(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113557515 B
(45)授权公告日 2025.01.28

(21)申请号 202080020060.3
(22)申请日 2020.10.31
(65)同一申请的已公布的文献号
申请公布号 CN 113557515 A
(43)申请公布日 2021.10.26
(30)优先权数据
62/929,514 2019.11.01 US
(85)PCT国际申请进入国家阶段日
2021.09.09
(86)PCT国际申请的申请数据
PCT/US2020/058445 2020.10.31
(87)PCT国际申请的公布数据
WO2021/087418 EN 2021.05.06
(73)专利权人 谷歌有限责任公司
地址 美国加利福尼亚州
(72)发明人 斯科特·D·约翰森
蒂莫西·杰伊·陈
马克·戴维·海特
多米尼克·安托尼·里佐 金恩赞
迈克尔·斯特法诺·弗里茨·沙夫纳
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
专利代理师 邓聪惠 周亚荣
(51)Int.Cl.
G06F 21/72(2013.01)
G06F 21/60(2013.01)
G06F 11/10(2006.01)
(56)对比文件
US 2003115503 A1,2003.06.19
CN 109844725 A,2019.06.04
审查员 刘佳菡

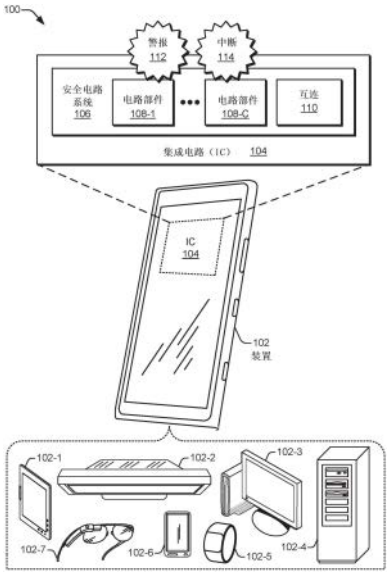
权利要求书3页 说明书32页 附图13页

(54)发明名称

外围设备与安全电路系统的兼容性

(57)摘要

IC芯片可以提供硅信任根(RoT)功能。在所描述的实现方式中,IC芯片包括处理器(202)、互连(110)和多个外围设备(250)。这些兼容电路部件被设计来促进安全电路系统的互操作性和一致的预期通信。每个外围设备包括接口(302),该接口遵守用于与处理器和其他外围设备交互的公共框架。该接口包括将外围设备耦合到互连的互连接口(304)和将外围设备耦合到至少一个其他外围设备的设备间接口(306)。根据接口规范的设备间方案,基于指示设备间信令(316)的外围设备设计代码来实现外围设备。制造商基于设计代码制造外围设备,以便以可预测的方式在物理和逻辑上耦合到另一外围设备。这促进了更鲁棒和可靠的安全电路系统。



CN 113557515 B

1.一种装置,包括:

包括安全电路系统的集成电路芯片,所述安全电路系统包括:

互连;

耦合到所述互连的处理器;

至少一个总线;以及

多个外围设备,每个外围设备耦合到所述互连以及所述至少一个总线,每个外围设备包括接口,所述接口被配置为遵守用于与所述处理器和所述多个外围设备中的一个或多个其他外围设备交互的公共框架,所述接口包括:

互连接口,所述互连接口被配置为将相应的外围设备耦合到所述互连,所述相应的外围设备被配置为使用所述互连接口经由所述互连与所述处理器通信;以及

设备间接口,所述设备间接口被配置为将所述相应的外围设备耦合到所述多个外围设备中的所述一个或多个其他外围设备,所述相应的外围设备被配置为使用所述设备间接口经由所述至少一个总线与所述多个外围设备中的所述一个或多个其他外围设备通信,其中,所述设备间接口响应于包括在用于所述相应的外围设备的设计代码中的属性而耦合到延伸到所述多个外围设备中的另一外围设备的至少一条导线。

2.根据权利要求1所述的装置,其中,每个外围设备包括相应的安全功能模块,所述相应的安全功能模块被配置为提供相应的安全相关功能。

3.根据权利要求2所述的装置,其中,所述相应的安全相关功能包括以下中的至少一项:

警报处置;

密码操作;

安全的数据存储;

随机数生成;以及

所述安全电路系统的输入/输出通信。

4.根据权利要求1所述的装置,其中,所述接口包括时钟接口,所述时钟接口包括对于下述的访问:

主要系统时钟,所述相应的外围设备被配置为至少基于所述主要系统时钟使用所述互连与所述处理器通信;以及

一个或多个次要系统时钟,所述相应的外围设备被配置为至少基于所述一个或多个次要系统时钟使用所述至少一个总线执行功能或与所述多个外围设备中的另一外围设备进行通信。

5.根据权利要求1所述的装置,其中:

所述多个外围设备中的所述相应的外围设备包括至少一个警报发送器模块;以及

所述至少一个警报发送器模块被配置为经由信令通路传输来自所述相应的外围设备的警报指示。

6.根据权利要求5所述的装置,其中:

所述信令通路包括至少一个差分路径;以及

所述至少一个警报发送器模块被配置为响应于检测到所述信令通路的所述至少一个差分路径的完整性故障而传输警报完整性故障信号。

7.根据权利要求1所述的装置,其中,所述集成电路芯片包括以下中的至少一个:

片上系统(SoC);以及

信任根(RoT)芯片。

8.根据权利要求1至7中任一项所述的装置,其中:

所述相应的外围设备包括寄存器接口,所述寄存器接口包括用于与所述相应的外围设备相关联的中断的至少一个中断入口;以及

所述相应的外围设备被配置为将所述寄存器接口的至少一部分暴露给所述处理器。

9.根据权利要求8所述的装置,其中:

所述至少一个中断入口包括:

中断使能指示;

中断状态指示;以及

中断测试寄存器;以及

所述相应的外围设备被配置为提供所述处理器访问以清除所述中断状态指示。

10.根据权利要求1所述的装置,其中,所述至少一个总线专用于所述多个外围设备。

11.一种用于外围设备与安全电路系统的兼容性的方法,所述安全电路系统是集成电路芯片的一部分,所述方法包括:

基于互连方案根据用于处理器和多个外围设备之间的交互的公共框架,由所述处理器通过互连与所述多个外围设备中的外围设备进行通信;所述安全电路系统包括所述处理器、所述多个外围设备,所述互连以及至少一个总线;所述外围设备包括接口,所述接口包括互连接口和设备间接口;

基于所述互连方案根据所述公共框架,由所述外围设备通过所述互连并且经由所述互连接口与所述处理器进行通信;以及

基于设备间方案根据用于在所述多个外围设备中的至少两个外围设备之间的交互的所述公共框架,由所述外围设备通过所述至少一个总线并且经由所述设备间接口与所述多个外围设备中的另一外围设备进行通信,其中,由所述外围设备通过所述至少一个总线并且经由所述设备间接口与所述多个外围设备中的所述另一外围设备进行通信包括:

由所述外围设备使用从通过用于所述外围设备的设计代码指定的属性导出的电路系统向所述另一外围设备传输设备间信号。

12.根据权利要求11所述的方法,其中,由所述外围设备通过所述至少一个总线并且经由所述设备间接口与所述多个外围设备中的所述另一外围设备进行通信包括:

由所述外围设备绕过所述互连与所述另一外围设备进行通信。

13.根据权利要求11所述的方法,其中:

由所述外围设备通过所述至少一个总线并且经由所述设备间接口与所述多个外围设备中的所述另一外围设备进行通信包括由所述外围设备从所述另一外围设备接收升级命令,所述另一外围设备包括警报处置器;以及

所述方法进一步包括响应于从所述警报处置器接收到所述升级命令,由所述外围设备激活对策。

14.根据权利要求11至13中任一项所述的方法,其中:

由所述外围设备通过所述互连并且经由所述互连接口与所述处理器进行通信包括由

所述外围设备基于所述外围设备的中断入口的中断状态指示向所述处理器传输中断信号；以及

由所述处理器通过所述互连与所述外围设备进行通信包括清除所述中断入口的所述中断状态指示。

外围设备与安全电路系统的兼容性

背景技术

[0001] 电子设备在制造、通信、运输、医疗保健、商业、社交互动和娱乐中扮演着不可或缺的角色。例如,电子设备为服务器群提供动力,服务器群为商业和通信提供基于云的分布式计算功能。电子设备还嵌入到许多不同类型的现代设备中,从医疗设备到电器,从车辆到工业工具。个人电子设备使能便携式视频观看和方便地访问智能数字助理。此外,一种多功能电子设备——智能手机——实际上已成为触手可及的必需品。随着电子设备对于现代生活的许多方面变得普遍且至关重要,设备安全已变得势在必行。

[0002] 许多人熟悉恶意软件,其有时被统称为“计算机病毒”。某些恶意软件被设计来未经授权访问电子设备存储的信息或以其他方式危害电子设备。几种策略可以通过抗击某些类型的恶意软件来帮助保护用户的设备和信息免受安全威胁。这些策略包括采用并定期更新弹性操作系统、参与安全计算实践以及安装反恶意软件程序。不幸的是,这些策略无法使电子设备免受所有恶意软件攻击。

[0003] 此外,除了由基于软件的恶意软件执行的攻击之外,电子设备也可能容易受到其他类型的攻击。例如,电子设备的安全和可靠运行以及此类设备存储的信息的安全性可能受到硬件上的物理攻击和对于无线通信的射频攻击的危害。换句话说,某些形式的攻击可以规避或破坏上面列出的策略,使不法分子能够破坏电子设备并获得对与该设备一起使用的任何账户的访问。

[0004] 电子设备包括至少一个集成电路(IC),其提供智能以使能各种功能。这些功能促进商业、简化医疗保健访问、提供娱乐、支持社交媒体交互并使能上述其他服务。电子设备还可以存储或否则利用要保护的信息。为了支持这些功能并促进安全操作,一些电子设备以作为IC一部分的安全电路系统的形式包含基于硬件的保护。不幸的是,现有的安全电路系统方法不足以对抗当今对电子设备发动的各种软件、硬件和无线攻击。

发明内容

[0005] 某些电子设备——如服务器计算机和智能手机——负责向用户提供服务。用户依靠这些电子设备来获取使用一个或多个帐户访问的关键服务,例如用于金融服务或航空旅行的那些。由于电子设备和账户之间的链接,被破坏的电子设备可能允许对链接到账户的服务进行不希望的访问或允许对账户本身进行未经授权的访问。此外,为了提供与账户相关联的服务,这些电子设备可能存储需要保护的与账户相关的信息,诸如财务数据、用户名、密码和用于加密的密钥。不幸的是,反恶意软件程序无法阻止针对电子设备的所有攻击途径。例如,反恶意软件程序可能无法针对使用微型探针检测在集成电路(IC)芯片上的电压电平的直接物理攻击提供保护。因此,将可以识别、阻止、排斥或否则阻挠对电子设备的攻击——包括抵制物理攻击——的基于硬件的措施并入电子设备是有益的。

[0006] 因此,电子设备可以包括安全电路系统以抗击来自不良行为者的攻击。在某些情况下,安全电路系统检测到不适当或可疑的活动并采取保护措施。安全电路系统可以以不同的方式实现。例如,计算机工程师可以将安全电路系统制造为独立的IC芯片或另一芯片

的一部分,诸如片上系统(SoC)。在任一情况下,安全电路系统可以是受保护的飞地、可信芯片平台、基于硬件的信任根(RoT)(例如硅RoT)或其组合的一部分。不管安全电路如何或在何处合并到电子设备中,计算机工程师都可以设计安全电路来抗击许多不同类型的攻击,如下所述。

[0007] 对电子设备的攻击可以采取以下形式:观察屏幕图像或监测重复行为以推断信息的程序、尝试从存储器的受保护区域读取数据的应用程序和电路系统的直接物理探测等。安全电路系统执行多种功能来对抗这些攻击中的一种或多种。例如,安全电路系统可以在使用过程中、传输时或存储中保护加密密钥。为此,可以采用专用存储器和专用数据总线。安全电路系统还可以在与可能作为恶意软件运行的应用分开的区域中生成高质量的伪随机数或运行加密引擎。此外,安全电路系统可以确保使用正确的、未篡改的启动基本输入/输出系统(BIOS)来启动硬件。

[0008] 因此,安全电路系统可以负责实现多种功能以对抗对电子设备的各种攻击。然而,对于安全电路系统的现有方法采用专门设计的硬件架构。安全电路系统的不同电路部分也可以设计成彼此相对隔离。因此,旨在对抗各种安全威胁的电路部分可能无法按预期进行互操作,从而使硬件安全性降低。此外,不良的部件间通信为潜在的不良行为者创造了另一种攻击途径。此外,这种专门的方法使安全电路系统的设计和测试阶段更加艰巨、耗时且成本更高。这可能导致在开发安全架构时忽略或未充分解决某些安全威胁。因此,这些专门的架构使得保护电子设备免受各种不同的安全威胁变得更加困难。

[0009] 相比之下,本文件描述了提供适应性强和灵活的框架或平台的手段,该框架或平台可以产生弹性和可编程的安全硬件以对抗对电子设备的各种形式的攻击。在安全电路系统的一些实现方式中,不同类型的电路或提供不同安全相关功能的电路部分使用扩展协议进行通信,该协议仍然产生特定且一致的信令。通信协议使提供不同安全相关功能的电路能够根据指定的设计框架进行无缝交互。

[0010] 设计框架和通信协议产生兼容部件,使得即使是彼此分开设计的电路部件也适合与稳定、可预测的交互一致地部署在一起。例如,可以至少部分标准化通信和其他形式的交互(例如,诸如总线、接口或存储器的资源的共享),以提供可预测性和互操作性的度量。如本文所用,“兼容部件”包括被设计为遵守公共框架以使得这些部件适合一起使用的那些部件。在某些情况下,兼容性在集成电路芯片的两个或更多个安全相关部件之间提供了一定程度的即插即用能力。

[0011] 在一些实现方式中,除了处理器和互连之外,安全电路系统还包括多个外围设备。多个外围设备中的每个外围设备执行有助于安全电路系统的安全或正常运行的一些功能。因此,每个外围设备都可以提供核心或支持安全相关的功能。该功能,如控制对数据的访问或执行加密操作,支持安全电路系统的总体目的,包括提供特征以通过电子设备的其他电路系统和/或IC实现安全计算。为了可预测性和互操作性,可以将每个外围设备实现为兼容部件。

[0012] 为了生产兼容部件,可以将每个外围设备设计成遵守指定的通信接口。由于每个外围设备根据相同或协调的通信协议进行通信,因此互操作性的可能性要大得多。因此,计算机工程师和计算机科学家可以专注于设计每个外围设备的安全相关功能。由于至少两个原因,这使得能够产生卓越的安全电路系统。首先,两个或更多个外围设备之间的计划通信

按预期发生,因为每个外围设备遵循相同的设计接口规范。其次,在安全电路系统上投入的工时可以被分配到设计和测试安全功能,而不是检测和调试部件间的通信问题。

[0013] 在示例实现方式中,每个外围设备包括被设计为遵守接口规范以使用公共或协调通信协议的接口。通信接口可以包括与主互连或主机处理器交互的互连接口、与其他外围设备交互的设备间接口或用于进入或离开给定外围设备的其他信号的另一接口。另一接口可以指定外围设备如何使用一个或多个时钟信号与至少一个芯片输入/输出接口和与至少一个中断信号等进行通信。例如,为了产生设备间接口,基于接口规范的设备间方案来准备外围设备的设计代码。因此,设计代码识别外围设备要使用的属性,如设备间信号。

[0014] 接口规范还可以定义用于外围设备的寄存器接口。在这里,寄存器接口的每个寄存器可以用于控制、状态或通信。例如,中断寄存器可以被实例化以用于例如外围设备和处理器之间的通信。中断寄存器可以包括中断使能指示、中断状态指示和中断测试指示。这些指示可用于在主机处理器和外围设备之间提供一致的交互以处置中断。在其他实现方式中,外围设备参与用于警报处置和警报升级的兼容通信。

[0015] 在这些方式中,安全电路系统可以被并到硅RoT芯片和/或SoC中。安全电路系统包括多个外围设备,每个外围设备都与其他外围设备兼容,以确保外围设备之间预期的兼容性和一致的通信。通过遵守通信框架,外围设备的设计工作可以集中在与安全相关的功能上。因此,通过利用在通信接口规范中阐述的定义的设备间通信,可以以可预测的方式实现适应性强和多样化的安全响应。

[0016] 下面描述的方面包括用于外围设备与安全电路系统的兼容性的集成电路。集成电路的安全电路系统包括互连、耦合到互连的处理器和多个外围设备。每个相应的外围设备被耦合到互连并且包括被配置为遵守用于与处理器和多个外围设备中的其他外围设备交互的公共框架的接口。该接口包括被配置为将相应外围设备耦合到互连的互连接口。该接口还包括设备间接口,其被配置为将相应的外围设备耦合到多个外围设备中的其他外围设备。

[0017] 下面描述的方面包括用于外围设备与安全电路系统的兼容性的方法,该方法可以由集成电路的至少一部分来执行。该方法包括由处理器通过互连基于互连方案根据用于处理器和多个外围设备之间的交互的公共框架与多个外围设备中的外围设备进行通信。该方法还包括由外围设备通过互连基于互连方案根据公共框架与处理器进行通信。该方法还包括由外围设备基于设备间方案根据用于多个外围设备中的至少两个外围设备之间的交互的公共框架与多个外围设备中的另一外围设备进行通信。

[0018] 下面描述的方面包括用于外围设备与安全电路系统的兼容性的方法,该方法可以由集成电路的至少一部分执行。该方法包括接收对应于安全电路系统的外围设备的外围设备设计代码,其中,外围设备设计代码包括设备间信令的一个或多个指示。该方法还包括分析外围设备设计代码,包括将设备间信令的一个或多个指示与用于至少在安全电路系统内进行通信的公共框架的接口规范的设备间方案进行比较。该方法还包括,响应于分析,提供指示外围设备设计代码是否与接口规范的设备间方案一致的兼容性报告。

附图说明

[0019] 参考以下附图描述用于外围设备与安全电路系统的兼容性的装置和技术。贯穿附

图使用相同的数字来表示相同的特征和部件。

[0020] 图1图示了具有集成电路(IC)的示例装置,该集成电路包括可以实现外围设备兼容性的安全电路系统。

[0021] 图2图示了包括多个电路部件的示例安全电路系统,其包括可以实现为可兼容的多个示例外围设备。

[0022] 图3图示了包括至少一个接口以支持与其他电路部件的兼容性的示例外围设备。

[0023] 图4图示了分析外围设备设计以确保满足可兼容目标的示例手段。

[0024] 图5-1图示了包括寄存器接口和示例通信信号的示例外围设备。

[0025] 图5-2图示了具有多个中断入口的示例寄存器接口。

[0026] 图5-3图示了示例中断入口。

[0027] 图5-4图示了用于处理外围设备和处理器之间的中断的示例时序图。

[0028] 图6图示了在警报处置器的警报接收器模块和外围设备的警报发送器模块之间的示例通信关系。

[0029] 图7图示了在警报处置器的升级发送器模块和升级处置器类型的外围设备的升级接收器模块之间的示例通信关系。

[0030] 图8图示了装置实现外围设备与安全电路系统的兼容性的示例方法。

[0031] 图9图示了的装置实现外围设备与安全电路系统的兼容性的其他示例方法。

[0032] 图10示出了根据所描述的一个或多个方面可以实现外围设备与安全电路系统的兼容性的示例电子设备的各种部件部件。

具体实施方式

[0033] 概述

[0034] 电子设备对现代社会做出重要贡献,诸如用于通信、安全和制造的那些。每个电子设备都依赖于具有处理能力来提供一些功能的集成电路(IC)。由于这些功能中的许多功能的关键性质,电子设备可能包括带有安全电路系统的IC以提供保护。安全电路系统减少了信息被无意暴露或以有害或未经授权的方式使用一些功能的机会。安全电路系统可以以多种形式实现,其中一种涉及信任根(RoT)范式。

[0035] 对于RoT硅,基于硬件的机制在防止对信息的不当访问和阻止对设备的未授权使用等方面保持计算安全。硅RoT原则可以帮助确保硬件基础设施和在其上执行的软件都保持在其预期的、值得信赖的状态。为此,硅RoT可以使用授权和可验证的代码验证关键系统部件安全启动。因此,它可以确保服务器或另一电子设备用正确的固件启动,并且固件没有被低级恶意软件感染。硅RoT可以提供额外的或替代的安全优势。例如,它可以提供加密性独特的机器身份;这种独特的身份使操作员能够验证电子设备是合法的。此外,它可以将加密密钥和其他信息维持在防篡改的孤岛中,这甚至可以防止那些可以物理访问设备的人获取信息。锚定在硬件中的RoT服务还可以提供权威的、防篡改的审计记录和其他运行时安全服务。

[0036] 芯片设计者可以将硅RoT技术合并到专注于提供安全功能的单个IC芯片中。或者,RoT硅可以与其他电路系统集成,包括在中央处理单元(CPU)芯片或封装中、在图形处理单元(GPU)芯片或卡中、在片上系统(SoC)中和在存储器存储设备中等。通常,安全电路系统可

以在服务器主板、网卡、客户端设备(例如膝上型电脑和智能手机)、消费者路由器、物联网(IoT)设备以及固定和便携式存储单元中操作,仅举几个示例。通过将RoT锚定在硅中,无论应用或电子设备如何,在硬件、固件和软件级别上增强计算安全性。硅RoT还增强了直接或通过网络相互通信的不同设备上的安全性。尽管本文档中使用硅或硬件RoT环境描述了一些安全和电路设计原则,但这仅作为示例进行,因为所描述的原则通常适用于安全电路系统。

[0037] 在当今的计算环境中,不良行为者可以使用多种攻击向量在无数级别上攻击电子设备。例如,可以使用通过互联网传输的恶意软件进行攻击,以尝试获取存储在膝上型电脑中但用户希望受到安全保护的信息。此外,攻击可能涉及在设备运输期间或设备在未观察到的位置操作时将恶意软件注入用于启动电子设备——如Wi-Fi®路由器或IoT设备——的固件。作为另一示例,不良行为者可能窃取电子设备,并有足够的时间对设备进行直接物理攻击。这种直接物理攻击可以包括切断导线、探测电压以及重复运行代码以观察趋势和推断信息等。

[0038] 因此,安全电路系统可以负责实现多种功能以对抗对电子设备的各种攻击。然而,现有的安全电路系统方法采用临时设计的硬件架构。安全电路系统的不同电路部分也可以设计成彼此相对隔离。因此,被设计为对抗各种安全威胁的电路部分可能无法按预期进行互操作,从而使硬件安全性降低。此外,不良的部件间通信为潜在的不良行为者创造了另一种攻击途径。此外,这种临时方法使安全电路系统的设计和测试阶段更加艰巨、耗时且成本更高。这可能导致在开发安全架构时忽略或未充分解决某些安全威胁。因此,这些临时架构使得保护电子设备免受各种不同的安全威胁变得更加困难。

[0039] 相比之下,该文档描述了提供适应性强且灵活的框架或平台的方法,该框架或平台可以产生弹性和可编程的安全硬件以对抗对电子设备的各种形式的攻击。在安全电路系统的一些实现方式中,不同类型的电路或提供不同安全相关功能的电路部分使用扩展协议进行通信,该协议仍然产生特定且一致的信令。通信协议使提供不同安全相关功能的电路能够根据指定的设计框架进行无缝交互。

[0040] 设计框架和通信协议产生兼容的部件,使得即使是彼此分开设计的电路部件也适合与稳定、可预测的交互一致地部署在一起。例如,通信和其他形式的交互(例如,诸如总线、接口或存储器的资源的共享)可以至少部分标准化,以提供可预测性和互操作性的度量。如本文所用,“兼容部件”包括被设计为遵守公共框架以使得这些部件适合一起使用的那些部件。在某些情况下,兼容在集成电路芯片的两个或更多个安全相关部件之间提供了一定程度的即插即用能力。

[0041] 在一些实现方式中,除了处理器和互连之外,安全电路系统包括多个外围设备。多个外围设备中的每个外围设备执行一些有助于安全电路系统的安全或正常运行的功能。因此,每个外围设备可以提供核心或支持安全相关的功能。该功能——如控制对数据的访问或执行加密操作——支持安全电路系统的总体目的,其包括提供特征以通过电子设备的其他电路系统和/或IC实现安全计算。为了可预测性和互操作性,可以将每个外围设备实现为兼容部件。

[0042] 为了生产兼容部件,可以将每个外围设备设计成遵守指定的通信接口。由于每个外围设备都根据相同或协调的通信协议进行通信,因此互操作性的可能性大得多。因此,计

算机工程师和计算机科学家可以专注于设计每个外围设备的安全相关功能。由于至少两个原因,这使得能够产生卓越的安全电路系统。首先,两个或更多个外围设备之间的计划通信按预期发生,因为每个外围设备都遵循相同的设计接口规范。其次,在安全电路系统上投入的工时可以被分配用于设计和测试安全功能,而不是检测和调试部件间的通信问题。

[0043] 在示例实现方式中,每个外围设备包括被设计为遵守接口规范以使用公共或协调通信协议的接口。通信接口可以包括与主互连或主机处理器交互的互连接口、与其他外围设备交互的设备间接口或用于进入或离开给定外围设备的其他信号的另一接口。另一接口可以指定外围设备如何使用一个或多个时钟信号与至少一个芯片输入/输出接口和与至少一个中断信号等进行通信。例如,为了产生设备间接口,基于接口规范的设备间方案准备外围设备的设计代码。因此,设计代码标识外围设备要使用的属性,如设备间信号。在下面参考图3、4和5-1描述外围设备接口和设计代码分析的示例。

[0044] 接口规范还可以定义用于外围设备的寄存器接口。在这里,寄存器接口的每个寄存器都可以用于控制、状态或通信。例如,中断寄存器可以被实例化以用于例如外围设备和处理器之间的通信。中断寄存器可以包括中断使能指示、中断状态指示和中断测试指示。这些指示可用于在主机处理器和外围设备之间提供一致的交互。下面参考图5-2到5-4描述以可兼容方式在安全电路系统中使用中断的示例。本文档还描述了外围设备与安全电路系统的兼容性的其他方面和实现。在此描述的这些方面和实现中的每一个都可以单独使用或以任何组合使用。

[0045] 在其他实现方式中,设备外设可以交换警报。通常,警报被认为比中断更重要或更令人担忧。换句话说,在RoT或其他安全硅环境中不应忽视的安全风险可能被指定为警报,而不是基本或默认处理器中断。尽管如此,系统仍然可以尝试利用处理器的智能和资源来解决潜在的安全事件。如果处理器未能解决中断,则称为警报处置器的外围设备采取补救措施,包括可能引导激活安全对策。根据所描述的实现方式,其他外围设备可以以规定的方式向警报处置器传输警报指示。可以通过差分路径来实现警报处置器中的模块与外围设备中的模块之间的信令通路,以促进弹性。此外,警报处置器或警报发送外围设备可以包括完整性故障电路系统,其检查信令通路的正确差分功能。在其他实现方式中,警报处置器升级未解决的警报,并且升级处置器可以作为响应激活对策。在下面参考图6和7描述警报处理和升级的示例,包括可以变得兼容的相关联的通信信令。

[0046] 以这些方式,安全电路系统可以被合并到硅RoT芯片和/或SoC中。安全电路系统包括多个外围设备,其各自与其他外围设备兼容,以确保外围设备之间预期的兼容性和一致的通信。通过遵守通信框架,外围设备的设计工作可以集中在与安全相关的功能上。因此,通过利用在通信接口规范中阐述的定义的设备间通信,可以以可预测的方式实现适应性强和多样化的安全响应。尽管在安全电路系统环境中描述了兼容性的一些方面,但是所公开的兼容性概念适用于设计、创建和操作其他类型和目的的电路系统。

[0047] 下面参考相关图讨论各种细节级别的示例实现方式。下面的讨论首先阐述示例操作环境,然后描述示例硬件、方案和技术。此后参考流程图或图表描述示例方法。最后,描述了示例计算设备。

[0048] 外围设备与安全电路系统的兼容性的示例操作环境

[0049] 图1通常在100处示出了具有集成电路104(IC 104)的示例装置102,该集成电路

104(IC 104)包括安全电路系统106。装置102、集成电路104和/或安全电路系统106可以实现这里描述的外围设备与安全电路系统的兼容性。在该示例中,装置102被描绘为智能电话。然而,装置102可以被实现为任何合适的计算或电子设备。

[0050] 装置102的示例包括移动电子设备、移动通信设备、调制解调器、蜂窝或移动电话、移动站、游戏设备、导航设备、媒体或娱乐设备(例如,媒体流传输器或游戏控制器)、膝上型电脑、台式电脑、平板电脑、智能电器、车载电子系统、可穿戴计算设备(例如衣服、手表或现实改变眼镜)、物联网(IoT)设备、传感器、库存管理设备、机器或设备(例如车辆或机器人)的电子部分、存储器存储设备(例如固态驱动器(SSD))和服务器计算机或其一部分(例如服务器刀片或机架或数据中心的另一部分))等。装置102的图示示例包括平板设备102-1、智能电视102-2、台式计算机102-3、服务器计算机102-4、智能手表102-5、智能手机(或文档阅读器)102-6和智能眼镜102-7。

[0051] 在示例实现方式中,装置102包括至少一个集成电路104。集成电路104可以被安装在模块、卡或印刷电路板(PCB)(未示出)上。PCB的示例包括柔性PCB、刚性PCB、单层或多层PCB、表面安装或通孔PCB和它们的组合等等。每个集成电路104可以被实现为通用处理器、片上系统(SoC)、面向安全的IC(例如,RoT IC芯片)、存储器芯片、通信IC(例如,调制解调器或射频IC)、图形处理器、人工智能(AI)加速器及其组合等。集成电路104可以单独封装,或与其他IC芯片一起封装。

[0052] 如图所示,集成电路104包括安全电路系统106。安全电路系统106可以包括多个部分,包括:多个电路部件108-1…108-C,其中,C代表正整数;以及互连110。除了互连110之外,电路部件108的示例包括处理器和多个外围设备。这些在图2中进行了描绘并在下面进行了描述。尽管图1中没有明确示出,集成电路104可以包括除安全电路系统106之外的其他部分。虽然多个电路部件108-1…108-C和互连110可以如图所示一起被集成在单个IC上,部件也可以分布在两个或更多个IC上。安全电路系统106可以被实现为例如受保护的飞地、可信芯片平台和基于硬件的可信根(RoT)芯片(例如,硅RoT)等等。不管安全电路106如何或在何处合并到电子设备中,安全电路106都可以抗击许多不同类型的攻击。

[0053] 在示例操作中,一旦检测到攻击——或潜在攻击——或异常发生,则一些部件生成警报112或中断114。例如,电路部件108可以生成警报112并且可以将警报112传输到警报处置器,如下所述。附加地或替代地,另一电路部件108可以生成中断114以供处理器处理。根据用于安全电路系统106的处理器和/或外围设备之间的交互的公共框架在两个或更多个部件108之间传送警报112、中断114和其他信号。公共框架可以指定在每个外围设备处的接口和信令,以促进跨多个外围设备的互操作性和一致通信协议的使用。因此,虽然在安全电路系统方面呈现了兼容性的某些方面,但外围设备兼容性也可以用于其他类型的电路系统。本文档描述了示例框架以及示例通信接口。参考图3和4描述示例通信接口和接口规范。下面参考图5-1到5-4描述示例信令方案和对应的硬件,重点是中断。然而,参考图2,接下来描述安全电路系统106的示例架构。

[0054] 图2图示了示例安全电路系统106,其包括多个电路部件,包括可以实现为可兼容的多个示例外围设备250。如图所示,安全电路系统106包括耦合到互连110的处理器202。可以使用例如总线、交换结构或使各种电路部件能够通信的总线网络来实现互连110。除了互连110和处理器202之外,多个电路部件108-1…108-C(图1)可以包括多个存储器和多个外

围设备。处理器202、多个存储器和多个其他外围设备250中的每一个都直接或间接地耦合到互连110。

[0055] 在示例实现方式中,多个存储器可以包括只读存储器206(ROM206)、静态随机存取存储器208(SRAM 208)和闪存210。多个外围设备250可以包括警报处置器204、高级加密标准(AES)引擎212(AES引擎212)、基于散列的消息认证代码(HMAC)引擎214(HMAC引擎214)、串行外围接口(SPI)设备230(SPI设备230)和快闪控制器216。多个外围设备250还可以包括通用异步接收器/传输器(UART)单元218(UART单元218)、通用输入/输出(GPIO)接口220(GPIO接口220)、引脚多路复用器222(pin mux 222)和板控制器224。多个外围设备250还可以包括随机数发生器232(RNG 232)和定时器234。此外,外围设备250可以包括任何存储器,如图2所示。虽然在图2中描绘或在此描述存储器和其他外围设备250的某些示例,安全电路系统106的给定实现方式可以包括处理器、控制器、存储器、模块或外围设备的更多、更少和/或不同实例,包括其副本。

[0056] 所示的电路部件可以基于一个或多个时钟信号同步操作。尽管图2中未示出,但是安全电路系统106可包括至少一个时钟生成器以生成时钟信号,或可包括重置电路系统以彼此独立地重置一个或多个单独部件、联合重置多个部件或重置整个IC芯片。或者,安全电路系统106可以从安全电路106外部的源接收至少一个时钟信号或重置信号,该源可以在或可以系统不在单独的芯片上。一个或多个单独的外围设备250可以在相应的独立时钟域中操作。例如,输入/输出(I/O)外围设备可以与相应I/O设备或信道本地的时钟同步。不同时钟域中的外围设备可以相对于彼此异步操作或通信。

[0057] 下面描述所示部件的示例实现方式。处理器202可被实现为安全电路系统106的“主”、“中央”或“核心”处理器。仅作为示例,处理器202可用有多阶段管道的32位、按顺序精简指令集计算(RISC)核心来实现。借助例如RISC-V功能,处理器可以实现M(机器)和U(用户)模式。激活重置引脚(未示出)(例如,通过低电平有效重置引脚的无效)使处理器202退出重置并开始在其重置向量处执行代码。重置向量可以在ROM 206中开始,其在跳转到仿真嵌入式闪存(e-flash)之前验证其中的代码。换句话说,预期代码在重置释放之前已经被实例化到e-flash中。在一些情况下,根据兼容性规范,贯穿安全电路系统106的重置可以被设为异步活跃低,以支持各种电路部件之间的互操作性。警报处置器204可以作为安全对策和通过看门狗定时器等等生成重置。重置信号也可以被发送到其他电路部件,诸如存储器之一或其他外围设备250之一。

[0058] 耦合到处理器202的是调试模块226(DM 226)和中断控制器228(ItC 228),也可以使得调试模块226(DM 226)和中断控制器228(ItC 228)中的任一个是可兼容的。调试模块226提供对处理器202的调试访问。通过与IC的某些引脚对接,调试模块226中的逻辑允许处理器202进入调试模式并提供将代码注入设备(例如,通过模拟指令)或注入存储器的能力。中断控制器228可以靠近处理器202布置。中断控制器228可以从安全电路系统106内接受中断源的向量。中断控制器228还可以向中断分配等级和优先级,然后将它们转发到处理器202处理。

[0059] 处理器202可以提供任何期望的性能等级或包括任何内部电路部件。例如,处理器202可以包括至少一个算术逻辑单元(ALU)(例如,包括用于计算分支目标的“附加”ALU以去除在所采取的条件分支上的延迟周期)和多个流水线级。通过多个流水线级,流水线可以执

行寄存器写回以减少来自负载和存储的延迟周期,并防止在请求之后的周期对负载或存储的响应可用的情况下的流水线停顿。处理器202可以实现单周期乘法器或对于对存储的错误响应产生不精确的异常,这允许处理器在不等待响应的情况下继续超过存储执行。尽管未描绘,但具体处理器202或通常安全电路系统106可包括指令高速缓存以提供指令的单周期访问时间。

[0060] 在所示示例中,安全电路系统106包括用于指令和数据的三个存储器地址空间。ROM 206是重置释放后处理器202的目标。ROM 206包含硬编码指令以在检查下一级代码之前执行平台检查的子集。下一级代码——例如,存储在电子闪存中的引导加载程序——可以是未硬编码到设备的硅中的第一段代码。因此,下一级代码被签名检查用于完整性以提高安全性。ROM 206可以通过对引导加载程序的全部内容实施RSA检查算法来执行该签名检查。

[0061] 闪存210可以被实现为用于代码存储的电子闪存。这个电子闪存可以容纳上面提到的引导加载程序,以及位于顶层的操作系统和应用程序。SPI设备230可用于批量加载电子闪存。调试模块226还可用于代码加载。SRAM 208可以作为可用于通过处理器202的数据存储(例如,用于堆栈和堆信息)的便签式SRAM操作。SRAM 208还可以存储代码。

[0062] 安全电路系统106可以包括一套“外设”或“外围设备”。这些外围设备250可以是经由互连110耦合到处理器202的从属执行单元。这些外围设备250中的每一个可以遵循确保彼此之间以及与处理器202的兼容性的接口框架。兼容性方案可以指定处理器202如何与给定的外围设备通信(例如,使用互连110)、外围设备如何与芯片I/O通信(例如,通过固定或可复用的I/O)、外围设备如何与处理器202通信(例如,使用中断)、外围设备如何将安全事件(例如,使用警报指示)传达给其他电路部件(例如警报处置器204);外围设备如何与其他外围设备通信——例如,经由至少一个寄存器、同步或异步;或其组合。所描绘的外围设备250可以包括相对于警报处置器204提供的警报相关功能的、相对于处理器202的、相对于一个或多个存储器的和相对于芯片I/O的等等的外围设备。因此,存储器还可以包括相对于彼此或其他描绘的电路部件的外围设备250。

[0063] 电路或芯片I/O外设包括引脚多路复用器222和焊盘控制器224。引脚多路复用器222提供外围设备250的至少一部分与安全电路系统106的可用的可复用I/O节点之间的信令路由(例如,集成了各种部件的芯片引脚或对于SoC其他部分的接口)。焊盘控制器224管理每个电路(例如,芯片的)外部I/O的控制或焊盘属性,如驱动强度、技术以及上拉相对于下拉等。引脚多路复用器222和焊盘控制器224本身是互连110上的外围设备。因此,每个可以具有或可以否则与提供软件可配置性的至少一组寄存器相关联。

[0064] UART单元218可以实现UART特征,诸如单通道双工UART功能。其输出和输入可被配置为经由引脚多路多路复用器222连接到任何电路I/O。GPIO接口220经由引脚多路多路复用器222创建G位与外部电路系统的双向通信,其中,G是正整数,如16、32或64。关于存储器I/O,SPI设备230可以实现固件模式。这里,固件模式可以使能以下特征,其提供了使得外部驱动器将固件升级代码发送到闪存210的组中以用于现场固件更新的能力。固件模式可以包括使用SPI事务对存储器进行寻址。尽管未描绘,但安全电路系统106可包括集成电路间(I2C)主机以使能I2C设备的命令。I2C设备的此命令可能包括标准、完整和快速模式。

[0065] 还描述了若干“核心安全”外设,包括加密引擎和警报处置器204。AES引擎212可以

使用一种或多种协议和不同的密钥大小——如128b、192b或256b——提供对称加密和解密。该部件可以选择例如使用不同的块密码操作模式加密或解密的16字节数量对到达的数据进行加密或解密。AES引擎212可以支持电子码本(ECB)模式、密码块链接(CBC)模式、密码反馈(CFB)模式、输出反馈(OFB)模式和计数器(CTR)模式等。数据传送可以使处理器可用,例如,密钥和数据材料可以经由寄存器写入传递到密码引擎中。或者,可以包括用于传送密钥和数据材料的专用信道,以减少潜在不受信任的处理器活动的暴露。

[0066] HMAC引擎214可以利用例如安全散列算法(SHA)SHA-256作为散列算法。SHA-256是SHA-2系列散列算法的成员,其中,摘要(或散列输出)的长度为256b,无论要散列的输入的数据大小如何。数据在声明散列请求开始后被发送到HMAC外围设备。这将内部状态归零到初始条件,例如一次32b。一旦部件客户端已经发送了数据,客户端可以指示散列请求的完成(带有可选的部分字最终写入)。根据示例便携性接口方案,HMAC引擎214产生散列结果并使其可用于由请求客户端读取的寄存器。可以使数据传送是处理器可用的,也可以是私有的以减少对潜在不可信处理器活动的暴露。

[0067] HMAC是分层在散列函数(例如,SHA-256)之上的消息认证协议,并且HMAC混合在用于加密目的的秘密密钥中。HMAC是一种特殊的应用程序,它以规定的方式(例如两次)围绕消息的散列(通过SHA-256)附加密钥。为了提供此功能,可以在消息散列开始之前将256b密钥编程到电路部件中。身份验证完成的时间可能会有所不同,并且在延迟上可能比使用本机SHA-256更长。再次,为了方便或处理效率,可以使得散列信息或秘密密钥是处理器可用的,或者可以以某种方式将散列信息或秘密密钥变得专用以提高安全性。

[0068] 警报处置器204负责处理和响应于警报,包括从其他外围设备250提供的警报。警报可以被认为是安全敏感中断,它们将被及时处置以响应于感知的安全威胁。与“标准”中断不同,警报不仅仅由在处理器202上执行的软件处置。警报可以触发第一阶段请求,以由软件作为“常规”中断处置。然而,如果软件不能响应并正确地补救警报触发的中断,则警报处置器204触发第二阶段响应。第二阶段响应可以包括制定安全对策,包括终止进程、擦除或否则删除数据、从电路部分撤出电源或重置IC芯片或其部分。这确保即使处理器202忙碌、受阻或也受到攻击,潜在问题——感知的安全威胁——得到解决。

[0069] 因此,(例如,图1的)警报112可以被实现为警报处置器204从其他外围设备接收并且指示潜在安全威胁的提升的中断类型信号或警报指示。在操作中,警报处置器204可以从安全电路系统106的其他电路部件108收集警报并将它们转换成处理器202可以寻址的中断。然而,如果处理器202没有清除中断,则警报处置器204提供硬件响应以解决潜在的安全威胁。

[0070] 对于一些设备间通信,警报处置器204从外围设备源接收以不同方式发送通知的同步或异步警报指示。外围设备250可以基于外围设备250的功能、知识或感测到的参数生成警报。对于其他设备间通信,警报处置器204执行警报源的ping测试作为稳健的心跳机制。警报处置器204的ping监测器(未明确示出)请求来自每个警报源的周期性警报响应以确保与警报源的通信信道正常运行。

[0071] 警报处置器204还可以基于通信故障产生本地来源的硬件警报。如果具有警报源或升级处置器的差分信令或其他规定的通信协议故障(例如,如果信号完整性检查故障),则生成第一个本地来源的警报。如果警报源或升级处置器未能响应ping请求,则警报处置

器204生成第二这样的警报。通常,警报处置器204可以接收来自整个系统的传入警报,对警报进行分类,基于分类的警报发出中断,并且如果处理器202没有清除所发出的中断,则将中断升级为基于硬件的响应。因此,如果处理器不能或未处置安全警报,则警报处置器204可以起作用——例如,作为安全响应的替身。

[0072] 在一些架构中,至少相对于“标准”中断而言,安全警报旨在是罕见事件。因此,在设计阶段,如果该事件预计不会频繁发生并且该事件具有潜在的安全后果,则可以将可能的事件指定为警报事件。此类事件的示例是奇偶校验错误(其可能指示攻击)、对加密或安全相关部件的未授权动作和来自物理传感器的指示环境修改的感测值(例如,电压或温度)等。系统通过警报处置器204路由警报,警报处置器204将警报转换为处理器202潜在寻址的中断。对于某些实现方式,潜在的期望是安全操作系统具有用于在软件中处置由于警报引起的任何此类中断的协议。如果这样,则安全操作系统通常可以解决中断,然后使用警报处置器204清除中断。

[0073] 每个外围设备250可以呈现代表要处置的各个潜在威胁的单独警报的列表。外围设备可以使用特定编码机制将警报作为警报指示传输到警报处置器204。在下面参考图6和7描述用于处置警报的兼容通信信令方案。图6的信令方案涉及警报处置器204和可以生成警报的另一外围设备250之间的通信。图7的信令方案涉及警报处置器204和事件处置器(图2中未示出)之间的通信,该事件处置器可以在触发的警报的适当升级之后响应于来自警报处置器204的升级命令来实施安全对策。

[0074] 安全电路系统106还可以包括RNG 232。通常,随机性可以通过提供可以阻止攻击者预测发起攻击的好时机的执行变化来对安全功能做出贡献。例如,随机数可以提供用于身份和加密目的的秘密材料。RNG 232可以被植入算法计算中以模糊敏感数据值。通常,RNG 232提供更好的性能,因为它的数字生成越来越变得真正随机,并且在此程度上它也可以抵御攻击。RNG 232可以被实现为“真正的”RNG(TRNG),其可以涉及具有模拟部分的设计以利用一些非确定性的物理事件或进程。示例TRNG设计依赖于亚稳态、电子噪声、时序变化、热噪声和量子变化等。TRNG过滤一个或多个结果变量并将它们发送到设备可以在给时序间为当前随机函数采样的熵池中。在某些情况下,熵池的接口可以包括对可用随机位的读取请求。TRNG接口指示有多少位可用,请求的外围设备或软件可以从该池中读取范围位。尝试读取不可用的熵位可能触发中断或警报。

[0075] 两个其他外围设备250包括定时器234和闪存控制器216,后者在以下段落中描述。定时器234可以例如支持处理器202的准确性能。定时器234由多个位(例如,64位)形成并且作为自由运行的定时器操作,其具有在某个百分比内的保证频率。另一定时器(未明确示出)可以充当看门狗定时器以在处理器变得无响应的情况下支持处理器202。无响应可能是由于楔入的开发代码和安全攻击等造成的。

[0076] 闪存控制器216控制闪存210,其可用于代码和数据存储。此数据的主要读取路径可以在标准存储器地址空间中。但是,可以忽略对该地址空间的写入,因为闪存不是以标准方式写入的。相反,为了写入闪存210,软件与闪存控制器216交互。闪存功能可以包括三个主要命令:读取、擦除和编程。读取命令可以被标准化,且可以使用芯片存储器地址空间。擦除命令在页面级别执行,其中,页面大小可由闪存控制器216参数化。在接收到擦除请求后,闪存控制器216擦去目标页面的内容,这将数据呈现为“1”状态(例如,每个字0xFFFFFFFF)。

之后,软件可以将单个单词编程为任何值。闪存位在没有另一次擦除的情况下不返回“1”状态,因此可以通过当前内容和写入值的AND有效地改变未来的内容。擦除和编程命令相对慢。典型的擦除时间以毫秒测量,编程时间在微秒范围内。安全性也是令人担忧,因为秘密数据可以存储在闪存210中。因此闪存控制器216可以提供一些存储器保护。

[0077] 图2中描绘了安全电路系统106,其具有一组特定的电路元件。然而,给定的安全电路系统106可以具有更多、更少或不同的电路部件。电路部件也可以不同地互连或以除上述那些示例方式之外的方式操作。此外,可以省略一些电路部件,而在多个实例中实现其他电路部件。例如,警报处置器204可以是重复的或分布式的,或者多个AES加密引擎212可以存在于一些安全电路系统106中。此外,可以从用于IC芯片的安全电路系统106的外围设备250中省略GPIO接口220,其中,安全电路系统106仅形成几十个核心中的一个。

[0078] 外围设备与安全电路系统的兼容性的示例方案、技术和硬件

[0079] (例如,图1和2的)安全电路系统106可以包括兼容电路部件,其包括外围设备250。该文件描述了使外围设备兼容的示例方法。每个外围设备250可以遵守安全电路系统106的兼容性规范。通过遵守定义至少一个接口方案或通信协议的兼容性规范,外围设备250被实现为具有至少一个接口,该接口在外围设备250和其他外围设备之间产生一致和预期的交互。这提高了通信的可预测性和确定性,并减少了设计和测试安全电路系统所涉及的时间。

[0080] 图3在300处图示了示例外围设备250,其包括至少一个接口302以支持与其他电路部件的兼容性。更一般地,图3包括互连110、耦合到互连110的处理器202以及耦合到互连110的多个外围设备。因此,多个外围设备可以至少经由互连110耦合到处理器202。然而,每个外围设备250也可以在不使用互连110的情况下直接或以其他方式耦合到处理器202。图3明确地描绘了P个外围设备250-1、250-2、……、250-P,其中,P代表正整数。

[0081] 在示例实现方式中,每个外围设备250包括至少一个接口302,其使外围设备250能够遵守为互操作外围设备提供确定性的通信框架。例如,接口302或通信接口302可以使外围设备250能够实现至少一种通信协议320。接口302包括至少一个互连接口304、至少一个设备间接口306和至少另一接口308。在下面描述这些接口。如图所示,外围设备250还包括至少一个寄存器接口310和至少一个安全功能模块312。通常,接口302使外围设备250能够遵守公共框架以与处理器202和多个外围设备250-1…250-P的其他外围设备交互。

[0082] 寄存器接口310包括一个或多个寄存器或寄存器入口。例如,每个寄存器入口可以用于到和来自外围设备250的通信(例如,进出外围设备250的通信)。例如,处理器202或另一外围设备可以设置或清除寄存器入口,或者可以加载具有与外围设备250通信的值的寄存器入口。相反,外围设备250可以改变寄存器入口的值以与处理器202或另一外围设备通信。为了使能这种通信,外围设备250可以将寄存器接口310的至少一部分暴露给处理器202或另一外围设备。例如,外围设备250可以提供处理器访问以清除中断状态指示,如下面参考图5-2到5-4所描述的。

[0083] 通常,寄存器块可用于与外围逻辑的其余部分通信以管理例如与软件的配置和状态通信。在一些情况下,可以使用控制和状态寄存器(CSR)来实现寄存器接口310。CSR提供外围设备250内的寄存器集合,其中的寄存器至少可由本地主机处理器202经由电路范围或芯片范围的地址映射来寻址。CSR可以被标准化以增强软件的一致性并促进电路重用和文档一致性。在下面参考图5-1和5-2描述寄存器接口310的示例方面。

[0084] 安全功能模块312实现外围设备250的安全相关功能。安全相关功能包括核心或主要安全功能和支持或次要安全功能。核心安全功能包括例如警报处理、密码操作(包括加密和解密)、随机数生成和安全数据存储(包括存储和访问秘密数据(例如,密钥管理))等。支持安全功能包括使能或促进核心功能执行的功能。支持安全功能的示例包括存储器存储、存储器控制、时序、电路和芯片I/O控制、环境传感器个总线托管等。

[0085] 通常,接口302或任何特定示例接口(例如,互连接口304、设备间接口306或另一接口308)可以为寄存器接口310建立至少一个寄存器以使能相应的接口通信能力或特征。关于互连接口304,互连接口304实现通信接口,该通信接口耦合到互连110以使能例如外围设备250和处理器202之间遵守公共框架的连接。由于外围设备250和处理器202与同一公共框架兼容,两个方向上的设备-处理器通信可以是标准化的和可预测的。互连接口304可以跨互连110操作,可以使用寄存器接口310的至少一个寄存器,可以使用单独的总线或独立的导线以及它们的某种组合等等。在操作中,外围设备250可以使用互连接口304来参与至少一个互连通信314。附加地或替代地,外围设备250可以使用互连接口304经由互连110与另一外围设备通信。

[0086] 设备间接口306实现外围设备250和遵守公共框架的一个或多个其他外围设备之间的通信接口。由于外围设备250和每个其他外围设备与同一公共框架兼容,两个方向上的设备-设备通信可以是标准化的和可预测的。设备间接口306可以使用寄存器接口310的至少一个寄存器,可以使用专用于外围设备的总线,可以使用在两个外围设备之间延伸的一条或多条独立导线以及它们的某种组合等等。

[0087] 在操作中,外围设备250可以使用设备间接口306来参与至少一个设备间通信316。在某些实现方式中,通过绕过互连110与另一外围设备通信,外围设备250可以与另一外围设备“直接”通信。此外,通过建立和遵守设备间通信方案,促进了两个或更多个设备之间通信的一致性和确定性。因此,设计者可以专注于实现安全功能模块312的预期安全相关功能,而不是花费时间和资源来跟踪和复查多个临时通信机制。

[0088] 另一接口308实现外围设备250和遵守公共框架的另一电路部件之间的通信接口。由于外围设备250和其他电路部件与同一公共框架兼容,两个方向的外围设备信令可以是标准化的和可预测的。另一接口308的示例是用于与外部通信信息的芯片I/O接口。如果中断没有通过互连110完全通信,另一接口308的另一示例是中断接口。另一接口308的另一示例是时钟接口。在一些情况下,安全电路系统106(未在图3中单独指示)包括主要系统时钟和一个或多个次要系统时钟。时钟接口可以利用主要系统时钟和次要系统时钟的至少所选部分来用于通信时序和通用功能。时钟接口可以根据安全电路系统106的时钟方案进行操作,并且外围设备250的设计代码可以指定与外围设备250相关的时钟。在操作中,外围设备250可以使用其他接口308与另一电路部件(如I/O电路系统或时钟树)进行至少一个其他通信318。

[0089] 图4图示了用于分析外围设备设计以确保满足可兼容的目标的示例方法400。在示例实现方式中,方法400使用接口规范402,其可以包括互连方案404、设备间方案406或另一方案408(包括每个方案)。接口规范402对应于(图3的)接口302。互连方案404对应于互连接口304,设备间方案406对应于设备间接口306,而另一方案408对应于另一接口308。这些方案可以附加地或替代地包括本地或芯片级I/O方案、中断方案和时钟方案等。

[0090] 因此,接口规范402可以为接口302建立规则、协议、属性、选项、能力等。类似地,互连方案404、设备间方案406和其他方案408中的每一个可以分别为互连接口304、设备间接口306和其他接口308建立规则、协议、属性、选项、能力等。在设计时间期间,设计者开发每个外围设备250以遵守接口规范402的每个相关方案。例如,设备间方案406可以建立用于定义绕过安全电路系统106的互连110的设备间信令的格式。通过这样做,可以产生可兼容外围设备250,这增强了互操作性并减少了设计和开发时间以及测试和调试工作。例如,外围设备250可以使用从外围设备的设计代码指定的属性导出的电路系统将信号(例如,设备间信号)传送到另一外围设备。

[0091] 在示例方法中,兼容性分析模块410可以执行设计代码的分析414以检查兼容性。设计者参考接口规范402产生外围设备设计代码412。因此,外围设备设计代码412通过遵守接口规范402来满足兼容性目标。可以至少部分地使用例如配置文件实现外围设备设计代码412。外围设备设计代码412可以包括处理器-设备信令418的一个或多个指示(例如,定义外围设备250和处理器202之间的互连通信314的方面)和设备间信令420的一个或多个指示(例如,定义外围设备250和另一外围设备之间的设备间通信316的方面)等等。设备间信令420的一个或多个指示可以例如涉及在两个或更多个外围设备之间交换的信号,包括不使用安全电路系统106的互连110。这些指示可以遵循寄存器的规则和指南、这些信号的信号命名、数据类型和时序等。

[0092] 外围设备设计代码412中的描述导致安全电路系统106中的电路部件。例如,关于(例如图3的)相应外围设备250的设备间接口306,基于包括在用于其的设计代码412中的属性,设备间接口306可以耦合到延伸到另一外围设备的至少一条导线以使能设备间信令。通过在设计代码412中指定设备间信令420,增加了互操作性和通信确定性。接口规范402或设计代码412的配置文件可以指示在给定的兼容性框架中的强制性的外围特征和可选的外围特征。因此,在某些情况下,兼容设计代码可能包括强制性部分和可选部分。通常,设计代码412可以根据任何IC设计或配置平台进行格式化。示例包括Verilog、Python和Hjson等。下面阐述了示例配置文件格式。

[0093] 在操作中,兼容性分析模块410接受外围设备设计代码412。参考接口规范402,兼容性分析模块410执行分析414以检查外围设备设计代码412是否符合指定的公共框架。兼容性分析模块410可以将外围设备设计代码412与互连方案404、设备间方案406或另一方案408中的一个或多个进行比较以检查代码是否满足每个方案的规范。这些方案中的任何一个可以包括与中断和寄存器使用等相关的规范。基于分析414,兼容性分析模块410产生兼容性报告416。

[0094] 兼容性报告416通过满足接口规范402的标准来指示外围设备设计代码412是否通过分析414。如果不是,则兼容性分析模块410可以在兼容性报告416中包括“违规”列表。每个违规可以包括对导致故障指示的代码部分的引用或对接口规范402中被违反的部分的引用。虽然可以关于示例安全电路系统环境来描述接口规范402、兼容性分析模块410和外围设备设计代码412,但是可以在其他环境中实现接口规范402、兼容性分析模块410或外围设备设计代码412。因此,兼容性报告416可以涵盖一般电路设计的分析。

[0095] 图5-1在500-1处图示了包括寄存器接口310和示例通信信号的示例外围设备250。在图5-1中,一般但仅作为示例,用实线描绘了强制性的通信信道或信号,用虚线描绘了可

选的通信信道或信号。然而,在其他情况下,不同的信道或信号可能是强制性的或可选的。此外,在给定的接口规范下,其他图中的实线或虚线不一定分别指示要求或缺乏要求。

[0096] 在示例实现方式中,可以将各种信号指定为外围设备250要遵守的兼容性框架的一部分。从左上角开始,描绘了使用互连110的双向信令502-1,其中,外围设备250相对于互连110用作设备(例如,用作跟随器)。在其下方,示出了外围设备250,其接收至少一个时钟信号504和至少一个开发模式信号505。开发模式信号505代表对外围设备250的安全电路系统106或整个SOC当前正在以什么模式操作的指示。换言之,可以有多种操作模式。通过两个示例模式,多种模式可以包括开发模式和生产模式。例如,模式指示可以确定如何处置软件错误。其他模式可以使能将完整生命周期模式状态传达给外围设备的安全特征。

[0097] 外围设备250还可以生成或输出至少一个中断信号506或至少一个警报信号508。此外,使用相对于互连110用作主机(例如,作为,引导器)的外围设备250描绘使用互连110的双向信令502-2。外围设备250可以进一步参与与GPIO接口220或其他芯片I/O电路系统的双向发信号通知507。关于寄存器接口310,至少一个输出信号509-1被标记为寄存器到硬件(Reg2Hw)信号。另一方面,至少一个输入信号509-2被标记为硬件到寄存器(Hw2Reg)信号。下面进一步描述图5-1中描绘的这些信号。下面参考图5-3在中断上下文中描述传入和传出寄存器信号的示例。然而,在描述中断寄存器信号之前,先参考图5-2描述示例中断寄存器入口。

[0098] 通常,在一些实现方式中,某些特征被认为是强制性的,而其他特征被认为是可选的。然而,这些强制性和可选类别可能在不同的实现方式之间不同。通过可兼容的设计,可以按特征分配这两个类别,以便每个外围设备250与其他外设适当地互操作。接下来阐述强制性和可选类别之间的示例分配。首先,时钟规范是强制性的。每个外围设备指定其主要功能时钟和任何其他要使用的时钟。主要时钟是驱动外围设备通过其进行通信的互连的主要时钟。时钟部分还列出了可用的时钟。如果希望使用其他时钟,则可以指定它们。其次,总线设备(或跟随器)接口是强制性的。每个外围设备250可以包括一个或多个寄存器;因此,每个这样的外围设备250被配置为在芯片总线或其他互连110上的设备。第三,一个或多个寄存器是强制性的。因此,每个外围设备250以指定的寄存器格式定义寄存器集合。基于外围设备250的设计代码,可以通过实例化相关硬件来自动生成寄存器。同样可以创建相应的软件或说明文档。

[0099] 第四,总线主机(或引导器)接口是可选的。如果包括,则外围设备250在某些情况下可以充当总线主机,即使通过使处理器成为主要主机可以增加整体芯片的简单性。通过示例的方式,直接存储器存取单元(DMA单元)类型的外围设备250可以实例化总线主机接口。第五,可用I/O的规范是可选的。如果外围设备250要连接到专用或复用的I/O引脚,外围设备250可以指示可用于芯片I/O的其外围输入和输出。第六,中断是可选的。外围设备可以生成用于中断主处理器的信号。使用对应信号的列表指定这些中断。每个指定的中断导致发送到处理器202以作为其中断向量输入的一部分被收集的单线或捆绑输出。第七,警报也是可选的。外围设备可以生成指示潜在安全威胁的信号。还使用信号列表指定这些警报。每个指定的警报导致发送到警报处置器204的互补信号对。第八,设备间信号是可选的。外围设备可以指定与其他外围设备连接的单独信号,这里称为设备间信号。在其他实现方式中,可以以各种方式将不同的特征指定为强制性的或可选的。在其他实现方式中,特征可能不

被指定为强制性对可选性,或者可以使用不同的类别来指定它们。

[0100] 图5-2在500-2处图示了具有多个中断入口的示例寄存器接口310。通常,寄存器接口310包括多个寄存器入口。如针对中断相关方面所示,寄存器接口310包括多个中断入口510-1、510-2、…、510-I,其中,I代表正整数。多个中断入口510-1…510-I的数量I可以针对每个外围设备250并且从设计到设计而变化。

[0101] 在示例实现方式中,每个中断入口510包括三个指示或寄存器:中断使能指示512、中断状态指示514和中断测试寄存器516。每个指示具有至少一位。通过示例的方式,如果每个指示是一位并且寄存器接口310包括16个中断入口510-1…510-I(例如,I=16),则寄存器接口310包括48位(3×16=48)来处理该外围设备250的中断。寄存器接口310可以包括其他入口。

[0102] 在操作中,中断使能指示512确定对应的中断是否被激活以供使用。在某些情况下,处理器202可以设置使能指示;在其他情况下,外围设备250或两者可以设置使能指示。如果中断被触发,则中断状态指示514是有效的,如果中断被清除则中断状态指示514是非有效的。处理器202可以使用中断测试寄存器516来测试中断;例如,处理器202可以触发寄存器以触发用于测试目的的中断。参考图5-2的中断硬件和图5-3的中断信令进一步描述这些指示。

[0103] 图5-3在500-3处图示了示例中断入口510(或中断寄存器510)。中断入口510包括中断使能指示512、中断状态指示514和中断测试寄存器516。例如,中断入口510左侧(如所描绘的)上的信令代表可以通过互连110传送的信号。指示或寄存器512、514和516中的每一个从例如处理器202接收两个信号wd和we。we信号代表写使能,而wd信号代表写数据。处理器202可以读取由qs信号代表的中断状态指示514的当前状态或条件。(例如,图5-1的)外围设备250可以将中断状态指示514的d输入与“1”(例如,高)或有效电压电平联系起来。

[0104] 对于测试模式,处理器202将wd和we信号驱动为有效的进入中断测试寄存器516以触发中断测试。中断测试寄存器516输出这两个有效信号作为q和qe信号,它们被耦合到AND门534的两个输入。当两个信号都有效时,AND门534向OR门536的较低输入提供有效值。基于至少一个信号是有效的,OR门536将中断状态指示514的de输入驱动为有效的。这将中断状态指示514的当前状态呈现为设置的。处理器202经由qs信号访问该状态。

[0105] 对于常规或操作模式,外围设备250检测对应于中断的事件并将OR门536的上部输入处的中断事件信号(Interrupt_Event)驱动为高。基于至少一个信号是有效的,OR门536将中断状态指示514的de输入驱动为有效的。这将中断状态指示514的当前状态呈现为被设置的。该设置状态渗透通过中断状态指示514的电路系统(未明确示出)并作为中断状态指示514的有效的q信号输出。该有效状态信号被耦合到AND门532的上部输入。

[0106] 同时,处理器202也可以将wd和we信号驱动为有效的进入中断使能指示512。如果是,则中断使能指示512将其输出q信号驱动为有效的。该有效信号被传播到AND门532的上部输入。在AND门532的两个输入都有效的情况下,AND门532将中断入口510的输出驱动为有效的。因此,外围设备250响应于中断事件的检测而将中断信号506(Interrupt_Signal)驱动为有效的。该有效的中断信号506被路由或耦合到处理器202的中断处置硬件。

[0107] 尽管上面针对示例中断入口510描述了特定的门和某些信令关系,但是可以以替代方式实现中断入口510(或寄存器接口310的另一个寄存器入口)。例如,外围设备250可以

控制寄存器使能。此外,wd信号可能有多个位。此外,可以经由互连110或通过另一(例如,直接的、排他的或仅外围设备的)信令通路与另一外围设备250进行到和来自外围设备250的信令。

[0108] 图5-4图示了用于处置外围设备250和处理器202之间的中断的示例时序图500-4。时序图500-4包括跨14个周期或半个时钟周期从时隙0到13扩展的时钟信号(Clock)。同样参考图5-3,中断使能信号(Interrupt_Enable(we信号进入中断使能指示512))在整个时隙0到13期间处于高电平有效。在时隙2或3附近,外围设备250检测触发中断的事件。外围设备250在时隙3将中断事件信号(Interrupt_Event)驱动为有效的。

[0109] 在例如一个时隙内,中断状态指示514的中断状态(Interrupt_State)变为有效的。如图所示,该信号在时隙4期间变高,并且该值可以由处理器202读取(作为qs信号)。假设中断使能指示512也有效,(图5-3的)AND门532在同一时隙4期间将中断信号506(Interrupt_Signal)驱动为高电平有效。响应于有效的中断信号,在处理器202上操作的软件在一定数量的时隙上处理中断。在中断被处置之后,软件可以清除在中断状态指示514中的中断状态。时序图500-4描绘了在时隙8期间用信号(SW写到清除)清除中断的软件。因此,中断状态、中断信号和中断清除信号在第9时隙变为低电平有效。

[0110] 接下来描述不同外围设备特征的各种示例实现方式。首先,在相对较高的级别上简要描述多个特征。这些特征包括计时、重置、总线设备对接、总线主机对接、I/O通路、I/O复用、中断、警报和设备间信令。其次,在呈现了示例配置文件和对应的文档之后,在相对较低的级别且更详细地描述了几个特征。这些特征包括配置描述(或外围设备编码)、中断处置、警报处置和设备间信号处置。各种示例如果被实施则可以单独地、联合地和全部地或部分地等地实施。可以以各种方式进一步修改各种示例。

[0111] 关于计时,每个外围设备定义至少一个时钟:主要时钟。这在配置文件中定义为“clock_primary”,并被设置为已知时钟名称之一。该主要时钟被定义为用于为总线设备计时的主要时钟,以向顶级指示是否要使用总线接口的异步处置。外围设备还可以请求其他时钟供内部使用。这些在外围设备中创建由公共框架处置的异步时钟域。在配置文件中的“other_clock_list”下定义其他时钟。

[0112] 关于重置,外围设备译码可以指定重置方案。或者,可以不提供附加信息来指示用于给定外围设备的重置方案。替代地,可以制定默认条件,由此每个时钟都带有其针对该时钟域的相关重置引脚。在某些情况下,设计中的重置被配置为异步低电平有效。如果这样,对安全敏感的存储元件应用特别注意。对于异步低电平有效重置,重置的断言与任何时钟都是异步的。然而,取消断言与相关存储元件的时钟同步。安全存储元件可能“泄漏”敏感的状态内容,因此无论重置方法如何,都应谨慎处置存储元件。在这种情况下,“谨慎处置”可能涉及同步地——在芯片范围重置后的某个时间——将它们的值重置为被随机化的值,以使得寄存器值和全零之间的汉明距离不能产生对攻击者有价值的信息。异步低电平有效可能需要稍微更多的面积和更多的实施计划,但与同步高电平有效相比,它更常见,因此为许多设计人员所更熟知。另一方面,同步高电平有效略高效率,但它涉及使用时钟边沿来生效。

[0113] 关于总线设备接口(例如,作为总线跟随器),每个外围设备使用“bus_device”关键字指定总线操作的类型。例如,外围设备代码可以指定TileLink-Uncached-Lite(TL-UL)

作为其对于互连110或对于芯片范围框架的接口。在某些情况下,外围设备的地址映射不是由外围设备本身或其配置文件确定的。替代地,更高级别的全芯片配置文件可以将地址范围分配给包含的总线外围设备中的每个。

[0114] 关于总线主机接口(例如,作为总线引导器),每个外围设备具有至少临时或按需声明自己为总线主机的选项。此能力被包含在带有“bus_host”关键字的配置文件中。如果外围设备不具有此特征,则配置文件可以如此指示(例如,经由空字符串)。如果外围设备具有此特征,则在关键字中包含总线主机协议名称。为了提高兼容性,每个总线主机可以使用与定义的主要主机时钟相同的时钟。在某些情况下,为每个总线主机提供主机标识符或标识(ID)(例如,四位)以区分系统内的主机。这是由框架强制执行的,以确保每个主机的唯一性。

[0115] 关于I/O可用性,每个外围设备可以指定可用于芯片I/O的信号(例如,输入、输出或输入输出)。框架为每个信号确定信号是直接路由到专用芯片引脚还是在到达芯片引脚之前与来自其他外设的信号复用。可以用“available_input_list”、“available_output_list”和“available_inout_list”的配置文件入口来指定每个外围设备的可用I/O。但是,这些入口中的任何一个都可以被跳过或可以包含一个空列表“[]”。如果不为空,则这些文件入口中的任何一个都可以包含以逗号分隔的信号名称列表。在某些情况下,“name”形式的输入列表上的项目引发“cio_name_i”形式的外围输入。“name”形式的输出列表上的项目引发“cio_name_o”形式的外围输出以及输出使能“cio_name_en_o”。“name”形式的inout列表中的项目引发所有三个。

[0116] 关于复用芯片I/O和焊盘控制,在顶级芯片框架中,可以实例化引脚多路复用单元(pinmux)。引脚多路复用单元提供到/来自外围I/O和芯片引脚I/O的灵活的分配。可兼容外围设备不需要指定它们的可用I/O是硬连线到芯片I/O还是可用于复用。替代地,此规范是在更高级用配置文件(例如,Hjson配置文件)完成的。此外,外围逻辑不执行全焊盘控制,因为焊盘控制器设备执行此功能。焊盘控制器设备可以提供对焊盘驱动强度、引脚映射和焊盘类型(例如,推/拉、开漏等)等的软件配置控制。

[0117] 关于中断,每个外围设备可以将一个或多个输出信号指定为目的地为本地主机处理器的中断。这些中断信号是非安全关键信号(例如,与警报相关),并被发送到处理器以使用其中断服务例程进行处置。外围设备设计代码在配置文件中使用“interrupt_list”属性列出其中断集合。中断列表中“name”形式的每一项期望名为“intr_name_o”的模块输出。

[0118] 关于警报,每个外围设备可以将一个或多个输出信号指定为去往硬件警报处置器设备的安全关键警报。这些警报信号被实现为差分信号,以避免创建单点故障。外围设备将警报信号传输给警报处置器,以发送给处理器进行一线防御处置。如果处理器无法解决警报,警报处置器提供硬件安全响应。外围设备设计代码在配置文件中使用“alert_list”属性列出其警报集合。对于安全电路系统中的每个警报,在警报处置器中生成对应的一组信号以执行在给定外围设备的警报发送器和警报处置器设备之间的通信。下面参考图6描述了容纳警报的示例通信信令,下面参考图7描述了处理升级警报的示例通信信令。

[0119] 关于设备间信令,外围设备可以产生、传输、接收或处理在至少两个外围设备之间交换的信号。这些设备间信号可以扩展到中断和警报之外。外围设备设计代码在配置文件中用“inter_signal_list”属性列出了其设备间信号的集合。外围设备可以定义每个指定

的设备间信号的类型。可以在更高级(例如,顶级)配置文件中定义两个或更多个外围设备之间的逻辑或物理连接。

[0120] 外围设备设计代码412的至少一部分可以被实现为配置描述。在一些实现方式中,配置文件是用Hjson准备的或符合Hjson的。配置文件可以描述外围设备250,包括寄存器接口310的寄存器。下面呈现示例配置文件。该示例包括强制性和可选类别,如注释中所示;尽管如此,其他实现方式可能有一个或另一个类别(但不是两者),也可能没有类别。在该示例中,外围设备250的名称是“uart”。然而,其他配置字段是作为解释提供的,不一定与UART外围设备的功能一致。换句话说,在下面的示例配置文件中显示了一些配置字段以用于启迪的目的。

[0121]

```
{
  name: "uart",
  clock_primary: "clk_fixed",                    // optional; default "clk"
  other_clock_list: [ "clk", "clk_lowpower" ],   // optional; default []
  bus_device: "tlul",
  bus_host: "",                                  // optional; default undefined
  available_input_list: [                        // optional; default []
    { name: "rx", desc: "Receive bit" }
  ],
  available_output_list: [                       // optional; default []
    { name: "tx", desc: "Transmit bit" }
  ],
  available_inout_list: [],                      // optional; default []
  interrupt_list: [                              // optional; default []
    { name: "tx_watermark",    desc: "raised if the transmit FIFO..."}
```

```
        { name: "rx_watermark",    desc: "raised if the receive FIFO..."}
        { name: "tx_overflow",     desc: "raised if the transmit FIFO..."}
        { name: "rx_overflow",     desc: "raised if the receive FIFO..."}
        { name: "rx_frame_err",    desc: "raised if a framing error..."}
        { name: "rx_break_err",    desc: "raised if break condition..."}
        { name: "rx_timeout",      desc: "raised if the receiver..."}
        { name: "rx_parity_err", desc: "raised if the receiver..."}
      ],
      alert_list: [                                          // optional; default []
        { name: "uart_breach", desc: "Someone has attacked the ..."}
        { name: "uart_frozen", desc: "The UART lines are frozen..." }
      ],
      inter_signal_list: [
        { name: "msg_fifo",
          struct: "fifo",
          package: "msg_fifo_pkg",
          type: "req_rsp",
          act: "req",
          width: 1
        }
        { name: "suspend",
          struct: "logic",
          package: "",
          type: "uni",
          act: "rcv",
          width: 1
        }
      ]
      regwidth: "32",                                        // standard register width
      register: [
                                                             // Register information.
      ]
    }
```

[0122]

[0123] 上面的示例配置文件对应于下面呈现的示例文档格式输出：

[0124] Primary Clock:clk_fixed

[0125] Other Clocks:clk,clk_lowpower

[0126] Interconnect Device Interface:tlul

[0127] Interconnect Host Interface:none

[0128] Peripheral Pins available for Chip-Level I/O:

[0129]

引脚名称	方向	描述

[0130]

tx	输出	传输位

[0131] rx 输入 接收位

[0132] 中断:

[0133] Intrpt名称 描述

[0134] tx_watermark 如果传输FIFO超过高水位标记,则引发

[0135] rx_watermark 如果接收FIFO超过高水位标记,则引发

[0136] tx_overflow 如果传输FIFO溢出,则引发

[0137] rx_overflow 如果接收FIFO溢出,则引发

[0138] rx_frame_err 如果在接收时检测到帧错误,则引发

[0139] rx_break_err 如果在接收时检测到断开条件,则引发

[0140] rx_timeout 如果接收器没有收到任何字符(可编程时间段),则引发

[0141] rx_parity_err 如果接收器检测到奇偶校验错误,则引发

[0142] 安全警报:

[0143] 警报名称 描述

[0144] uart_breach 有人攻击了UART设备

[0145] uart_frozen UART 线路被冻结,可能受到攻击

[0146] 这里进一步描述了中断处置的示例方法。在一些实现方式中,中断具有通用名称、硬件接口和软件接口。中断是已发生但尚未由本地主机处理器寻址的已定义外围事件的锁存指示。中断作为高电平有效电平中断(与边沿中断相反)被发送到处理器。触发事件可以是边沿或电平以及高电平有效或低电平有效,如由相关的外围设备定义。例如,GPIO设备可以将其输入位之一的上升沿或下降沿解释为中断事件。事件的锁存可由自动生成的寄存器文件执行,如下所述。事件的清除由处理器写入响应于事件处置完成来执行。也在上面参考图5-2和5-3描述了寄存器接口310的示例中断入口510。上面参考图5-4描述了示出事件发生的时序、中断值的对应锁存以及处理器清除中断的示例波形。

[0147] 关于给定外围设备的中断,该外围设备可以为每个事件生成单独的中断,但是将它们作为捆束一起发送到本地处理器的中断模块。可以在处理器在中断处理器中执行“消除歧义”或确定哪个中断唤醒了处置器。在替代模型中,每个外围设备一次只发送一个中断,处理器可以通过查询外设以确定触发了哪个中断来消除歧义。为了定义一个或多个中断,外围设备设计代码可以指定它们。例如,上述配置文件指定了中断的相关属性。电路生成工具可用于基于上述示例中描述的配置文件生成额外的设计方面。

[0148] 关于寄存器创建,对于每个外围设备,自动创建三个寄存器来管理该外设的每个中断(例如,如在Hjson文件的“interrupt_list”部分中所定义的)。但是,可以代替使用不同的寄存器目的或不同数量的寄存器来实现替代的默认寄存器格式。此外,可以覆盖自动生成。每个中断对于三个寄存器中的每一个都有一个字段位。这三个寄存器是INTR_STATE寄存器、INTR_ENABLE寄存器和INTR_TEST寄存器,其分别由中断状态指示514、中断使能指示512和中断测试寄存器516(图5-2和5-3的)表示。中断寄存器可以通过自动生成工具被放置在外围设备地址图的顶部。

[0149] INTR_ENABLE寄存器可由处理器(rw)读取和写入,每个中断一位,其当为真(true)时,使外围设备的中断能够报告给处理器的中断输入。INTR_STATE寄存器可由处理器读取,每个位都可以写入1以将其清除(rw1c)。因此,寄存器的读取指示所有锁存中断的当前状

态,并且向任何字段写入1清除对应中断的状态。INTR_TEST是只写(wo)寄存器,它允许软件通过模拟实际中断事件的触发、INTR_STATE寄存器的设置以及输出到处理器的中断信号电平的升高来测试中断的报告(以INTR_ENABLE的效果为模)。INTR_STATE寄存器的内容不需要受使能值影响。代替地,INTR_STATE寄存器示出锁存硬件中断事件的原始状态。被发送到处理器的输出中断信号在发送到处理器进行促织之前,将中断状态与中断使能寄存器(例如,与与门532)进行AND运算。

[0150] 关于处置中断,被发送到处理器的中断是具有相同严重性的高电平有效电平中断(例如,图5-3的中断信号506可以是高电平有效的,如图5-4所示)。或者,中断可以具有不同的严重性级别。例如,更高优先级的中断可以被实现为不可屏蔽中断(NMI)。参考图5-3,三个指示(例如,中断使能指示512、中断状态指示514和中断测试寄存器516)可以被实现为面向软件的寄存器。在图5-3中,interrupt_event信号被显示为从外围设备250的另一部分到达中断入口510。在寄存器文件内,中断事件触发将INTR_STATE寄存器中的相关位设置为1。另外,向INTR_TEST寄存器中与此中断关联的位写入1可以设置对应的INTR_STATE位。INTR_STATE寄存器的输出在使用INTR_ENABLE的值进行屏蔽(例如,AND运算)后成为向处理器的输出中断。

[0151] 在一些情况下,INTR_STATE寄存器的ro/rw1c功能的处置允许软件控制INTR_STATE内容的清除。向INTR_STATE的对应位写入1清除锁存值。然而,如果由interrupt_event信号表示的触发事件本身仍然有效,则INTR_STATE寄存器返回真。在这个示例中,硬件没有清除锁存中断状态的能力;清除是为软件保留的。但是,可以设计硬件以使能此功能。被发送到处理器的中断由其中断控制器处置。在中断控制器逻辑中,可能有另一级的控制用于启用、优先化和枚举多个中断。

[0152] 这里进一步描述了警报处理的示例手段。在一些实现方式中,警报跨外围设备被标准化以保持一致性。与中断不同,在始发外围设备上没有警报的软件部件,但是可以在硬件警报处置器处有。在始发外围设备处,一个或多个警报可以作为捆束输出从外围设备发送到警报处置器。每个外围设备可以被设计为发送零个或多个警报,每个警报对应可区分的安全威胁。每个警报源于相应外围设备内部的某个事件,并且外围设备可以首先尝试解决检测到的事件。在外围设备将警报传达给警报处置器之后,警报处置器处理警报,该处理可以包括升级到实施安全对策的升级处置器。

[0153] 在外围设备内,检测到的内部事件高电平有效地被发送到被称为警报发送器模块的在外设内的模块。在给定的外围设备中,每个不同的警报事件类型实例化一个警报发送器模块。外围设备的设计者确定什么是不同的警报事件。根据在模块内所需的区别(例如,高优先级威胁与低级威胁),多个警报可以被捆束在一起。警报发送器模块将警报事件转换为差分编码的信号对,其被路由到警报处置器的硬件。下面参考图6描述了该警报信令的示例实现方式。可以自动生成警报处置器以具有足够的警报接收端口,以具有与在各种包括的外围设备的配置文件中声明的每个警报相对应的一个端口。

[0154] 这里进一步描述了设备间信号处置的示例方法。设备间信号可以指连接在顶层设计中的外围设备实例的单独或捆束的信号。一些外围设备可以是独立的外设,如GPIO或UART外设。这些外围设备向主处理器报告中断,但不需要与其他外围设备对话。相比之下,一些外围设备和主处理器可以直接或间接地与其他外围设备通信。例如,闪存控制器向闪

存宏发送对于读取、编程和擦除操作的请求。

[0155] 通过在外围设备配置文件中指定设备间信号的方面,促进了一致性和互操作性。这避免了在两个或更多个外围设备之间在信令间进行手动链接和测试的繁琐过程。通过对每个外围设备250进行适当的定义编码,更高级别的设计工具可以将每个外围设备250适当地连接到预期的其他外围设备。上面提供的示例配置文件指定了设备间信号的两种情况,“msg_fifo”和“挂起”。

[0156] 下面阐述了示例设备间方案406(或设备间信令方案406)。每个方面都根据属性、强制/可选类别和描述进行描述。在替代实现方式中,这些方面可以变化。例如,强制性类别和可选类别可以不同或者可以被省略,或者可以增加另一方面。这些方面可用于在外围设备设计代码412中提供设备间信令420(图4的)的一个或多个指示。

[0157] 首先,“name”是强制性属性。name属性指定设备间信号的端口名称。如果端口类型为“req_rsp”(请求和响应),则该类型表示外设有两个端口:“name_req”端口和“name_rsp”端口。每个名称都可以包含“_i”或“_o”后缀,以分别指定“输入”或“输出”。

[0158] 其次,“struct”属性也具有强制性类别。“struct”字段定义了信号的数据结构。设备间信号通常可以捆束成“struct”打包类型。这个“struct”与“package(包)”属性一起用于定义信号。如果设备间信号是逻辑类型,则“package”字段可以省略。因此,“package”属性是可选的。

[0159] 第三,“type”属性是强制性的。在该示例设备间信令方案中可以有两种类型的设备间信号。“req_rsp”类型是一种连接,其中,一个外围设备发送请求,第二个外围设备返回响应。另一方面,“uni”型连接是单向信号。例如,单向信号可用于广播信号或用于不需要响应的信号。

[0160] 第四,“act”属性也是强制性的。“act”属性与“type”属性配对。“act”属性指定外围设备中信号的输入/输出(I/O)。“req_rsp”类型可以在“act”字段中具有“req(requester)”或“rsp(responder)”。“uni”类型可以在“act”字段中具有“req”或“rcv(receiver)”。

[0161] 第五,“width”是可选属性。如果“width”不为1或未定义,则对应的端口被定义为“struct”的向量。因此,该端口可以连接到多个外围设备。

[0162] 图6图示了警报处置器204的警报接收器模块612和外围设备250的警报发送器模块622之间的示例通信关系600。信令通路632包括至少一个差分路径。如图所示,信令通路632包括多对导线(例如,三对)以使能跨越三个差分路径的差分信号。每对导线包括一根正极线和一根负极线。模块可以通过信令通路632同步或异步通信。警报处置器204还包括ping监测器604以将pinging机制实现为双向心跳方案以确保物理和逻辑通信容量。

[0163] 在示例实现方式中,外围设备250包括至少一个警报发送器模块622。外围设备250检测警报事件602。警报事件602可以对应于传感器输入(例如,传感器感测的参数)、观察到的活动模式和从另一部件接收到的指示等。响应于警报事件信号602,警报发送器模块622在第一对导线(例如,如图所示的上对)上向警报接收器模块612传输警报指示652。响应于接收警报指示652,警报接收器模块612向警报处置器204的控制器(未示出)提供触发警报662。警报接收器模块612还在第二对导线(例如,如图所示的中间一对)上将警报确认信号606传输回警报发送器模块622以确认收到警报指示信号652。

[0164] 对于pinging协议,警报接收器模块612从ping监测器604接收ping指令658。在ping指令658的提示下,警报接收器模块612在第三对导线(例如,如图所示的较低的一对)上向警报发送器模块622传输ping请求654。为了指示到外围设备250的连接是活动的和起作用的,警报发送器模块622——例如,在第一对导线上——将ping响应656传输回警报接收器模块612。为了弹性,警报发送器模块622可以在同一对导线上传输警报指示652和ping响应656。这确保不良行为者没有切断警报指示652的导线,同时保持用于ping响应656的导线完好无损。警报接收器模块612从警报发送器模块622接收ping响应656。为了完成ping协议循环,警报接收器模块612响应于ping响应656的接收,将ping okay消息660转发到ping监测器604。

[0165] 在一些情况下,完整性故障电路系统618的至少一部分被耦合到或合并到警报接收器模块612中。完整性故障电路系统618监视至少一对导线以确定适当的差分信令是否存在于差分路径上和预期的信令模式是否匹配实际的信令模式。如果不是,则完整性故障电路系统618生成警报完整性故障信号668,并将该信号作为警报处置器204的内部警报提供给控制器。

[0166] 在一些实现方式中,在正/负警报指示导线(例如,第一对导线)和正/负警报确认导线(例如,第二对导线)上使用“完全”握手对警报进行差分编码和信号发出。采用完全握手协议允许警报信令机制用于异步时钟策略,其中,一些外围设备可以驻留在与警报处置器204不同的时钟域中。完全握手协议确保警报消息被正确地反压并且由于(可能是可变的)时钟比大于或小于1.0,在异步边界不“丢失”警报。如果警报事件602在外围设备250内仍然为真,则可以在差分警报指示线上重复本地警报指示。因此可以在警报为真时重复握手模式。警报发送器模块622可以等待例如在握手之间的两个周期。

[0167] 在异步环境中,一旦警报指示线上的初始电平变化已经被接收并且与警报接收器模块612处的本地时钟同步,警报指示652可以被“立即”传播到触发警报信号662。这确保了警报指示652的第一次出现被传播,即使握手线已被操纵以模拟背压。在模拟背压的情况下,后续的警报指示可能被背压;然而,ping监测器604的ping测试机制最终检测到不良行为者篡改了导线。

[0168] 在一些实现方式中,为了确保警报发送器模块622未被破坏,警报接收器模块612用ping或心跳消息周期性地(例如,每几微秒)“ping”或线路测试发送器。ping监测器604可以随机化ping时序,因此ping请求654消息的出现不能被预测。ping时序由警报处置器204内的中央基于LFSR的定时器生成(例如,使用ping监测器604的ping定时器),其随机断言特定警报接收器模块612的ping指令信号658。

[0169] 一旦ping指令信号658被断言,警报接收器模块612就将ping请求消息654编码为ping请求差分路径(例如,第三对导线)上的电平变化。警报接收器模块612等待,直到警报发送器模块622在正/负警报指示线(例如,第一对导线)和正/负确认线(例如,第二对导线)上以完全握手响应。一旦握手完成,警报接收器模块612就断言ping okay消息660。基于LFSR的定时器可以具有可编程的ping超时。在没有发生完全握手的可编程ping定时器期满之后,ping监测器604使用警报ping故障信号(未示出)断言“ping故障”内部警报。该超时可以是系统中存在的时钟比率的函数,并且可以在系统启动时相应地编程。

[0170] 在ping请求654与警报发送器模块622处的本地警报指示652冲突的相对不太可能

的情况下,警报指示652被阻挡直到ping握手协议完成。尽管这种方法稍微延迟了警报指示652的传输,但是警报指示652最终被用信号通知。此外,如果就在ping请求654到达警报发送器模块622紧前从警报发送器模块622发出警报指示652,则警报接收器模块612将警报指示652视为ping响应。刚好在警报握手完成之后仍然返回“真”ping响应,因此仅以轻微的延迟用信号通知警报,并且警报接收器模块612如此解释。在这两种冲突情况下,信令延迟的数量级为握手长度加上握手之间的恒定数量的暂停周期(例如,两个发送方周期)。

[0171] 在一些实现方式中,完整性故障电路系统618针对信号完整性问题监视差分对。如果检测到编码故障,则警报接收器模块612断言警报完整性故障信号668。这至少可以在以下故障情况中发生:首先,警报指示差分路径(例如,第一对导线)可能没有在警报接收器模块612处被正确编码。这可以在接收器侧被直接标记为完整性故障。其次,在警报发送器模块622处,确认差分路径(例如,第二对导线)或ping请求差分路径(例如,第三对导线)可能没有被正确编码。后两种故障中的任一种都可以由警报发送器模块622处的完整性故障电路系统(未示出)检测,且通过使警报发送器模块622将正负警报指示线设置为相同值而用信号通知回警报接收器模块612。此外,警报发送器模块622可以连续切换该值。这在警报接收器模块612处隐含地触发信号完整性警报。若干信令模式可以表示故障。例如,如果差分对的正负线都具有低电压或同时都具有高电压,则观察到故障。

[0172] 图7图示了警报处置器204的升级发送器模块714和升级处置器750的升级接收器模块724之间的示例通信关系700,升级处置器750是一种类型的外围设备。如图所示,信令通路734包括多对导线(例如,两对)以使能跨越两个差分路径的差分信令。每对导线包括一根正导线和一根负导线。模块可以至少同步地跨信令通路734通信。在示例实现方式中,升级处置器750基于激活对策指令702执行或至少开始安全对策。

[0173] 作为警报处置器204内的警报处置路径的一部分,升级定时器(未示出)向升级发送器模块714提供升级指令776。响应于接收到升级指令776,升级发送器模块714在第二对导线(例如,如图所示的较低对)上将升级命令778传输到升级接收器模块724。响应于接收升级命令778,升级接收器模块724生成激活对策指令702。因此,升级处置器750响应于传输的升级命令778至少启动如本文所述的安全对策的执行。

[0174] 对于pinging协议,升级发送器模块714从ping监测器604接收ping指令658。在ping指令658的提示下,升级发送器模块714在第二对导线上将ping请求780传输到升级接收器模块724。为了指示到升级处置器750的连接是有效的和功能性的,升级接收器模块724在第一对导线(例如,如图所示的上对)上将ping响应782传输回升级发送器模块714。升级发送器模块714从升级接收器模块724接收ping响应782。为了完成ping协议循环,响应于ping响应782的接收,升级发送器模块714将ping okay消息660转发到ping监测器604。

[0175] 在一些情况下,完整性故障电路系统618的至少一部分被耦合到或合并到升级发送器模块714中。该完整性故障电路系统618监视至少一对导线以确定适当的差分信令是否存在于差分路径上和预期的信令模式匹配实际的信令模式。如果不是,则完整性故障电路系统618生成升级完整性故障信号770并将该信号提供给警报处置器204的控制器(未示出)作为警报处置器204的内部警报。

[0176] 在一些实现方式中,对于S个升级严重性中的每一个(其中,S表示正整数,如四),警报处置器204实例化升级发送器模块714。对应的S个升级处置器750每个实例化对应的升

级接收器模块724。升级信令机制可以类似于告警信令机制。然而,如果升级处置器750与警报处置器204在相同的时钟域中,升级信令机制可以是完全同步的协议。为了促进同步通信,升级发送器模块714和升级接收器模块724可以使用相同的时钟和重置信号。

[0177] 如图7所示,每个发送器-接收器对与两个差分线对连接。一对从发送者延伸到接收者,另一对从接收者延伸到发送者。在接收到具有K>0的脉冲宽度的升级指令信号776时,升级发送器模块714将该信号编码为用于ping请求780的在差分路径上(例如,在第二个对导线)上的宽度(K+1)的差分脉冲。升级接收器模块724解码该消息并在一个周期(或一个时隙)的延迟之后输出的断言激活对策702。此外,当升级命令778被断言时,升级接收器模块724通过连续切换第一对导线上的正/负信号来确认接收到该消息。升级接收器模块724未能正确响应触发来自完整性故障电路系统618的升级完整性故障信号770。

[0178] 此外,任何一对导线路上的差分信令不匹配也触发针对升级完整性故障的警报770。可以在升级发送器模块714处直接检测用于ping响应和确认的在第一对导线上的不匹配。用于升级命令和ping请求的在第二对导线上的不匹配由升级接收器模块724用信号通知回升级发送器模块714,升级接收器模块724还可以包括完整性故障电路系统(未示出)以使能对在第二对导线上的不匹配的检测。为了执行该信令,升级接收器模块724可以将第一对导线的正响应线和负响应线两者设置为相同值,且在每个时钟周期或时隙切换该值。这在发送方侧隐含地触发升级信号完整性警报。可以利用这种反向信令机制来快速跟踪升级并在警报处置器204检测到特定升级信令路径已被篡改的情况下使用另一种对策。

[0179] 在一些实现方式中,升级处置器的ping测试类似于警报信令方案的ping测试。升级信令线可以被进行ping和/或线路测试以确定升级接收器模块724是否已经被篡改。这可以通过在升级发送器模块714断言ping指令658的输入来实现。ping请求780被编码为第二对导线上的单个周期脉冲,第二对导线也用于升级命令778的传输。然而,对于用于ping请求780的单周期脉冲,升级接收器模块724不将该单周期脉冲信令解码为升级命令。代替地,升级接收器模块724在第一对导线上以“1010”模式响应以传送ping响应782。

[0180] 响应于ping响应782,如果在一个等待周期之后正确接收到预期模式,则升级发送器模块714断言ping okay消息660。否则,升级发送器模块714首先断言升级完整性故障信号770以通知警报处置器204的控制器。随后,在达到可编程ping超时之后,ping监测器604使用升级ping故障信号(未显示)发出“ping故障”警报。在这种情况下,升级发送器模块714触发升级完整性故障信号770,因为“无ping响应”和“错误的ping响应”在该场境中是不明确的。

[0181] 此外,在该升级和对策场境中,升级信号优先于ping消息传递。因此,如果升级指令776已经被断言,则用ping okay消息660确认ping指令658。如果升级指令776变为被断言,则正在进行的ping序列也被中止。在某些情况下,ping和升级响应序列预计在发出ping请求或升级命令后开始一个周期。否则,升级发送器模块714断言升级完整性故障信号770。

[0182] 已经一般性地描述了用于外围设备与安全电路系统的兼容性的方案、技术和硬件,现在该讨论转向示例方法。

[0183] 外围设备与安全电路系统的兼容性的示例方法

[0184] 下面参考图8和9的流程图描述示例方法。图8通过流程图800图示了用于实现外围设备与安全电路系统的兼容性的装置的示例方法。流程图800包括三个块802-806。

[0185] 在块802,处理器基于互连方案根据用于处理器和多个外围设备之间的交互的公共框架,通过互连与多个外围设备中的外围设备通信。例如,处理器202可以基于互连方案404根据用于处理器202和多个外围设备2501…250-P之间的交互的公共框架通过互连110与多个外围设备250-1…250-P中的外围设备250-P通信。例如,在处理器202上执行的软件可以使用基于互连方案404制造的电路系统与外围设备250P通信。

[0186] 在块804,外围设备基于互连方案根据公共框架通过互连与处理器通信。例如,外围设备250-P可以基于互连方案404根据公共框架通过互连110与处理器202通信。在一些情况下,外围设备250-P可以如通过使用互连110提供解密结果,来响应在处理器202上执行的软件。或者,如果经由互连110传输中断,则中断信号506可被传送到处理器202的中断处置电路系统。

[0187] 在块806,外围设备基于设备间方案根据用于多个外围设备中的至少两个外围设备之间的交互的公共框架与多个外围设备中的另一外围设备通信。例如,外围设备250-P可以基于设备间方案406根据用于在多个外围设备250中的至少两个外围设备之间交互的公共框架与多个外围设备250-1…250-P中的另一外围设备250-1进行通信。为此,外围设备250-P可以使用电路系统(例如,一根或多根导线、缓冲器或模块)和基于接口规范402的设备间方案406建立的通信协议320来向外围设备250-1传输至少一个信号。

[0188] 图9通过流程图900图示了用于实现外围设备与安全电路系统的兼容性的装置的附加示例方法。流程图900包括三个块902-906。

[0189] 在框902,电子设备接收对应于用于安全电路系统的外围设备的外围设备设计代码,其中,该外围设备设计代码包括设备间信令的一个或多个指示。例如,在电子设备1000(如下所述的图10的)上执行的兼容性分析模块410可以接收对应于安全电路系统106的外围设备250的外围设备设计代码412,外围设备设计代码412包括设备间信令420的一个或多个指示。设备间信令420的一个或多个指示可以包括例如要在至少两个外围设备之间通信的信号的名称和其他属性,如至少一种设备间通信316。

[0190] 在块904,电子设备分析外围设备设计代码,包括将设备间信令的一个或多个指示与用于至少在安全电路系统内进行通信的公共框架的接口规范的设备间方案进行比较。例如,在电子设备1000上执行的兼容性分析模块410可以分析外围设备设计代码412,包括将设备间信令420的一个或多个指示与用于至少在安全电路系统106内进行通信的公共框架的接口规范402的设备间方案406进行比较。在一些情况下,兼容性分析模块410可以确保设备间信令420的一个或多个指示符合设备间方案406中在两个或更多个允许的属性之间的存在、语法和关系的方面提出的约定。

[0191] 在块906,响应于分析,电子设备提供指示外围设备设计代码是否与接口规范的设备间方案一致的兼容性报告。例如,响应于分析,电子设备1000的兼容性分析模块410可以提供指示外围设备设计代码412是否与接口规范402的设备间方案406一致的兼容性报告416。这里,作为生成兼容性报告416的一部分,兼容性分析模块410可以识别至少一个不遵守设备间方案406的设备间信令指示420。兼容性分析模块410还可以在兼容性报告416中包括对接口规范402的相关部分的引用或关于修复违规以使设备间信令指示420符合设备间方案406的提示。

[0192] 这些方法的方面可以被实现在例如硬件(例如,固定逻辑电路系统或与存储器结

合的处理器)、固件、软件或其某种组合中。可以使用图1和至7和10中所示的装置或部件中的一个或多个来实现这些方法,该部件可以进一步被划分和组合等。这些图中的装置和部件一般代表硬件,诸如电子器件、PCB、封装模块、IC芯片、部件或电路;固件;软件;或其组合。因此,这些图图示了能够实现所描述的方法的许多可能的系统或装置中的一些。

[0193] 对于本文描述的方法和相关联的流程图,显示和/或描述操作的顺序不旨在被解释为限制。相反,所描述的方法操作的任意数量或组合可以以任意顺序组合以实现给定方法或替代方法。也可以从所描述的方法中省略操作或向其添加操作。此外,可以完全或部分重叠的方式实施所描述的操作。

[0194] 用于外围设备与安全电路系统的兼容性的示例电子设备

[0195] 图10示出了根据一个或多个所描述的方面的示例电子设备1000的各种部件,其可以实现外围设备与安全电路系统的兼容性。电子设备1000可以被实现为固定设备、移动设备、独立设备或嵌入式设备中的任何一种或组合;以消费者、计算机、便携式、用户、服务器、通信、电话、导航、游戏、音频、相机、消息传递、媒体播放和/或其他类型的电子设备1000——诸如在图1作为装置102描述的智能电话——的任何形式实现。一个或多个所示部件可以实现为电子设备1000的至少一个集成电路上的分立部件或集成部件。

[0196] 电子设备1000可以包括一个或多个通信收发器1002,其使能设备数据1004——诸如接收的数据、传输的数据或上面标识的其他信息——的有线和/或无线通信。示例通信收发器1002包括近场通信(NFC)收发器、符合各种IEEE 802.15(Bluetooth™)标准的无线个域网(PAN)(WPAN)无线电、符合各种IEEE 802.11(Wi-Fi™)标准的任一标准的无线局域网(LAN)(WLAN)无线电、用于蜂窝电话的无线广域网(WAN)(WWAN)无线电(例如符合3GPP的那些)、符合各种IEEE 802.16(WiMAX™)标准的无线城域网(MAN)(WMAN)无线电、符合红外数据协会(IrDA)协议的红外(IR)收发器和有线局域网(LAN)(WLAN)以太网收发器。

[0197] 电子设备1000还可以包括一个或多个数据输入端口1006,经由该端口可以接收任何类型的数据、媒体内容和/或其他输入,其他输入诸如是用户可选择的输入、消息、应用程序、音乐、电视内容、录制的视频内容以及从任何内容和/或数据源——包括像麦克风或相机这样的传感器——接收的任何其他类型的音频、视频和/或图像数据。数据输入端口1006可以包括USB端口、同轴电缆端口、用于光纤互连或布线的光纤端口以及用于闪存、DVD和CD等的其他串行或并行连接器(包括内部连接器)。这些数据输入端口1006可用于将电子设备耦合到部件、外设或附件,例如键盘、麦克风、相机或其他传感器。

[0198] 该示例的电子设备1000包括至少一个处理器1008(例如,应用处理器、微处理器、数字信号处理器(DSP)和控制器等中的任何一个或多个),其可以包括组合处理器以及存储器系统(例如,实现为SoC的一部分),其处理(例如,执行)计算机可执行指令以控制设备的操作。处理器1008可以被实现为应用处理器、嵌入式控制器、微控制器、安全处理器和人工智能(AI)加速器等。通常,处理器或处理系统可以至少部分地以硬件实现,该硬件可以包括集成电路或片上系统的部件、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、复杂可编程逻辑器件(CPLD)和使用硅和/或其他材料的其他实现。

[0199] 替代地或另外地,电子设备1000可以用电子电路系统中的任何一个或组合来实现,该电子电路系统可以包括软件、硬件、固件或结合处理和控制电路实现的固定逻辑电路系统,这些处理和控制电路系统通常是以1010表示(为电子电路系统1010)。该电子电路系

统1010可以诸如通过存储在计算机可读介质上的处理/计算机可执行指令和通过逻辑电路系统和/或硬件(例如,诸如FPGA)等实现可执行的或基于硬件的模块(图10中未示出)。

[0200] 虽然未示出,但是电子设备1000可以包括系统总线、互连、交叉开关、数据传输系统或耦合设备内的各种部件的其他交换结构。系统总线或互连可以包括不同总线结构中的任何一种或组合,诸如存储器总线或存储器控制器、外围总线、通用串行总线和/或利用多种总线架构中的任何一种的处理器或本地总线。

[0201] 电子设备1000还包括一个或多个使得能够存储数据的存储器设备1012,其示例包括随机存取存储器(RAM)、非易失性存储器(例如只读存储器(ROM)、闪存、EPROM和EEPROM)以及磁盘存储设备。因此,存储器设备1012可以分布在系统的不同逻辑存储级上以及分布在不同的物理部件处。存储器设备1012提供数据存储机制以存储设备数据1004、其他类型的代码和/或数据以及各种设备应用程序1020(例如,软件应用程序或程序)。例如,操作系统1014可以被保存为存储器设备1012内的软件指令并且由处理器1008执行。

[0202] 在一些实现方式中,电子设备1000还包括音频和/或视频处理系统1016,其处理音频数据和/或将音频和视频数据传递到音频系统1018和/或显示系统1022(例如,视频缓冲区或智能手机或相机的屏幕)。音频系统1018和/或显示系统1022可以包括处理、显示和/或否则呈现音频、视频、显示和/或图像数据的任何设备。显示数据和音频信号可以通过RF(射频)链接、S-video链接、HDMI(高清多媒体接口)、复合视频链接、分量视频链接、DVI(数字视频接口)、模拟音频连接、视频总线或其他类似的通信链路——诸如媒体数据端口1024——传送到音频部件和/或显示部件。在一些实现方式中,音频系统1018和/或显示系统1022是电子设备1000的外部或独立部件。或者,显示系统1022例如可以是示例电子设备1000的集成部件,诸如集成触摸界面的一部分。

[0203] 图10的电子设备1000是图1的装置102的示例实现方式、能够实现图4的分析414的设备的示例实现方式以及能够实现图8和9的任何方法的设备的示例实现方式。电子设备1000因此可以包括安全电路系统106,其可以是单独的IC芯片或包括为另一IC芯片或设备的一部分——如,处理器1008、电子电路系统1010或存储器设备1012。因此例如,一个或多个所示部件可以集成在同一个IC芯片——如SoC——上,或者至少集成在单个PCB上。如图所示,电子设备1000可以附加地或替代地包括兼容性分析模块410。例如,存储器设备1012可以存储兼容性分析模块410,并且处理器1008可以执行兼容性分析模块410。因此,存储器设备1012还可以存储外围设备设计代码412和接口规范402等。电子设备1000可替代地使用通信收发器1002或数据输入端口1006来访问接口规范402或外围设备设计代码412。因此,如本文所述的外围设备与安全电路系统的兼容性的原理可通过图10的电子设备1000或结合图10的电子设备1000实现。

[0204] 其他示例

[0205] 在下文中,描述了一些示例。

[0206] 示例1:一种包括安全电路系统的集成电路,所述安全电路系统包括:互连;耦合到所述互连的处理器;以及,多个外围设备,每个相应的外围设备耦合到互连并且包括接口,所述接口被配置为遵守用于与处理器和所述多个外围设备的其他外围设备交互的公共框架,所述接口包括:互连接口,其被配置为将所述相应的外围设备耦合到所述互连;以及,设备间接口,其被配置为将所述相应的外围设备耦合到所述多个外围设备中的其他外围设

备。

[0207] 示例2:示例1的集成电路,其中,每个相应的外围设备包括相应的安全功能模块,所述相应的安全功能模块被配置为提供相应的安全相关功能。

[0208] 示例3:示例1或2的集成电路,其中,所述相应的安全相关功能包括以下至少一项:警报处置;密码操作;安全的数据存储;随机数生成;或者,所述安全电路系统的输入/输出通信。

[0209] 示例4:根据前述示例中任一项所述的集成电路,其中,所述设备间接口响应于包括在用于所述相应的外围设备的设计代码中的属性而耦合到延伸到所述多个外围设备中的另一外围设备的至少一条导线。

[0210] 示例5:根据前述示例中任一项所述的集成电路,其中,所述接口包括时钟接口,所述时钟接口包括对于下述的访问:主要系统时钟,所述相应的外围设备被配置为至少基于所述主要系统时钟访问所述互连;以及,一个或多个次要系统时钟,所述相应的外围设备被配置为基于所述一个或多个次要系统时钟执行功能或与所述多个外围设备中的另一外围设备进行通信。

[0211] 示例6:根据前述示例中任一项所述的集成电路,其中:所述相应的外围设备包括寄存器接口,所述寄存器接口包括用于与所述相应的外围设备相关联的中断的至少一个中断入口;以及,所述相应的外围设备被配置为将所述寄存器接口的至少一部分暴露给所述处理器。

[0212] 示例7:根据前述示例中任一项所述的集成电路,其中:所述至少一个中断入口包括:中断使能指示;中断状态指示;以及,中断测试寄存器;以及,所述相应的外围设备被配置为提供所述处理器访问以清除所述中断状态指示。

[0213] 示例8:根据前述示例中任一项所述的集成电路,其中:所述多个外围设备中的所述相应的外围设备包括至少一个警报发送器模块;以及,所述警报发送器模块被配置为经由信令通路传输来自所述相应的外围设备的警报指示。

[0214] 示例9:根据前述示例中任一项所述的集成电路,其中:所述信令通路包括至少一个差分路径;以及,所述警报发送器模块被配置为响应于检测到所述信令通路的所述至少一个差分路径的完整性故障而传输警报完整性故障信号。

[0215] 示例10:根据前述示例中的任一个所述的集成电路,其中,所述集成电路包括以下至少一个:片上系统(SoC);或者,信任根(RoT)芯片。

[0216] 示例11:一种用于外围设备与安全电路系统的兼容性的方法,该方法包括:基于互连方案根据用于处理器和多个外围设备之间的交互的公共框架,由所述处理器通过互连与所述多个外围设备中的外围设备进行通信;基于所述互连方案根据所述公共框架,由所述外围设备通过所述互连与所述处理器进行通信;以及,基于设备间方案根据用于在所述多个外围设备中的至少两个外围设备之间进行交互的所述公共框架,由所述外围设备与所述多个外围设备中的另一外围设备进行通信。

[0217] 示例12:根据示例11的方法,其中,所述外围设备与所述多个外围设备中的所述另一外围设备进行通信包括:所述外围设备绕过所述互连与所述另一外围设备进行通信。

[0218] 示例13:根据示例11或12的方法,其中,所述外围设备与所述多个外围设备中的所述另一外围设备进行通信包括:由所述外围设备使用从通过用于所述外围设备的设计代码

指定的属性导出的电路向所述另一外围设备传输设备间信号。

[0219] 示例14:根据示例11至13中任一项的方法,其中:由所述外围设备通过所述互连与所述处理器的所述通信包括由所述外围设备基于所述外围设备的中断入口的中断状态指示向所述处理器传输中断信号;以及,由所述处理器通过所述互连与所述外围设备的所述通信包括清除所述中断入口的所述中断状态指示。

[0220] 示例15:根据示例11至14中任一项的方法,其中:由所述外围设备与所述多个外围设备中的所述另一外围设备的所述通信包括由所述外围设备从所述另一外围设备接收升级命令,所述另一个外围设备包括警报处置器;以及,所述方法还包括响应于从所述警报处置器接收到所述升级命令,由所述外围设备激活对策。

[0221] 示例16:一种用于外围设备与安全电路系统的兼容性的方法,所述方法包括:接收对应于用于安全电路系统的外围设备的外围设备设计代码,该外围设备设计代码包括设备间信令的一个或多个指示;分析外围设备设计代码,包括将设备间信令的一个或多个指示与用于至少在安全电路系统内进行通信的公共框架的接口规范的设备间方案进行比较;并且响应于分析,提供指示外围设备设计代码是否与接口规范的设备间方案一致的兼容性报告。

[0222] 示例17:根据示例16的方法,其中:设备间信令的一个或多个指示涉及在不使用安全电路系统的互连的情况下在两个或更多外围设备之间交换的信号;并且设备间方案建立用于定义绕过互连的设备间信令的格式。

[0223] 示例18:根据示例16或17的方法,其中,设备间方案包括强制性部分和可选部分。

[0224] 示例19:根据示例16至18中任一项的方法,其中,外围设备设计代码包括处理器-设备信令的一个或多个指示,并且该方法进一步包括:分析外围设备设计代码,包括将处理器设备信号的一个或多个指示与公共框架的接口规范的互连方案进行比较;响应于包括比较处理器-设备信令的一个或多个指示的分析,生成兼容性报告以指示外围设备设计代码是否与接口规范的互连方案一致。

[0225] 示例20:根据示例16至19中任一项的方法,其中,外围设备设计代码包括中断信令的一个或多个指示,并且该方法进一步包括:分析外围设备设计代码,包括将中断信令的一个或多个指示与用于公共框架的接口规范的中断方案相比较;且响应于包括比较中断信令的一个或多个指示的分析,生成兼容性报告以指示外围设备设计代码是否与接口规范的中断方案一致。

[0226] 除非上下文另有说明,否则本文中使用词“或”可被视为使用“包含性或”或允许包含或应用由词“或”链接的一个或多个项目的术语(例如,短语“A或B”可以解释为仅允许“A”、仅允许“B”或允许“A”和“B”)。此外,如本文所用,提及项目列表中的“至少一个”的短语是指那些项目的任何组合,包括单个成员。例如,“a、b或c中的至少一个”可以涵盖a、b、c、a-b、a-c、b-c和a-b-c,以及与多个相同元素的任何组合(例如,a-a、a-a-a、a-a-b、a-a-c、a-b-b、a-c-c、b-b、b-b-b、b-b-c、c-c和c-c-c或a、b和c的任何其他顺序)。此外,在附图中表示的项目和在此讨论的术语可以指示一个或多个项目或术语,并且因此可以互换地参考本书面描述中的单数或复数形式的项目和术语。尽管已经以特定于某些特征和/或方法的语言描述了用于外围设备与安全电路系统的兼容性的实现方式,但所附权利要求的主题不一定限于所描述的特定特征或方法。相反,特定特征和方法被公开为用于外围设备与安全电路系

统的兼容性的示例实现方式。

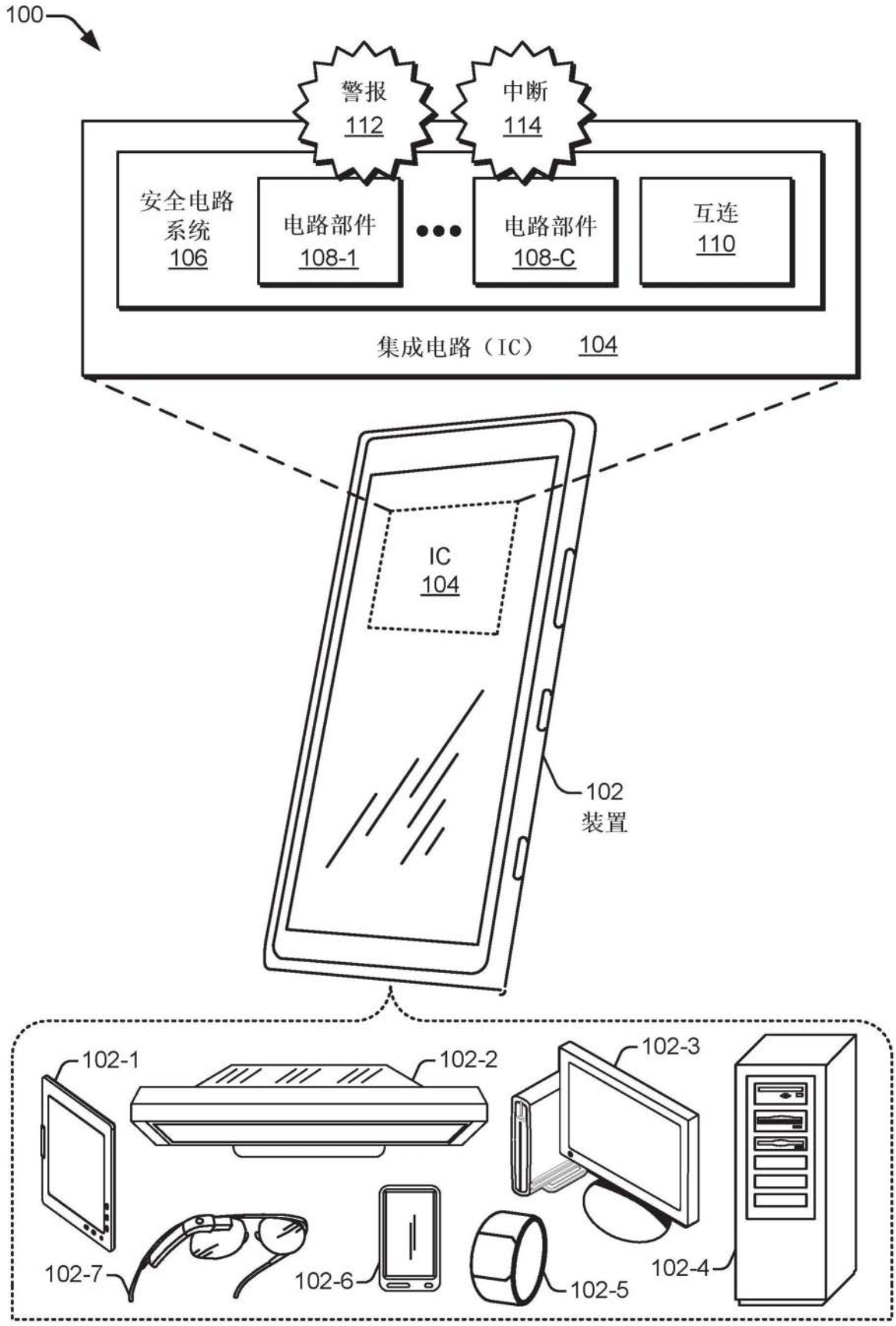

100
警报
112
中断
114
安全电路
系统
106
电路部件
108-1
电路部件
108-C
互连
110
集成电路（IC） 104
IC
104
102
装置
102-1
102-2
102-3
102-4
102-5
102-6
102-7

图1

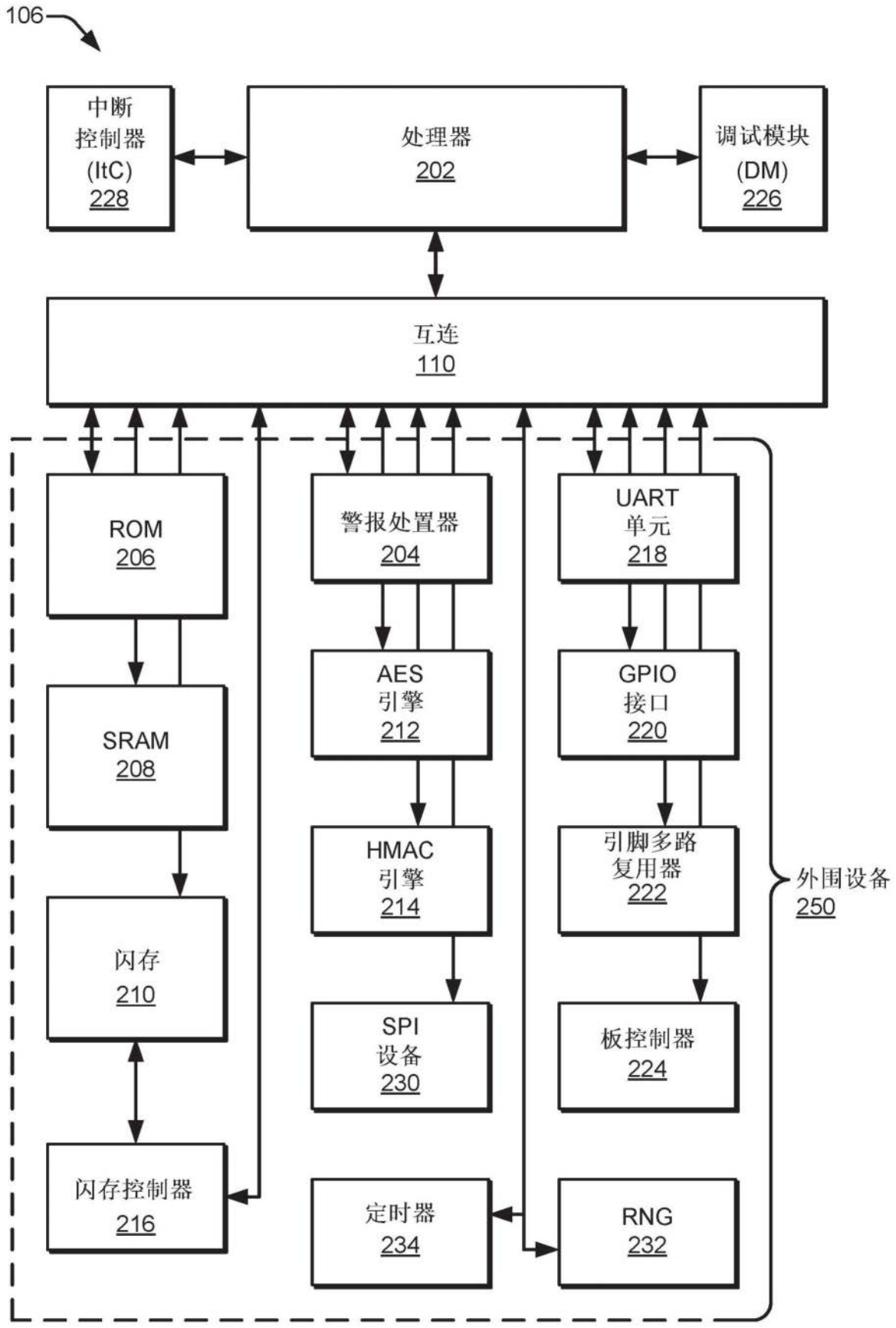

106
中断
控制器
(ItC)
228
处理器
202
调试模块
(DM)
226
互连
110
ROM
206
SRAM
208
闪存
210
闪存控制器
216
警报处置器
204
AES
引擎
212
HMAC
引擎
214
SPI
设备
230
定时器
234
UART
单元
218
GPIO
接口
220
引脚多路
复用器
222
板控制器
224
RNG
232
外围设备
250

图2

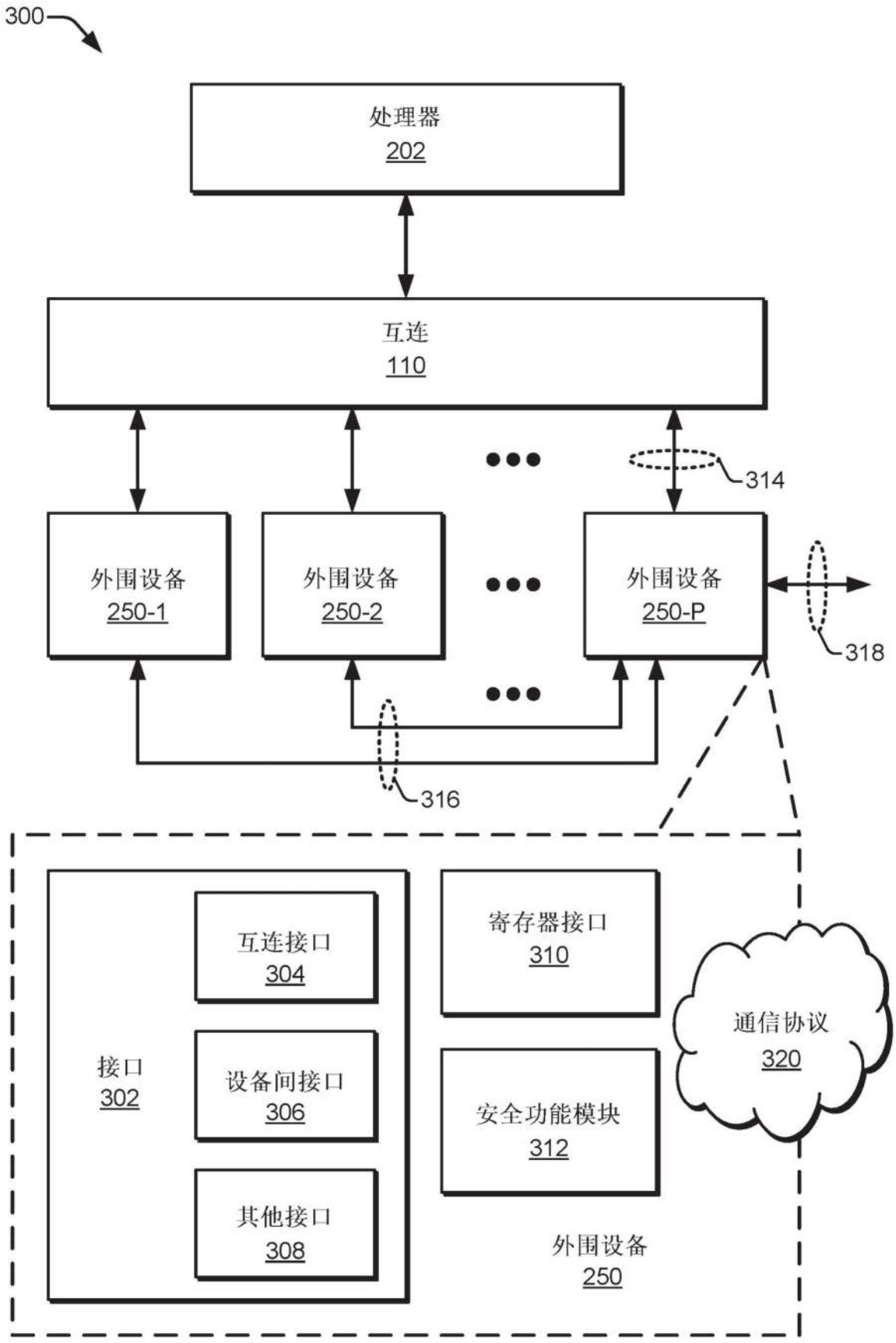

300
处理器
202
互连
110
314
外围设备
250-1
外围设备
250-2
外围设备
250-P
318
316
互连接口
304
接口
302
设备间接口
306
其他接口
308
寄存器接口
310
安全功能模块
312
通信协议
320
外围设备
250

图3

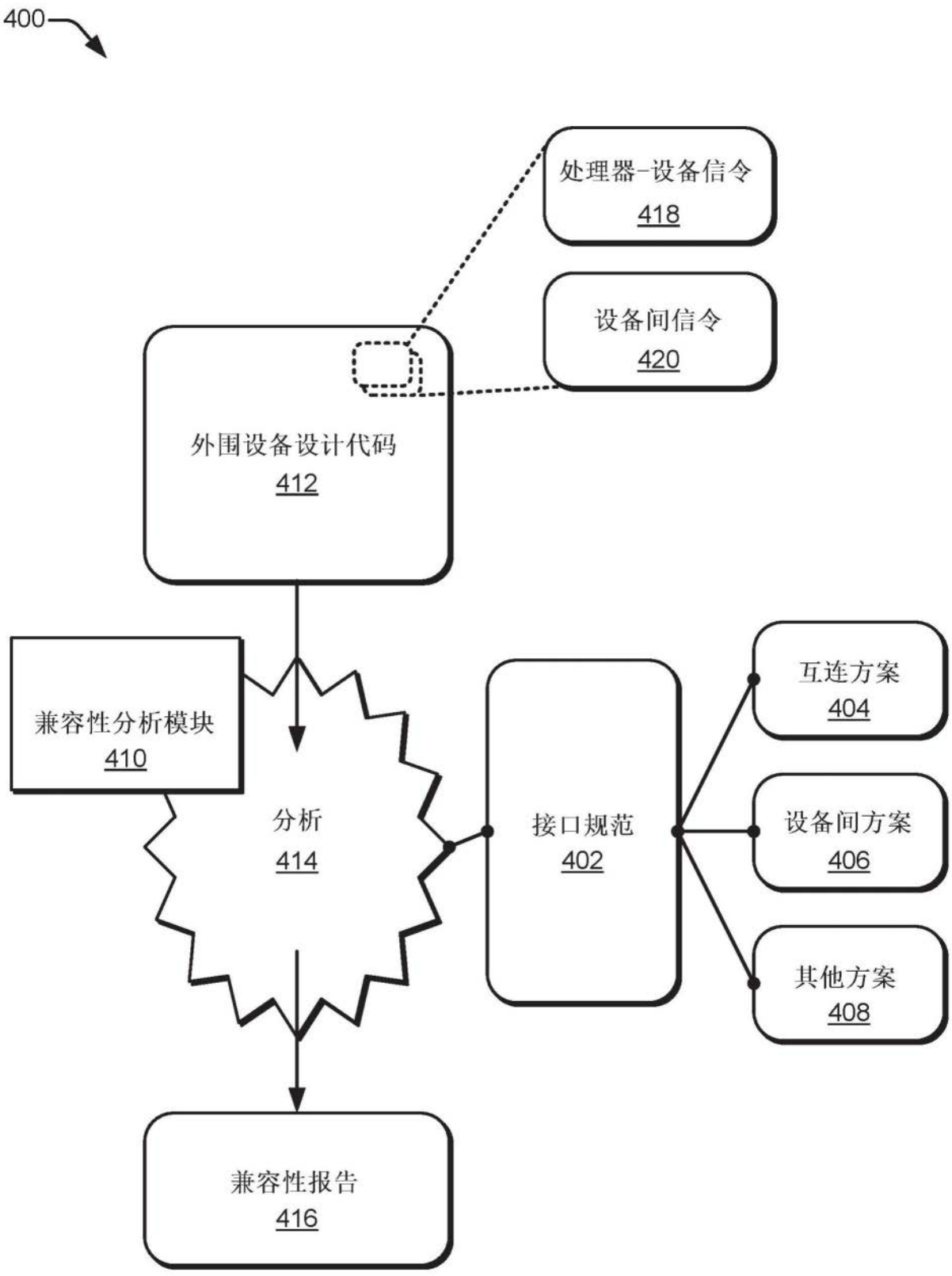

400
处理器-设备信令
418
设备间信令
420
外围设备设计代码
412
兼容性分析模块
410
分析
414
接口规范
402
互连方案
404
设备间方案
406
其他方案
408
兼容性报告
416

图4

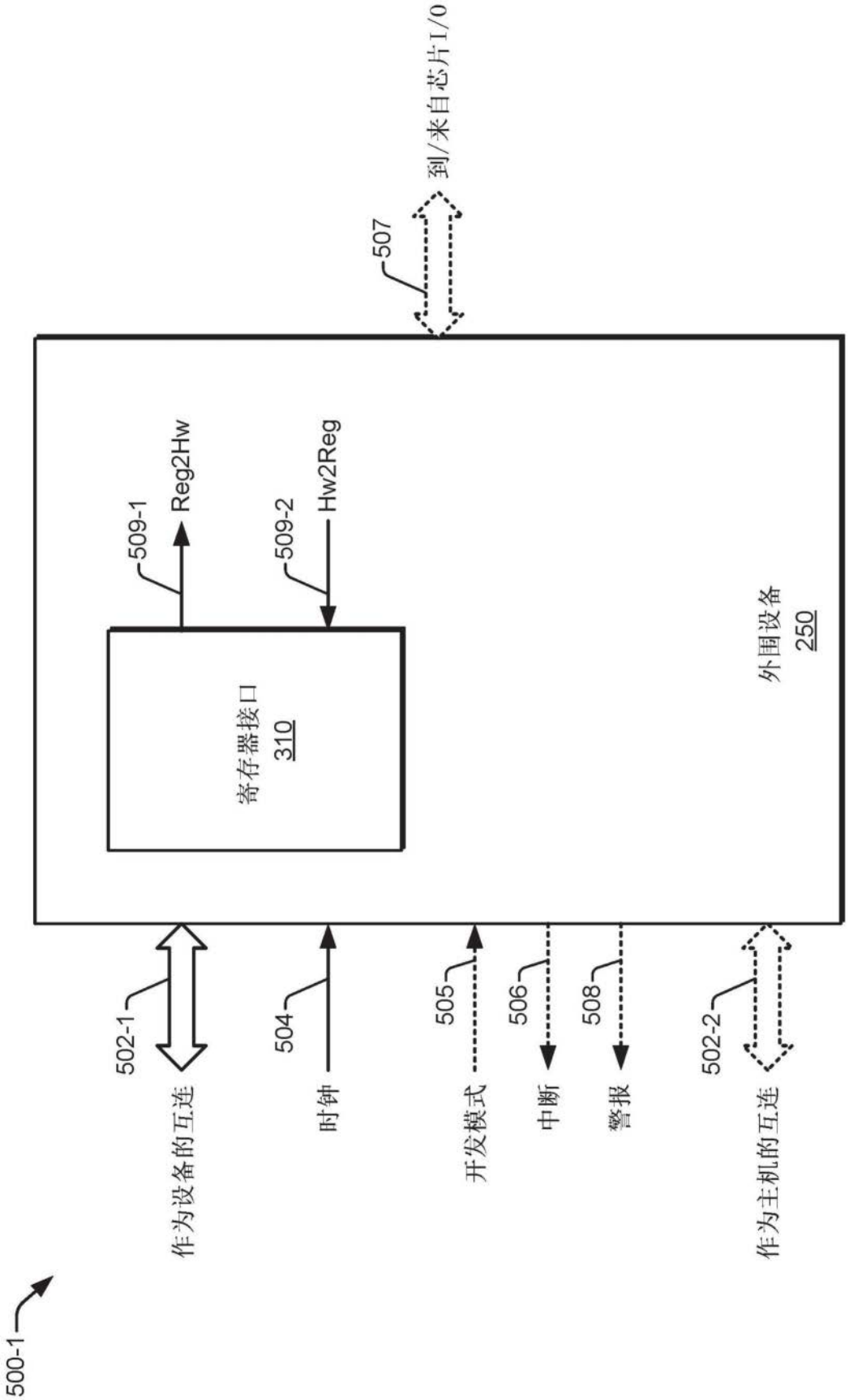

500-1
502-1
作为设备的互连
504
时钟
505
开发模式
506
中断
508
警报
502-2
作为主机的互连
外围设备
250
寄存器接口
310
509-1
Reg2Hw
509-2
Hw2Reg
507
到/来自芯片I/O

图5-1

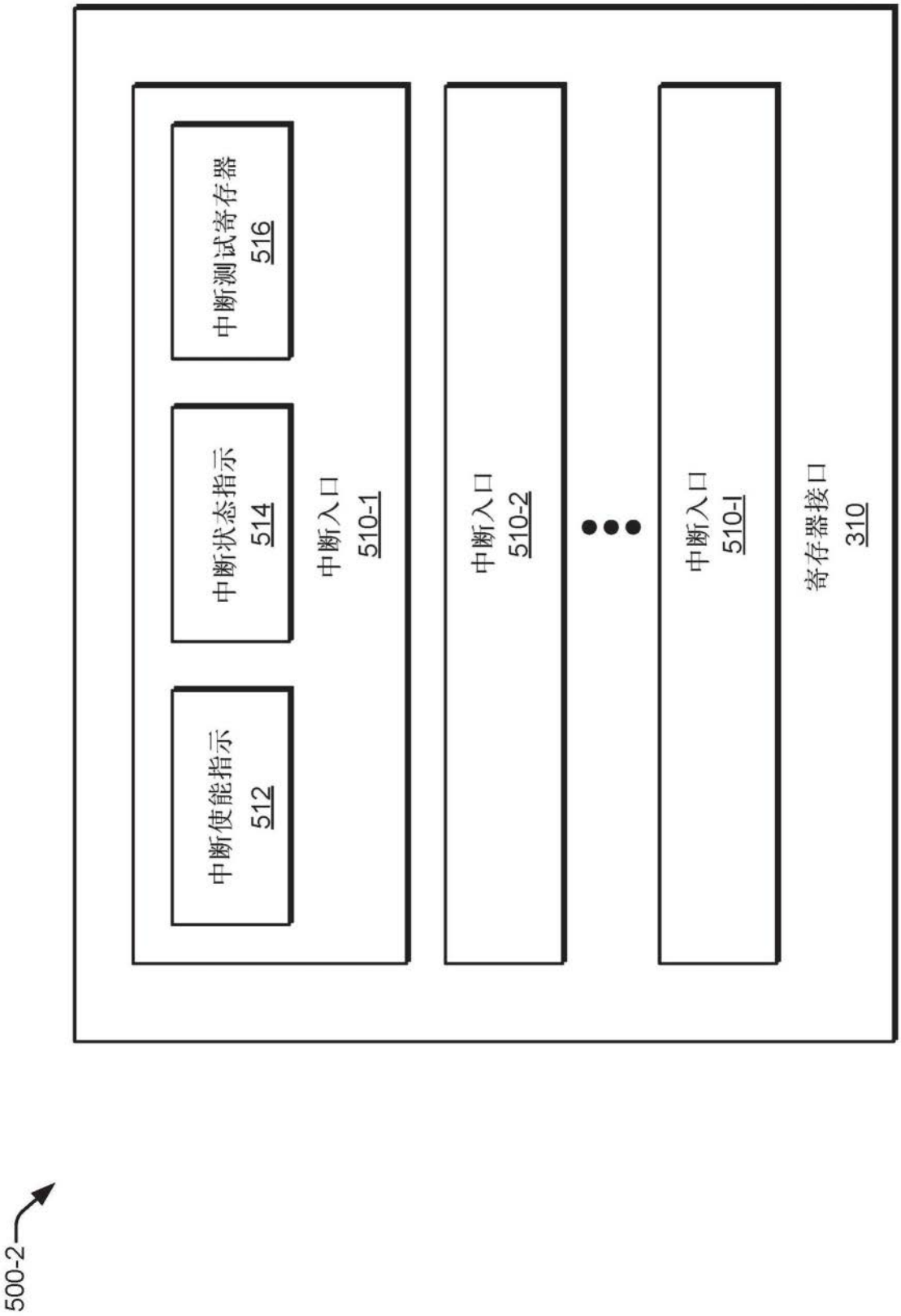

寄存器接口
310
中断入口
510-1
中断使能指示
512
中断状态指示
514
中断测试寄存器
516
中断入口
510-2
中断入口
510-I
500-2

图5-2

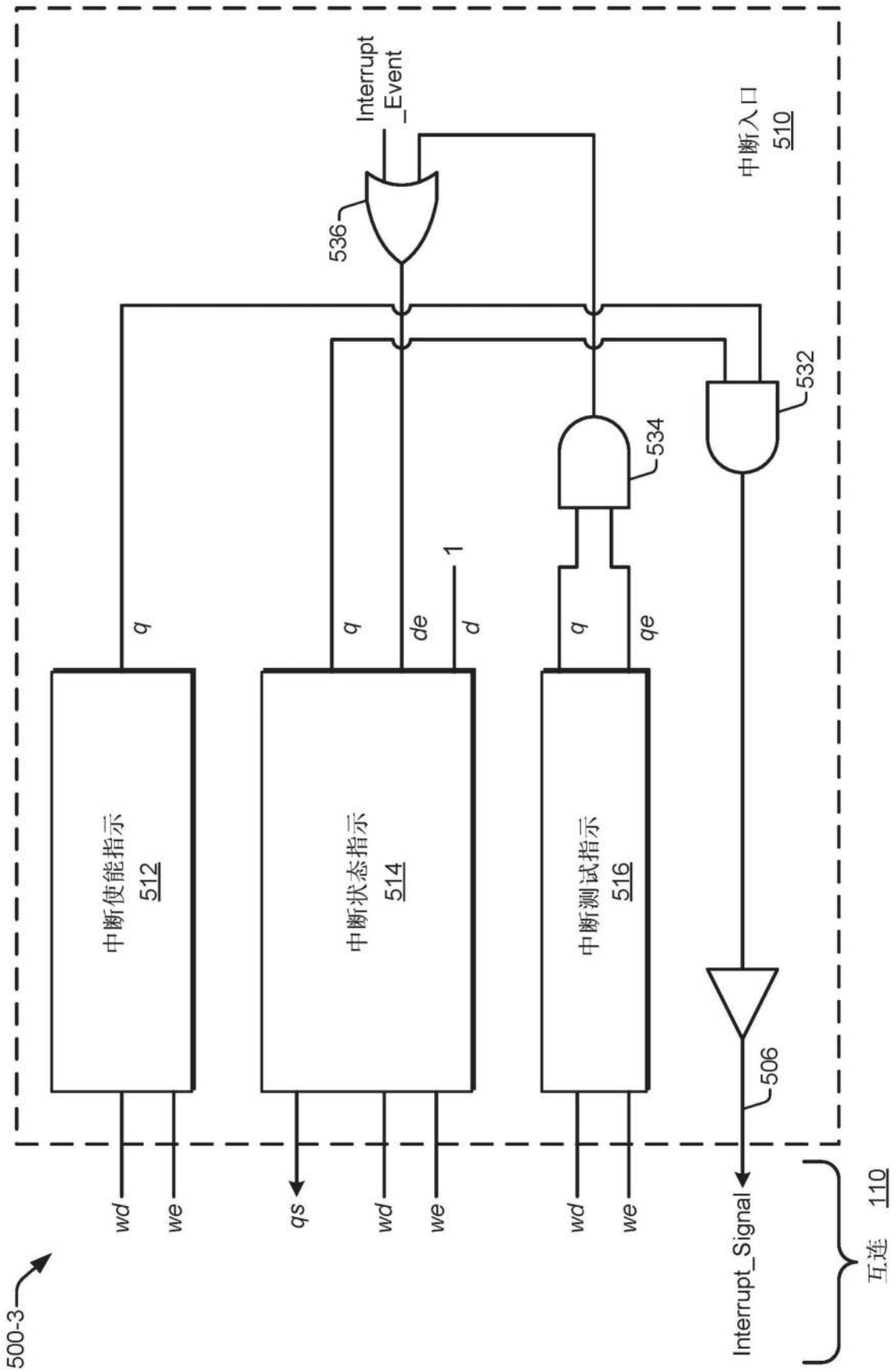

Interrupt_Event
536
中断入口
510
532
534
q
q
de
1
d
q
qe
中断使能指示
512
中断状态指示
514
中断测试指示
516
506
wd
we
qs
wd
we
wd
we
Interrupt_Signal
互连 110
500-3

图5-3

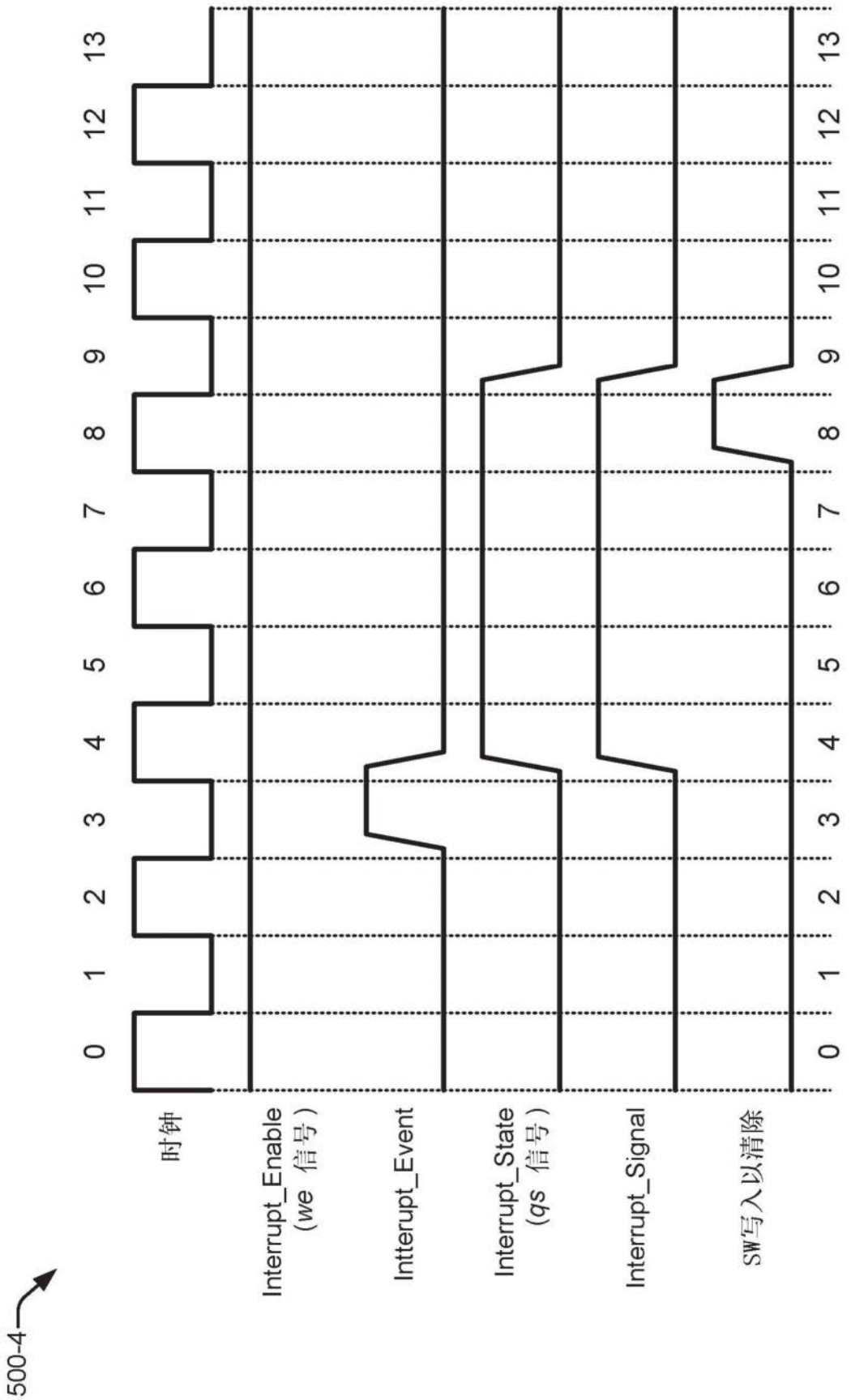

500-4
时钟
Interrupt_Enable
(we 信号)
Intterupt_Event
Interrupt_State
(qs 信号)
Interrupt_Signal
SW写入以清除
0
1
2
3
4
5
6
7
8
9
10
11
12
13

图5-4

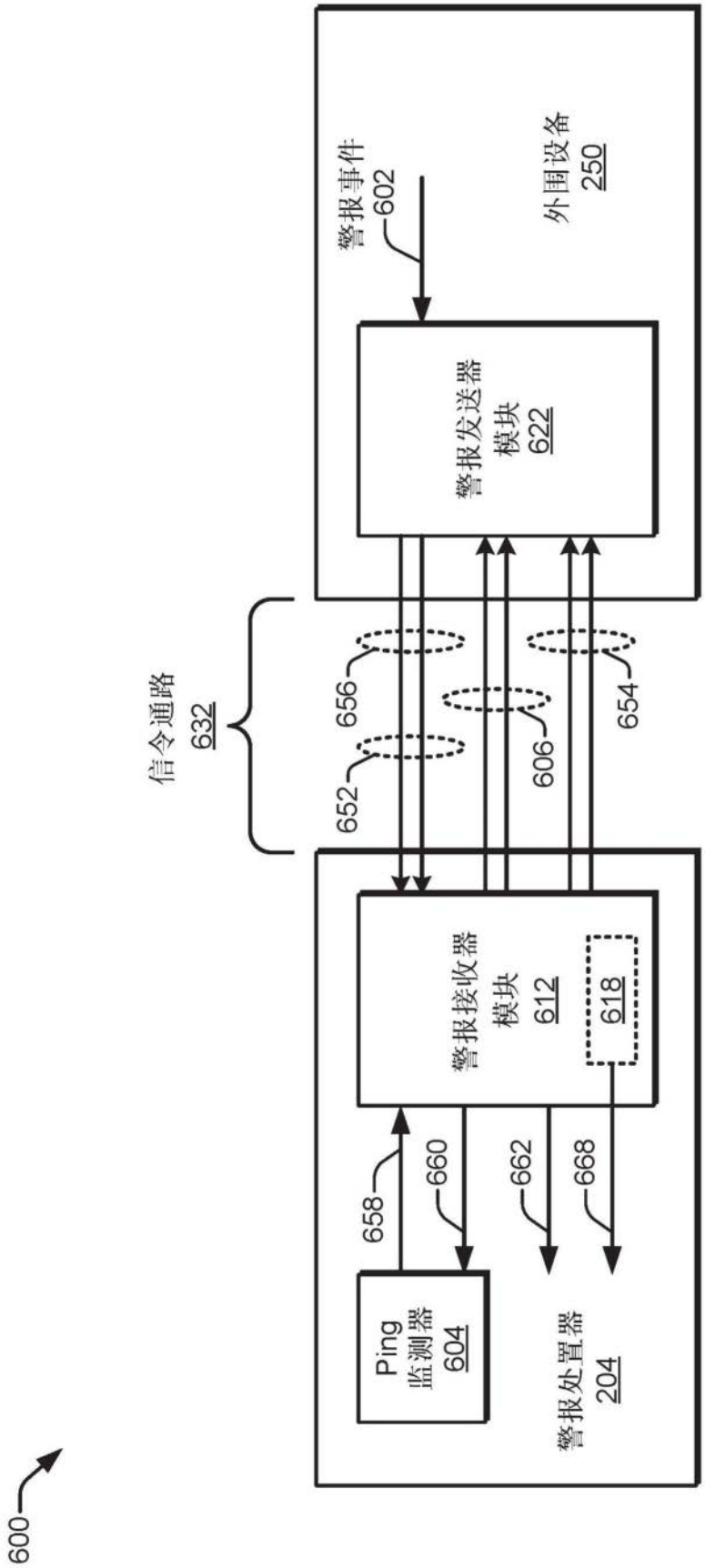

600
外围设备
250
警报事件
602
警报发送器
模块
622
信令通路
632
656
652
606
654
警报接收器
模块
612
618
658
660
662
668
Ping
监测器
604
警报处置器
204

图6

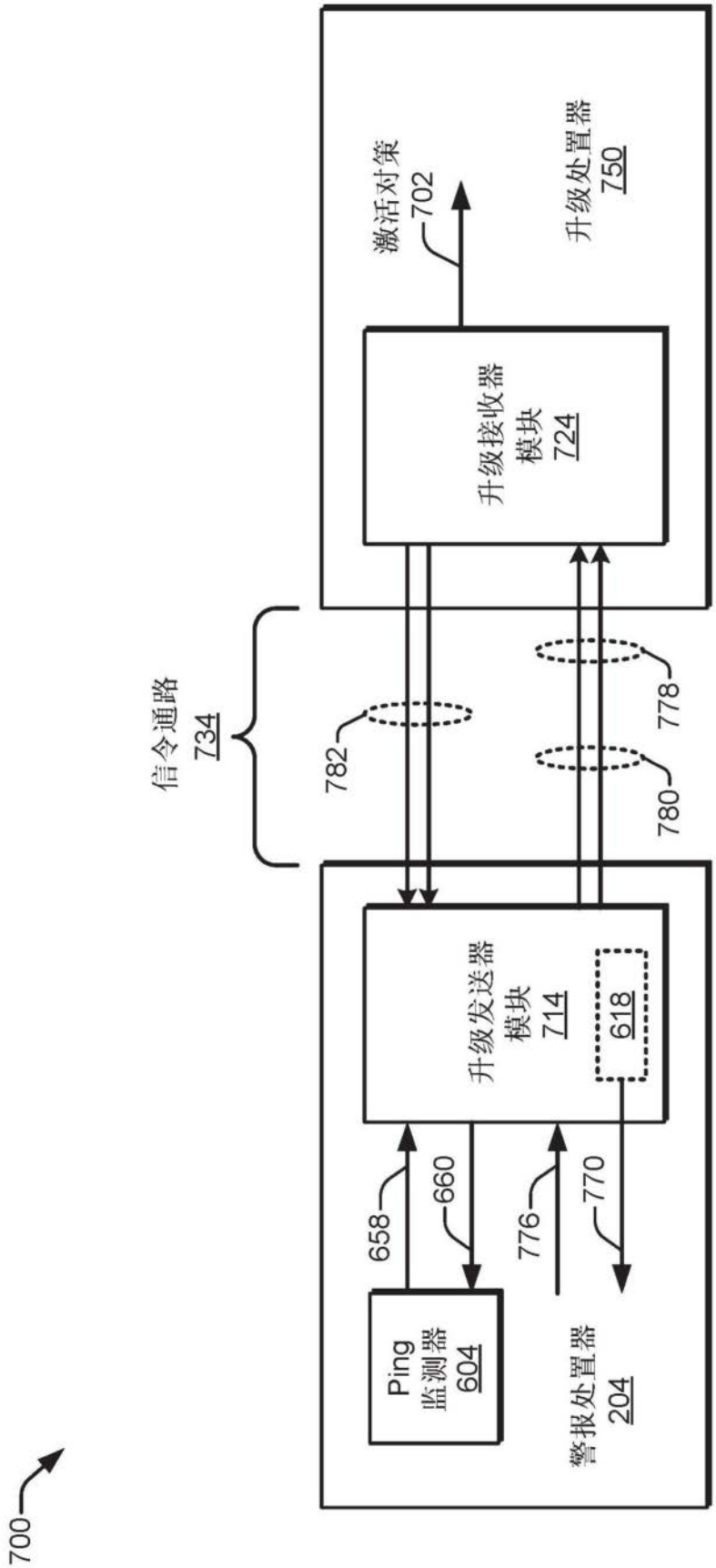

700
警报处置器
204
Ping
监测器
604
658
660
776
770
升级发送器
模块
714
618
信令通路
734
782
780
778
升级接收器
模块
724
激活对策
702
升级处置器
750

图7

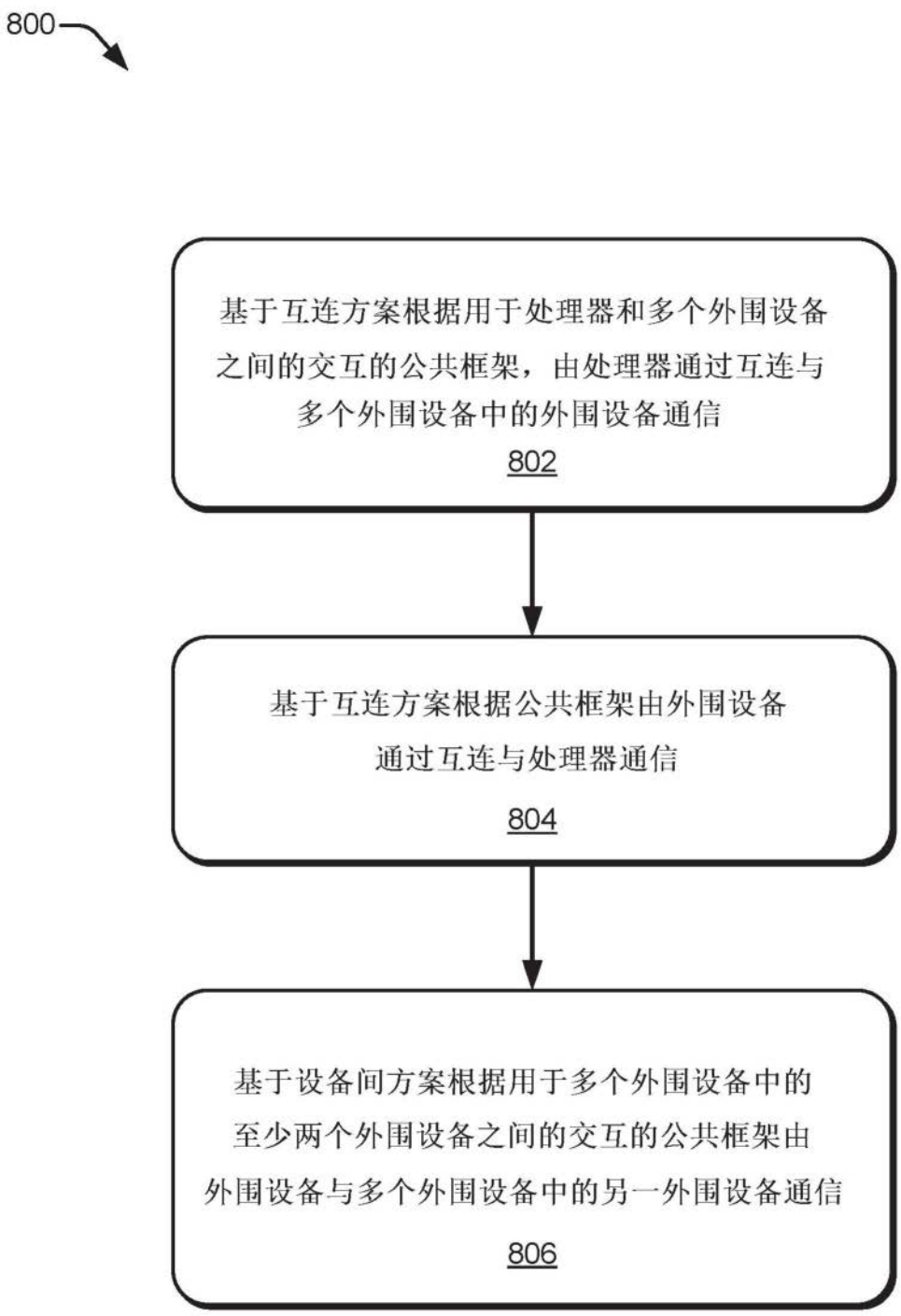

800
基于互连方案根据用于处理器和多个外围设备之间的交互的公共框架，由处理器通过互连与多个外围设备中的外围设备通信
802
基于互连方案根据公共框架由外围设备通过互连与处理器通信
804
基于设备间方案根据用于多个外围设备中的至少两个外围设备之间的交互的公共框架由外围设备与多个外围设备中的另一外围设备通信
806

图8

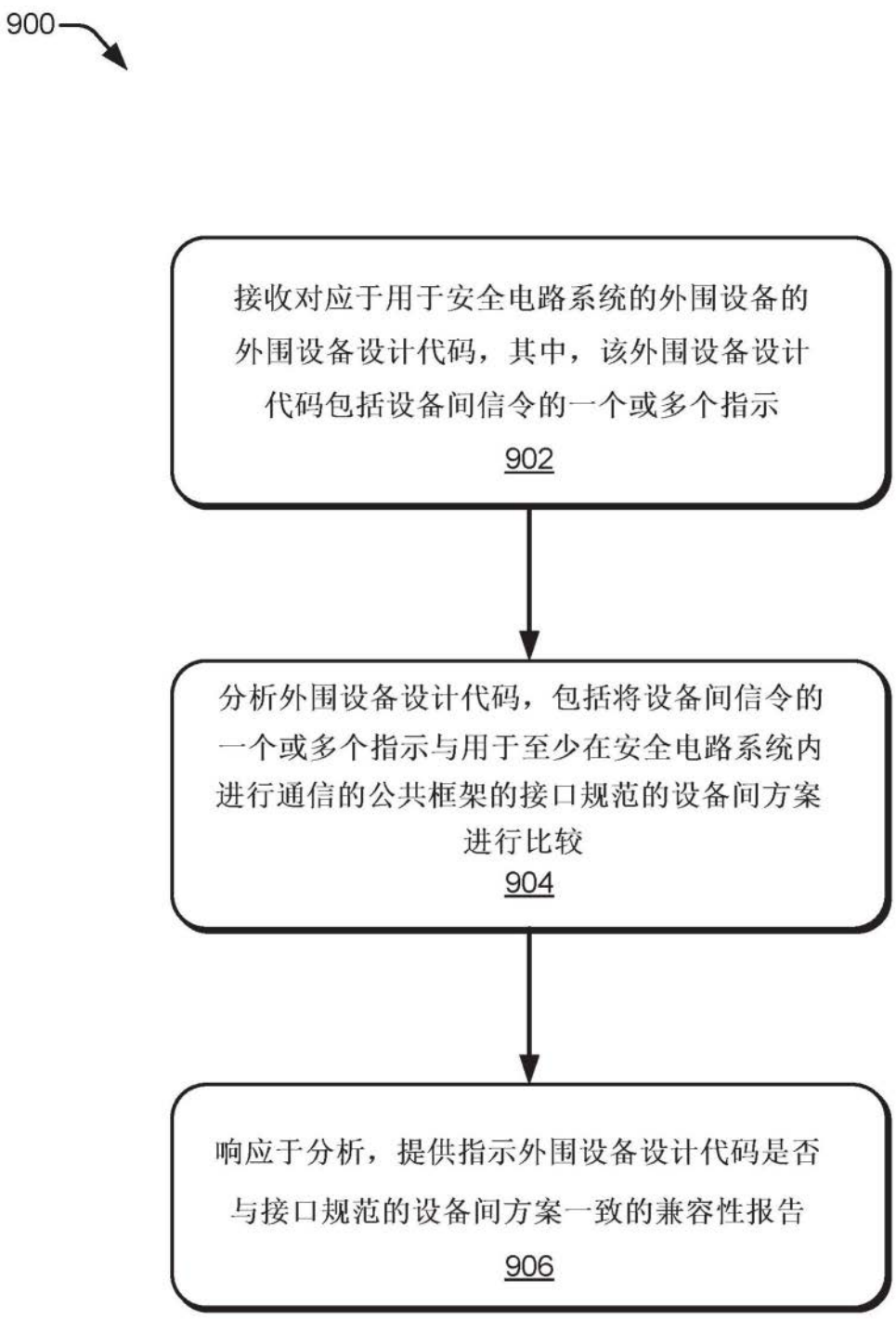

900
接收对应于用于安全电路系统的外围设备的外围设备设计代码，其中，该外围设备设计代码包括设备间信令的一个或多个指示
902
分析外围设备设计代码，包括将设备间信令的一个或多个指示与用于至少在安全电路系统内进行通信的公共框架的接口规范的设备间方案进行比较
904
响应于分析，提供指示外围设备设计代码是否与接口规范的设备间方案一致的兼容性报告
906

图9

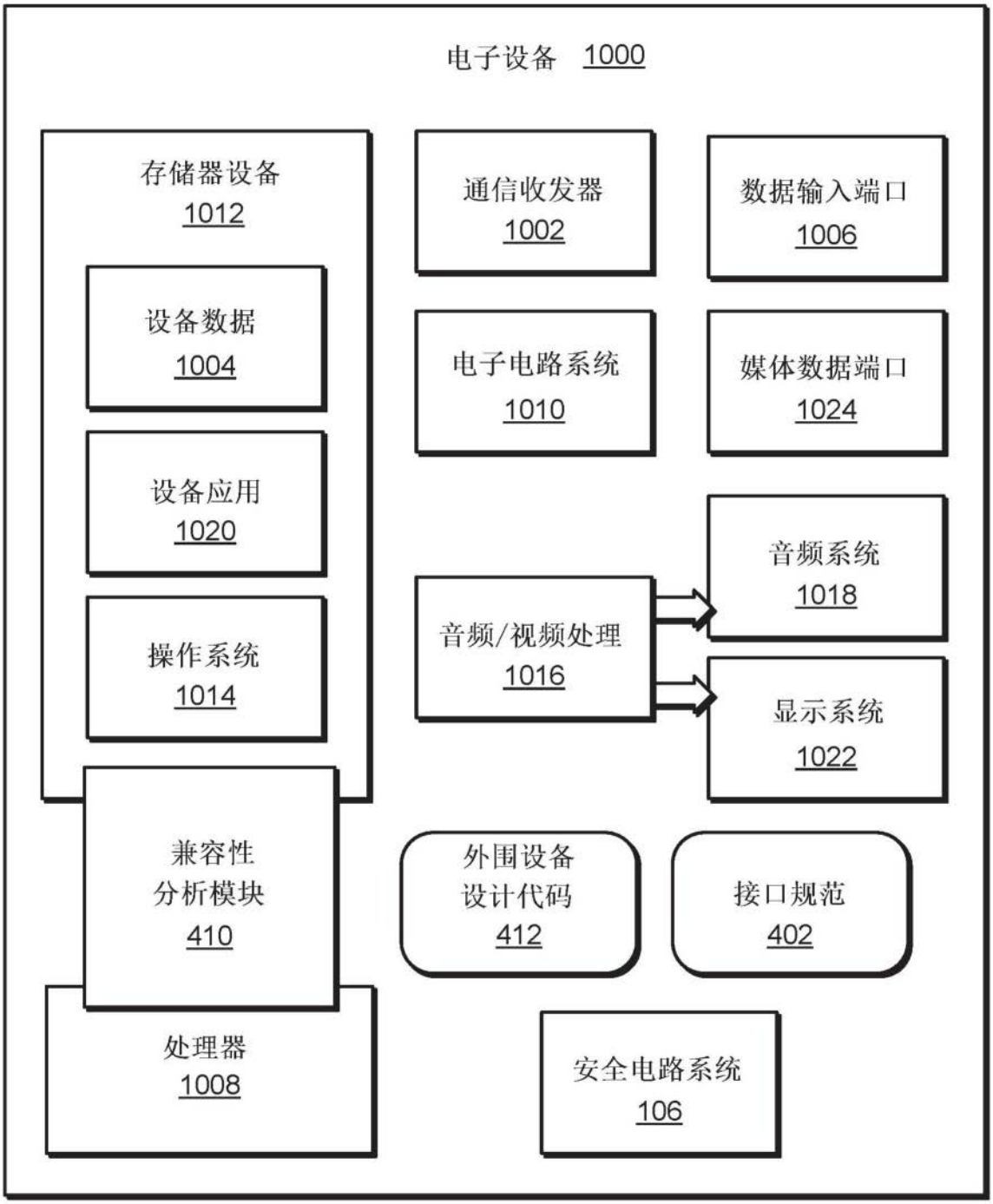

电子设备 1000
存储器设备
1012
设备数据
1004
设备应用
1020
操作系统
1014
兼容性
分析模块
410
处理器
1008
通信收发器
1002
电子电路系统
1010
音频/视频处理
1016
外围设备
设计代码
412
安全电路系统
106
数据输入端口
1006
媒体数据端口
1024
音频系统
1018
显示系统
1022
接口规范
402

图10