arXiv:2611.30631v1 [cs.AR] 23 Nov 2026

面向重构片上电源控制电路的可验证的逻辑—物理契约

Sabrina Yarzada、Paul Yi-Chia Chen、Yuanhan Li、Jeongeun Kim、Yujie Cai 和 Christopher Torng 南加州大学电气与计算机工程系 洛杉矶，加利福尼亚州，美国

摘要——**近期文献提出，可将彼此独立的硬件实验部署在同一块芯片上，从而实现可扩展且高性价比的硅原型。在这一框架下，包括低功耗控制机制在内的专用硬件功能可以作为可复用的片上微服务提供。然而，这要求建立明确的契约，将数字请求与物理行为连接起来。我们提出一种**可检查的逻辑—物理契约形式化，**其中包含**物理契约模型，**通过形式化验证的数字保证和物理验证的完成条件，描述客户端与提供方之间的服务完成过程。我们介绍了*Lightswitch*，一种概念验证片上电源控制微服务。我们评估了台积电 28纳米工艺下的版图后设计，并展示了可检查契约如何提供形式化保证。**

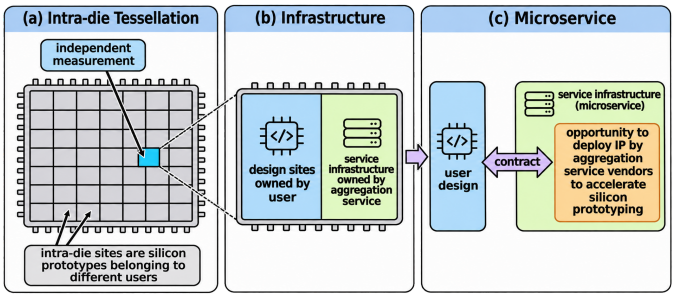

图 1. **用于硅原型的片上微服务。**（a）独立用户位置共享同一芯片。（b）用户设计与共享基础设施共存。（c）可复用微服务通过定义明确的契约提供功能。

I. 引言

硅原型对于在真实物理条件下评估硬件设计至关重要，但制造成本和设计工作量使得及早且频繁地获得硅片反馈变得困难 [1]。传统的多项目晶圆（MPW）方法在不同设计之间分摊制造成本 [2],[3], [4], [5],，但每个项目仍然面临大量的集成工作、实现开销和成本。

近期关于硅查询架构的研究提出了一种新能力：可在单个芯片上的片内镶嵌结构中，将相互独立的硬件实验与其他实验并置 [6]。图 1(a) 展示了最终的全芯片集成如何由外部片上聚合服务单独处理，该服务类似于多项目晶圆服务 [7], [8], ，其设计理念是利用先前工作的研究成果，在整个片内镶嵌结构中提供研究级时序和高速多吉赫兹时钟分发，同时实现实用且可由构造正确性保证的物理集成优势。

除了共享芯片面积之外，这类架构还创造了共享硬件功能的机会。电源控制、时钟管理和监控等通用服务可以只实现一次，然后通过可复用接口向各个实验位置提供 [9]。如图 1(b) 和 (c) 所示，用户设计与共享服务基础设施分别由不同的参与方所有。这种分离要求通过明确的契约来定义客户端的预期以及提供方的保证 [10], [11]。对于与物理硬件交互的服务，这些保证必须将数字接口行为与可检查的物理条件联系起来。

一个核心挑战在于，同一芯片上集成了由不同方设计的不同设计，并定义什么构成物理服务完成。仅凭数字验证无法根据有限的观测建立连续的物理行为。因此，逻辑–物理契约必须包含一个 物理契约模型 ，用于定义哪些观测足以满足客户端的要求。例如，该模型可以规定电压阈值、测量位置和观测时间。客户端和提供方将这一模型作为契约的一部分达成一致，从而明确数字确认的物理含义。不同模型可以在物理覆盖范围、响应延迟和实现成本之间进行权衡。最终形成的保证相对于双方同意的模型及其运行假设成立。

电源控制体现了这一挑战。位置可以通过数字接口请求打开或关闭，但操作完成取决于模拟电源轨行为。上电期间，开关电源必须通过功率开关充电，位置才能安全恢复运行。这一转换取决于负载电容、寄生效应、工艺-电压-温度（PVT）变化和开关活动。固定的等待时间可能会不必要地延迟确认，而过早确认则可能使位置暴露于尚未稳定的电源电压。此外，同时启用过多功率开关可能引发浪涌电流和电源扰动，从而影响芯片上的其他位置 [12], [13], [14]。

以往工作通过功率门控唤醒调度 [15], [16], 、基于环形振荡器（RO）的电源监控 [17], [18], [19], 以及分阶段电源切换 [20], [13]。这些技术为电源控制提供了构建模块，但并未建立将数字确认与客户端接受的模型相连接的明确协议

与物理完成之间的协议。

本文提出了一种面向片上微服务的可检查逻辑–物理契约制定。其核心洞见是，服务完成的物理含义必须明确纳入契约之中。该制定将约定的物理契约模型、数字服务保证以及连接二者的证据分离开来。形式化验证检查控制器是否遵循其数字保证，而物理表征则验证传感器决策与约定物理模型之间的关系。通过这些工作，在指定运行条件下，数字确认与物理行为之间建立了可检查的联系。

本文还介绍了*Lightswitch*，这是一种电源控制机制，也是首个概念验证片上微服务；我们利用它详细研究所提出的契约制定。Lightswitch 最初建立在 Chipstitch 的 [6] 基础站点架构和基于外围的电源切换之上。随后，Lightswitch 提供了通用的请求–确认接口，并对确认、隔离、切换顺序和故障处理进行了形式化检查。经过物理表征的环形振荡器（RO）哨兵电路可检测开启就绪状态，经过表征的放电时序则确定关闭完成，而分阶段周界切换控制唤醒扰动。可配置的感测和切换机制使我们能够在具有不同物理要求的各个位置研究该契约制定。

本文有三项贡献：

- **逻辑–物理契约制定**。一种可检查的契约，其中包含客户端认可的物理契约模型，将经过形式化验证的数字保证与经物理验证的完成条件连接起来。
- **一种概念验证微服务**。Lightswitch 通过通用客户端接口，利用基于环形振荡器的就绪状态检测、经表征的关闭完成条件和分阶段周界切换来实现该制定方案。
- **对契约验证与权衡的评估**。采用三个尺寸各异的台积电 28纳米位置，研究契约正确性、不同物理模型、确认延迟、电源完整性和实现开销。

据我们所知，我们是首个为片上微服务开发形式化契约机制的团队，旨在为由不同各方集成在同一芯片上的不同设计建立逻辑–物理契约保证。

II. 逻辑–物理微服务契约

本节介绍一种面向片上微服务的逻辑-物理契约表述。该契约定义了客户端和提供方的职责、双方约定的物理完成含义，以及核验每项保证所需的证据。Lightswitch 是一个以电源控制为例的具体实例。

A. 客户端与提供方职责

芯片上的微服务将客户端的请求与提供方执行这些请求的责任分离开来。在设计阶段，客户端指定其需求，并接受一个定义

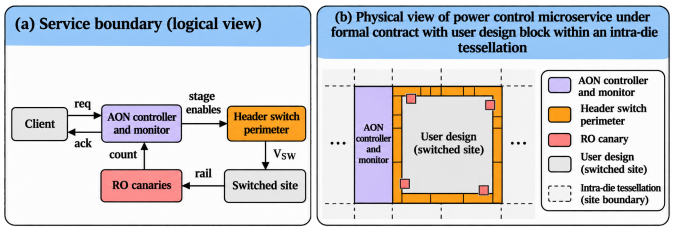

图 2. Lightswitch 架构。(a) 客户端与提供方之间服务边界的逻辑视图。(b) 片内镶嵌结构中，围绕用户设计的电源控制微服务的物理视图。

表 I. LIGHTSWITCH 客户端与提供方职责。

阶段	客户端职责	提供方责任
设计	规定 site 要求并接受物理合约模型。	定义，验证 物理模型；实现开关-控制、感测和电源意图。
运行时	发出有效的开/关请求并等待相应的确认。	控制转换，维持—持隔离，检查就绪—状态，报告状态或故障。

物理服务完成的模型。提供方实现并验证服务。在运行时，客户端发出请求，而提供方报告服务完成或故障。

图 2 展示了 Lightswitch 的抽象视图。一个实验占用一个受电源域开关控制的电源域。平台包含一个常开（AON）控制器、外围头部开关和环形振荡器（RO）哨兵电路。通过请求-确认接口 [21], , 客户端请求切换到电源状态 $q \in \{$关闭，开启$\}$，并接收确认和状态信息。提供方负责管理切换、电源轨监控和故障处理。

表 I 总结了 Lightswitch 的职责。客户端和提供方在集成期间就物理完成要求达成一致。在运行时，提供方会在确认前检查这些要求。收到开启确认后，客户端会执行所需的时钟与复位序列，然后启动实验。

B. 物理契约模型与保证

逻辑–物理微服务契约定义为 $\mathcal{C} = (A,\ G,\ \mathcal{E},\ \mathcal{M})$，其中 A 规定客户端和环境的假设，G 定义提供方保证，$\mathcal{E}$ 规定受支持的运行范围，而 $\mathcal{M}$ 则是物理契约模型。该模型定义了客户端和提供方一致认可、足以确认服务完成的物理观测。

对于操作 q，令 $R_{\mathcal{M}}(q,t)$ 表示在约定物理模型下的完成。核心契约保证为

$$A \wedge ack_q(t) \implies R_{\mathcal{M}}(q,t), \tag{1}$$

对于 $\mathcal{E}$ 范围内的运行条件，从而形式化数字确认与服务完成的物理含义之间的联系。

对于 Lightswitch，开启完成要求开关电源稳定至可接受电压。给定的物理契约模型将这一含义形式化。令 $V_{\mathrm{SW}}(x,\ t)$ 表示

位置 x 和时间 t 处的切换电源轨电压。物理模型可以指定观测位置 $\mathcal{X}$、采样时间 $\mathcal{U}_t \subseteq [t-\tau, t]$、稳定间隔 τ 以及最小电压 $V_{\min}$，并制定双方约定的开启就绪条件

$$R^{\mathsf{ON}}_{\mathcal{M}}(t) = \bigwedge_{x\in\mathcal{X}} \bigwedge_{u\in\mathcal{U}_t} [V_{\mathrm{SW}}(x,u) \geq V_{\min}]. \tag{2}$$

图 2(b) 展示了可观测位置的抽象视图$\mathcal{X}$，具体以环形振荡器金丝雀绘制，但该契约并不要求必须采用这种实现方式。提供方通过物理表征选择候选位置和采样时间，客户端则认可由此得到的模型。采样在空间或时间上无需均匀分布。例如，客户端可以接受较少的观测位置，以降低感测开销和响应延迟。满足该模型即可证明在约定的观测位置上已就绪。

对于 Lightswitch 关闭确认，约定的完成条件要求开关已禁用、隔离状态得以维持，并经过经表征的放电间隔。该契约还规定了电源完整性限制。令 D_{AON} 表示源极/AON 电源压降的最大值，S_I 表示电源电流转换速率的最大值。约定的要求为

$$D_{\mathrm{AON}} \leq D_{\max}, \qquad S_I \leq S_{\max}. \tag{3}$$

响应延迟相对于约定的完成模型进行测量。令 c_{oracle} 表示模型首次满足时的控制器时钟沿，c_{ack} 表示确认沿。额外等待时间为

$$\Delta = c_{\mathrm{ack}} - c_{\mathrm{oracle}}. \tag{4}$$

负值 Δ表示按照约定的模型发生了提前确认，正值 Δ则表示额外等待时间。

客户端可在设计时选择不同的物理契约模型，在保真度、覆盖范围、延迟和成本之间进行权衡，同时以数学形式表述，以确保严谨证明。

C. 检查数字与物理保证

该契约通过两项义务进行检查。数字验证用于确认，确认信号是在实现的完成指示之后发出的。物理验证用于检查，在受支持的运行条件下，该指示是否满足约定的物理契约模型。

在 Lightswitch 中，开启请求的完成指示是同步传感器就绪信号 Q_θ。控制器只有在该信号有效时才能发出确认，而感测机制只有在满足约定的开启完成模型时才能指示就绪状态：

$$\underbrace{ack_{\mathsf{ON}} \Rightarrow Q_\theta}_{\text{RTL proof}}, \qquad \underbrace{A \wedge Q_\theta \Rightarrow R^{\mathsf{ON}}_{\mathcal{M}}}_{\text{physical validation}}. \tag{5}$$

这两项义务均适用于支持的工作范围。第一项通过对确认、开关时序、隔离、故障处理和恢复进行 RTL 形式验证来检查。第二项则通过将传感器决策与在约定位置和时间进行的独立电源轨电压测量结果进行比较来评估。不同的 RO 配置可以根据同一个物理契约模型进行验证。

对于关闭确认，形式化验证会检查开关是否已关闭、隔离是否得到维持，以及配置的放电间隔是否已结束。物理表征则会在约定的运行条件下验证放电时序。这些检查共同将数字保证与已接受的物理契约模型联系起来。

III. Lightswitch 架构与配置

Lightswitch 是一种概念验证电源控制微服务，用于研究逻辑-物理契约表述。它通过分阶段周界切换和基于环形振荡器的就绪检测来实现该契约。配置感测和切换参数，可满足不同的物理契约模型，同时保留通用的客户端接口。

A. 分阶段周边开关控制

Lightswitch 通过布置在各位置周边的头部开关来控制电源传输。这些开关将共享电源连接到该位置的内部电源轨，并划分为可独立控制的多个区段。上电期间，AON控制器依次启用各区段，使充电电流分散到一段时间内。可配置的上电分阶段控制可限制峰值浪涌电流，并减少对共享电源的扰动 [13], [15]。

切换序列由 $\pi = \{(w_k,\ \delta_k)\}_{k=1}^{K}$ 描述，其中 w_k 是第 k 级启用的开关宽度，δ_k 是进入下一级之前的延迟。头部开关的数量、尺寸和布局决定了可用的电流容量，而级调度控制启用该容量的速度。这些选择会影响电源轨恢复时间、电源完整性和实现开销。

分阶段控制会在唤醒时间与电源扰动之间引入权衡。增加级数可以降低峰值电流，但会增加唤醒延迟；增大开关则能降低电源电阻，但代价是面积增加，且可能产生更高的浪涌电流。Lightswitch 可根据每个位置的需求调整这些参数，而无需更改客户端接口。

B. 基于环形振荡器的就绪检测

Lightswitch 使用环形振荡器哨兵检测物理电源轨的就绪状态，因为它们的频率会随局部电源电压变化，其跃迁也可以通过数字方式测量 [18]。每个环形振荡器均由开关电源供电，AON监视器会在固定的采样窗口内计数其振荡次数。分布式哨兵可用于估算一个位置内不同位置的就绪状态。

一个关键挑战在于区分电压变化与工艺和温度变化，因为后者同样会影响环形振荡器频率。Lightswitch支持两种感测方法。单环形振荡器感测将每个哨兵的绝对计数值与经过校准的阈值进行比较。双环形振荡器感测使用由AON电源供电的参考 RO 对这些计数值进行归一化

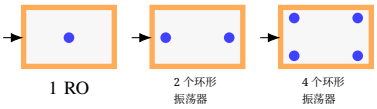

图 3. 一个、两个和四个分布式环形振荡器哨兵（蓝色）及周边电源开关（橙色）。可选的 AON参考环形振荡器支持归一化。

，以减少共享变化。对于采样窗口 i 中的哨兵 k，

$$x_i[k] = \begin{cases} n_i[k], & \text{single RO}, \\ n_i[k]/n_{\text{ref}}[k], & \text{dual RO}, \end{cases} \tag{6}$$

其中 $n_i[k]$ 和 $n_{\text{ref}}[k]$ 分别为振荡计数。两种方法都需要校准，因为归一化无法完全消除 PVT敏感性。

当每个选定的金丝雀连续 m个窗口均满足其校准限值时，Lightswitch 才会判定电源轨合格：

$$Q_\theta[k] = \bigwedge_{i=1}^{N_{\text{RO}}} \bigwedge_{j=0}^{m-1} [H_i^{\min} \le x_i[k-j] \le H_i^{\max}]. \tag{7}$$

采样窗口和 m在测量分辨率、稳定性与确认延迟之间取得平衡。对于双环形振荡器感测，判定合格需要新的同步测量结果，以及有效且非零的参考计数。

可调整环形振荡器哨兵的数量和位置，以满足不同的物理契约模型。图 3 展示了第 IV 节评估的一哨兵、二哨兵和四哨兵配置。双环形振荡器感测会在每种配置中增加一个共享的 AON参考环形振荡器。这些配置的感测覆盖范围和开销各不相同，但使用前必须根据所选物理模型进行验证。

C. 特定站点配置

Lightswitch 展示了不同实现如何满足共同的逻辑—物理契约形式化要求。对于双方商定的物理契约模型 $\mathcal{M}$，提供方选择配置 $z = (W, \pi, E, C, \theta)$，其中 W为开关总容量，π 为级调度，E 为电源连接位置，C 为环形振荡器哨兵的数量和位置，θ为感测参数。这些选择会影响确认延迟、电源扰动和实现开销。

要配置一个位置，客户端和提供方首先就物理完成要求及支持的运行条件达成一致。随后，提供方从预先表征的配置中选择候选感测参数，包括感测方法、采样窗口和阈值，并将其与站点特定开关配置及布局选择相结合。独立的电源轨电压测量用于确定所得配置在表征条件下是否满足双方约定的物理模型。未通过验证的配置将被调整或拒绝。

提供方选择一种配置，以在满足约定的合同要求的前提下，将确认延迟降至最低：

$$\min_z T_{\text{ack}}(z) \quad \text{s.t.} \quad \begin{cases} \Delta(z,e) \ge 0, & e \in \mathcal{E}, \\ D_{\text{AON}}(z,e) \le D_{\max}, & e \in \mathcal{E}, \\ S_I(z,e) \le S_{\max}, & e \in \mathcal{E}, \\ A_{\text{area}}(z) \le A_{\max}. \end{cases} \tag{8}$$

此处，e 表示范围 $\mathcal{E}$内的一个运行条件，而 Δ 是相对于在双方商定的物理模型 $\mathcal{M}$下的就绪状态进行测量的。过早确认或违反电源完整性和面积限制的配置将被拒绝。

开关布局和环形振荡器位置在物理实现期间固定。如果硬件支持，阶段时序和感测阈值可以编程设置。选定的参数存储在AON控制器中。因此，不同位置可以使用不同的物理模型和实现，同时保持相同的数字接口和契约验证方法。

IV. 评估

本节以Lightswitch作为概念验证微服务，评估所提出的逻辑-物理契约形式化。首先检查数字契约和物理契约的保证，然后研究不同物理契约模型对确认延迟、感测要求和实现开销的影响。

A. 评估方法

我们构建了三种台积电 TSMC 28纳米布局后客户端设计变体，每种设计都包含一个与合成负载（例如，连接成环的FO4负载反相器、NAND门和NOR门）相耦合的数字电源控制状态机，且具有不同的负载特性和物理版图（150×150um、 175×175um和 350×350um）。所有位置均共享相同的数字接口和契约形式化，但采用各自的位置专用物理契约模型和实现配置。Yosys通过有界模型检查和归纳法验证数字控制器。Spectre利用通过Cadence Innovus实现的物理设计，对环形振荡器行为和电源轨就绪状态进行表征。独立的电压预言机根据商定的物理契约模型，在不同PVT和负载条件下验证传感器决策和确认时序。Voltus测量唤醒电源完整性，而面积和功耗分析则量化实现和检查契约所产生的开销。

B. 数字契约验证

第一个实验验证逻辑-物理契约的数字保证。Lightswitch 控制器接收开/关请求，分阶段启用功率开关，检查电源轨就绪状态，并确认已完成的转换或报告故障。我们使用 Yosys SAT [22] 和 SystemVerilog 断言，针对控制器的 RTL 检查这些行为。表 II 总结了经验证的保证。

验证涵盖三种控制器配置，其独立控制的电源开关组数量和关闭放电延迟各不相同。放电延迟是

表 II 可检查的数字服务契约保证。

属性	检查的保证
确认有效性	确认与请求状态相符，且仅在控制器处于空闲且无故障状态时发出。
开启确认	轨道就绪信号已置为有效、开关已启用、隔离已移除，并允许复位释放。
关闭确认	放电等待时间已完成，开关已禁用，位置已隔离，并保持复位。
开关顺序	转换期间保持隔离和复位；关闭在禁用开关前隔离该位置。
故障处理	超时或失去就绪状态会触发隔离，并阻止确认。
Responsebound	已接受的请求会在已配置的时间限制。

表 III 数字契约验证结果。

配置	组 (#)	关闭延迟（周期）	有界模型检测 / 归纳	见证
标准控制器	2	4	通过 / 通过	6/6
零延迟故障	2	0	通过 / 通过	1/1
扩展控制器	4	12	通过 / 通过	2/2

控制器在禁用开关后等待的时钟周期数，以便站点电源电压下降。这些配置分别测试正常运行、更大型的控制器，以及必须阻止关闭确认的无效零延迟设置。每种配置均使用 40 周期有界模型检查 [23]和最多 32 步的归纳证明 [24], [25]进行检查。验证使用原始控制器 RTL，并检查其在任意客户端请求和传感器输入下的行为。

如表 III 所示，三种配置均通过了两项验证检查，共计六项检查通过。独立的可达性测试发现了九个示例，涵盖正常转换、传感器等待、就绪状态丢失、故障恢复和看门狗超时。特别是，零延迟配置正确地拒绝了关闭确认，因为未提供放电等待时间。这些结果表明，该控制器满足数字契约保证，包括确认、隔离和故障处理。

C. RO 校准与就绪验证

第 III-B 节介绍了两种用于检测电源轨就绪状态的 RO 感测方法。本实验评估了这两种方法在 PVT 条件下对已达成一致的物理契约模型的支持效果。布局前 Spectre 仿真比较了 30 种电压和 PVT 条件下的绝对 RO 计数值与参考归一化计数。参考 RO 在 0.90V 下运行，金丝雀电压范围为 0.80 至 0.90 V。RO 频率随电源电压升高而增加，参考

归一化有助于减小 PVT效应。使用仿真的频率估算 512 个周期采样窗口内的计数。经评估的模型可区分低电压（$V_{\mathrm{SW}} \le 0.84\mathrm{V}$）与标称电压（$V_{\mathrm{SW}} = 0.90\,\mathrm{V}$）。

图4展示了归一化的RO频率比。绝对计数无法可靠地区分PVT条件下的低电压和标称

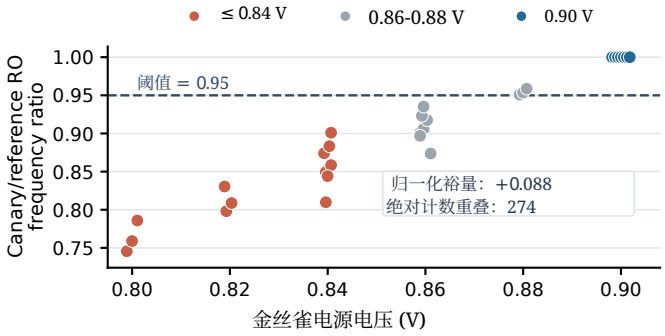

图 4. 30 种电压和 PVT 条件下的环形振荡器感测。参考归一化可区分低电压和标称电压。

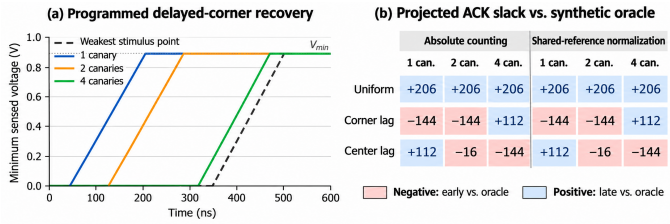

图 5. 合成电源轨恢复下的金丝雀布置和预计确认时序。（a）延迟斜坡站点角落恢复。（b）三种恢复场景下的确认裕量。负值表示相对于合成预言机提前确认。

电压，因为它们的估计计数范围有274个计数的重叠。参考归一化以0.088的裕量将这两种电压类别区分开来。阈值0.95可将采样数据中的全部13个低电压区间和7个标称电压区间区分开来。

这些结果表明，感测方法的选择如何影响微服务所能支持的物理契约模型。参考归一化可在所采样的 PVT 条件范围内提供一致的电压分类，从而无需针对角落进行特定校准即可使用同一阈值。这展示了物理表征如何指导选择满足约定契约要求的感测实现。

D. 物理契约模型与金丝雀敏感性

除选择感测方法之外，环形振荡器哨兵的数量与放置位置也会影响 Lightswitch 满足约定物理契约模型的程度。为研究这些影响，使用代表均匀恢复、延迟斜坡站点角落和延迟斜坡站点中心的合成电源轨电压轨迹，对图 3 中的单金丝雀、双金丝雀和四金丝雀配置进行了评估。先前表征的 RO频率用于借助 128周期采样窗口估计确认时间。将这些结果与跟踪斜坡最慢的电源轨位置的电压预言机进行比较。

图5展示了金丝雀布置如何影响确认时序。在延迟斜坡站点角落恢复下，一个和两个金丝雀配置比四个金丝雀在就绪状态后112个周期确认提前144个周期

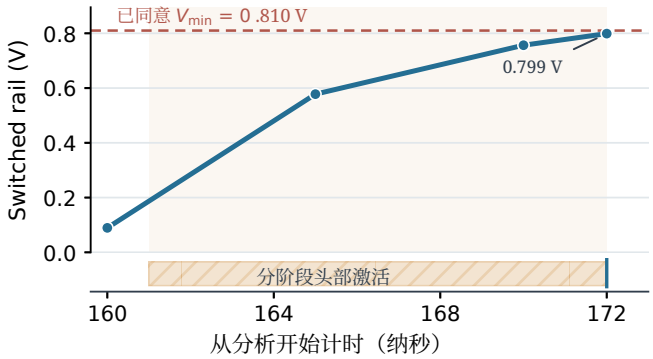

图6. 台积电28纳米脉动阵列站点的分阶段唤醒行为。全部236个外围头部开关在172纳秒前启用，同时伴随开关电源轨的电压响应。

于预言机，暴露出功能完整性违规。在延迟斜坡站点中心恢复下，居中的单金丝雀配置在就绪状态后112个周期确认，但四个角落金丝雀提前144个周期确认。在均匀恢复下，所有配置都需要额外等待206个周期。

这些结果表明，就绪检测取决于金丝雀的布置位置，而不仅仅是金丝雀的数量。物理契约模型允许客户端和提供方就必须监控哪些位置以建立就绪状态达成一致。这样，便可以根据客户端的要求选择感测配置，在物理覆盖范围、确认延迟和实现开销之间取得平衡。

E. 唤醒电源完整性与物理验证

除了验证数字控制并校准环形振荡器感测外，物理契约还要求开关电源达到约定的就绪条件。为此，Lightswitch 被部署在台积电28纳米脉动阵列站点中，并完成布局布线，其中包含236个外围头部开关。门级波形确认，开关在约161至172 ns之间分阶段启用，并在172 ns时全部开启。Voltus 报告称，在此切换过程中，峰值浪涌电流为11.05mA。

图6显示了开关电源轨电压的初始响应。随着头部开关开启，电源轨电压从约0.09 V上升至165 ns时的0.58 V，在170 ns时达到0.76 V，并在约172 ns时达到0.799 V。这些测量结果刻画了物理电源网络的初始充电行为，并为形式化验证的数字开关序列提供了补充性的电气证据。

F. 微服务复用与契约开销

最终实验测量了在具有不同物理要求的位置支持逻辑-物理契约的实现成本。Lightswitch 保持相同的数字接口和契约验证方法，同时针对不同位置采用特定的切换和感测配置。该评估

表 IV 位置特征和 Lightswitch开销。

Site	Area (毫米²)	周长 (μm)	平均标头数 (#)	增加面积 (毫米²)	O/H (%)
小型	0.02250	600	365.5	0.011810	52.49
中型	0.030625	700	583.6	0.010926	35.68
大型	0.12250	1400	1131	0.020026	16.35

涵盖三种站点规模的 20 个电源域。表 IV 总结了它们的物理特征和面积开销。

在这 20 个域中，Lightswitch 使用了 15,290 个头部开关。增加面积包括周边区域和 Lightswitch 实现部分，其中包含控制器、环形振荡器哨兵、AON 监控逻辑，以及任何额外的切换或隔离资源。小型位置在每侧延伸 16 μm，而中型和大型位置则在水平方向延伸 16 μm、垂直方向延伸 10 μm。总面积开销从小型位置的 52.49% 降至大型位置的 16.35%，表明随着位置尺寸增大，相对集成成本会降低。

这些结果展示了在不同位置集成 Lightswitch 的总面积开销。契约检查的额外成本取决于双方商定的物理模型，以及满足该模型所需的传感硬件。除了基本的电源切换和就绪检测外，更严格的模型可能要求在用户位置内增加环形振荡器哨兵，并在共享的 AON 基础设施中增加计数和资格判定逻辑。这些新增内容会增加面积和功耗，而更长的采样或稳定时间要求则可能增加确认延迟。因此，契约检查会给客户端和提供方双方带来成本，并需要在物理覆盖范围、响应时间和硬件开销之间进行权衡。

V. 相关工作

共享硅原型平台（包括多项目晶圆 [26], [2],Tiny Tapeout [27],和 Chipstitch [6],）让硅实验更加易于开展。Chipstitch 提供了促成 Lightswitch 的共享基础设施和每站点电源控制。将共享硬件功能作为可复用服务公开，借鉴了软件微服务 [28], [29]以及用于规定和验证组件保证的基于契约的方法 [30], [31], [10], [11], [32], [33]。本工作在这些方法的基础上，明确将由客户端约定的物理完成模型纳入服务契约，并将其与数字确认相连接。在低功耗硬件中，IEEE 1801 定义了电源意图 [34],，而形式化验证技术则支持对数字控制行为进行检查 [23], [24], [25], [35]。以往工作还涉及电源门控和分阶段唤醒 [36], [37], [38], [39], [13], [12], [15], 、电源网格完整性 [40], [41],以及基于环形振荡器的电源监控 [17], [18], [42], [19]。Lightswitch 将这些技术用于概念验证实现，以研究如何定义、验证逻辑—物理契约，并针对不同的场地要求进行配置。

VI. 结论

本工作提出了适用于可复用片上微服务的可检查逻辑-物理契约制定。该制定包括由客户端约定的物理契约模型，用于定义服务完成，并将经过形式化验证的数字保证与经过物理验证的条件相连接。Lightswitch 通过一个具备基于环形振荡器的就绪检测和分阶段周界切换功能的电源控制微服务，展示了这一方法。针对三个不同的台积电 28 纳米站点进行的评估，考察了契约正确性、替代物理模型、确认延迟、电源完整性以及契约检查的开销。这些结果表明，不同的物理要求可以通过通用接口和验证方法得到支持。

参考文献

[1] M. Venn，《Tiny Tapeout：人人都能使用的共享硅流片平台》，*IEEE* 固态电路杂志，第 16 卷第 2 期，第 20–29 页，2024 年。[2] A. B. Kahng、I. I. Mandoiu、X. Xu 和 A. Z. Zelikovsky，《面向多项目晶圆的增强型设计流程与优化》，*IEEE* 集成电路与系统计算机辅助设计学报（*TCAD*），2007 年 2 月。[3] D. Cohen 和 G. Lewicki，《Mosis：ARPA 的硅中介》，加州理工学院 *VLSI* 会议论文集，1981 年 1 月。[4] L. Conway，《MPC 探险：VLSI 设计与实现方法生成方面的经验》，加州理工学院 *VLSI* 会议论文集，1981 年 1 月。[5] C. Tomovich，《Mosis——通往硅的门户》，*IEEE* 电路与器件杂志，1988 年 3 月。[6] J. Kim、S. Yarzada、P. Y.-C. Chen、Y. Li、W. Zhu 和 C. Torng，《Chipstitch：用于加速硅原型设计的可扩展且经济高效的平台》，国际计算机辅助设计会议（*ICCAD*），2026 年。 [在线]。可访问：https://doi.org/10.1145/3831252.3833953[7] 《Mosis 服务》，在线网页，2025 年（访问日期：2025 年 4 月 1 日），https://themosisservice.com/about。[8] 《Muse Semiconductor》，在线网页，2025 年（访问日期：2025 年 4 月 1 日），https://www.musesemi.com。[9] A. Nayak、K. Zhang、R. Setaluri、A. Carsello、M. Mann、C. Torng、S. Richardson、R. Bahr、P. Hanrahan、M. Horowitz 和 P. Raina，《利用低开销细粒度电源域提升粗粒度可重构阵列的能效》，*ACM* 可重构技术与系统汇刊，第 16 卷第 2 期，2023 年。[10] A. Benveniste、B. Caillaud、D. Nickovic、R. Passerone、J.-B. Raclet、P. Reinkemeier、A. L. Sangiovanni-Vincentelli、W. Damm、T. A. Hen- zinger 和 K. G. Larsen，《系统设计契约》，电子设计自动化基础与趋势，2018 年 3 月。[11] A. Saoud、A. Girard 和 L. Fribourg，《连续时间系统的假设-保证契约》，*Automatica*，2021 年 6 月。[12] Y. Shin、J. Seomun、K.-M. Choi 和 T. Sakurai，《电源门控：标准单元 VLSI 设计的电路、设计方法与最佳实践》，*ACM* 电子系统设计自动化汇刊（*TODAES*），2010 年 10 月。[13] H. Jiang 和 M. Marek-Sadowska，《用于降低电源/地噪声的电源门控调度》，设计自动化会议（*DAC*），2008 年。[14] R. Singh、J. K. Woo、H. Lee、S. Y. Kim 和 S. Kim，《通过三步唤醒划分最小化电源门控噪声》，*IEEE* 电路与系统汇刊 *I*（*TCAS I*），第 59 卷第 4 期，第 749–762 页，2012 年。[15] M.-C. Lee、Y. Shi 和 S.-C. Chang，《兼顾资源使用与时序预算的电源门控设计高效唤醒调度》，*IEEE* 集成电路与系统计算机辅助设计学报（*TCAD*），2012 年 6 月。[16] S. Kim、S. Paik、S. Kang 和 Y. Shin，《电源门控电路的唤醒调度及其缓冲树综合》，*Integration*，《*VLSI* 杂志》，第 53 卷，第 157–170 页，2016 年。[17] Y. Ogasahara、M. Hashimoto 和 T. Onoye，《适用于片上系统电源完整性验证的由标准单元构成的动态电源噪声测量电路》，亚洲及南太平洋设计自动化会议（*ASP-DAC*），2008 年。[18] ——，《基于全数字环形振荡器的动态电源噪声波形感测宏单元》，IEEE固态电路期刊（JSSC），2009 年 5 月。[19] Y. Du、J. Qian、Z. Chen 和 W. Shan，《一种全数字、1.92–7.32 mV/LSB、0.5–2 GS/s 采样率且零延迟预测的电压传感器：用于压降检测和 AVS 系统的动态 PVT 校准》，IEEE 电路与系统汇刊 I（TCAS I），第 70 卷第 12 期，第 4888–4899 页，2023 年。[20] S. Kim 、 S. V. Kosonocky 和 D. R. Knebel，《理解并最小化电源门控结构模式转换期间的地弹》，低功耗电子与设计国际研讨会（ISLPED），2003 年。[21] I. E. Sutherland，《微流水线》，ACM 通讯，第 32 卷第 6 期，第 720–738 页，1989 年。[22] C. Wolf 和 J. Glaser，《Yosys——免费的 Verilog 综合套件》，Austrochip 研讨会（Austrochip），2013 年。[23] A. Biere、A. Cimatti、E. M. Clarke 和 Y. Zhu，《无需二元决策图的符号模型检验》，系统构造与分析工具和算法（TACAS），1999 年。[24] M. Sheeran、S. Singh 和 G. St˚almarck，《使用归纳证明和 SAT 求解器检验安全属性》，计算机辅助设计中的形式化方法（FMCAD），2000 年。[25] N. E´en 和 N. S¨orensson，《通过增量 SAT 求解进行时序归纳》，理论计算机科学电子札记，第 89 卷第 4 期，第 543–560 页，2003 年。[26] A. B. Kahng、I. I. Mandoiu、Q. Wang、X. Xu 和 A. Z. Zelikovsky，《多项目掩模版布局规划与晶圆切割》，物理设计国际研讨会（ISPD），2004 年。[27] M. Venn，《Tiny Tapeout：人人都能使用的共享硅流片平台》，IEEE 固态电路杂志，2024 年 5 月。[28] J. Lewis 和 M. Fowler，《微服务》，martinfowler.com，2014 年。[在线]。可访问：https://martinfowler.com/articles/microservices.html [29] N. Dragoni、S. Giallorenzo、A. Lluch-Lafuente、M. Mazzara、F. Montesi、R. Mustafin 和 L. Safina，《微服务：昨天、今天与明天》，载于《当下与未来的软件工程》。施普林格，2017 年，第 195–216 页。[30] L. de Alfaro 和 T. A. Henzinger，《接口自动机》，欧洲软件工程会议暨软件工程基础研讨会（ESEC/FSE），2001 年。[31] A. L. Sangiovanni-Vincentelli、W. Damm 和 R. Passerone，《驯服弗兰肯斯坦博士：面向信息物理系统的基于契约的设计》，欧洲控制杂志，第 18 卷，第 217–238 页，2012 年。[32] A. Cimatti、M. Dorigatti 和 S. Tonetta，《OCRA：用于检验时序契约精化的工具》，自动化软件工程国际会议（ASE），2013 年。[33] A. Cimatti 和 S. Tonetta，《基于组件的嵌入式系统契约精化证明系统》，《计算机程序科学》，第 97 卷，第 333–348 页，2015 年。[34] IEEE，《IEEE 标准 1801-2024：低功耗能量感知电子系统的设计与验证 IEEE 标准》，IEEE 标准，2024 年。[35] A. R. Bradley，《无需展开的基于 SAT 的模型检验》，验证、模型检验与抽象解释（VMCAI），2011 年。[36] S. Mutoh、T. Douseki、Y. Matsuya、T. Aoki、S. Shigematsu 和 J. Yamada，《采用多阈值电压 CMOS 的 1 V 电源高速数字电路技术》，IEEE固态电路期刊（JSSC），第 30 卷第 8 期，第 847–854 页，1995 年。[37] M. Powell、S.-H. Yang、B. Falsafi、K. Roy 和 T. N. Vijaykumar，《Gated-Vdd：一种降低深亚微米缓存存储器漏电的电路技术》，低功耗电子与设计国际研讨会（ISLPED），2000 年。[38] B. H. Calhoun、F. A. Honor´e 和 A. P. Chandrakasan，《分布式 MTCMOS 的漏电降低方法》，IEEE固态电路期刊（JSSC），第 39 卷第 5 期，第 818–826 页，2004 年。[39] A. Abdollahi、F. Fallah 和 M. Pedram，《MTCMOS 电路中的有效电源模式转换技术》，设计自动化会议（DAC），2005 年。[40] D. Kouroussis 和 F. N. Najm，《用于电源网格电压完整性验证的静态模式无关技术》，设计自动化会议（DAC），2003 年。[41] M. Popovich、A. V. Mezhiba 和 E. G. Friedman，《带片上去耦电容的电源分配网络》。施普林格，2007 年。[42] Y.-J. An、D.-H. Jung、K. Ryu、H. S. Yim 和 S.-O. Jung，《使用比例反相器环形振荡器的全数字片上工艺传感器》，IEEE

超大规模集成电路系统汇刊 *(TVLSI)*，第 24 卷，第 11 期，第 3232–3242 页，2016 年。