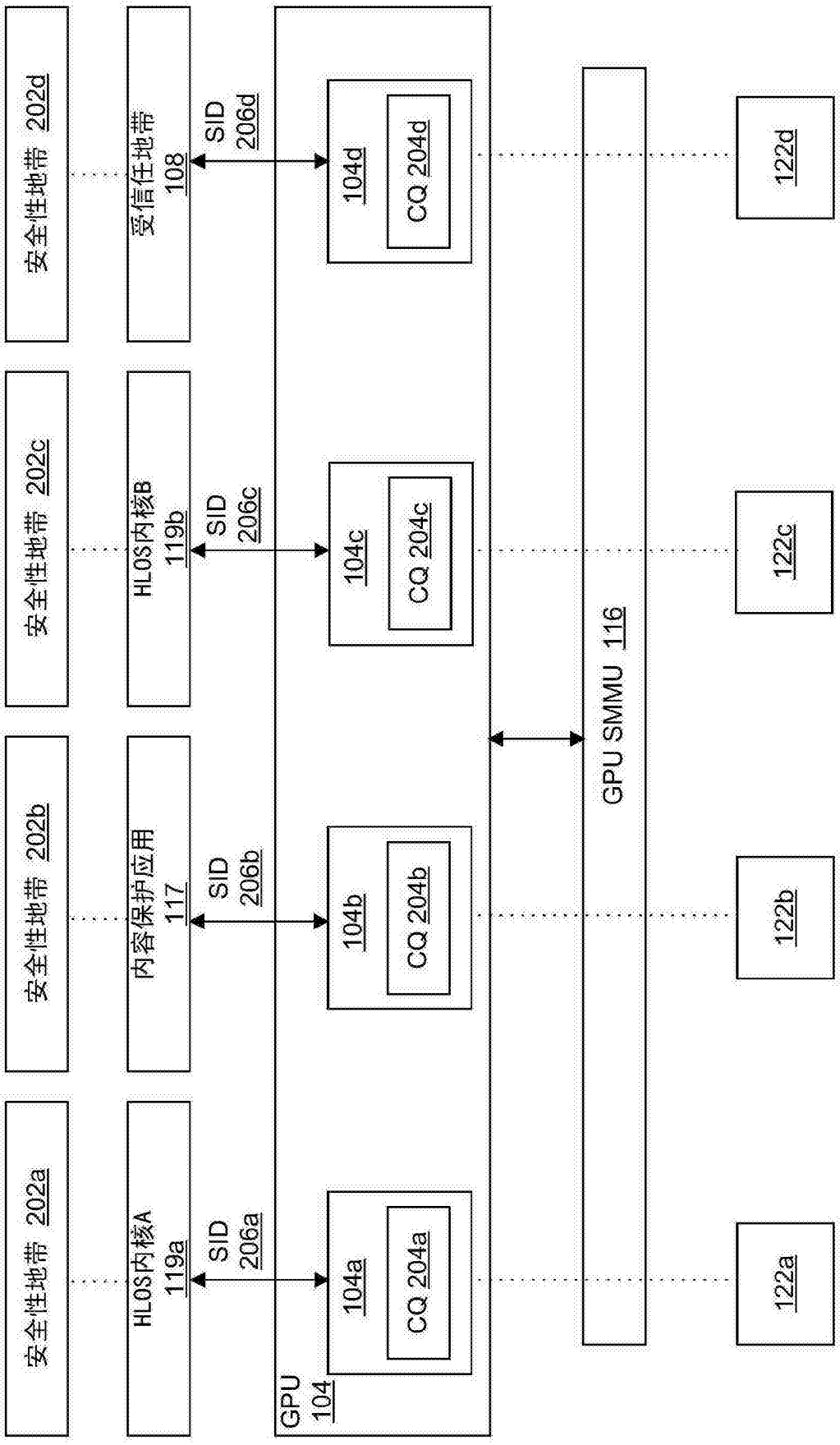

安全性地带 202a
安全性地带 202b
安全性地带 202c
安全性地带 202d
HLOS内核A 119a
内容保护应用 117
HLOS内核B 119b
受信任地带 108
SID 206a
SID 206b
SID 206c
SID 206d
GPU 104
104a
CQ 204a
104b
CQ 204b
104c
CQ 204c
104d
CQ 204d
GPU SMMU 116
122a
122b
122c
122d

图 2

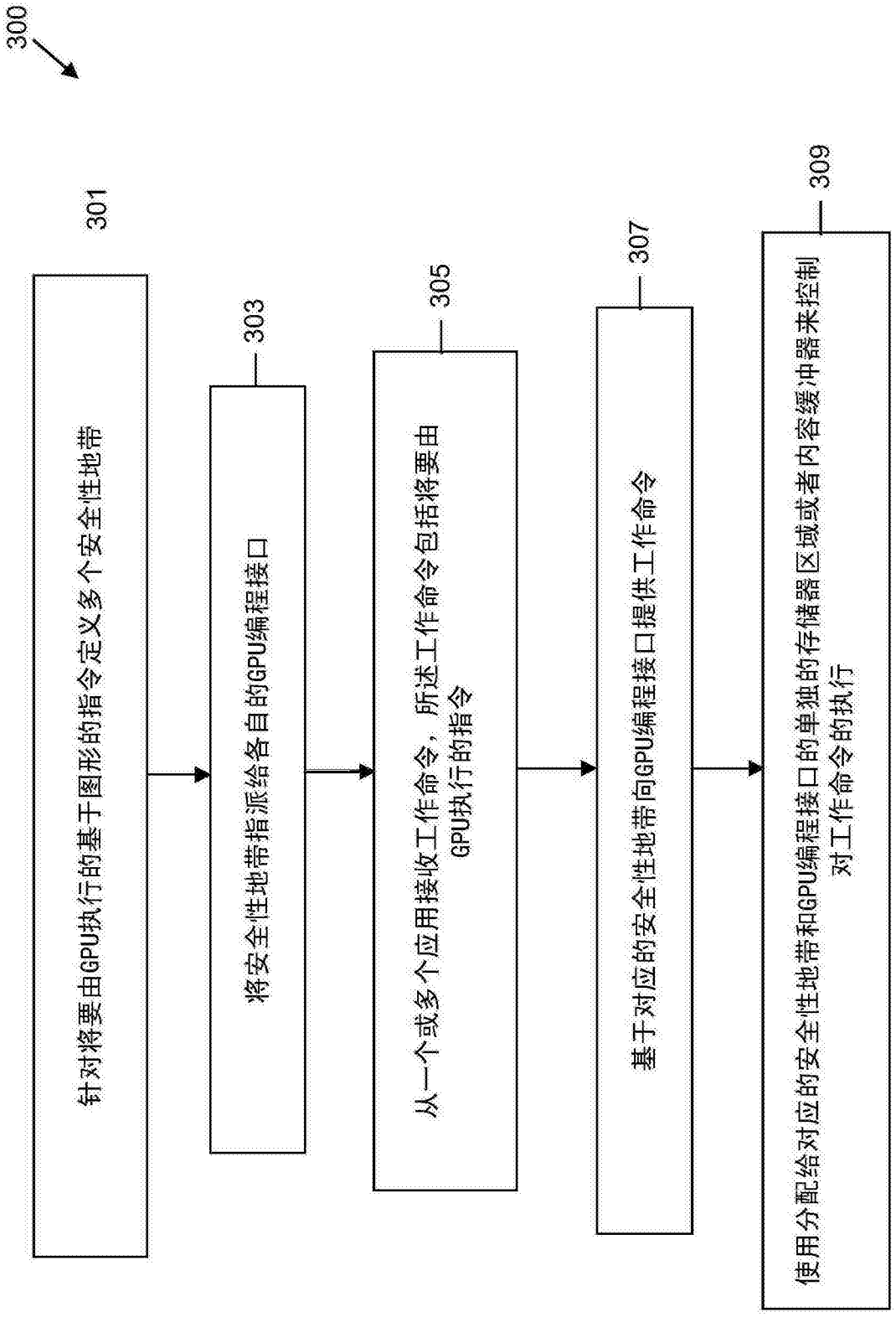

300
301
针对将要由GPU执行的基于图形的指令定义多个安全性地带
303
将安全性地带指派给各自的GPU编程接口
305
从一个或多个应用接收工作命令，所述工作命令包括将要由GPU执行的指令
307
基于对应的安全性地带向GPU编程接口提供工作命令
309
使用分配给对应的安全性地带和GPU编程接口的单独的存储器区域或者内容缓冲器来控制对工作命令的执行

图 3

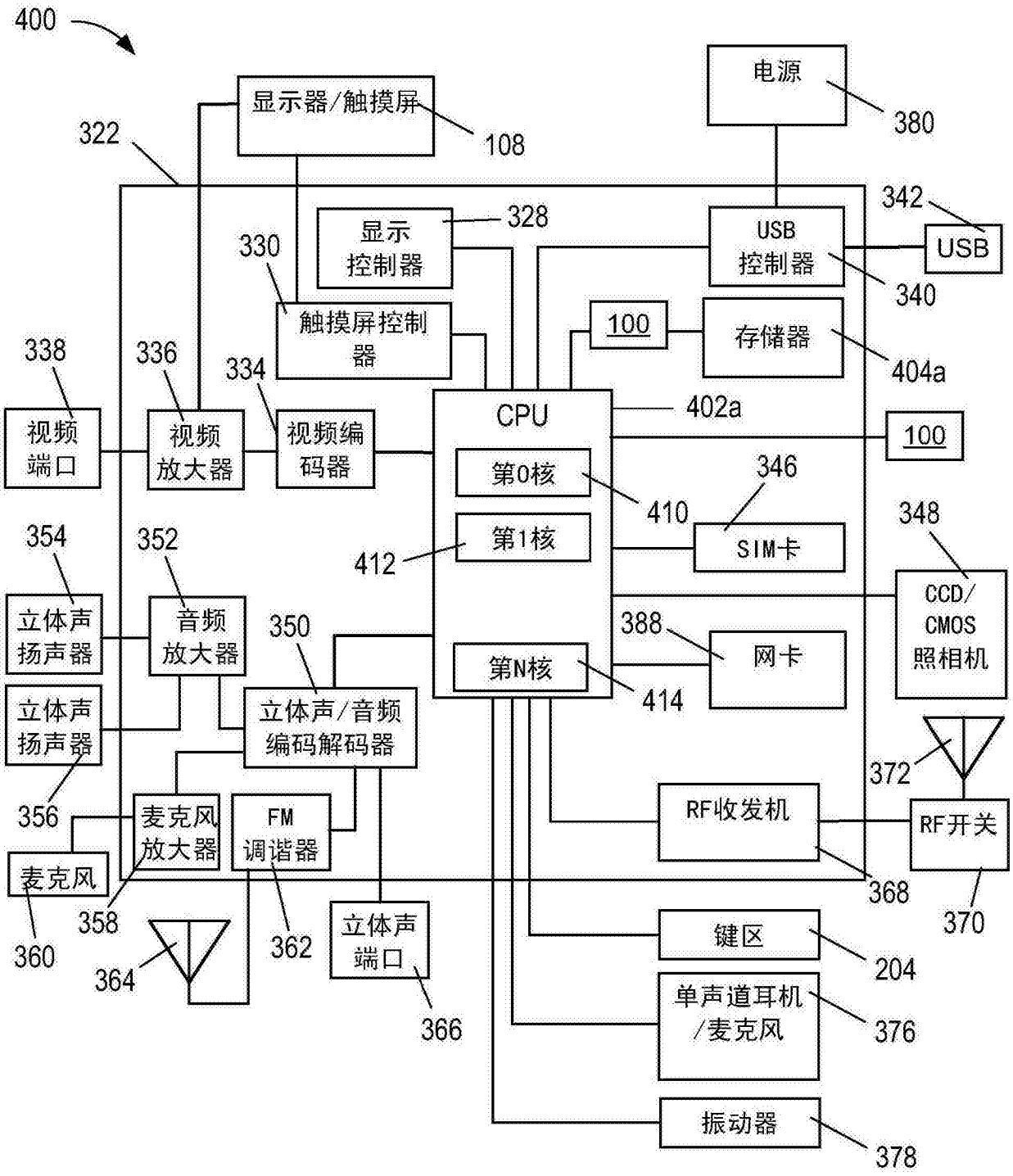

400
显示器/触摸屏
108
322
电源
380
显示
控制器
328
330
触摸屏控制
器
USB
控制器
340
342
USB
100
存储器
404a
338
336
334
视频
端口
视频
放大器
视频编
码器
CPU
402a
100
第0核
410
346
SIM卡
412
第1核
348
CCD/
CMOS
照相机
354
352
立体声
扬声器
音频
放大器
350
388
网卡
第N核
414
立体声
扬声器
立体声/音频
编码解码器
372
356
麦克风
放大器
FM
调谐器
RF收发机
RF开关
麦克风
368
370
358
360
362
立体声
端口
键区
204
364
366
单声道耳机
/麦克风
376
振动器
378

图 4