(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110874096 B
(45)授权公告日 2024.08.20

(21)申请号 201910806582.5

(22)申请日 2019.08.28

(65)同一申请的已公布的文献号
申请公布号 CN 110874096 A

(43)申请公布日 2020.03.10

(30)优先权数据
18306142.3 2018.08.29 EP

(73)专利权人 恩智浦有限公司
地址 荷兰埃因霍温高科技园区60邮编：5656 AG

(72)发明人 简·彼得·斯考特 泽维尔·乌尔安德烈斯·巴里拉多·冈萨雷斯

(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 纪雯

(51)Int.Cl.
G05B 23/02(2006.01)

(56)对比文件
US 5428624 A,1995.06.27

审查员 师长义

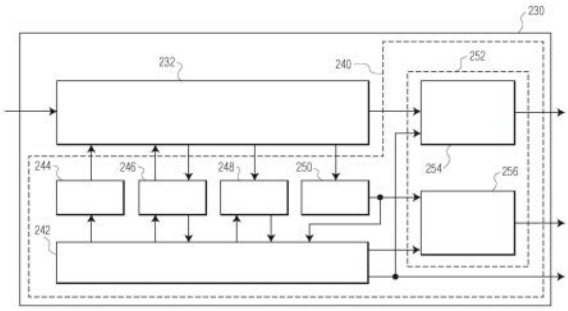
权利要求书2页 说明书10页 附图5页

(54)发明名称

具有集成故障监测系统的集成电路装置

(57)摘要

本文公开了一种集成电路装置。所述装置包括被配置成执行功能的电路、故障管理部件、至少一个用户寄存器、模拟测试总线部件、内置自测部件、安全监测部件和门控逻辑。另外，所述电路与所述故障管理部件、所述至少一个用户寄存器、所述模拟测试总线部件、所述内置自测部件、所述安全监测器和所述门控逻辑分离。



CN 110874096 B

1.一种集成电路IC装置,其特征在于,包括:

电路,所述电路被配置成执行功能;

故障管理部件,所述故障管理部件被配置成管理所述电路的故障监测;

至少一个用户寄存器,所述至少一个用户寄存器被连接以从所述故障管理部件接收控制信号并且被连接以向所述电路提供寄存器值从而控制所述电路的一方面;

模拟测试总线部件,所述模拟测试总线部件被配置成与所述电路中的节点建立连接以将模拟信号传递到所述节点并且与所述故障管理部件就数字信号进行通信;

内置自测部件,所述内置自测部件连接到所述电路以测试所述电路并且与所述故障管理部件就数字信号进行通信;

安全监测部件,所述安全监测部件连接到所述电路以从所述电路接收信号并且响应于从所述电路接收的所述信号输出安全监测信号;以及

门控逻辑,所述门控逻辑被配置成响应于来自所述故障管理部件的信号对来自所述电路和/或来自所述安全监测部件的信号进行门控;

其中所述电路与所述故障管理部件、所述至少一个用户寄存器、所述模拟测试总线部件、所述内置自测部件、所述安全监测部件和所述门控逻辑分离。

2.根据权利要求1所述的IC装置,其特征在于,所述故障管理部件被配置成处理数字信号。

3.根据权利要求1或2所述的IC装置,其特征在于,所述至少一个用户寄存器从所述故障管理部件接收数字控制信号。

4.根据权利要求3所述的IC装置,其特征在于,所述数字控制信号用于控制所述电路中的参数。

5.根据权利要求1或2所述的IC装置,其特征在于,所述模拟测试总线部件被配置成经由模拟测试总线将模拟信号注入到所述电路中。

6.根据权利要求1或2所述的IC装置,其特征在于,所述模拟测试总线部件包括数模转换器DAC和模数转换器ADC中的至少一个,所述DAC用于将来自所述故障管理部件的数字信号转换为模拟信号以注入到所述电路中,所述ADC用于将来自所述电路的模拟信号转换为数字信号以用于所述故障管理部件。

7.根据权利要求1或2所述的IC装置,其特征在于,所述内置自测部件被配置成测试安全关键性电路的参数偏差。

8.根据权利要求1或2所述的IC装置,其特征在于,所述安全监测部件被配置成响应于来自所述电路的信号监测环形振荡器的温度、电源电压、电源噪声、输出信号电平、输入信号电平和频率中的至少一个。

9.根据权利要求1或2所述的IC装置,其特征在于:

所述至少一个用户寄存器从所述故障管理部件接收数字控制信号;

所述模拟测试总线部件包括:模拟测试总线;数模转换器DAC和模数转换器ADC中的至少一个,所述DAC用于将来自所述故障管理部件的数字信号转换为模拟信号以注入到所述电路中,所述ADC用于将来自所述电路的模拟信号转换为数字信号以用于所述故障管理部件;

所述内置自测部件被配置成测试安全关键性电路的参数偏差;并且

所述安全监测部件被配置成响应于来自所述电路的信号监测环形振荡器的温度、电源电压、电源噪声、输出信号电平、输入信号电平和频率中的至少一个。

10.一种用于监测集成电路IC装置中的故障的方法,其特征在于,所述方法包括:

在所述IC装置的故障管理部件处,控制故障通过所述IC装置的用户寄存器、通过所述IC装置的模拟测试总线部件并且通过所述IC装置的内置自测部件注入到所述IC装置的电路中;以及

在所述IC装置的所述故障管理部件处,接收与所述注入的故障有关的输出,其中,与所述注入的故障有关的输出作为数字值从所述IC装置的安全监测部件接收。

具有集成故障监测系统的集成电路装置

技术领域

[0001] 本发明涉及一种集成电路IC装置,特别涉及一种具有集成故障监测系统的集成电路装置。

背景技术

[0002] 在推动可以实施如驾驶员辅助和自动驾驶等先进功能的更加智能的汽车的过程中,利用了许多电子部件。电子部件,通常也称为电子控制单元(ECU),用在如视觉系统(相机、雷达、LIDAR)、防抱死制动系统和安全气囊系统等安全关键性应用中。ECU包括功能部件(FC),如包括安全关键性电路的微控制器(MCU)、智能传感器和智能致动器。ECU经常通过使ECU能够传送的车载网络(IVN)彼此连接。

[0003] 为了确保下一代汽车的安全性,业界已经转向实施国际标准化组织的标准(ISO)26262,这是电气和电子系统的功能性安全标准。包括用于汽车应用的安全关键性电路的集成电路(IC)装置必须在考虑到ISO26262的情况下进行设计和操作。

发明内容

[0004] 公开了一种装置和方法的实施例。在一个实施例中,公开了一种集成电路(IC)装置。所述IC装置包括:故障管理部件,所述故障管理部件被配置成管理电路的故障监测;至少一个用户寄存器,所述至少一个用户寄存器被连接以从所述故障管理部件接收控制信号并且被连接以向所述电路提供寄存器值从而控制所述电路的一方面;模拟测试总线部件,所述模拟测试总线部件被配置成与所述电路中的节点建立连接以将模拟信号传递到所述节点并且与所述故障管理部件就数字信号进行通信;内置自测部件,所述内置自测部件连接到所述电路以测试所述电路并且与所述故障管理部件就数字信号进行通信;安全监测部件,所述安全监测部件连接到所述电路以从所述电路接收信号并且响应于从所述电路接收的所述信号输出安全监测信号;以及门控逻辑,所述门控逻辑被配置成响应于来自所述故障管理部件的信号对来自所述电路和/或来自安全监测器的信号进行门控。另外,所述电路与所述故障管理部件、所述至少一个用户寄存器、所述模拟测试总线部件、所述内置自测部件、安全监测器和所述门控逻辑分离。

[0005] 在一个实施例中,所述故障管理部件被配置成处理数字信号。

[0006] 在一个实施例中,所述至少一个用户寄存器从所述故障管理部件接收数字控制信号。

[0007] 在一个实施例中,所述数字控制信号用于控制所述电路中的参数。

[0008] 在一个实施例中,所述模拟测试总线部件被配置成经由模拟测试总线将模拟信号注入到所述电路中。

[0009] 在一个实施例中,所述模拟测试总线部件包括数模转换器(DAC)和模数转换器(ADC)中的至少一个,所述数模转换器用于将来自所述故障管理部件的数字信号转换为模拟信号以注入到所述电路中,所述模数转换器用于将来自所述电路的模拟信号转换为数字

信号以用于实施故障管理部件。

[0010] 在一个实施例中,所述内置自测部件被配置成测试安全关键性电路的参数偏差。

[0011] 在一个实施例中,所述安全监测器被配置成响应于来自所述电路的信号监测环形振荡器的温度、电源电压、电源噪声、输出信号电平、输入信号电平和频率中的至少一个。

[0012] 在一个实施例中,所述至少一个用户寄存器从所述故障管理部件接收数字控制信号;所述模拟测试总线部件包括:模拟测试总线;数模转换器(DAC)和模数转换器(ADC)中的至少一个,所述数模转换器用于将来自所述故障管理部件的数字信号转换为模拟信号以注入所述电路中,所述模数转换器用于将来自所述电路的模拟信号转换为数字信号以用于所述故障管理部件;所述内置自测部件被配置成测试安全关键性电路的参数偏差;并且所述安全监测器被配置成响应于来自所述电路的信号监测环形振荡器的温度、电源电压、电源噪声、输出信号电平、输入信号电平和频率中的至少一个。

[0013] 在一个实施例中,所述电路执行的所述功能是安全关键性功能。

[0014] 在一个实施例中,所述电路与所述故障管理部件、所述至少一个用户寄存器、所述模拟测试总线部件、所述内置自测部件、所述安全监测器和所述门控逻辑分离,因为所述电路和故障监测系统的部件具有单独的电源线、单独的电源接地线、单独的时钟信号、单独的启用和/或复位信号和单独的测试控制信号中的至少一个。

[0015] 一种用于监测IC装置中的故障的方法涉及:在所述IC装置的故障管理部件处,控制故障通过所述IC装置的用户寄存器、通过所述IC装置的模拟测试总线部件并且通过所述IC装置的内置自测部件处注入到所述IC装置的电路中;以及在所述IC装置的所述故障管理部件处,接收与所述注入的故障有关的输出。

[0016] 在所述方法的一个实施例中,控制故障通过所述IC装置的用户寄存器注入到所述IC装置的所述电路中涉及通过所述用户寄存器中的至少一个用户寄存器的寄存器值以数字方式控制所述电路的一方面。

[0017] 在所述方法的一个实施例中,控制故障通过所述IC装置的模拟测试总线部件注入到所述IC装置的所述电路中涉及以数字方式控制至少一个开关经由模拟测试总线将信号注入到所述电路中。

[0018] 在所述方法的一个实施例中,控制故障通过所述IC装置的内置自测部件注入到所述IC装置的所述电路中涉及以数字方式控制所述内置自测部件以使用内置自测电路将故障信号注入到所述电路中。

[0019] 在所述方法的一个实施例中,控制故障通过所述IC装置的用户寄存器注入到所述IC装置的所述电路中涉及通过所述用户寄存器中的至少一个用户寄存器的寄存器值以数字方式控制所述电路的一方面;控制故障通过所述IC装置的模拟测试总线部件注入到所述IC装置的所述电路中涉及以数字方式控制至少一个开关经由模拟测试总线将信号注入到所述电路中;并且控制故障通过所述IC装置的内置自测部件注入到所述IC装置的所述电路中涉及以数字方式控制所述内置自测部件以使用内置自测电路将故障信号注入到所述电路中。

[0020] 在所述方法的一个实施例中,所述方法涉及在故障注入期间对来自所述IC装置的安全监测器的输出进行门控以及在故障注入期间对来自所述IC装置的所述电路的输出进行门控中的一种。

[0021] 在所述方法的一个实施例中,与所述注入的故障有关的输出作为数字值从所述IC装置的安全监测器接收。

[0022] 在所述方法的一个实施例中,与所述注入的故障有关的输出作为数字状态值从所述IC装置的安全监测器接收,其中来自所述安全监测器的所述数字状态值反映所述电路的一方面的状态。

[0023] 在所述方法的一个实施例中,所述IC装置的所述电路执行安全关键性功能。

[0024] 从结合通过举例说明本发明的原理的附图进行的以下详细描述中,根据本发明的其它方面将会变得显而易见。

附图说明

[0025] 图1描绘了包括连接到总线的多个ECU的车载网络(IVN)的例子。

[0026] 图2描绘了包括安全关键性电路和故障监测系统的IC装置的例子实施例。

[0027] 图3描绘了IC装置的模拟测试总线部件的例子实施例。

[0028] 图4描绘了图2的IC装置,其中指示了安全关键性电路与安全监测系统的部件的分离。

[0029] 图5是用于监测IC装置中的故障的方法的过程流程图。

[0030] 贯穿本说明书,类似的附图标记可以用于指代类似的元件。

具体实施方式

[0031] 应当容易理解的是,如本文中总体上描述的并且在附图中示出的实施例的部件可以被布置和设计成各种不同配置。因此,如附图中表示的对各个实施例的以下更详细描述并不旨在限制本公开的范围,而仅仅是表示各个实施例。虽然在附图中呈现了实施例的各个方面,但是除非特别指示,否则附图不一定按比例绘制。

[0032] 可以在不脱离本发明的精神或基本特性的情况下以其它具体形式体现本发明。所描述实施例应当在所有方面均仅被视为是说明性的并且不是限制性的。因此,本发明的范围由所附权利要求书而非本详细说明来指示。落入权利要求书的同等意义和范围内的所有变化均应包含在权利要求书的范围内。

[0033] 贯穿本说明书中对特征、优点或类似语言的引用并不暗示可以利用本发明实现的所有特征和优点应当或已经存在于本发明的任何单个实施例中。相反,引用特征和优点的语言应被理解成意味着结合实施例描述的特定特征、优点或特性包括在本发明的至少一个实施例中。因此,贯穿本说明书,对特征和优点以及类似语言的讨论可以但不一定指代同一个实施例。

[0034] 此外,本发明的所描述特征、优点和特性可以通过任何适合的方式组合在一个或多个实施例中。相关领域技术人员应认识到,鉴于本文中的描述,可以在没有特定实施例的具体特征或优点中的一个或多个具体特征或优点的情况下实践本发明。在其它实例下,在某些实施例中可以认识到可能并不存在于在本发明的所有实施例中的另外的特征和优点。

[0035] 贯穿本说明书,对“一个实施例”、“实施例”或类似语言的引用意味着结合所指示实施例描述的特定特征、结构或特性包括在本发明的至少一个实施例中。因此,贯穿本说明书,短语“在一个实施例中(in one embodiment/in an embodiment)”和类似语言可以但不

一定均指代同一个实施例。

[0036] 如上所述,具有安全关键性电路的电子控制单元(ECU)连接到车载网络(IVN)。图1描绘了经由IVN总线连接多个ECU的车载网络(IVN)100的例子。在图1的例子中,IVN是包括CAN节点102(还被称为ECU)的控制器局域网络(CAN),每个CAN节点102连接到CAN总线104。在图1的实施例中,每个CAN节点包括微控制器110和收发器120。微控制器通常连接到至少一个装置(未示出)如传感器、致动器或其它某个控制装置等并且被编程成确定所接收消息的含义并且生成适合的传出消息。还被称为主机处理器、主机或数字信号处理器(DSP)的微控制器通常包括安全关键性电路,如用于实施视觉系统(相机、雷达、LIDAR)、防抱死制动系统和安全气囊系统的电路。收发器120位于微控制器110与CAN总线104之间并且实施物理层操作。CAN总线104承载模拟差分信号并且包括CAN高(CANH)总线124和CAN低(CANL)总线126。CAN总线在本领域中是已知的。尽管IVN被描述为CAN网络,但也可以使用其它IVN技术,包括例如FlexRay、局域互连网络(LIN)和以太网。

[0037] 如高级驾驶员辅助系统(ADAS)、自主驾驶和线控(X-by-wire)等新兴汽车应用需要经过改进的功能安全要求。根据ISO 26262标准中的规范,可以通过实施检测例如单点故障和潜在故障的状况监测功能来增加汽车安全完整性等级。状况监测是用于观察功能部件由于例如磨损而造成的退化。监测输出可以用于检测失效或即将发生的失效。

[0038] IC装置中的安全关键性电路的功能安全在很大程度上取决于集成到IC装置中的安全监测器的校正功能。这种安全监测器监测许多内部信号和/或状态,例如温度、电源电压、信号电平、信号失真、时钟占空比、锁相环(PLL)锁定状态等。

[0039] 如ISO 26262等汽车安全标准要求对安全性关键性故障进行最小诊断覆盖。具体地说,ISO 26262要求对多个故障进行最小诊断覆盖,例如在多于一个电路节点处发生故障。例如,ISO 26262要求在安全关键性电路中的一个故障和安全监测器中的并发故障的情况下进行诊断覆盖,这可能导致这样的情况:未检测到安全关键性电路中的故障。诊断覆盖还适用于这样的情况:一条电源线同时供应安全关键性电路的一部分和安全监测器两者,从而使得电源线的单个缺陷导致安全关键性电路和安全监测器两者中均有故障。因此,需要半导体制造商提供可以满足所需多故障检测覆盖目标的IC装置。

[0040] 用于提供多故障检测覆盖的三种常规方法包括故障树分析(FTA)、失效模式及影响分析(FMEA)和故障注入。故障树分析方法涉及规定每个可能的故障对发生的可能性和被检测到的可能性。这一方法在存在有限数量的易量化可能故障(例如,少于20个)时很好地工作。然而,故障树分析方法可能难以在可以有约10,000个可能故障的IC装置的上下文中实施。失效模式及影响分析方法涉及总结在故障树分析中看到的不同失效模式。这一方法会比故障树分析方法更有效,但是失效模式及影响分析方法在约100个节点的情况下是可行的,而针对节点数较多(例如10,000个或更多个节点)的IC装置则可能变得不切实际。故障注入方法涉及在不同的节点对处注入故障的情况下运行仿真。故障注入技术针对多达约几百个节点是可行的。然而,因为ISO 26262还要求对瞬时故障进行诊断覆盖,所以故障注入方法可能变得不切实际。在不同时间将故障注入不同的节点对中可能会导致极长的仿真时间。

[0041] 在根据本发明的一个实施例中,公开了一种IC装置。所述IC装置包括:电路,所述电路被配置成执行如安全关键性功能等安全关键性功能;故障管理部件,所述故障管理部

件被配置成管理所述电路的故障监测;至少一个用户寄存器,所述至少一个用户寄存器被连接以从所述故障管理部件接收控制信号并且被连接以向所述电路提供寄存器值从而控制所述电路的一方面;模拟测试总线部件,所述模拟测试总线部件被配置成与所述电路中的节点建立连接以将模拟信号传递到所述节点并且与所述故障管理部件就数字信号进行通信;内置自测部件,所述内置自测部件连接到所述电路以测试所述电路并且与所述故障管理部件就数字信号进行通信;安全监测部件,所述安全监测部件连接到所述电路以从所述电路接收信号并且响应于从所述电路接收的所述信号输出安全监测信号;以及门控逻辑,所述门控逻辑被配置成响应于来自所述故障管理部件的信号对来自所述电路和/或来自安全监测器的信号进行门控。另外,所述电路与所述故障管理部件、所述至少一个用户寄存器、所述模拟测试总线部件、所述内置自测部件、安全监测器和所述门控逻辑分离。这种故障监测系统集成在同一IC装置上作为执行安全关键性功能的电路(也被称为"安全关键性电路")的IC装置提供了用于对可以满足ISO 26262要求的安全关键性电路进行故障监测的全面"芯片上"解决方案。例如,集成的故障监测系统使故障能够注入到安全关键性电路中并且使这种故障注入的影响能够被测量和记录。另外,集成的故障监测系统可以支持实现和证明如ISO 26262中规定的足够的多故障诊断覆盖。集成的故障监测系统允许故障在电路操作期间注入到安全关键性电路中并且从一个或多个安全监测器接收反馈,以确定是否检测到对应的故障。集成的故障监测系统不仅可以将灾难性故障注入到安全关键电路,还可以将边缘、参数故障注入到安全关键性电路中。电路与故障监测系统的部件分离,因为电路和故障监测系统的部件有单独的电源线、单独的电源接地线、单独的时钟信号、单独的启用和/或复位信号和/或单独的测试控制信号。因为电路与故障监测系统分离,所以同一故障/缺陷将不会引起电路和假设正在监测电路的状况的监测系统两者的故障。

[0042] 图2描绘了包括安全关键性电路232和故障监测系统240的IC装置230的例子实施例。在图2的实施例中,故障监测系统240包括故障管理部件242、用户寄存器244、模拟测试总线(ATB)部件246、内置自测(BIST)部件248、安全监测器250和门控逻辑252。

[0043] 在一个实施例中,IC装置230的安全关键性电路232可以是在例如汽车中、在医疗装置或航空器中执行安全关键性功能的电路。在汽车中,安全关键性电路可以在例如雷达系统、安全气囊系统、制动系统或引擎控制系统中找到。在医疗装置中,安全关键性电路可以在例如心脏起搏器或如患者监测器等医疗监督电路中找到。在航空器中,安全关键性电路可以在例如雷达系统或引擎控制系统中找到。安全关键性电路可以包括模拟电路、数字电路和/或混合信号电路。在一个实施例中,安全关键性电路是微控制器、智能传感器和/或智能致动器的一部分。在一个实施例中,安全关键性功能是IC装置的功能,所述功能如果执行不当则可能危及个人或财产。

[0044] 在一个实施例中,故障监测系统240的模拟测试总线部件246包括在IC装置230中路由的一对模拟线,具有允许连接到安全关键性电路232的模拟部分中的关键节点的模拟开关。两条线通常用于总线,因为模拟电路常常使用差分信号。在一个实施例中,安全关键性电路中的关键节点可以包括如滤波器、混频器、放大器、限幅器、二倍频器或三倍频器等子电路的输入或输出。模拟测试总线部件可以用于例如将电压或电流注入到安全关键性电路的节点中以便注入故障,从而探测来自所述节点的电压或电流、以便检测故障和/或将节点连接到如电容器或电阻器等内部部件、以便模拟电容器的电容的增大或减小和/或模拟

电阻器的电阻的增大或减小。在一个实施例中,模拟测试总线部件通过来自故障管理部件242的数字信号进行控制,并且包括用于将从故障管理部件接收的数字信号转换为提供到安全关键性电路的模拟信号的数模转换器(DAC)。模拟测试总线部件还可以包括用于将从安全关键性电路接收的模拟信号转换为提供到故障管理部件的数字信号的模数转换器(ADC)。

[0045] 图3描绘了图2中示出的模拟测试总线部件246的例子实施例。如图3所示,模拟测试总线部件346包括双线模拟测试总线(ATB)350、模数转换器(ADC)模块354、锁相环(PLL)模块356和数模转换器(DAC)模块358,所述ADC模块354包括ADC 354A和用于连接到ATB 350的至少一个开关354B,所述PLL模块356包括PLL 356A和用于连接到ATB 350的至少一个开关356B,所述DAC模块358包括DAC 358A和用于连接到ATB 350的至少一个开关358B。模拟测试总线部件可以连接到安全关键性电路中的节点,如电源和接地测试点360、电压参考362和其它模拟电路系统364。在一个实施例中,模拟测试总线部件从故障管理部件(图2,242)接收数字控制信号,并且向故障管理部件提供数字响应信号。从故障管理部件接收的数字控制信号用于控制ADC模块354、PLL模块356和DAC模块358的开关,所述开关可以包括允许在模拟测试总线部件与安全关键性电路中的不同节点之间进行不同连接的数控开关。在一个实施例中,ATB 350连接到在其输入/输出方向上由控制单元371控制的IC焊盘370。在一个实施例中,ATB 350可以由DAC 380控制,这用于测试目的。在一个实施例中,ATB 350可以通过ADC 390观察到,这用于测试目的。虽然图3中示出了模拟测试总线部件的例子,但是模拟测试总线部件的其它实施例是可能的。

[0046] 返回参照图2,在一个实施例中,故障监测系统240的安全监测器250包括用于监测控制安全关键性电路232的一方面的一个或多个信号或状态的监测电路。例如,安全监测器可以包括用于测量例如环形振荡器的温度、电源电压、电源噪声、输出信号电平、输入信号电平和/或频率的电路以测量电路老化的电路。在一个实施例中,安全监测器提供了反映安全关键性电路的一方面的状态数字输出,例如通过/失败或正常/异常。在一个实施例中,IC装置230上可以有多于一个安全监测器。在一个实施例中,安全监测器的安全相关值可以是例如温度、电源电压等的绝对值,但安全相关值也可以是类似值之间的差。例如,如果有相同模块的多个实例,则安全相关值可以是相同模块之间值的差。例如,在汽车雷达IC中,可以有从中可以获得差分值的三个相同的发射器和四个相同的接收器。在类似或相同的模块中,可以这样:温度、信号电平和/或电源电压应当与彼此例如一个接收器模块与任何其它接收器模块仅相差较小百分比。

[0047] 故障监测系统240的BIST部件248包括用于测试IC装置230的安全关键性电路232的电路系统。BIST部件可以被配置成启用在线测试(例如,与正常操作同时或在正常操作期间非同时例如在空闲时间期间)或离线测试(例如,生产测试和/或验证)。在一个实施例中,BIST部件包括用于根据不同缺陷模型注入故障的电路,所述缺陷模型例如硬固定0缺陷(hard stuck-at 0 defect)、硬固定1缺陷、电阻式固定0或1缺陷、两个节点之间的硬桥或电阻桥、使用电容桥接的串扰、使用例如段时间(例如,瞬时)固定缺陷的瞬时故障。与安全监测器250(所述安全监测器250通常提供数字输出,如通过/失败或正常/异常)不同,BIST部件输出安全关键性电路的测量结果,如噪声、灵敏度和串扰的测量结果。因此,BIST部件可以监测可能损害系统安全性的边缘和/或参数偏差,如增加的噪声水平、降低的灵敏度

和/或增加的串扰。

[0048] 故障监测系统240的用户寄存器244是可以被用户设置为一个值以控制安全关键性电路230的各个参数的寄存器。例如,一个或多个寄存器可以通过故障管理部件242设置成影响安全关键性电路中的参数,如例如:模拟电路的偏压电流;模拟时钟信号、模拟/混合信号或数字电路(例如添加时钟抖动、抑制时钟周期或使单个时钟周期加倍);供电电压;电压调节器的参考电压;放大器的增益设置;电压调节器、带隙参考、ADC等的修整值;以及PLL的分频器值。在一个实施例中,用户寄存器中的值可以永久地改变,如以用于硬故障(例如,对由例如短路引起的电路的完全崩溃进行仿真)。在另一个实施例中,可以在较短时间段内改变用户寄存器的值,并且然后将寄存器的值改为其原始值,以对短时或瞬时故障进行仿真。具有暂时改变用户寄存器的值的能力是有益的,因为ISO 26262要求对瞬时故障进行足够的"诊断覆盖"。在另一个实施例中,可以使用经过修改的用户寄存器来注入故障,如由例如将PLL解调谐10%或20%或将参考电压或电流降低或增加10%或20%引起的边缘、参数故障。

[0049] 故障监测系统240的门控逻辑252被配置成对某些信号进行门控以免提供到IC装置230上的其它元件和/或从IC装置提供。在图2的实施例中,门控逻辑252包括用于在故障注入期间对从安全关键性电路生成的功能信号进行门控的门控逻辑254和用于在故障注入期间对来自安全监测器250的信号进行门控的门控逻辑256。在一个实施例中,门控逻辑252由故障管理部件242控制。例如,门控逻辑256可以用于对来自安全监测器250的错误信号进行门控,使得由注入的故障引起的错误不会传播到对安全监测器的错误信号进行评估和处理的电路(例如,片外(off-chip)电路)。在一个实施例中,门控逻辑254在故障注入期间对从安全关键性电路232生成的功能信号进行门控,使得来自安全关键性电路的功能信号不在片外传输,例如在IC装置外。在一个实施例中,故障注入在允许安全关键性电路的操作中断的恰当时间执行。例如,故障注入可以在啁啾脉冲之间支持用于进行驾驶员辅助的雷达功能的安全关键性电路中实施。

[0050] 故障监测系统240的故障管理部件242管理由用户寄存器244、ATB部件246、BIST部件248和安全监测器250执行的故障监测功能。由故障管理部件管理的故障管理功能可以包括例如:触发故障注入电路永久地或短时间内修改一个或多个用户寄存器的再一个设置;检查以查看安全监测器是否在所需时间帧内注意到对应故障;和/或检查以查看BIST部件是否在所需时间帧内注意到对应故障。在一个实施例中,故障管理部件包括被配置成处理数字数据的数字电路系统。故障管理部件可以在启动时、断电时和/或根据要求以例如规则间隔开启故障监测操作。在一个实施例中,故障管理部件被配置成当安全监测器250未检测到对注入的故障的对应响应时发出错误信号。在一个实施例中,重复注入故障并确定是否检测到对应故障的过程,直到注入所需一组故障。故障管理部件还控制门控逻辑252。例如,可以控制门控逻辑对来自安全监测器250的错误信号进行门控,使得由注入的故障引起的错误不会传播到对安全监测器的错误信号进行评估和处理的电路。在一个实施例中,控制门控逻辑在故障注入期间对从安全关键性电路232生成的功能信号进行门控,使得来自安全关键性电路的功能信号不在片外传输,例如在IC装置外。在一个实施例中,故障管理部件包括被配置成实施故障监测逻辑的数字电路系统并且可以包括被配置成执行故障管理功能的计算机可执行代码(例如,软件和/或固件)。

[0051] 在根据本发明的一个实施例中,安全关键性电路232与安全监测系统240的部件之间严格分离。如本文所使用的,安全关键性电路与安全监测系统的部件之间“严格分离”确保了不存在导致安全关键性电路和安全监测系统的部件的故障的缺陷。在一个实施例中,安全关键性电路与安全监测系统的部件之间严格分离涉及电源线、电源接地线、时钟信号、启用或复位信号和测试控制信号分离。在一个实施例中,安全关键性电路与安全监测系统的部件分离,因为存在逻辑分离(例如,安全关键性电路是单独的逻辑实体/模块)。严格分离还可以定义为分层分离和逻辑分离,例如,分层还意味着电路由如示意性网表、定时、布局等视图定义,所述示意性网表、定时、布局分别与于BIST、安全监测器和门控逻辑的视图相比完整地定义了所述电路。在一个实施例中,故障注入部件(例如,用户寄存器244和ATB部件246)和故障检测部件(例如,ATB部件246和安全监测器250)彼此分离。故障注入部件和故障检测部件彼此分离,因为,为了确定诊断覆盖,在故障检测部件中检测到的故障计算在内,而故障注入部件中的故障不计算在内。因此,由于期望将故障检测部件与故障注入部件分离以用于簿记目的,所以有理由分离IC装置中的故障检测部件、故障注入部件。

[0052] 与只需要分离安全关键性电路与安全监测器的常规IC装置相比,在本文所描述的IC装置中,故障注入部件、故障检测/探测部件于安全关键电路之间存在分离。图4描绘了图2的IC装置230,其中指示了安全关键性电路232与安全监测系统的部件分离。具体地说,图4标识了包括安全关键性电路232的安全关键性电路域270和包括故障监测系统的部件的故障监测系统域272,所述部件包括用户寄存器244、模拟测试总线部件246、BIST部件248、安全监测器250、门控逻辑252和故障管理部件242。在一个实施例中,安全关键性电路域270和故障监测系统域272彼此分离,因为例如同一故障(例如,电力损耗)不会投射到安全关键性电路和故障监测系统两者上。另外,尽管未用不同的域示出,但在一个实施例中,用户寄存器244、模拟测试总线部件246、BIST部件248、安全监测器250、门控逻辑252彼此分离。

[0053] 使用如上文所描述的故障监测系统240,可以实施各个故障监测操作以监测安全关键性电路232的一个或多个方面。下文提供了使用上述系统实施故障监测的各个方面。

[0054] 在一个例子中,故障注入由故障管理部件242通过用户寄存器244触发。例如,用户寄存器用于直接控制模拟或混合信号块的性质和/或参数。例如,可以通过用户寄存器操作如限幅器电路和/或接收信号强度指示器(RSSI)电路的参考电压、偏压电流、滤波器特性、电源电压、上限或下限等参数。在一个实施例中,故障管理部件向用户寄存器提供数字控制信号,以设置用户寄存器中的一个或多个值,从而触发故障条件注入到安全关键性电路中。

[0055] 在一个例子中,故障注入由故障管理部件242通过模拟测试总线部件246触发。例如,模拟测试总线部件可以由故障管理部件控制,以操纵安全关键性电路中的参数,如通过增大或减小参考电压、增大或减小偏压电流、修改一个或多个电阻器的值和/或修改一个或多个电容器的值。

[0056] 在一个实施例中,故障监测系统240可以注入本质上“永久”的故障,例如故障的状态或条件在相关时间段内不会改变。永久性故障的例子包括硬固定0、硬固定1、电阻式固定0或电阻式固定1、两个节点之间的硬桥或电阻桥、参考电压或偏压电流的较小参数偏差。当实际IC装置上的非预期粒子提供了在两个节点之间具有或多或少高电阻的传导路径时,IC装置中可能发生如这些故障等故障。

[0057] 在一个实施例中,故障监测系统240可以注入本质上“瞬时”的故障,例如故障的状

态或条件随时间改变或持续仅相对较短时间段,例如比时钟周期更短的时间段。例如,在数字电路中,瞬时故障可以涉及交换触发器的内容或者交换例如SRAM、DRAM或MRAM的存储器单元的内容。在模拟电路中,瞬时故障可以涉及注入可以触发安全监测器或者可以使自动增益控制(AGC)电路改变放大率(例如,由于因瞬时故障引起的突然增大的信号幅度而降低放大率)的高短信号尖峰。在混合信号电路中,注入的瞬时故障可能在临时解锁(PLL)和/或在选择错误信道(例如经由多路复用器)时导致位错误(例如,在ADC和/或DAC中)。因此,瞬时故障的影响可以在瞬时故障结束后很快结束,或者瞬时故障可以持续更长的时间,在许多情况下如经过交换的触发器、锁存器或存储器单元,瞬时故障可以持续未定义的时间段。当由宇宙辐射引起的单事件翻转导致在实际IC装置的硅的较小区域内临时生成电子-空穴对时,IC装置中可能发生如这些故障等故障。电子-空穴对可以在IC装置的较小零件中形成导电通道。

[0058] 在一个实施例中,故障监测系统240可以在安全关键性电路232“在线”的同时注入故障。在线故障注入是指在安全关键性电路操作期间注入故障,例如,当安全关键性电路和关联部件按其预期用途例如在应用模式下操作时。例如,于在线故障注入期间,安全关键性电路处于其预期操作模式下,包括其中与可以在专用测试模式下使用的可能不现实的水平相比,将如偏压电流、参考电压、滤波器设置、增益设置等操作设置设置在现实水平。此外,与可以在专用测试模式下注入的信号相比,注入到安全关键性电路中的外部信号是现实信号,在所述专用测试模式下,可能根本没有输入信号。在一个实施例中,在线故障注入还包括在输出信号可能扰乱后续电路系统的情况下对安全监测器的输出进行门控和对来自安全关键性电路的输出信号进行门控。

[0059] 在一个实施例中,故障监测系统240可以在安全关键性电路232“离线”的同时注入故障。离线故障注入是指在例如专用测试模式下注入故障,所述注入在应用模式下可以在电路启动时、电路断电时或间歇性地进行。可能需要实施离线故障注入,因为可能不需要将来自安全监测器的信号和/或来自安全关键性电路的输出信号门控断开(gate off)和/或因为有可能注入特别选定的故障和/或操纵在安全关键性电路的在线操作期间不应当操纵的某些参数。例如,可以选择如偏压电流设置、参考电压设置、增益设置和/或滤波器设置等参数来反映安全关键性电路最容易有注入缺陷的最坏情况条件。在一些实施例中,可能发现不同组设置是不同故障模式的最坏情况设置,例如,一组设置对于固定0故障而言是最坏情况,而另一组设置对于固定1故障而言最坏情况,并且第三组设置对于瞬时故障而言是最坏情况。

[0060] 在一个实施例中,故障监测系统240可以通过故障监测系统的部件将参数故障、边缘故障和/或瞬时故障注入到安全关键性电路232中。参数故障、边缘故障和/或瞬时故障的例子包括如电阻器、电容器或晶体管等单个部件或者如电流镜或单个放大级等子模块或者如滤波器、ADC、DAC、PLL等完整模块的电路参数的变化,所述电路参数如电阻、电容、电感、电压、电流、放大率、滤波器角频率、延迟时间、串扰衰减、电源抑制比、共模抑制比和类似的特性值。

[0061] 图5是用于监测IC装置中的故障的方法的过程流程图。在框502处,在IC装置的故障管理部件处,控制故障通过IC装置的用户寄存器、通过IC装置的模拟测试总线部件并且通过IC装置的内置自测部件注入到IC装置的电路中。在框504处,在IC装置的故障管理部件

处,接收与注入的故障有关的输出。

[0062] 在以上描述中,提供了各个实施例的具体细节。然而,一些实施例可以在少于全部这些具体细节的情况下实践。在其它实例中,为简洁和清晰起见,对某些方法、程序、部件、结构和/或功能的描述不如用于实现本发明的各个实施例时详细。

[0063] 尽管以特定的顺序示出和描述了本文中的一种和多种方法的操作,但是可以改变每种方法的操作的顺序,使得某些操作可以按相反顺序执行,或者使得某些操作可以至少部分地与其它操作同时执行。在另一个实施例中,不同操作的指令或子操作可以通过间歇和/或交替的方式实施。

[0064] 还应注意,本文所描述的方法的操作中的至少一些操作可以使用存储在计算机可用存储媒体上以供计算机执行的软件指令实施。举例来说,计算机程序产品的实施例包括用于存储计算机可读程序的计算机可用存储媒体。

[0065] 计算机可用或计算机可读存储媒体可以是电子、磁性、光学、电磁、红外或半导体系统(或者设备或装置)。非暂时性计算机可用和计算机可读存储媒体的例子包括半导体或固态存储器、磁带、可移除计算机磁盘、随机存取存储器(RAM)、只读存储器(ROM)、刚性磁盘和光盘。光盘的当前例子包括压缩盘只读存储器(CD-ROM)、压缩盘读/写(CD-R/W)和数字视频盘(DVD)。

[0066] 可替代地,本发明的实施例可以完全以软件或以包含硬件元件和软件元件两者的实施方案实施。在使用软件的实施例中,软件可以包含但不限于固件、驻留软件、微代码等。

[0067] 尽管已经描述和示出了本发明的具体实施例,但是本发明不应限于如此描述和示出的零件的具体形式或布置。本发明的范围应由在此所附权利要求书及其等同物限定。

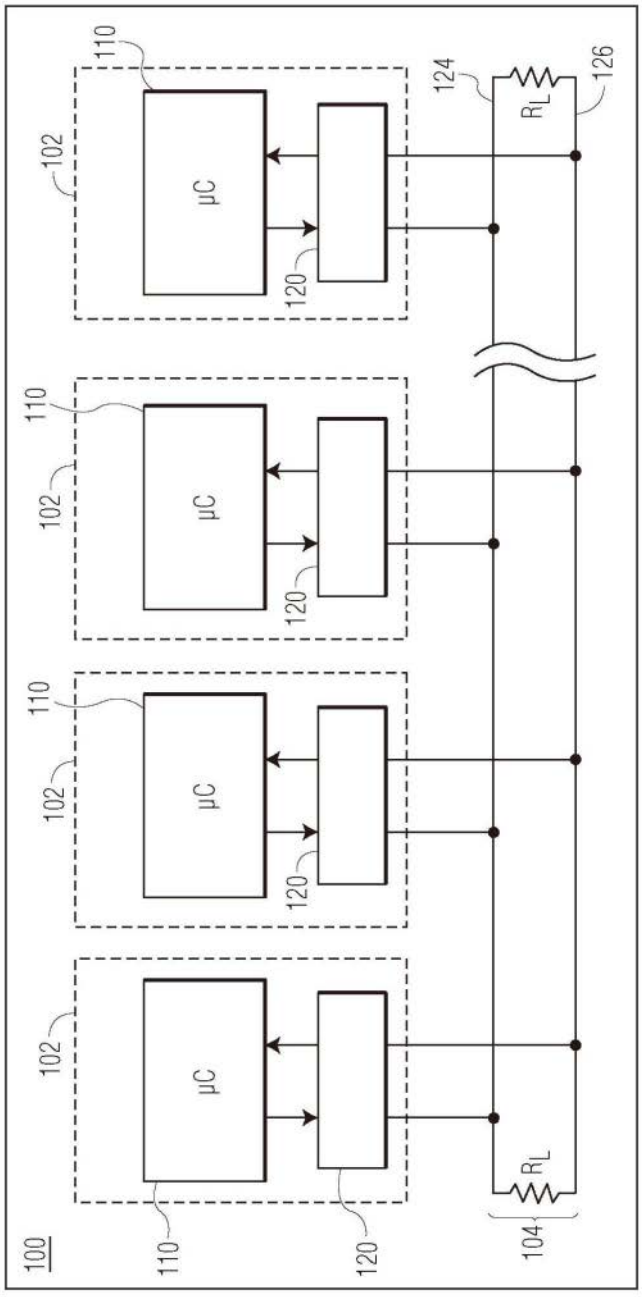


图1

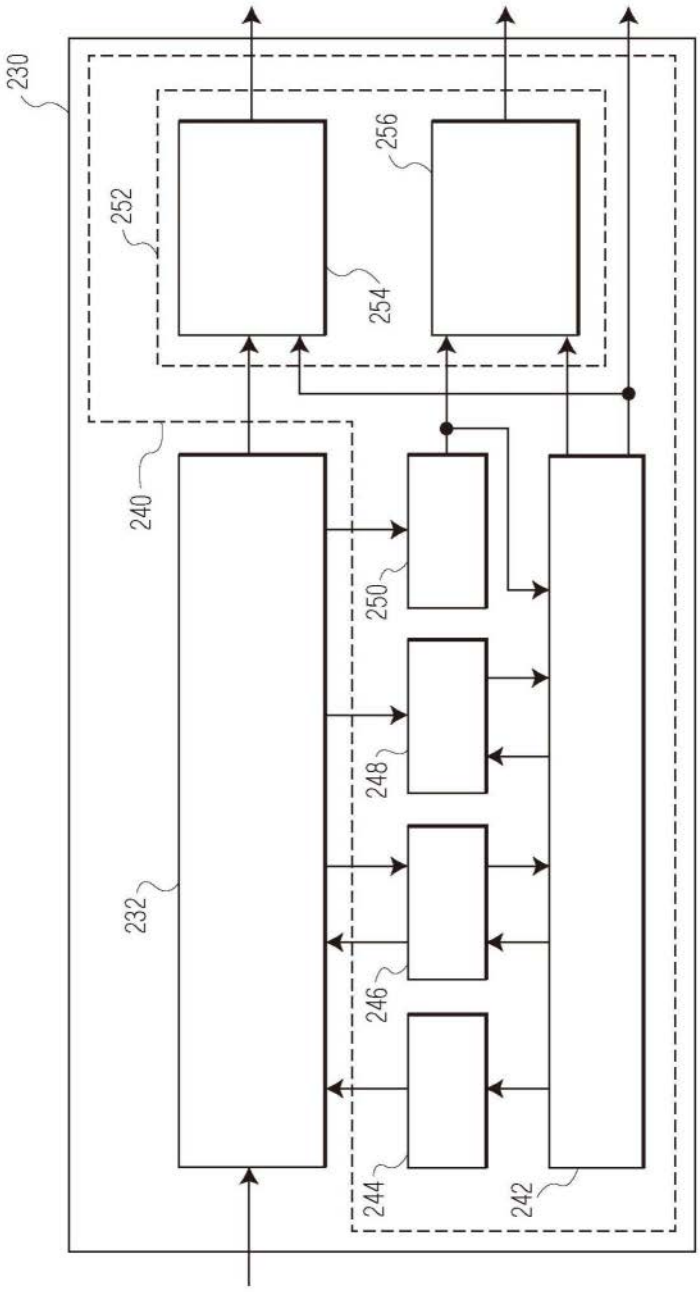


图2

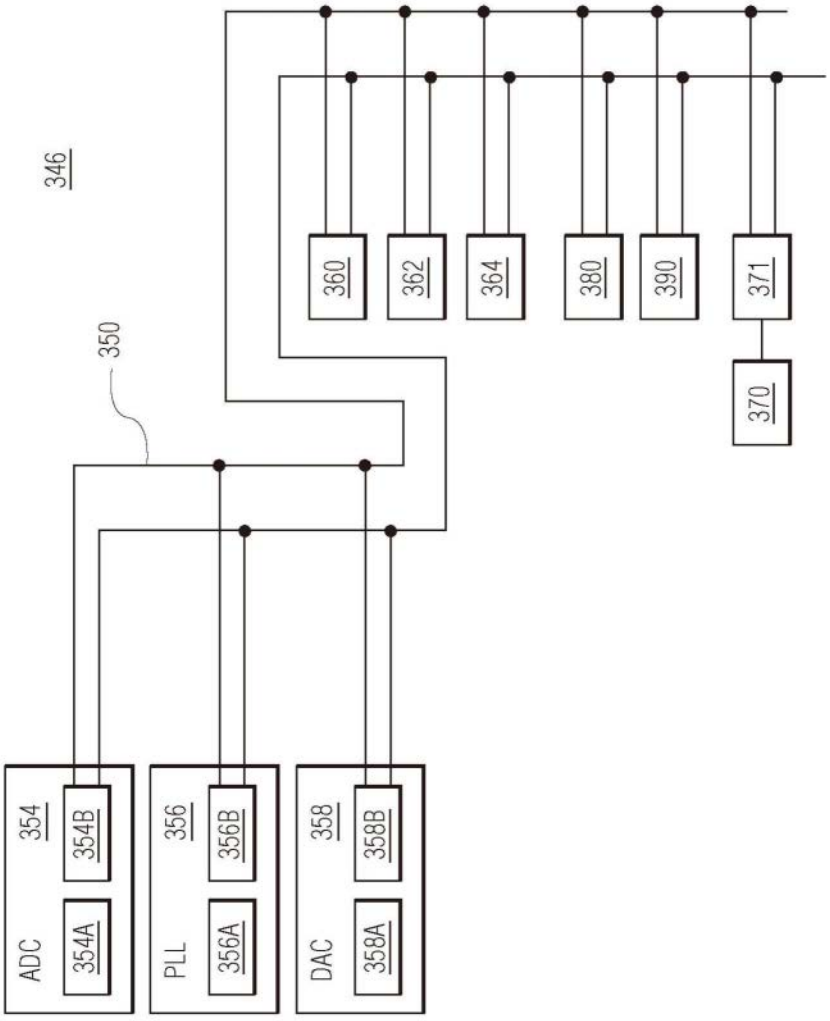

346
350
360
362
364
380
390
371
370
ADC
354
354B
354A
PLL
356
356B
356A
DAC
358
358B
358A

图3

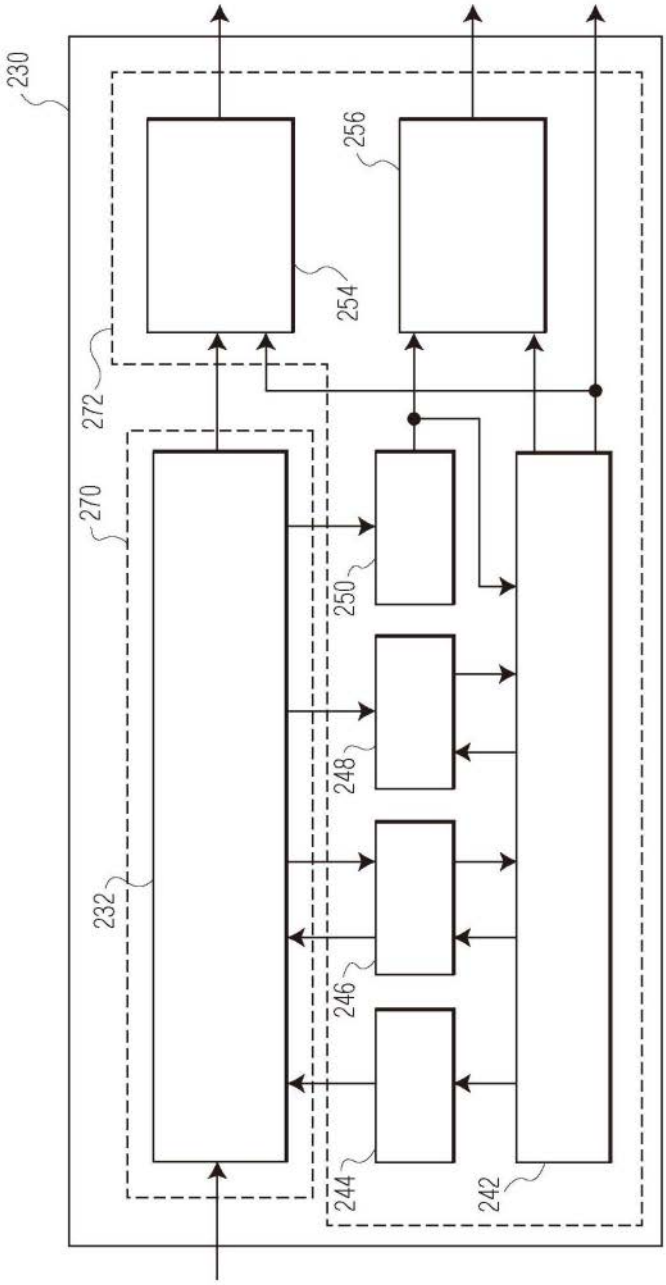


图4

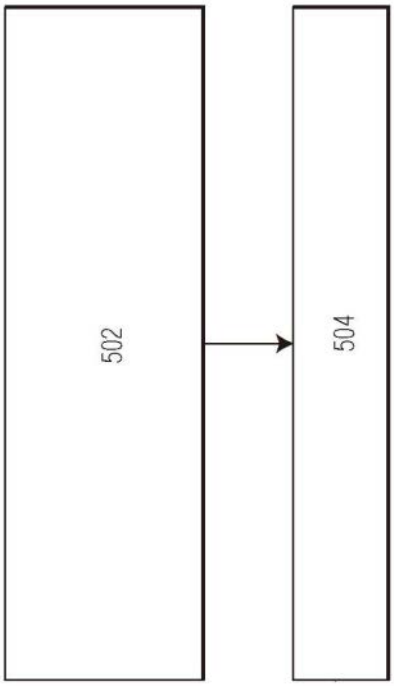


图5