

机载电子跨时钟域同步电路验证及可靠性分析

范毓洋^{1,2}, 邓智¹, 李子航^{1,2}

(1.中国民航大学 民航航空器适航审定技术重点实验室, 天津 300300; 2.中国民航大学 适航学院, 天津 300300)

摘 要:在航空器的机载设备中存在大量的多时钟域电路,数据在进行跨时钟域传输时可能会产生亚稳态,导致数据传输错误,电路可靠性降低。但亚稳态导致的故障具有偶发性、不易重现,且现有的跨时钟域专用验证软件使用成本高昂,不支持三模冗余场景下的跨时钟域电路验证。针对此问题,提出了一种基于传统工具的寄存器传输级(RTL)验证、板级加速测试和计算评估相结合的方法。该方法能够在设计早期使用通用仿真工具发现三模应用场景或正常场景下的跨时钟域传输问题,并评估潜在跨时钟域传输风险,降低了高安全等级机载复杂电子验证经济成本和时间成本,提高电路可靠性。

关 键 词:机载电子;跨时钟域;寄存器传输级验证;可靠性
中图分类号:V243 **文献标志码:**A **文章编号:**1000-2758(2022)02-0369-08

随着机载电子设备复杂性增加、机载电子芯片设计规模的扩大,集成电路设计中跨时钟域信号传输也逐渐增多。而信号跨时钟域传输不可避免地会在电路中引入亚稳态^[1],若亚稳态处理不当,则可能给电路带来数据丢失、位错、重汇聚等风险,造成设备关键功能的丧失或错误。如时钟检查电路功能丧失^[2]、飞机显示图像异常、AFDX 交换机数据错误等。更严重的是,若亚稳态沿信号通道上的寄存器级联传播,可能造成芯片烧毁的严重后果。如某航天器在为期一年多的地面测试中突然出现故障,经分析发现,航天器出现故障的原因是跨时钟域电路传输引入亚稳态,亚稳态传播导致片上大量 MOS (metal oxide semiconductor)管同时工作致使电路板烧毁^[3]。

目前电子设计技术的进步和一些机载电子设计部门的扩张,客观上也增大了设计中发生亚稳态问题的可能性。如一些硬件综合工具支持软件工程师使用高级语言设计硬件电路,与使用 RLT 代码进行电路设计相比,跨时钟域电路的亚稳态问题更容易被设计人员忽略^[4]。另外,机载电子设计部门因为人员快速扩张,员工技术水平良莠不齐,不仅使得在设计过程中容易出现同步器功能设计错误,也使得

同行评审质量下降,不能依靠评审有效发现问题。且随着特征尺寸的下降、新设计技术的出现^[5],芯片电压下降、时钟频率和数据频率提高、同步路径增多,导致芯片中已有的功能正确的跨时钟域信号同步器的可靠性下降。若这些同步设计不经过可靠性评估而直接应用到航空领域,则会产生安全隐患。虽然目前跨时钟同步电路的问题存在的可能性增大,但是目前的机载电子的验证活动中,常常会忽视掉针对跨时钟域传输功能和可靠性的验证活动。

FAA Order 8110.105 A 提及了机载电子硬件需进行最好或最坏情况下时序分析^[6]。但是 Order 8110.105 A 及 DO-254 标准中都未具体提及如何验证跨时钟域时序问题^[7]。而机载电子行业针对机载复杂电子硬件验证活动是基于需求开展的。时钟相关的需求一般只会描述各个时钟的时钟频率、占空比、抖动等内容。针对这些时钟需求的验证一般通过时序仿真和静态时序分析来进行覆盖。因此基于需求的验证及对应的验证方法并不能有效发现跨时钟域传输的问题。若未在设计活动中把概要设计或详细设计中明确的跨时钟域路径反馈到衍生需求,或未在概要设计中明确描述跨时钟路径及同步策略方法,则针对跨时钟域的验证活动很容易被忽

视。若把亚稳态问题带到终端产品上去,则可能会使机载设备产生安全隐患。

因此,为了减少亚稳态问题发生概率,保证同步正确性,需要对跨时钟域电路可能带来的问题(同步器可靠性问题^[8-9]、同步器结构问题^[5,9-10]、跨时钟域数据传输协议问题^[5,11]、重汇聚^[5,12-13]问题)进行全面验证。而跨时钟域信号验证通常只能对多个实际电路进行长期测试以发现亚稳态隐患。但由于亚稳态造成的故障具有偶发性和不可重现性,极大增加了电子硬件的研制时间和验证成本。如果直接使用国外专用 CDC 分析软件(如 spyglass, questa_cdc),在高安全等级机载电子电路验证活动(例如 DAL A, B)中需承担工具成本及使用此工具所需的工具鉴定^[14]活动所带来的时间和经济成本。另外,由于航空单粒子问题,常常要求使用三模冗余对跨时钟域模块进行加固设计^[15],但目前的专用 CDC 分析软件不支持三模跨时钟同步电路验证,容易出现错误的验证结果,给验证活动带来问题。

针对此情况,本文对跨时钟域同步可能存在的问题开展全面的验证方法研究,提出了一套基于传统 FPGA(field programmable gate array)设计工具、功能仿真工具的 RTL 级验证、板级加速测试和计算评估相结合的跨时钟域验证的解决方法。该方法有较强的实用性和适用性,能够有效弥补专用工具缺陷,在机载电子设计早期发现并评估潜在的跨时钟域传输风险,达到降低安全隐患的目的。

1 方法概述

完整的跨时钟域同步电路验证及可靠性分析方法主要包括 RTL 级验证、板级加速测试、计算评估三部分,具体验证流程如图 1 所示。

RTL 级验证(包括结构分析、协议验证、重汇聚验证)旨在证明跨时钟域信号传输所使用的同步方法功能正确,保证了单比特的使能信号或多比特的数据信号能传输到目的时钟域,且不会出现数据丢失。

板级加速测试通过构建加速亚稳态生成环境获取亚稳态相关数据,并根据板级测试所得亚稳态相关数据计算出亚稳态参数值。

对于航空机载设备电路的设计,需对这些功能正确的同步电路的可靠性进行分析。为评估电路可靠性,需通过亚稳态参数计算同步电路的 MTBF(mean time between failure)。从而最终判断出设计

中使用的同步策略是否可接受。

如果在 RTL 级验证或计算评估中发现问题应及时提出问题报告,依据问题报告提出更改请求,增加对应的衍生需求。并依据需求修改对应的概要设计及设计代码。最后将修改后的代码重新进行 RTL 级验证、板级加速测试、MTBF 计算评估,如果发现问题应继续提出问题报告并修改直至得到可接受的同步策略。

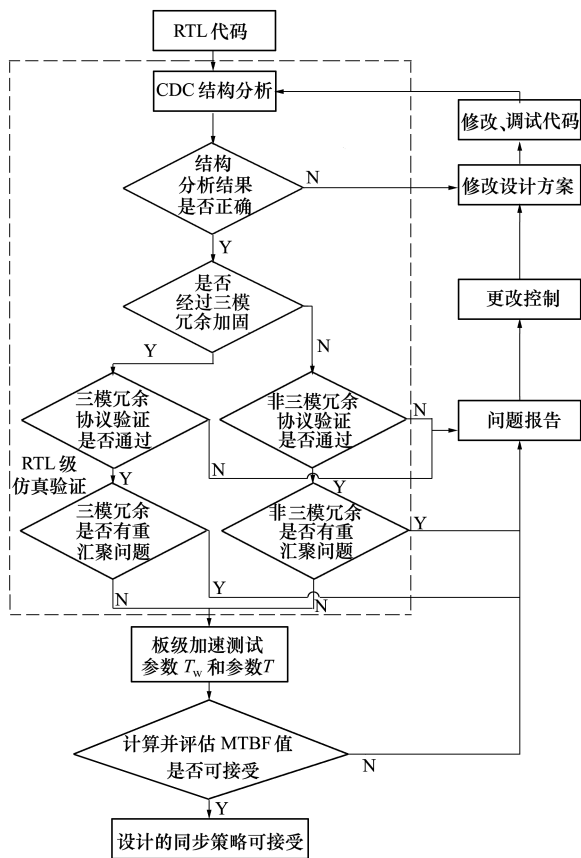


图 1 验证流程图

2 RTL 级验证

在电路 RTL 设计及功能仿真完成后,需要针对跨时钟域信号进行结构分析、协议验证和重汇聚验证,作为静态时序分析的补充。其中结构分析用以确保同步电路具有正确的同步电路单元,协议验证对同步电路是否满足相应的传输协议进行检查,重汇聚验证判断数据在目的时钟域内是否存在重汇聚问题。

2.1 结构分析

能够将数据正确跨时钟域传输的同步电路(如握手协议、异步 FIFO 等同步电路)都包含至少连续 2 级且中间无组合逻辑运算的寄存器级联的结构单元,本文把其定义为同步单元(或电平同步电路),如图 2 所示。

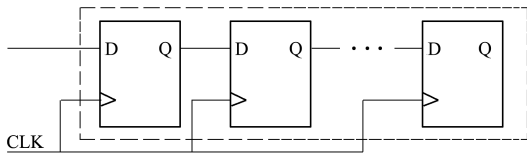


图 2 同步单元

结构分析主要确定跨时钟域路径上是否含有该同步单元的结构以降低亚稳态传输概率,进而确定设计所采用的同步电路结构或方法,可通过使用常用的 EDA 工具来快速分析。如在 Xilinx 的 Vivado 开发环境下,对 RTL 级代码进行综合后可得到原理图,在原理图上同时选定不同时钟域的时钟信号,便可快速定位出数据跨时钟域交互模块。定位出 CDC 设计模块后,便可分析该模块所采用的同步策略、模块是否含同步单元、同步路径是否含组合逻辑。如果没有正确的同步电路结构,则说明需要增加合适的同步电路使数据正确传输。

2.2 协议验证

电路具有正确的同步电路结构,并不能保证该数据可以正确地传输到目的时钟域,还需满足相应的传输协议。为快速验证电路是否符合传输协议,可使用传统的仿真软件,并在基于断言的仿真测试平台上进行动态仿真。为模拟出真实环境,保证数据在任何情况下都满足传输协议,动态仿真的输入激励须覆盖需求规定的所有情况。在进行动态仿真时,如果传输的数据在某一时刻不满足相应的传输协议,则断言宣告失败,说明该数据不能被正确地跨时钟域传输,需重新修改同步策略直至验证通过;如果断言成功,则表示该同步电路能正确地将数据传输到目的时钟域。

本文以适用于三模冗余的多周路径(multi-cycle-path, MCP)传输电路为例,说明 CDC 电路的传输协议验证过程。适用于三模的 MCP 电路如图 3 所示,发送电路在更新数据 tx_data 的同时发出脉冲信号 tx_en。tx_en 经过结绳模块后变为电平信号 en_tx_clk。q2_A 为同步后的 en_tx_clk 信号,q2_B、q2_C 则为另外 2 个冗余电路的电平同步后信号。

3 个信号经过 voter 表决后通过边沿检测生成 en_rx_clk 信号,并把其作为 data_sending 的读时钟域接收寄存器的使能信号。

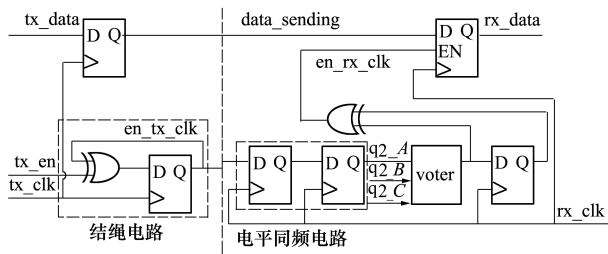


图 3 多周路径传输路径电路

假设发送时钟域中的脉冲信号间隔为 nT_1 (T_1 代表发送时钟周期),考虑到亚稳态的情况下,接收时钟域中的数据信号必须经过 1 个发送时钟周期和至少 4 个接收时钟信号的上升沿,才能保证该组数据的正确传输,即 $nT_1 > 4T_2 + T_1$ (T_2 代表接收时钟周期)。因此,使能信号 tx_en 的间隔应满足公式(1)。

$$T_{tx_en} - 1 \geq 4 \cdot \frac{T_2}{T_1} \tag{1}$$

式中: $T_{tx_en} - 1$ 表示 tx_en 信号下降沿到下一个 tx_en 上升沿之间包括的最少发送时钟周期,在此期间 tx_en 应保持低电平。

发送数据 tx_data 在整个数据发送过程中均应保持稳定,协议可以表示为公式(2)。

$$T_{data} \geq 4 \cdot \frac{T_2}{T_1} + 1 \tag{2}$$

T_{data} 表示发送数据 tx_data 需要在多少个发送时钟周期内保持稳定。

根据上述分析,使 CDC 数据正确传输发送数据和脉冲信号间隔断言表示如下,仿真波形如图 4 所示。

```
property DATA_SEND;
@ (posedge tx_clk) $rose(tx_en) | => ($stable(tx_data) [ * ($ceil(4 * T2/T1)) ] );
endproperty : DATA_SEND

property TX_EN;
@ (posedge tx_clk) $fell(tx_en) | -> ((! tx_en) [ * ($ceil(4 * T2/T1)) ] );
endproperty : TX_EN
```

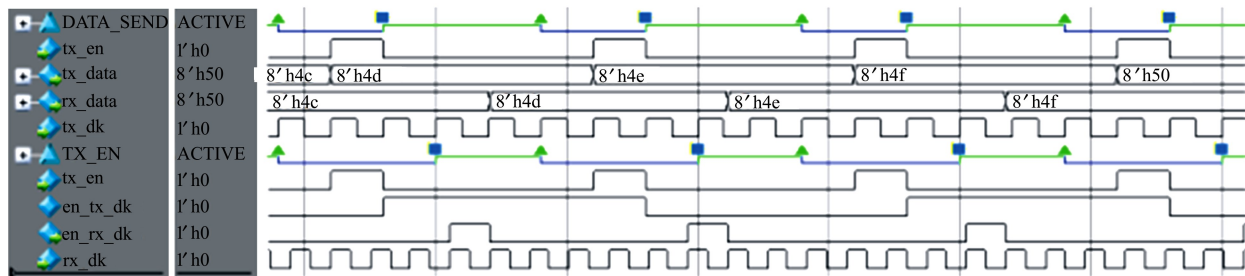


图 4 电路断言波形图

2.3 重汇聚验证

当数据经过不同的同步电路后,无法保证同步电路的路径、环境(如时钟相位、寄存器电压、电磁干扰)及器件工艺参数完全相同,因此经过不同同步电路的传输数据可能会出现不可预测的提前或延迟。在目的时钟域内,如果经过不同跨时钟域路径传输的数据进行组合逻辑运算,可能会造成整个电路的功能错误。为避免电路出现无有效保护的重汇聚运算,须对设计进行亚稳态重汇聚验证。重汇聚验证可基于传统仿真工具,通过随机注入延迟来判定电路对亚稳态的容忍度。如果进行延迟注入后仿真结果与预期一致,则表明该电路符合需求。与协议验证一样,重汇聚验证需要仿真测试平台的输入激励覆盖需求规定的所有情况。

下面描述的亚稳态注入方案与已有研究的注入方法相比^[12]主要区别是固定了注入随机延迟的变化频率,注入随机延迟的时机由状态机进行控制。该方法保证了进行一次使能信号传输时,随机延迟的注入不会突然变化而导致单比特使能信号缩短。相比于已有研究论文,其能应用在如对接接收使能信号有长度要求(一般为 2 个接收时钟长度)的三模冗余电路。需注意的是,一般情况下在目的时钟域的重汇聚是不允许的,但在抗单粒子翻转使用的三模冗余设计中,不同同步路径会在三模投票电路处出现计划内的汇聚点^[13],一些专用的跨时钟域分析工具如 Questa CDC 可能误报该错误。使用本文的亚稳态注入方法,可以对该投票电路功能在翻转场景下是否失效进行动态判别。避免一些静态跨时钟域分析工具直接对该汇聚现象报错的情况出现。

如图 5 所示,亚稳态注入位置选取在跨时钟模块信号传输完成后三模冗余投票之前的节点,本设计使用状态机确保 3 个亚稳态注入点注入亚稳态时,该信号不会被截短导致三模冗余验证不能通过。

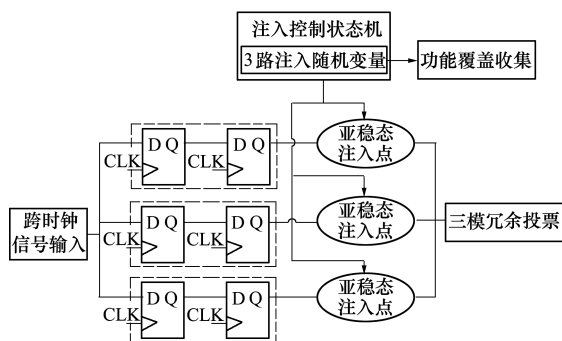


图 5 亚稳态注入电路

且在动态仿真过程中,为保证验证的全面性,需要收集功能覆盖率情况。确认在验证过程中覆盖了亚稳态的一路注入、两路同时注入、三路同时注入的情况。使验证活动更为完整可靠。

协议验证和重汇聚验证可以使用相同的输入激励,因此可以在一次仿真验证过程中同时检查电路的传输协议和重汇聚问题。

3 加速测试和可靠性分析评估

本节通过构建加速亚稳态的生成和采集电路获取亚稳态相关数据,并根据板级测试所得亚稳态相关数据计算出亚稳态参数值,使用该亚稳态参数值,就可以计算出电路全部跨时钟域路径的 T_{MTBF} (平均无故障时间)值。

3.1 加速测试方法

跨时钟域传输时通过单触发器后发生亚稳态的概率常使用公式(3)进行评估^[15]:

$$T_{MTBF} = \frac{1}{T_w \cdot f_c \cdot f_d} e^{t_r/\tau} \quad (3)$$

式中: t_r 为亚稳态解决时间,即预留给触发器使其从亚稳态恢复到稳定的时间; τ 为触发器的亚稳态解

析时间常数; T_w 为亚稳态窗口时间常数; f_c 为设计的接收时钟频率; f_d 为设计的异步信号变化频率,即输入的异步信号翻转率。

对于具体的电路设计来说,参数 f_c 、 f_d 和 t_τ 已知。因此要对 MTBF 进行计算的关键是确定触发器的亚稳态参数 T_w 和 τ 。

对公式 (3) 两边取自然对数,得到如下公式:

$$\ln(T_{\text{MTBF}}) = \frac{t_\tau}{\tau} - \ln(T_w \cdot f_c \cdot f_d) \tag{4}$$

易知方程 (4) 是一条直线,其自变量为亚稳态决断时间 t_τ ,因变量为 $\ln(T_{\text{MTBF}})$,直线斜率 k 为 $1/\tau$,截距为 $-\ln(T_w \cdot f_c \cdot f_d)$ 。得到 τ 的计算公式,如公式 (5) 所示

$$\tau = \frac{1}{k} \tag{5}$$

得到 T_w 的计算公式,如公式 (6) 所示

$$T_w = \frac{e^{-b}}{f_c \cdot f_d} \tag{6}$$

所以可以通过改变 t_τ ,测得到不同 t_τ 下的 T_{MTBF} 值,拟合出 $t_\tau - \ln(T_{\text{MTBF}})$ 直线,从而算出 T_w 和 τ 。目前半导体器件的亚稳态参数测试方法都是基于该测试理论。

基于该测试理论,FPGA 芯片厂商推荐使用的亚稳态参数的测试电路为半周期测试电路^[8],通过改变时钟周期的频率改变 t_τ 。本文推荐使用器件的时间管理模块以实现 t_τ 更精确的控制,以便获得更多更广泛的数据和更高的测试效率。亚稳态参数测试需采集大量的亚稳态数据,为计算 T_{MTBF} 值,需测得亚稳态发生次数和其对应的时间。在设计亚稳态采集电路时,测试前规定亚稳态采集停止次数 S 。开始亚稳态采集时,计时计数器开始计时,当亚稳态采集次数计数器达到亚稳态采集停止次数 S 时,使计时计数器停止,并把该时间 T 记录下来。 S/T 即可计算得出采集到 2 次亚稳态的平均时间间隔。通过改变 t_τ ,经过不同次的测试计算获得对应的 T_{MTBF} 值。需注意的是,测试时要使亚稳态采集点在 FPGA 上的位置尽可能分散。

为方便在使用某些器件时进行跨时钟域的可靠性评估,本文对 6 种典型 FPGA 芯片的亚稳态相关参数进行采集计算。在不同采样点多次规定次数进行亚稳态采样后,对数据点进行最小二乘法直线拟合,绘制出 6 种典型芯片亚稳态参数采集 Matlab 图(图中 t_τ 和 T_{MTBF} 的单位为 ps) 如图 6 所示。

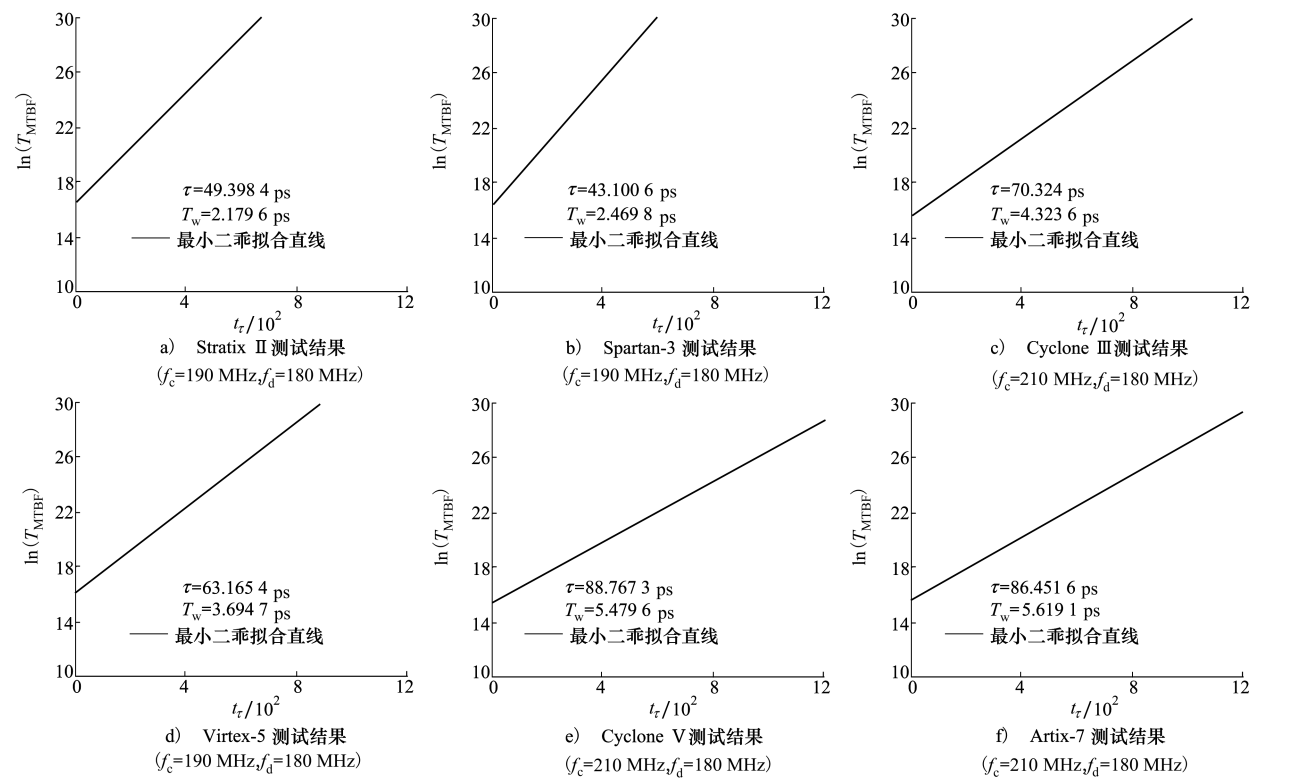


图 6 不同芯片亚稳态参数采集图

对多组数据拟合成直线,计算得到的亚稳态参数数值如表 1 所示。

表 1 被测芯片亚稳态参数值

工艺/nm	厂家	具体型号	τ/ps	T_w/ps
90	Altera	stratix II	49.40	2.18
90	Xilinx	Spartan-3	43.10	2.47
65	Altera	cyclone III	70.32	4.32
65	Xilinx	Virtex-5	63.17	3.69
28	Altera	cyclone V	88.77	5.48
28	Xilinx	Artix-7	86.45	5.62

3.2 计算评估

不同的同步策略解决亚稳态的核心原理都是增加亚稳态的解决时间,核心电路为同步单元结构。其中双级同步单元的 MTBF 计算公式如公式(1)所示。

当双级同步单元不能满足 MTBF 的需求时,可以提高同步单元的串联级数来增大亚稳态的实际解决时间。多级触发器风险评估公式(7)^[16]

$$T_{\text{MTBF}}(M) = \frac{1}{T_w \cdot f_c \cdot f_d} e^{(M-1) \cdot t_p / \tau} \tag{7}$$

式中, M 为一个同步单元中寄存器个数。

FPGA 整体的同步电路的 MTBF 值由设计中所有的跨时钟域同步单元决定。一个同步单元失效率 $F(P_n)$ 为 $1/T_{\text{MTBF}}(M)$, P_n 表示第 n 个同步单元。整个设计由亚稳态导致的失效率是把所有同步链的失效率相加,如公式(8)所示。假设 FPGA 整体设计含 N 个同步单元,其 MTBF 计算公式如公式(9)~(10)所示:

$$F(N) = F(P_1) + F(P_2) + \cdots + F(P_n) \tag{8}$$

$$T_{\text{MTBF}}(N) = \frac{1}{F(N)} \tag{9}$$

$$T_{\text{MTBF}}(N) = \frac{1}{\frac{1}{T_{\text{MTBF}}(P_1)} + \frac{1}{T_{\text{MTBF}}(P_1)} + \cdots + \frac{1}{T_{\text{MTBF}}(P_n)}} \tag{10}$$

在计算跨时钟域同步电路可靠性时,需关注两点:第一是同步单元数目的确定;第二是对数据变换速度 f_d 的确定约束。在确定同步单元数目时,要注意每种同步电路含有的同步单元的个数不同,同步电路与其含有的同步单元不是一一对应关系(如握手同步策略,异步 FIFO 同步策略)。在确定公式使

用 f_d 数值时,如果数据变换速度 f_d 未知,一般 f_d 可按照发送时钟域的时钟频率 f_w 估计,这样计算出的 MTBF 值可认为是保守的可靠性值。但在某些场景可对 f_d 进行更精确约束时,建议使用更精确的方法约束 f_d 最高变换频率,以求得更符合实际的 MTBF 值。下面举例说明如何确定计算 MTBF 所需的同步单元的个数 N 和 f_d 的值。假设一个电路设计中含有一个异步 FIFO,其指向数据存储器的地址采用二进制码编写。其中,异步 FIFO 中的写满标志判断需要把读地址同步到写时钟域,读空标志需要把写地址同步到读时钟域^[17]。当读写地址码进行跨时钟域传输时,需把二进制编码转化为格雷码。若地址总线位宽为 W ,由于读写地址都要同步,因此该异步 FIFO 中具有 $2W$ 个同步单元,即 $N = 2W$ 。确定 N 之后,需确定约束每个同步单元的 f_d 。对于地址总线为 W 的异步 FIFO,存在 2^W 个写地址,其中最高位为状态位, 2^{W-1} 个地址对应实际存储器的地址。自然二进制码转换成二进制格雷码,其法则是保留自然二进制码的最高位作为格雷码的最高位,而次高位格雷码为二进制码的高位与次高位相异或,而格雷码其余各位与次高位的求法相类似。经分析计算,第 n 位格雷码最快变换频率如公式(11)所示。

$$f_n = \begin{cases} \frac{f_w}{2^n}, & 0 < n < W \\ \frac{f_w}{2^n - 1}, & n = W \end{cases} \tag{11}$$

以 $W=4$ 为例,代入公式(11),可得到各同步单元最快变换频率表。

表 2 4 位格雷码同步单元最快变换频率表

数据位置 (从低到高)	相应同步单元最快 变换频率 f_d/Hz
第一位	$f_w/2$
第二位	$f_w/4$
第三位	$f_w/8$
第四位	$f_w/8$

依据表 2 中的各同步单元最快变换频率 f_d ,便可以使用公式(7)进行单个同步单元 T_{MTBF} 计算。之后使用公式(10)进行该异步 FIFO 的 T_{MTBF} 计算。

通过计算所得的 MTBF 值即可判断同步电路是否符合可靠性要求。如不符合,需修改同步电路设

计,增加相应同步单元内寄存器的级数。

4 结 论

本文介绍了一种适用于机载复杂电子硬件的基于传统工具的RTL级验证、板级加速测试和计算评估相结合的跨时钟域验证及可靠性评估方法,可以在设计早期发现三模场景和普通场景下的跨时钟域信号的隐患。对于含跨时钟域同步电路的电子设计,电路验证应关注跨时钟域路径上的同步电路结构,数据传输要求,目的时钟域重汇聚等问题。

对于应用在DAL A/B的机载复杂电子硬件的跨时钟域同步电路,则需在RTL级验证通过后,对亚稳态参数未知的芯片进行实际板级加速测试,最后根据测试结果计算评估其 T_{MTBF} 值,判断同步器的可靠性是否符合需求。另外,本文提供了Altera和Xilinx公司的共6款不同特征尺寸的亚稳态参数测试参考值,使验证人员能更方便快捷地进行该器件的跨时钟域可靠性评估计算。建议该方法可作为静态时序分析工作的补充,共同完成对电路的时序分析工作。

参考文献:

- [1] WU J, MA Y, ZHANG J, et al. Research on metastability based on FPGA[C]//Proceedings of 2009 9th International Conference on Electronic Measurement & Instruments, 2009
- [2] STEININGER S, SCHWENDINGER M. A systematic approach to clock failure detection[C]//Proceedings of 2019 Austrochip Workshop on Microelectronics, 2019
- [3] GINOSAR R. Metastability and synchronizers: a tutorial[J]. IEEE Design & Test of Computers, 2011, 28(5): 23-35
- [4] OMAR R, JASON H A. High-level synthesis of FPGA circuits with multiple clock domains[C]//Proceedings of 2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines, 2018
- [5] DATTA G, CONG H L, KUNDU S, et al. qCDC: metastability-resilient synchronization FIFO for SFQ logic[C]//Proceedings of 2019 IEEE International Superconductive Electronics Conference, 2019
- [6] FAA. Simple and complex electronic hardware approval guidance[S]. Order8110.105A
- [7] RTCA. Designed assurance guidance for airborne electronic hardware[S]. DO-254-2000
- [8] DORIS Chen, DESHANAND Singh, JEFFREY Chromczak, et al. A comprehensive approach to modeling, characterizing and optimizing for metastability in FPGAs[C]//Proceedings of Symposium on Field Programmable Gate Arrays, Monterey, 2010
- [9] 肖安洪, 曾辉, 秦友用, 等. 基于FPGA的“龙鳞”通信模块跨时钟域验证实践[J]. 上海交通大学学报, 2019, 53(增刊1): 84-87, 103
XIAO Anhong, ZENG Hui, QIN Youyong, et al. Cross-clock domain verification practice of naspic communication module based on FPGA[J]. Journal of Shanghai Jiao Tong University, 2019, 53(suppl 1): 84-87, 103 (in Chinese)
- [10] 张启晨. 静态形式验证在跨时钟域和复位验证中的应用[J]. 中国集成电路, 2019, 28(4): 38-43
ZHANG Qichen. Application of static formal method in CDC and reset verification[J]. China Integrated Circuit, 2019, 28(4): 38-43 (in Chinese)
- [11] 罗莉, 何鸿君, 徐炜遐, 等. 面向SOC芯片的跨时钟域设计和验证[J]. 计算机科学, 2011, 38(9): 279-281
LUO Li, HE Hongjun, XU Weixia, et al. Design and verification of clock domain crossing for SOC[J]. Computer Science, 2011, 38(9): 279-281 (in Chinese)
- [12] 梁骏, 唐露, 张明. 基于随机延时注入的跨时钟域信号验证方法[J]. 微电子学与计算机, 2014, 31(2): 1-4
LIANG Jun, TANG Lu, ZHANG Ming. A random delay injection based clock domain crossing verification method[J]. Microelectronics & Computer, 2014, 31(2): 1-4 (in Chinese)
- [13] LI Y B, NELSON B, WIRTHLIN M. Synchronization techniques for crossing multiple clock domains in FPGA-Based TMR circuits[J]. IEEE Trans on Nuclear Science, 2010, 57(6): 3506-3514
- [14] RTCA. Software tool qualification considerations[S]. DO-330-2011
- [15] JENNIFER S. Understanding metastability in FPGAs[EB/OL]. (2018-12-20) [2021-3-25]. <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/wp/wp-01082-quartus-ii-metastability.pdf? wapkw=Understanding%20Metasta>

bility%20in%20FPGAs.

- [16] BEER S, GINOSAR R, PRIEL M, et al. The devolution of synchronizers[C]//2010 IEEE Symposium on Asynchronous Circuits and Systems, 2010
- [17] CUMMINGS C E. Simulation and synthesis techniques for asynchronous FIFO design[EB/OL].(2002-06-16)[2021-02-18].
<http://www.sunburst-design.com/papers/>

Verification and reliability analysis of synchronizers in clock domain crossing

FAN Yuyang^{1,2}, DENG Zhi¹, LI Zihang^{1,2}

(1.Civil Aircraft Airworthiness and Repair Key Laboratory of Tianjin, Civil Aviation University of China, Tianjin 300300, China;)
(2.Airworthiness College, Civil Aviation University of China, Tianjin 300300, China)

Abstract: There are a large number of multi-clock domain circuits in the airborne equipment of aircraft. When data is transmitted across the clock domain, meta-stability may occur, resulting in data transmission errors and reduced circuit reliability. However, due to the occasional and non-reproducible faults caused by metastability, and the high cost of existing cross-clock domain specific verification software, cross-clock domain circuit verification in three-mode redundancy scenarios is not supported. To solve this problem, a method that combines register transfer level (RTL) validation, board-level accelerated testing and computational evaluation based on traditional tools is presented. This method can detect the cross-clock domain transmission problems in three-mode application scenarios or normal scenarios and assess potential cross-clock domain transmission risks using generic simulation tools at an early stage of design. It reduces the cost of economy and time for high safety level airborne complex electronic verification, and improves the reliability of the circuit.

Keywords: airborne electronics equipment; clock domain crossing(CDC); register transfer level (RTL) verification; Reliability

引用格式: 范毓洋, 邓智, 李子航. 机载电子跨时钟域同步电路验证及可靠性分析[J]. 西北工业大学学报, 2022, 40(2): 369-376

FAN Yuyang, DENG Zhi, LI Zihang. Verification and reliability analysis of synchronizers in clock domain crossing[J]. Journal of Northwestern Polytechnical University, 2022, 40(2): 369-376 (in Chinese)