(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 103858131 B
(45)授权公告日 2017.03.29

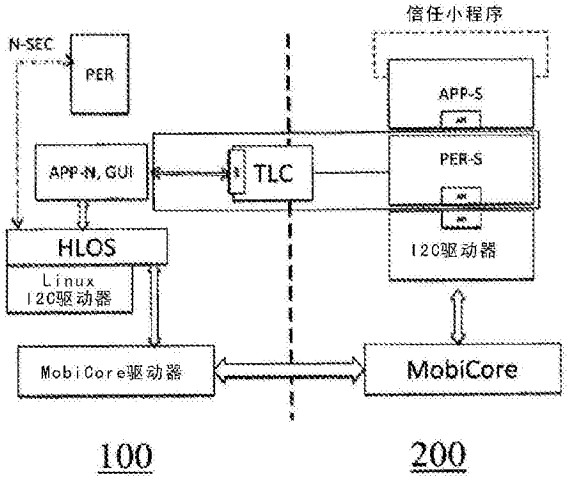
(21)申请号 201280049509.4
(22)申请日 2012.10.04
(65)同一申请的已公布的文献号
申请公布号 CN 103858131 A
(43)申请公布日 2014.06.11
(30)优先权数据
102011115135.8 2011.10.07 DE
(85)PCT国际申请进入国家阶段日
2014.04.08
(86)PCT国际申请的申请数据
PCT/EP2012/004159 2012.10.04
(87)PCT国际申请的公布数据
WO2013/050154 DE 2013.04.11
(73)专利权人 信特尼有限公司
地址 英国剑桥
(72)发明人 斯蒂芬·斯匹兹 马库斯·蔻尔 乌尔里奇·马丁尼
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 李晓冬
(51)Int.Cl.
G06F 21/53(2006.01)
G06F 9/54(2006.01)
(56)对比文件
CN 1813244 A,2006.08.02,
CN 101078922 A,2007.11.28,
CN 101211277 A,2008.07.02,
Wei Huang等.Vitual Machine Aware Communication Libraries for High Performance Computing.《proceedings of the 2007 ACM/IEEE conference on supercomputing》.2007,正文第2-3页,附图1.
审查员 刘义乐
权利要求书2页 说明书6页 附图3页

(54)发明名称

带有安全运行时环境的微控制器系统

(57)摘要

微处理器系统,该微处理器系统被实现或者能够被实现在移动终端中并且包括:被设计为生成并且维护不安全运行时环境的正常操作系统和被设计为生成并且维护安全运行时环境的安全操作系统,以及正常操作系统与安全操作系统之间的操作系统接口,该操作接口被设计成在操作系统层上安全地控制不安全运行时环境与安全运行时环境之间的通信,以及至少一个过滤器接口,该至少一个过滤器接口被设计成在不同于操作系统层的层上安全地控制不安全运行时环境与安全运行时环境之间的通信。



CN 103858131 B

1.一种微处理器系统,能实现或者被实现在移动终端中并且包括:

-正常操作系统,该正常操作系统被设计用于生成并且维护不安全运行时环境,

-安全操作系统,该安全操作系统被设计用于生成并且维护安全运行时环境,以及

-在所述正常操作系统与所述安全操作系统之间的操作系统接口,所述操作系统接口被设计成在操作系统层安全地控制所述不安全运行时环境与所述安全运行时环境之间的通信,

其特征在于

至少一个过滤器接口,该至少一个过滤器接口被设计成在不同于所述操作系统层的层安全地控制所述不安全运行时环境与所述安全运行时环境之间的通信,

其中所提供的所述过滤器接口是应用过滤器接口,该过滤器接口被设计成在应用层安全地控制所述不安全运行时环境与所述安全运行时环境之间的通信,以及

用于所述移动终端的外围结构的至少一个驱动器,所述至少一个驱动器能够由所述正常操作系统驱动并且能够在所述不安全运行时环境中执行,以及

其特征还在于

用于所述外围结构的简化的驱动器,所述驱动器能够由所述安全操作系统驱动并且能够在所述安全运行时环境中执行以及仅具有能够在所述不安全运行时环境中执行的所述驱动器的功能的子集。

2.如权利要求1所述的微处理器系统,其中所提供的所述过滤器接口是硬件过滤器接口,该硬件过滤器接口被设计成在硬件层安全地控制所述不安全运行时环境与所述安全运行时环境之间的通信。

3.如权利要求2所述的微处理器系统,其中在所述硬件层处的控制被实现为经由总线系统的控制。

4.如权利要求2或3所述的微处理器系统,其中所述硬件过滤器接口被设计成在所述硬件层安全地控制能够在所述不安全运行时环境中执行的用于外围结构的所述驱动器与能够在所述安全运行时环境中执行的用于所述外围结构的简化的驱动器之间的通信。

5.如权利要求4所述的微处理器系统,其中所述硬件过滤器接口被设计为:针对与安全的相关性来检查对外围结构的驱动器的访问,并且在其中所述访问被识别为与安全相关的情况下,将所述访问传达至所述安全运行时环境中的简化的驱动器,以及在其中所述访问被识别为不与安全相关的情况下,将所述访问传达至所述不安全运行时环境中的驱动器。

6.如权利要求1所述的微处理器系统,还包括:

至少一个应用,

其特征在于

所述应用至少部分地是能够由所述正常操作系统驱动并且能够在所述不安全运行时环境中执行的,并且至少部分地是能够由所述安全操作系统驱动并且能够在所述安全运行时环境中执行的,

以及在于

所述应用过滤器接口被设计成在所述应用层安全地控制能够在所述不安全运行时环境中执行的至少部分应用与能够在所述安全运行时环境中执行的至少部分应用之间的通信。

7.如权利要求6所述的微处理器系统，其中所述应用过滤器接口被设计成：针对与安全的相关性来检查对所述应用的访问，并且在其中所述访问被识别为与安全相关的情况下，将所述访问传达至所述安全运行时环境中的所述至少部分应用，以及在其中所述访问被识别为不与安全相关的情况下，将所述访问传达至所述不安全运行时环境中的所述至少部分应用。

8.如权利要求1所述的微处理器系统，其中过滤器接口以这样一种方式被耦合到用户输出设备，即：在经由所述过滤器接口从所述不安全运行时环境到所述安全运行时环境或/和从所述安全运行时环境到所述不安全运行时环境实现的任何访问之时，用户消息被所述用户输出设备输出。

9.如权利要求8所述的微处理器系统，其中所述过滤器接口被以这样一种方式耦合到所述用户输出设备，即：对于一方面从所述不安全运行时环境到所述安全运行时环境以及另一方面从所述安全运行时环境到所述不安全运行时环境的访问来说，不同用户输出被输出。

带有安全运行时环境的微控制器系统

技术领域

[0001] 本发明涉及可实现于或被实现于移动终端中的带有安全运行时环境(runtime environment)的微处理器系统。

背景技术

[0002] 微处理器系统包括微处理器以及一个或多个易失性和非易失性存储器，从功能观点看该一个或多个易失性和非易失性存储器具体是：操作系统被存储在其中的至少一个操作系统存储器、可由微处理器在操作系统的控制下执行的应用被存储在其中的一个或多个应用存储器、以及待由微处理器处理的数据能够被存储在其中的主存储器。操作系统在其操作期间生成并且维护其中应用可在微处理器系统上执行的运行时环境。微处理器系统一般地被实现在一个芯片，例如半导体芯片上，还可能被实现在多个相连的芯片上。

[0003] 移动终端被理解成是指蜂窝电话、智能电话、PDA(个人数字助理)或类似终端。

[0004] 指定ARM信任区域架构表示来自公司ARM用于微处理器系统的已知的两部分的运行时架构，此架构包括两个运行时环境。被称作“正常区域”或“正常世界”的第一不安全运行时环境由正常操作系统控制。被称作“信任区域”或“可信世界”或“安全世界”的第二安全或值得信任的运行时环境由安全操作系统控制。

[0005] 正常操作系统可以是例如常规操作系统，诸如Android、Windows Phone、Symbian等等。

[0006] 本专利申请的申请人制造并且出售用于将被实现在移动终端中的芯片的、商品名为MOBICORE的安全操作系统。特别地，安全关键应用和一些外围功能(例如键盘驱动器)被安全操作系统MOBICORE安全地控制。在安全操作系统下的应用还被按照术语“信任(Trust)”和“小程序(Applet)”类似地命名为信任小程序(trustlet)。另外的应用和其它外围功能(例如显示器驱动器、NFC接口驱动器、无线电接口层RIL)被正常操作系统(还被称作富OS或HLOS)控制。安全操作系统包括秘密密钥、认证密钥Kauth，借助于其安全操作系统能够相对于后台系统标识它自己。可选地，认证密钥Kauth被附加地提供用于操作芯片或移动终端与后台系统之间的安全通信信道。后台系统是例如移动无线电网络的本身已知的后台系统。

[0007] 例如为了调用安全运行时环境中的应用(信任小程序)或者为了交换数据，就正常操作系统而言，从不安全运行时环境到安全运行时环境的访问专用地借助于安全驱动器被作为标准执行，所述安全驱动器(例如Mobicore驱动器)被实现在不安全运行时环境内，但被安全操作系统控制并且在操作系统层起作用。安全驱动器能够例如将正常操作系统的任务转移到安全操作系统并且将关于任务的结果转发至正常操作系统，所述结果是由安全操作系统提供的。安全驱动器转交正常操作系统与安全操作系统之间的安全通信信道，所述信道完全足够用于交换相对少量的数据。

[0008] 在安全运行时环境中实现的应用(信任小程序)或外围功能只能够由安全操作系统访问。相比而言，不能够从正常操作系统直接地访问信任小程序。

[0009] 实际上，移动终端的所有外围结构(除例如键盘之外)(也就是说中央微处理器之外的移动终端的结构)被实现在正常操作系统下并且因此在极大程度上是不安全的，因为相应的外围驱动器被实现在不安全运行时环境“正常区域”中。

[0010] 外围结构与操作系统或经由操作系统的通信的一些过程是安全关键的，例如那些在其中处理诸如例如秘密号码PIN之类的秘密数据的过程，或者那些在其中处理安全相关命令的过程，例如用于确认或者发起支付交易的命令。对于这样的安全关键通信过程，外围结构的安全链路将是所希望的以便阻止对数据的隐秘观察或者对命令的操纵。

[0011] 用于使外围结构的操作变得更加安全的最直接的可能性是在安全操作系统下而非在正常操作系统下实现相应的外围驱动器。(例如，采用MobiCore作为安全操作系统的移动终端中相对小且紧凑的键盘驱动器常常已经被作为标准实现在安全操作系统下。)然而，这具有对外围结构的所有访问必定必须由安全操作系统来实现的后果。因为，在安全操作系统下，诸如认证和加密之类的复杂安全措施对于所有访问来说是需要的，所以将驱动器从正常操作系统移动到安全操作系统相当大地使移动终端的操作慢下来。然而，对外围结构的访问的相当大的比例不是安全关键的，并且能够在不安全但较快的正常操作系统下也可良好地进行。

[0012] 用于各种广泛的使用目的的应用，例如支付交易(银行业务(banking)、支付)、或用于交通方式的票销售(售票)或积分和折扣系统(信用)，以可在安全执行环境中执行的方式至少部分在安全操作系统的控制下被广泛地实现。在这种情况下，至少部分的应用以可在不安全执行环境中执行的方式被附加地或者仅在正常操作系统的控制下实现，具体是针对与移动终端的用户或用户接口的交互的部分应用。如果在安全和不安全运行时环境中的应用的部分之间需要通信，则这借助于安全驱动器在操作系统层发生，这会使通信变慢。

发明内容

[0013] 本发明基于给在移动终端中可实现的或者被实现的微处理器系统提供安全运行时环境的目的，所述微处理器系统使得能实现不安全运行时环境与安全运行时环境之间的安全且同时高效的通信。

[0014] 该目的借助于如权利要求1所述的微处理器系统来实现。本发明的有利实施例在从属权利要求被指定。

[0015] 如独立权利要求1所述的根据本发明的微处理器系统可实现或者被实现在移动终端中，并且包括：

[0016] -正常操作系统，其被设计用于生成并且维护不安全运行时环境，

[0017] -安全操作系统，其被设计用于生成并且维护安全运行时环境，以及

[0018] -在正常操作系统与安全操作系统之间的操作系统接口，所述操作系统接口被设计成在操作系统层安全地控制不安全运行时环境与安全运行时环境之间的通信。

[0019] 所述微处理器系统的特征在于至少一个过滤器接口，所述至少一个过滤器接口被设计成在不同于操作系统层的层安全地控制不安全运行时环境与安全运行时环境之间的通信。

[0020] 所述过滤器接口使得能实现加速的且同时安全的通信，因为它除了提供在操作系统层的通信信道之外还提供另外的安全通信信道，其能够被用于比经由操作系统的迂回

(detour)的通信更直接的通信。

[0021] 因此,权利要求1提供了使得能实现不安全运行时环境与安全运行时环境之间的安全且同时高效的通信的微处理器系统。

[0022] 所述过滤器接口具有第一不安全的部分过滤器接口,其被设计成在不安全运行时环境中运行,以及第二安全的部分过滤器接口,其被设计成在安全运行时环境中运行。结果,所述过滤器接口能够在安全和不安全运行时环境之间进行转交。

[0023] 依据一个可替代方案,所提供的过滤器接口是硬件过滤器接口,其被设计成在硬件层安全地控制不安全运行时环境与安全运行时环境之间的通信。安全和不安全运行时环境之间的安全通信因此能够立即并且直接地在硬件层以及因此以加速的方式发生。

[0024] 在硬件层的控制被可选地实现为通过诸如例如显示器、SIM卡等这样的外围结构的硬件组件的直接驱动的控制(参考下文),或可选地实现为经由总线系统(例如经由I2C总线)的控制。

[0025] 依据根据其所提供的过滤器接口是硬件过滤器接口的可替代方案,所述微处理器系统可选地还包括:

[0026] 用于移动终端的外围结构的至少一个驱动器,所述至少一个驱动器可由正常操作系统驱动并且可在不安全运行时环境中执行,以及用于外围结构的-优选地简化的-驱动器,所述驱动器可由安全操作系统驱动并且可在安全运行时环境中执行以及优选地仅具有可在不安全运行时环境中执行的驱动器的功能的子集。在这种情况下,硬件过滤器接口被设计成在硬件层安全地控制可在不安全运行时环境中执行的用于外围结构的驱动器与可在安全运行时环境中执行的用于外围结构的优选地简化的驱动器之间的通信。

[0027] 所述硬件过滤器接口因此使得能通过硬件过滤器接口实现在正常操作系统下实现的驱动器部分与在安全操作系统下实现的驱动器部分之间的直接通信。

[0028] 作为终端的外围结构,例如配设(provision)由以下各项组成:NFC接口、在将连接设置到移动无线电网络时涉及的无线电接口层RIL、用于认证和加密的安全元件SE(例如SIM卡或USIM卡或安全MicroSD卡或永久地实现的嵌入式安全元件)、显示器(具体是触摸屏显示器)、能够被用来验证经由键盘输入的秘密号码PIN(个人标识号码)的PIN校查例行程序(PIN checking routine)、用于拨号到不同于移动无线电网络的网络(如,因特网(IP)或虚拟专用网络(VPN))中的拨号例行程序、缓冲存储器(例如帧缓冲器)。

[0029] 可选地,如果驱动器被实现用于在微处理器系统中的多个外围结构,则为所有外围结构提供通用硬件接口,所述硬件接口使得能实现专用于与相同的外围结构相关联的驱动器之间的不安全和安全运行时环境之间在硬件层的访问,并且阻止与不同的外围结构相关联的驱动器之间在硬件层的访问。依靠直接的硬件层访问被保留仅用于相对于相同的外围结构相互对应的驱动器,通过恶意软件(例如木马等等)对驱动器的不正确访问被避免了。

[0030] 在与不同的外围接口相关联的驱动器之间的访问至多借助于在操作系统层的安全驱动器而发生,假如这些访问依据安全驱动器的检查是被许可的。例如,安全驱动器将识别并且避开恶意软件。

[0031] 可选地,硬件过滤器接口被设计成针对与安全的相关性来检查(例如在不安全运行时环境中)对外围结构的驱动器的访问,并且在其中访问被识别为与安全相关的情况下,

该硬件过滤器接口设计成将访问传达至安全运行时环境中的简化的驱动器，以及在其中访问被识别为不与安全相关的情况下，该硬件过滤器接口被设计成将访问传达至不安全运行时环境中的驱动器。

[0032] 可选地，可在安全运行时环境中执行的用于外围结构的驱动器被简化为它仅包括对于处理安全相关的访问所需要的功能的效果。对比之下，可在不安全运行时环境中执行的用于外围结构的驱动器优选地包括驱动器的所有功能。

[0033] 依据另一可替代方案，所提供的过滤器接口是应用过滤器接口，其被设计成在应用层安全地控制不安全运行时环境与安全运行时环境之间的通信。应用过滤器接口在应用层提供直接的安全通信信道，所述通信信道使能相比经由通过操作系统层和在操作系统层操作的安全驱动器的迂回更快的通信。

[0034] 微处理器系统可选地还包括至少一个应用，其至少部分地可由正常操作系统驱动并且可在不安全运行时环境中执行，并且至少部分地可由安全操作系统驱动并且可在安全运行时环境中执行。在这种情况下，应用过滤器接口被设计成在应用层安全地控制可在不安全运行时环境中执行的至少部分应用与可在安全运行时环境中执行的至少部分应用之间的通信。

[0035] 应用可以是例如用于支付交易的银行业务或支付应用、或针对各种广泛目的(例如交通方式)用于票的购买和管理的售票应用。至少应用的安全相关功能可选地被实施在安全操作系统下。补充的非安全相关功能性可选地被附加地或排他地实现在正常操作系统下。

[0036] 与其中驱动在大多数情况下将主要地被实现在正常操作系统下的驱动器对比，例如，至于诸如银行业务应用之类的应用，绝大多数通常将被实现在安全操作系统下。

[0037] 可选地，如果多个应用被实现在微处理器系统中，则通用应用过滤器接口被提供用于所有应用，所述应用过滤器接口使得能实现专用于分别在不安全运行时环境和安全运行时环境中的与相同应用相关联的部分之间的、不安全和安全运行时环境之间在应用层的访问，并且阻止与不同的应用相关联的部分之间在应用层的访问。依靠直接的应用层访问被保留仅用于相同应用的相互对应的部分，通过恶意软件(例如木马等等)对驱动器的不正确访问被避免了。

[0038] 跨越安全和不安全运行时环境之间的边界地在不同的应用之间的应用访问借助于安全驱动器仅至多在操作系统层发生。

[0039] 可选地，应用过滤器接口被设计成针对与安全的相关性来检查(例如在不安全运行时环境中)对应用的访问，并且在其中访问被识别为与安全相关的情况下，设计成将访问传达至安全运行时环境中的至少部分应用，以及在其中访问被识别为不与安全相关的情况下，设计成将访问传达至不安全运行时环境中的至少部分应用。

[0040] 应用过滤器接口能够被设为硬件过滤器接口的可替代方案或者除硬件过滤器接口之外的另一方案。可选地，应用过滤器接口和硬件过滤器接口两者都被提供和设计以用于交互。

[0041] 依据本发明的一个发展，过滤器接口被以这样一种方式耦合到用户输出设备，例如移动终端(例如蜂窝电话)的扩音器、振动铃声器等等，即在经由过滤器接口从不安全运行时环境到安全运行时环境或/和从安全运行时环境到不安全运行时环境(也就是说跨越

安全和不安全运行时环境之间的边界)实现的任何访问之时,微处理器的用户可感觉到的用户消息被用户输出设备输出。结果,用户被使得知道跨越安全和不安全运行时环境之间的边界发生的任何访问,并且能够例如识别安全关键数据是否到达以及被从过滤器接口转发到安全运行时环境或/和数据是否被从安全运行时环境输出到不安全运行时环境。用户输出能够被配置例如为被移动终端输出的旋律。

[0042] 可选地,对于一方面从不安全运行时环境到安全运行时环境以及另一方面从安全运行时环境到不安全运行时环境跨越安全和不安全运行时环境的访问,用户可区别的不同用户输出被输出。通过示例的方式,不同的旋律取决于访问方向(从不安全运行时环境到安全运行时环境或从安全运行时环境到不安全运行时环境)而被输出。

[0043] 依据一个变例,用户消息总是在微处理器在安全运行时环境内的操作期间被操作。在这个变例中,因此,在从不安全运行时环境到安全运行时环境的访问之时输出的用户消息在在访问之后立即被输出,以便向用户通知操作现在实际上正在安全运行时环境中发生。在从安全运行时环境到不安全运行时环境的访问之时,在这个变例中,用户消息在在访问之前被立即输出以便向用户报警随即将离开安全运行时环境。可替代地或附加地,能够在程序执行实际上已经离开了安全运行时环境之后输出用户消息。同样地,可替代地或附加地,能够在安全运行时环境被程序执行进入之前输出用户消息。

附图说明

[0044] 下面基于示例性实施例并且参考附图对本发明更详细地说明,其中在示意图示中:

[0045] 图1示出了依据本发明的一个实施例的包括应用过滤器接口的微处理器系统;

[0046] 图2示出了依据本发明的一个实施例的包括硬件过滤器接口的微处理器系统;

[0047] 图3示出了依据本发明的一个实施例的包括应用过滤器接口和硬件过滤器接口的微处理器系统;

具体实施方式

[0048] 图1示出了依据本发明的一个实施例的微处理器系统,其具有ARM架构,具有不安全运行时环境100和安全运行时环境200以及具有在所有情况下部分实现在不安全运行时环境100中和部分实现在安全运行时环境200中的应用过滤器接口TLC(信任小程序连接器)。不安全运行时环境100被正常操作系统HLOS控制。安全运行时环境200被安全操作系统MobiCore控制。不安全运行时环境100与安全运行时环境200之间在操作系统层的访问借助于安全驱动器MobiCore驱动器来执行。应用APP(例如支付交易应用)中的多数APP-S被以可在安全运行时环境200中执行的方式实现在安全操作系统MobiCore下。应用APP(例如支付交易应用)的剩余部分APP-N被以可在不安全运行时环境100中执行的方式实现在正常操作系统HLOS下。根据本发明的应用过滤器接口TLC(信任小程序连接器)直接地在应用层使得能实现被以可在安全运行时环境200中执行的方式实现在安全操作系统MobiCore下的应用APP的部分APP-S与被以可在不安全运行时环境100中执行的方式实现在正常操作系统HLOS下的应用APP的部分APP-N之间的直接访问。用于外围结构PER(例如触摸屏显示器)的驱动器被以常规方式实现在依据图1的正常操作系统HLOS下,并且能够至多经由安全驱动器

MobiCore驱动器与安全运行时环境200进行通信。能够至多经由安全驱动器MobiCore驱动器从不安全运行时环境100达到在安全操作系统MobiCore下实现的新颖简化的驱动器PER-S。在不安全运行时环境100中，外围驱动器PER以由Linux I2C驱动器所控制的方式经由I2C总线系统与正常操作系统HLOS进行通信。在安全运行时环境200中，经简化的外围驱动器PER-S以由其中的I2C驱动器所控制的方式经由在安全运行时环境200中实现的I2C总线系统与安全操作系统MobiCore进行通信。外围驱动器PER与PER-S之间的通信能够借助于MobiCore驱动器至多在操作系统层发生。

[0049] 图2示出了依据本发明的一个实施例的微处理器系统，其包括硬件过滤器接口即虚拟I2C驱动器。除非在这里另外描述，否则具有与图1中相同的命名的部分对应于来自图1的部分。用于外围结构PER(例如触摸屏显示器)的驱动器被实现在正常操作系统HLOS下。用于外围结构的新颖简化的外围驱动器PER-S被实现在安全操作系统MobiCore下。在每种情况下部分地实现在不安全运行时环境100中并且部分地实现在安全运行时环境200中的虚拟I2C驱动器(示例性的硬件过滤器接口)在硬件层更准确地说在I2C总线层使得能实现在正常操作系统HLOS下实现的外围驱动器PER与在安全操作系统下实现的经简化的外围驱动器PER-S MobiCore之间的安全通信。在不安全运行时环境100中，外围驱动器PER经由Linux I2C驱动器与正常操作系统HLOS进行通信。在安全运行时环境200中，经简化的外围驱动器PER-S经由其中的I2C驱动器与安全操作系统MobiCore进行通信。硬件过滤器接口(即虚拟I2C驱动器)在比操作系统层更接近于外围驱动器的层的硬件层处在总线系统在HLOS下的LinuxI2C驱动器与总线系统在MobiCore下的I2C驱动器之间提供安全通信信道。在来自图2的示例性实施例中，应用APP中的部分APP-N、APP-S能够主要借助于MobiCore驱动器仅至多在操作系统层与彼此进行通信。

[0050] 图3示出了依据本发明的一个实施例的微处理器系统，其包括应用过滤器接口TLC和硬件过滤器接口虚拟I2C驱动器。图3因此首先图示了来自图1和图2的实施例的组合。此外，应用过滤器接口TLC和硬件过滤器接口虚拟I2C驱动器协作。就不安全运行时环境100而言，硬件过滤器接口(虚拟I2C驱动器)经由总线系统Linux I2C驱动器与外围驱动器PER进行通信。对于安全运行时环境200，硬件过滤器接口(虚拟I2C驱动器)与应用过滤器接口TLC进行通信并且因此从硬件层改变为应用层。最后，应用过滤器接口TLC在应用层进入到安全运行时环境200中与经简化的外围驱动器PER-S进行通信。

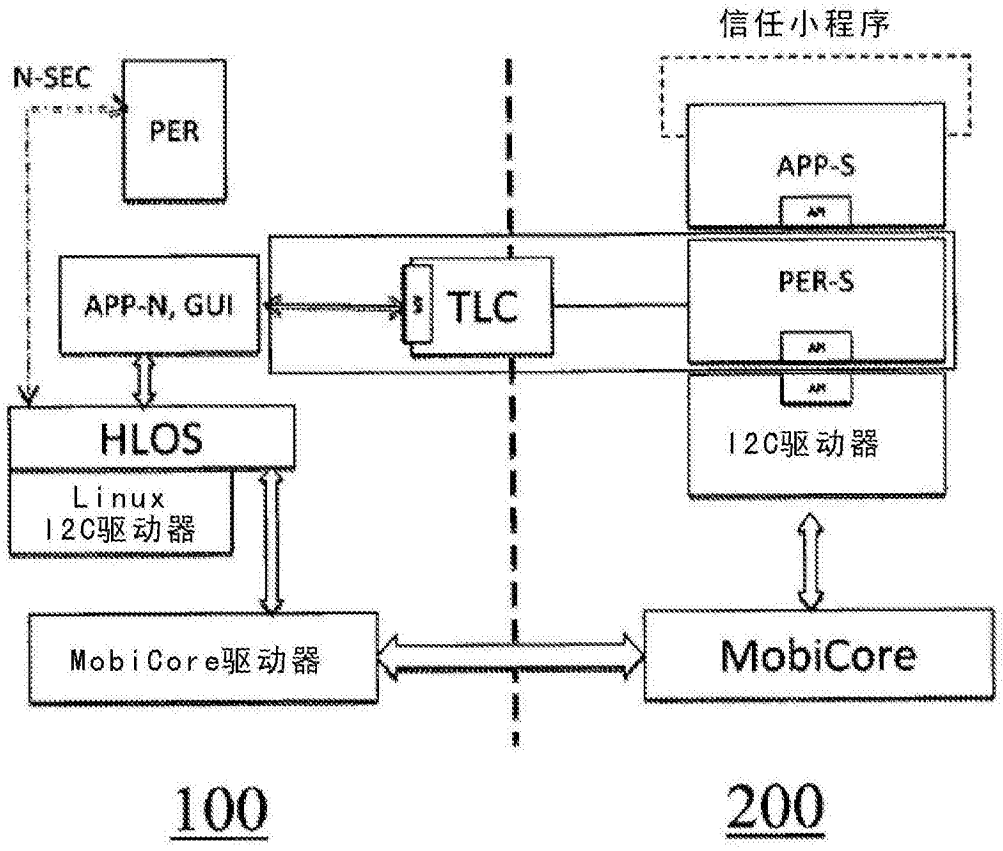

信任小程序
N-SEC
PER
APP-S
APP-N, GUI
TLC
PER-S
HLOS
Linux
I2C驱动器
I2C驱动器
MobiCore驱动器
MobiCore
100
200

图1

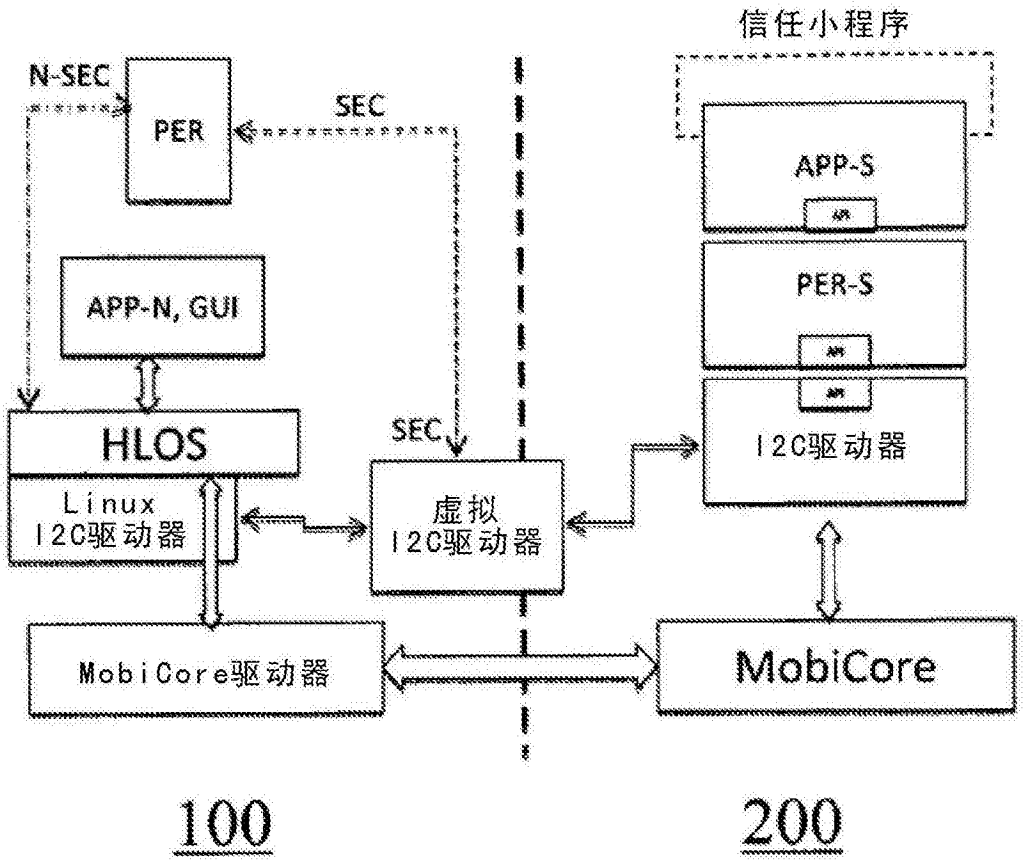

信任小程序
N-SEC
PER
SEC
APP-S
APP-N, GUI
PER-S
HLOS
SEC
I2C驱动器
Linux
I2C驱动器
虚拟
I2C驱动器
MobiCore驱动器
MobiCore
100
200

图2

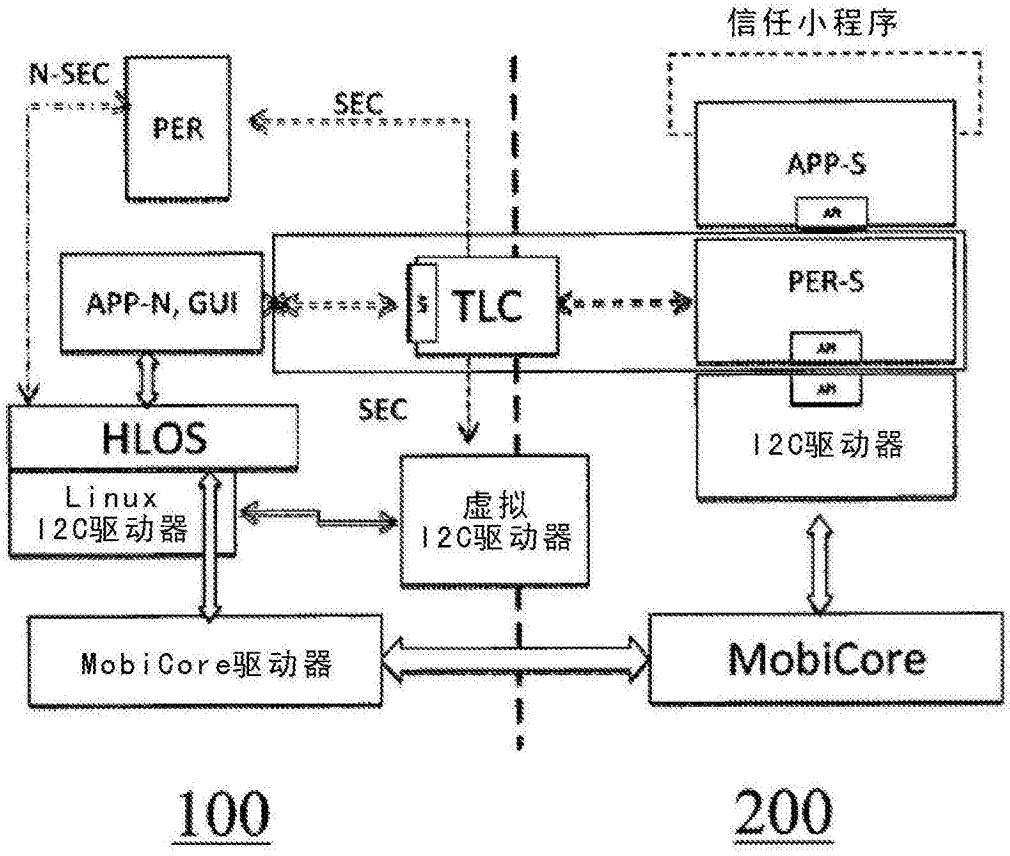

信任小程序
N-SEC
PER
SEC
APP-S
APP-N, GUI
TLC
PER-S
HLOS
SEC
I2C驱动器
Linux
I2C驱动器
虚拟
I2C驱动器
MobiCore驱动器
MobiCore
100
200

图3