一种安全可控的 SoC 可测性设计*

王新成,孙 宏,蔡吉仁,杨义先
(北京邮电大学 信息安全中心,北京 100876)

摘 要:提出了一种安全可控的可测性设计DFT(Design For Test)。DFT既能够完成对SoC的测试,又能保障SoC自身敏感信息和关键技术的安全。

关键词:可测性设计 集成电路 微系统芯片

1 背景

测试是集成电路设计和生产过程中最重要的环节之一,是检测集成电路设计是否达到既定设计要求的重要手段。集成电路的测试可以分为功能测试和结构测试两种。功能测试的目的在于验证设计是否能正确地按照技术条件实现其功能,保证与设计意图相匹配;结构测试的目的在于检查所生产的每一芯片是否合格。具体的测试又可分为[1]:

(1)分析性测试:对错误进行定位,也叫物理测试。

(2)功能性测试:确定制造出的芯片功能是否正确。

(3)参数化测试:在一定的工作条件下(特定温度与电压下),测试噪声容限、传输延时、最大时钟频率等。

可测性设计是指在集成电路设计的初始阶段,除了要考虑集成电路的功能、性能和芯片面积之外,还要将芯片的可测性作为设计目标之一。DFT及EDA工具支持的可测性设计技术[2]包括:(1)全扫描技术;(2)部分扫描技术;(3)边界扫描技术;(4)内建自测试技术。

JTAG(Joint Test Action Group)[3]是目前大多数SoC芯片采用的测试标准。JTAG利用边界扫描技术,在测试时不需要其他的测试设备,能够测试芯片的逻辑功能和IC之间的连接是否存在故障。本文将以JTAG测试方法为例,进行相关分析,在此基础上引入一种安全可控的可测性设计,并将该设计与传统的JTAG测试方法进行对比,最后给出结论。

2 JTAG 技术原理

JTAG边界扫描测试结构是在芯片的每一I/O引脚及内部的关键部位增加一个边界扫描寄存器(BSR)单元,并把这些寄存器依次连成扫描链。在正常工作时这

些扫描单元是透明的,不影响芯片的正常工作。在测试期间边界扫描寄存器可以串行地存储测试数据和从中读出测试数据。边界扫描测试结构包括以下四个部分:

(1)测试存取通道(TAP):提供测试所需的各种数据,TAP 的端口有 4 个:测试时钟(TCK),测试模式选择(TMS),测试数据输入(TDI),测试数据输出(TDO)。

(2)TAP 控制器:将串行输入的 TMS 信号进行译码,使边界扫描系统进入相应的测试模式,并产生各种控制信号。

(3)指令寄存器(IR):是一个附有锁存器的移位寄存器,用来寄存测试指令。

(4)测试数据寄存器组(TDR):包括旁路寄存器和边界扫描寄存器。

JTAG 边界扫描测试结构具有以下功能:

(1)能用于 IC 内部的功能测试。

(2)能较好地控制 IC 引脚使之用于参数测试(测试输出缓冲的驱动能力、漏电、输入阀值等交流和直流特性)。

(3)可用于访问内部扫描路径,以提高从引脚难以访问的内部节点的可观测性。

(4)可用于片上调试功能,并且不需要额外的引脚。

3 DFT 与 IP 保护

DFT 实际上是在原器件的内部增加可观测性的逻辑电路,使得 SoC 芯片能够很方便地观察和控制电路的输入、输出及内部的各个节点,便于系统的测试、仿真和软件的跟踪开发与调试。但是可测性设计使 SoC 系统失去了最根本的安全性,使得 IP 得不到保障。对于 SoC 的核提供商来说,这意味着知识产权的潜在丧失。以 JTAG 为例,攻击者能够轻而易举地利用 JTAG 查看 SoC 芯片内部的状态信息,从而获取 SoC 中的全部程序与数据。尤其是对于安全芯片,可测性设计与 JTAG 接口的存在使得其中的密钥与敏感信息毫无安全可言,芯片的安全性受到严重威胁。

为了解决 SoC 系统设计中可测性与可靠性及安全的矛盾,目前采用的方法一般有以下两种:

(1)人工破坏法:在 SoC 系统测试完成及 SoC 中的 FIRMWARE 装载完成后,人为破坏 JTAG 接口的引脚,使得攻击者的难度加大,但由于芯片内部的可测性结构与 JTAG 电路并没有破坏,因而并不能从根本上防止被攻击。同时,这种方法对于大批量的芯片生产效率太低。

(2)消除 JTAG 接口法:为了保护 SoC 的 IP 和敏感信息,特别是密码芯片中的密钥,在 FIRMWARE 开发时提供可供仿真与调试的 JTAG 接口芯片样片,待 FIRMWARE 开发调试后,再进行第二次流片,去掉 JTAG 接口。这种方法既要花费第二次流片的成本,又为以后 FIRMWARE 的升级开发带来不便。

4 一种可控的 DFT 设计

本文提供一种软硬件结合的安全可控的 SoC 可测性设计方案,从而解决 SoC 系统设计中可测性与可控性及安全性的矛盾,避免现有方法引起的低可靠性、低安全性、低效率和高成本等问题。

安全可控的 SoC 可测性设计方案的核心是在方案中设计一种针对 JTAG 的可控安全模块。这一模块可以用控制字的方式控制 JTAG 边界扫描测试结构中的测试存取通道(TAP)以防止对 SoC 的跟踪与攻击。在芯片的测试与 FIRMWARE 的调试开发时,此安全模块不干预芯片的测试与开发流程。在芯片的裸片测试完毕及 FIRMWARE 的调试开发结束后,安全模块在相应的控制字的操作下关闭 JTAG 边界扫描测试结构中的测试存取通道(TAP),即封闭 JTAG 接口中的时钟、输入、输出信号,从而使攻击者无法利用 JTAG 接口获取 SoC 芯片内部的数据。具体流程见图 1。

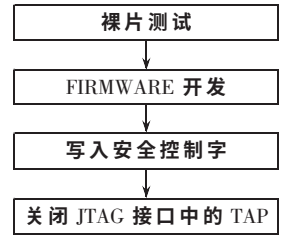

图 1 安全可控的 SoC 可测试设计

图 2 所示为带有普通 JTAG 边界扫描链的芯片。通过 JTAG 边界扫描链可以直接探测芯片内部的状态和数据。

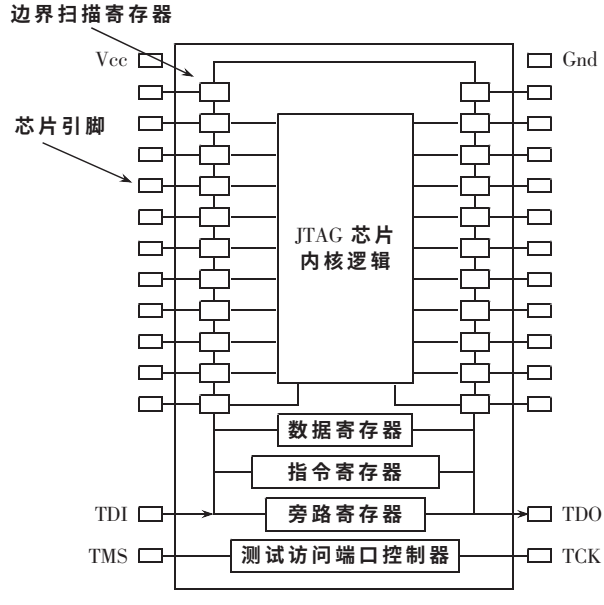

图 2 带普通 JTAG 边界扫描链的芯片

图 3 是带有安全模块的 JTAG 边界扫描链的芯片。图中,JTAG 边界扫描链受到安全模块的控制,在关闭安全模块的情况下可以获取芯片内部状态及数据,方便调试。当调试完毕时,启动安全模块,能够封闭 JTAG 边界扫描链的输入、输出。这样,外部将无法通过 JTAG 边界扫描链获取芯片内部状态、数据。

图 4 给出一种安全模块的实施方案。在该方案中,安全模块采用 4 个寄存器分别控制 TMS、TDI、TDO、TCK 信号线。调试期间,安全模块内部的寄存器写入的数据

分别是 1、0、0、1。由图 4 可以看出，此时 Inner_TMS、Inner_TDI、Inner_TDO、Inner_TCK 信号与 TMS、TDI、TDO、TCK 信号相同，对 JTAG 接口没有影响，可以通过 JTAG 接口进行调试。当调试完毕时，改变 FIRMWARE 控制安全模块部分的代码，使得加在 TMS、TDI、TDO、TCK 上的数据分别是 0、1、1、0，此时信号 Inner_TMS、Inner_TDI、Inner_TDO、Inner_TCK 的输出永远是 0、1、1、0，与 TMS、TDI、TDO、TCK 信号没有任何关系。因此能够封闭 JTAG 接口，阻止非法用户通过 JTAC 接口对芯片进行测试。

整个安全可控的可测性设计应用流程如图 5 所示。

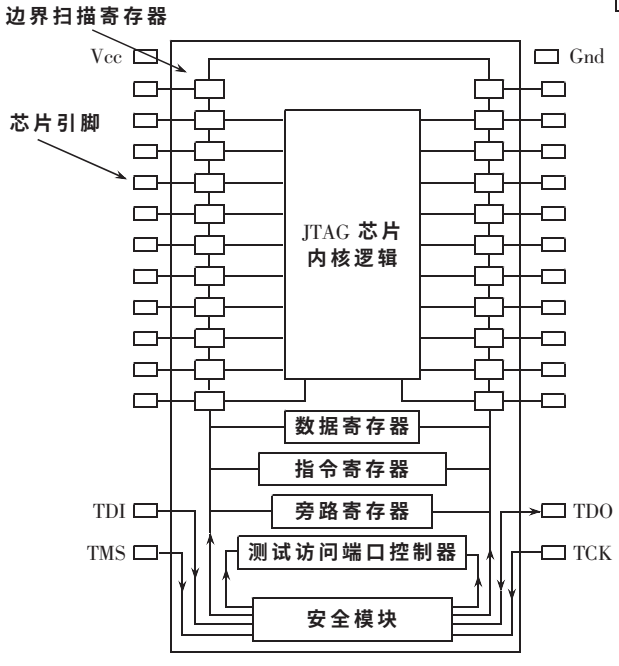

图 3 带有安全模块的 JTAG 边界扫描链的芯片

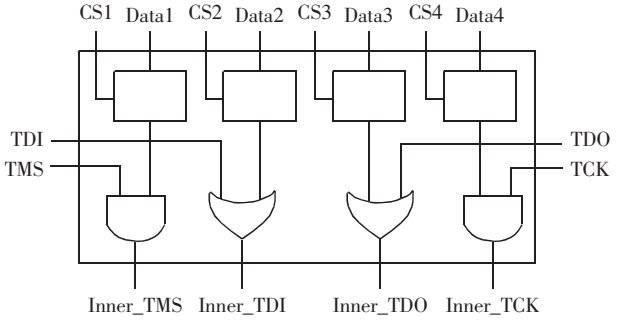

图 4 安全模块实施图例

图 5 所示的流程如下：

(1)系统启动，安全模块的寄存器根据控制字完成初始化；

(2)检测安全模块中寄存器的设置值；

(3)用户判断当前 FIRMWARE 是否调试完毕，若需要启动安全模块，则转至(9)执行，否则执行(4)；

(4)根据检测的安全模块寄存器当前设定值，判断是否正常关闭了安全模块，如果是，则执行(5)，否则转至(6)；

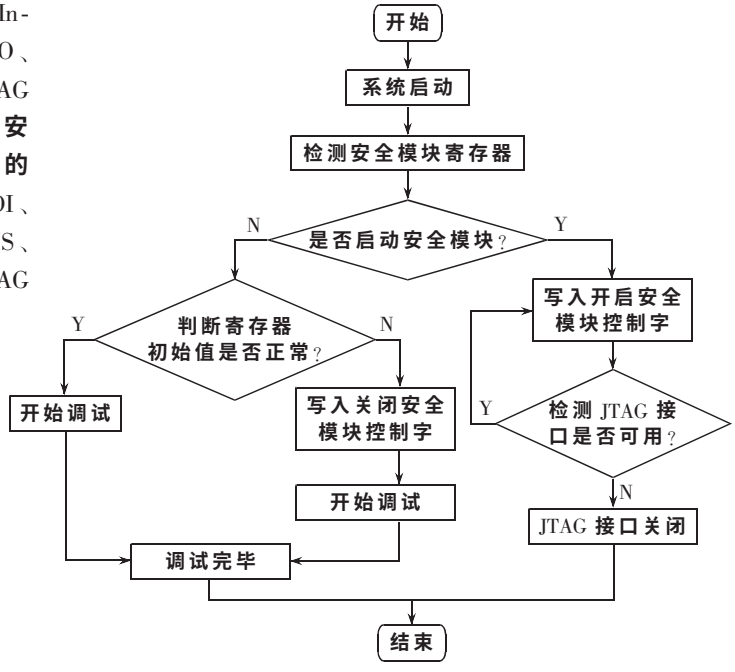

图 5 封闭 JTAG 接口的处理流程

(5)开始对 FIRMWARE 和芯片的调试；

(6)向寄存器中写入关闭安全模块的控制字；

(7)开始对 FIRMWARE 和芯片的调试；

(8)结束对 FIRMWARE 和芯片的调试；

(9)向寄存器中写入开启安全模块的控制字；

(10)检测是否可以通过 JTAG 接口检测芯片内部状态、数据，如果可以则转向(9)，否则执行(11)；

(11)确认 JTAG 接口关闭，不可能再通过 JTAG 接口检测芯片内部状态、数据，达到设计目的。

这种安全可控的 SoC 可测试方案的主要优点在于：实现方式简单，成本低廉，与人工破坏法相比，可以达到相同的效果，但实现工艺上人工破坏法需要生产厂商具备专用的生产设备，实现难度大；与消除 JTAG 接口法相比，无需进行第二次流片，成本低廉，并且本方法可以通过更新 FIRMWARE 来实现关闭安全模块，重启 JTAG 接口，方便升级调试。

本文提供了一种安全可靠的可测性设计。通过灵活可靠的设计方法，在不影响设计过程中测试的情况下，解决了 SoC 可测性设计中的 IP 安全问题和其他敏感部件和信息的安全问题，具有实际应用价值。

参考文献

1 D&T Roundtable.Testing Embedded Cores.IEEE Design and Test of Computer, April-June 1997, 81~89

2 Rajsuman R.Challenge of the 90's: Testing CoreWare based ASICs.Panel on DFT for Embedded Cores, Proc IEEE Int Test Conf, 1996: 940

3 IEEE Std 1149.1 Standard Test Access Port and Boundary-Scan Architecture.IEEE Press, 1990

(收稿日期：2006-07-12)