



(12)发明专利申请

(10)申请公布号 CN 106355096 A

(43)申请公布日 2017.01.25

(21)申请号 201610556888.6

(22)申请日 2016.07.14

(30)优先权数据

14/799,341 2015.07.14 US

(71)申请人 德州仪器公司

地址 美国德克萨斯州

(72)发明人 埃尔坎·比尔汗

拉吉塔·帕达坎蒂

阿姆里特帕尔·辛格·蒙德拉

(74)专利代理机构 北京律盟知识产权代理有限

责任公司 11287

代理人 林斯凯

(51)Int.Cl.

G06F 21/57(2013.01)

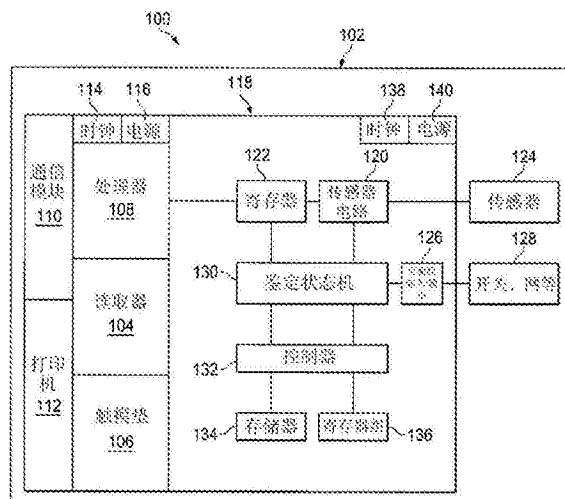
权利要求书2页 说明书5页 附图3页

(54)发明名称

篡改检测

(57)摘要

本申请案涉及篡改检测。一种金融交易系统(100)包含传感器(124)、篡改检测模块(118)及电路(122)，所述电路(122)可配置以控制哪些传感器被使用，且所述电路(122)可在所述篡改检测模块已制造出之后配置。



1. 一种金融交易系统,其包括:

多个传感器;

篡改检测模块,其包括:

第一电路,其耦合到所述传感器,可配置以控制哪些传感器被使用;且其中所述第一电路可在所述篡改检测模块已制造出之后配置。

2. 根据权利要求1所述的金融交易系统,其进一步包括:

处理器,其耦合到所述第一电路;

其中所述第一电路包括可由所述处理器写入的寄存器。

3. 根据权利要求1所述的金融交易系统,其中所述传感器中的至少一者包括温度传感器。

4. 根据权利要求1所述的金融交易系统,其中所述传感器中的至少一者包括频率传感器。

5. 根据权利要求1所述的金融交易系统,所述篡改检测模块进一步包括:

可编程输入/输出端口;

其中所述可编程输入/输出端口可在所述篡改检测模块已制造出之后配置。

6. 根据权利要求5所述的金融交易系统,其中所述可编程输入/输出端口可被配置为开关状态监测器。

7. 根据权利要求5所述的金融交易系统,其中所述可编程输入/输出端口可被配置为用于金属丝网的驱动器/接收器对。

8. 根据权利要求5所述的金融交易系统,其中所述可编程输入/输出端口可经配置以从所述篡改检测模块外部的硬件接收系统状态信息。

9. 根据权利要求5所述的金融交易系统,其进一步包括:

第二电路,其经配置以接收来自所述第一电路的响应及来自所述可编程输入/输出端口的响应且产生触发信号;且

其中用于产生触发信号的准则可在所述篡改检测模块已制造出之后配置。

10. 根据权利要求9所述的金融交易系统,其中所述第二电路包括状态机。

11. 根据权利要求9所述的金融交易系统,其中所述第二电路可配置以在由传感器检测到的故障的数目超过可配置阈值计数时产生篡改触发信号。

12. 根据权利要求9所述的金融交易系统,其中所述第二电路可配置以在由传感器检测到的故障的数目在可配置时间窗内超过可配置阈值计数时产生篡改触发信号。

13. 根据权利要求9所述的金融交易系统,其中所述第二电路可配置以在所监测温度处于可配置范围之外时产生篡改触发信号。

14. 根据权利要求9所述的金融交易系统,其中所述第二电路可配置以在所监测时钟频率超过可配置阈值时产生篡改触发信号。

15. 根据权利要求9所述的金融交易系统,其中所述第二电路可配置以在两个所监测频率之间的差超过可配置阈值时产生篡改触发信号。

16. 根据权利要求9所述的金融交易系统,其进一步包括:

第三电路,其经配置以从所述第二电路接收触发信号并调用对所述篡改触发信号的系统响应;且

其中对所述篡改触发信号的所述响应可在所述篡改检测模块已制造出之后配置。

17. 根据权利要求16所述的金融交易系统，其中对篡改触发信号的可配置响应是擦除存储器。

18. 一种用于配置金融交易系统的方法，其包括：

由处理器将控制信息写入到篡改检测模块中耦合到传感器的寄存器，其中所述寄存器确定哪些传感器是作用的。

19. 根据权利要求18所述的方法，其进一步包括：

由所述处理器将控制信息写入到耦合到鉴定状态机的寄存器，其中所述寄存器确定用于由所述鉴定状态机产生篡改触发信号的条件。

20. 一种篡改检测模块，其包括：

多个传感器；

传感器电路，其耦合到所述传感器；

处理器；及

第一电路，其耦合到所述处理器及所述传感器电路，包括可由所述处理器写入的寄存器，所述第一电路可由所述寄存器配置以控制哪些传感器被使用。

篡改检测

技术领域

[0001] 本申请案涉及一种篡改检测，且特定来说，涉及一种篡改检测设备及方法。

背景技术

[0002] 金融交易的安全是持续关注点。举例来说，一个世界性的问题是信用卡诈骗，其会导致金钱损失及身份盗用。一个特定的关注点是存取、处理及存储与金融交易有关的敏感数据的交互点(POI)处的安全，所述交互点(POI)例如是销售点终端或智能仪表系统。POI可有人照管(举例来说，在零售商店内部)或无人照管(举例来说，汽车燃料施配器、自动贩卖机、停车计时器及自动取款机)。一些POI从卡上的磁条读取信息并另外需要签名。一些POI从嵌入于卡中的电子电路读取信息并另外需要对个人识别号(PIN)的输入。一些POI从附近的手机或其它电子装置读取信息。POI易受到多种欺诈行为的攻击，举例来说，被添加用以读取卡的外部硬件(盗读(skimming))、被添加用以拦截或监测交易的内部电子器件、或盗窃并拆解装置且接着读取存储在存储器中的敏感数据。

[0003] 金融支付行业已为POI的制造商实施了多种标准。在美国，支付卡行业(PCI)已开发出数据安全标准(DSS)。在欧洲，一些支付行业公司(Europay、MasterCard及Visa(EMV))已针对使用嵌入式电子芯片的卡开发出一组单独的标准。对于PIN交易安全(PTS)，PCI具有一组单独的标准。对POI系统的一个实例性安全要求是篡改检测并在检测到篡改后使系统立即不能操作。另外，POI系统需要在检测到篡改后即刻擦除任何敏感数据。所述标准确立了若干目标，但其并未详细地指定必须如何满足所述目标。而是，支付行业对POI系统制造商给出了进行构建及测试所依据的安全准则，且POI系统制造商在实施符合所述安全准则的POI时仍具有某一设计自由度。

发明内容

[0004] 在一个实施例中，揭示一种金融交易系统。所述金融交易系统包括：多个传感器；篡改检测模块，其包括：第一电路，其耦合到所述传感器，可配置以控制哪些传感器被使用；且其中所述第一电路可在所述篡改检测模块已制造出之后配置。

[0005] 在一个实施例中，揭示一种用于配置金融交易系统的方法。所述方法包括：由处理器将控制信息写入到篡改检测模块中耦合到传感器的寄存器，其中所述寄存器确定哪些传感器是作用的。

[0006] 在另一实施例中，揭示一种篡改检测模块。所述篡改检测模块包括：多个传感器；传感器电路，其耦合到所述传感器；处理器；及第一电路，其耦合到所述处理器及所述传感器电路，包括可由所述处理器写入的寄存器，所述第一电路可由所述寄存器配置以控制哪些传感器被使用。

附图说明

[0007] 图1是POI系统的实例性实施例的框图示意图。

- [0008] 图2A是用于监测壳体完整性的实例性电路的示意图。
- [0009] 图2B是壳体的实例性实施例的一部分的横截面,其图解说明图2A中所图解说明的开关的实例性实施例。
- [0010] 图3A是用于监测壳体完整性的另一实例性电路的框图示意图。
- [0011] 图3B是图3A中所图解说明的金属丝网的实例性实施例的一部分的额外细节的平面图。
- [0012] 图4是用于检测篡改的方法的实例性实施例的流程图。

具体实施方式

[0013] 在以下说明中,POI系统包含篡改检测模块。如果篡改检测模块检测到篡改,那么所述篡改检测模块经配置以立即擦除存储器,甚至在POI系统的其余部分不能使用或被破坏的情况下也如此。所述篡改检测模块是现场可配置的。也就是说,POI系统的制造商可编程监测哪些条件、用于确定是否应起始篡改触发信号的准则及由篡改触发信号引起的行为。

[0014] 以下是篡改检测模块的属性的实例性列表:

- [0015] 自含式电源(电池)及时钟。
- [0016] 壳体完整性监测。
- [0017] 温度监测。
- [0018] 系统时钟监测。
- [0019] 传感器的可编程启用。
- [0020] 用于确定篡改的可编程准则。
- [0021] 用于向外部指示篡改的可编程输入/输出(I/O)。
- [0022] 修改存储器中的数据以防止对静态存储器的压印。
- [0023] 在检测到篡改时立即进行系统关闭及存储器擦除。
- [0024] 不可擦除的篡改记录存储器。

[0025] 图1图解说明实例性POI系统100。POI系统100至少部分地被容纳于壳体102内。读取器104从卡上的磁条或从卡上的电子电路或从被紧密接近读取器104保持的电子装置(举例来说,手机)无线地读取金融账户信息。触摸垫106接收被手动输入的信息,例如PIN或电话号码。或者,可获取其它个人标识,举例来说,生物识别数据,例如指纹扫描、面部辨识、视网膜扫描等。处理器108控制POI系统100。通信模块110向POI系统100外部发送及从POI系统100外部接收信息。举例来说,通信模块110可向支付公司发送帐户ID及交易金额并接收交易批准。举例来说,通信模块110可使用电话陆线或者有线或无线网络。打印机112打印收据。如果POI 100是自动取款机,那么将存在现金施配器(未展示)。POI 100包含至少一个主系统时钟114及至少一个主系统电源116。图1中的POI系统100仅是用于图解说明及论述的实例。在一些实施例中,一些逻辑分区/块/模块可被集成为较大功能单元的一部分,一些功能单元可在物理上分离,一些功能单元可不被包含,可存在未图解说明的额外功能单元,且划分形式可能不同于所图解说明的形式。

[0026] 图1中所图解说明的实例性POI系统100还包含篡改检测模块118。篡改检测模块118包括由配置寄存器122启用的多个传感器电路120。传感器电路120耦合到各种传感器

124。如下文将更详细地论述,传感器124监测温度、时钟频率、电源电压及其它操作条件。篡改检测模块118还包含可编程输入/输出(PIO)126。如下文将更详细地论述,PIO 126耦合到各种开关及金属丝网或用于监测壳体的状态及物理完整性以及其它系统工作状态信息(举例来说,硬件自测试)的其它装置。传感器电路120及PIO 126的输出通过个别可编程的鉴定状态机(QSM)130来处理。当满足某些条件时,QSM 130会产生触发信号,且所述触发信号用于起始例如系统复位、存储器擦除等可编程行动。篡改检测模块118还包含控制器132、存储器134及寄存器组136。篡改检测模块118还包含内部时钟138,内部时钟138用于监测主系统时钟114,且在主系统时钟114出故障或不能使用的情况下还由篡改检测模块118用作备用时钟。篡改检测模块118还包含带备用电池的电源140,使得其可在POI系统100的主系统电源116出故障或不能使用的情况下继续操作。POI系统100将经加密的敏感数据存储在存储器134中及寄存器组136中。篡改检测模块118经配置以在某些条件被满足时擦除存储器134及/或寄存器组136。

[0027] 传感器124可为壳体102内的单独装置,或者可为POI系统100的功能部件的一部分(举例来说,主系统时钟114的一部分或系统电源116的一部分)。举例来说,一或多个温度传感器可监测壳体102内的温度,其它温度传感器可监测处理器108的温度,频率传感器可监测主系统时钟114的频率,且电压传感器可监测来自系统电源116的电压。

[0028] PIO 126可例如被配置为开关状态检测器、金属丝网对(驱动器/接收器)或用以接收自测试信息的电路。PIO 126可经配置以监测常开开关或常闭开关。其可被配置为驱动器或接收器,且经配置以用三态输出进行驱动、提供输入上拉等。

[0029] 篡改检测模块118可由POI系统100的制造商配置。举例来说,配置寄存器122可由POI系统100的制造商编程以确定哪些传感器124被使用。优选地,配置寄存器122被加以存储器映射且可由处理器108直接存取。另外,QSM 130可由POI系统100的制造商编程以确定某些条件何时被满足而产生触发信号。另外,由触发信号引起的内部行动(例如对系统的全部或一部分进行复位或擦除存储器)是可编程的。另外,POI系统100的未处于篡改检测模块118内的部分可包含单独的传感器、测试电路或篡改检测电路,且来自那些外部传感器及电路的信息可被发送到篡改检测模块118(经由可编程PIO 126)以起始适当行动。

[0030] 如上文所论述,QSM 130可由POI系统100的制造商配置以确定某些条件何时被满足而产生触发信号。可编程条件的一个实例性目的是防止误触发信号。QSM 130的可配置参数是通过配置寄存器122来控制。在一个实例性实施例中,由传感器电路120及PIO 126周期性地对条件进行取样。QSM 130可经配置以需要检测到多个故障后才产生触发信号。举例来说,QSM 130可经配置以在两个模式中的一者中操作。第一实例性模式是其中在故障的数目超过可编程阈值计数时产生篡改触发信号的阈值计数模式。第二实例性模式将可编程计时器与可编程阈值相组合。在第二模式中,在可编程时间窗内对故障进行计数,且当故障的数目在所述时间窗内超过可编程阈值时,产生篡改触发信号。下文更详细地论述关于温度感测及时钟频率感测的额外实例性QSM鉴定。

[0031] 监测壳体及物理完整性的一个实例是监测弹簧负载式开关的状态,所述弹簧负载式开关可通过松动螺丝或拆卸其它类型的紧固件而被激活。另一实例是检测放置在壳体内部或敏感硬件周围的一个或多个金属丝网的连续性。

[0032] 图2A是用以指示壳体完整性的实例性电路200的示意图。开关204耦合到NAND门

208的第一输入。上拉电阻器206将NAND门208的第一输入保持为高,直到开关204将NAND门208的第一输入拉到接地。NAND门208的第二输入是ENABLE信号。开关204是图1中的开关128的实例。NAND门208是图1中的PIO 126的实例。ENABLE信号是来自配置寄存器122(图1)的用以配置哪些开关128及哪些传感器电路120作用的信号的实例。NAND门208及上拉电阻器206是PIO 126的可配置性的实例。如上文所论述,PIO 126可被配置为驱动器或接收器,且经配置以用三态输出进行驱动、提供输入上拉等。

[0033] 图2B图解说明POI壳体102的实例的一部分的剖视图。在图2的实例中,壳体102的外部部分210可使用螺丝214被紧固到内部分212。在其它实施例中,可使用其它紧固形式(举例来说,铆钉、夹具、粘合剂等)。当壳体外部部分210接近壳体内部分212而定位时,被附接到外部部分210的突片216会激活内部分212上的开关218。开关218是图2A中的开关204的实例。在POI系统100内壳体的一部分可被移除的任何位置处可定位有多个开关。在一个实例性实施例中,开关218是弹簧负载式开关,其在柔性表面形成圆顶状从而指示突片216不再压靠所述表面时断开。

[0034] 图3A是用以监测壳体完整性的另一实例性电路300的示意图。驱动器302由伪随机信号驱动。驱动器302驱动金属丝网304的一端,金属丝网304是被制作成蜿蜒状区域填充图案的连续导体(图3B中所图解说明)。金属丝网304的第二端耦合到接收器306。如果侵入者将要钻通、切割或以其它方式割断导体网304,那么篡改检测模块118中的所连接PIO 126将检测到此破坏。所述伪随机信号通过向外部产生信号而确保侵入者无法轻易地绕过所述网。驱动器302及接收器306是PIO 126的可配置性的实例。如上文所论述,PIO 126可被配置为驱动器或接收器,且经配置以用三态输出进行驱动、提供输入上拉等。

[0035] 图3B图解说明图3A的金属丝网304的一部分的额外细节。如所图解说明,导体308被制作成区域填充蜿蜒状图案。金属丝网304可被制作于印刷电路板上或制作于柔性衬底上。所述区域填充蜿蜒状图案使得侵入者难以找到钻通或切通所述网的安全位置。

[0036] 传感器124内可存在用于监测POI系统100中的多个位置处的温度的多个温度传感器。超出所指定温度范围而操作可指示处理器108即将要出故障且可需要关闭POI系统100。或者,远超出所指定温度范围而操作可指示在存储器可被擦除之前使POI系统100不能使用或受破坏的恶意企图。

[0037] 用于监测温度的实例性可配置QSM 130具有可编程最小温度、可编程最大温度及两个可编程百分比。如果所监测温度处于所编程最小温度或最大温度的第一百分比内,那么QSM 130产生警告信号以给出POI系统100采取行动的机会,例如通过接通加热或冷却。如果所监测温度比所编程最小温度高出第二百分比或比所编程最大温度高出第二百分比,那么QSM 130产生触发信号以起始较高级响应,例如系统关闭。

[0038] POI系统100可具有多个主系统时钟114、多个篡改检测模块内部时钟138,且传感器124内可存在用于监测时钟频率的多个传感器。用于时钟频率监测的一个实例性传感器124包括两个计数器。一个计数器对来自主系统时钟114的时钟循环进行计数,且第二计数器对来自篡改检测模块118中的篡改检测内部时钟138的时钟循环进行计数。将两个计数进行比较会实现检测主系统时钟114是否处于所指定范围内。时钟频率失败事件由QSM 130处理以确定是否将产生篡改触发信号。作为实例,如果两个连续频率样本指示超出范围的系统时钟,那么QSM 130可产生篡改触发信号。在时钟频率篡改触发信号的情况下,篡改检测

模块118切换到其内部时钟138。

[0039] 一种恶意攻击方法是用极高频率的电磁性刺激干扰电子器件以企图在存储器可被擦除之前使系统不能使用。用于时钟频率监测的传感器124的第二实例包括高速延迟线。所述延迟线在时钟的一个边缘处被触发。如果时钟的下一边缘在延迟线的输出之前出现，那么所述延迟线会产生指示所述时钟太快的篡改触发信号。第二实例性时钟频率传感器比第一实例性时钟频率传感器快，但第二实例性传感器无法检测到低频率故障。

[0040] 篡改检测模块118包含寄存器组136，以用于存储执行交易所需的关键安全数据。寄存器组136被划分成两个区段：用于存储数据的一个区段及用于存储加扰密钥的第二区段。加扰是可经由PIO 126启用的选项。当加扰被启用时，使用“异或”电路将来自处理器108的数据与加扰密钥进行逻辑组合，然后写入到寄存器组136中。对于一些存储器技术，静态存储器状态可被压印(经由氧化物聚集、对电荷或磁场的不完整擦除等)，使得在擦除之后有时可识别出静态值。为防止静态压印，寄存器组136中的数据被周期性地反转。反转过程对于处理器108来说是透明的(硬件将始终返回正确值)。

[0041] 存储器134被划分成两个区段，其中的一个区段用于存储在篡改事件的情况下被擦除的经加密敏感数据，且第二不可擦除区段用于存储篡改记录及在篡改事件之后用于分析的其它调试信息。篡改记录指示传感器124的输出恰在触发信号之前的最后状态。

[0042] 对触发信号的响应可经由到控制器132的输入来配置。响应可选自可能响应列表的任一组合。实例性可能响应列表包含接通加热或冷却、向处理器108发布中断、重新启动POI系统100、快速(2到3个时钟循环)擦除寄存器组136(包含加扰密钥寄存器)、擦除存储器134、关闭POI系统100等。特定来说，一些篡改触发信号不需要引起对存储器134的擦除。举例来说，如果篡改检测模块118感测到带有备用电池的电源140已出故障，那么可产生引起对寄存器组136的擦除的复位，但存储器134可不被擦除。如果自测试(举例来说，处理器108的边界扫描测试)指示硬件故障，那么系统可被重新启动。

[0043] 篡改检测模块118内的带有备用电池的电源140通常由POI系统100从外部供电，但电源140可在外部电力丢失时回复到内部电池。

[0044] 图4是图解说明用于配置金融交易系统的实例性方法400的流程图。在步骤402处，处理器将控制信息写入到篡改检测模块中耦合到传感器的寄存器，其中所述寄存器确定哪些传感器是作用的。

[0045] 尽管已在本文中详细描述了本发明的说明性及当前优选实施例，但应理解，可以其它方式不同地体现及采用发明性概念，且所附权利要求书打算理解为包含此些变化形式，受现有技术限制的除外。

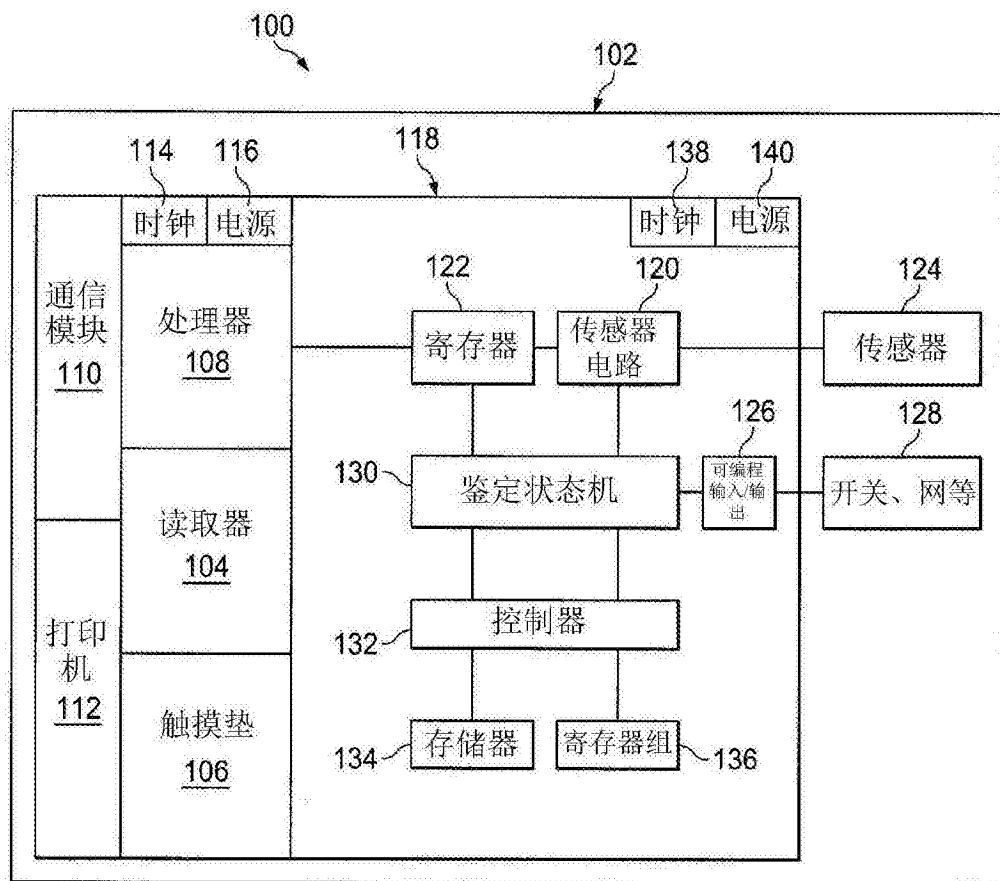


图1

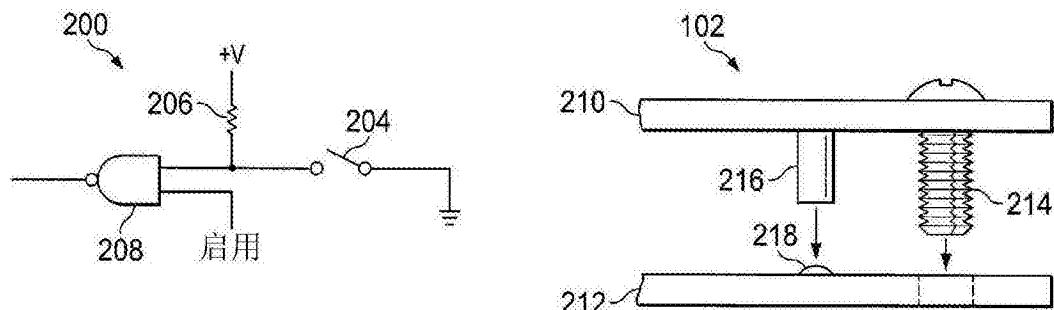


图2A

图2B

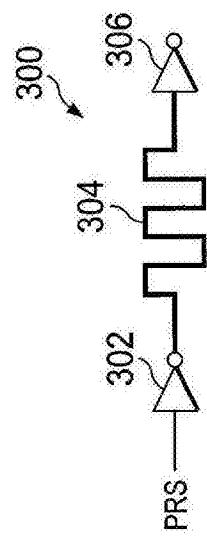


图3A

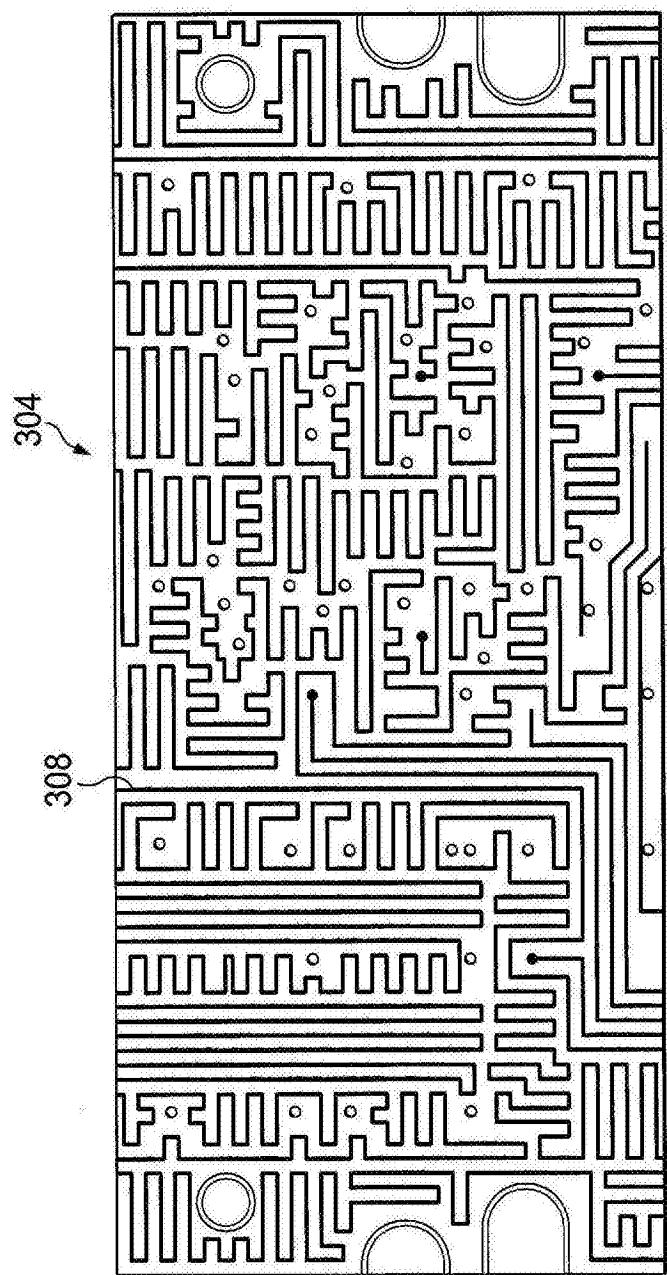


图3B



图4