(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 107660332 B
(45)授权公告日 2021.05.28

(21)申请号 201680026950.9
(22)申请日 2016.05.31
(65)同一申请的已公布的文献号
申请公布号 CN 107660332 A
(43)申请公布日 2018.02.02
(30)优先权数据
62/172,968 2015.06.09 US
14/863,496 2015.09.24 US
(85)PCT国际申请进入国家阶段日
2017.11.09
(86)PCT国际申请的申请数据
PCT/US2016/035078 2016.05.31
(87)PCT国际申请的公布数据
WO2016/200644 EN 2016.12.15
(73)专利权人 英特尔公司
地址 美国加利福尼亚
(72)发明人 N·黑尔特-谢勒 N·M·史密斯
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
US 2012042362 A1,2012.02.16
US 2002029349 A1,2002.03.07
CN 101808420 A,2010.08.18
CN 101945370 A,2011.01.12
CN 102404726 A,2012.04.04
CN 103364365 A,2013.10.23
CN 101097526 A,2008.01.02
CN 103313343 A,2013.09.18
US 2014123276 A1,2014.05.01
审查员 程杰

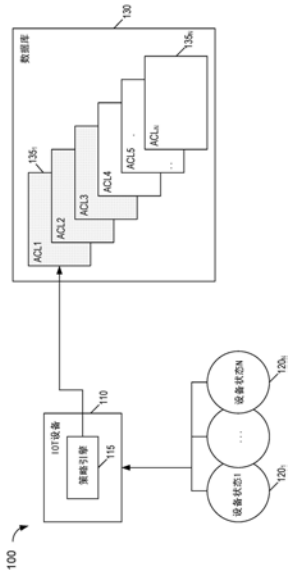
权利要求书2页 说明书10页 附图9页

(54)发明名称

用于控制数据在设备中的有状态的应用的系统、装置和方法

(57)摘要

在一个实施例中，系统包括具有用于在可信执行环境中执行的第一逻辑的处理器，以及用于存储多个访问控制策略的存储器，多个访问控制策略中的每个访问控制策略与系统的复合设备状态相关联，并且包括针对要由第一逻辑保护的资源的访问策略，其中，第一逻辑用于响应于一个或多个访问控制策略的相关联的复合设备状态与系统的当前复合设备状态匹配，而将多个访问控制策略中的一个或多个访问控制策略应用于对资源进行访问的请求。描述并要求保护其他实施例。



CN 107660332 B

1.一种用于执行访问控制策略的设备,包括:

处理器,其用于执行指令;以及

策略逻辑,其用于从耦合到所述设备的请求者接收对要由所述设备保护的资源进行访问的请求,其中,所述策略逻辑用于访问与所述资源相关联的控制数据,所述控制数据具有第一值的第一设备状态字段以指示所述设备的设备状态,所述策略逻辑用于借助所述第一值来确定所述设备是否处于匹配于所述控制数据的相关联的复合设备状态的所述设备的当前复合设备状态,并且如果是,则应用所述控制数据的访问策略来确定是否准许允许所述请求者对所述资源进行访问的所述请求,其中,所述控制数据包括访问控制列表,所述访问控制列表包括多个设备状态字段,每个设备状态字段具有第一值或第二值中的一个,所述第一值用于指示所述设备的当前复合设备状态的对应的设备状态因子是有效的,所述第二值用于指示所述设备的当前复合设备状态的对应的设备状态因子是无效的,并且其中,所述策略逻辑用于访问索引数据库以执行所述匹配,所述索引数据库具有多个条目,每个条目与多个控制数据中的一个相关联并且存储针对所述多个设备状态字段的所述第一值或所述第二值。

2.根据权利要求1所述的设备,其中,所述多个设备状态字段中的一个设备状态字段包括所述设备的操作临界度状态。

3.根据权利要求1所述的设备,其中,所述多个设备状态字段中的一个设备状态字段包括所述设备的操作优化目标。

4.根据权利要求1所述的设备,其中,所述策略逻辑用于接收多个设备状态输入,并且确定所述多个设备状态输入中的每个设备状态输入是否与存储在所述控制数据的所述多个设备状态字段中的对应的一个设备状态字段中的值匹配。

5.根据权利要求4所述的设备,其中,所述多个设备状态输入中的至少一个设备状态输入是从经由网络耦合到所述设备的一个或多个第二设备接收的。

6.根据权利要求1所述的设备,其中,所述控制数据包括至少一个状态向量,所述至少一个状态向量包括多个字段,每个字段用于设备状态因子,并且指示当所述设备状态因子在所述设备中有效时所述控制数据的访问策略是否要被应用。

7.根据权利要求1所述的设备,还包括用于存储所述索引数据库的存储装置。

8.根据权利要求1所述的设备,还包括用于存储所述多个控制数据的存储装置,其中,所述策略逻辑基于所述设备的当前复合设备状态来从网络的权威策略存储装置获得多个控制数据。

9.根据权利要求8所述的设备,其中,所述策略逻辑用于响应于对所述当前复合设备状态进行的改变而逐出所述多个控制数据中的一个或多个控制数据。

10.根据权利要求1所述的设备,其中,所述策略逻辑用于基于所述设备的设备状态来预过滤多个控制数据,以及基于所述预过滤的结果来访问所述控制数据。

11.一种用于执行访问控制的方法,包括:

确定系统的当前复合设备状态,所述系统包括物联网(IoT)设备;

确定当所述系统处于基于访问控制列表的相关联的复合设备状态而确定的当前复合设备状态时,与资源相关联的所述访问控制列表是否要被应用,所述访问控制列表包括多个设备状态字段,每个设备状态字段具有第一值或第二值中的一个,所述第一值用于指示

所述系统的当前复合设备状态的对应的设备状态因子是有效的，所述第二值用于指示所述系统的当前复合设备状态的对应的设备状态因子是无效的，所述确定基于对索引数据库的访问，所述索引数据库具有多个条目，每个条目与多个访问控制列表中的一个相关联并且存储针对所述多个设备状态字段的所述第一值或所述第二值；以及

如果确定当所述系统处于所确定的设备状态时所述访问控制列表要被应用，则基于所述访问控制列表来确定与所述系统耦合的请求者是否被准许对所述资源进行访问，否则阻止由所述请求者访问而不对所述访问控制列表进行进一步应用。

12.根据权利要求11所述的方法，还包括响应于所述系统的设备状态改变，而请求所述访问控制列表并且从位于所述系统远处的权威策略存储装置获得所述访问控制列表。

13.根据权利要求11所述的方法，还包括对与所述资源相关联的多个访问控制列表进行访问，所述多个访问控制列表中的每个访问控制列表包括与所述系统的复合设备状态匹配的复合设备状态。

14.根据权利要求13所述的方法，还包括响应于对所述复合设备状态进行的改变，而从所述系统的存储装置中逐出所述多个访问控制列表中的一个或多个访问控制列表。

15.根据权利要求13所述的方法，还包括基于所访问的多个访问控制列表中的至少一些来准许所述请求者对所述资源的访问。

16.一种机器可读存储介质，包括机器可读指令，所述机器可读指令当被处理器执行时，实现根据权利要求11至15中任一项所述的方法。

17.一种用于执行访问控制的系统，包括：

处理器，其具有用于在可信执行环境中执行的第一逻辑；以及

存储装置，其用于存储多个访问控制策略，所述多个访问控制策略中的每个访问控制策略与所述系统的复合设备状态相关联，并且包括针对要由所述第一逻辑保护的资源的访问策略，其中，所述第一逻辑用于响应于一个或多个访问控制策略的相关联的复合设备状态与所述系统的当前复合设备状态匹配，而将所述多个访问控制策略中的一个或多个访问控制策略应用于对所述资源进行访问的请求，其中，与第一访问控制策略相关联的所述复合设备状态包括多个设备状态字段，每个设备状态字段具有第一值或第二值中的一个，所述第一值指示所述系统的当前复合设备状态的对应设备状态因子是有效的，所述第二值指示所述系统的当前复合设备状态的对应设备状态因子是无效的，其中，所述存储装置还用于存储具有多个条目的索引数据库，每个条目与所述多个访问控制策略中的一个访问控制策略相关联，并且用于存储所述多个设备状态字段的所述第一值或所述第二值，所述第一逻辑用于访问所述索引数据库以执行所述匹配。

18.根据权利要求17所述的系统，还包括多个传感器，所述多个传感器用于提供所述当前复合设备状态的一个或多个设备状态因子，其中，所述多个传感器中的至少一个传感器经由控制信道被耦合到所述处理器以提供所述一个或多个设备状态因子。

19.一种用于执行访问控制的系统，包括用于实现根据权利要求11至15中任一项所述的方法的模块。

用于控制数据在设备中的有状态的应用的系统、装置和方法

背景技术

[0001] 物联网(IoT)系统平衡有时在安全性、保障性、弹性、以及可用性之间存在冲突的权衡。例如,在正常操作条件下,传感器、控制器、以及致动器的可用性可能是至关重要的。系统目标可能会随着连接的IoT设备的给定操作状态改变而改变。IoTivity是Linux基础开源示例IoT框架,其中安全集成是中心设计目标。IoT框架设计者面临的主要挑战是IoT设备如何可以利用访问控制列表(ACL)、证书、密钥、或其他数据来实现预期的系统行为目标。

附图说明

[0002] 图1是根据本发明的实施例的环境的框图。

[0003] 图2A是根据本发明的实施例的包括访问控制列表的数据库的框图。

[0004] 图2B是根据本发明的实施例的访问控制列表的框图。

[0005] 图2C是根据本发明的实施例的另一访问控制列表的框图。

[0006] 图3是根据本发明的实施例的方法的流程图。

[0007] 图4是根据本发明的另一实施例的方法的流程图。

[0008] 图5是实施例可以与其一起使用的示例系统的框图。

[0009] 图6是根据本发明的另一实施例的系统的框图。

[0010] 图7是根据另一实施例的可穿戴模块的框图。

具体实施方式

[0011] 在各种实施例中,诸如IoT设备的计算设备可以以各种设备状态中的给定状态进行操作。在一些情况下,这种设备状态可以采取复合设备状态的形式,在复合设备状态中多个单独的设备状态因子共同形成设备的复合或最终设备状态。根据上下文应理解,如本文使用的术语“设备状态”可以指示这种共同最终设备状态,或者可以指示多个这种设备状态因子中的单个设备状态因子。如下面将描述的,安全策略决策可以考虑这样的设备状态:其中当应用特定访问控制策略时设备正在操作。这种操作是通过将状态信息(即,设备状态信息)包括在要由设备处理和/或传送的各种不同类型的控制数据中来实现的。应理解,如本文所使用的,“控制数据”可以指示关于安全策略的各种信息类型,包括但不限于访问控制列表(ACL)、证书、密钥等。

[0012] 应理解,可以被包括在设备状态中的信息的类型可以采取许多不同的形式。在示例实施例中,不同类别的设备状态是可能的。更具体地,在一个实施例中,一种设备状态类别可以涉及可管理性状态,例如,设备配置状态,其示例将在下文讨论。另一设备状态类别可以包括操作和控制状态(包括但不限于安全相关的状态)。另一设备状态类别可以包括分类法相关的状态,例如,本地/远程、设备类型、当前部件等。当然应理解,在其他实施例中,可以将许多其他不同类型的信息编码为设备状态字段或因子。

[0013] 在缺少如本文描述的状态信息的情况下对控制数据进行正确且完整地定义可能是困难且容易出错的任务,特别是因为系统行为目标可以基于IoT设备状态而改变。例如,

当车辆运动时，可以禁用允许汽车经销商重置某些车载娱乐信息(IVI)IoT设备的ACL。在另一示例中，只有当IoT温度传感器确定其接近或低于冰点时，公司才可以允许除雪机服务打开其IoT前门。在第三示例中，当连接的IoT烟雾报警器检测到建筑物中的危险烟雾等级时，IoT门锁可以允许应急人员进入。

[0014] 实施例可以通过将明确的状态信息并入到现有控制数据来增强安全性和IoT设备行为，以使得特定控制目标何时意图应用于设备并且不意图应用于设备是清楚且确定的。这不仅实现对控制数据的更丰富的定义，而且还可以简化控制数据制作者对潜在设备状态的理解。另外，下面描述了另外的功率/性能优点。

[0015] 在各种实施例中，可以通过利用状态信息明确地标注控制数据来将IoT设备控制数据映射到现有设备状态信息上，在一个实施例中，状态信息可以作为一个或多个状态标志被包含。当IoT设备做出策略决策(例如，是否允许访问特定请求者)时，在将控制数据应用于策略决策之前，针对设备状态来检查附接到控制数据或包含于控制数据的状态标志(其中设备状态可以包括一组连接的设备中的一个或多个设备的状态以及本地设备状态)。

[0016] 实施例提供了IoT控制数据描述，包括将设备状态映射到控制数据数据库中。利用实施例，可以实现以下：以直接且直观的方式对IoT设备进行的复杂系统行为进行正确描述；数据制作者可以具有对要考虑的设备状态可能性的简明描述，这改进了正确描述预期行为的能力；以及设备行为在被部署时可以是明确且确定的，减少了设备软件错误应用控制数据的可能性。

[0017] 在IoTivity IoT框架中，控制数据由安全资源管理器模块(SRM)来应用，安全资源管理器模块(SRM)在本文中也称为策略引擎。SRM加载控制数据的数据库。控制数据数据库由SRM应用以过滤传入的请求，并且准许(或拒绝)访问。

[0018] 表达为ACL的控制数据可以具有多个状态信息向量。例如，许多ACL结构包括“日期/时间”状态向量，指定其中ACL有效的时间窗。实施例提供包括操作临界度状态的附加状态向量。可能存在多个级别的临界度，其范围从低临界度到高临界度。也可以列举中间临界度级别。此外，可以在操作优化目标方面表达操作状态，其中可以针对性能优化当前操作状态，同时可以针对功率优化第二操作目标。附加的操作目标可以针对安全性、弹性、可用性等进行优化。

[0019] 在一些实施例中，各种状态(时间、临界度、操作等)不是相互排斥的，并且因此可以彼此组合地应用。对于每个有效的组合，存在设备拥有的单个最终状态和关联于该状态的控制数据元素(例如，ACL)。因此，安全性可以一致且正确地应用于每个定义的设备状态处。

[0020] 利用实施例，控制数据是自描述的，以使得SRM的策略引擎不需要关于何时应用控制数据做出复杂且容易出错的决策。只有当设备处于适当的状态时，控制数据上的明确标志才可以启用该数据，而策略引擎不必解释和实现预期的系统行为。

[0021] 经常受约束的IoT设备可以使用控制数据上的设备状态(例如，标志)针对功率和性能做出简单的优化决策。例如，不频繁地改变控制状态的设备(例如，灯泡)可以选择仅将应用于其当前状态的那些控制数据加载到其本地存储器中。考虑到可能仅应用于异常状态的数据量以及IoT设备的高度受约束的性质，这些节省可能是意义重大的。

[0022] 也就是说，在实施例中，受约束的IoT设备(例如，具有相对有限量的处理和存储能

力的设备)可以被配置为存储相对小的一组ACL或其他控制数据。即,在上面的示例中,这种受约束的设备可以被配置为存储与当前设备状态匹配的一个或几个ACL。应理解,在这种情况下,可以应用于设备的附加ACL可以存储在权威策略存储装置中,例如,与远程访问管理器服务(AMS)或其他实体相关联。此外,通过登载有限数量的ACL,可以以更高的性能水平来执行安全策略确定。作为示例,安全策略操作包括匹配功能以确定哪些本地存储的ACL(如果有的话)可应用于给定请求,可以快速且高效地分析索引数据库以确定匹配的ACL,索引数据库存储本地存储的ACL的可应用设备状态的表示。注意,该索引数据库还可以存储在设备中(并且在设备状态改变时进行更新)以便易于访问,以响应于接收到对资源进行访问的请求而识别匹配的ACL。然后可以对这种匹配的ACL进行访问和处理/分析,以将其中的访问策略应用于请求。在实施例中,SRM可以通过对ACL内容进行引用完整性检查审查这些匹配的ACL。如果发现冲突的ACL策略(即,第一ACL与定义资源R1的许可P1的主体S1匹配,而第二ACL识别S1和R1但指定不同的许可P2),则SRM将这些ACL标记为冲突的并寻求解决方案。在实施例中,SRM评估逻辑将通过选择由P1和P2准许的最小权限来确保安全性不被损害(即使发现冲突的ACL)。例如,P1和P2的交集是准许的权限,或者没有任何许可被准许。

[0023] 在这样的实施例中,当设备状态改变时,本地存储的ACL可以从本地设备页入(page in)和页出(page out)到安全策略存储层级的另外的部分。在这样的示例中,与当前设备状态匹配的ACL可以存储在本地,而先前设备状态的ACL可以存储在中间高速缓存中,例如,与位于IoT网络的公共部分的中间设备(例如,主控制器或次控制器)相关联的ACL高速缓存。相反,相对不频繁地活动的设备状态和匹配的ACL可以存储在更远处,在权威安全策略存储装置中。应理解,在一些情况下,除了本地存储与当前设备状态匹配的ACL之外,一个或多个可能不与当前设备状态匹配但与设备的临界操作相关联的临界ACL也可以存储在本地。

[0024] 因此,如在控制数据内表示的设备状态(例如,ACL)可以用作预过滤器,以确定对于访问给定资源的特定请求而言哪组控制数据是可应用的。基于当前设备状态与控制数据中表示的设备状态的匹配而执行的这种预过滤操作可以生成较小的一组控制数据(例如,ACL),该较小的一组控制数据随后由策略引擎或其他逻辑应用,以确定是否准许对资源进行访问的给定请求。

[0025] 现在参考图1,示出了环境100,其可以是根据本发明的实施例的IoT网络的一部分。如所示出的,环境100包括耦合到数据库130的IoT设备110。在实施例中,数据库130可以存储在设备110的存储装置中。在其他情况下,设备110可以与数据库130无线地通信,例如,经由本地或短距离无线区域网络,其中数据库130可以是策略高速缓存层级的一部分,其可以在耦合到设备110的主控制器或次控制器中实现。另外,在其他情况下,数据库130可以与IoT网络的更远部分(例如,AMS)相关联。注意,这样的AMS可以位于IoT设备110远处,并且可以经由一个或多个中间设备(例如,主控制器和/或次控制器)耦合到IoT设备110。

[0026] 为了执行安全策略检查,IoT设备110包括策略引擎115(其在实施例中可以实现SRM)。在实施例中,策略引擎115可以在IoT设备的安全环境中实现,例如,可信执行环境(TEE)。在各种实施例中,可以经由硬件电路、软件、和/或固件的组合来实现TEE和策略引擎115。更具体地,策略引擎115可以被配置为接收来自给定请求者的对特定受保护资源(为了便于说明而未示出)的传入访问请求并对其进行处理。虽然本发明的范围不限于此方面,但

是这种受保护资源可以是IoT设备110的内部资源，例如，存储在IoT设备的特定存储装置中的信息。在其他情况下，IoT设备110可以针对外部资源(例如，IoT网络内的各种传感器、致动器、或其他设备，并且设备110保护对其的访问)执行安全策略决策。

[0027] 为了确定是否针对对应的请求准许访问，策略引擎115可以寻求访问一个或多个控制数据(例如，一个或多个ACL)的信息。具体如图1所示，在数据库130中存在多个ACL 135_1-135_n。在实施例中，每个ACL可以与要被保护的一个或多个特定资源和/或寻求访问所请求的资源的一个或多个特定请求者相关联。

[0028] 为了简化安全策略，改进性能并潜在地降低功耗，作为安全策略执行机制中的初始操作，实施例可以基于设备状态来确定是否应用一个或多个安全策略。如图1所示，IoT设备110接收多个设备状态输入120_1-120_n。每个这种输入可以提供设备110或者IoT网络内的另一设备的设备状态因子。利用设备状态信息，策略引擎115可以首先基于所确定的(例如，复合的)当前设备状态来确定是否应用给定的控制数据(例如，ACL)。因此，如图1所示，对于ACL 135_1-135_n，只有有限数量的ACL可以潜在地应用于当前设备状态(例如，阴影ACL)。以这种方式，可以更高效地做出安全策略决策。

[0029] 现在参考图2A，示出了根据本发明的实施例的包括若干访问控制列表的数据库的框图。如图2A所示，可以在系统的存储装置内实现的数据库200包括ACL 212和214。应理解，ACL可以在网络制作工具的用户接口中示出，以使得终端用户能够通过生成这些ACL(并且组成可应用的设备状态)来确定安全策略。注意，为了易于说明，仅示出了两个这样的ACL 212和214。在图2A的视图中，每个ACL包括名称字段215，其可以用于标识对应的ACL。另外，示出了多个设备状态字段216_0-216n。应理解，虽然为了说明的目的而示出了特定的字段，但在其他实施例中可以存在更多的且不同的字段。如本文描述的，这些字段216可以包含于给定ACL中或与给定ACL相关联。

[0030] 如所示出的，与给定设备状态相关联的每个字段216可以处于以下两种状态之一，即置位状态(如利用“X”示出的)以及重置或逻辑零状态(图2A所示的“空白”字段)，置位状态在ACL内可以被表示为逻辑高或逻辑一值。注意，这些字段可以由控制数据制作者设置，以指示当设备处于给定状态时是否应用对应的ACL。

[0031] 如图2A所示，可能的设备状态包括：操作状态(isOp)，其用于指示当设备处于操作状态时是否应用ACL；拥有状态(isOwned)，其用于指示当设备被识别为由特定所有者拥有时是否应用ACL；预备状态(isProv)，其用于指示当已经对设备进行预备时是否应用ACL；秘钥状态(hasKeys)，其用于指示当设备具有存在于设备中的一个或多个特定秘钥时是否应用ACL；重置状态(inReset)，其用于指示当设备处于重置状态时是否应用ACL；连接状态(isConnect)，其用于指示当设备在特定IoT网络中连接时是否应用ACL；错误状态(inError)，其用于指示当设备处于错误状态时是否应用ACL；以及紧急状态(inEmergency)，其用于指示当设备处于紧急状态时是否应用ACL。参考ACL 212，注意，如果设备处于操作状态、拥有状态、预备状态、密钥状态、以及连接状态中的全部，则应用该访问控制列表。相反，如果设备被指示为处于重置状态、错误状态、或紧急状态中的任何一个，则不应用ACL 212。

[0032] 如图2B所示，示出了根据实施例的访问控制列表的细节。在图2B中，ACL 212提供用于两个资源(即，恒温器资源222和主入口资源224)的控制数据，其可以由网络制作工具

提供给保护这些资源的特定IoT设备，这些资源可以是实体的要由该ACL保护的资源。另外，ACL向特定请求者提供许可准许的指示，如请求者字段226_0-226_n所指示的。每个这种字段226指示特定资源的请求者被准许的许可(如果有的话)的类型。因此，例如，如所示出的，安全人员可以对恒温器222和主入口224具有完全控制。类似的字段存在于图2C的ACL 214中。

[0033] 现在参考图3，示出了根据本发明的实施例的方法的流程图。更具体地，方法300可以由给定设备的策略引擎执行，该策略引擎可以在设备的TEE中实现。如图所示，方法300开始于接收对第一资源的访问请求(框310)。应理解，可以从寻求对资源的访问的给定请求者接收该访问请求，资源可以在设备内部或外部。接下来在框320处，对设备状态进行确定。应理解，该设备状态可以是设备的各种不同设备状态因子的复合状态(并且其在一些实施例中可以进一步包括在IoT网络中与该设备耦合的一个或多个其他设备的设备状态)。接下来在框330处，可以获得针对第一资源的访问控制策略(例如，ACL)。注意，该访问控制策略可以是存储在本地的，或者可以从远程位置访问。在其他情况下，可以获得与安全策略确定相关的多个ACL。

[0034] 接下来在菱形340处，确定设备是否处于访问控制策略中所指示的设备状态(或多个状态)。对于多因子设备状态情况，该确定可以指示是否满足在设备状态向量中指示的所有设置设备状态或访问控制策略的置位设备字段是否被满足(例如，存在/真/激活)。如果否，则控制传递到框350，在框350处拒绝对第一资源的访问(而不进一步将请求应用于访问控制策略)。

[0035] 相反，如果在菱形340处确定设备处于所指示的(多个)设备状态，则控制传递到框360，在框360处可以确定访问控制策略的访问策略。该确定可以包括识别请求者并且确定要向这种请求者准许(或不准许)的对资源的访问的类型。因此，在菱形370处，确定访问策略是否允许请求者所请求的访问。如果否，则控制传递回上面讨论的框350。否则，控制传递到框380，在框380处可以准许对第一请求的访问。应理解，虽然在图3的实施例中以此高级别示出，但是许多变化和替代是可能的。

[0036] 如上面讨论的，在一些情况下，例如在受约束的IoT设备的上下文中，可以使用设备状态来实现仅有限量的与特定IoT设备相关联的控制数据的本地存储。在这种情况下，可以将IoT设备配置为基于当前设备状态来页入和页出诸如ACL的控制数据。

[0037] 现在参考图4，示出了根据本发明的另一实施例的方法的流程图。如图4所示，方法400可以在受约束的IoT设备内实现，以实现对有限量的本地ACL或其他控制数据的高效存储和访问。作为示例，在受约束的IoT设备的TEE内执行的策略引擎可以执行方法400。如图所示，方法400开始于确定是否已发生设备状态改变(菱形410)。如果是，则控制传递到框420，在框420处可以针对受约束的设备确定新的复合设备状态。更具体地，可以对各种设备状态字段或因子进行分析以确定复合设备状态。然后，在框430处，可以逐出与旧的设备状态相关联的任何本地存储的ACP(例如，逐出到策略存储高速缓存层级的更远部分)。注意，在一些情况下，一个或多个其他安全策略(例如，临界安全策略)可以继续存储在本地，即使这种策略与新的复合设备状态不相关联，以使得该策略可以存在，而不管连接条件。

[0038] 接下来，在框440处，可以请求具有新的复合设备状态的一个或多个ACP。在实施例中，可以对位于IoT设备远处的AMS做出该请求。在其他情况下，该请求可以通过安全策略存储层级来进行，安全策略存储层级可以包括IoT设备与权威策略存储提供方(例如，AMS)之

间的一个或多个中间设备。

[0039] 仍然参考图4，接下来在框450处，可以接收并本地存储具有新的复合设备状态的一个或多个ACP。最后，在框460处，可以接收传入的访问请求并基于所存储的ACP对其进行处理。应理解，虽然在图4的实施例中以此高级别示出，但是许多变化和替代是可能的。

[0040] 实施例还可以具有控制数据制作的含义。IoT设备控制数据制作工具可以将所有已知的设备状态变量公开为对其本身或其他(多个)IoT设备启用控制数据对象的标志。作为示例，图2B和图2C的ACL可以使用根据实施例的示例制作工具的用户接口来呈现(并生成)，并且使用图2A所示的设备状态来进行门控或预过滤。以这种方式，策略制作者可以对定义的控制数据将导致预期的系统行为具有更高的置信度。

[0041] 在诸如IoTivity的实现方式中，存在设备可以对输入状态变得感知的各种方式。例如，对于ACL有效期，使用时钟。类似地，对于临界度状态，温度、压力、湿度、空气质量、能量流等可以通知该类状态。操作优化状态可以由电池充电传感器、运动、加速度、功率的效用成本、通信资源等来通知。所有这些输入可以通过对通知和直接状态转换进行推断来融合或组合。然后，这些状态成为到控制数据制作过程中的一组输入，减轻了策略引擎(其对控制数据进行应用)对在设备状态与控制目标之间做出复杂推断的需求。

[0042] 使用实施例，IoT设备可以具有更高质量的控制数据，针对IoT设备产生更好的用户体验。另外，受约束的IoT设备可以具有改进的存储器占用区和工作集大小，产生改进的功率/性能和/或减少的材料清单(BoM)成本。

[0043] 现在参考图5，示出了实施例可以与其一起使用的示例系统的框图。如图所示，系统900可以是智能电话或其他无线通信器或任何其他IoT设备。基带处理器905被配置为关于要从系统发送或由系统接收的通信信号来执行各种信号处理。接下来，基带处理器905耦合到应用处理器910，该应用处理器910可以是系统的主CPU，除了诸如许多公知的社交媒体和多媒体应用的用户应用之外，应用处理器910还用于执行OS和其他系统软件。应用处理器910还可以被配置为执行设备的各种其他计算操作。

[0044] 接下来，应用处理器910可以耦合到用户接口/显示器920，例如，触摸屏显示器。另外，应用处理器910可以耦合到存储器系统，其包括非易失性存储器(即，闪速存储器930)和系统存储器(即，DRAM 935)。在一些实施例中，闪速存储器930可以包括安全部分932，在其中可以存储秘密和其他敏感信息。如进一步示出的，应用处理器910还耦合到捕获设备945，例如，可以记录视频和/或静止图像的一个或多个图像捕获设备。

[0045] 仍然参考图5，通用集成电路卡(UICC)940包括订户身份模块，其在一些实施例中包括用于存储安全用户信息的安全存储装置942。系统900还可以包括安全处理器950，其可以实现如较早描述的TEE，并且其可以耦合到应用处理器910。此外，应用处理器910可以实现安全操作模式，例如，用于给定指令集架构和电路的Intel®软件保护扩展(SGX)，以用于托管TEE。包括一个或多个多轴加速度计的多个传感器925可以耦合到应用处理器910，以使得能够输入各种感测到的信息，例如，运动和其他环境信息。另外，一个或多个认证设备995可以用于接收例如在认证操作中使用的用户生物计量输入。

[0046] 注意，一个或多个推理引擎可以在处理器910和/或各种控制器和协处理器中实现，例如，基带处理器905、安全处理器950、传感器925、显示器/用户接口920等。在一些实施例中，传感器925可以包括传感器中心，其具有感测引擎、传感器接口集中器、以及传感器融

合和推断引擎逻辑。

[0047] 如进一步示出的，提供了近场通信(NFC)非接触式接口960，其经由NFC天线965在NFC近场中进行通信。虽然在图5中示出了分离的天线，但是应理解，在一些实现方式中，可以提供一个天线或不同的一组天线，以实现各种无线功能。

[0048] 功率管理集成电路(PMIC)915耦合到应用处理器910，以执行平台级功率管理。为此，PMIC 915可以向应用处理器910发出功率管理请求，以按需进入特定低功率状态。此外，基于平台约束，PMIC 915还可以控制系统900的其他组件的功率级别。

[0049] 为了使得通信能够例如在一个或多个IoT网络中发送和接收，可以在基带处理器905与天线990之间耦合各种电路。具体地，可以存在射频(RF)收发器970和无线局域网(WLAN)收发器975。一般地，RF收发器970可以用于根据给定的无线通信协议(例如，3G或4G无线通信协议，例如根据码分多址(CDMA)、全球移动系统通信(GSM)、长期演进(LTE)、或其他协议)来接收和发送无线数据和呼叫。另外，可以存在GPS传感器980，当在配对过程中使用上下文信息时，位置信息被提供给安全处理器950以供如本文所描述地使用。还可以提供其他无线通信，例如，接收或发送诸如AM/FM和其他信号的无线电信号。另外，经由WLAN收发器975，还可以实现例如根据Bluetooth ™或IEEE 802.11标准的局部无线通信。

[0050] 现在参考图6，示出了根据本发明的另一实施例的系统的框图。如图6所示，多处理器系统1000是点对点互连系统(例如，服务器系统)，并且包括经由点对点互连1050耦合的第一处理器1070和第二处理器1080。如图6所示，处理器1070和1080中的每一个都可以是诸如SoC的多核处理器，其包括第一处理器核心和第二处理器核心(即，处理器核心1074a和1074b，以及处理器核心1084a和1084b)，但是在处理器中可能存在更多的核心。另外，处理器1070和1080各自可以包括安全引擎1075和1085，以执行安全操作，例如，证言、IoT网络登载、访问控制策略处理等。

[0051] 仍然参考图6，第一处理器1070还包括存储器控制器中心(MCH)1072以及点对点(P-P)接口1076和1078。类似地，第二处理器1080包括MCH1082以及P-P接口1086和1088。如图5所示，MCH的1072和1082将处理器耦合到相应的存储器，即存储器1032和存储器1034，其可以是本地附接到相应处理器的主存储器(例如，DRAM)中的部分。第一处理器1070和第二处理器1080可以分别经由P-P互连1052和1054耦合到芯片组1090。如图5所示，芯片组1090包括P-P接口1094和1098。

[0052] 此外，芯片组1090包括用于通过P-P互连1039来耦合芯片组1090与高性能图形引擎1038的接口1092。接下来，芯片组1090可以经由接口1096耦合到第一总线1016。如图6所示，各种输入/输出(I/O)设备1014可以耦合到第一总线1016，以及总线桥1018将第一总线1016耦合到第二总线1020。各种设备可以耦合到第二总线1020，包括例如，键盘/鼠标1022、通信设备1026、以及数据存储单元1028(例如，非易失性存储装置或其他大容量存储设备)。如图所示，在一个实施例中，数据存储单元1028可以包括代码1030。如进一步示出的，数据存储单元1028还包括可信存储装置1029，以用于存储要保护的敏感信息。此外，音频I/O 1024可以耦合到第二总线1020。

[0053] 实施例可以用于其中IoT设备可以包括可穿戴设备或其他小形状因子IoT设备的环境中。现在参考图7，示出了根据另一实施例的可穿戴模块1300的框图。在一个特定实现方式中，模块1300可以是Intel®Curie™模块，其包括在能够实现为可穿戴设备中的全部或

部分的单个小型模块内适用的多个组件。如图所示，模块1300包括核心1310(当然在其它实施例中可以存在多于一个核心)。这种核心可以是相对较低复杂度的按次序核心，例如，基于Intel Architecture® Quark™设计。在一些实施例中，核心1310可以实现如本文所描述的TEE。核心1310耦合到包括传感器中心1320的各种组件，该传感器中心1320可以被配置为与多个传感器1380(例如，一个或多个生物计量、运动环境、或其他传感器)进行交互。存在电力输送电路1330以及非易失性存储装置1340。在实施例中，该电路可以包括可充电电池和充电电路，其在一个实施例中可以无线地接收充电电力。可以存在一个或多个输入/输出(IO)接口1350，例如，与USB/SPI/I^2C/GPIO协议中的一个或多个兼容的一个或多个接口。另外，存在无线收发器1390，其可以是Bluetooth ™低能量或其他短距离无线收发器，以用于实现如本文所描述的无线通信。应理解，在不同的实现方式中，可穿戴模块可以采取许多其他形式。

[0054] 以下示例涉及另外的实施例。

[0055] 在示例1中，一种设备，包括：用于执行指令的处理器；以及用于接收对要由设备保护的资源进行访问的请求的策略逻辑，其中策略逻辑用于访问与资源相关联的控制数据，控制数据具有第一值的第一设备状态字段。策略逻辑可以被配置为确定设备是否处于与第一值相关联的设备状态，并且如果是，则应用控制数据的访问策略来确定是否准许对资源进行访问的请求。

[0056] 在示例2中，控制数据包括访问控制列表，访问控制列表包括多个设备状态字段，每个设备状态字段指示当设备处于对应的设备状态时访问控制列表的访问策略是否要被应用。

[0057] 在示例3中，多个设备状态字段中的一个设备状态字段包括设备的操作临界度状态。

[0058] 在示例4中，多个设备状态字段中的一个设备状态字段包括设备的操作优化目标。

[0059] 在示例5中，上述示例中一个或多个示例的策略逻辑用于接收多个设备状态输入，并且确定多个设备状态输入中的每个设备状态输入是否与存储在控制数据的多个设备状态字段中的对应的一个设备状态字段中的值匹配。

[0060] 在示例6中，多个设备状态输入中的至少一个设备状态输入是从经由网络耦合到设备的一个或多个第二设备接收的。

[0061] 在示例7中，控制数据包括至少一个状态向量，至少一个状态向量包括多个字段，每个字段用于设备状态因子，并且指示当设备状态因子在设备中有效时控制数据的访问策略是否要被应用。

[0062] 在示例8中，上述示例中一个或多个示例的设备还包括用于存储索引的存储装置，索引包括多个条目，每个条目与多个控制数据中的一个控制数据相关联，并且指示设备的复合设备状态，在复合设备状态下策略逻辑将相关联的控制数据应用于访问请求。

[0063] 在示例9中，上述示例中一个或多个示例的设备还包括用于存储多个控制数据的存储装置。策略逻辑可以被配置为基于设备的当前复合设备状态，从网络的权威策略存储装置获得多个控制数据。

[0064] 在示例10中，示例9的策略逻辑用于响应于对当前复合设备状态进行的改变而逐出多个控制数据中的一个或多个控制数据。

[0065] 在示例11中，上述示例中一个或多个示例的策略逻辑用于基于设备的设备状态来预过滤多个控制数据，以及基于预过滤的结果来访问控制数据。

[0066] 在示例12中，一种方法，包括：确定包括IoT设备的系统的设备状态；确定当系统处于所确定的设备状态时与资源相关联的访问控制列表是否要被应用；以及如果确定当系统处于所确定的设备状态时访问控制列表要被应用，则基于访问控制列表来确定请求者是否被准许对资源进行访问，否则阻止访问而不对访问控制列表进行进一步应用。

[0067] 在示例13中，该方法还包括：响应于系统的设备状态改变，而请求访问控制列表并且从位于系统远处的权威策略存储装置获得访问控制列表。

[0068] 在示例14中，该方法还包括对索引进行访问，索引包括多个条目，每个条目与多个访问控制列表中的一个访问控制列表相关联，并且指示系统的复合设备状态，在复合设备状态下系统的策略逻辑用于将相关联的访问控制列表应用于访问请求，以确定访问控制列表是否要被应用。

[0069] 在示例15中，该方法还包括对与资源相关联的多个访问控制列表进行访问，多个访问控制列表中的每个访问控制列表包括与系统的复合设备状态匹配的复合设备状态。

[0070] 在示例16中，该方法还包括响应于对复合设备状态进行的改变，而从系统的存储装置中逐出多个访问控制列表中的一个或多个访问控制列表。

[0071] 在示例17中，该方法还包括基于所访问的多个访问控制列表中的至少一些来准许请求者对资源的访问。

[0072] 在另一示例中，一种计算机可读介质，包括用于执行上述示例中的任一个示例的方法的指令。

[0073] 在另一示例中，一种计算机可读介质，包括由至少一个机器用于制造至少一个集成电路以执行上述示例中的任一个示例的方法的数据。

[0074] 在另一示例中，一种装置，包括用于执行上述示例中的任一个示例的方法的模块。

[0075] 在示例18中，一种系统，包括：具有用于在可信执行环境中执行的第一逻辑的处理器；以及用于存储多个访问控制策略的存储装置，多个访问控制策略中的每个访问控制策略与系统的复合设备状态相关联，并且包括针对要由第一逻辑保护的资源的访问策略。第一逻辑可以被配置为响应于一个或多个访问控制策略的相关联的复合设备状态与系统的当前复合设备状态匹配，而将多个访问控制策略中的一个或多个访问控制策略应用于对资源进行访问的请求。

[0076] 在示例19中，与第一访问控制策略相关联的复合设备状态包括多个设备状态字段，每个设备状态字段具有第一值或第二值中的一个，第一值指示系统的当前复合设备状态的对应设备状态因子是有效的；第二值指示系统的当前复合设备状态的对应设备状态因子是无效的。

[0077] 在示例20中，存储装置用于存储具有多个条目的索引，每个条目与多个访问控制策略中的一个访问控制策略相关联，并且用于存储多个设备状态字段的第一值或第二值。

[0078] 在示例21中，第一逻辑用于对索引进行访问，以识别多个访问控制策略中的一个或多个访问控制策略以供应用于针对访问的请求。

[0079] 在示例22中，上述示例中的一个或多个示例的系统还包括多个传感器，其用于提供当前复合设备状态的一个或多个设备状态因子，其中多个传感器中的至少一个传感器经

由控制信道耦合到处理器以提供一个或多个设备状态因子。

[0080] 在示例23中，一种系统，包括：用于在可信执行环境中执行的模块；用于存储多个访问控制策略的存储模块，多个访问控制策略中的每个访问控制策略与系统的复合设备状态相关联，并且包括针对要被保护的资源的访问策略；以及用于响应于一个或多个访问控制策略的相关联的复合设备状态与系统的当前复合设备状态匹配而将多个访问控制策略中的一个或多个访问控制策略应用于对资源进行访问的请求的模块。

[0081] 在示例24中，存储模块用于存储具有多个条目的索引，每个条目与多个访问控制策略中的一个访问控制策略相关联，并且用于存储多个设备状态字段的第一值或第二值。

[0082] 在示例25中，该系统还包括用于对索引进行访问以识别多个访问控制策略中的一个或多个访问控制策略以供应用于针对访问的请求的模块。

[0083] 应理解，上述示例的各种组合是可能的。

[0084] 实施例可以用于许多不同类型的系统中。例如，在一个实施例中，通信设备可以被布置为执行本文描述的各种方法和技术。当然，本发明的范围不限于通信设备，并且相反，其他实施例可以针对用于处理指令的其他类型的装置，或者包括指令的一个或多个机器可读介质，该指令响应于在计算设备上执行而使得设备执行本文描述的方法和技术中的一个或多个。

[0085] 实施例可以以代码来实现，并且可以存储在非暂时性存储介质上，该非暂时性存储介质上存储有指令，指令可以用于对执行指令的系统进行编程。实施例还可以以数据来实现，并且可以存储在非暂时性存储介质上，该数据如果由至少一个机器使用，则使得至少一个机器制造至少一个集成电路以执行一个或多个操作。存储介质可以包括但不限于：包括软盘、光盘、固态驱动器(SSD)、压缩盘只读存储器(CD-ROM)、可重写压缩盘(CD-RW)、以及磁光盘的任何类型的盘，诸如只读存储器(ROM)、随机存取存储器(RAM)(例如，动态随机存取存储器(DRAM)、静态随机存取存储器(SRAM))、可擦除可编程只读存储器(EPROM)、闪速存储器、电可擦除可编程只读存储器(EEPROM)的半导体设备，磁或光卡，或者适于存储电子指令的任何其它类型的介质。

[0086] 虽然已经关于有限数量的实施例描述了本发明，但是本领域技术人员将理解其许多修改和变化。所附权利要求旨在涵盖落入本发明的真实精神和范围内的所有这些修改和变化。

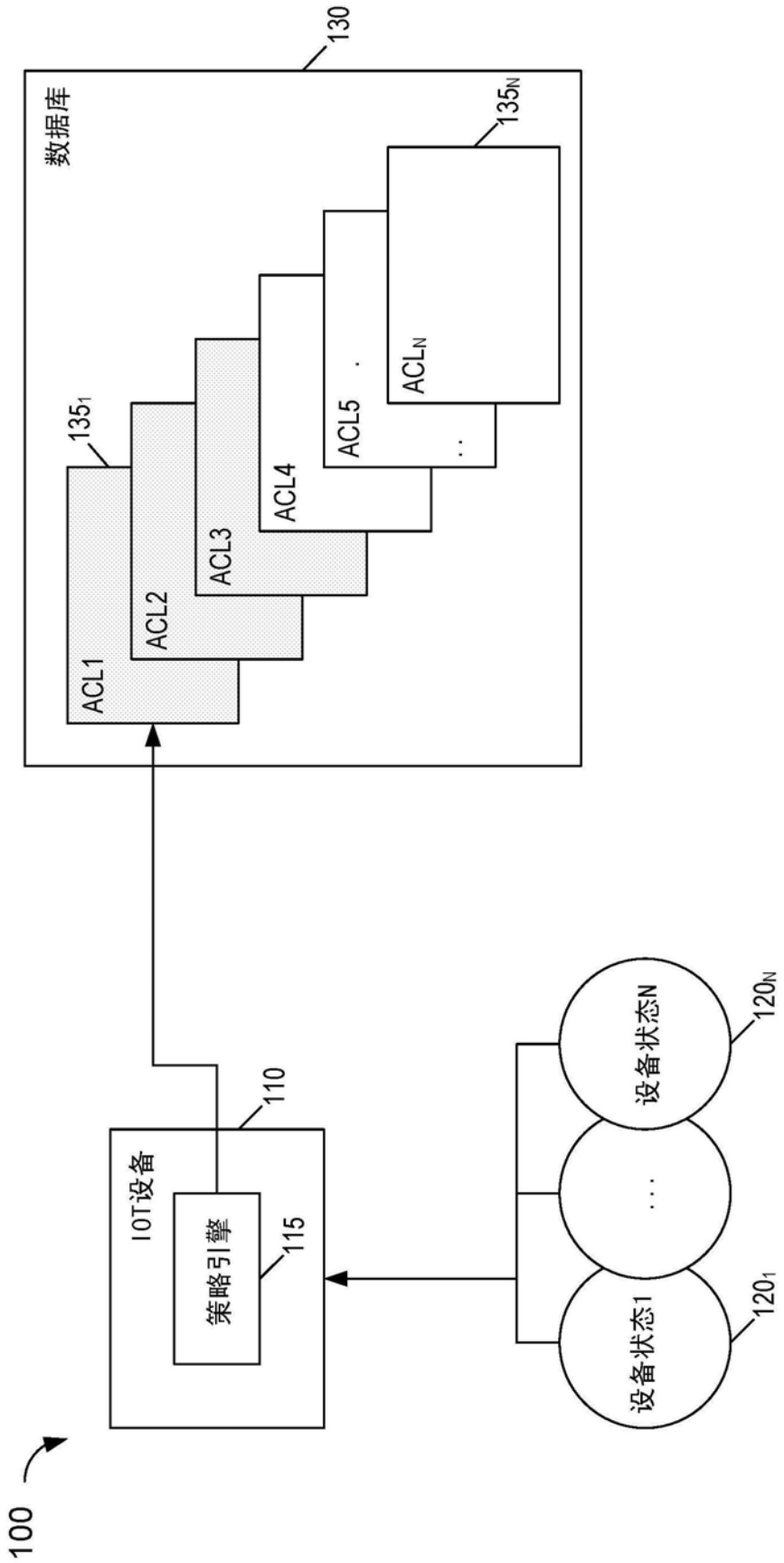
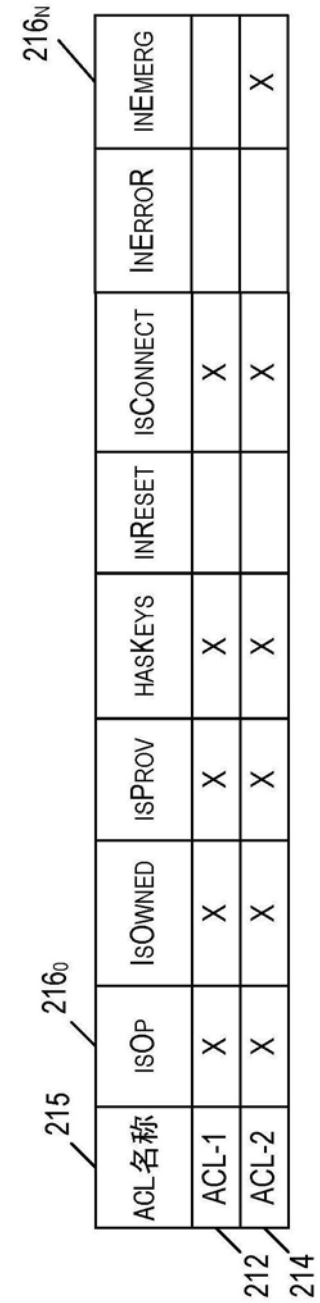

100
IOT设备
策略引擎
110
115
数据库
130
ACL1
ACL2
ACL3
ACL4
ACL5
ACLN
135₁
135N
设备状态1
设备状态N
120₁
120N

图1


216N
216₀
215
ACL名称
ISOP
ISOWNED
ISPROV
HASKEYS
INRESET
ISCONNECT
INERROR
INEMERG
ACL-1
X
X
X
X
X
ACL-2
X
X
X
X
X
212
214

200

图2A

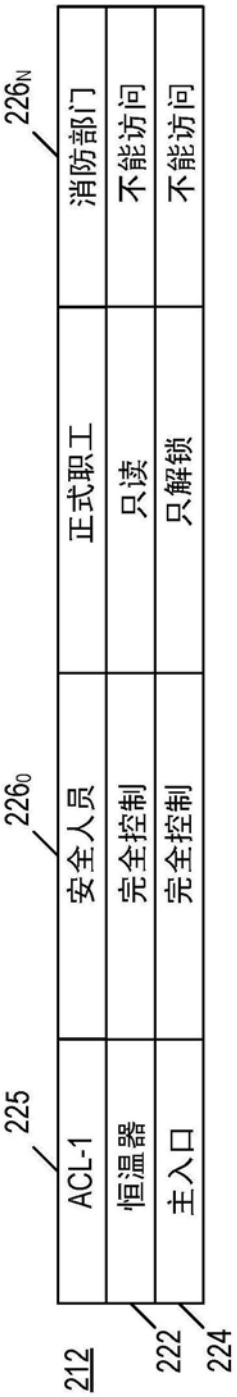

212
225
ACL-1
恒温器
主入口
222
224
226$_0$
安全人员
完全控制
完全控制
正式职工
只读
只解锁
226$_N$
消防部门
不能访问
不能访问

图2B

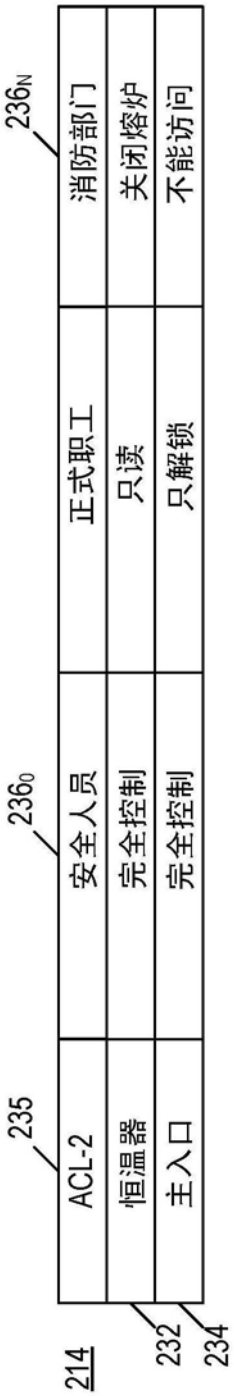

214
235
ACL-2
恒温器
主入口
232
234
236$_0$
安全人员
完全控制
完全控制
正式职工
只读
只解锁
236$_N$
消防部门
关闭熔炉
不能访问

图2C

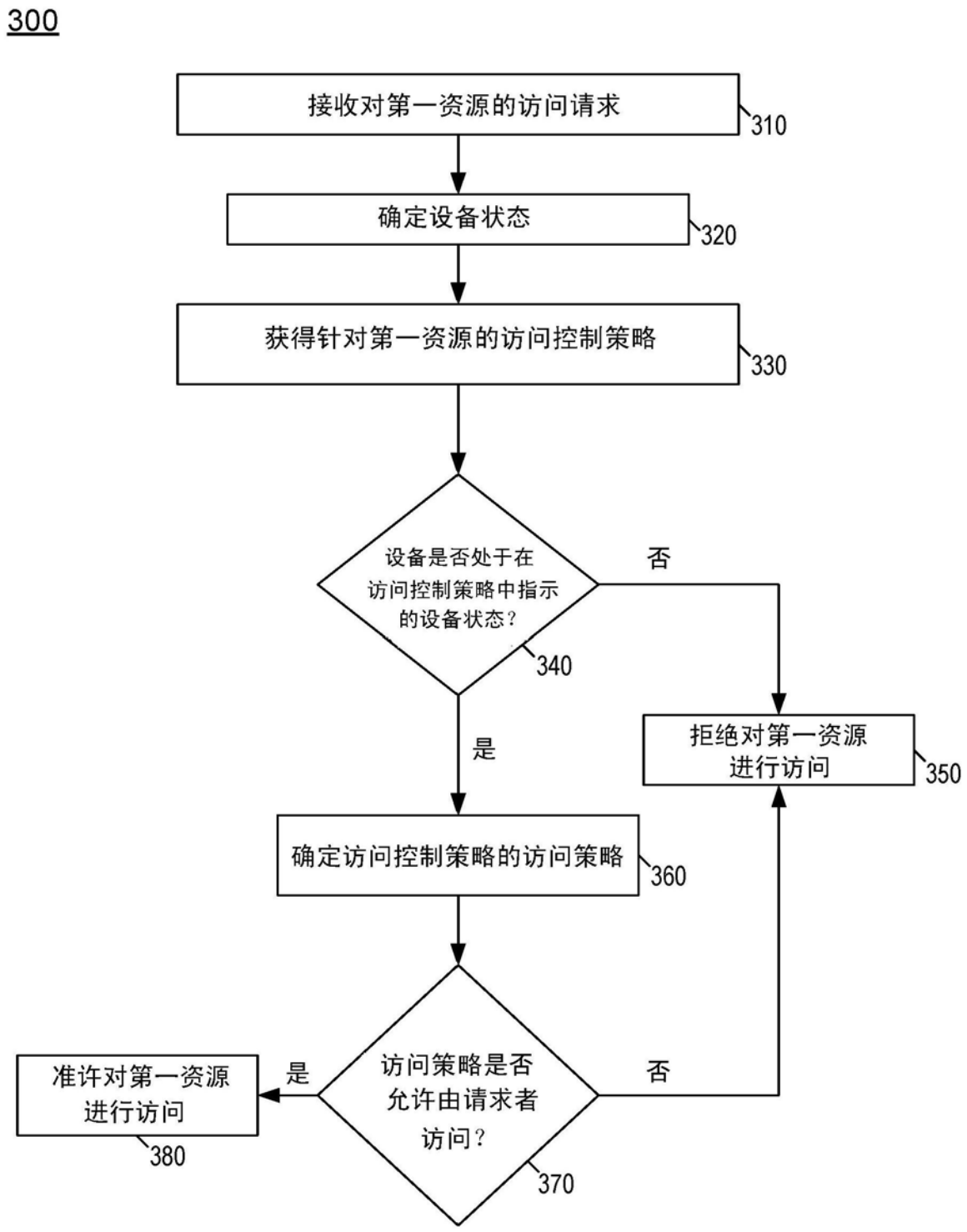

300
接收对第一资源的访问请求
310
确定设备状态
320
获得针对第一资源的访问控制策略
330
设备是否处于在访问控制策略中指示的设备状态？
340
否
是
拒绝对第一资源进行访问
350
确定访问控制策略的访问策略
360
访问策略是否允许由请求者访问？
370
是
否
准许对第一资源进行访问
380

图3

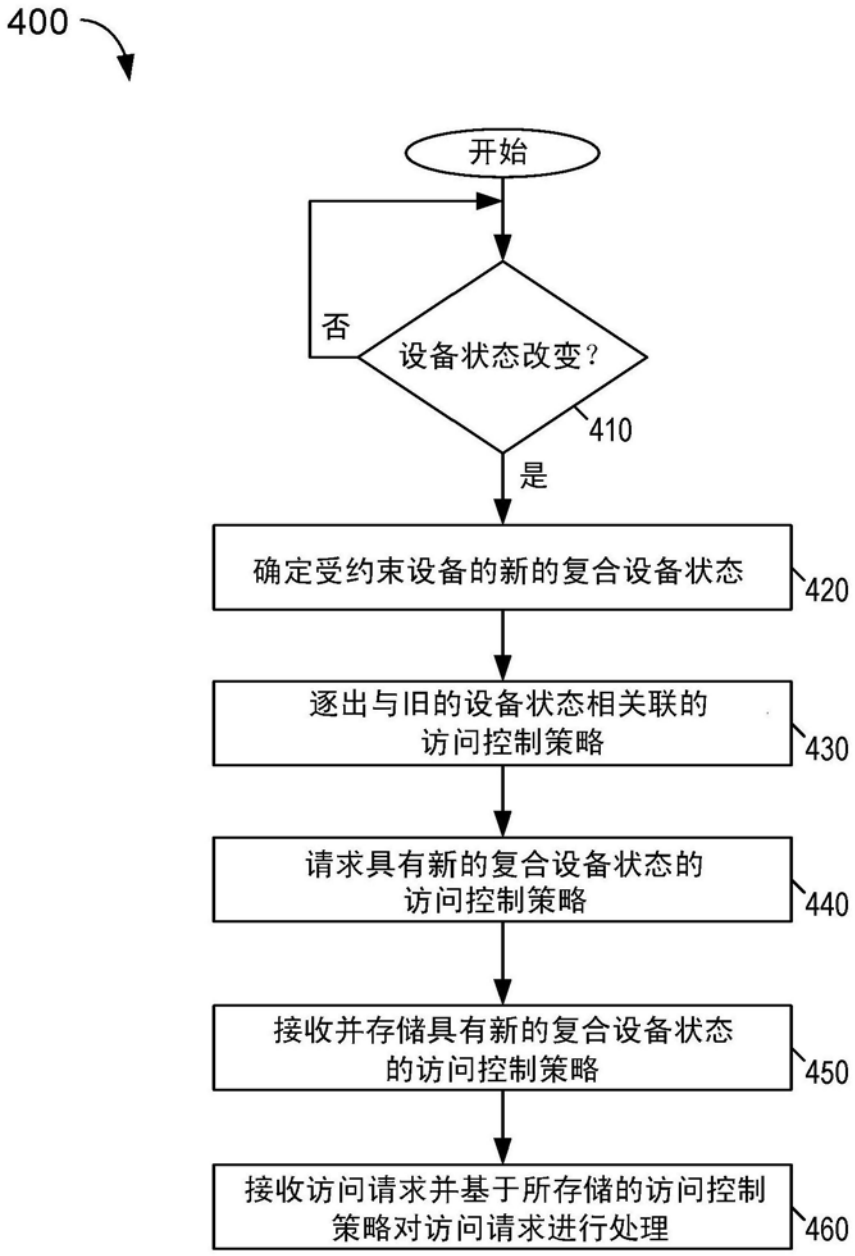

400
开始
设备状态改变？
否
410
是
确定受约束设备的新的复合设备状态
420
逐出与旧的设备状态相关联的
访问控制策略
430
请求具有新的复合设备状态的
访问控制策略
440
接收并存储具有新的复合设备状态
的访问控制策略
450
接收访问请求并基于所存储的访问控制
策略对访问请求进行处理
460

图4

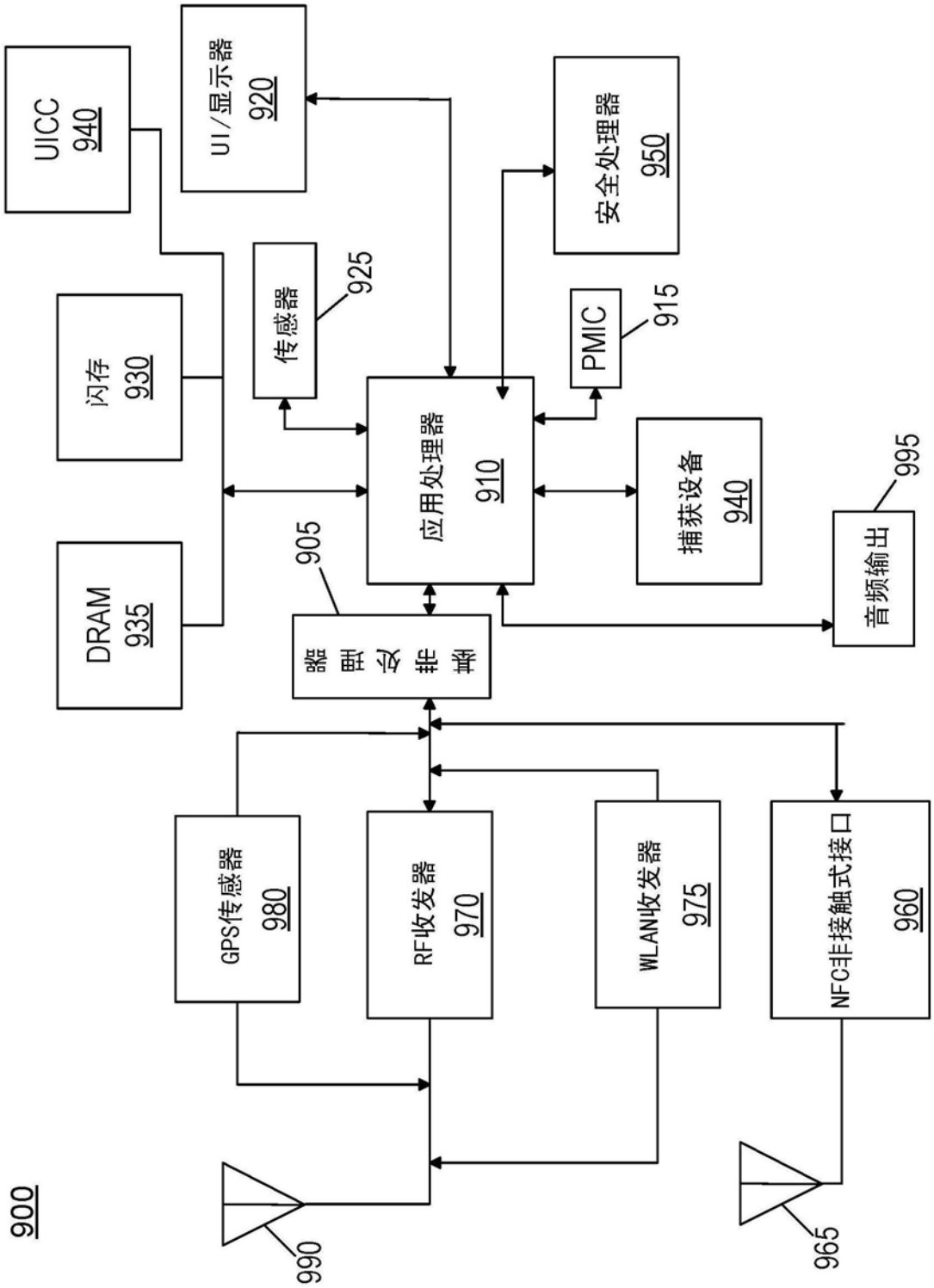

900
UICC
940
UI/显示器
920
安全处理器
950
闪存
930
传感器
925
PMIC
915
应用处理器
910
捕获设备
940
DRAM
935
905
995
音频输出
GPS传感器
980
RF收发器
970
WLAN收发器
975
NFC非接触式接口
960
990
965

图5

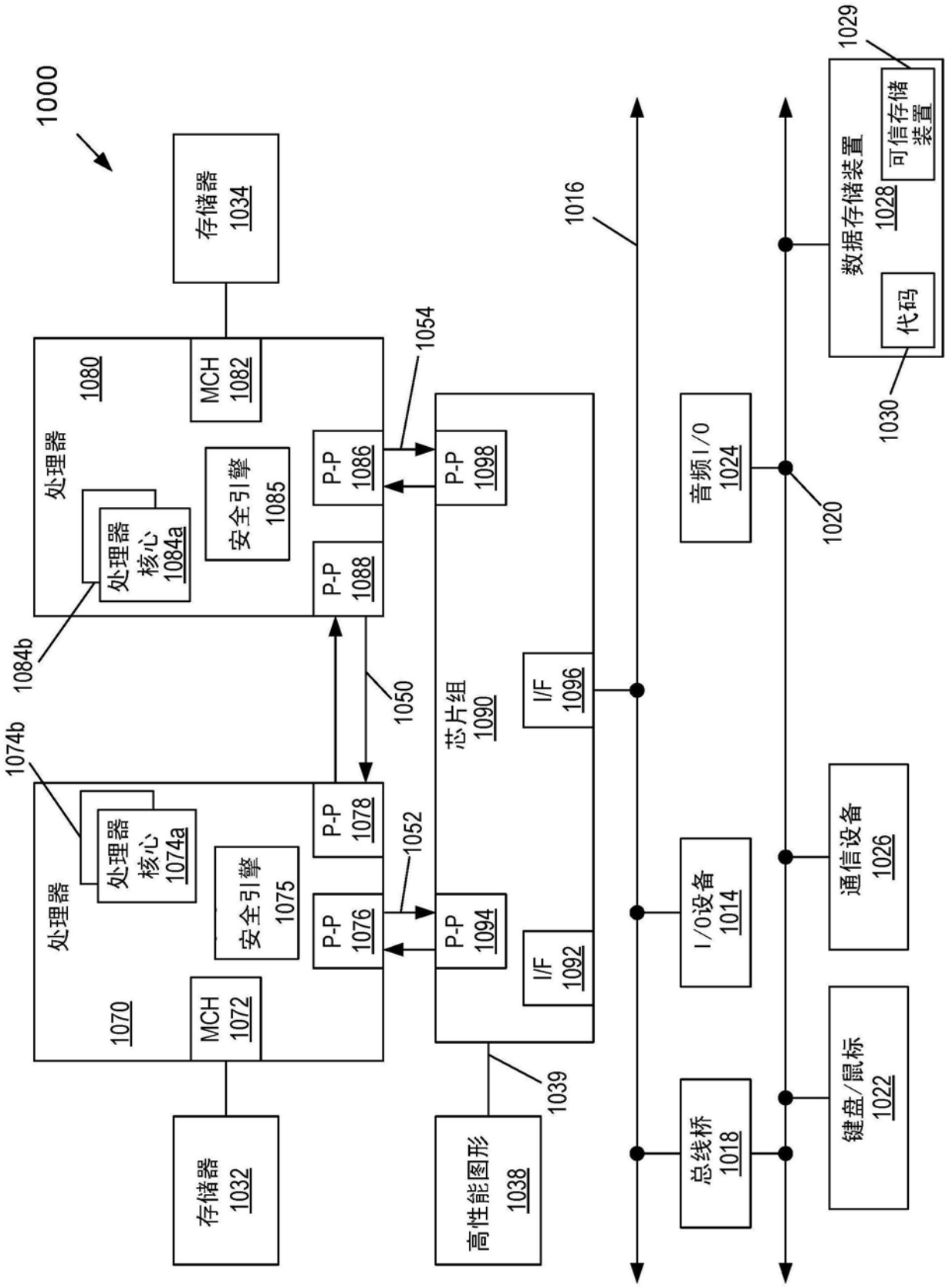

1000
存储器 1034
1080
MCH 1082
处理器
处理器核心 1084a
安全引擎 1085
P-P 1086
P-P 1088
1054
1084b
1050
1074b
处理器
处理器核心 1074a
安全引擎 1075
P-P 1078
P-P 1076
1052
1070
MCH 1072
存储器 1032
芯片组 1090
P-P 1098
I/F 1096
P-P 1094
I/F 1092
1039
高性能图形 1038
1016
音频I/O 1024
I/O设备 1014
总线桥 1018
1020
数据存储装置 1028
可信存储装置
代码
1029
1030
通信设备 1026
键盘/鼠标 1022

图6

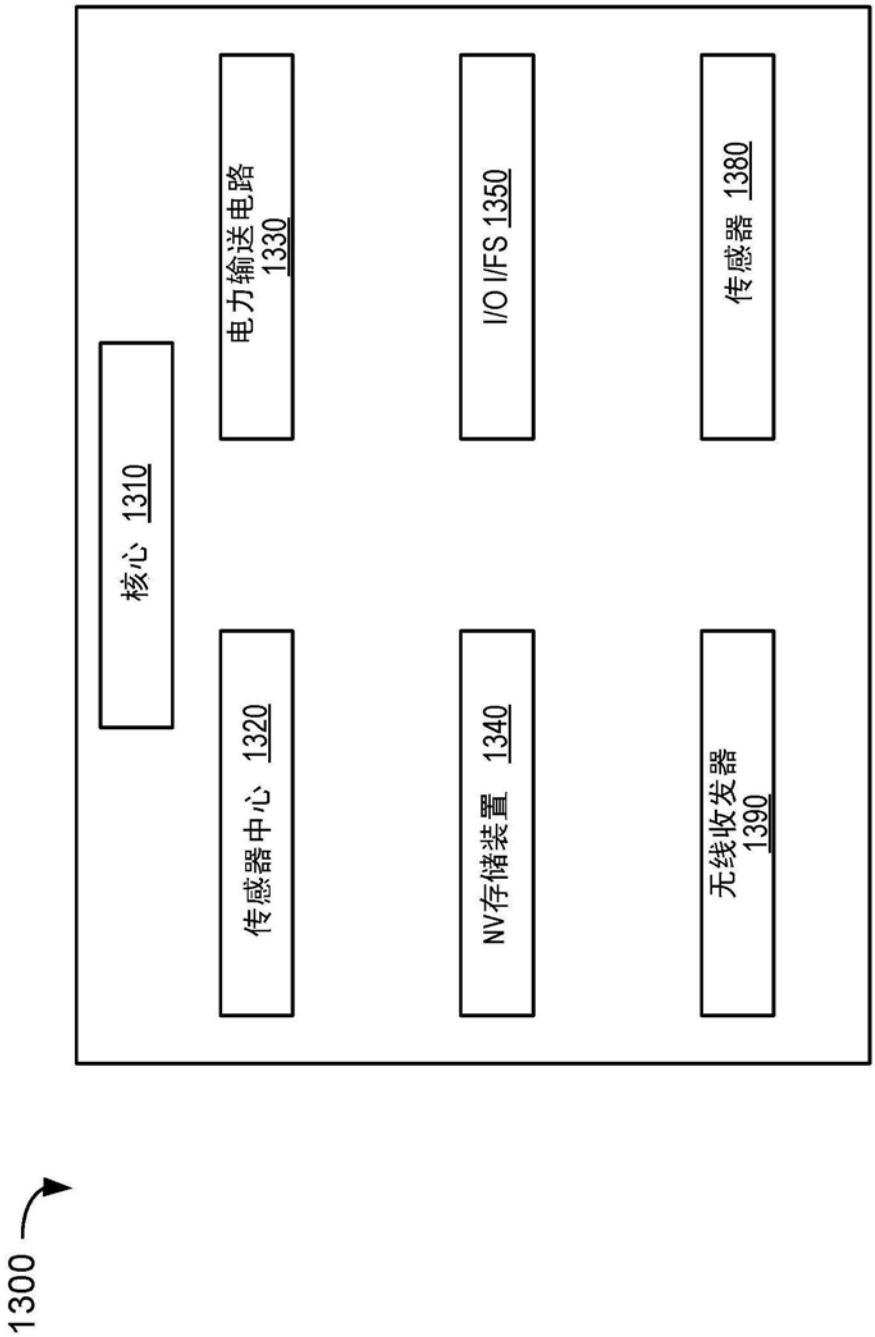

核心 1310
电力输送电路 1330
传感器中心 1320
I/O I/FS 1350
NV存储装置 1340
传感器 1380
无线收发器 1390
1300

图7