(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107924365 B
(45)授权公告日 2022.01.04

(21)申请号 201680043460.X

(22)申请日 2016.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 107924365 A

(43)申请公布日 2018.04.17

(30)优先权数据
14/841,469 2015.08.31 US

(85)PCT国际申请进入国家阶段日
2018.01.24

(86)PCT国际申请的申请数据
PCT/US2016/049523 2016.08.30

(87)PCT国际申请的公布数据
WO2017/040542 EN 2017.03.09

(73)专利权人 路安股份有限公司
地址 美国纽约

(72)发明人 弗兰克·N·纽曼 丹·纽曼

(74)专利代理机构 上海华诚知识产权代理有限公司 31300
代理人 徐颖聪

(51)Int.Cl.
G06F 12/14(2006.01)
G06F 12/16(2006.01)
G06F 9/50(2006.01)

审查员 郑攀

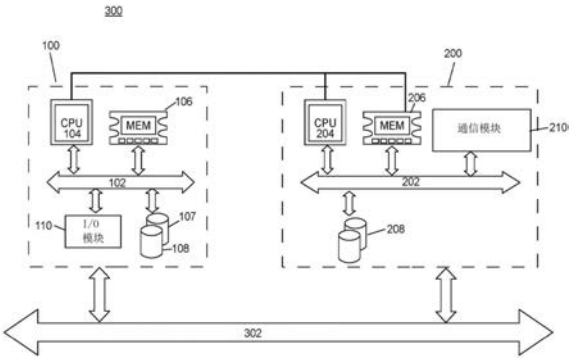
权利要求书6页 说明书9页 附图6页

(54)发明名称

防黑客计算机设计

(57)摘要

公开了一种用于实现防黑客计算装置的计算机结构。可以是大型计算机、个人计算机、智能手机、或者适用于网络通信的任何其他的计算装置的计算装置包含第一分区和和第二分区。第二分区能够通过例如互联网的网络而通信。相比之下，第一分区不能连接到互联网，并且能够仅仅与第二分区通过总线直接通信或者与直接连接到第一分区的输入/输出装置直接通信。进一步，第一分区将它的存储器寻址分割为计算机可执行代码，关键数据文件，以及从第二分区读取的数据文件。第二分区被硬件限制不能从第一分区的存储器寻址读取或者向第一分区的存储器寻址写入。结果，存储在第一分区上的关键数据文件和程序代码被保护防御感染第二分区的恶意代码。



CN 107924365 B

1.一种计算机系统,其特征在于,包含:

第一分区和第二分区;

所述第一分区包含:

第一CPU,

第一存储模块,所述第一存储模块包含:

至少一个用于程序代码的存储地址范围,其中所述程序代码包含计算机可执行代码,并且其中所述用于程序代码的存储地址范围通过硬件开关被硬件保护以防止修改;

至少一个用于第一分区数据的存储地址范围;以及

至少一个用于从所述第二分区读取的数据的存储地址范围;并且

其中,所述第一CPU被硬件配置为仅仅执行在所述用于程序代码的存储地址范围中的所述计算机可执行代码;并且

所述第二分区包含:

第二CPU,

第二存储模块,以及

至少一个通信模块,所述通信模块被配置为耦合到网络;并且

其中,所述第一CPU被配置为访问所述第二存储模块;

其中,所述第一CPU被配置为仅仅将数据从所述第二分区读取到所述至少一个用于从所述第二分区读取的数据的存储地址范围中;并且

其中,所述第二CPU对所述第一CPU或者所述第一存储模块的访问被限制。

2.根据权利要求1所述的计算机系统,其特征在于,所述至少一个用于程序代码的存储地址范围通过硬件电路被配置。

3.根据权利要求2所述的计算机系统,其特征在于,所述硬件电路包含至少一个现场可编程门阵列。

4.根据权利要求1所述的计算机系统,其特征在于,所述第一存储模块包含:

第一存储单元,所述第一存储单元包含所述至少一个用于程序代码的存储地址范围;

第二存储单元,所述第二存储单元包含所述至少一个用于第一分区数据的存储地址范围;以及

第三存储单元,所述第三存储单元包含所述至少一个用于从所述第二分区读取的数据的存储地址范围。

5.根据权利要求1所述的计算机系统,其特征在于,所述程序代码包含操作系统。

6.根据权利要求1所述的计算机系统,其特征在于,包含至少一个数据存储。

7.根据权利要求1所述的计算机系统,其特征在于,

其中,所述第一CPU访问所述第二存储模块的能力通过硬件电路实现;并且

其中,对所述第二分区访问所述第一CPU或者所述第一存储模块的限制通过硬件电路实现。

8.根据权利要求1所述的计算机系统,其特征在于,利用直接连接到所述第一分区的外部装置的硬件特征被配置为使用户能够命令所述第一CPU控制所述第二分区的输入/输出装置。

9.根据权利要求1所述的计算机系统,其特征在于,进一步包含:

总线，

其中，所述第一分区通过所述总线与所述第二分区互连；

其中，所述第一CPU被配置为通过所述总线执行拉取命令，以从所述第二分区读取数据并且将数据仅仅写入到所述至少一个用于从所述第二分区读取的数据的存储地址范围；

其中，所述第一CPU被配置为通过所述总线执行推送命令，以将数据写入到所述第二分区；

其中，所述第一分区不能接受来自所述第二分区的推送命令或者来自所述第二分区的拉取命令；以及

其中，对所述第二分区访问所述第一CPU或者所述第一存储模块的限制通过硬件电路实现。

10.根据权利要求1所述的计算机系统，其特征在于，所述硬件开关包含至少一个被配置为打开或者关闭的外部物理开关，其中所述第一CPU仅仅当所述外部物理开关接通时能够修改存储在所述至少一个用于程序代码的存储地址范围中的数据。

11.根据权利要求1所述的计算机系统，其特征在于，包含：

至少一个被配置为打开或者关闭的外部物理开关；

其中，所述第一CPU被配置为仅仅当所述外部物理开关接通时修改所述至少一个用于程序代码的存储地址范围的内容；

其中，当所述外部物理开关接通时，所述第一CPU不能够从所述第二分区读取或者向所述第二分区写入。

12.根据权利要求1所述的计算机系统，其特征在于，

所述第一CPU访问所述第二存储模块的能力以虚拟分区配置实现；

对所述第二CPU访问所述第一CPU或者所述第一存储模块的限制以虚拟分区配置实现。

13.根据权利要求1所述的计算机系统，其特征在于，

其中，所述第一分区包含至少一个输入/输出模块；并且

其中，多个输入/输出装置被耦合到至少一个输入/输出模块。

14.根据权利要求1所述的计算机系统，其特征在于，进一步包含芯片，所述芯片包含所述第一分区和所述第二分区。

15.根据权利要求1所述的计算机系统，其特征在于，进一步包含第一芯片和第二芯片，所述第一芯片包含所述第一分区，所述第二芯片包含所述第二分区。

16.根据权利要求1所述的计算机系统，其特征在于，利用直接连接到所述第一分区的外部装置的硬件特征被配置为使所述第一CPU能够从所述至少一个用于程序代码的存储地址范围、所述至少一个用于第一分区数据的存储地址范围、或者所述至少一个用于从所述第二分区读取的数据的存储地址范围向所述第二分区写入数据。

17.根据权利要求1所述的计算机系统，其特征在于，

所述第一分区包含一个或多个虚拟子分区；并且

所述第二分区包含一个或多个虚拟子分区。

18.根据权利要求1所述的计算机系统，其特征在于，

其中，对向所述至少一个用于程序代码的存储地址范围写入的限制以虚拟分区配置实现；

其中,所述虚拟分区配置被配置为打开或者关闭所述限制;并且

其中,通过所述虚拟分区配置,所述第一CPU被配置为不能从所述第二分区读取或者向所述第二分区写入。

19.一种计算机系统,其特征在于,包含:

第一分区,所述第一分区包含:

第一CPU;以及

第一存储模块,所述第一存储模块包含:

第一存储地址范围,其中所述第一存储地址范围包含程序代码,其中所述程序代码包含计算机可执行代码,并且其中所述程序代码通过硬件开关被硬件保护以防止修改;

第二存储地址范围;

其中,所述第一CPU被硬件配置为仅仅执行在所述第一存储地址范围中的所述计算机可执行代码;以及

第二分区,所述第二分区包含:

第二CPU;

第二存储模块;以及

至少一个通信模块,所述通信模块被配置为耦合到网络;并且

其中,所述第一CPU被配置为访问所述第二存储模块;

其中,所述第一CPU被配置为仅仅将数据从所述第二分区读取到所述第二存储地址范围中;并且

其中,所述第二CPU对所述第一CPU或者所述第一存储模块的访问被限制。

20.根据权利要求19所述的计算机系统,其特征在于,所述第一存储地址范围通过硬件电路被配置。

21.根据权利要求20所述的计算机系统,其特征在于,所述硬件电路包含至少一个现场可编程门阵列。

22.根据权利要求19所述的计算机系统,其特征在于,所述第一存储模块包含:

第一存储单元,所述第一存储单元包含所述第一存储地址范围;

第二存储单元,所述第二存储单元包含所述第二存储地址范围。

23.根据权利要求19所述的计算机系统,其特征在于,所述程序代码包含操作系统。

24.根据权利要求19所述的计算机系统,其特征在于,包含至少一个数据存储。

25.根据权利要求19所述的计算机系统,其特征在于,

其中,所述第一CPU访问所述第二存储模块的能力通过硬件电路实现;并且

其中,对所述第二分区访问所述第一CPU或者所述第一存储模块的限制通过硬件电路实现。

26.根据权利要求19所述的计算机系统,其特征在于,利用直接连接到所述第一分区的外部装置的硬件特征被配置为使用户能够命令所述第一CPU控制所述第二分区的输入/输出装置。

27.根据权利要求19所述的计算机系统,其特征在于,进一步包含:

总线,

其中,所述第一分区通过所述总线与所述第二分区互连;

其中，所述第一CPU被配置为通过所述总线执行拉取命令，以从所述第二分区读取数据并且将数据仅仅写入到所述第二存储地址范围；

其中，所述第一CPU被配置为通过所述总线执行推送命令，以将数据写入到所述第二分区；

其中，所述第一分区不能接受来自所述第二分区的推送命令或者来自所述第二分区的拉取命令；以及

其中，对所述第二分区访问所述第一CPU或者所述第一存储模块的限制通过硬件电路实现。

28.根据权利要求19所述的计算机系统，其特征在于，所述硬件开关包含至少一个被配置为打开或者关闭的外部物理开关，其中所述第一CPU被配置为仅仅当所述外部物理开关接通时修改存储在所述第一存储地址范围中的数据。

29.根据权利要求19所述的计算机系统，其特征在于，包含：

至少一个被配置为打开或者关闭的外部物理开关；

其中，所述第一CPU被配置为仅仅当所述外部物理开关接通时修改所述第一存储地址范围的内容；

其中，当所述外部物理开关接通时，所述第一CPU不能够从所述第二分区读取或者向所述第二分区写入。

30.根据权利要求19所述的计算机系统，其特征在于，

所述第一CPU访问所述第二存储模块的能力以虚拟分区配置实现；

对所述第二CPU访问所述第一CPU或者所述第一存储模块的限制以虚拟分区配置实现。

31.根据权利要求19所述的计算机系统，其特征在于，

其中，所述第一分区包含至少一个输入/输出模块；并且

其中，多个输入/输出装置被耦合到至少一个输入/输出模块。

32.根据权利要求19所述的计算机系统，其特征在于，进一步包含芯片，所述芯片包含所述第一分区和所述第二分区。

33.根据权利要求19所述的计算机系统，其特征在于，进一步包含第一芯片和第二芯片，所述第一芯片包含所述第一分区，所述第二芯片包含所述第二分区。

34.根据权利要求19所述的计算机系统，其特征在于，利用直接连接到所述第一分区的外部装置的硬件特征被配置为使所述第一CPU能够从所述第一存储模块向所述第二分区写入数据。

35.根据权利要求19所述的计算机系统，其特征在于，

所述第一分区包含一个或多个虚拟子分区；并且

所述第二分区包含一个或多个虚拟子分区。

36.根据权利要求19所述的计算机系统，其特征在于，

其中，对向所述第一存储地址范围写入的限制以虚拟分区配置实现；

其中，所述虚拟分区配置被配置为打开或者关闭所述限制；并且

其中，通过所述虚拟分区配置，所述第一CPU被配置为能够或者不能够从所述第二分区读取或者向所述第二分区写入。

37.一种计算机系统，其特征在于，包含：

第一分区和第二分区；

所述第一分区包含：

第一CPU；和

第一存储模块，所述第一存储模块包含：

至少一个用于程序代码的存储地址范围，其中所述程序代码包含计算机可执行代码，并且其中所述至少一个用于程序代码的存储地址范围通过硬件电路被配置；以及

至少一个用于其他数据的存储地址范围，其中所述其他数据包含从所述第二分区读取的数据；

其中，所述第一CPU被硬件配置为仅仅执行在所述用于程序代码的存储地址范围中的所述计算机可执行代码；并且

所述第二分区包含：

第二CPU；

第二存储模块；以及

至少一个通信模块，所述通信模块被配置为耦合到网络；

其中，所述第一CPU被配置为访问所述第二存储模块，并且仅仅将数据从所述第二分区读取到所述至少一个用于其他数据的存储地址范围中；并且

其中，所述第二CPU对所述第一存储模块的访问被限制。

38.根据权利要求37所述的计算机系统，其特征在于，所述第一存储模块包含：

第一存储单元，所述第一存储单元包含所述至少一个用于程序代码的存储地址范围；以及

第二存储单元，所述第二存储单元包含所述至少一个用于其他数据的存储地址范围。

39.根据权利要求37所述的计算机系统，其特征在于，所述至少一个用于其他数据的存储地址范围包含：

至少一个用于从所述第二分区读取的数据的存储地址范围，以及至少一个用于第一分区数据的存储地址范围。

40.根据权利要求37所述的计算机系统，其特征在于，所述第一存储模块包含：

第一存储单元，所述第一存储单元包含所述至少一个用于程序代码的存储地址范围；

第二存储单元，所述第二存储单元用于从所述第二分区读取的数据；以及

第三存储单元，所述第三存储单元用于第一分区数据。

41.根据权利要求37所述的计算机系统，其特征在于，进一步包含总线，

其中，所述第一分区通过所述总线与所述第二分区互连；

其中，所述第一分区被配置为通过所述总线执行拉取命令，以从所述第二分区读取数据并且将数据仅仅写入到所述至少一个用于其他数据的存储地址范围；

其中，所述第一分区被配置为通过所述总线执行推送命令，以将数据写入到所述第二分区；

其中，所述第一分区被配置为不接受来自所述第二分区的推送命令或者来自所述第二分区的拉取命令；以及

其中，所述总线的硬件电路不允许所述第二分区访问所述第一存储模块。

42.根据权利要求37所述的计算机系统，其特征在于，包含至少一个被配置为打开或者

关闭的外部物理开关，其中所述第一CPU被配置为仅仅当所述外部物理开关接通时修改存储在所述至少一个用于程序代码的存储地址范围中的数据。

43.一种计算机系统，其特征在于，包含：

至少一个CPU，

至少一个I/O模块，所述I/O模块连接到至少一个其他的计算机，以及

至少一个存储模块，包含：

至少一个用于程序代码的存储地址范围，所述用于程序代码的存储地址范围通过硬件电路被配置，其中所述程序代码包含计算机可执行代码；

至少一个用于其他数据的存储地址范围，其中所述其他数据包含从所述至少一个其他的计算机读取的数据；

其中，所述至少一个CPU被硬件配置为仅仅执行在所述用于程序代码的存储地址范围中的所述计算机可执行代码；

其中，从所述至少一个其他的计算机读取的数据仅仅能够被写入到所述至少一个用于其他数据的存储地址范围中；

其中，所述至少一个存储模块不能够被所述至少一个其他的计算机访问。

44.根据权利要求43所述的计算机系统，其特征在于，所述至少一个存储模块包含：

第一存储单元，所述第一存储单元用于所述至少一个用于程序代码的存储地址范围；以及

第二存储单元，所述第二存储单元用于所述至少一个用于其他数据的存储地址范围。

45.根据权利要求43所述的计算机系统，其特征在于，包含至少一个能够被打开或者关闭的外部物理开关，其中所述至少一个CPU仅仅当所述外部物理开关接通时能够修改存储在所述至少一个用于程序代码的存储地址范围中的数据。

46.根据权利要求43所述的计算机系统，其特征在于，进一步包含：

总线，

其中，所述计算机系统通过所述总线被通信地耦合到所述至少一个其他的计算机；

其中，所述计算机系统被配置为通过所述总线执行拉取命令，以从所述至少一个其他的计算机读取数据并且将数据仅仅写入到所述至少一个用于其他数据的存储地址范围；

其中，所述计算机系统被配置为通过所述总线执行推送命令，以将数据写入到所述至少一个其他的计算机；

其中，所述计算机系统被配置为不接受来自所述至少一个其他的计算机的推送命令或者来自所述至少一个其他的计算机的拉取命令；以及

其中，所述总线的硬件电路不允许所述至少一个其他的计算机访问所述至少一个存储模块。

防黑客计算机设计

[0001] 相关申请的交叉引用

[0002] 本申请要求2015年8月31日提交的第14/841,469号美国专利申请的权益。

技术领域

[0003] 公开了一种用于实现防黑客计算装置的计算机结构。

背景技术

[0004] 潜入计算机的常用方法是通过借助于互联网或者其他的网络连接将恶意的计算机可执行代码(恶意软件)置入计算机。这种入侵已经成为主要的威胁,并且入侵的主要情况已经被广泛报导。阻挠这种入侵的广泛流行的方法依赖于软件来识别和禁用或者删除恶意软件。然而,黑客正在变得越来越富有经验,并且通常的保护是不足够的。

[0005] 因此,在本领域中具有对利用硬件方法的防黑客计算机系统结构的需要。这种硬件方法将对用于各种应用的各种计算机可用。例如,使用本发明中公开的硬件方法的银行、公司、政府机构、或者个人将被更好的保护,防御可能企图控制他们的计算机以窃取或者破坏存储在计算机上的机密数据、个人信息、或者密码的黑客。本文公开的硬件方法保护防御黑客至利用当前基于软件的解决方案不可能达到的程度。

发明内容

[0006] 用于实现防黑客计算装置的计算机系统结构被公开。计算机系统结构通过限制关键数据文件对互联网的直接访问的硬件,以及分割关键数据文件、从互联网接收的文件和计算机可执行代码的存储地址的硬件,防止从互联网接收的恶意计算机可执行代码访问或者感染关键数据文件。可以是大型计算机、个人计算机、智能手机、或者适用于网络通信的任何其他的计算装置的计算装置包含第一分区和第二分区。第二分区能够通过例如互联网的网络而通信。相比之下,第一分区能够直接与第二分区通过总线通信,或者与直接连接到第一分区的输入/输出装置通信。结果,第一分区被硬件限制不能连接到互联网以及任何其他的装置,例如连接到互联网的服务器。由第一分区对互联网的所有访问受限于第一分区和相比之下能够连接到互联网的第二分区之间的硬件连接。

[0007] 进一步,第一分区包括利用操作系统将第一分区的存储地址分割为三个部分的硬件电路,该三个部分为计算机可执行代码;存储在第一分区上的关键数据文件;以及通过总线从第二分区读取的数据文件。本方法也能够受到第一分区中三个分立的存储单元的使用的影响。为了保护关键数据文件,第二分区被硬件限制不能从第一分区的存储器寻址读取或者向第一分区的存储器寻址写入。来自第二分区的数据通过由第一分区的操作系统执行的“拉取”命令而被传送至第一分区。进一步,第二分区不能够将数据“推送”至第一分区或者控制第一分区发送“拉取”命令。通过硬件设计,由第一分区从第二分区拉取的所有数据被存储在专门用于从第二分区读取的数据文件的第一分区的存储器部分中。进一步,通过硬件限制,第一分区防止从第二分区读取的数据文件被执行。结果,存储在第一分区上的关

键程序和关键数据文件被保护,防御来自互联网或者来自任何其他来源的感染第二分区的恶意代码。

附图说明

[0008] 将引用附图进行详细的说明,其中:

[0009] 图1说明了示例性的网络图;

[0010] 图2是根据本发明的各个实施例的描绘用于实现防黑客计算装置的计算机系统结构的框图;

[0011] 图3描绘了根据优选实施例的计算装置的存储器寻址;

[0012] 图4是描绘根据优选实施例的进程的流程图;

[0013] 图5是描绘了适合于利用现有计算机结构的计算装置使用的本发明的实施例的框图;以及

[0014] 图6是描绘适合于利用现有计算机结构的计算装置使用的本发明的软件实施例的框图。

[0015] 本发明的其他的目的、特征和特性,以及操作的方法和结构的相关元件的功能和部件的组合在考虑了以下参考附图的详细说明后将变得更加显而易见,以上所有构成本说明书的一部分。

具体实施方式

[0016] 此处公开了本发明的详细的说明性的实施例。然而,根据本发明的技术、方法、处理、系统和操作结构可以以各式各样的形式和模式被具体化,其中的一些可以完全不同于被公开的实施例中的那些。因此,此处公开的具体的结构上的和功能上的细节仅仅是代表性的,然而在这方面,它们被认为出于公开目的提供了最好的实施例。

[0017] 除非上下文另有明确要求,遍及说明书和权利要求书的词语“包含”,“包括”等等将以包容性的意义被解释,与排外的或者详尽无遗的意义相反;也就是说,是“包括,但不限于”的意义。当在此处被使用时,术语“连接”“耦合”或者其任意变体,意味着两个或以上的元件之间直接的或者间接的、电子的或以其他方式的任意的连接或者耦合;元件之间的连接的耦合可以是物理上的、逻辑上的、或者其结合。此外,单词“此处”,“以上”,“以下”以及类似含义的词语,当在本申请中被使用时,应该指的是作为一个整体的本申请而非本申请的任意特定部分。上下文允许之处,使用单数或者复数的优选实施例的详细说明中的词语也可以分别包括复数或者单数的含义。关于一列两个或以上的项,词语“或者”包括该词语的所有以下解释:列表中的任意项,列表中的所有项,以及列表中项的任意组合。以下参考图呈现本发明的优选实施例的详细说明。

[0018] 首先参考图1,示出的是防黑客计算装置的示例性的网络图。计算装置300能够包含任意大规模的商业或者政府计算机或者“主机”、一组联合操作的连接在一起的计算机、单个个人计算机(Personal Computer,PC)或者移动通信装置,移动通信装置包括但不限于移动电话、蜂窝电话、智能电话、便携计算机、上网本、个人数字助理(Personal Digital Assistant,PDA)、家用电器、家庭的或者商业的建筑控制器、或者适用于网络通信的任何其他的计算装置。计算装置300包含第一分区100和第二分区200。第一分区100被直接与例如

键盘、数据存储驱动器、打印机等等的输入/输出装置互连。在用于大规模使用的实施例中，通过直接的硬线，第一分区能够被连接至处于计算装置的用户的控制下的物理位置的较小的计算机或者PC。在该实施例中，用户能够禁用较小计算机或者PC的任意形式的互联网连接，包括电线、电缆、或者Wi-Fi。第二分区200通过网络500与终端600通信。如以下参考图2详细描述的那样，第一分区100能够使用总线直接与第二分区200通信，但是第一分区100与网络500的通信被硬件限制。在优选实施例中，第一分区的CPU能够直接访问第二分区的存储器和第二分区的CPU，但是第二分区的CPU对第一分区的存储器和第一分区的CPU的访问被硬件限制。

[0019] 网络500可以是局域网(Local Area Network，LAN)、广域网(Wide AreaNetwork，WAN)、互联网、蜂窝网络、卫星网络或者上述的结合，或者允许向计算装置300的数据的传送和/或来自计算装置300的数据的接收的任意其他的网络。通过网络500从终端600被发送到计算装置300或者从计算装置300被发送到终端600的数据能够利用标准通信协议或者标准网络协议而被发送和/或接收。在优选实施例中，系统利用传输控制协议/网际协议(Transmission Control Protocol/Internet Protocol，TCP/IP)并且网络500是互联网和/或内联网。用于发送和/或接收数据的协议的其他实例包括但不限于网络电话(Voice Over IP，VOIP)协议、短消息服务(Short Message Service，SMS)、蓝牙无线传输、以及全球移动通信系统(Global System for Mobile Communications，GSM)。网络500能够利用计算装置300和终端600的一个或多个协议。此外，网络500能够将其他的协议转换为终端600的一个或多个协议，也能够将终端600的一个或多个协议转换为其他的协议。在一些情况下，第二分区200暴露在试图访问或者感染存储在计算装置300上的关键数据文件的恶意计算机可执行代码下。如下参考图2和3所描述的，优选实施例防止这种恶意软件访问或者感染第一分区100的关键数据文件和存储器。

[0020] 现在参考图2，示出的是描绘用于实现计算装置300的计算机系统结构的框图，该计算装置300被硬件保护以防止感染来自互联网和来自能够通过网络500通信的任意其他来源的恶意计算机可执行代码。计算装置300包含第一分区100。第一分区100包含与第一分区总线102互连的计算机处理单元(Computer Processing Unit，CPU)104。第一分区存储器106通过第一分区总线102与CPU 104互连。如上参考图1所述，第一分区100通过输入/输出模块110与一个或多个输入/输出装置互连。在优选实施例中，分区100进一步包含数据存储107和108。关键数据文件被存储在存储器106和/或数据存储107上。数据存储108由第一分区用来存储其他的数据，包括已经被处理的来自第二分区200的数据。第一分区100包括用于执行计算机可执行代码的操作系统。如以下参考图3详细描述的那样，CPU 104能够仅仅执行存储在存储器106的程序代码地址范围内的、以及存储在数据存储107和108上的计算机可执行代码。这借助于硬件电路，通过CPU 104(通过本实施例其本身被保护以防御恶意软件)的操作系统的控制而实现。当前计算机系统结构的根本弱点是执行控制常常被移交给通过互联网已到达计算机的恶意计算机可执行代码。本实施例限制从互联网被下载至第二分区的恶意计算机可执行代码的任何的执行。

[0021] 计算装置300进一步包含第二分区200。第二分区200包含与第二分区总线202互连的CPU 204。至少一个存储器206通过第二分区总线202与CPU 204互连。通信模块210允许第二分区200通过网络与终端通信。计算机系统结构进一步包括至少一个数据存储208。数据

存储208用于不被认为是关键性的数据文件的存储。第二分区200包括用于执行计算机可执行代码的操作系统。如以下参考图3详细描述的那样，CPU 204可以执行来自存储器206的全地址范围和数据存储208的计算机可执行代码。

[0022] 如图2所示，第一分区100通过总线302与第二分区200直接互连。此外，在优选实施例中，CPU 104可以向第二分区200的存储器206的全地址范围和数据存储208写入。该设计的一个优势是第一分区100能够恢复已经被恶意计算机可执行代码感染的第二分区200的操作系统和数据文件。此外，CPU 104可以从存储器206的全地址范围和数据存储208读取数据，但是仅仅是通过CPU 104的“读取”命令(拉取)。通过硬件限制，CPU 104不能接受由第二分区200推送至其的任意数据或者其他文件。此外，第二分区200不能从第一分区100拉取任意数据。进一步，第一分区100的操作系统和支援程序限定CPU 104将从第二分区200接受的数据的格式和其他文件特性。第二分区200向第一分区100提供不是适当预期形式的文件的任意企图将被CPU 104拒绝。如以下参考图3详细描述的那样，由CPU 104从第二分区200读取的所有数据文件被写入存储器106的第二分区地址范围和/或数据存储108。第一分区100被保护防御存储在第二分区200上的任意恶意计算机可执行程序，因为CPU 104仅仅能够执行存储在存储器106的程序代码地址范围和数据存储107上的计算机可执行代码。

[0023] 图2中描述的计算机系统结构能够被应用于各种计算装置，包括但不限于大型计算机，个人计算机，平板电脑，平板计算机以及智能电话。进一步，计算机系统结构能够被应用于新产品或者适配到现有的计算机设计。虽然图2中描述的计算机结构作为单组芯片被公开，但是该技术可以被应用于具有两个分开的计算机系统的系统，假如该计算机系统根据此处公开的原理而被设计。在具有两个分开的计算机系统的实施例中，第一计算机系统(具有类似于第一分区的角色)会存储被保护防御恶意代码的关键数据文件，而第二计算机系统(具有类似于第二分区的角色)与远程终端通信。进一步，第一计算机系统会被直接连接到第二计算机系统。

[0024] 接下来参考图3，示出的是第一分区和第二分区的存储器寻址。第一分区存储器寻址700(在图2所示的存储器106中)包含至少一个程序代码地址块702、至少一个第一分区数据地址块704、以及至少一个第二分区数据地址块706。在优选实施例中，通过将第一分区的CPU设计为物理地限制可用的存储器寻址空间，对第一分区存储器寻址700的每个地址块的数据的写入和读取被限制。例如，支持32位或者64位寻址的CPU能够将用于执行计算机可执行代码的操作系统的访问限制到被映射为程序代码地址的位。结果，位于第一分区数据地址块704和第二分区数据地址块706上的恶意计算机可执行代码不被操作系统执行，即使这种数据文件中的一些可以被标记为有效的计算机可执行代码。进一步，第一分区的CPU只向第二分区数据地址块706写入不能用于执行的从第二分区读取的任意数据。该设计防止第二分区中的恶意计算机可执行代码被写入第一分区存储器寻址700的程序代码地址块702。硬连线设计的进一步优势是写入和读取命令的地址范围不能够被恶意计算机可执行代码感染，因为要感染存储地址范围，第一分区的CPU将需要被物理地改变。利用三个单独的存储器用于使第一分区的编址分开也是可能的，这对本领域技术人员将是显而易见的。

[0025] 还可以为程序代码地址块702中的程序实现另外的硬件保护程度。这可以包括不经常被更新并且与程序代码地址块702中的程序关联的非常关键的数据文件。更新程序代码地址块702的内容的权利被限于直接连接到第一分区100的装置。利用可选择的硬件开

关,CPU 104、总线102和I/O模块110的结合能够被控制,以便修改程序代码地址块702的内容的能力需要通过被授权人员启动。结果,对程序代码地址块702的任意更新需要在提供更新的直接连接装置处的被授权人员的访问以及被授权接通开关的人员的单独动作。对于高度安全的系统,该设计会提供额外的保护度,防止甚至被授权的、直接连接的用户不适当地试图(无意地或者有意地)修改存储在程序代码地址块702中的程序或者非常关键的数据。

[0026] 相比之下,第二分区的CPU被限制为读取和写入第二分区存储地址800。如图3所示,利用本领域中已知的技术,数据或者程序代码能够从第二分区存储地址800的全地址范围被读取或者被写入第二分区存储地址800的全地址范围。然而,第二分区的CPU对第一分区的存储地址的访问或者修改被硬件限制。该设计防止第二分区的CPU向第一分区写入通过互联网来自远程终端的已经感染第二分区的恶意计算机可执行代码。进一步,第一分区的CPU能够直接访问第二分区存储地址800,由此通过避免由使第一分区和第二分区互连的总线上的活动引起的延迟,来提高第一分区的CPU的读取和写入性能。第一分区的CPU可以仅从存储地址800读取到第二分区数据地址块706中,第二分区数据地址块706专门用于从第二分区读取的数据。

[0027] 图4描绘了表示第二分区获取位于第一分区上的数据文件的进程的流程图。首先在步骤902中,第一分区的CPU周期性地检查第二分区的CPU的当前的数据请求。数据请求可以是获取数据项、更新数据项或者第一分区的动作请求,例如,第一分区的动作请求是从一个帐户向另一个账户传送资金,或者改变建筑物中的温度设置。接下来,在步骤904中,位于第一分区上的常驻程序验证数据请求的合法性。如上所述,位于第一分区上的常驻程序被硬件保护防止来自互联网以及来自任何其他网络的恶意计算机可执行代码的感染。对于已由位于第一分区上的程序验证的数据请求,该进程进行到步骤910。否则,对于失败的验证,该进程进行到步骤906。在步骤906中,由于在步骤904中检测到的任意可疑的活动,第一分区的CPU可以请求直接连接至第一分区的被授权人员的确认。如果直接连接至第一分区的被授权人员确认了数据请求,该进程进行到步骤910。否则,该进程进行到步骤908。在步骤908中,第一分区的CPU警告被授权人员数据请求已经被拒绝并且前往另一个数据请求。在验证和/或确认之后,在步骤910中,第一分区的CPU访问数据文件并且将数据适当的部分提供给第二分区。在该设计下,第二分区不能够获得对第一分区上任意关键数据文件的直接访问。如上所述,在优选实施例中公开的计算机系统结构的硬件被安排以便从第一分区发送数据文件的命令不能够被第二分区控制。结果,位于第二分区上的任意恶意代码不能将恶意代码置入第一分区的可执行代码并且因此访问或者感染任意关键数据文件。

[0028] 除了保护第一分区,本优选实施例能够允许第一分区恢复被恶意计算机可执行代码感染的第二分区的数据文件。恶意计算机可执行代码可以破坏第二分区和其对屏幕和键盘的控制,由此阻止用户通过第二分区访问远程终端。在一个实施例中,第一分区包括硬件特征,该硬件特征利用按键序列允许直接连接到第一分区的用户命令第一分区的CPU控制被恶意计算机可执行代码感染的第二分区的屏幕和键盘以及程序控制。通过第一分区,直接连接到第一分区的被授权用户可以触发第二分区上的保护软件。用户也可以命令第一分区完全擦除第二分区的存储器和/或数据文件以删除恶意计算机可执行代码,或者将第二分区恢复至没有这种恶意代码的先前保存的状态。在该实施例中,第二分区的操作系统和应用被第一分区记录。结果,第一分区可以在删除恶意计算机可执行代码之后恢复第二分

区的操作系统和应用。在恶意代码被删除之后，第二分区将是可操作的，由此允许计算装置对远程终端的访问。

[0029] 此外，优选实施例使得引入各种类型的保护软件切实可行。如上所述，优选实施例利用各种硬件方法防止恶意计算机可执行代码访问和感染第一分区的程序代码或者数据文件。这种方法包括但不限于，阻止第一分区通过互联网对远程终端的直接访问并且限制第一分区的存储器寻址。虽然该设计限制了来自第二分区的对第一分区的数据文件的请求，该计算装置的其他方面将作为本领域中公知的标准计算机系统来运行。例如，当第一分区的CPU从第二分区读取数据时，来自第一分区的CPU将经常收到个别的数据项被发送回第二分区的请求。然后该被请求的信息能够通过网络被第二分区转发至远程终端。优选实施例允许保护程序被第一分区的CPU执行以单独地或在一段时间内集中地检查这种数据请求是否是可疑的。示例性的可疑数据请求是第二分区上的程序请求关键数据文件，该关键数据文件被第一分区上的软件映射为财务信息。结果，当可疑的活动被检测到时，第一分区的CPU能够触发适当的验证手段，包括请求来自与第一分区直接连接的被授权人员的参与。在进一步的实例中，第一分区的硬件保护的程序代码被编程以仅将数据的特定项而不是整个文件或者全套关键数据文件发送给第二分区。示例性的程序也可以拒绝将例如密码和信用卡安全码的机密数据发送给第二分区。这种程序在已知的系统中不是切实可行的，因为恶意计算机可执行代码可以直接获取关键数据文件并且可能改变保护程序。

[0030] 通过为应用程序创建硬件“沙箱”，本发明也可以被并入到移动装置的结构中。就像当前在一些蜂窝电话操作系统上使用的软件“沙箱”一样，这会允许应用程序访问一些功能和数据同时限制对其他的关键的存储器的访问。不像那些现有的方法，该实施例提供了对恶意计算机可执行代码的访问的硬件限制。关键数据和操作系统本身可以被保护防止任何应用的修改，因为所有的辅助的程序将被载入到第二分区中。

[0031] 此外，本发明可以被用于保护主要接口用于非计算功能的联网装置。例如冰箱和恒温器的家用电器越来越多地被设计成连接到互联网。这种装置也可以被设计有优选实施例的计算机系统结构，以保护主要分区的功能防御通过互联网或者通过网络接收的恶意计算机可执行代码。其他的“智能家居”和“智能建筑”装置以及车辆中的计算机控制台可以相应地利用计算机系统结构。

[0032] 虽然优选实施例在集成的新的计算机系统结构的背景中被描述，本发明能够适合于利用现有结构连同硬件和软件的组合的计算装置，该硬件和软件的组合利用优选实施例的关健特征。对于已经在现有的计算机上做出重大投资并且想继续使用它们但是想要增强的保护防御入侵的用户，这样的实施例可以是有用的。在一个实施例中，集成系统的第一分区能够被连接到现有的计算机，现有的计算机可以保存大部分关键的文件和程序。结果，如以上对于集成系统的第一分区所描述的那样，计算机将被与互联网及其他的外部源隔离。通过总线或者I/O模块，第一分区可以与计算机进行通信、读取和写入，并且计算机将被硬件和操作系统保护，防御恶意软件。

[0033] 另一个可供选择的实施例在图5中示出，包含第一计算机1300和第二计算机1400。第一计算机1300和第二计算机1400利用本领域中已知的计算机结构，例如，x86，ARM，和PowerPC。正因为如此，第一计算机1300和第二计算机1400包含用于执行计算机可执行代码的操作系统。正如以上的讨论，这些已知结构的缺点是第一计算机1300和第二计算机1400

的处理器容易受到从互联网接收的恶意计算机可执行代码的执行的影响，恶意计算机可执行代码能够访问和感染关键数据文件。进一步，这样的恶意计算机可执行代码能够规避已知的软件解决方案。在本实施例中，第二计算机1400可以连接到互联网。结果，第二计算机1400容易受到来自互联网的恶意计算机可执行代码的影响。然而，第一计算机1300不被连接到互联网并且通过计算装置1000与第二计算机1400互连。第一计算机1300通过操作系统方法的使用可以实现一些保护度，如以下参考图6详细描述的那样。然而，这样的保护将是有限的并且容易遭受富有经验的黑客的损害。同样，采用计算装置1000以保护第一计算机1300防御感染第二计算机1400的任意恶意计算机可执行代码将获得更多的保护，计算装置1000使用本优选实施例的硬件设计和技术。计算装置1000包含了上述全集成系统的大部分结构，允许第一计算机1300以抵御对计算机1300的入侵企图的方式，处理通过计算机1400从互联网接收的数据和请求。

[0034] 如图5所示，计算装置1000包含第一分区1100和第二分区1200。第二分区1200包含通过总线1202互连的CPU 1204，存储器1206，数据存储1208，以及I/O模块1212。CPU 1204执行位于数据存储1208和/或存储器1206上的操作系统以通过I/O模块1212与第二计算机1400通信。I/O模块1212可以是USB端口、eSATA、WiFi、或者用于将计算装置1000连接到第二计算机1400的任何其他的已知的通信接口。在该实施例中，软件在第二计算机1400上执行，这允许CPU 1204从第二计算机1400接收数据。通过CPU 1204从第二计算机1400读取的数据文件被存储在存储器1206和/或数据存储1208上。CPU 1204与第一计算机1300的直接通信被硬件限制。第二分区1200，进一步包含通信模块1210。通信模块1210允许第二分区1200通过例如互联网的网络而通信。结果，第一计算机1300能够利用通信模块1210访问来自互联网的数据，而不是利用第二计算机1400访问来自互联网的数据。

[0035] 计算机1300和计算装置1000与例如键盘、数据存储驱动、打印机等等的输入/输出装置直接互连。在大规模使用的实施例中，通过直接的硬线，计算机1300和计算装置1000可以被连接至处于计算装置的用户的控制下的物理位置的较小的计算机或者PC。在该实施例中，用户可以禁用较小计算机或者PC任意形式的互联网连接，包括电线、电缆、或者Wi-Fi。计算装置1000通过网络与远程终端的通信被硬件限制。优选地，计算机1300通过网络与远程终端的通信被通过其他方式限制，例如，禁用计算机1300的操作系统中的远程连接。

[0036] 第一计算机1300被直接连接到第一分区1100的I/O模块1110。I/O模块1110能够是USB端口、eSATA、或者用于将计算装置1000连接到第一计算机1300的任意已知的通信接口。第一分区1100进一步包含通过总线1102互连的CPU1104、存储器1106、以及至少一个数据存储1108。如以上参考图3详细描述的那样，CPU 1104能够仅仅执行存储在存储器1106的程序代码地址范围以及数据存储1108上的计算机可执行代码。这借助于硬件电路，通过CPU 1104(通过本实施例其本身被保护防御恶意软件)的操作系统的控制而实现。

[0037] 在该实施例中，软件在第一计算机1300上执行，这允许CPU 1104从第一计算机1300发送和接收数据。软件允许第一计算机1300的用户将用于第一计算机1300的存储器的区域分为关键程序、关键数据文件、以及从计算装置1000接收的数据和请求。此外，该软件防止第一计算机1300的CPU将执行控制移交给具有从计算装置1000接收的文件的存储区段。用于将存储区段与执行控制分开的计算机安全的一个实例是沙箱安全机制的使用。第一分区1100通过总线1002与第二分区1200直接互连。CPU 1104能够向第二分区1200的存储

器1206的全地址范围和数据存储1208进行写入。此外，CPU 1104能够从存储器1206的全地址范围和数据存储1208读取数据，但是仅仅通过CPU 1104的“读取”命令(拉取)。通过硬件限制，CPU 1104不能接受由第二分区1200推送至其的任意数据或者其他文件。在该实施例中，在直接连接到第一分区1100的第一计算机1300上运行的软件可以请求CPU 1104从第二分区1200拉取任意数据。计算装置1000的第一分区1100被保护防御存储在第二计算机1400或者存储器1206上的任意恶意计算机可执行代码，因为CPU 1104仅仅能够执行存储在存储器1106的程序代码地址范围内和数据存储1108上的计算机可执行代码。

[0038] 在该实施例中，第一分区1100利用写入模块1112将数据写入被运行在第一计算机1300上的软件选择的用于从计算装置1000接收的数据文件的存储区段。写入模块1112包含映射第一计算机1300的存储区段的硬件电路，该存储区段被分割用于从计算装置1000接收的数据文件。示例性的硬件电路包括能够通过直接连接到计算装置1000的被授权人员的控制而被编程的现场可编程门阵列(FPGA)。在该实施例中，计算装置1000包含使能更新开关1004。使能更新开关1004包括接通位置和断开位置。使能更新开关1004的接通位置允许写入模块1112的硬件电路对用于从计算装置1000接收的数据文件的存储区段的编程。此外，使能更新开关1004的接通位置防止计算装置1000向第一计算机1300发送数据。相反地，使能更新开关1004的断开位置允许计算装置1000向运行在第一计算机1300上的软件发送数据。使能更新开关1004的断开位置防止对写入模块1112的硬件电路的非授权改变。计算装置1000和计算机1300还可以利用额外的保护开关和上述保护软件。

[0039] 在又一个实施例中，图6描绘了适合于利用具有软件解决方案的现有结构的计算装置的本发明。虽然软件解决方案可能容易受到恶意可执行计算机代码的影响，但是它能够提供上述硬件解决方案的一些益处，包括限制对关键数据文件的访问，限制程序执行访问第一计算机，并且避免将程序控制给予来自第二计算机的任意输入。在该实施例中，利用例如USB、eSATA、WiFi或者以太网的已知通信接口，第一计算机1500被连接到第二计算机1600。第一计算机1500和第二计算机1600利用本领域中已知的计算机结构，例如，x86，ARM以及PowerPC。正因为如此，第一计算机1500和第二计算机1600包含用于执行计算机可执行代码的操作系统。关键的文件和系统位于第一计算机1500上，而第二计算机1600被用于连接到互联网。该设计提供了第一计算机1500的软件以减少入侵第一计算机1500的风险的方法与第二计算机1600交互。可能由第二计算机1600从互联网接收的恶意软件被在第一计算机1500上执行的软件阻止，不能到达第一计算机1500上可执行代码的位置。

[0040] 第一计算机1500包含由在第一计算机1500上执行的常驻软件创建的虚拟分区1510。虽然虚拟分区1510能够利用第一计算机1500的一些计算资源(即CPU和存储)，但是使用本领域中已知的技术，例如软件“沙箱”，虚拟分区1510被隔离不能访问第一计算机1500的操作系统。结果，在虚拟分区1510已经被从第二计算机1600的虚拟分区1606接收的恶意计算机可执行代码感染的情况下，虚拟分区1510被限制不能感染第一计算机1500的操作系统。进一步，虚拟分区1510被限制为访问来自直接附接至第一计算机1500的输入装置和第二计算机1600的虚拟分区1606的数据。结果，虚拟分区1510被限制不能访问能够通过网络连接到远程终端的第一计算机1500的计算资源。

[0041] 在该实施例中，第一计算机1500的操作系统将第一计算机1500的一部分内存分配给虚拟分区1510。虚拟分区1510的操作系统1502被编程为仅仅执行位于虚拟分区1500的程

序代码地址块1504的程序代码。从第二计算机1600的虚拟分区1606接收的所有数据被存储在第二分区数据地址块1508中。最后，虚拟分区1510的关键数据文件被存储在第一分区数据地址块1506中。在该设计中，第一计算机1500的关键数据文件被保护防止可能已被置入第二计算机1600的恶意软件的访问。虚拟分区1510可以使用以上参考图4详细描述的进程来请求第一计算机1500的操作系统访问存储在第一计算机1500上的数据文件。第一计算机1500的操作系统可以访问分配给虚拟分区1510的内存的全地址范围。然而，由于从第二计算机1600读取的任意数据被存储在第一计算机1500的第二分区数据地址块1508中，并且第一计算机1500的操作系统被限制不能执行存储在第二分区数据地址块1508上的数据文件，因此第一计算机1500将不会执行从第二计算机1600传送的任意的恶意可执行代码。

[0042] 第二计算机1600包含由在第二计算机1600上执行的常驻软件创建的虚拟分区1606。在该实施例中，第二计算机1600通过网络被连接到远程终端。虚拟分区1606能够利用第二计算机1600的一些计算资源(即CPU和存储)。第二计算机1600的操作系统将第二计算机1600的一部分内存分配给虚拟分区1606。进一步，第二计算机1600的操作系统允许虚拟分区1602访问资源以通过网络与远程终端通信。虚拟分区1602包含能够访问并且执行程序代码/数据地址块1604的全地址范围的操作系统1602，程序代码/数据地址块1604被第二计算机1600的操作系统分配给虚拟分区1606。虚拟分区1510的操作系统1502被编程为使用拉取命令从程序代码/数据地址块1604的全地址范围读取数据。然而，通过软件限制，操作系统1502不能接受由第二计算机1600的虚拟分区1606推送至其的任意数据或者其他文件。第二计算机1600中的软件以操作系统1502要求的形式规定第一计算机1500要读取的数据的格式。第二计算机1600可能被互联网黑客潜入。如果恶意软件改变了被提供给第一计算机1500的数据格式，那么操作系统1502将不会接受不正确的格式的数据。此外，该软件可以利用以上参考图4详细描述的进程，用于第一计算机从第二计算机获取数据。

[0043] 虽然图6中公开的实施例利用虚拟环境保护第一计算机的程序和数据以防御恶意计算机可执行代码，但是公开的技术(即限制对关键数据文件的访问，限制程序执行访问第一计算机，并且避免将程序控制给予来自第二计算机的任意输入的软件)可以被直接应用于第一和第二计算机的操作系统而不用虚拟环境的使用。在任何情况下，这样的实施例能够减少入侵的风险，但是不能提供利用硬件以及软件保护的优选实施例中的全集成系统给予的增强的保护。

[0044] 虽然已经参考被非常详细地陈述用于进行本发明的完整公开目的的优选实施例来初步描述了本发明，论述的优选实施例及其他实施例仅仅是示例性的并且不意欲限制或者代表本发明的所有方面的穷举。进一步，可以在不背离本发明的精神和原则的情况下，在细节上进行很多改变，这对本领域的技术人员将是显而易见的。应当理解的是在不背离本发明基本特征的情况下，本发明能够以其他的形式被具体化。

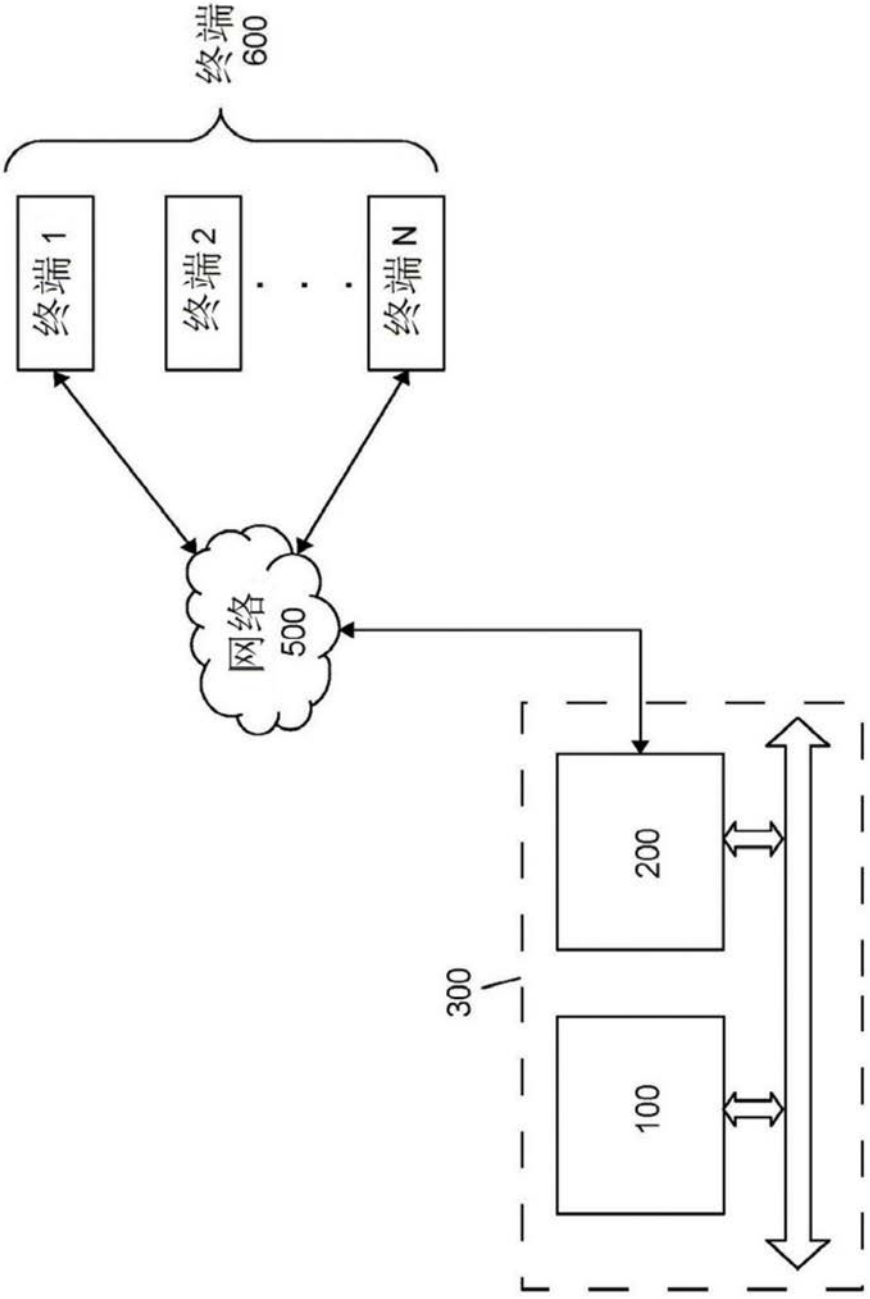


图1

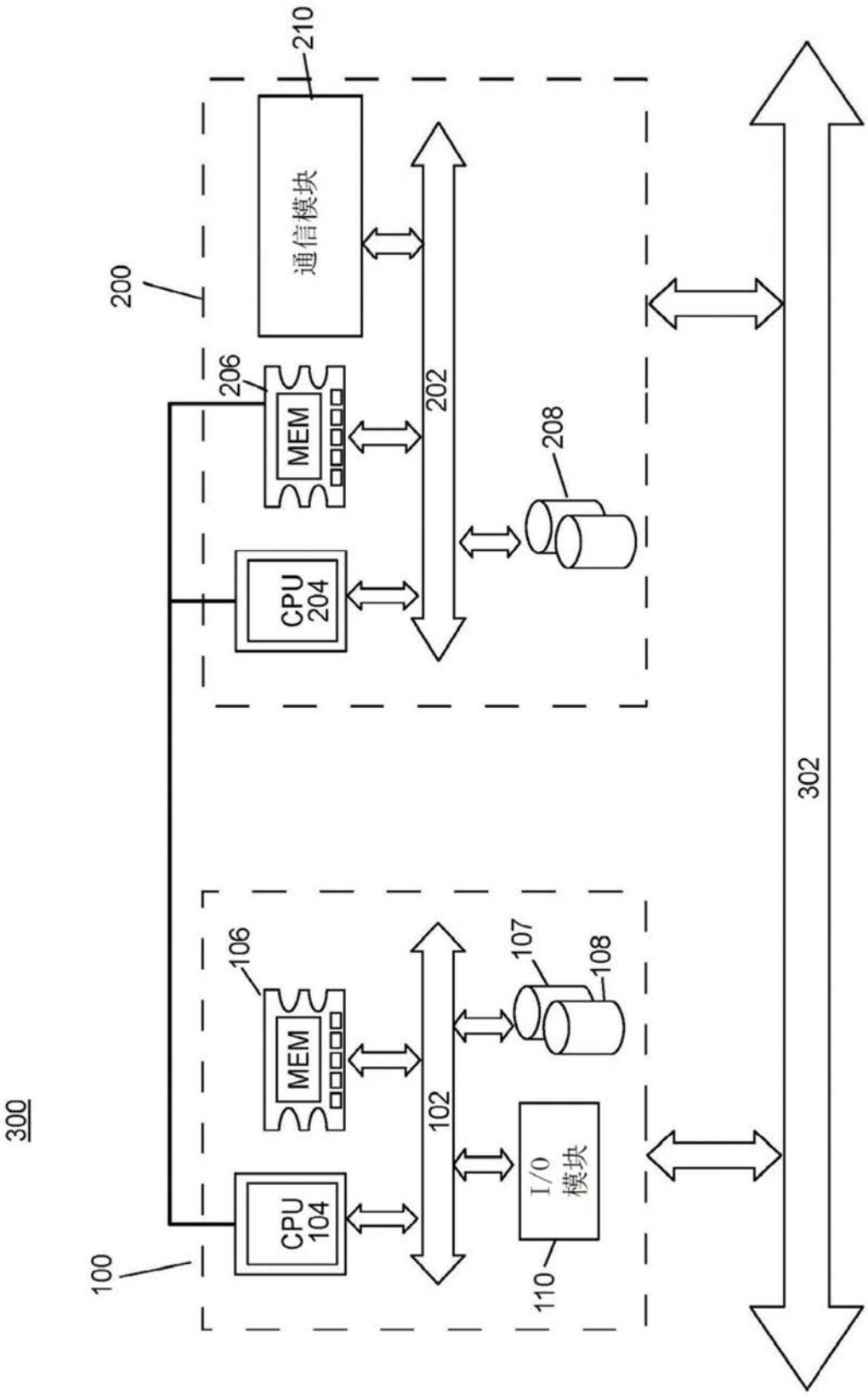

300
100
CPU 104
MEM
106
102
I/O 模块
110
107
108
200
CPU 204
MEM
206
202
208
通信模块
210
302

图2

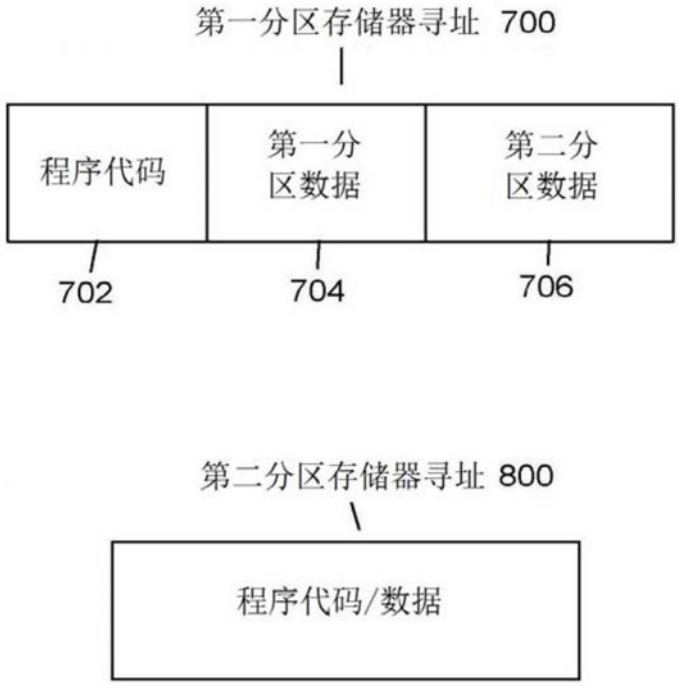

第一分区存储器寻址 700
程序代码
第一分区数据
第二分区数据
702
704
706
第二分区存储器寻址 800
程序代码/数据

图3

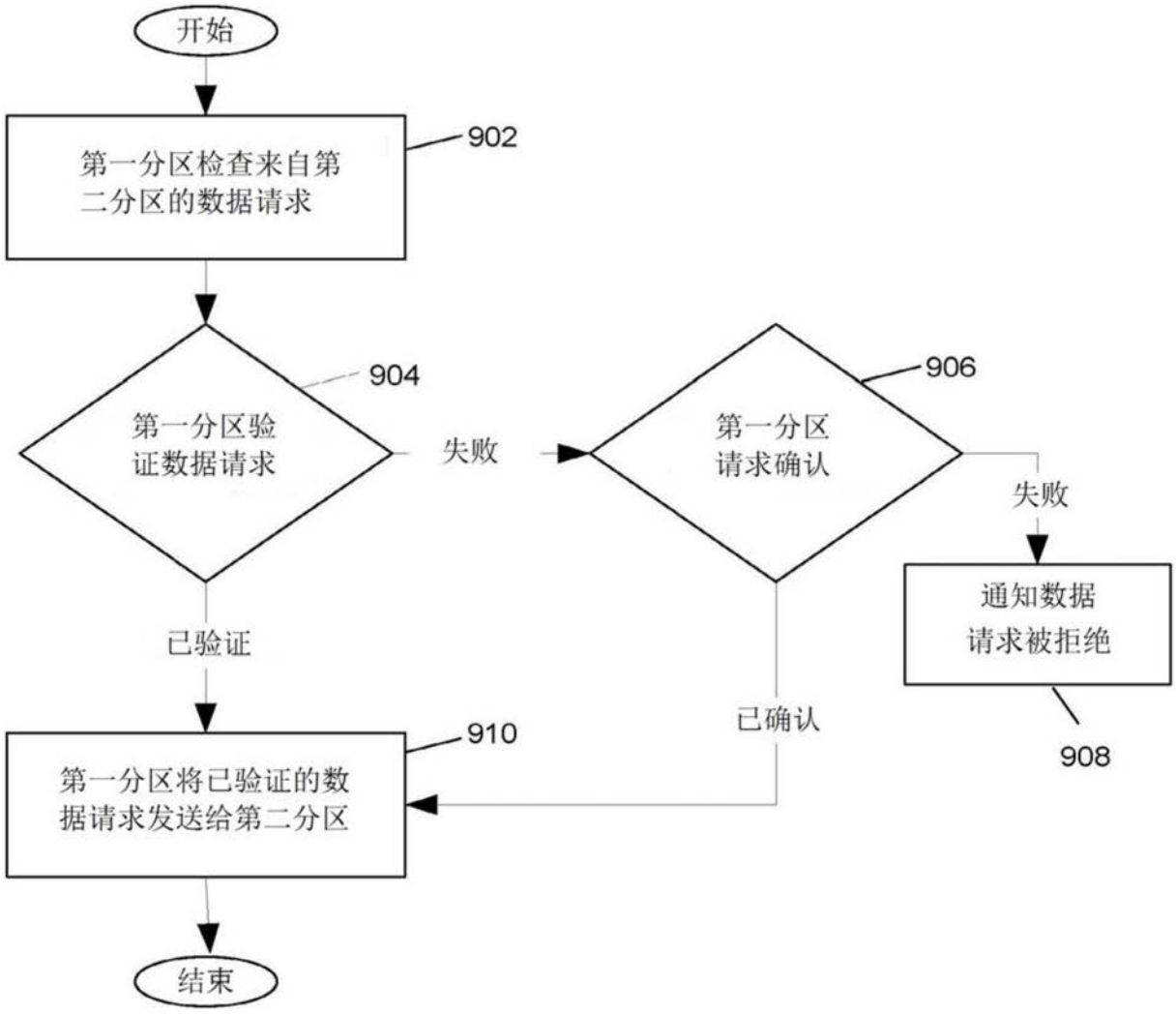

开始
第一分区检查来自第二分区的数据请求
902
第一分区验证数据请求
904
失败
第一分区请求确认
906
失败
通知数据请求被拒绝
908
已验证
已确认
第一分区将已验证的数据请求发送给第二分区
910
结束

图4

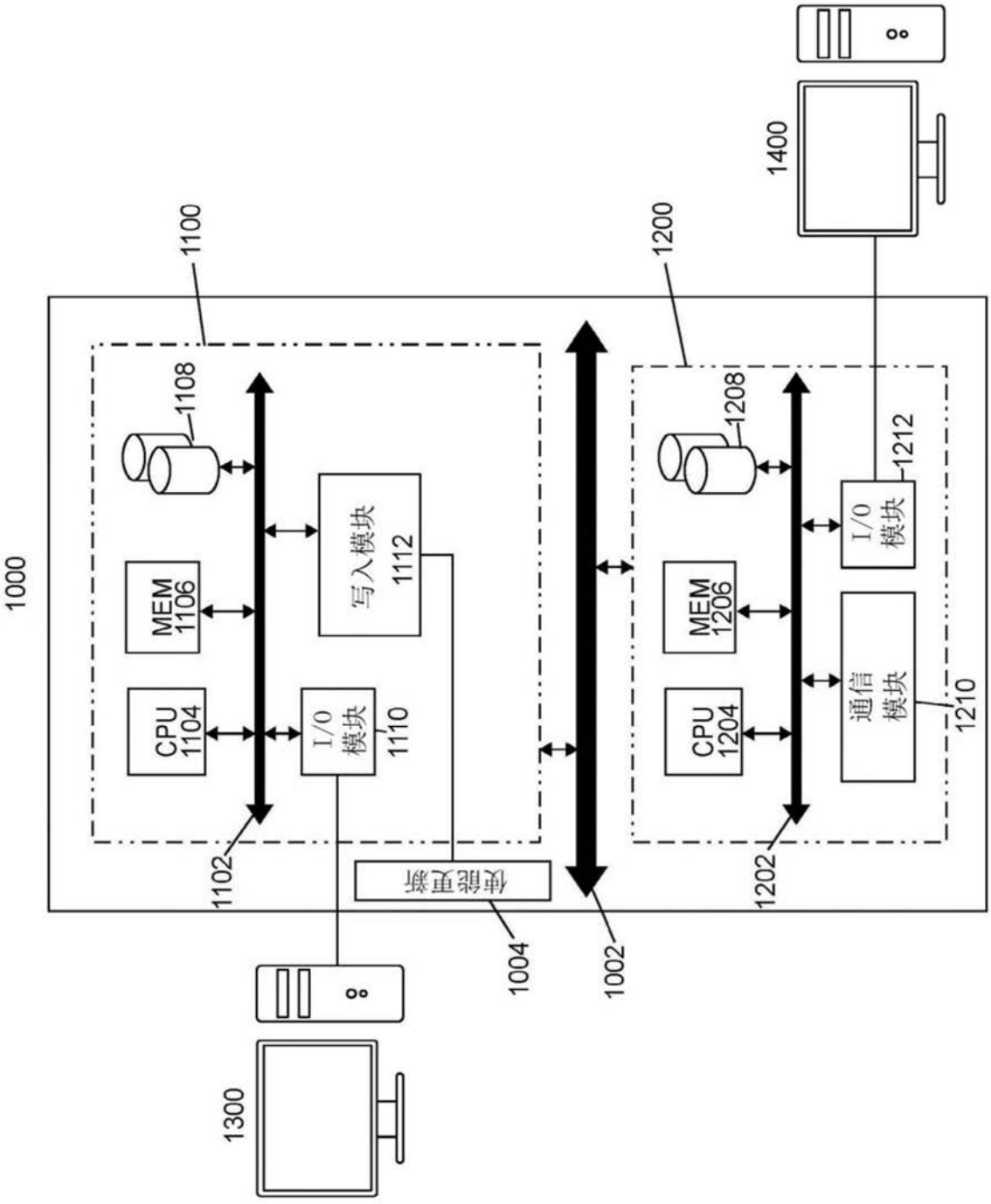

1000
1100
1102
1108
MEM 1106
CPU 1104
I/O 模块 1110
写入模块 1112
1200
1202
1208
MEM 1206
CPU 1204
I/O 模块 1212
通信模块 1210
1400
1300
1002
1004
使能更新

图5

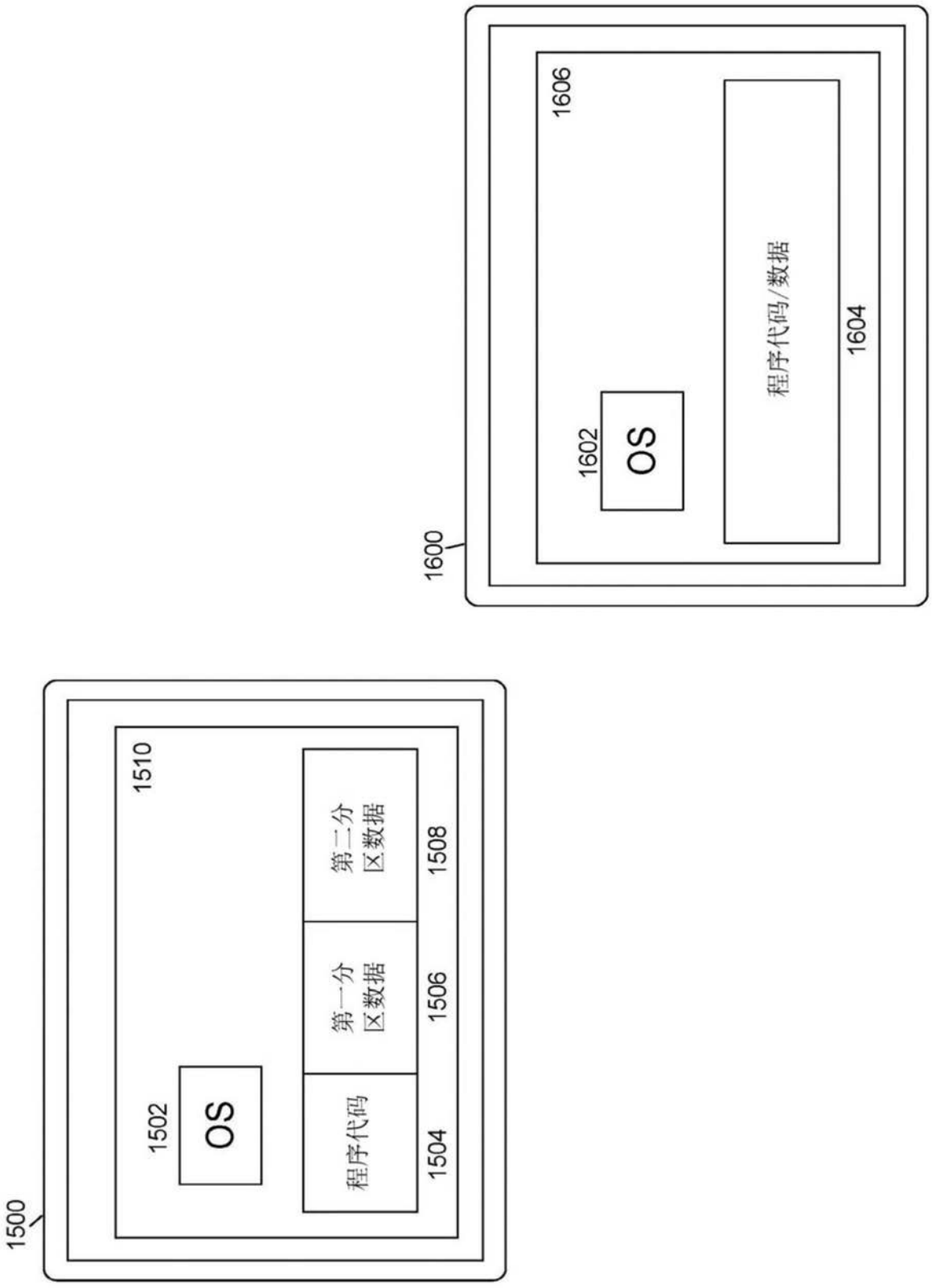

1600
1606
1602
OS
程序代码/数据
1604
1500
1510
1502
OS
程序代码
1504
第一分区数据
1506
第二分区数据
1508

图6