(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 106918773 B
(45)授权公告日 2019.07.05

(21)申请号 201710116996.6

(22)申请日 2017.03.01

(65)同一申请的已公布的文献号
申请公布号 CN 106918773 A

(43)申请公布日 2017.07.04

(73)专利权人 中国电子产品可靠性与环境试验研究所
地址 510610 广东省广州市天河区东莞庄路110号

(72)发明人 王力纬 池源 恩云飞 侯波 何春华

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 黄晓庆

(51)Int.Cl.
G01R 31/28(2006.01)
G06F 21/76(2013.01)

(56)对比文件
CN 104239616 A,2014.12.24,
CN 105158674 A,2015.12.16,
CN 101464921 A,2009.06.24,
CN 104950248 A,2015.09.30,
CN 104636686 A,2015.05.20,
CN 104849648 A,2015.08.19,
WO 2016080380 A1,2016.05.26,

审查员 薛园兵

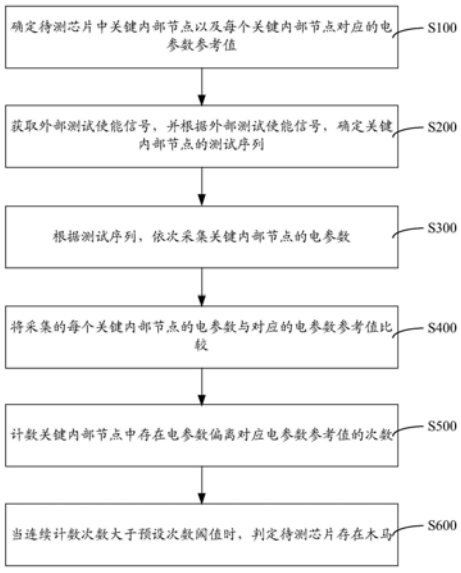
权利要求书2页 说明书5页 附图3页

(54)发明名称

工艺型硬件木马监测方法与装置

(57)摘要

本发明提供一种工艺型硬件木马监测方法与装置，确定待测芯片中关键内部节点以及每个关键内部节点对应的电参数参考值，根据外部测试使能信号，确定关键内部节点的测试序列，依次采集关键内部节点的电参数，将采集的电参数与对应的电参数参考值比较，计数关键内部节点中存在电参数偏离对应电参数参考值的次数，当连续计数次数大于阈值时判定待测芯片存在木马。整个过程中，一方面对关键内部节点进行定时监测，另一方面将采集到的电参数与对应的电参数参考值比较，充分考虑了工艺扰动的影响，能够高效且准确对工艺型硬件木马进行监测。



CN 106918773 B

1.一种工艺型硬件木马监测方法,其特征在于,包括步骤:

确定待测芯片中关键内部节点以及每个所述关键内部节点对应的电参数参考值;

获取外部测试使能信号,并根据所述外部测试使能信号,确定所述关键内部节点的测试序列;

根据所述测试序列,依次采集所述关键内部节点的电参数;

将采集的每个所述关键内部节点的电参数与对应的电参数参考值比较;

计数所述关键内部节点中存在电参数偏离对应电参数参考值的次数;

当连续计数次数大于预设次数阈值时,判定所述待测芯片存在木马;

所述确定待测芯片中关键内部节点包括:

遍历所述待测芯片,查找所述待测芯片中整体功能、性能或可靠性相关的电路节点;

将查找到的电路节点作为所述待测芯片中关键内部节点;

所述确定每个所述关键内部节点对应的电参数参考值的步骤包括:采用蒙特罗仿真算法,确定每个所述关键内部节点对应的电参数参考值;

所述将采集的每个所述关键内部节点的电参数与对应的电参数参考值比较之后还包括:

当所述关键内部节点中存在电参数偏离对应电参数参考值时,控制所述待测芯片重启,并返回所述根据所述测试序列,依次采集所述关键内部节点的电参数的步骤。

2.根据权利要求1所述的工艺型硬件木马监测方法,其特征在于,所述预设次数阈值为3次。

3.一种工艺型硬件木马监测装置,其特征在于,包括依次连接的测试序列生成模块、信号传感模块、测试反馈模块以及木马判定模块,所述信号传感模块与待测芯片中关键内部节点连接,所述测试反馈模块存储有所述待测芯片中关键内部节点对应的电参数参考值,所述待测芯片中关键内部节点是指待测芯片中整体功能、性能或可靠性相关的电路节点,所述关键内部节点对应的电参数参考值是基于蒙特罗仿真算法所确定;

所述测试序列生成模块用于接收外部测试使能信号,并根据所述外部测试使能信号,确定所述关键内部节点的测试序列,所述信号传感模块用于根据所述测试序列,依次采集所述关键内部节点的电参数,所述测试反馈模块用于将采集的每个所述关键内部节点的电参数与对应的电参数参考值比较,所述木马判定模块用于计数所述关键内部节点中存在电参数偏离对应电参数参考值的次数,并当连续计数次数大于预设次数阈值时,判定所述待测芯片存在木马,所述木马判定模块还用于当所述测试反馈模块监测到所述关键内部节点中存在电参数偏离对应电参数参考值时,控制所述待测芯片重启。

4.根据权利要求3所述的工艺型硬件木马监测装置,其特征在于,所述信号传感模块包括相互连接的开关阵列单元和测量单元,所述开关阵列单元与所述测试序列生成模块连接,所述测量单元与所述测试反馈模块连接,所述开关阵列单元还与所述待测芯片中关键内部节点连接;

所述开关阵列单元用于根据所述测试序列,选择接入的所述关键内部节点,所述测量单元用于采集所述接入的关键内部节点的电参数。

5.根据权利要求3所述的工艺型硬件木马监测装置,其特征在于,还包括测试使能信号生成模块,所述测试使能信号生成模块与所述测试序列生成模块连接。

6.根据权利要求5所述的工艺型硬件木马监测装置,其特征在于,所述测试使能信号生成模块包括时钟单元。

工艺型硬件木马监测方法与装置

技术领域

[0001] 本发明涉及木马监测技术领域，特别是涉及工艺型硬件木马监测方法与装置。

背景技术

[0002] 近年来，集成电路的安全性受到了人们越来越多的关注。由于成本的原因，目前绝大多数的集成电路设计公司都没有自己的制造工艺线，而是依赖于专业的芯片制造代工厂来进行芯片的生产。这种设计和生产相分离的情况，给集成电路的安全带来了隐患——硬件木马，它指的是对手在集成电路的设计或制造过程中，往芯片中加入的一些恶意电路逻辑，它将导致芯片在使用过程中出现一系列不受使用方控制的安全问题。

[0003] 目前通常采用基于旁路分析的方法来实现硬件木马的监测。但是该类方法存在以下缺陷：(1)监测的准确性容易受到制造工艺扰动的影响；(2)该类方法需要利用安全芯片(已知无木马的芯片)进行比对，但安全芯片一般很难获得。

[0004] 另外，工艺型硬件木马通过改变某些器件的类型或者工艺参数来改变芯片的电气参数或缩短其使用寿命，其触发一般是一个十分缓慢的过程，因此在芯片测试阶段进行若干小时的测试并不能完全保证监测出来，而需要对目标芯片进行长时间的实时监控，其监测效率极度低下。

发明内容

[0005] 基于此，有必要针对传统硬件木马监测方法应用于工艺型硬件木马监测时，存在监测结果不准确且监测效率低下的问题，提供一种监测结果准确且监测效率高的工艺型硬件木马监测方法与装置。

[0006] 一种工艺型硬件木马监测方法，包括步骤：

[0007] 确定待测芯片中关键内部节点以及每个关键内部节点对应的电参数参考值；

[0008] 获取外部测试使能信号，并根据外部测试使能信号，确定关键内部节点的测试序列；

[0009] 根据测试序列，依次采集关键内部节点的电参数；

[0010] 将采集的每个关键内部节点的电参数与对应的电参数参考值比较；

[0011] 计数关键内部节点中存在电参数偏离对应电参数参考值的次数；

[0012] 当连续计数次数大于预设次数阈值时，判定待测芯片存在木马。

[0013] 一种工艺型硬件木马监测装置，包括依次连接的测试序列生成模块、信号传感模块、测试反馈模块以及木马判定模块，信号传感模块与待测芯片中关键内部节点连接，测试反馈模块存储有待测芯片中关键内部节点对应的电参数参考值；

[0014] 测试序列生成模块用于接收外部测试使能信号，并根据外部测试使能信号，确定关键内部节点的测试序列，信号传感模块用于根据测试序列，依次采集关键内部节点的电参数，测试反馈模块用于将采集的每个关键内部节点的电参数与对应的电参数参考值比较，木马判定模块用于计数关键内部节点中存在电参数偏离对应电参数参考值的次数，并

当连续计数次数大于预设次数阈值时，判定待测芯片存在木马。

[0015] 本发明工艺型硬件木马监测方法与装置，确定待测芯片中关键内部节点以及每个关键内部节点对应的电参数参考值，根据外部测试使能信号，确定关键内部节点的测试序列，依次采集关键内部节点的电参数，将采集的电参数与对应的电参数参考值比较，计数关键内部节点中存在电参数偏离对应电参数参考值的次数，当连续计数次数大于阈值时判定待测芯片存在木马。整个过程中，一方面对关键内部节点进行定时监测，另一方面将采集到的电参数与对应的电参数参考值比较，充分考虑了工艺扰动的影响，能够高效且准确对工艺型硬件木马进行监测。

附图说明

[0016] 图1为本发明工艺型硬件木马监测方法第一个实施例的流程示意图；

[0017] 图2为本发明工艺型硬件木马监测方法第二个实施例的流程示意图；

[0018] 图3为本发明工艺型硬件木马监测装置第一个实施例的结构示意图；

[0019] 图4为本发明工艺型硬件木马监测装置第二个实施例的结构示意图；

[0020] 图5为本发明工艺型硬件木马监测装置其中一个应用实例的结构示意图。

具体实施方式

[0021] 如图1所示，一种工艺型硬件木马监测方法，包括步骤：

[0022] S100：确定待测芯片中关键内部节点以及每个关键内部节点对应的电参数参考值。

[0023] 首先，需要对待测芯片的属性参数进行了解，确定待测芯片中关键内部节点。待测芯片中关键内部节点是指待测芯片中整体功能、性能或可靠性相关的电路节点。确定待测芯片中关键内部节点的步骤包括遍历待测芯片，查找待测芯片中整体功能、性能或可靠性相关的电路节点，将查找到的电路节点作为待测芯片中关键内部节点。简单来说即对待测芯片进行一些常规的研究与测试，查找其中影响硬件整体功能、性能或可靠性的电路节点，并将这些节点标示出来。每个关键内部节点对应的电参数参考值可以通过各类仪器设备确定每个关键内部节点对应的电参数参考值，或直接基于历史经验数据获取每个关键内部节点对应的电参数参考值。例如针对全新的待测芯片，可以采用各类仪器设备获取每个关键内部节点对应的电参数参考值，针对历史已经进行数据采集分析的待测芯片，可以直接读取历史记录中已获得的其每个关键内部节点对应的电参数参考值。更进一步来说，通过各类仪器设备确定每个关键内部节点对应的电参数参考值的过程具体包括：采用蒙特罗仿真算法，确定每个关键内部节点对应的电参数参考值。即采用蒙特罗仿真算法对待测芯片进行仿真处理，基于仿真处理之后的参数确定每个关键内部节点对应的电参数参考值。

[0024] S200：获取外部测试使能信号，并根据外部测试使能信号，确定关键内部节点的测试序列。

[0025] 一般来说关键内部节点有多个，每个关键内部节点都有自身相应的电参数参考值，在对整个待测芯片进行木马监测过程中，需要针对所有这些关键内部节点都进行电参数采集。为了高效且准确采集这些关键内部节点的电参数，需要针对这些关键内部节点测试顺序进行设定。在这里，获取外部测试使能信号，外侧测试使能信号决定当前接入的关键

内部节点，即决定当前采集电参数的关键内部节点。在实际应用中，可以采用包括含多个控制开关的开关组，其中每个控制开关的一端分别连接单个关键内部节点，每个控制开关的另一端与电参数采集组件连接，每个控制开关的控制端分别接收外部测试使能信号，这样外部测试使能信号可以控制当前闭合的控制开关，从而实现对关键内部节点的有序电参数采集。

[0026] S300：根据测试序列，依次采集关键内部节点的电参数。

[0027] 按照测试序列的顺序，依次采集关键内部节点的电参数。非必要的，可以针对采集的不同关键内部节点的电参数分配识别标识，例如可以先对不同关键内部节点分配标识，如1、2、3……，在采集到对应的关键内部节点的电参数时，记录为1关键内部节点的电参数、2关键内部节点的电参数、3关键内部节点的电参数……。

[0028] S400：将采集的每个关键内部节点的电参数与对应的电参数参考值比较。

[0029] 在步骤S100确定不同关键内部节点对应的电参数参考值，在步骤S300采集不同关键内部节点的电参数，在这里，将真实采集值与参考值进行比较。

[0030] S500：计数关键内部节点中存在电参数偏离对应电参数参考值的次数。

[0031] 电参数偏离对应电参数参考值偏离是指真实采集的电参数与对应电参数参考值不相等。具体来说，在实际应用可以设定一定的缓冲值，例如只有当偏离大于5％才判定为关键内部节点中存在电参数偏离对应电参数参考值。

[0032] S600：当连续计数次数大于预设次数阈值时，判定待测芯片存在木马。

[0033] 只有当连续多次测试都显示有异常时，才判定待测芯片中存在工艺型硬件木马，从而排除由于某些异常情况而造成的芯片误动作，可以提高硬件木马的真实检测率。需要指出的这里是需要考虑是连续出现异常情况次数大于预设次数阈值，以预设次数阈值为3为例，当采用上述S100-S500步骤对待测芯片进行工艺型硬件木马监测过程，第一次监测异常、第二次监测异常、第三次监测正常、第四次监测异常时，其连续计数次数并未大于预设次数阈值3，此时不能判定待测芯片存在木马。换言之，只有当第N次监测异常、第N+1次监测异常、第N+2次监测异常时，才能判定待测芯片存在木马。

[0034] 本发明工艺型硬件木马监测方法，确定待测芯片中关键内部节点以及每个关键内部节点对应的电参数参考值，根据外部测试使能信号，确定关键内部节点的测试序列，依次采集关键内部节点的电参数，将采集的电参数与对应的电参数参考值比较，计数关键内部节点中存在电参数偏离对应电参数参考值的次数，当连续计数次数大于阈值时判定待测芯片存在木马。整个过程中，一方面对关键内部节点进行定时监测，另一方面将采集到的电参数与对应的电参数参考值比较，充分考虑了工艺扰动的影响，能够高效且准确对工艺型硬件木马进行监测。

[0035] 如图2所示，在其中一个实施例中，步骤S400之后还包括：

[0036] S420：当关键内部节点中存在电参数偏离对应电参数参考值时，控制待测芯片重启，并返回步骤S300。

[0037] 当出现关键内部节点中存在电参数偏离对应电参数参考值时，表明当前已经监测到一次待测芯片异常，为了确保监测结果的准确，控制待测芯片重启，重新执行步骤S300～S600的步骤。

[0038] 如图3所示，一种工艺型硬件木马监测装置，包括依次连接的测试序列生成模块

100、信号传感模块200、测试反馈模块300以及木马判定模块400，信号传感模块200与待测芯片中关键内部节点连接，测试反馈模块300存储有待测芯片中关键内部节点对应的电参数参考值；

[0039] 测试序列生成模块100用于接收外部测试使能信号，并根据外部测试使能信号，确定关键内部节点的测试序列，信号传感模块200用于根据测试序列，依次采集关键内部节点的电参数，测试反馈模块300用于将采集的每个关键内部节点的电参数与对应的电参数参考值比较，木马判定模块400用于计数关键内部节点中存在电参数偏离对应电参数参考值的次数，并当连续计数次数大于预设次数阈值时，判定待测芯片存在木马。

[0040] 测试序列生成模块100用来产生自动检测序列，当系统进行定期自检时，外部输入会产生一组特殊激励信号，通过芯片输入管脚，加载到该模块上，从而使该模块产生一个测试序列信号，并输出给信号传感模块200。

[0041] 信号传感模块200用来监测原始电路(待测芯片)中某些关键内部节点上电压、电流等参数的变化，该模块由开关阵列和测量模块两部分组成，其中，开关阵列在测试序列的控制下，选择将某一个内部节点的信号传输给测量模块，而测量模块则对该信号进行测量、数模转换。

[0042] 测试反馈模块300用来检测信号传感模块200所输出的信号。测试反馈模块300内部存储了各个关节节点上电压、电流等参数的参考值，它把信号传感模块200输出的信号与这些参考值进行对比，当信号偏离参考值时，它输出一个信号控制木马判定模块400进行工作。

[0043] 木马判定模块400用来判断是否真实存在工艺型硬件木马。一旦测试反馈模块300检测到关键节点上的信号异常后，木马判定模块400将重启芯片并再次进行测试，只有当连续三次测试都显示有异常时，才判定芯片中存在工艺型硬件木马，从而排除由于某些异常情况而造成的芯片误动作，可以提高硬件木马的真实检测率。由于测试序列每个时钟周期可以监测一个关键节点上的信号，因此可以在很短的时间内完成所有关键节点的自检测。

[0044] 本发明工艺型硬件木马监测装置，测试序列生成模块100接收外部测试使能信号，并根据外部测试使能信号，确定关键内部节点的测试序列，信号传感模块200根据测试序列，依次采集关键内部节点的电参数，测试反馈模块300将采集的每个关键内部节点的电参数与对应的电参数参考值比较，木马判定模块400计数关键内部节点中存在电参数偏离对应电参数参考值的次数，并当连续计数次数大于预设次数阈值时，判定待测芯片存在木马。整个过程中，一方面对关键内部节点进行定时监测，另一方面将采集到的电参数与对应的电参数参考值比较，充分考虑了工艺扰动的影响，能够高效且准确对工艺型硬件木马进行监测。

[0045] 在其中一个实施例中，信号传感模块200包括相互连接的开关阵列单元和测量单元，开关阵列单元与测试序列生成模块100连接，测量单元与测试反馈模块300连接，开关阵列单元还与待测芯片中关键内部节点连接，开关阵列单元用于根据测试序列，选择接入的关键内部节点，测量单元用于采集接入的关键内部节点的电参数。

[0046] 如图4所示，在其中一个实施例中，工艺型硬件木马监测装置还包括测试使能信号生成模块500，测试使能信号生成模块500与测试序列生成模块100连接。

[0047] 在其中一个实施例中，测试使能信号生成模块500包括时钟单元。

[0048] 测试使能信号生成模块500主要用于在时钟信号的控制下，定时向待测芯片发送测试使能信号，从而使得测试序列生成模块100产生测试序列。

[0049] 在其中一个实施例中，木马判定模块400还用于当测试反馈模块300监测到关键内部节点中存在电参数偏离对应电参数参考值时，控制待测芯片重启。

[0050] 下面将采用具体应用实例，并结合附图5对本发明工艺型硬件木马监测装置的工作过程及其效果进一步说明。

[0051] 在该具体应用实例中，本发明工艺型硬件木马监测装置的工作过程包括如下步骤：

[0052] (1)确定关键节点

[0053] 明确待测芯片原始电路中的关键内部节点。关键内部节点指的是与芯片整体功能、性能或可靠性密切相关的电路节点，一旦这些节点上的电参数发生变化，将导致芯片无法正常工作。

[0054] (2)嵌入片上监测电路

[0055] 往待测芯片中嵌入片上监测电路，该电路由测试序列生成、信号传感、测试反馈和木马判定四个部分组成，如图5中所示。

[0056] (3)确定各关键节点电参数的参考值

[0057] 利用仿真手段，确定在不同工艺角下，各个关键节点上电压、电流等参数的参考值，并将这些参考值存入测试反馈的内部存储器中。

[0058] (4)定时生成测试序列

[0059] 在时钟信号的控制下，“外部测试使能信号生成”电路定时向待测芯片发送测试使能信号，从而使得测试序列生成产生测试序列信号。

[0060] (5)信号传感与反馈

[0061] 信号传感在测试序列的控制下，选择对某一个内部节点的信号进行测量、数模转换。测试反馈把信号传感输出的信号与其内部预先存储的参考值进行对比，当信号偏离参考值时，它控制木马判定进行工作。

[0062] (6)木马判定

[0063] 一旦测试反馈检测到关键节点上的信号异常后，木马判定将重启芯片并再次进行测试，当连续三次测试都显示有异常时，判定芯片中存在工艺型硬件木马，从而排除由于某些异常情况而造成的芯片误动作，提高硬件木马的真实检测率。

[0064] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

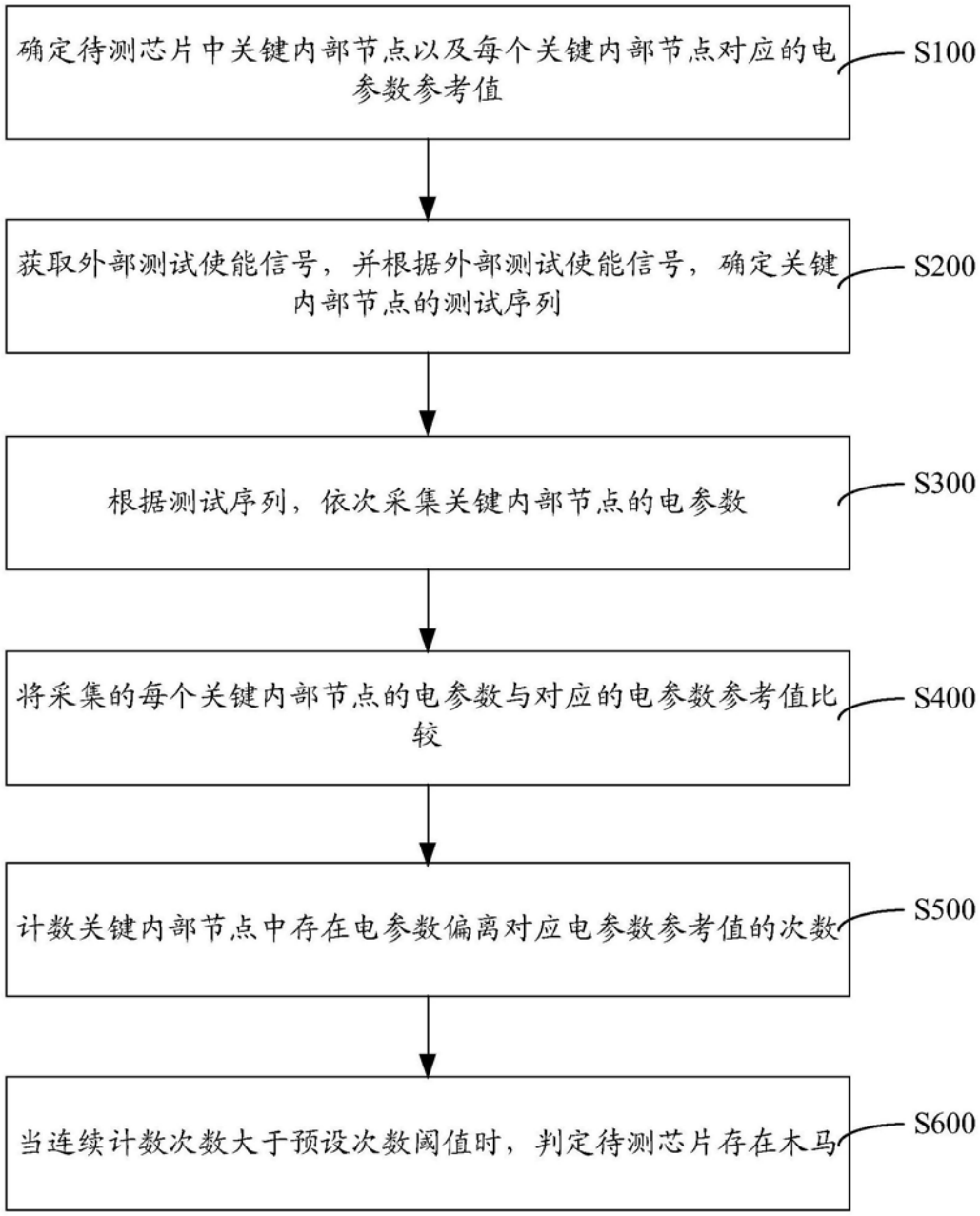

确定待测芯片中关键内部节点以及每个关键内部节点对应的电参数参考值
S100
获取外部测试使能信号，并根据外部测试使能信号，确定关键内部节点的测试序列
S200
根据测试序列，依次采集关键内部节点的电参数
S300
将采集的每个关键内部节点的电参数与对应的电参数参考值比较
S400
计数关键内部节点中存在电参数偏离对应电参数参考值的次数
S500
当连续计数次数大于预设次数阈值时，判定待测芯片存在木马
S600

图1

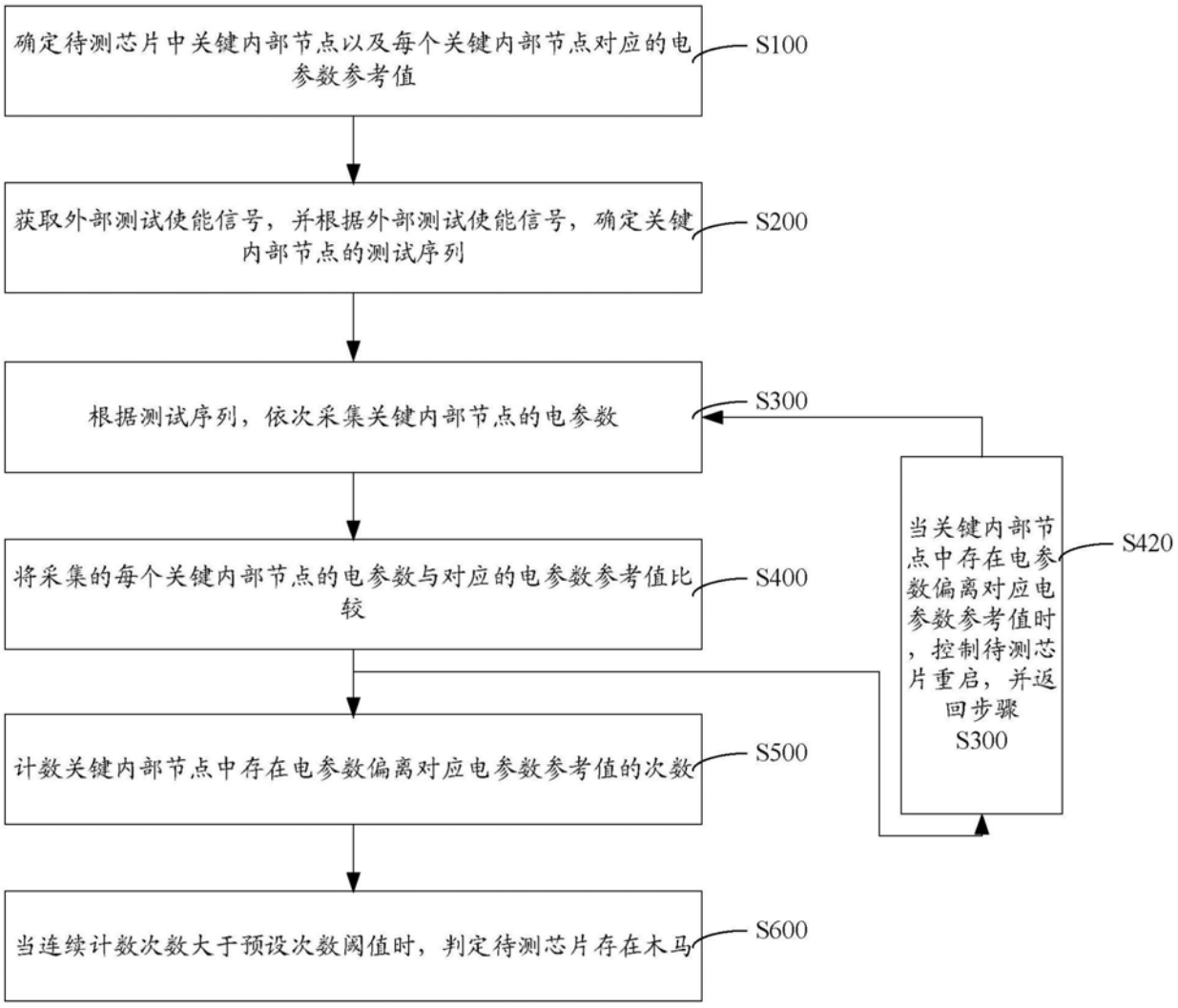

确定待测芯片中关键内部节点以及每个关键内部节点对应的电参数参考值
S100
获取外部测试使能信号，并根据外部测试使能信号，确定关键内部节点的测试序列
S200
根据测试序列，依次采集关键内部节点的电参数
S300
将采集的每个关键内部节点的电参数与对应的电参数参考值比较
S400
计数关键内部节点中存在电参数偏离对应电参数参考值的次数
S500
当连续计数次数大于预设次数阈值时，判定待测芯片存在木马
S600
当关键内部节点中存在电参数偏离对应电参数参考值时，控制待测芯片重启，并返回步骤S300
S420

图2

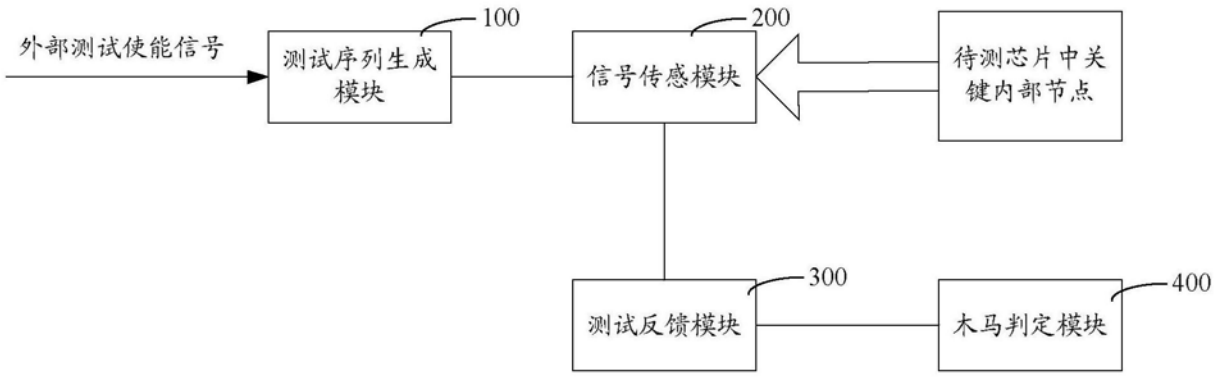

外部测试使能信号
测试序列生成模块
100
信号传感模块
200
待测芯片中关键内部节点
测试反馈模块
300
木马判定模块
400

图3

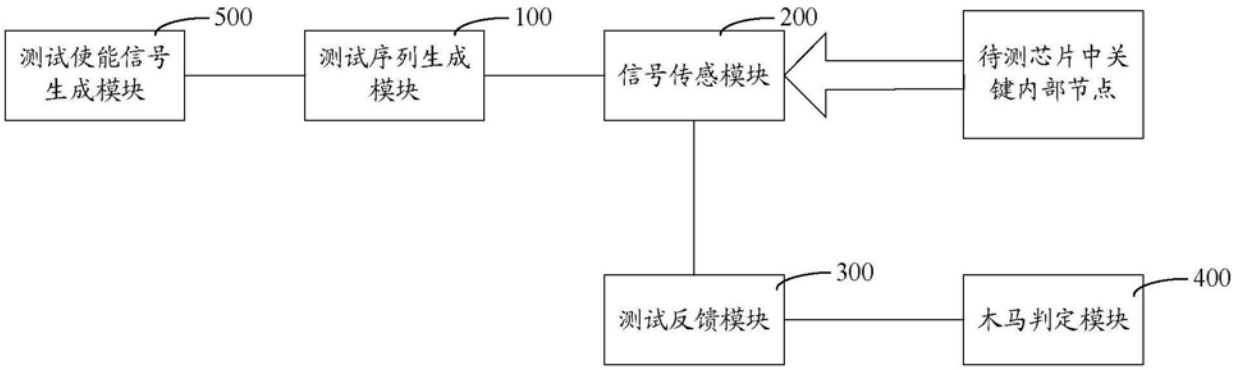

500
测试使能信号生成模块
100
测试序列生成模块
200
信号传感模块
待测芯片中关键内部节点
300
测试反馈模块
400
木马判定模块

图4

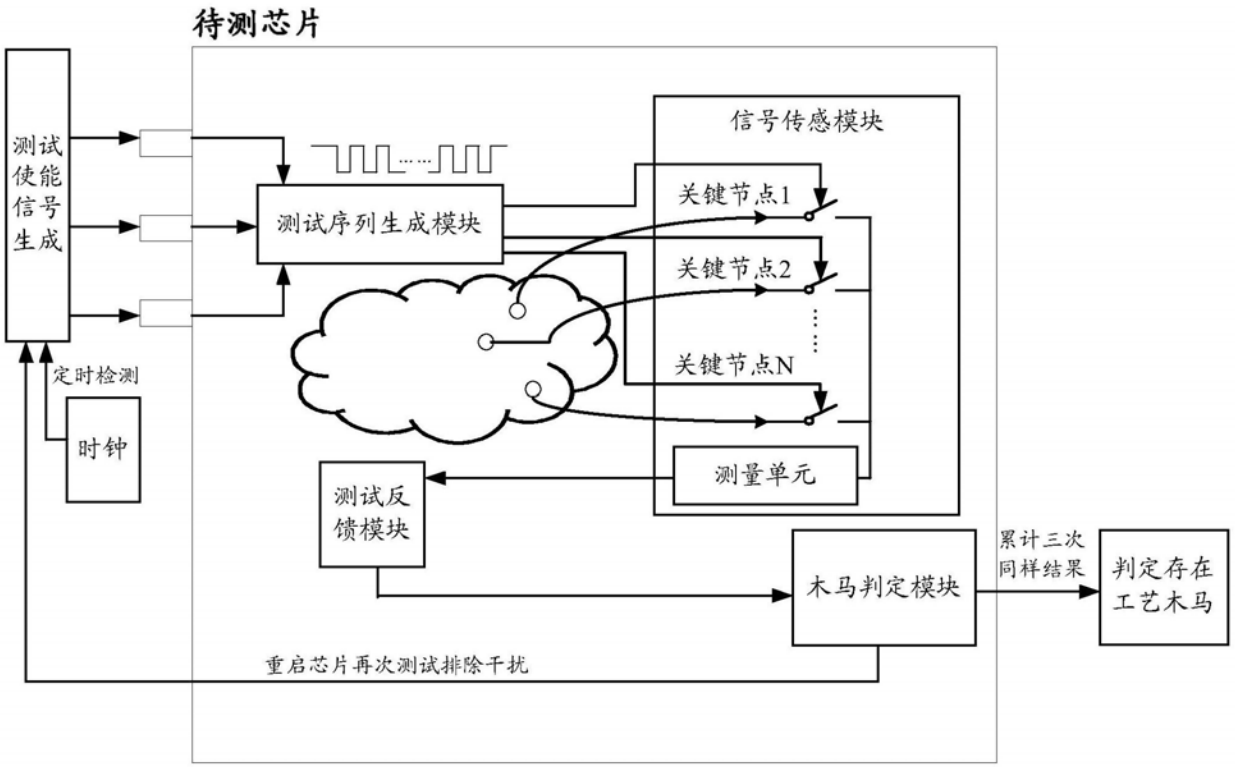

待测芯片
测试使能信号生成
测试序列生成模块
信号传感模块
关键节点1
关键节点2
关键节点N
测量单元
定时检测
时钟
测试反馈模块
木马判定模块
累计三次同样结果
判定存在工艺木马
重启芯片再次测试排除干扰

图5