多领域验证：
当时钟、电源和复位域发生冲突时

PING YEUNG — MENTOR A SIEMENS BUSINESS

Mentor®
A Siemens Business

WHITEPAPER

FUNCTIONAL VERIFICATION

www.mentor.com

简介

许多新的 SoC 设计必须集成大量功能并且功耗很低。一个设计可能有多个处理器内核，以平衡不同的负载情况。它可以有多个复杂的逻辑集群来处理系统内存、系统图形、I/O 接口、外设和其他功能。为了满足这些要求，设计通常以一系列时钟频率运行，并使用一组复杂的电源管理策略。它可以整合高级设计技术，例如异步时钟、比率同步时钟、时钟门控、多电压、功率切换、动态电压和频率调整 (DVFS) 等。例如，我们最近分析的一个设计具有近 20 个电源域、200 多个异步时钟域和多达 32 个复位域。但是，在处理 SoC 顶层的这些域的复杂交互之前，更好的办法是先验证 IP。我们分析了一系列复杂的 IP。一个接口 IP 具有大约 10 个电源域、20 个时钟域和 3 个复位域。另一个处理器 IP 具有 6 个电源域、7 个比率同步时钟域和 15 个异步复位域 [1]。

涉及不同电源、时钟和复位域的逻辑功能的交互可能会导致芯片失效。为确保这些领域彼此正常工作，设计团队面临多项挑战。尽管设计团队通常会在芯片级上很好地将设计划分为多个电源域、时钟域和复位域，但要理解这些域在模块级或更低级别上如何相互作用是很困难的。当设计团队将他们知之甚少的多个 IP 集成在一起时，情况变得更糟。当今设计为了节省功耗，模块会不断地开启和关闭。标准验证工具和方法无法可靠地对不同领域进行整体分析并全面验证其间的互操作。Power-Aware 仿真是一个好的开始，但功耗域、时钟域和复位域的组合太多了。通过仿真无法实现足够的覆盖率来动态验证领域间的交互。因此，静态领域分析对于彻底检查设计空间至关重要。开发多领域验证 (MDV) 就是为了解决这方面的挑战。

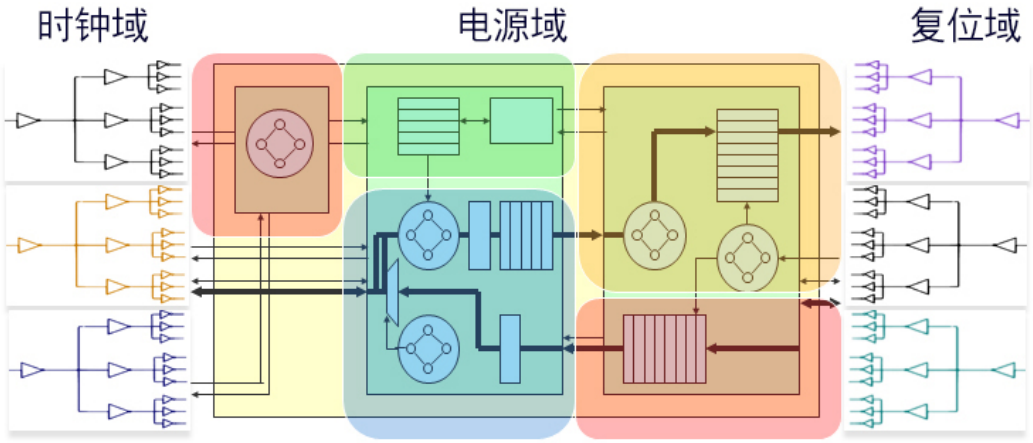

图 1.多领域验证

本文分为三个部分。

- 第一部分概述当前的电源域验证、跨时钟域验证和跨复位域验证方法。它们能对同质域进行全面验证，但未能考虑其他域的影响。
- 第二部分解释多领域验证的一般概念及其数据模型。在异构域之间执行检查首先要解决现有工具的两个限制：(1) 其他异构域（例如电源域）对时钟和复位之类的域定义信号有何影响？(2) 域控制信号（例如时钟门控信号）跨越异构域时会发生什么情况？
- 由于多领域验证是一门新学科，因此在最后一部分中，我们将介绍来自一些设计的成果，并分享一些经验教训。

各领域验证

跨时钟域

跨时钟域 (CDC) 逻辑必须遵循严格的设计原则，以实现可靠的设计功能 [5] [6]。但是，由于电路中的晶体管级模拟效应，采用标准仿真和静态时序分析技术无法验证 CDC 逻辑。

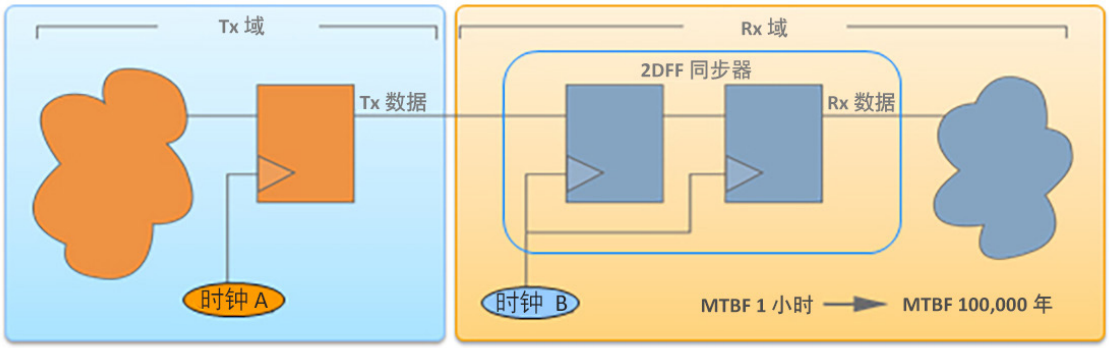

图 2.跨时钟域

为了解决这个难题，CDC 验证分为三个阶段 [7]：

1. 识别 CDC 信号并静态验证目标 CDC 方案。
2. 动态和/或形式验证 CDC 协议。此过程确保 CDC 控制和数据信号在跨过域边界和可能的同步之后保持稳定。
3. 通过亚稳态注入对设计进行仿真和/或从形式上验证再收敛结构。这是为了确保芯片能够容忍 CDC 路径中嵌入的同步器的不可预测延迟。

CDC 的结构和方案已经过充分研究。但是，当一个具有 100s 异步时钟和 1000s 时钟门控信号的设计在多个电源域中工作时，其相互作用很难预测。

跨复位域

当今的大型 SoC 设计可能集成出自多个来源的内部 IP 和外部 IP。这就给设计团队提出了重大挑战，因为模块级复位电路没有标准。系统级复位策略包含多种复位源，因而也变得越来越复杂 [8]。例如，每个电源域都需要复位信号，并且在使用之前，复位信号还必须与目标时钟域同步。

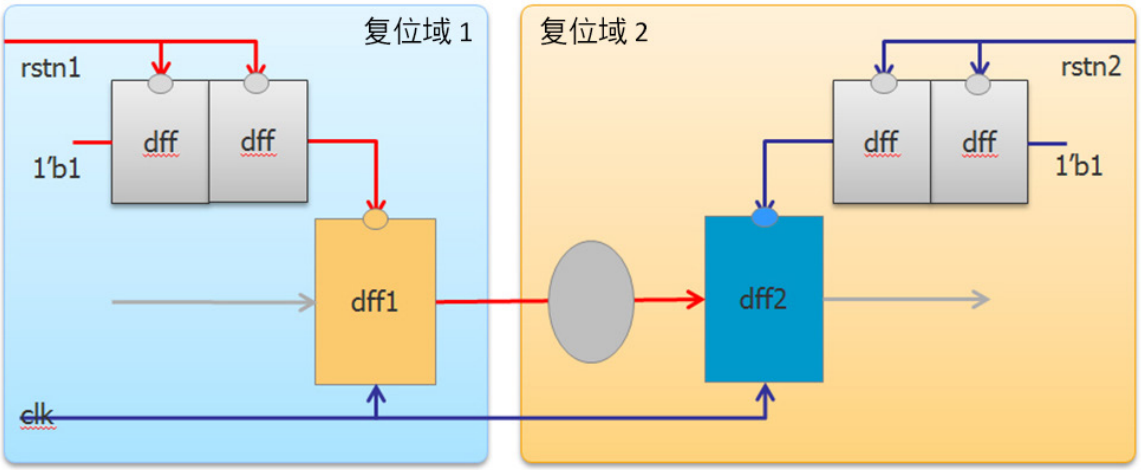

图 3.跨复位域

当同一时钟域中的一组数据相关寄存器由不同复位信号驱动时（如图 3 所示），源寄存器上的异步复位信号会导致接收寄存器发生异步事件。如果 rstn1 被断言而 rstn2 未被断言，则来自 dff1 的异步输出数据可能导致 dff2 出现亚稳态。这就是我们关注的跨复位域情况。

跨复位域验证可以分为三个部分 [9]：

1. 使用静态分析来查找和构建设计中所有复位信号的树结构。复位可分为同步复位或异步复位，以及高电平有效或低电平有效。
2. 可以不依赖门级仿真，而是使用支持芯片级精度 X 传播语义的 RTL 仿真来查找与未初始化设计元素有关的问题。
3. 形式验证可用来验证复位树的许多方面，包括所有复位源到其预期目的地的连通性，以及检测带有未知逻辑值的正确复位存储元件的损坏。

为了降低功耗，设计团队会给设计增添更加复杂的电源域。复位信号的活动（作为电源序列的一部分）已大幅增加。很难预测所连模块上复位信号的可能交互。

跨电源域

利用统一功耗格式 (UPF) 标准 [2]，项目团队可以捕获设计的功耗意图。功耗意图规范包括电源域、电源网络、电源结构和电源状态。验证目标是检查电源管理元件的功能以确保其正常工作。每个子系统都可以独立地开启、转变功耗模式和关闭。

Power-Aware 验证工具可以检查跨电源域信号上隔离单元和电平转换器的布局。隔离单元的加电和掉电序列将由功率控制器控制。如果使用了储值寄存器，则还需要验证保存和恢复操作。为了指导验证团队应对这一新挑战，[3] 中提出了一个电源验证清单。该清单聚焦于电源域切换、隔离单元、存储器和寄存器储值的各个方面。

随着设计中电源域的数量不断增加，电源域给设计和验证均带来了沉重负担。通过支持 UPF 标准，我们让设计团队得以在 RT 级别尽早验证其实现。

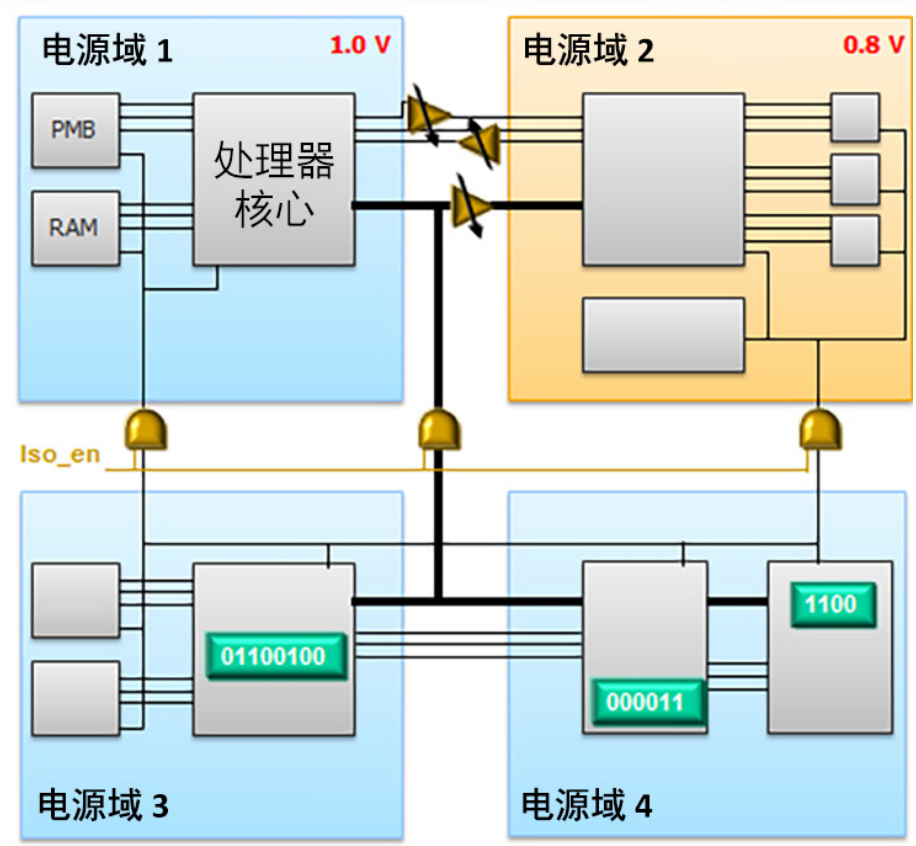

图 4.跨电源域

多领域验证

随着设计变得越来越复杂，异构域之间的交互越来越多，一次验证一个域是不够的。为了解决电源域的引入问题，一些 CDC 验证工具 [10] [11] 开始利用 UPF 规范中的电源域信息。它有助于识别和验证跨时钟域的功率控制信号。这是验证域间交互的正确步骤。但是，它仍然缺乏设计的完整域特定视图。因此，我们要向前迈出一大步，构建一个新的验证环境。所有域信息都会被永久提取并表示。这将使环境能够全面验证所有域交互。与此同时，可以按需调出来自其他域的额外信息，以便细化和了解所识别情况的严重性。

我们将这种方法命名为多领域验证 (MDV)。它从统一功耗格式 (UPF) 规范中提取电源域信息，从时钟树中提取时钟域信息，从复位树中提取复位域信息。表示控制不同域的逻辑功能同样重要，包括功率控制信号、时钟门控信号和复位使能信号。为了真正了解域间交互，我们必须检查控制信号的功能。例如，如果关闭一个寄存器的时钟或寄存器处于储值模式，该寄存器将非常稳定。因此，来自该寄存器的跨时钟域或跨复位域将不是问题。如图 5 所示，每个域有三类信息：域结构信息、域控制逻辑和跨域信号。

	域结构	域控制	跨域
域验证	结构验证	控制验证	跨域验证
电源域	电源网络	电源切换、隔离和储值控制	跨电源域 (PDC) 隔离、储值、电平转换
复位域	异步和同步复位、树结构、连通性	复位同步、极性、控制和门控条件	跨复位域 (RDC)
时钟域	异步和同步时钟、树结构、连通性	时钟分频、控制和门控条件	跨时钟域 (CDC) 同步器、2DFF、FIFO 和握手结构

图 5.域控制和跨域信号

如图 6 所示，多领域验证过程沿垂直方向分为三个阶段：域结构验证、域控制验证和跨域验证。这种垂直的逐阶段（异构）方法很独特，它不是一次验证一个同质域。用户可以首先专注于全局。例如，如果电源域规范不正确，或者时钟树的定义不明确，那么检查跨电源域或跨时钟域信号所产生的细节违规将不会有成效。用户首先应专注于完善 UPF 规范、时钟树和复位树。一旦完成早期阶段，用户便可进入后一阶段。这样，后面的阶段便可考虑并利用先前阶段中执行的所有信息、扩充和细化。

图 6.多领域验证的三个阶段

域结构验证

多领域验证不是一次验证一个域的结构，而是同时提取、表示、验证电源域、时钟域和复位域的结构。它使我们能够了解其他域的存在如何影响域结构（例如时钟树和复位树）。

	电源	复位树	时钟树
电源域		多个电源域中的复位树	多个电源域中的时钟树
复位域	多个复位域中的电源		多个复位域中的时钟树
时钟域	多个时钟域中的电源	多个时钟域中的复位	

图 7.不同域的结构

例如，图 7 显示了若干具有挑战性的场景：

1. 多个电源域中的复位树 – 如果复位信号是从一个始终开启的域中产生，并在其他各种电源域中消耗，那么这种情况是很理想的。然而，如果复位信号是从一个电源域产生并扇出到另一个电源域，那么这种情况具有潜在的风险。

2. 多个电源域中的时钟树 – 与复位树类似，如果时钟信号是从一个始终开启的域中产生，并在其他各种电源域中消耗，那么这种情况是很好的。如果时钟信号是从一个电源域产生并扇出到另一个电源域，那么这种情况存在风险。
3. 多个复位域中的时钟树 – 会有潜在的异步跨复位域问题。此外，设计的一部分可以复位，而另一部分不复位。正确初始化这样的设计可能具有难度。

设计中还有一些常见场景。

1. 多个复位域中的电源 – 电源网络覆盖多个复位域是很正常的。
2. 多个时钟域中的电源 – 电源网络覆盖多个时钟域是很正常的。
3. 多个时钟域中的复位树 - 复位树用于多个时钟域是很正常的。但是，复位信号在使用之前必须同步到各时钟域中 [12]。复位信号被异步断言，但必须相对于目标时钟域同步移除。

结构验证的目的是确保电源网络、时钟信号和复位信号正确分配到设计的不同部分。此过程会对域进行着色，对域边界进行蚀刻，并计算域的数量。这样，对于设计中的每个设计元素（例如寄存器、存储器阵列和模块），我们将知道与之关联的电源域、时钟域和复位域。

域控制验证

功率切换、频率切换和时钟门控是低功耗设计的常见做法，因此验证域控制信号也很重要。从图 5 可以看出，域控制信号包括：功率开关、隔离和储值控制信号；时钟选择、控制和门控信号；复位控制和门控信号。功率控制信号由功率控制器产生。时钟控制信号可以来自多个源。对于动态电压和频率切换，时钟频率选择信号将来自功率控制器。对于可测试性设计，扫描和功能时钟选择信号将来自测试控制器。其他内部时钟由工作模式决定，并可以通过软件编程。它们由配置寄存器直接或间接控制。在局部，驱动数据路径元件的时钟可以通过使能信号控制以节省功耗。检查完所有扇入时钟树的控制逻辑之后，控制时钟的逻辑网络很有可能比时钟树本身还复杂。

域控制信号有两个重要方面需要验证：

1. 域相关性 – 必须确保控制信号：
   a. 来自始终开启的电源域或位于同一电源域
   b. 来自一些稳定的寄存器，或来自同一同步时钟和复位域
2. 功能 – 为了让某个域正确加电或掉电，必须按照一个精确序列将电源、时钟和复位信号断言和移除。为此，相应的控制信号、功率开关、时钟和复位门控逻辑在正确的时间必须具有正确的值。

域控制逻辑，尤其是时钟控制逻辑，可能非常复杂。要仿真所有可能的功能场景和极端情况是不可能的。因此，形式连通性验证是验证时钟树结构基于条件的连通性的自然选择。

跨域验证

完成域结构验证之后，我们就会知道电源、时钟和复位域如何与设计中的每个设计元素（例如寄存器、存储器阵列和模块）相关联。跨域分析将检查设计中所有与数据相关的元素。

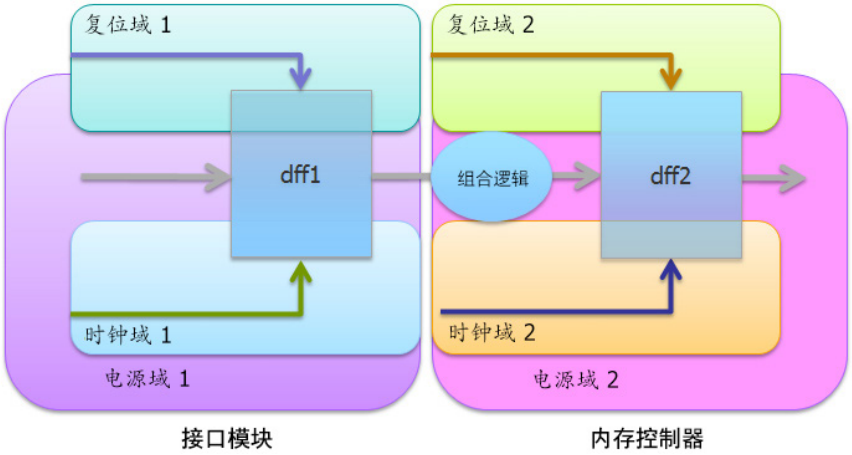

图 8.跨电源、时钟和复位域

域控制验证将验证设计元素的电源、时钟和复位域。如有任何类型的跨域（电源、时钟或复位），可以执行传统跨域验证来确保跨域得到正确实现。利用第二部分中介绍的现有同质域验证技术非常有益。跨时钟域和其他域验证工具已经很成熟，并具有完善的调试环境。一旦确立了跨域验证要求，便可将其在局部部署以验证模块之间的所有跨域。

例如在图 8 中，一个接口模块连接到内存控制器。在某种工作模式下，如果接口模块完全断电，则只需在接口模块和内存控制器之间执行跨电源域分析。不需要跨时钟域和跨复位域分析。另一方面，如果接口模块和内存控制器位于同一电源域，则将检查其时钟域和复位域，以确定是否需要跨时钟域或跨复位域验证。

结果

原型多领域验证环境已拼接在一起。我们已对一些客户设计应用了多领域验证方法。验证是在 RT 级别使用 UPF 规范执行的。使用 UPF 进行验证的一个主要好处是电源结构尚未固化，可以进行任何修改（确实发生了修改）而不会对实施进度产生重大影响。下面的表 1 总结了三个模块的结果。通过多领域验证，工具能够正确识别所有电源、时钟和复位域。用户可以通过为控制信号指定显式值，或通过指令显式地对时钟和复位信号进行分组，来修改每个域内的电源网络分组、时钟和复位树分组。

域数量	模块 1	模块 2	模块 3
电源域	2	3	4
异步时钟域	3	4	16
异步复位域	2	11	9

跨域树数量	模块 1	模块 2	模块 3
跨电源域的时钟树	2	2	6
跨复位域的时钟树	2	3	5
跨电源域的复位树	1	2	7
跨时钟域的复位树	2	5	16

跨域控制信号数量	模块 1	模块 2	模块 3
来自不同电源域的时钟控制信号	0	4	5
来自不同电源域的复位控制信号	0	2	13
来自不同时钟域的功率控制信号	2	4	6

跨域数据信号数量	模块 1	模块 2	模块 3
跨电源域	5/0	142/0	441/0
跨时钟域	20/6	5845/4047	10956/3074
跨复位域	3/0	25768/129	225/15

m/n：评估数/违规数

表 1. 多领域验证总结

模块 1 是具有两个电源域的外设接口控制器。时钟树和复位树跨越电源域几次，主要是从始终开启的电源域进入其他可切换电源域。当时钟树跨越复位域时，这意味着使用不同复位信号来初始化同一时钟域内的寄存器。由于某些寄存器相互依赖，因此导致在表格后面报告了三个跨复位域。跨电源和时钟域的复位树一般是设计使然。这意味着不同的时钟或电源域中使用相同的复位树。但是，如果电源域需要相对于设计中的其他域独立复位，那么这会是一个问题。由于此模块的时钟和复位信号是在外部生成，因此没有用于它们的控制信号。

另一方面，功率控制信号存在问题。从图 9 所示的原理图可知，一个隔离单元用来隔离可切换的电源域与始终开启的电源域。这两个电源域属于同一时钟域。然而，隔离信号来自其他时钟域（例如功率控制器时钟域）。结果是，隔离信号将一个跨时钟域信号引入设计中。为了正确设计这种电路，隔离信号在使用之前应与 RX 时钟同步。因此，对所有输出端口使用单个隔离信号很容易造成此问题。

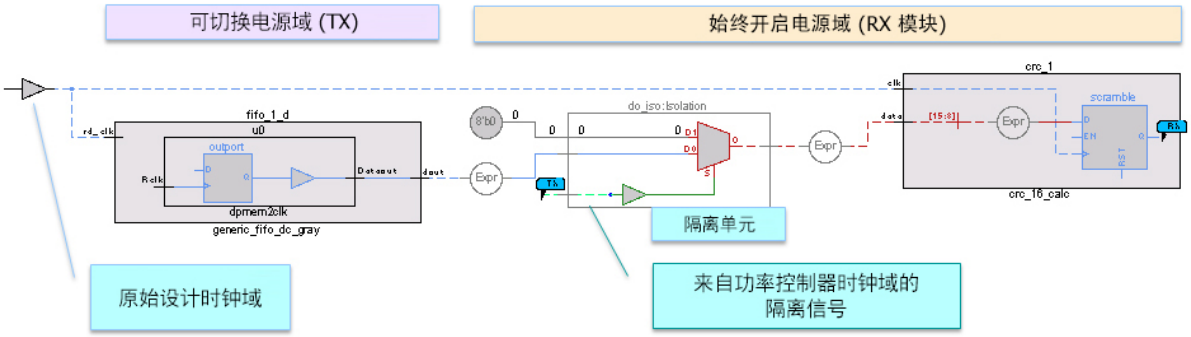

图 9.跨时钟域电源隔离信号

我们观察到的另一个有趣情况是来自不同电源域的 CDC 路径的再收敛，如图 10 所示。当来自不同模块的数据在控制器上重新收敛时，就会发生这种情况。我们知道，再收敛对 CDC 验证而言是一个问题。电源域给该问题增加了一个维度。如果可切换电源域关闭，则 CDC 路径将不会再收敛。当开启时，我们需要认真考虑再收敛问题。

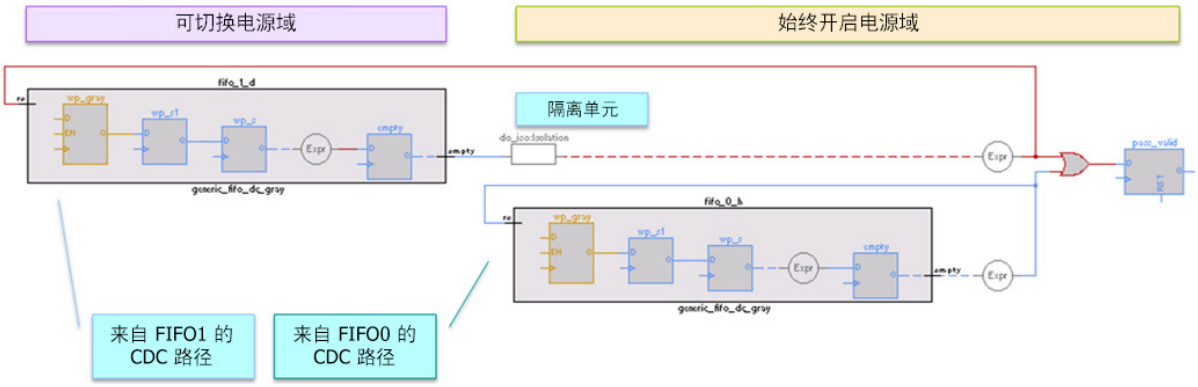

图 10.来自不同电源域的 CDC 路径再收敛

模块 2 是一个设计的功能控制器。它有数个时钟域和电源域，但它会给局部控制结构和设计的其他模块生成大量复位信号。对于此模块，我们聚焦于验证复位结构。电源域和复位信号密切相关。每个可切换电源域都应有一个复位信号，以在每次上电时初始化存储元件。但是，当数据从一个电源域流向另一个电源域时，如果寄存器位于同一时钟域内，不建议使用不同的复位信号来初始化寄存器。在图 11 中，可切换电源域中的 RX 模块需要一个复位信号。设计人员没有使用 TX 模块中的 reset1，而是同步了 RX 模块的外部复位信号 reset2。结果，从 TX 模块到 RX 模块的数据路径使用了不同的复位信号，进而引入了不需要的跨复位域路径。

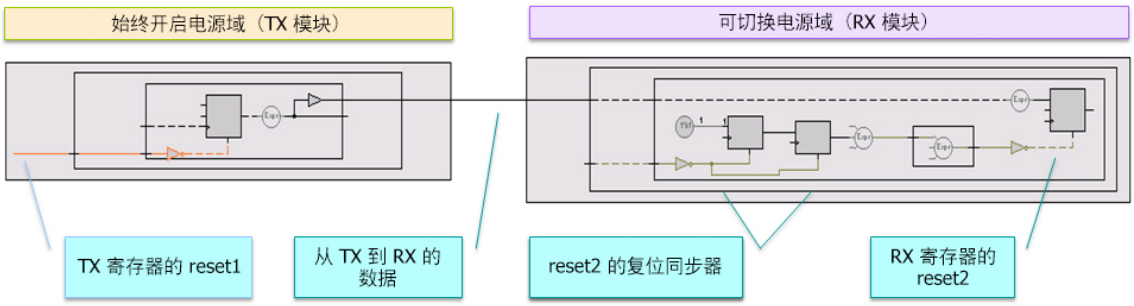

图 11.两个电源域之间的跨复位域

除了时钟和复位信号之外，其相应的控制和门控信号也非常重要。当今设计中的时钟门控和复位控制信号越来越多，这些信号应与时钟和复位树一起加以表示和验证。在图 12 中，外部复位信号已同步并用于 RX 模块。此复位信号可通过其他电源域中的 TX 模块的控制信号来禁用。正常操作中，一旦 RX 模块已正确初始化并进入功能模式，RX 模块中的复位信号就会被禁用。但是，当 RX 模块断电并再次上电时，禁用的复位信号无法用于初始化设计。这是设计团队非常担忧的问题。因此，对复位树和相关控制信号进行了广泛的连通性验证。目的是确保所有生成的复位信号都可以在期望的条件下置为有效。除了使用形式化方法来验证连通性之外，生成用于仿真的断言也非常有用。当不同模块上电和断电时，利用 Power-Aware 仿真可以验证复位树和控制信号，就像在目标系统环境中一样。

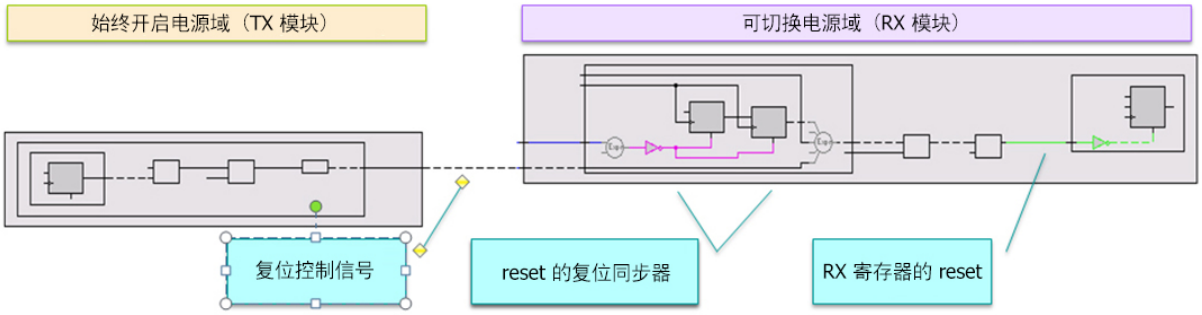

图 12. 来自不同电源域的复位控制信号

模块 3 是用于多个处理器内核的互连控制器的一部分。设计有 10 个主时钟信号。有些时钟信号是特定于接口的，仅进入特定接口模块。有些系统级时钟信号则分布广泛。设计的顶层位于始终开启的电源域中，因此从顶部到可切换电源域的大多数时钟树都不是什么问题。我们特别担心的是从一个可切换电源域进入另一个可切换电源域的时钟树。仔细检查结果之后，我们很高兴这种情况没有发生。

然而，复位信号不是这样。设计有三个主复位信号。设计内部从它们产生内部复位信号、热复位信号和同步复位信号。从顶层开始，复位信号被驱动到各电源域中，并且同时分别同步到各时钟域中。检查完工具报告的问题之后，我们发现了一些情况，即复位信号跨越电源域。如图 13 所示，RX 模块的两个复位信号正在通过一个可切换电源域。IP 模块是一个数据计算单元。它从顶层模块获取复位信号，输入复位信号也用于驱动接收数据路径的两个输出复位信号。潜在问题是：如果可切换电源域掉电，便再也无法复位 RX 模块。从原理图可以非常清楚地看出，RX 模块不需要从 IP 模块获取复位信号，而是可以直接从顶层获得复位信号。当我们与设计团队一起审查这种情况时，他们告诉我们他们不知道该 IP 模块的功能。他们使用来自 IP 模块的复位信号来确保接收数据路径将与 IP 模块中的计算同步。

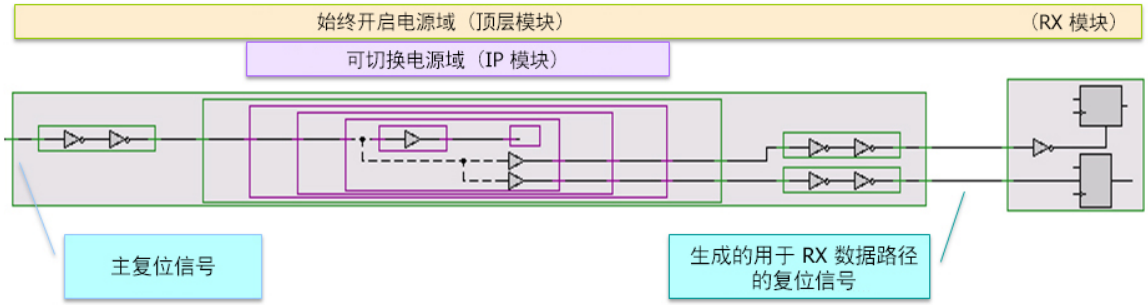

图 13. 跨不同电源域的复位信号

结语

本文提出的多领域验证方法可在 RT 级别利用 UPF 规范并行验证电源、时钟和复位域。它既能分析横跨同质域的逻辑，又能分析横跨异构域的逻辑。将这三个域一同进行表示和验证，可以更直观地了解其间的交互，从而在设计周期中尽早预判可能的域问题。多领域验证过程分为三个阶段：域结构验证、域控制验证和跨域验证。这种分而治之的方法使我们能够专注于多领域验证问题的不同方面。尽管我们必须为多领域结构和控制验证开发新算法，但我们可以利用既有同质工具来执行正常的跨时钟、电源和复位域验证。采用多领域验证，现在可以完全放心地验证所有域间问题。

参考文献

[1] "ARM® Cortex®-A17 MPCore Processor Technical Reference Manual Revision: r1p0", http://infocenter.arm.com.

[2] Unified Power Format, "1801-2013 IEEE Standard for Design and Verification of Low-Power Integrated Circuits", IEEE.

[3] Freddy Bembaron, Sachin Kakkar, Rudra Mukhejee, Amit Srivastava, "Low Power Verification Methodology Using UPF", DVCon 2011.

[4] Amit Srivastava, Madhur Bhargava, "Stepping into UPF 2.1 world: Easy solution to complex Power Aware Verification", DVCon 2014.

[5] Ran Ginosar, "Metastability and Synchronizers, A Tutorial", IEEE Design and Test 2011.

[6] Cliff Cummings, "Clock Domain Crossing (CDC) Design & Verification Techniques Using SystemVerilog", Synopsys User Group Meeting (SNUG) 2008.

[7] Chris Kwok, Vijay Gupta & Tai Ly, "Using Assertion-Based Verification to Verify Clock Domain Crossing Signals", DVCon 2003

[8] Kaowen Liu, Penny Yang, Jeremy Levitt, Matt Berman, Mark Eslinger, "Using Formal Techniques to Verify System on Chip Reset Schemes", DVCon 2013.

[9] Chris Kwok, Priya Viswanathan, Ping Yeung, "Addressing the Challenges of Reset Verification in SoC Designs", DVCon 2015.

[10] Anindya Chakraborty, Naman Jain, Saumitra Goel, "Power Aware CDC Verification at RTL for Faster SoC Verification Closure", DVCon India, 2014.

[11] Kurt Takara, "Next-generation Power Aware CDC Verification – What have we learned", DVCon 2015

[12] Cliff Cummings, Don Mills, Steve Golson, "Asynchronous & Synchronous Reset Design Techniques", SNUG 2003 Boston.

本文最初于加利福尼亚州圣何塞 DVCon（2015 年 3 月）大会上发表。

如需最新信息，请致电联系我们，或者访问： **www.mentor.com**

©2020 Mentor Graphics Corporation，保留所有权利。本文档包含 Mentor Graphics Corporation 的专有信息，只能由原始接收者出于内部商业目的全部或部分复制本文档，前提是在所有副本中都包含此完整声明。接受本文档即表示接收者同意采取一切合理措施，防止未经授权使用这些信息。本文档中提及的所有商标属于其各自所有者。

公司总部
Mentor Graphics Corporation
8005 S.W. Boeckman Road
Wilsonville, Oregon 97070 USA
电话：+1-503-685-7000
传真：+1-503-685-1204

销售和产品信息
电话：+86-21-6101-6301
sales_info@mentor.com

上海
明导（上海）电子科技有限公司
上海市浦东新区杨高南路 759 号
陆家嘴世纪金融广场 2 号楼 5 楼
邮编：200127
电话：+86-21-6101-6301
传真：+86-21-5047-1379

北京
明导（上海）电子科技有限公司
北京办事处
北京市南礼士路 66 号
建威大厦 1512 室
邮编：100045
电话：+86-10-5930-4001
传真：+86-10-6808-0319

深圳
明导（上海）电子科技有限公司
深圳办事处
深圳市福田区金田路 3088 号
中洲大厦 24 楼 2401 室
邮编：518040
电话：+86-755-8282-2700
传真：+86-755-8826-7750

Mentor®
A Siemens Business

MGC 10-20 TECH17240-w-CN