User’s Guide

TMS320F28004x 功能安全手册

摘要

本文档是适用于德州仪器 (TI) TMS320F28004x 安全关键型微控制器产品系列的功能安全手册。该产品系列采用了可在面向多应用的产品中实现的通用安全架构。

内容

插图清单

表格清单

商标

1 引言

WARNING

TMS320F28004x 作为一种功能安全合规型独立安全要素 (SEooC) 产品提供，这意味着，TMS320F28004x 的开发遵循了 TI 符合 ISO 9001/IATF 16949 标准的硬件产品开发流程。第二，该产品经过独立评估，符合 ASIL D（根据 ISO 26262:2018）和 SIL 3（根据 IEC 61508:2010）的系统能力合规性要求，具体请参阅*德州仪器 (TI) 的功能安全硬件开发流程*。因此，本功能安全手册仅用于提供相关信息，说明如何使用 TMS320F28004x 器件的特性来帮助系统设计人员实现给定的 ASIL 或 SIL 等级。系统设计人员负责在其系统环境中评估该器件，并确定其实现的系统级 ASIL 或 SIL 覆盖率。

本文档支持的产品经评估符合 ASIL D（根据 ISO 26262）和 SIL 3（根据 IEC 61508）的系统能力合规性。如需了解更多信息，请参阅*德州仪器 (TI) 的功能安全硬件开发流程*。

本功能安全手册是功能安全合规型设计包的一部分，旨在帮助客户设计出符合 ISO26262 或 IEC61508 功能安全标准的系统。

本文档是适用于德州仪器 (TI) TMS320F28004x 安全关键型微控制器产品系列的功能安全手册。该产品系列采用了可在面向多应用的产品中实施的通用安全架构。

本功能安全手册支持的产品配置包括表 1-1 中所列以下产品的器件版本 B。器件版本可由产品数据表中列出的器件识别寄存器的 REVID 字段确定。

表 1-1. 本功能安全手册支持的产品

可订购器件	支持的安全完整性等级
F280048CPMQR	ASIL B
F280048PMQR	ASIL B
F280049CPMS	ASIL B
F280049CPZQR	ASIL B
F280049CPZS	ASIL B
F280049PMS	ASIL B
F280049PMSR	ASIL B
F280049PZQ	ASIL B
F280049PZQR	ASIL B
F280049PZS	ASIL B
F280049PZSR	ASIL B
F280040CPMQR	QM
F280040PMQR	QM
F280041CPMS	QM
F280041CPZQR	QM
F280041CPZS	QM
F280041CRSHSR	QM
F280041PMS	QM
F280041PMSR	QM
F280041PZQR	QM
F280041PZS	QM
F280041PZSR	QM
F280041RSHSR	QM
F280045PMS	QM
F280045PMSR	QM
F280045PZS	QM
F280045PZSR	QM

表 1-1. 本功能安全手册支持的产品 (continued)

可订购器件	支持的安全完整性等级
F280045RSHSR	QM
F280049CRSHSR	QM
F280049CRSHS	QM
F280049RSHSR	QM

本功能安全手册提供系统开发人员所需的信息，以帮助他们使用受支持的 TMS320F28004x MCU 来创建安全关键型系统。该文档包含：

- 组件架构概述
- 用于降低系统失效概率的开发流程概述
- 用于管理随机失效的功能安全架构概述
- 架构分区和实现的功能安全机制的详细信息

以下信息记录在*适用于 TMS320F28004x C2000™ MCU 的详细功能安全分析报告 (SAR)*中，该报告仅在功能安全 NDA 下提供，本文档中不再赘述：

- 组件故障率 (FIT)
- 用于估计器件故障率以计算定制故障率的故障模型
- 硬件组件针对目标标准（即 IEC 61508:2010 和 ISO 26262:2018）的功能安全指标
- 定量功能安全分析（也称为 FMEDA，失效模式、影响和诊断分析），包含组件不同部分的详细信息，可实现功能安全机制的自定义应用
- 计算功能安全指标时使用的假设

我们假设使用本文档的用户大体上熟悉 TMS320F28004x 产品系列。可以在 www.ti.com/C2000 上找到更多信息。

本文档旨在与所提供产品的相关数据表、技术参考手册和其他文档一同使用。

有关所列交付物以外的信息，请与您的 TI 销售代表联系，或访问 www.ti.com。

2 TMS320F28004x 产品安全能力和约束

本节总结了 TMS320F28004x 产品的安全能力。每个 TMS320F28004x 产品均：

- 作为独立功能安全要素 (SEooC) 提供
- 经评估符合 IEC 61508:2010 和 ISO 26262:2018 的相关系统能力合规性要求，并且
  - 达到 SIL 3 和 ASIL D 的系统完整性
- 通过实现适当的安全概念（如软件互惠式比较），该器件可以满足高达 ASIL B 的硬件架构指标。
- 包含多种特性以支持防止干扰 (FFI)功能，从而符合分配给不同子要素的混合关键性安全要求
- 按照 IEC 61508-2:2010 中的定义，TMS320F28004x MCU 是 B 类器件
- 该器件不要求硬件容错（例如，未要求 HFT > 0），如 IEC 61508:2010 中所定义
- 对于按照很多安全标准开发的安全组件，组件功能安全手册将提供产品安全约束条件列表。对于一个简单组件，或者为单一应用而开发的更复杂组件，这是一个合理的办法。然而，TMS320F28004x MCU 产品系列设计复杂，并非针对单一特定应用而开发。因此，一组单一的产品安全约束条件无法管理该产品所有可行用途

3 TI 针对系统故障管理的开发流程

对于功能安全开发，必须同时对系统故障和随机故障进行管理。德州仪器 (TI) 对其所有组件都遵循新产品开发流程，这有助于降低发生系统失效的可能性。节 3.1 中描述了该新产品开发流程。为功能安全应用而设计的组件还将遵循 TI 的功能安全开发流程的要求，如节 3.2 中所述。

3.1 TI 新产品开发流程

自 1996 年以来，德州仪器 (TI) 一直致力于为汽车和工业市场开发各种器件。汽车市场对质量管理和产品可靠性有着严苛的要求。TI 新产品开发流程具有管理系统故障所需的很多要素。此外，这些组件的文档和报告有助于遵循面向客户最终应用（包括汽车和工业系统）的各种标准，例如 ISO 26262-4:2018 和 IEC 61508-2:2010。

该组件是使用 TI 的新产品开发流程开发的，此流程经 Bureau Veritas (BV) 评估，符合 ISO 9001/IATF 16949 标准。

该标准开发流程将开发分成以下几个阶段：

- 评估
- 计划
- 创建
- 验证

图 3-1 显示了标准流程。

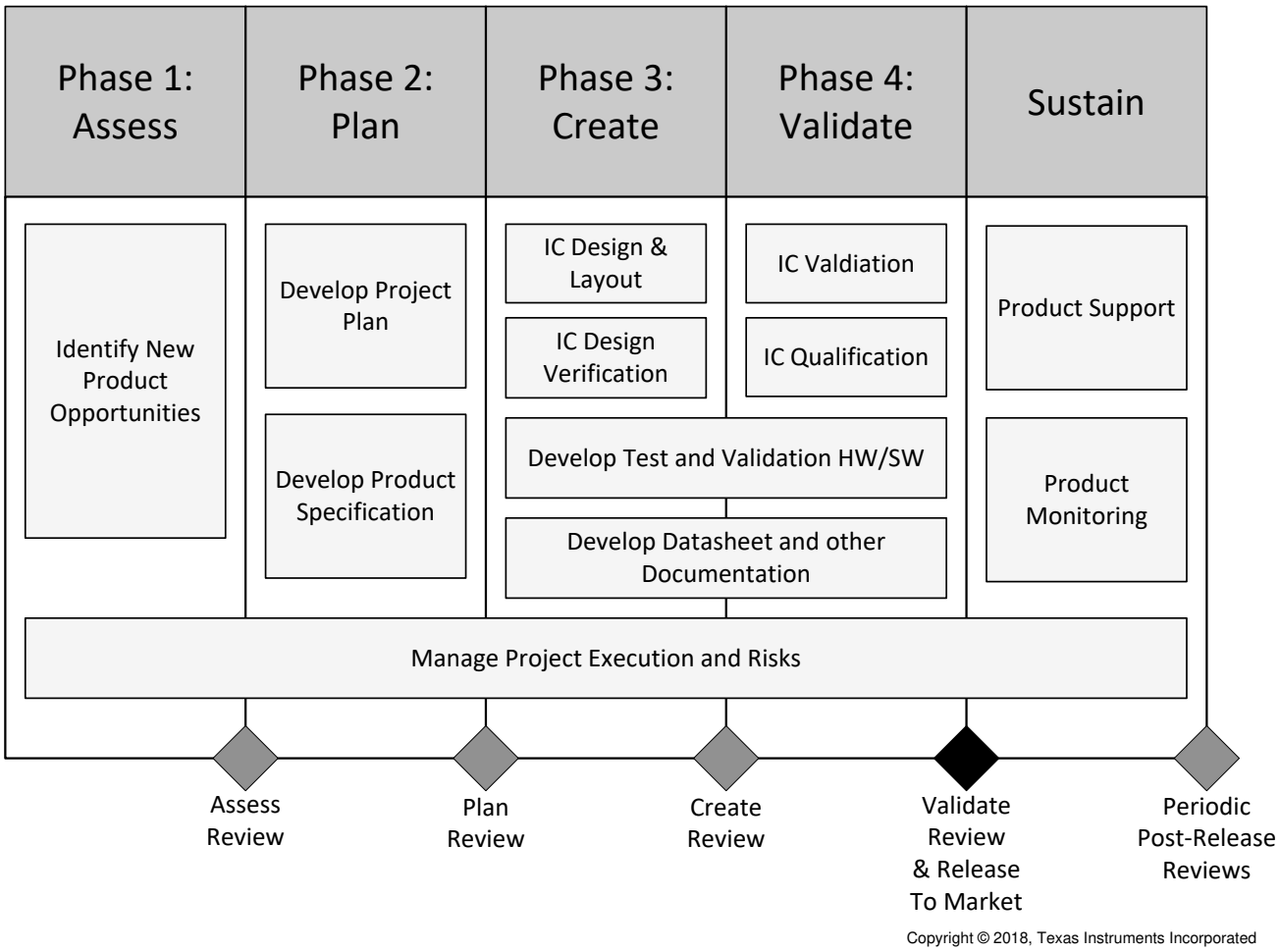


图 3-1. TI 新产品开发流程

3.2 TI 功能安全开发流程

TI 的功能安全开发流程源自 ISO 26262:2018 和 IEC 61508:2010，是一套用于半导体开发的要求和方法。该流程与 TI 的标准新产品开发流程相结合，可用于开发功能安全合规型组件。TI 内部规范“功能安全硬件”中描述了该功能安全开发流程的详细信息。

TI 功能安全开发流程的关键要素如下：

- 基于 TI 在功能安全应用组件方面的经验对系统级设计、功能安全概念和要求作出的假设
- 定性和定量功能安全分析技术，包括器件失效模式分析和功能安全机制的应用
- 基于多项行业标准和 TI 制造数据的基础时基故障率估算
- 组件开发期间功能安全工作产品的文档
- 整合通过多项功能安全组件开发、功能安全标准工作组和 TI 客户专业知识获得的经验教训

表 3-1 列出了基于图 3-1 所示标准开发流程的功能安全开发活动。

更多有关 TI 执行哪些功能安全生命周期活动的信息，请参阅附录 B。

面向客户的工作产品采用这种功能安全合规型流程，并适用于 ISO 26262:2018 和 IEC 61508:2010 之外的许多其他功能安全标准。

表 3-1. 基于 TI 标准开发流程的功能安全活动

评估	计划	创建	验证	维持和停产
确定是否需要执行功能安全流程	确定元件的目标 SIL/ASIL 等级	制定元件级功能安全要求	在器件上验证功能安全设计	记录出现的任何问题（如需要）
任命功能安全经理	制定功能安全计划	在设计规格中添加功能安全要求	说明功能安全设计的特性	报告后续操作中出现的事件（如需要）
阶段末审查	验证功能安全计划	验证设计规格	鉴定功能安全设计（根据 AEC-Q100 标准）	更新工作产品（如需要）
	提交功能安全案例	开始功能安全设计	敲定功能安全案例	
	分析目标应用，作出系统级功能安全假设	对设计进行定性分析（即失效模式分析）	进行工程评估	
	阶段末审查	验证定性分析	发布功能安全手册	
		验证功能安全设计	发布功能安全分析报告	
		对设计进行量化分析（即 FMEDA）	发布功能安全报告	
		验证量化分析	阶段末审查	
		重复功能安全设计流程（如需要）		
		阶段末审查		

4 TMS320F28004x 产品概述

4.1 C2000 架构和产品概述

TMS320F28004x 器件是功能强大的 32 位浮点微控制器单元 (MCU)，专为汽车和工业应用中的高级闭环控制应用而设计。

4.1.1 TMS320F28004x MCU

TMS320F28004x 支持将 C28x 和 CLA 作为处理要素，这有助于提高闭环控制应用的系统性能。这是一个功能强大的 32 位浮点微控制器单元 (MCU)，使系统集成商能够访问单个器件上的关键控制外设、差分模拟和非易失性存储器。

C28x CPU 的性能通过三角函数加速器 (TMU) 得到了进一步提升，TMU 加速器可快速执行包含变换和转矩环路计算中常见的三角运算的算法。Viterbi、复杂数学和 CRC 单元 (VCU) 加速器减少了已编码应用中常见的复杂数学运算所需的时间。用户可以参考*加速器：增强 C2000™ MCU 系列的功能*，了解如何使用该加速器来提高 MCU 在许多实时应用中的性能。

CLA 是一个独立的 32 位浮点加速器，以与主 C28x CPU 相同的频率运行，从而以极低的事件延迟来响应外设触发，并与主 CPU 并行执行代码。

TMS320F28004x 支持高达 256KB (128KW) 的片上闪存（含纠错码 (ECC)）以及高达 100KB (50KW) 的 SRAM（含奇偶校验或 ECC）。

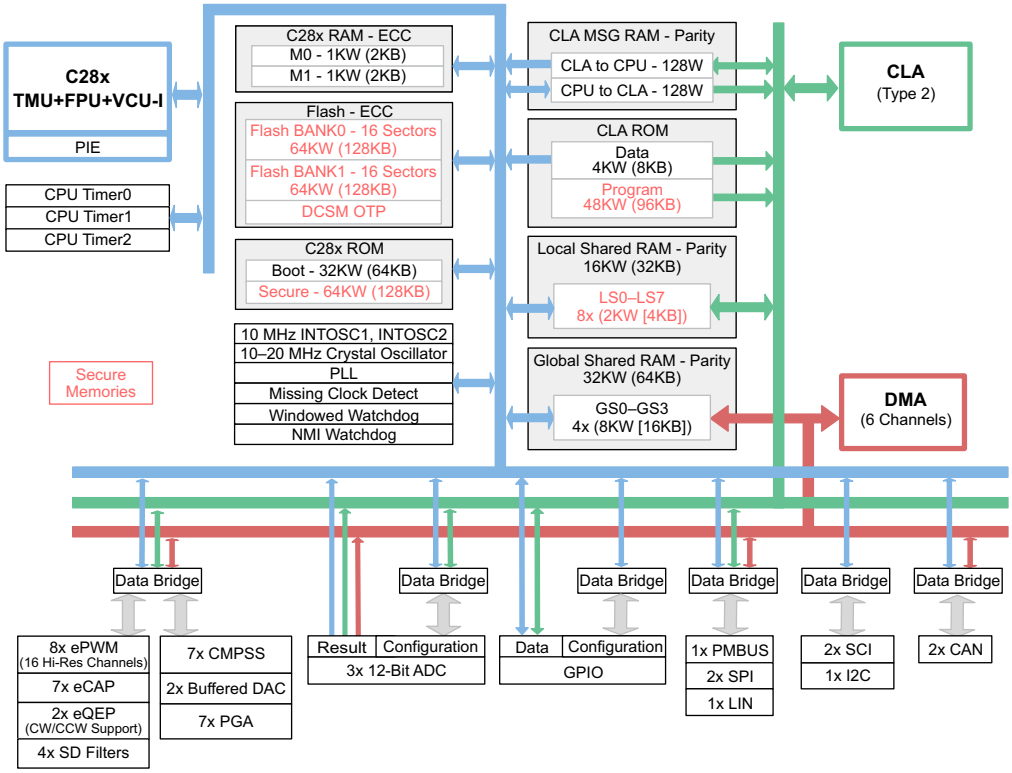


图 4-1. TMS320F28004x MCU 的功能方框图

此外该 MCU 上还集成了高性能模拟和控制外设，进一步实现系统整合。三个独立的 12 位 ADC 可准确、高效地管理多个模拟信号，最终提高了系统吞吐量。新型 Σ-Δ 滤波器模块 (SDFM) 与 Σ-Δ 调制器搭配使用可实现隔离分流测量。包含窗口比较器的比较器子系统 (CMPSS) 可在超过或未满足电流限制条件的情况下保护功率级。其他模拟和控制外设包括数模转换器 (DAC)、增强型脉宽调制 (ePWM)、增强型捕捉 (eCAP)、增强型正交编码器脉冲 (eQEP) 和可编程增益放大器 (PGA)。可编程增益放大器 (PGA) 用于放大输入电压，以提高下游 ADC 和 CMPSS 模块的有效分辨率。

控制器局域网 (CAN) 模块（符合 ISO11898-1/CAN 2.0B）、内部集成电路 (I2C) 总线、本地互连网络 (LIN)、串行通信接口 (SCI)、串行外设接口 (SPI)、电源管理总线 (PMBus) 接口和快速串行接口 (FSI) 等外设扩展了 TMS320F28004x MCU 的连接性。快速串行接口 (FSI) 模块是一个串行通信外设，能够跨隔离器件实现可靠的高速通信。

*TMS320F28004x 微控制器数据表*中概述了本 TMS320F28004x MCU 功能安全手册支持的器件配置。并非所有型号都适用于所有封装或所有温度等级。若要确认可用性，请联系您当地的德州仪器 (TI) 销售和营销部门。

4.2 功能安全概念

为了尽可能保持通用性，功能安全概念假定 MCU 扮演处理单元（或其中的一部分）的角色，并通过通信总线连接到远程控制器，如图 4-2 所示。通信总线直接或间接连接到传感器和执行器。

IEC 61508-1:2010 将合规项定义为根据 IEC 61508:2010 系列条款提出要求的任何相关项（例如要素）。如图 4-2 所示，包含 TMS320F28004x 微控制器的系统可用于符合 IEC 61508:2010 标准的合规项。

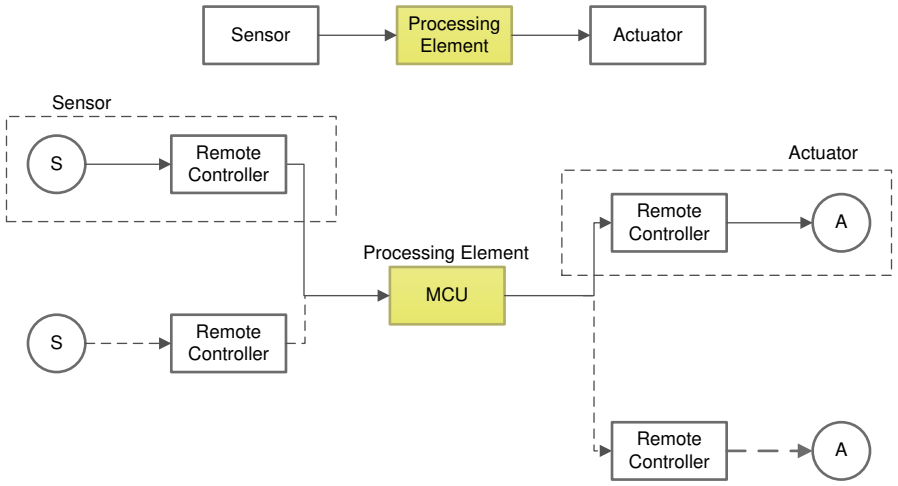


图 4-2. 合规项所用的 TMS320F28004x MCU 定义

4.2.1 应用于 TMS320F28004x MCU 的 VDA E-GAS 监测概念

德国 VDA 工作组“E-GAS-Arbeitskreis”提出的发动机管理系统的标准化 E-GAS 监测概念 [6] 是一个值得信赖的安全架构示例，该架构可用于发动机管理系统以外的应用，前提是它符合新应用在诊断可行性、环境约束、时间约束、稳健性等方面的目标 [7]。如需了解更多信息，请参阅图 4-3。

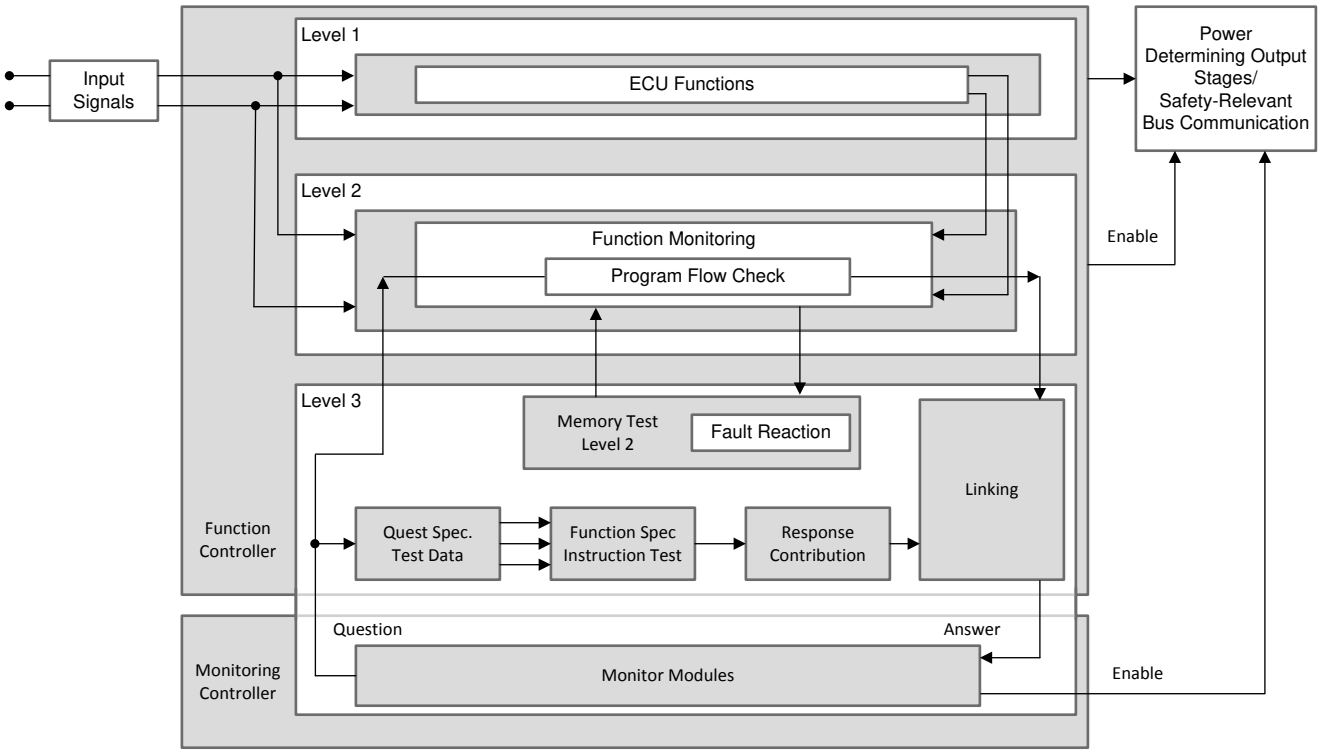


图 4-3. 标准 E-GAS 系统概述

MCU 器件系列支持异构非对称架构，其功能安全特性有助于在系统级实现 E-GAS 概念，如图 4-4 所示。在第一级（1 级），计算系统任务所需的功能。第二级（2 级）根据选定的一组参数检查第一级中的形成是否正确。第三级（3 级）实现一个额外的外部监测要素，用于在第一级正确执行任务和/或在第二级进行监测。确切的功能安全实现和用于实现 1 级和 2 级的模块以及实现 3 级的外部监测器件交由系统设计人员负责。

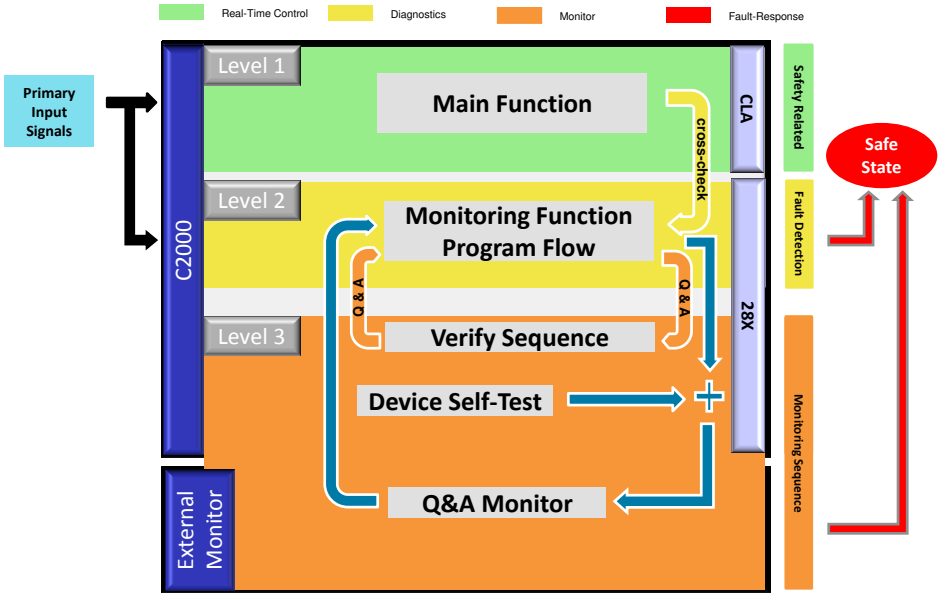


图 4-4. 应用于 F28004x MCU 的 VDA E-Gas 监测概念

由于器件架构固有的多功能性，可以使用几种基于软件表决的功能安全配置。表 A-1 中解释了 TMS320F28004x 具有的可能有助于提高诊断覆盖率的一些功能安全配置。在实现这些配置时，系统集成商需要考虑并以适当方式解决潜在的共模失效问题。这可以根据处理单元的可用性进行适当修改，以适应 TMS320F28004x 要求。（如前所述，该器件不要求硬件容错（例如，未要求 HFT > 0），如 IEC 61508:2010 中所定义）。

TMS320F28004x 的主要安全特性如图 4-5 中所示。

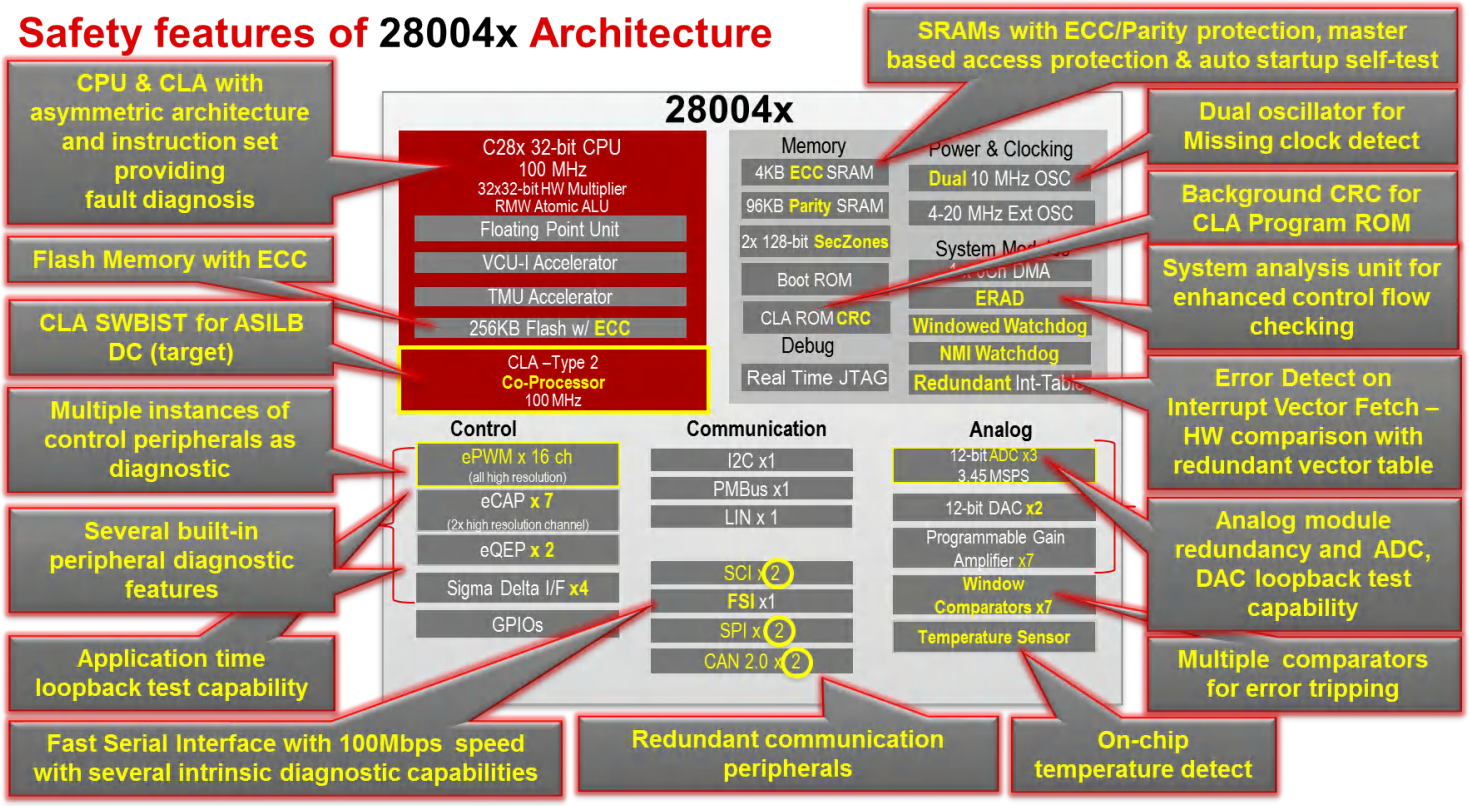


图 4-5. 具有安全特性的 TMS320F28004x MCU

4.2.2 容错时间间隔 (FTTI)

器件中的各种功能安全机制要么始终开启（参阅 CPU 对于非法操作、非法结果和指令陷入的处理等），要么由应用软件定期执行（参阅静态存储器内容的 VCU CRC 检查等）。安全机制检测故障所需的最长时间被称为故障诊断测试时间间隔 (FDTI)。一旦检测到故障，根据相关故障的故障反应（例如，外部系统对 ERRORSTS 引脚置位的反应），系统将进入安全状态。在危险事件发生之前，系统中可能出现一个或多个故障的时间跨度被称为容错时间间隔 (FTTI)，如 ISO 26262 中所定义。这类似于 IEC 61508 中定义的过程安全时间 (PST)。图 4-6 说明了 FDTI、故障反应时间和 FTTI 之间的关系。

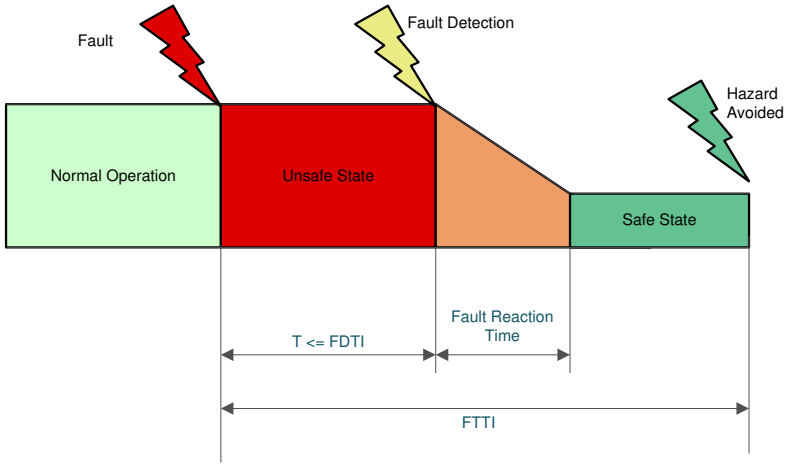


图 4-6. FDTI、故障反应时间和 FTTI 之间的关系

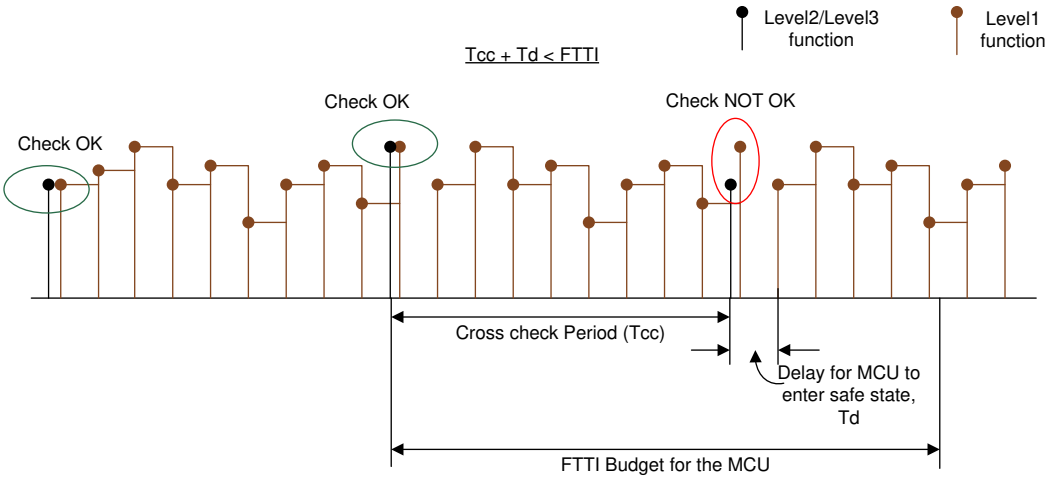


图 4-7. FTTI 图示

E-GAS 监测概念中的各项 2 级和 3 级检查的频率和范围应与容错时间间隔 (FTTI) 相一致。图 4-7 说明了所需检查的频率。这些检查应确保检测并响应微控制器的单点故障，使 TMS320F28004x MCU 在 FTTI 预算范围内进入安全状态。在检测到故障时，微控制器进入如图 4-8 所示的其中一种安全状态。单点故障诊断的一个示例是存储器的 ECC/奇偶校验。

本文档中介绍的功能安全概念、后续功能安全特性和配置仅供参考。系统和设备设计人员或制造商有责任确保终端系统（和任一德州仪器 (TI) 硬件或包含在系统内的软件组件）符合全部应用安全、规定和系统级性能要求。

4.2.3 TMS320F28004x MCU 安全状态

参考图 4-8，TMS320F28004x MCU 的安全状态定义为具有以下特征：

- 置位 TMS320F28004x MCU 复位
- 由于 3 级检查失败，通过外部监控器来禁用 TMS320F28004x MCU 的电源。通常会假设存在系统级功能来处理这种情况，因此在该分析中不会详细考虑电源故障。
- 由于 2 级检查失败（例如，ERRORSTS 引脚被置位），通过 C2000 MCU 的其中一个 IO 引脚告知外部系统。
- 由于 2 级检查失败（例如，与任务功能对应的 GPIO 引脚为三态），驱动执行器的 TMS320F28004x MCU 的输出被迫进入非活动模式。

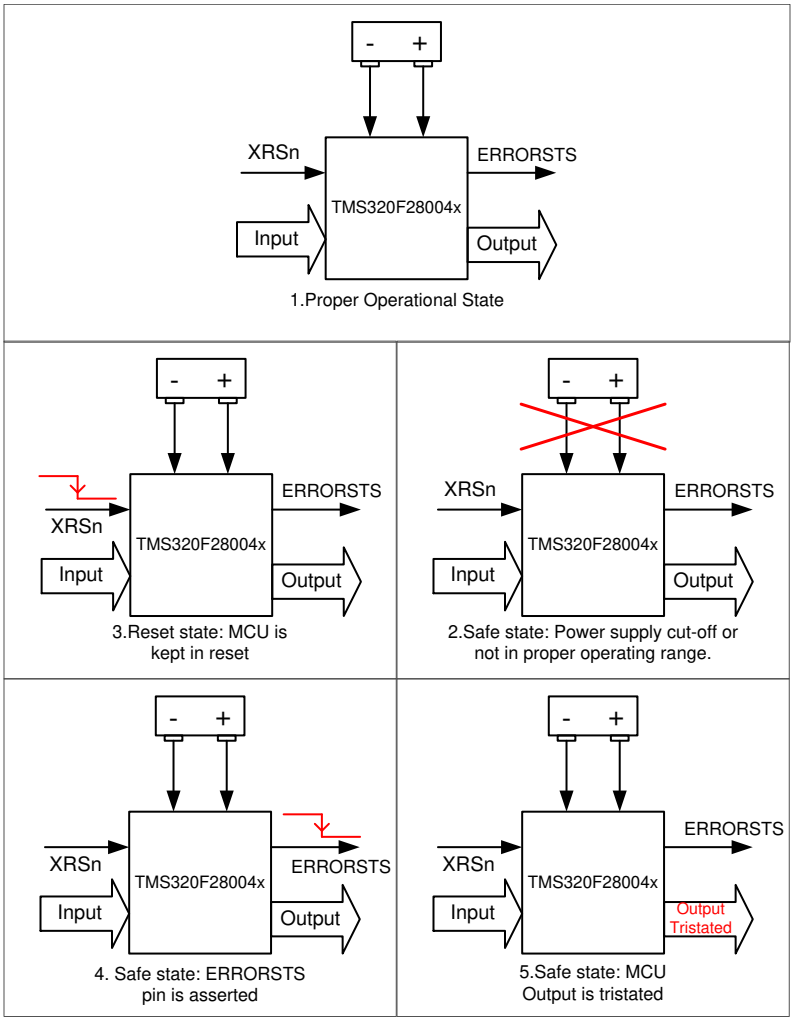


图 4-8. TMS320F28004x MCU 安全状态定义

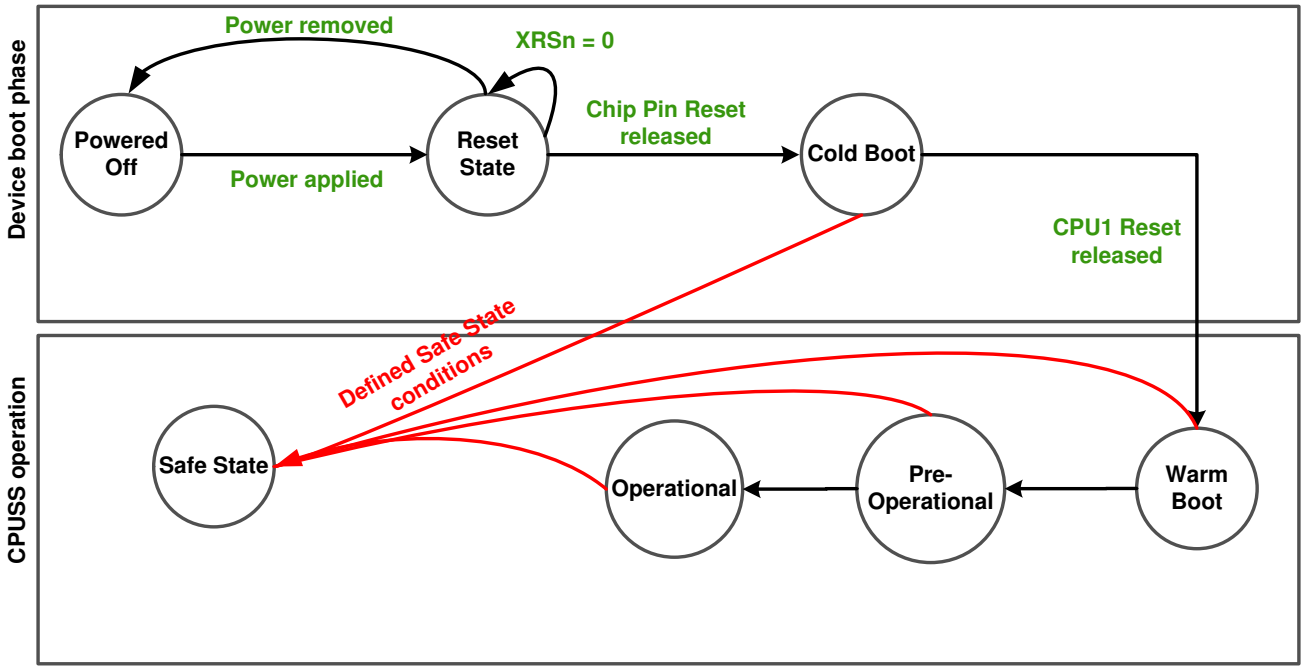


图 4-9. TMS320F28004x MCU 器件运行状态

4.2.4 运行状态

C2000 MCU 产品有一个运行状态的共用架构定义。这些运行状态应该由系统开发人员在其软件和系统级设计概念中进行观测。运行状态状态机如图 4-9 所示。运行状态可分为器件启动阶段和 CPU 子系统 (CPUSS) 运行阶段。

器件运行状态状态机的各种状态如下：

- 断电 - 这是 TMS320F28004x MCU 的初始运行状态。内核或者 I/O 电源均未加电，器件处于非功能状态。作为对系统级故障情况或 TMS320F28004x MCU 指示的故障情况的响应，外部监控器可在任何 TMS320F28004x MCU 状态下执行这项操作（使 TMS320F28004x MCU 断电）。
- 复位状态 – 在该状态下，使用外部引脚或使用任何内部源来置位器件复位。
- 安全状态 – 在安全状态下，器件要么不执行任何功能操作，要么使用器件 I/O 引脚指示内部故障情况。
- 冷启动 - 在冷启动状态下，关键模拟要素、数字控制逻辑和调试逻辑实现了初始化。CPU 保持通电但处于复位状态。当冷启动过程完成时，CPU 的复位在内部释放，从而进入热启动阶段。
- 热启动 - CPU 在热启动阶段从引导 ROM 开始执行。
- 运行前 - 在此阶段，控制权从引导代码转移到客户代码。在该阶段执行应用特定的配置（例如，时钟频率、外设启用、引脚多路复用等）。需要进行启动时间自检/验证测试，以确保在该阶段执行正确的器件操作。有关详细信息，请参阅 ROM8 加电预运行安全。
- 运行 – 这标志着系统退出预运行状态并进入功能状态。器件能够在运行模式下支持安全关键功能。

两个 CPU 的器件启动时间线如图 4-10 所示。

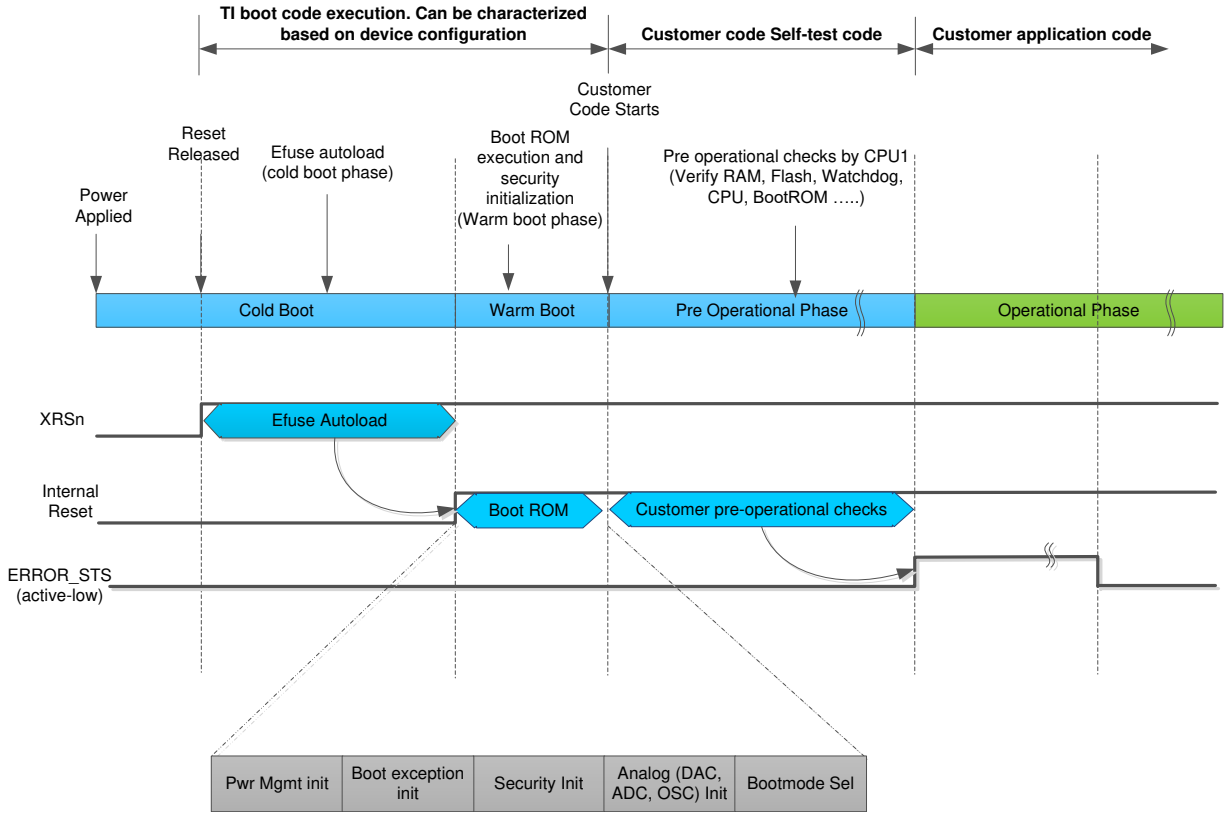


图 4-10. TMS320F28004x MCU CPU 启动序列

4.2.5 故障管理

TMS320F28004x MCU 产品架构使用 CPU 中断、不可屏蔽中断 (NMI)、ERRORSTS 引脚置位、CPU 输入复位置位和热复位 (XRSn) 置位，以通过内部安全机制提供不同级别的故障指示。故障响应是 TMS320F28004x MCU 或系统在指示故障时采取的操作方式。在故障指示期间，可能会有多个潜在的故障响应。系统集成商负责确定应采取哪种故障响应以确保与系统安全概念相一致。故障指示按严重程度（器件断电最为严重）排序，如图 4-11 所示。

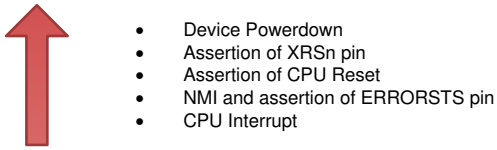


图 4-11. 故障响应严重程度

- 器件断电：这是最高优先级的故障响应，其中外部组件（参阅节 4.4.1）检测到器件或其他系统组件故障，因此使 TMS320F28004x MCU 断电。在此状态下，可以重新进入冷启动以尝试恢复。
- XRSn 置位：XRSn 复位可由内部或外部监控器生成，该监控器检测可能违反安全目标的严重故障。当 TMS320F28004x MCU 无法自行处理内部故障情况（例如，CPU1（主 CPU）无法自行处理 NMI）时，内部源会生成该故障响应。在此状态下，可以重新进入冷启动并尝试恢复。

- CPU 复位置位：CPU 复位将 CPU 状态从运行前或运行状态更改为热启动阶段。CPU 复位由检测任何安全违规情况的内部监控器生成。安全违规可能是故障条件产生的影响。
- 不可屏蔽中断 (NMI) 和 ERRORSTS 引脚置位：C28x CPU 支持不可屏蔽中断 (NMI)，其优先级高于所有其他中断。TMS320F28004x MCU 配备了一个 NMIWD 模块，负责为 C28x CPU 生成 NMI。ERRORSTS 引脚也将与 NMI 一同置位。根据系统级要求，可以使用软件在 TMS320F28004x MCU 内部或使用 ERRORSTS 引脚信息在系统级处理故障。
- CPU 中断：CPU 中断允许 CPU 外部的事件生成一个程序序列，然后传输给中断处理程序，在那里软件有机会管理该故障。外设中断扩展 (PIE) 块将大量中断源多路复用成较小的 CPU 中断输入集。

4.2.6 关于改善防止干扰特性的建议

使用 TMS320F28004x MCU 时，应采用以下技术和安全措施（如适用）来提高功能的独立性：

1. 如果未使用可用的外设，则保持外设时钟处于禁用状态（CLK14-外设时钟门控 (PCLKCR)）。
2. 如果未使用可用的外设，则保持外设处于复位状态（RST9-外设软复位 (SOFTPRES)）。
3. 如果可能，通过使用非相邻 I/O 引脚/焊球来分离关键 I/O 功能。
4. 根据应用要求将存储器分区到各个处理单元，并为每个存储器实例配置存储器访问保护机制，以便只有获批准的主器件才能访问存储器。
5. 双代码安全模块 (DCSM) 可用于实现功能安全（可从不同的安全区域（zone1、zone2 和非安全区域）执行具有不同安全完整性等级的功能），充当防火墙，从而降低从一个安全区到另一个安全区的干扰所造成的风险。有关详细信息，请参阅 *使用 C2000™ MCU 实现 EV/HEV 安全功能共存*
6. TMS320F28004x 支持 SYS10-外设访问保护 - 0 类。在对外设访问保护寄存器进行编程后，每个主器件均能做到专门控制外设，以防止特定应用的使用对系统中其他主器件造成错误写入或破坏。这是通过使用每个外设的专用访问控制位来实现的，该控制位允许或禁止来自给定主器件的访问。每个外设在每个主器件上都有两个位限定符，用于解码允许的访问。更多详细信息，请参阅 *TMS320F28004x 技术参考手册*中的“PERIPH_AC_REGS 寄存器”。
7. ADC11-禁用 ADC 的未使用 SOC 输入源有助于避免未使用的外设对 ADC 的功能造成干扰。
8. DMA9-禁用未使用的 DMA 触发源将有助于最大限度地减少无意 DMA 传输造成的干扰。
9. CLA11-禁用未使用的 CLA 触发源将降低触发事件造成的干扰风险。
10. 为避免虚假活动对 MCU 的调试端口造成干扰，可以使用 JTAG1-JTAG 端口的硬件禁用。
11. 在 CPU 上运行的安全应用可能会受到 PIE 模块的意外故障中断事件的干扰。PIE7-为未使用的中断维护中断处理程序和 PIE8-在线监测中断和事件将检测到此类干扰故障。
12. 支持 CPU 执行的 MCU 资源（如存储器、中断控制器等）可能会受到来自同一 MCU 上共存的较低安全完整性安全功能的资源的影响。SRAM11-存储器访问保护机制、SRAM16 – 信息冗余技术、SRAM17-CPU 对于非法操作、非法结果和指令陷入的处理之类的安全机制将能够检测到此类干扰。
13. 关键配置寄存器可能会受到 MCU（实现较低安全完整性功能）上总线主器件的干扰。这些会受到 SYS1-控制寄存器的多位使能键、SYS2-针对控制寄存器的锁定机制、SYS8-关键寄存器的 EALLOW 和 MEALLOW 保护等安全机制的保护。

4.2.7 关于解决共因失效问题的建议

系统集成商需要执行共因失效分析，以考虑 TMS320F28004x MCU 的子要素（包括引脚级连接）上可能存在的从属/共因失效。

1. 考虑相关的从属失效引发器列表，例如 ISO 26262-11:2018 中的列表。从属失效的分析应包括功能冗余器件之间以及功能与各安全机制之间的共因失效。
2. 验证从属失效分析考虑了在 TMS320F28004x MCU 上运行的软件任务的影响，包括硬件和软件交互。
3. 验证从属失效分析考虑了引脚或焊球级交互对 TMS320F28004x MCU 封装的影响，包括与所选 I/O 多路复用相关的方面。

在使用 TMS320F28004x MCU 时，应考虑以下事项来解决共因失效问题：

1. 冗余功能和安全机制可能会受到常见电源故障的影响。PWR1-外部电压监控器、PWR2-外部看门狗可以检测到电源的共因失效。
2. 通常，应对冗余功能常用的时钟源进行监测，CLK1-时钟丢失检测 (MCD)、CLK2-使用 CPU 计时器进行时钟完整性检查、CLK5-通过 XCLKOUT 对时钟进行外部监测和 CLK8-静态配置寄存器的定期软件读回等安全机

制可以检测到该时钟源上的任何失效。具体来说，为了避免出现会影响内部看门狗 (WD) 和 CPU 的常见时钟失效，建议使用 INTOSC2 或 X1/X2 作为 PLL 的时钟源。

3. 可通过 RST1-热复位的外部监测 (XRSn)、RST2-复位原因信息检测冗余功能的常见复位信号失效。
4. 互连逻辑上的共因失效可能以同样的方式影响冗余功能和功能安全机制。除了其他安全机制外，也可以通过 INC1-包括错误测试在内的功能软件测试来检测互连逻辑上的故障。
5. 共因失效可能会影响以冗余方式使用的两个功能。对于通信外设，可以实现特定于模块的包括端到端安全状态恢复的信息冗余技术以检测共因失效，例如 CAN2-包括端到端安全状态恢复的信息冗余技术、SPI2-包括端到端安全状态恢复的信息冗余技术、SCI3-包括端到端安全状态恢复的信息冗余技术、I2C3-包括端到端安全状态恢复的信息冗余技术。
6. 对 ADC 使用不同的电压基准和 SOC 触发源（请参阅节 6.5.8）。
7. 使用来自不同同步组的 ePWM 模块来实现硬件冗余。
8. 在实现 GPIO 引脚硬件冗余时，请使用不同组的 GPIO 引脚。
9. 以冗余方式使用的两个 PGA 模块不要共享同一个接地引脚。有关 PGA 共享共用接地的详细信息，请参阅器件特定数据表。

4.3 C2000 安全诊断库

为 F28004x 系列器件设计的诊断库包含三个库，即 CLA_STL、C28x_STL 和 SDL。这些库旨在帮助 TI 客户使用 F28004x 开发可满足汽车 (ISO 26262)、工业 (IEC 61508) 和电器 (IEC 60730) 市场终端产品的广泛标准且功能安全的系统。CLA_STL 和 C28x_STL 实现 CLA2 - CLA 的软件测试和 CPU3 - CPU 的软件测试安全机制，而 SDL 提供了功能安全手册中描述的几种安全机制的示例。

表 4-1. 针对 F28004x 诊断库的 DC 和 SCC

库	永久性故障诊断覆盖	系统能力合规性	说明
CLA_STL	≥ 60%	ASIL D/SIL 3	该 STL 实现 CLA2 - CLA 的软件测试
C28x_STL	≥ 60%	ASIL D/SIL 3	该 STL 实现 CPU3 - CPU 的软件测试
SDL	仅示例	不适用	SDL 提供了安全手册中描述的几种安全机制的示例

CLA_STL 和 C28x_STL 经独立评估，发现其分别适合集成到高达 ASIL D (ISO 26262:2018) 和 SIL 3 (IEC 61508:2010) 等级的安全相关系统中。CLA_STL 表示一种能够检测控制律加速器 (CLA) 永久性故障的安全机制。C28x_STL 表示一种能够检测 C28x CPU 永久性故障的安全机制。有关适用于各 STL 产品的确切 DC 要求，请参阅随 CSP 提供的 SPS。

SDL 通常被称为软件诊断库，是 TI 提供的整体安全相关配套资料的组成部分。它包括几种安全机制的一般示例实现。SDL 示例是使用基线质量软件开发流程开发的，不需要遵循任何特定的标准。因此，SDL 未经 TÜV SÜD 认证。用户应研究提供的示例并将其应用到安全相关应用中，并且负责相关产品级第三方认证。

为帮助客户获得相关产品级认证，TI 开发了 F28004x 合规性支持包 (CSP)。CSP 提供文档、源代码、静态分析结果、MISRA C 合规性结果、单元测试报告、动态分析结果、功能测试和集成示例。STL (C28x_STL 和 CLA_STL) 库和 CSP 中发布的相应源代码展示了符合 ISO 26262 ASIL D 系统功能的软件开发流程的产品。

WARNING

为了保持诊断覆盖率，C28x_STL 和 CLA_STL 的源代码必须按照 TI 提供的方式使用，并且在将库集成到客户应用时不得修改该源代码。任何修改必会导致最终产品的安全目标受损，从而导致终端用户的工作环境不安全。请参阅软件交付表 (SDF)，以查找与 STL 对应的每个文件的参考 MD5 校验和。SDF 文件作为 CSP 的一部分提供。

表 4-2 显示了用于开发 F28004x 库的工具。

表 4-2. 集成 F28004x STL 所需的工具

软件/硬件/工具	版本	依赖项
Code Composer Studio	9.2.0.00013	集成开发环境
CGT	20.2.1.LTS	代码生成工具链（编译器、汇编器、链接器）
C2000Ware	V3.01.00.00	F28004x 头文件
TMDSCNCD280049C	修订版 A	F280049 controlCARD 信息指南

系统集成商必须查阅 C28x_STL 和 CLA_STL 用户指南，了解与安装和开发相关的所有详细信息。

在 F28004x controlCARD 上对 STL 进行了测试。

4.3.1 使用假设 - F28004x 自检库

本节提供了与系统集成商在定义和构建基于 F28004x 的安全架构过程中必须考虑的问题相关的总体详情。

F28004x 中各种安全机制的软件支持可分为以下三类：

- C28x 自检库
- SDL – 软件诊断库
- CLA 自检库

基于 F28004x 器件构建的安全产品分层部署了 TI 提供的每种软件解决方案。第一层是 C28x_STL，它通过实现 CPU3 - CPU 的软件测试安全机制来检测 CPU 内部的永久故障。第二层是 SDL，它提供了一系列安全机制示例，旨在检测 F28004x 器件中几个关键要素内部的永久性故障。最后一层是实现 CLA2 - CLA 的软件测试安全机制的 CLA_STL，可用于检测 CLA 内部的永久性故障。

CLA_STL 利用并依赖 C28x CPU 和 CLA 来测试 CLA。因此，首先运行 C28x_STL 以确保 CPU 正常运行并能够执行所需的安全操作非常重要。SDL 支持许多安全机制，例如：CLK2 - 使用 CPU 计时器进行时钟完整性检查、CLK10 - 看门狗 (WD) 操作的软件测试、CLK12 - 时钟丢失检测功能的软件测试、SRAM14 - 奇偶校验逻辑的软件测试、SRAM13 - ECC 逻辑的软件测试、SRAM3 - SRAM 的软件测试和其他几个关键处理要素。系统集成商必须研究 SDL 支持的所有安全机制，并确定它们对所设计的安全系统的适用性。必须根据启动和运行时限制以及软件诊断测试能否在 POST 和/或 PEST 期间运行来评估安全系统。

软件诊断（由系统集成商选择）的成功完成可用作运行 CLA_STL 支持的测试向量的限定条件。

4.3.2 运行详细信息 - F28004x 自检库

C28x_STL、SDL 和 CLA_STL 共同托管在 F28004x 目标上，以便理解主机应用程序的安全性。因此，系统集成商必须充分理解 STL 集成所施加的相关系统约束条件的所有方面，以理解安全性，这非常重要。

4.3.2.1 运行详细信息 – C28x 自检库

C28x_STL 实现 CPU3 - CPU 的软件测试。该库已通过 TÜV SÜD 认证，符合 ISO26262:2018 ASIL B 的 LFM。C28x_STL 直接在 CPU 上运行，并有效地测试 CPU 寄存器、CPU 指令、CPU 标志、FPU、TMU 和 VCU-CRC 功能的子集。VCU 中的 Viterbi 和复杂数学指令未包含在 C28x_STL 中，不得用于安全相关软件。

为了运行这些测试，C28x_STL 会占用程序存储器的存储空间和专用的执行 RAM 空间。所有 C28x_STL 测试本质上都具有破坏性，无法将系统恢复到原始状态。由于 C28x_STL 测试和报告 CPU 本身的运行状况，并且无法有效地保存和恢复系统状态，因此必须将其集成到应用的启动部分。系统集成商应启用看门狗，确保应用免受失控代码的影响。

系统集成商必须查阅 C28x_STL 用户指南，了解将该库集成到主机应用程序的所有方面。

4.3.2.2 运行详细信息 – CLA 自检库

CLA_STL 实现 CLA2 - CLA 软件测试。与 C28x_STL 类似，CLA_STL 的启动测试在本质上也具有破坏性，应在启动操作期间运行。CLA_STL 的运行时测试包含大部分旨在与主机应用程序一同运行的测试。CLA 主机应用程序必须为运行时测试分配时间和空间。CPU 必须同时运行 CLA_STL POST 和 PEST 测试以获得更高的诊断覆盖率。有关适用于 CLA_STL 的确切 DC 要求，请参阅随 CSP 提供的 SPS。

系统集成商必须查阅 CLA_STL 用户指南，了解将该库集成到主机应用程序的所有方面。

4.3.2.3 运行详细信息 – SDL

表 4-3 是 SDL 软件模块和 API 到安全特性和诊断的映射。

表 4-3. 模块到安全机制映射

模块 名称	唯一标识符
STL_CAN_RAM	CAN4、CAN15
STL_CPU_REG	无唯一标识符，为 IEC 60730 添加
STL_CRC	FLASH2
STL_March	SRAM3
STL_OSC_CT	CLK2
STL_OSC_HR	OTTO1、CLK3
STL_PIE_RAM	PIE6
sdl_ex_dcsm_ffi	无唯一标识符，演示使用 DCSM 防止干扰
sdl_ex_flash_ecc_test	FLASH6
sdl_ex_flash_prefetch_test	FLASH8
sdl_ex_mcd_test	CLK12
sdl_ex_ram_access_protect	SRAM10
sdl_ex_ram_ecc_parity_test	SRAM13、SRAM14
sdl_ex_watchdog	CLK10

4.3.3 C2000 安全 STL 软件开发流程

C28x-STL 和 CLA-STL 是使用通过 TUV-SUD 认证的 TI 内部软件开发流程规范开发的，该规范针对基线、汽车和功能安全的软件开发流程。（对于功能安全，具体而言，目标是系统能力符合 IEC 61508 和 ISO 26262 标准）。可在此处获得 TI 软件开发流程的 TUV-SUD 证书。

软件开发流程规范描述了四个阶段（即评估、计划、创建和验证）中每个阶段所需交付物的内容。通过遵守本规范并遵循工作产品中包含的基本流程，包括方法和技术（IEC 61508-3、ISO 26262-6），可确保 TI SW/FW 开发实现 ASIL D (ISO 26262-6) 和 SIL 3 (IEC 61508-3) 等级的系统功能。

- 图 4-12 描述了与该流程支持的各种质量等级相关的 TI（经 TUV-SUD 认证）软件开发生命周期。
- 以文档形式记录详细的支持程序，可确保整个工程生命周期的功能安全。在每个开发阶段都应用了与目标标准的安全完整性等级相关的其他工具和技术。
- 按照规定的程序计划并执行功能安全审计和评估。根据目标标准和安全级别的要求，由具有足够独立性的合格人员来执行这些审计和评估。

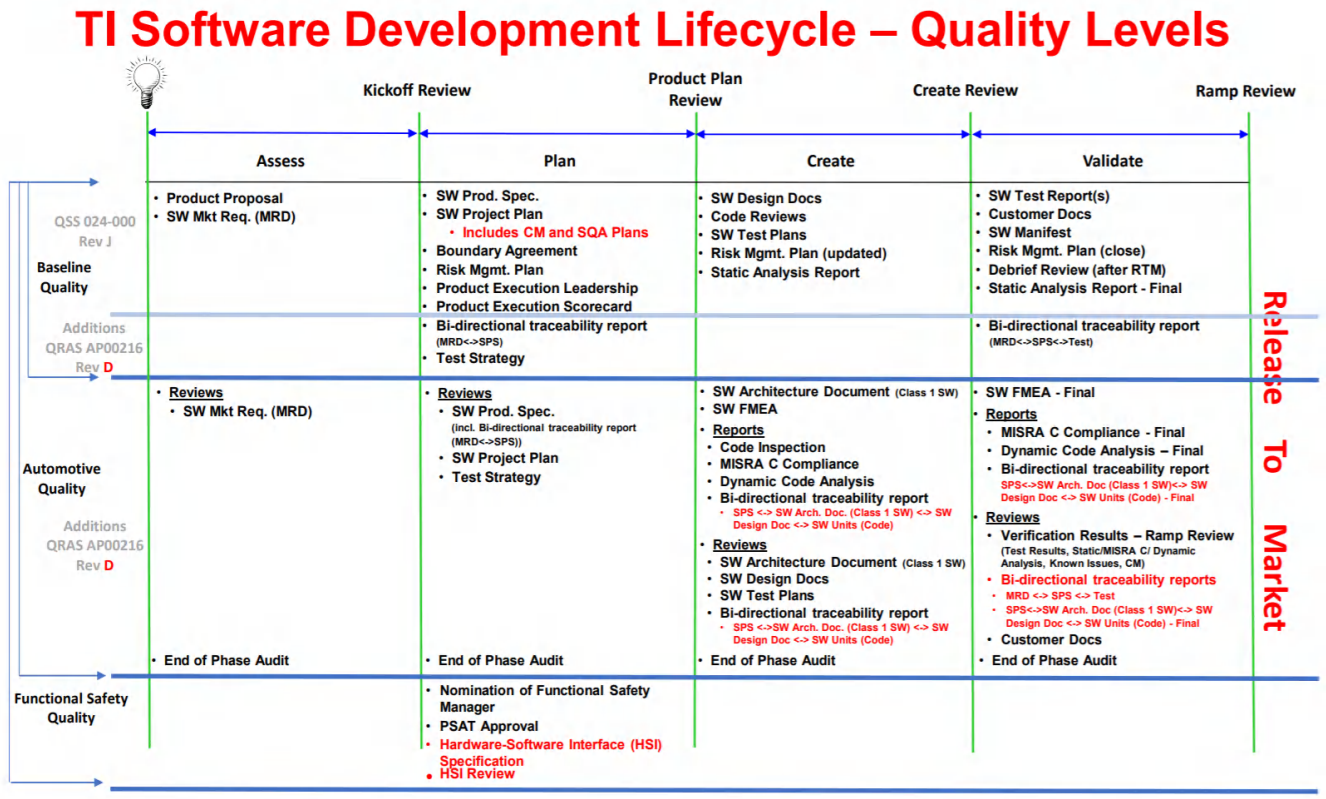


图 4-12. TI 软件开发生命周期 - 质量等级

4.3.4 STL 的软件交付表 (SDF)

对于与 C28x_STL 和 CLA_STL 一同交付的源代码，必须使用 SDF 文件中为每个 STL 提供的参考 MD5 信息进行验证。唯一的 MD5 签名适用于每个用来创建自检库的源文件。作为预防措施，强烈建议检查 MD5 签名，以确保源代码与 TÜV SÜD 认证的代码完全相同。

为了确保实现所需的基于诊断覆盖率的指标，不得以任何方式修改源代码，而是要按原样使用。违反该条件将导致 CLA_STL 的运行出现潜在失效，并可能无法满足所需的安全要求。

SDF 文件作为合规性支持包 (CSP) 的一部分提供。

4.4 TMS320F28004x MCU 安全实现

4.4.1 假设的安全要求

需要通过 3 级校验器（VDA E-gas 概念）使用外部组件来实现以下假设的安全要求。

- 用于监控提供给 TMS320F28004x MCU 的电源的外部电压监测器
- 外部看门狗计时器（可用于诊断目的）
- 根据节 4.2.3 中定义的 TMS320F28004x MCU 安全状态将系统置于安全状态所需的组件。

4.4.2 TMS320F28004x MCU 上的示例性安全概念实现选项

TMS320F28004x 类器件支持一对具有异构非对称架构、指令集和软件工具的不同处理单元（C28x 和 CLA）。任一处理单元均可用来执行预期功能（主要实时控制功能）。安全功能（确保满足每个安全目标）可由其中一个处理单元利用另一个处理单元来实现，通过在单独的处理单元中运行软件互惠式比较来诊断随机硬件失效，从而为

处理单元提供高诊断覆盖率（ISO 26262-5:2018 的表 D.4 和 IEC 61508-2:2010 的表 A.4）。也可以利用 CPU 对于非法操作、非法结果和指令陷入的处理、CLA 对于非法操作和非法结果的处理、内部看门狗 (WD) 等安全机制。CLA 的软件测试 和 CPU 的软件测试可用于实现诊断功能的潜在故障覆盖。异构 CPU 内核在实现这种互惠式比较的同时最大限度地降低了共模失效的可能性，从而提高了诊断覆盖的可靠性。对于时钟、电源和复位等共因失效，应使用外部看门狗。以下是一些定义：

- 预期功能：在 TMS320F28004x 上实现的控制应用（PFC、DCDC、牵引逆变器等）
- 安全功能：降低风险，并根据 HARA 确定的安全目标实现
  - 示例：防止过流、过压/欠压、过温、正向/反向扭矩等
  - 对于两个永久性故障，应满足 >= 60% LFM
- 诊断功能：确保安全功能在需要时正确运行
  - 对于 ISO 26262:2018（针对 ASIL B 合规性）系统，应满足 >= 60% LFM

以下是可在 TMS320F28004x 上实现的安全概念选项。

4.4.2.1 安全概念实现：选项 1

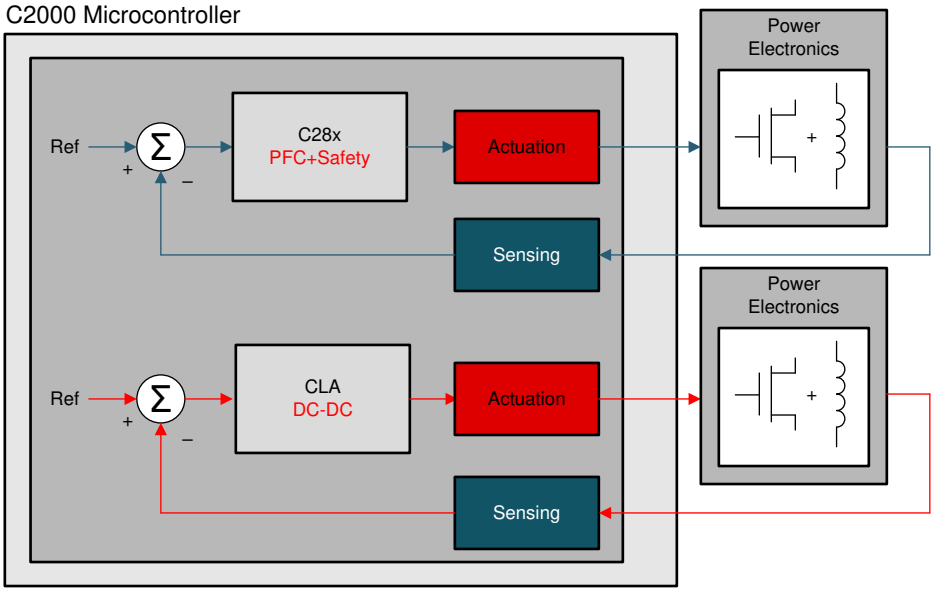


图 4-13. 安全概念实现选项 1

- 预期功能：可在 C28x 和 CLA 上实现。
- 安全功能：在 C28x 或 CLA 上实现。
  - 可通过软件互惠式比较来满足 SPFM
- 诊断功能：在另一个处理单元上实现。
  - 可通过 CLA 的软件测试或 CPU 的软件测试来满足 LFM

4.4.2.2 安全概念实现：选项 2

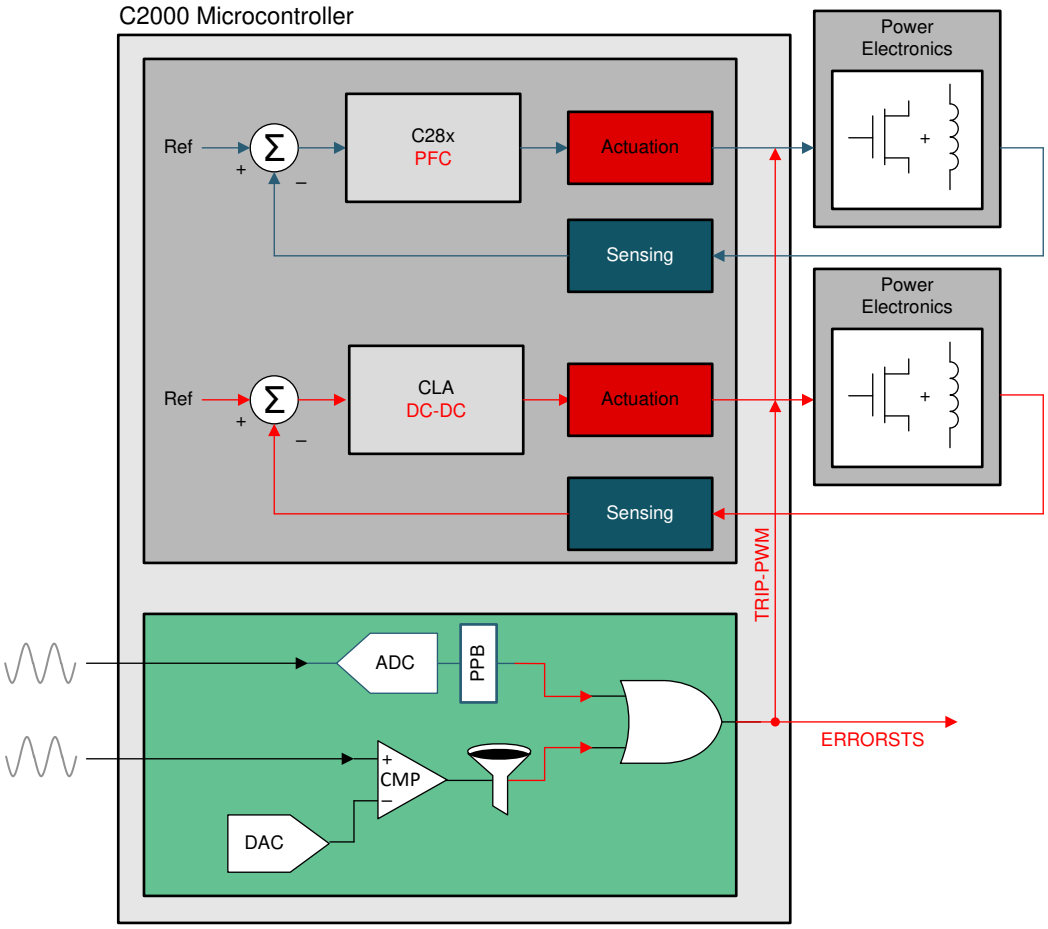


图 4-14. 安全概念实现选项 2

- 预期功能：可在 C28x 和 CLA 上实现。
- 安全功能：使用 ADC-PPB、CMPSS、SDFM 次级滤波器、CLB 等硬件模块实现。
  - 安全目标的 SPFM 可通过用于实现安全功能的模块之间的硬件冗余、静态配置寄存器的定期软件读回等来满足。
- 诊断功能：使用 ADC-PPB、CMPSS、SDFM 次级滤波器、CLB 等硬件模块实现
  - 可通过包括错误测试在内的功能软件测试等来满足 LFM。

5 安全要素简述

本节简要描述了 TMS320F28004x MCU 器件系列的各要素，这些要素根据系统通用硬件的器件分类进行了整理，如图 5-1 所示。有关上述任何模块的完整功能描述，请参阅器件特定技术参考手册。在对硬件元器件进行简要描述之后，本文档列出了可用于为硬件元器件提供诊断覆盖的主要安全机制。一些安全标准要求为主要诊断措施提供诊断覆盖（例如，ISO 26262:2018 中的潜在故障指标要求）。这些措施被称为诊断测试。“软件”和“硬件/软件”类型的初步诊断涉及在处理单元上执行软件，也涉及使用许多 MCU 器件，如互连、存储器（闪存、SRAM 和 ROM）和 TMS320F28004x MCU 基础设施组件（时钟、电源、复位和 JTAG）。为确保完整实现初步诊断及其相关的诊断覆盖率值，需要采取一些保护措施以在各处理单元上执行初步诊断。建议对有助于处理单元成功运行的 MCU 器件实现适当的诊断测试组合。有关这些器件的诊断，请参阅本安全手册中的相应章节。

如果针对初步诊断措施存在单独的诊断措施测试，则会将测试与相应的硬件元器件一同提及。

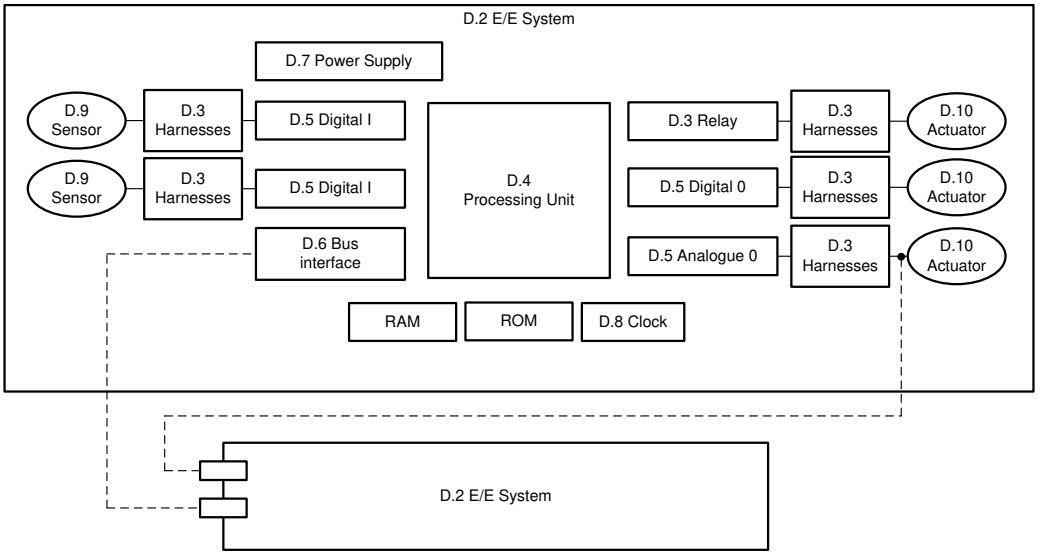


图 5-1. 系统的通用硬件

5.1 TMS320F28004x MCU 基础设施组件

5.1.1 电源

C2000 MCU 器件系列需要一个外部器件来提供必要的电压和电流以确保正常运行。为内核 (1.2V)、模拟 (3.3V)、闪存 (3.3V) 和 I/O 逻辑 (3.3V) 提供了独立的电压轨。以下机制可用于提高 C2000 MCU 电源的诊断覆盖率。

- 外部电压监控器
- 外部看门狗（使用 GPIO 或串行接口）
- 内部看门狗 (WD)
- 欠压复位 (BOR)
- 控制寄存器的多位使能键
- 针对控制寄存器的锁定机制
- 写入配置的软件读回
- 静态配置寄存器的定期软件读回
- 在线监测温度
- 关键寄存器的 EALLOW 和 MEALLOW 保护功能

备注

- 在进行安全分析时，假设在系统级具有独立的电压监控。
- 器件可由在系统印刷电路板 (PCB) 上组合在一起的多个电源轨来实现。为了确保正确运行电源诊断，建议针对每一个成组的电源轨安排一个电压监控器。
- 外部电压监控器以及 TMS320F28004x MCU 的共模失效分析可用于在电压生成和监控电路中确定从属关系。
- 客户可以考虑使用 TI 的 TPS6538x 电源和安全配套器件在系统级进行电压监控。

5.1.2 时钟

TMS320F28004x MCU 器件系列产品主要是同步逻辑器件，因此需要时钟信号才能正常运行。时钟管理逻辑包括时钟源、时钟生成逻辑（包括锁相环 (PLL) 的时钟倍乘）、时钟分频器和时钟分配逻辑。用于对时钟管理逻辑进行编程的寄存器位于系统控制模块内。以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 时钟丢失检测 (MCD)
- 使用 CPU 计时器进行时钟完整性检查
- 使用 HRPWM 进行时钟完整性检查
- 双路时钟比较器 (DCC) - 0 类
- 通过 XCLKOUT 对时钟进行外部监测
- 内部看门狗 (WD)
- 外部看门狗
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 使用片上计时器进行 PLL 锁定性能评测
- 外设时钟门控 (PCLKCR)
- 电子保险丝 ECC

以下测试可用作该模块的诊断用测试，以满足潜在故障指标要求：

- 看门狗 (WD) 操作的软件测试
- 时钟丢失检测功能的软件测试

备注

- 在使用计时器 2 检查时钟完整性时，通过设置更严格的界限可以获得更高的诊断覆盖率。
- TI 建议使用外部看门狗而不是内部看门狗，以降低共模失效导致的风险。由于其他失效模式可被更高级的看门狗检测出来，相对于单一阈值看门狗，TI 还建议使用一个具有程序序列的窗口式或问答式看门狗。
- 在 XCLKOUT 引脚上驱动一个高频时钟输出有可能会产生电磁干扰 (EMI)。在通过 IO 发出之前，需要对所选时钟进行适当调节。

5.1.3 复位

作为启动过程的一部分，加电复位 (PORn) 会生成一个内部热复位信号以复位大部分数字逻辑。热复位也可以作为具有开漏实现的 I/O 引脚 (XRSn) 在器件级提供。NMI 看门狗和其他看门狗等诊断功能可以发出热复位。更多有关复位功能的信息，请参阅器件特定数据表。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 热复位的外部监测 (XRSn)
- 复位原因信息
- 复位的软件测试
- 复位引脚上的干扰滤波
- NMIWD 影子寄存器
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- NMIWD 复位功能
- 外设软复位 (SOFTPRES)
- 内部看门狗 (WD)
- 外部看门狗

以下测试可用作该模块的诊断用测试，以满足潜在故障指标要求：

- 看门狗 (WD) 操作的软件测试

备注

- 由于监测到的复位信号与内部看门狗相互作用，内部看门狗不是复位诊断的一个可行选项。
- 客户可以考虑使用 TI 的 TPS6538x 电源和安全配套器件在系统级进行复位监控。

5.1.4 系统控制模块和配置寄存器

系统控制模块包含用于配置时钟、模拟外设设置和其他系统相关控制的存储器映射寄存器。该系统控制模块也负责生成系统复位的同步并传递热复位 (XRSn)。配置寄存器包括外设中不需要定期更新的寄存器。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 控制寄存器的多位使能键
- 针对控制寄存器的锁定机制
- 写入配置的软件读回
- 静态配置寄存器的定期软件读回
- 在线监测温度
- 外设时钟门控 (PCLKCR)
- 外设软复位 (SOFTPRES)
- 关键寄存器的 EALLOW 和 MEALLOW 保护功能
- ERRORSTS 功能的软件测试
- 外设访问保护 - 0 类

备注

- 检查时钟和复位部分，因为这些特性由系统控制模块严密控制。
- 客户可以考虑使用 TI 的 TPS6538x 电源和安全配套器件在系统级进行 ERRORSTS 引脚监控。

5.1.5 电子保险丝静态配置

借助电子保险丝结构，TMS320F28004x MCU 器件系列支持某些功能（例如模拟宏的修整值）的引导时间配置。在由一个自动负载功能执行的加电复位之后，系统将自动读取电子保险丝。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 电子保险丝自动负载自检
- 电子保险丝 ECC

以下测试可用作该模块的诊断用测试：

- 电子保险丝 ECC 逻辑自检
- SRAM ECC
- SRAM 奇偶校验

- SRAM 的软件测试
- 静态存储器内容的 VCU CRC 检查

5.1.6 JTAG 调试、跟踪、校准和测试访问

TMS320F28004x MCU 器件系列支持在 IEEE 1149.1 JTAG 调试端口上实现调试、测试和校准。物理调试接口在内部连接至一个 TI 调试逻辑 电路(ICEPICK)，该逻辑电路针对到测试、调试和校准逻辑的访问进行仲裁。为了实现最简单的制造板测试，边界扫描并行连接至 ICEPICK 以支持不含前导码扫描序列的用例。以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- JTAG 端口的硬件禁用
- 内部看门狗 (WD)
- 外部看门狗

5.2 处理元件

5.2.1 C28x 中央处理单元 (CPU)

CPU 是一个 32 位定点处理器，具有浮点、Viterbi、复杂数学和 CRC 单元 (VCU) 以及三角函数加速器 (TMU) 协处理器。该器件借鉴了数字信号处理的优异特性；精简指令集计算 (RISC)；以及微控制器架构、固件和工具集。CPU 的特性包括修改后的 Harvard 架构和循环寻址。RISC 特性是单周期指令执行和寄存器到寄存器操作。CPU 修改后的 Harvard 架构使指令和数据获取能够并行执行。CPU 通过六个独立的地址/数据总线执行该操作。其独特的架构使其能够在 CPU 外部（但在片上）集成安全特性，以提高诊断覆盖率。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 软件互惠式比较
- CPU 的软件测试
- 静态配置寄存器的定期软件读回
- 存储器访问保护机制
- CPU 对于非法操作、非法结果和指令陷入的处理
- 内部看门狗 (WD)
- 外部看门狗
- 信息冗余技术
- 栈溢出检测
- 嵌入式实时分析和诊断 (ERAD)

以下测试可用作该模块的诊断用测试：

- VCU CRC 自动覆盖

备注

缓解 CPU 子系统中的共因失效的措施：共因失效是在硅器件中实现安全相关设计时涉及的众多重要失效模式中的一种。硬件和软件从属失效的影响是在定性基础上估计的，因为不存在通用且足够可靠的方法用于量化此类失效。系统集成商应根据 ISO 26262-11:2018、第 4.7 节和 IEC 61508-2:2010 附录 E（BetaIC 方法）的输入进行详细分析。

5.2.2 控制律加速器

控制律加速器 (CLA) 是一个完全可编程的独立 32 位浮点数学加速器，具有独立的 ISA 和独立的编译器，有助于并发控制环路执行。CLA 的低中断延迟使其能够“及时”读取 ADC 样本。这显著降低了 ADC 采样到输出延迟，从而实现了更快的系统响应和更高的 MHz 控制环路。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 软件互惠式比较
- CLA 的软件测试
- CLA 对于非法操作和非法结果的处理
- 写入配置的软件读回
- 静态配置寄存器的定期软件读回

- 信息冗余技术
- 使用 CPU 进行 CLA 活跃度检查
- 存储器访问保护机制
- 禁用未使用的 CLA 触发源

以下分配给 CLA 的 SRAM 测试可用作该模块的诊断用测试：

- 静态配置寄存器的定期软件读回
- 包括错误测试在内的功能软件测试

5.3 存储器（闪存、SRAM 和 ROM）

5.3.1 嵌入式闪存

嵌入式闪存是一个与 C28x CPU 紧密耦合的非易失性存储器。每个 CPUSS 都有专用的闪存。CLA 或 DMA 无法访问该闪存。虽然也可进行数据访问，但闪存主要用于 CPU 指令访问。根据器件频率和闪存等待状态配置，访问闪存可能需要多个 CPU 周期。闪存包装程序逻辑提供预取和数据缓存以提高性能。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 闪存 ECC
- 静态存储器内容的 VCU CRC 检查
- 闪存阵列中的位多路复用
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 闪存程序验证和擦除验证检查
- 闪存预取、数据缓存和等待状态的软件测试
- 内部看门狗 (WD)
- 外部看门狗
- CPU 对于非法操作、非法结果和指令陷入的处理
- 信息冗余技术

以下测试可用作该模块的诊断用测试：

- ECC 逻辑的软件测试
- VCU CRC 自动覆盖

5.3.2 嵌入式 SRAM

TMS320F28004x MCU 器件系列具有以下类型的 SRAM（它们具有不同的特性）。

- 专用于每个 CPU（M0、M1）
- 在 CPU 及其自带的 CLA 之间共享 (LSx RAM)
- 用于在处理器之间发送和接收消息 (MSGRAM)

所有这些 RAM 均高度可配置，以实现对来自不同主器件的写入访问和获取访问的控制。所有专用 RAM 均启用 ECC 特性（数据和地址），共享 RAM 启用奇偶校验特性（数据和地址）。每个 RAM 都自带控制器，可为相应的 RAM 实现访问保护、安全相关特性和 ECC/奇偶校验特性。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- SRAM ECC
- SRAM 奇偶校验
- SRAM 的软件测试
- SRAM 存储器阵列中的位多路复用
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 数据清理以检测/校正存储器错误
- 静态存储器内容的 VCU CRC 检查
- 包括错误测试在内的功能软件测试
- 存储器访问保护机制
- 针对控制寄存器的锁定机制

- 信息冗余技术
- CPU 对于非法操作、非法结果和指令陷入的处理
- 内部看门狗 (WD)
- 外部看门狗
- CLA 对于非法操作和非法结果的处理
- 存储器开机自检 (MPOST)

以下测试可用作该模块的诊断用测试：

- ECC 逻辑的软件测试
- 奇偶校验逻辑的软件测试
- VCU CRC 自动覆盖

5.3.3 嵌入式 ROM

TMS320F28004x MCU 器件系列具有以下类型的 ROM：

- 引导 ROM 可帮助引导器件，并且包含用于安全初始化、器件校准和支持不同引导模式的功能
- 安全 ROM 功能的开发并非为了满足任何系统功能 (ISO 26262-6:2018/IEC 61508-3:2010) 的要求，不应在功能安全应用中使用。
- CLA 数据 ROM 包含用于 CLA 应用的数学表

可通过执行以下测试来诊断该模块（以提供特定功能的诊断覆盖）：

- 静态存储器内容的 VCU CRC 检查
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 包括错误测试在内的功能软件测试
- CPU 对于非法操作、非法结果和指令陷入的处理
- 内部看门狗 (WD)
- 外部看门狗
- 上电预运行安全检查
- 存储器开机自检 (MPOST)
- 软件互惠式比较

以下测试可用作该模块的诊断用测试：

- CLA-ROM 的背景 CRC (CLAPROMCRC)
- VCU CRC 自动覆盖

5.4 包括总线仲裁在内的片上通信

5.4.1 器件互连

器件互连将器件内的多个主器件和从器件链接在一起。器件互连逻辑电路包括各种总线主器件（CPU、CLA、DMA）通过外设和存储器处理事务时所需的静态主器件选择多路复用器、动态仲裁器和协议转换器。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- 内部看门狗 (WD)
- 外部看门狗
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- CPU 对于非法操作、非法结果和指令陷入的处理
- CLA 对于非法操作和非法结果的处理
- 传输冗余
- 硬件冗余
- 关键寄存器的 EALLOW 和 MEALLOW 保护功能

5.4.2 直接存储器访问 (DMA)

直接存储器访问 (DMA) 模块提供了一种在外设和/或存储器之间传输数据而无需 CPU 干预的硬件方法，从而释放了带宽给其他系统功能使用。此外，DMA 还能够在数据传输时对数据进行正交重排，以及在缓冲区之间对数据执行“乒乓”操作。这些特性对于将数据结构化为块以实现优化的 CPU 处理非常有用。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 信息冗余技术
- 传输冗余
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 包括错误测试在内的功能软件测试
- DMA 溢出中断
- 存储器访问保护机制
- 禁用未使用的 DMA 触发源

以下 SRAM 测试可用作该模块的诊断用测试：

- 静态配置寄存器的定期软件读回
- 包括错误测试在内的功能软件测试

5.4.3 增强型外设中断扩展器 (ePIE) 模块

增强型外设中断扩展器 (ePIE) 模块用于将外设中断连接至 C28x CPU。它基于每个中断提供可配置的屏蔽。PIE 模块包括一个本地 SRAM，用于保存每个中断的中断处理程序地址。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- PIE 双 SRAM 硬件比较
- SRAM 的软件测试
- 包括错误测试在内的 ePIE 运行软件测试
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 为未使用的中断维护中断处理程序
- 在线监测中断和事件
- 硬件冗余

以下测试可用作该模块的诊断用测试：

- PIE 双 SRAM 比较检查

5.4.4 双区域代码安全模块 (DCSM)

双代码安全模块 (DCSM) 是该器件中包含的安全特性。它可防止未经授权的人员访问和查看片上安全存储器（和其他安全资源）。它还可防止对专有代码进行复现和反向工程。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 控制寄存器的多位使能键
- 链路指针的多数表决和错误检测
- 静态配置寄存器的定期软件读回
- 包括错误测试在内的功能软件测试
- 写入配置的软件读回
- CPU 对于非法操作、非法结果和指令陷入的处理
- 静态存储器内容的 VCU CRC 检查
- 外部看门狗
- 硬件冗余

以下测试可用作该模块的诊断用测试：

- VCU CRC 自动覆盖

5.4.5 交叉开关 (X-BAR)

交叉开关 (X-BAR) 可灵活连接各种配置中的器件输入、输出和内部资源。该器件总共包含三个 X-BAR：输入 X-BAR、输出 X-BAR 和 ePWM X-BAR。输入 X-BAR 可以访问每个 GPIO，并可将每个信号路由到任何（或多个）IP 块（例如，ADC、eCAP、ePWM 等）。只需提供任何 GPIO 引脚，即可实现这种灵活性，从而解除了外设多路复用的一些限制。ePWM X-BAR 连接至每个 ePWM 模块的数字比较 (DC) 子模块，以执行跳变区等操作。GPIO 输出 X-BAR 从器件内部获取信号并将它们输出至 GPIO。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- 硬件冗余
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- X-BAR 标志的软件检查

5.4.6 计时器

CPU 子系统配有三个 32 位 CPU 计时器 (TIMER0/1/2)。该模块为器件提供操作系统 (OS) 计时器。OS 计时器功能用于根据需要生成内部事件触发器或中断，以提供安全关键功能的定期运行。该模块还具备时钟监测功能。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 使用次级自由运行计数器进行 1oo2 软件表决
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 包括错误测试在内的功能软件测试

5.5 数字 I/O

5.5.1 通用输入/输出 (GPIO) 和引脚多路复用

通用输入/输出 (GPIO) 模块提供内部模块 I/O 功能到器件引脚的软件可配置映射。可以单独选择这些引脚以作为数字 I/O 运行（也称为 GPIO 模式），也可以将它们连接到多个外设 I/O 信号中的一个。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 针对控制寄存器的锁定机制
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 使用 I/O 环回的功能软件测试
- 硬件冗余

5.5.2 增强型脉宽调制器 (ePWM)

增强型脉宽调制器 (ePWM) 外设是数字电机控制和电力电子系统的关键要素。一些 ePWM 模块实例支持高分辨率脉宽调制器 (HRPWM) 模式以提高时间分辨率。更多有关支持 HRPWM 模式的 ePWM 实例的信息，请参阅器件特定数据表和参考手册。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- 硬件冗余
- eCAP 对 ePWM 的监测
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 针对控制寄存器的锁定机制
- 使用 XBAR 进行 ePWM 故障检测
- ePWM 同步检查
- ePWM 应用级安全机制
- 在线监测中断和事件
- ADC 对 ePWM 的监测

5.5.3 高分辨率 PWM (HRPWM)

HRPWM 模块提高了采用传统方式产生的数字脉宽调制器 (PWM) 的时间分辨率水平。HRPWM 通常在 PWM 分辨率低于约 9-10 位时使用。HRPWM 基于微边沿定位器 (MEP) 技术。MEP 逻辑能够通过细分传统 PWM 发生器的一个粗略系统时钟来非常精细地定位边沿。时间阶跃精度约为 150ps。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- HRPWM 内置自检和诊断功能
- 硬件冗余
- eCAP 对 ePWM 的监测
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 针对控制寄存器的锁定机制

5.5.4 增强型捕捉 (eCAP)

增强型捕捉 (eCAP) 模块为外部事件的准确计时十分重要的系统提供输入捕捉功能。eCAP 模块特性包括测量旋转机械的速度（例如，通过霍尔传感器感应齿状链轮）、位置传感器脉冲之间的经过时间测量、脉冲序列信号的周期和占空比测量，以及解码来自占空比编码电流/电压传感器的电流或电压幅值。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- 信息冗余技术
- eCAP 对 ePWM 的监测
- 静态配置寄存器的定期软件读回

- 写入配置的软件读回
- eCAP 应用级安全机制
- 硬件冗余

备注

使用无传感器定位算法则可以通过对 eCAP 结果进行合理性检查来实现信息冗余。

5.5.5 高分辨率捕捉 (HRCAP)

高分辨率捕捉 (HRCAP) 外设可在数百皮秒内测量典型分辨率下的外部脉冲宽度。除了硬件校准块外，该模块还包括用以实现连续在线校准的捕捉通道，这大大减少了要校准的软件开销。HRCAP 输入可以使用 X-BAR 连接到 HRPWM 输出以启用周期性测试。HRCAP 增强功能已添加到 eCAP 6 和 eCAP 7。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- 硬件冗余
- HRCAP 对 HRPWM 的监测
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- HRCAP 校准逻辑测试特性

5.5.6 增强型正交编码器脉冲 (eQEP)

增强型正交编码器脉冲 (eQEP) 模块用于直接连接线性或旋转增量编码器，以便从高性能运动和位置控制系统所用的旋转机器中获得位置、方向和速度信息。以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- eQEP 正交看门狗
- 信息冗余技术
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- eQEP 应用级安全机制
- 硬件冗余

以下测试可用作该模块的诊断用测试：

- 正交看门狗功能的 eQEP 软件测试

备注

使用无传感器定位算法则可以通过对 eQEP 结果进行合理性检查来实现信息冗余。

5.5.7 Σ-Δ 滤波器模块 (SDFM)

Σ-Δ 滤波器模块 (SDFM) 是一种四通道数字滤波器，专为电机控制应用中的电流测量和旋转变压器位置解码而设计。每个通道都可以接收一个独立的 Δ-Σ 调制器位流。位流由四个独立可编程的数字抽取滤波器进行处理。这组滤波器包括一个快速比较器，用于过流和欠流监测的即时数字阈值比较。

- 用于在线监测的 SDFM 比较器滤波器
- 信息冗余技术
- SD 调制器时钟故障检测机制
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 包括错误测试在内的功能软件测试
- 硬件冗余

5.5.8 外部中断 (XINT)

借助 XINT 模块，可以使用 GPIO 引脚将来自外部源的中断提供给器件。该模块允许配置 GPIO 以将其选择为中断源。也可以使用该模块来配置中断的极性。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 硬件冗余

5.6 模拟 I/O

5.6.1 模数转换器 (ADC)

模数转换器 (ADC) 模块用于将模拟输入转换为数字值。结果被存储在内部寄存器内，用于之后的 CLA、DMA 或 CPU 传递。TMS320F28004x MCU 器件系列产品最多实现三个带有共享通道并用于快速转换的模块（乒乓操作方法）。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- DAC 至 ADC 环回检查
- ADC 信息冗余技术
- ADC 的开路/短路检测电路
- 写入配置的软件读回
- 静态配置寄存器的定期软件读回
- 通过改变采集窗口来检查 ADC 信号质量
- ADC 输入信号完整性检查
- ADC 对 ePWM 的监测
- 硬件冗余
- 禁用 ADC 未使用的 SOC 输入源

备注

- 应按照器件特定数据表中的说明监控 ADC 模块电压。
- 为了降低共模失效的可能性，用户应考虑使用非相邻引脚和不同的电压基准来实现多个通道（信息冗余）。

5.6.2 缓冲数模转换器 (DAC)

缓冲 DAC 模块由一个内部基准 DAC 和一个能够驱动外部负载的模拟输出缓冲器组成。DAC 输出上集成的下拉电阻器有助于在禁用输出缓冲器时提供一个已知的引脚电压。软件写入 DAC 值寄存器可立即生效，也可以与 PWMSYNC 事件同步。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- DAC 至 ADC 环回检查
- 针对控制寄存器的锁定机制
- 写入配置的软件读回
- 静态配置寄存器的定期软件读回
- DAC 至比较器环回检查
- 硬件冗余

以下 ADC 和 CMPSS 测试可用作该模块的诊断用测试：

- 包括错误测试在内的功能软件测试
- 静态配置寄存器的定期软件读回

5.6.3 比较器子系统 (CMPSS)

比较器子系统 (CMPSS) 由模拟比较器和配套组件组成，它们组合成一种拓扑结构，可用于峰值电流模式控制、开关模式电源、功率因数校正和电压跳变监测等电源应用。比较器子系统围绕一对模拟比较器而构建，有助于检测信号异常情况（包括高/低阈值）。比较器的正输入始终由外部引脚驱动，但负输入可由外部引脚或内部可编程的 12 位 DAC 驱动。每个比较器输出都会通过一个可编程的数字滤波器，该滤波器可以去除伪跳变信号。斜坡发生器电路可用于控制子系统中一个比较器的内部 DAC 值。

以下测试可用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的功能软件测试
- 硬件冗余
- 写入配置的软件读回
- 静态配置寄存器的定期软件读回
- 针对控制寄存器的锁定机制
- 通过 ADC 进行 VDAC 转换
- CMPSS 斜坡发生器功能检查

以下 ADC 测试可用作该模块的诊断用测试：

- 包括错误测试在内的功能软件测试
- 静态配置寄存器的定期软件读回

5.6.4 可编程增益放大器 (PGA)

可编程增益放大器 (PGA) 用于放大输入电压，以增加下游 ADC 和 CMPSS 模块的动态范围。集成的 PGA 有助于使传统上需要外部独立放大器的许多控制应用降低成本和设计工作量。软件可选增益和滤波器设置使 PGA 能够满足各种性能需求。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- PGA 至 ADC 环回测试
- 硬件冗余
- 写入配置的软件读回
- 静态配置寄存器的定期软件读回

- 针对控制寄存器的锁定机制

5.7 数据传输

5.7.1 控制器局域网 (DCAN)

控制器局域网 (DCAN) 接口提供与基于事件的触发互连的中等吞吐量，符合 CAN 协议。DCAN 模块需要一个外部收发器才能在 CAN 网络上运行。以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 使用 I/O 环回的功能软件测试
- 包括端到端安全状态恢复的信息冗余技术
- SRAM 奇偶校验
- SRAM 的软件测试
- SRAM 存储器阵列中的位多路复用
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 传输冗余
- DCAN 填充错误检测
- DCAN 格式错误检测
- DCAN 确认错误检测
- 位错误检测
- 消息中的 CRC
- 硬件冗余

以下测试可用作该模块的诊断用测试：

- 奇偶校验逻辑的软件测试

5.7.2 串行外设接口 (SPI)

串行外设接口 (SPI) 模块提供符合 SPI 协议的串行 I/O。SPI 通信通常用于与智能传感器和执行器、串行存储器以及外部逻辑（如看门狗器件）进行通信。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 使用 I/O 环回的功能软件测试
- 包括端到端安全状态恢复的信息冗余技术
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 传输冗余
- SPI 数据超限检测
- 硬件冗余

5.7.3 串行通信接口 (SCI)

该模块提供针对诸如 UART 等典型异步串行通信接口 (SCI) 协议的串行 I/O 功能。根据所使用的串行协议的不同，也许需要一个外部收发器。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 使用 I/O 环回的功能软件测试
- 消息中的奇偶校验
- 包括端到端安全状态恢复的信息冗余技术
- 超限错误检测
- SCI 中断错误检测
- 帧错误检测
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 传输冗余
- 硬件冗余

5.7.4 内部集成电路 (I2C)

内部集成电路 (I2C) 模块提供一个与 I2C 协议兼容的多主控串行总线。以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 使用 I/O 环回的功能软件测试
- I2C 数据确认检查
- 包括端到端安全状态恢复的信息冗余技术
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 传输冗余
- 使用片上计时器进行 I2C 访问延迟性能评测

5.7.5 快速串行接口 (FSI)

快速串行接口 (FSI) 是一种能够进行可靠、高速通信的串行外设。FSI 专门设计用于确保那些涉及跨隔离器件通信的系统场景的可靠、高速通信。FSI 包含独立发送器 (FSITX) 和接收器 (FSIRX) 内核。FSITX 和 FSIRX 内核是独立配置和运行的。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 包括错误测试在内的使用 I/O 环回的功能软件测试
- 包括端到端安全状态恢复的信息冗余技术
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 传输冗余
- FSI 数据超限/欠载检测
- FSI 帧超限检测
- FSI CRC 成帧检查
- FSI ECC 成帧检查
- FSI 帧看门狗
- FSI RX Ping 看门狗
- FSI 标签监控器
- FSI 帧类型错误检测
- FSI 帧结束错误检测
- FSI 寄存器保护机制

5.7.6 本地互连网络 (LIN)

支持的 LIN 模块符合 LIN 2.1 协议规范。可对该模块进行编程，以作为 SCI 或 LIN 运行。增强了 SCI 的硬件特性以实现 LIN 功能。SCI 模块是一个通用异步收发器 (UART)，可实现标准的非归零格式。例如，SCI 可用于通过一个 RS-232 端口或一条 K 线路进行通信。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- 使用 I/O 环回的功能软件测试
- 包括端到端安全状态恢复的信息冗余技术
- 传输冗余
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 数据奇偶校验错误检测
- 超限错误检测
- 帧错误检测
- LIN 物理总线错误检测
- LIN 无响应错误检测
- 位错误检测
- 校验和错误检测
- LIN ID 奇偶校验错误检测
- SCI 中断错误检测

- 使用片上计时器进行通信访问延迟性能评测

5.7.7 电源管理总线模块 (PMBus)

PMBus 模块提供了微控制器和器件之间的接口，该接口符合 SMI Forum PMBus 规范第 I 部分 1.0 版和第 II 部分 1.1 版的要求。PMBus 基于 SMBus，使用与 I2C 类似的物理层。该模块支持主模式和从模式。

以下测试用于诊断该模块（以提供特定功能的诊断覆盖）：

- I2C 数据确认检查
- 包括端到端安全状态恢复的信息冗余技术
- 静态配置寄存器的定期软件读回
- 写入配置的软件读回
- 传输冗余
- 消息中的 PMBus 协议 CRC
- 时钟超时

6 诊断简述

本节简要概述了 TMS320F28004x MCU 器件系列上可用的诊断机制。这些诊断机制按照图 5-1 中给出的器件分配进行排列。安全机制适用于多个组件时，根据适用的用例场景将其放置在适当的位置。有关诊断的详细描述或实现细节，请参阅器件特定技术参考手册。

6.1 TMS320F28004x MCU 基础设施组件

6.1.1 使用 CPU 计时器进行时钟完整性检查

建议使用 CPU 计时器模块来检测不正确的时钟频率以及时钟源之间的漂移。CPU 计时器 2 包含一个可编程计数器，可以选择该计数器的预分频值和时钟源。以系统时钟为参考时基，可以确定所选时钟与系统时钟之间的频率关系。更多有关所实现的时钟选择选项的信息，请参阅器件特定数据表。在使用计时器 2 检查时钟完整性时，通过设置更严格的界限可以获得更高的诊断覆盖率。通过对参考时钟和测量时钟使用不同的时钟源和不同的预分频值，可以减少共因失效。默认情况下不启用计时器诊断，必须通过软件启用。计时器模块采用的循环校验提供了一个自检的固有电平（自动覆盖），可考虑将其应用在延迟故障诊断中。

6.1.2 使用 HRPWM 执行时钟完整性检查

OTTO (HRPWM) 的校准逻辑可用于检测不正确的系统时钟 (SYSCLK) 频率。将需要测量频率的时钟配置为系统时钟，并执行自动校准函数。可以对照预定的值范围对从校准函数获得的结果进行校验，以检测不正确的时钟频率或频率漂移。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.1.3 关键寄存器的 EALLOW 和 MEALLOW 保护功能

EALLOW（CPU、DMA）和 MEALLOW (CLA) 保护功能支持对仿真和其他受保护寄存器执行写入访问。CPU (CLA) 可以使用 EALLOW (MEALLOW) 指令设置该位，并使用 EDIS (MEDIS) 指令清除该位。该保护功能可用于防止数据写入错误位置，这可能是超出边界、不正确的指针、栈溢出或损坏等情况所致。始终允许从受保护的寄存器中进行读取。一旦对受保护寄存器执行的写入完成，建议发出 EDIS（或 MEDIS）进行保护。

6.1.4 电子保险丝自动负载自检

电子保险丝提供了确保将电子保险丝值正确加载到所有寄存器的功能。该功能默认启用，并且不能通过软件更改配置。该过程中的任何错误都将通过 ERRORSTS 指示。发生错误时，器件复位被置位并重新尝试自动加载。

6.1.5 电子保险丝 ECC

电子保险丝使用 SECDED ECC 诊断来检测从保险丝 ROM 获取的配置值中的错误，并在可能时进行校正。通过 ERRORSTS 指示错误。该诊断默认为 ON，并且无法通过软件更改配置。它只涵盖了 EFUSE ROM 的数据位。发生错误时，器件复位被置位并重新尝试自动加载。

6.1.6 电子保险丝 ECC 逻辑自检

电子保险丝控制器有一个自检逻辑，该逻辑在电子保险丝运行之前自动执行。通过 ERRORSTS 和系统控制寄存器指示错误。只要发生错误，器件就会保持复位状态。

6.1.7 通过 XCLKOUT 对时钟进行外部监测

TMS320F28004x MCU 器件系列提供将选定的内部时钟信号导出以供外部监测的功能。通过在系统控制模块中对寄存器进行编程，可由软件对该特性进行配置。若要确定实现的外部时钟输出的数量以及可导出的内部时钟的寄存器映射，请参阅器件特定数据表。XCLKOUT 输出上的内部时钟导出默认情况下不启用，必须通过软件启用。

6.1.8 热复位的外部监测 (XRSn)

XRSn 热复位信号作为开漏 I/O 引脚实现。可使用一个外部监控器来检测对内部热复位控制信号状态的预期或者意外更改，并确保在置位时发出正确信号（例如，低电平持续时间）。错误响应、诊断的可测试性以及任一所需的软件要求由系统集成商所选择的外部监控器来定义。

6.1.9 外部电压监控器

德州仪器 (TI) 强烈建议使用一个外部电压监控器来监测所有的电压轨（VDDIO、VDDA 和 VDD）。电压监控器应在目标器件的建议运行条件下配置过压和欠压阈值，如器件特定数据表中所述。错误响应、诊断的可测试性以及任一所需的软件要求由系统集成商所选择的外部电压监控器来定义。

6.1.10 外部看门狗

外部看门狗有助于减少共模失效，因为它使用与被监测系统分离的时钟、复位和电源。错误响应、诊断的可测试性以及任一所需的软件要求由系统集成商所选择的外部看门狗来定义。

除了内部提供的看门狗外，德州仪器 (TI) 还强烈建议使用一个外部看门狗。内部或外部看门狗可以提供关于意外激活逻辑的指示，这会影响安全关键执行。任何从外部添加的看门狗都应包括对程序序列的时间和逻辑监测的组合 [IEC 61508-7:2010，第 A.9.3 条] 或其他适当方法，以便可以声称具有高诊断有效性。

6.1.11 复位引脚上的干扰滤波

干扰滤波器在器件的 XRSn 和 JTAG 复位时实现。这些结构可滤除输入复位引脚上的噪声和瞬态信号峰值，以减少复位电路的意外激活。干扰滤波器默认启用并连续运行。它们的行为不能通过软件更改。

6.1.12 JTAG 端口的硬件禁用

JTAG 调试端口能够被物理禁用以防止已部署系统中的 JTAG 访问。建议的方案是保持测试模式选择 (TMS) 为高电平。禁用 JTAG 端口还可以覆盖许多调试和跟踪活动的意外激活。

6.1.13 内部看门狗 (WD)

内部看门狗有两种运行模式：普通看门狗 (WD) 和窗口式看门狗 (WWD)。系统集成商可以选择使用一种模式或另一种模式，但不能同时使用两种模式。有关内部看门狗编程的详细信息，请参阅器件特定技术参考手册。WD 是一种传统的单阈值看门狗。用户为看门狗设定一个超时值并且必须在超时计数器终止前提供一个到看门狗的预先确定的 WDKEY。超时计数器的终止或者一个不正确的 WDKEY 会触发一个错误响应。WD 可在检测到失效时发出热系统复位或 CPU 可屏蔽中断。复位后启用 WD。

与 WD 实现相比，时间窗口的使用可检测其他时钟失效模式。用户设定上限和下限来创建一个时间窗口，在此期间，软件必须提供一个到看门狗的预先确定的 WDKEY。未在时间窗口内接收正确响应或不正确的 WDKEY 会触发一个错误响应。在检测到失效时，WWD 能够发出热系统复位或 CPU 可屏蔽中断。复位后默认启用常规 WD 运行。有关内部看门狗编程的详细信息，请参阅器件特定技术参考手册。

为避免内部看门狗 (WD) 和 CPU 的时钟输入出现共因失效，建议选择 INTOSC2 或 X1/X2 作为主 PLL 的时钟源。

6.1.14 针对控制寄存器的锁定机制

该模块包含一个用于保护关键控制寄存器的锁定机制。一旦设置了相关的 LOCK 寄存器位，对寄存器的写入访问就会受阻。锁定的寄存器无法通过软件进行更新。一旦锁定，只有执行复位才能解锁寄存器。

6.1.15 时钟丢失检测 (MCD)

时钟丢失检测器 (MCD) 采用安全诊断机制，可用于检测 PLL 参考时钟的失效。MCD 使用嵌入式 10MHz 内部振荡器 (INTOSC1)。该电路仅检测 PLL 参考时钟的完全丢失，不进行任何频率漂移检测。加电复位状态期间，默认启用 MCD 电路。该诊断可通过软件禁用。

6.1.16 NMIWD 复位功能

收到 NMI 后，软件可以尝试从 NMI 条件恢复。根据故障情况的严重程度和类型，恢复未必总能成功。在这种情况下，通过让独立的看门狗监测 NMI 恢复来提供额外的保护。如果尝试进行的恢复不成功，则会发出复位。可以根据器件的 FTTI 来配置复位超时（使用 NMIWDPRD）。

6.1.17 NMIWD 影子寄存器

在器件上使用两级冷和热复位方案可实现 NMIWD 影子寄存器。影子寄存器只通过加电复位来复位。这些寄存器用于在复位置位之前存储 NMIFLG 信息。应用软件可以使用该信息来提供有关上次热复位操作之前器件 NMI 状态的附加信息。

6.1.18 控制寄存器的多位使能键

一些模块包括支持避免无意识更新控制寄存器的特性。关键控制寄存器的多位密钥的实现就是这样一种特性（例如，EPWM_REGS.EPWMLOCK 等）。多位密钥对于避免意外激活特别有效。有关适用于诊断的寄存器的更多详细信息，请参阅器件特定技术参考手册。这种安全机制的运行是连续的，无法通过软件更改。可通过生成带有或不带有正确密钥的软件事务并观察更新的寄存器值来测试这种机制。

6.1.19 在线监测温度

内部温度传感器用于测量器件的结温。可通过内部连接，借助 ADC 对传感器的输出进行采样。这可通过设置 TSNSCTL 寄存器中的 ENABLE 位在 ADCB 的通道 ADCIN14 上启用。

6.1.20 静态配置寄存器的定期软件读回

配置寄存器通常在开始时配置一次，并在执行特定任务之前保持其值。配置寄存器的定期读回功能能够为这些寄存器的无意写入或干扰提供诊断。

通过将测试扩展到包括标志寄存器的读回，可以提高诊断覆盖率，这些标志寄存器预计在器件操作期间也保持不变（PLL 锁定状态、eQEP 相位误差标志等）。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

通过应用一些特定于模块的测试，可以进一步提高某些外设的诊断覆盖率，如下所示：

- 为了提高增强型外设中断扩展器 (ePIE) 的覆盖率，可以定期检查 PIE 标志寄存器，以确保通过读取 PIE 标志寄存器 (PIE_CTRL_REGS.PIEIFRx.all) 和外设中断标志寄存器来处理所有挂起的中断。
- 处理中断期间，ISR 例程可以检查外设和 PIE 模块中的中断标志，以确保正确的中断得到处理。

CLA 配置寄存器只能由 C28x CPU 访问，因此 CLA 模块的这种安全机制必须由 C28x CPU 执行。

6.1.21 外设时钟门控 (PCLKCR)

可以逐个外设进行时钟选通。这可用于禁用未使用的特性，这样它们就不会干扰已激活的安全功能。该安全机制在复位后启用。软件必须配置和禁用该机制才能使用特定外设。可以锁定特定配置以避免无意写入。

6.1.22 外设软复位 (SOFTPRES)

可以逐个外设保持复位。这可用于复位未使用的特性，这样它们就不会干扰已激活的安全功能。复位后，这些安全机制被禁用。软件必须配置并启用这些机制。

6.1.23 使用片上计时器进行 PLL 锁定性能评测

TMS320F28004x MCU 器件系列的时钟设置包括选择适当的时钟源、配置 PLL 倍频器、等待锁定状态，以及在设置内部锁定状态后将时钟切换到 PLL 输出。可以使用片上计时器来分析 PLL 锁定序列所需的时间，以检测 PLL 包装程序逻辑中的故障。一旦锁定 PLL，可以通过以下方式检查输出时钟的频率：

- 使用 CPU 计时器进行时钟完整性检查
- 使用 HRPWM 进行时钟完整性检查
- 通过 XCLKOUT 对时钟进行外部监测以确保正确的时钟输出

6.1.24 复位原因信息

该系统控制模块提供了一个状态寄存器 (RESC)，用于锁存最近发生的复位事件的原因。启动期间执行的应用软件可以检查该寄存器的状态，以确定上次复位事件的原因。软件可以根据这些信息来确定原因，并在需要时管理失效恢复。

6.1.25 写入配置的软件读回

为确保正确配置该模块中的存储器映射寄存器，建议由软件执行测试，通过读回内容来确认所有控制寄存器得到正确配置。该测试还为外设总线接口和外设互连网桥提供诊断覆盖。

CLA 配置寄存器只能由 C28x CPU 访问，因此 CLA 模块的这种安全机制必须由 C28x CPU 执行。

6.1.26 ERRORSTS 功能的软件测试

如图 4-8 所示，ERRORSTS 引脚是 MCU 安全概念的组成部分，用于向外部系统指示 MCU 内出现的严重错误。可以通过使用软件提供的方式之一（例如，通过更新 NMIFLGFRC.bit.CLOCKFAIL 来置位 CLOCLKFAIL NMIFLG）置位 ERRORSTS 引脚来检查 ERRORSTS 引脚是否正常运行以及 MCU 外部系统的错误处理。错误响应、诊断的可测试性以及任何必要的系统要求由系统集成商定义。

6.1.27 时钟丢失检测功能的软件测试

可通过配置 MCDCR.OSCOFF 来检查时钟丢失检测 (MCD) 功能是否正常运行。诊断测试可以检查时钟缺失 NMI 的问题和时钟缺失状态标志 (MCDCR.MCLKSTS) 的设置。

6.1.28 复位的软件测试

可以实现一个软件测试，用于检测基本功能以及复位源和复位逻辑的错误。除了 PORn 之外，每个复位源（包括外设复位、DEV_CFG_REGS.SOFTPRESx）均可在内部生成，并且可以通过确保正确设置复位原因寄存器并确保仅复位预期逻辑来检查基本复位功能。

为了确认各个外设是否正确接收到复位，软件可以运行特定于外设的功能测试并确认复位后外设的预期状态。根据外设的复杂性，该软件功能测试可以包括针对外设复杂特性的测试，其中包括确认复位正确传播所必需的误差测试。有关特定于外设的功能软件测试（包括误差测试），请参阅专为外设列出的器件特定安全机制。

6.1.29 看门狗 (WD) 操作的软件测试

内部看门狗运行的基本测试可通过软件执行，包括检查错误响应，方法是在编程阈值期间，配置维护 WDKEY 的预期下限和上限阈值，然后维护或不维护 WDKEY。如果复位对系统运行不利，可通过将内部看门狗配置为中断模式 (SCSR.WDENINT) 并在完成测试后恢复到复位模式来执行测试。

6.1.30 欠压复位 (BOR)

内部 BOR 电路可监测 VDDIO 电源轨的电压骤降，电压骤降会导致电源电压下降到工作范围之外。当 VDDIO 电压降至 BOR 阈值以下时，器件被强制复位，并且 XRSn 被下拉至低电平。XRSn 将保持复位状态，直到电压恢复到工作范围内。默认情况下启用 BOR。

6.1.31 双路时钟比较器 (DCC) - 0 类

双路时钟比较器模块可用于在定义的时间窗口内验证或监测 PLL (PLLRAWCLK) 的输出频率。在检查 PLL 时钟频率时，DCC 使用已知良好的参考时钟（即 INTOSC1、INTOSC2 或 XTAL）进行比较。如果 PLL 时钟频率偏离目标频率超过预定义阈值，DCC 将报告 ERROR 状态标志并向 PIE 发送中断。

通过在计数器 0 (DCCCNTSEED0) 和计数器 1 (DCCCNTSEED1) 之间以错误比率配置双路时钟比较器 (DCC) 以强制发生失效，可以检查 DCC 功能是否正常运行。然后可以检查失效标志/中断以验证 DCC 的功能。

6.1.32 外设访问保护 - 0 类

外设访问保护是一种故障避免措施，用于阻止来自每个主器件的意外访问。每个模块都有一个配置来控制要从每个主器件（CPU、CLA、DMA）提供服务的访问类型。在对外设访问保护寄存器进行编程后，每个主器件均能做到专门控制外设，以防止特定应用的使用对系统中其他主器件造成错误写入或破坏。这是通过使用每个外设的专用访问控制位来实现的，该控制位允许或禁止来自给定主器件的访问。每个外设在每个主器件上都有两个位限定符，用于解码允许的访问。有关详细信息，请参阅 *TMS320F28004x 技术参考手册* 中的“PERIPH_AC_REGS 寄存器”。

6.2 处理元件

6.2.1 CLA 对于非法操作和非法结果的处理

CLA 协处理器内置了可检测非法指令（非法操作码）的执行、浮点下溢或上溢情况的机制。在此类情况下，CLA 会中断 CPU。CPU 可以通过检查所需的 CLA 标志来解码中断原因。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.2.2 使用 CPU 进行 CLA 活跃度检查

CLA 本身不含独立看门狗。因此，建议由 CPU 定期执行活跃度检查。通常，使用顺序事件集来触发看门狗（例如，完成 CPU 任务 1、CLA 任务 1、CPU 任务 2 和 CLA 任务 2）。CLA 活跃度检查的输出可用作决定看门狗触发的任务之一，如图 6-1 所示。活跃度检查可以基于 VDA E-gas 概念 [6] 中所示的应用特定参数，以提高诊断覆盖率。

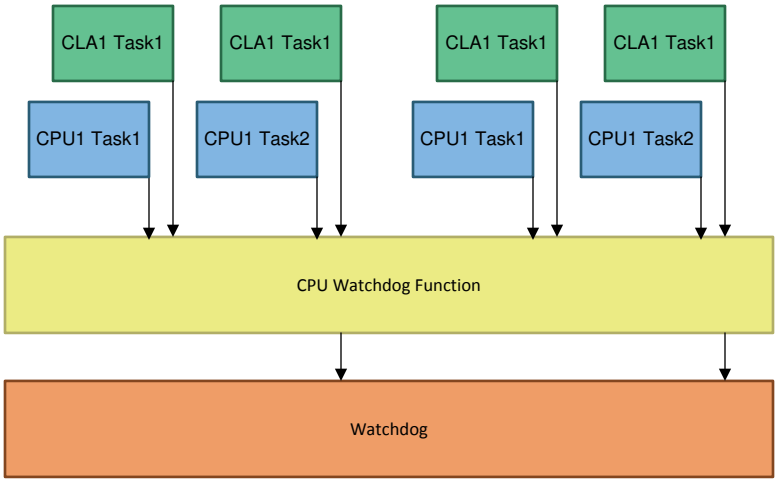


图 6-1. CLA 活跃度检查

6.2.3 CPU 对于非法操作、非法结果和指令陷入的处理

C28x CPU 包括可用作安全机制的针对非法操作、非法结果（下溢和上溢条件）和指令陷入（非法操作码）的诊断。对无效存储器范围的任何访问都将返回 0x00000000 数据。访问已擦除闪存（新器件的默认状态）将返回 0xFFFFFFFF。0x00000000 和 0xFFFFFFFF 均被解码为无效指令，因此已擦除的闪存或已清除的存储器或无效的地址将强制 CPU 执行 ITRAP。强烈建议安装软件句柄以支持硬件非法操作和指令陷入

CPU 非法操作、非法结果和指令陷入的示例包括：

- 非法指令
- *TMS320C28x 扩展指令集。技术参考手册*

6.2.4 软件互惠式比较

CPU 子系统有一对不同的处理单元（C28x 和 CLA），它们具有不同的架构和指令集。这使得一个处理单元能够用于处理时间关键部分代码（控制 CPU），而另一个处理单元（监督 CPU）则可以执行代码的非关键部分，执行诊断功能并监督控制 CPU 的执行。

如果在监督 CPU 的诊断功能期间发现故障，它可能会使 TMS320F28004x MCU 进入安全状态。根据 ISO 26262-5:2018 表 D.4，“在单独的处理单元中进行软件互惠式比较”这一概念充当 1oo1D 结构，为处理单元提供高诊断覆盖率。在 FTTI 过程中需要多次进行比较。互惠式比较是一种软件诊断特性，因此应注意避免共模失效。最终获得的覆盖率将取决于比较的质量（由交叉检查的扩展和频率决定）。提议的交叉检查机制支持硬件和软件的多样性，因为是使用具有不同指令集和编译器的不同处理器来实现这一点的。通过在两个内核中执行单独的算法，可以进一步增加多样性。如果在互惠式比较期间发现失效，可以通过软件触发 NMI，这反过来将置位 ERRORSTS。在运行期间，CLA 可以访问 GPIO_Data_Regs，它可以指示独立于 C28x 的 GPIO 引脚上的错误情况。

6.2.5 CLA 的软件测试

可以使用基于软件的自检库 (STL) 来测试各种 CLA 块（包括寄存器文件、控制单元、数据路径等）的完整性。根据安全要求，可以在启动时或应用期间执行该测试。有关实现该特定测试的详细信息，请参阅特定 TMS320F28004x MCU 器件随附的安全包。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.2.6 CPU 的软件测试

可以使用基于软件的自检库 (STL) 来测试各种 CPU 逻辑（C28x、FPU、TMU 等）的完整性。TI 将为 C28x、FPU 和 TMU 提供具有 60% 诊断覆盖率的 C28x-STL 启动测试库。有关实现该特定测试的详细信息，请参阅特定 TMS320F28004x MCU 器件随附的安全包。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.2.7 栈溢出检测

安全应用中的栈溢出可能会由于数据损坏和/或返回地址丢失而导致灾难性的软件崩溃。因此，检测即将发生的栈溢出非常重要。ERAD 模块中的增强型总线比较器 (EBC) 单元可以监测内部地址和数据总线，并在指定的总线和掩码与指定值匹配时触发 RTOSINT 中断。因此，检测栈溢出的基本方法是配置 EBC 单元，以在数据写入地址总线处于堆栈结束之前的某个范围内时触发中断。图 6-2 中展示了这一点。该存储器仅为堆栈使用而保留，因此指定地址范围内的数据写入表明堆栈使用量即将达到为其分配的大小限值。检测到即将发生的栈溢出会触发可屏蔽中断。程序编入的错误响应和任何必要的软件要求由系统集成商定义。

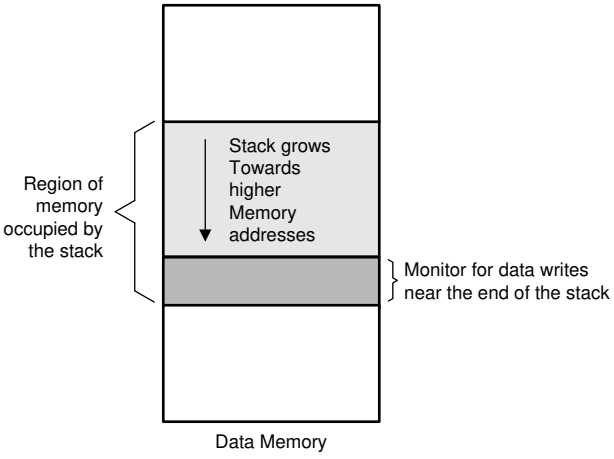


图 6-2. 栈溢出监测

6.2.8 静态存储器内容的 VCU CRC 检查

TMS320F28004x MCU 器件系列包括使用标准多项式来实现循环冗余校验 (CRC) 的协处理器。通过计算一个针对所有存储器内容的 CRC 并将得出的值与一个之前生成的“黄金”CRC 相比较，该 CRC 模块能够用于测试

SRAM、闪存和 OTP 内容的完整性。结果比较、故障指示和故障响应由管理该测试的软件负责。CRC 逻辑采用的循环校验提供了一个自检的固有电平（自动覆盖），可考虑将其应用在延迟故障诊断中。

6.2.9 VCU CRC 自动覆盖

VCU CRC 诊断基于最多 32 位多项式。对于给定测试，在 2^{32} 种可能性中只有一个代码有效。因此，如果 VCU CRC 逻辑或相关数据路径出现故障，则通过该故障生成正确的传递代码的可能性极低。

6.2.10 禁用未使用的 CLA 触发源

CLA 可以接收来自各种外设和软件的输入任务触发源。为避免未使用的触发源对 CLA 操作形成干扰，建议在应用中禁用这些触发源。

6.2.11 嵌入式实时分析和诊断 (ERAD) - 0 类

ERAD 模块提供系统分析功能，通过配置监测 CPU 总线的总线比较器单元和对事件进行计数的计数器单元，可用于检测 CPU 和 MCU 上其他逻辑中出现的故障。该模块由增强型总线比较器单元和基准系统事件计数器单元组成，可由应用软件访问。

增强型总线比较器单元用于监测各种 CPU 总线并生成可进一步处理或直接使用的事件。这些单元监测和检测到的活动可用于生成断点、观察点或中断 (RTOSINT)。

基准系统事件计数器单元用于分析和评测系统。当设置为事件模式时，它可以对事件进行计数，当设置为持续时间模式时，它可以计算系统事件之间的持续时间。

应用代码设置 ERAD 模块后，它可以独立工作并在发生事件匹配时生成 RTOSINT 中断。该模块可持续在线监测 MCU 上的系统事件。

6.3 存储器（闪存、SRAM 和 ROM）

6.3.1 闪存阵列中的位多路复用

TMS320F28004x MCU 器件系列中实现的闪存模块采用了一个位多路复用方案，这样的话，为生成一个逻辑 (CPU) 字而访问的位在物理上不相邻。该方案有助于降低会导致逻辑多位故障的物理多位故障发生的可能性。相反，它们表现为多个单一位故障。SECDED 闪存 ECC 可以校正一个逻辑字中的单一位故障并检测其中的双位故障，因此，该方案提高了闪存 ECC 诊断的有效性。位多路复用是闪存的一个特性，无法通过软件更改。

6.3.2 SRAM 存储器阵列中的位多路复用

TMS320F28004x MCU 器件系列中实现的 SRAM 模块实现了一个位多路复用方案，这样的话，被存取用来生成一个逻辑 (CPU) 字的位在物理上不相邻。该方案有助于降低会导致逻辑多位故障的物理多位故障发生的可能性。相反，它们表现为多个单一位故障。SECDED SRAM ECC 诊断可以校正一个逻辑字中的单一位故障并检测其中的双位故障。同样，SRAM 奇偶校验诊断可以检测单一位故障。该方案提高了 SRAM ECC 和奇偶校验诊断的有效性。位多路复用是 SRAM 的一个特性，无法通过软件更改。

6.3.3 清理数据以检测/校正存储器错误

总线主器件（CPU、CLA 或 DMA）可以配置为向存储器提供虚拟读取（假设特定的总线主器件可以访问存储器），并可以通过内置 ECC 或奇偶校验逻辑检查读取的数据。对于具有 ECC 保护的 SRAM，会校正并写回单一位错误。对于 SRAM 和闪存，一旦计数超过预设的阈值，如果是可校正错误，就会发出中断，而如果是不可校正错误，则会发出 NMI。

由于闪存的内容是静态的，与该诊断相比，静态存储器内容的 VCU CRC 检查可提供更高的诊断覆盖率。

6.3.4 闪存 ECC

片上闪存由单错校正双错检测 (SECDED) 错误校正码 (ECC) 诊断支持。在该 SECDED 机制中，使用一个 8 位代码字来存储 64 位数据的 ECC 和相应的地址。闪存组输出的 ECC 解码逻辑检查存储器内容的正确性。对读取的每个数据和程序都进行 ECC 评估。连接 CPU 和闪存的数据和程序互连不受 ECC 保护。根据是否启用校正功能，可以校正或不校正检测到的可校正错误。单一位地址 ECC 错误被标记为不可校正的错误。无法校正的错误将生成 NMI 并使 ERRORSTS 引脚置位。通过闪存包装程序监测已校正错误（单一位数据错误）的计数，一旦计数超过编程阈值，就会生成中断。最后一个错误位置的损坏存储器地址也记录在闪存包装程序中。

6.3.5 闪存程序验证和擦除验证检查

每当完成任何编程和擦除操作时，闪存控制器都会执行编程和擦除验证检查。如果编程和擦除操作失败，FSM 状态寄存器 (FMSTAT) 将通过在状态寄存器中设置相应的标志来指示错误。

6.3.6 ECC 逻辑的软件测试

在测试模式下注入单一位错误和双位错误，并对存在 ECC 错误的位置执行读取，以及检查是否存在错误响应，从而测试 SRAM ECC 的功能。可以借助 ECC 测试寄存器（FECC_CTRL、FADDR_TEST、FECC_TEST、FDATAH_TEST、FDATAL_TEST）来检查闪存 ECC 逻辑。也可以使用这项技术来验证与单一位错误相关的错误计数器和阈值中断能够正常运行。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

有关对 SRAM 和 FLASH 存储器实现该诊断的更多详细信息，请参阅 *TMS320F28004x 微控制器技术参考手册*中的*用于错误检测和校正的应用测试钩*和 *SECDED 逻辑正确性检查*这两节。

6.3.7 闪存预取、数据缓存和等待状态的软件测试

启用后，预取逻辑会继续从闪存组中获取下一个 128 位行（4 个 32 位字）。检测到不连续性时，将清除预取缓冲区。可以执行软件测试以确定该逻辑的行为是否正确。可以执行以下操作序列。

1. 禁用预取机制，启用计时器和看门狗。执行一项特定功能，该功能可能包含线性代码和涉及多个不连续性的代码。存储执行该功能所用的时间“time_1”（计时器值）。
2. 启用预取机制，再次执行相同的功能。存储执行该功能所用的时间“time_2”（计时器值）。该值应小于 time_1 (time_1 > time_2)。我们可以将该计时器值标记为一个黄金值，相同功能的每次运行都应具有相同的计时器值。
3. 每个闪存组行都有 4 个 32 位字，因此从闪存组中提取的行数根据该闪存组内的代码对齐方式而有所不同。因此，用户需要确保预取逻辑测试功能对齐/位于闪存内的特定位置，以保证相同的时序行为，并且不会因编译而异。

可以执行类似的基于计时器的性能评测，以确定数据缓存和等待状态正常运行。

6.3.8 存储器访问保护机制

除 M0/M1 外，包括外部存储器在内的所有易失性存储器块都具有不同的保护级别。该功能使用户能够启用或禁用从各个主器件（即 CPU、CLA、DMA）对各个 RAM 块的特定访问（例如获取、写入）。读取访问不受保护，因此，始终允许从有权访问该 RAM 块的所有主器件进行读取。若要确定主器件访问 SRAM 受阻的条件，请参阅器件特定技术参考手册。可以在运行时更改该配置，并允许存储器阻止来自特定主器件或同一主器件内特定应用线程的访问。该功能有助于支持某些应用所需的防止干扰特性。

6.3.9 SRAM ECC

选定的片上 SRAM 支持 SECDED ECC 诊断，并为数据和地址提供单独的 ECC 位。有关支持 ECC 的特定地址范围，请参阅 TMS320F28004x MCU 器件特定数据表。在 SECDED 方案中，使用一个 21 位代码字来存储为每个 16 位数据和地址独立计算的 ECC 数据。用于 SRAM 访问的 ECC 逻辑位于 SRAM 包装程序中。直接在存储器输出端评估 ECC，并在执行数据完整性检查后将数据发送至 CPU。从 SRAM 到 CPU 的数据和地址互连不受 ECC 保护。校正检测到的可校正错误，并且可以监测已校正错误的数量。SRAM 包装程序可配置为在已校正错误的数量超过阈值时触发中断。不可校正的 SRAM 错误会触发 NMI，并置位 ERRORSTS 引脚。SRAM 的 ECC 逻辑在复位时启用。更多有关支持 ECC 的存储器的信息，请参阅 TMS320F28004x MCU 器件特定数据表。

6.3.10 SRAM 奇偶校验

选定的片上 SRAM 支持奇偶校验诊断，并为数据和地址提供单独的奇偶校验位。有关支持奇偶校验的特定地址范围，请参阅器件特定数据表。在奇偶校验方案中，使用一个 3 位代码字来存储为每个 16 位数据和地址独立计算的奇偶校验数据。SRAM 的奇偶校验生成和校验逻辑位于 SRAM 包装程序中。直接在存储器输出端检查奇偶校验，并在执行数据完整性检查后将数据发送到 CPU。从 SRAM 到 CPU 的数据和地址互连不受奇偶校验保护。SRAM 奇偶校验错误会触发 NMI，并置位 ERRORSTS。SRAM 的奇偶校验逻辑在复位时启用。更多有关支持奇偶校验的存储器的信息，请参阅 TMS320F28004x MCU 器件特定数据表。

6.3.11 奇偶校验逻辑的软件测试

可以通过以下方式来测试奇偶校验错误检测逻辑的功能：强制奇偶校验错误进入数据或奇偶校验存储器位，并观察奇偶校验错误检测逻辑是否报告了错误。也可以手动计算奇偶校验，并与存储在奇偶校验存储器位中的硬件计算值进行比较。

有关在 SRAM 上实现该诊断的更多详细信息，请参阅 *TMS320F28004x 微控制器技术参考手册*中的*用于错误检测和校正的应用测试钩*一节。

6.3.12 SRAM 的软件测试

可以使用 CPU 测试 SRAM 的完整性（位单元、地址解码器和感测放大器逻辑）。根据安全要求，可以在启动时或应用期间执行该测试。如果 SRAM 内容是静态的，也可以使用 VCU 执行 CRC 校验来代替破坏性测试（测试后需要恢复存储器内容的测试）。有关实现该特定测试的详细信息，请参阅特定 C2000 MCU 器件随附的安全包。

6.3.13 CLA-PROM 的背景 CRC (CLAPROMCRC)

CLAPROMCRC 是一项安全特性，可对 CLA 程序 ROM 空间中的可配置存储器块执行 CRC。C28x 和 CLA 均无法在 CLA 程序 ROM 上以访问的方式计算 CRC。CLAPROMCRC 通过以非侵入方式（即不影响 CLA 对 CLA PROM 的访问）计算 CRC，解决了这个问题。它是一个硬件 CRC-32 模块，在空闲周期（当 CLA 未访问 CLA 程序总线上的 ROM 时）在后台自动获取 CLA 程序 ROM，并计算 CRC-32 以执行代码完整性检查。然后它将结果与黄金 CRC-32 值进行比较，并记录通过或失败的情况。该模块在测试完成时发出中断。

图 6-3 是 CLAPROMCRC 模块的功能图。

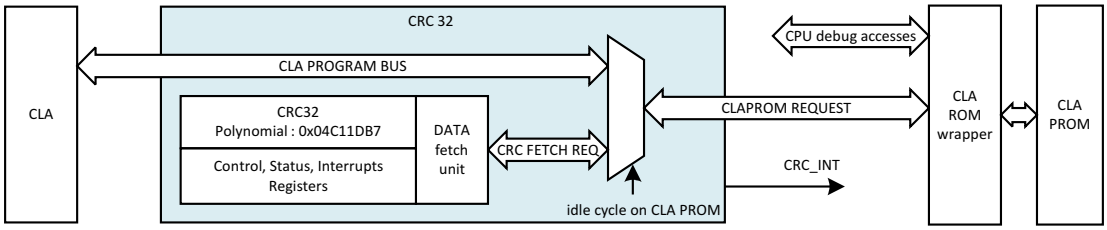


图 6-3. CLAPROMCRC 功能图

6.3.14 存储器开机自检 (MPOST)

存储器的启动测试可用于检测片上存储器内的永久性故障。某些 C2000 器件系列产品支持可编程内置自检 (PBIST)，这是通过配置客户 OTP 字段来测试存储器的一种简单有效的方法。PBIST 架构由一个小型协处理器和一个专门针对存储器测试的专用指令集组成。该协处理器在触发时执行存储在 PBIST ROM 中的测试例程，并在多个片上存储器实例上运行这些例程。片上存储器配置信息也存储在 PBIST ROM 中。针对已实现 SRAM 和 ROM 上的永久性故障，PBIST 提供了非常高的诊断覆盖率。如果配置了 PBIST，则在所有存储器实例上执行测试（对 SRAM 执行 March13n，对 ROM 执行 Triple_read_xor_read）。PBIST 测试状态存储在片上存储器中。PBIST 所涵盖的术语“存储器”指的是 SRAM 和 ROM。闪存测试并非本规范的一部分。

用于存储器测试的代码位于引导 ROM 中，所以无法用 PBIST 测试引导 ROM。因此，在 PBIST 之前，将进行单独的引导 ROM 校验和测试。在使用 PBIST 执行任何测试之前，会执行一个始终失败测试用例。这是为了验证 PBIST 控制器正常运行及其指示失效的能力。更多详细信息，请参阅 *C2000 存储器内置自检 (M-POST)*。

6.4 包括总线仲裁在内的片上通信

6.4.1 使用次级自由运行计数器进行 1oo2 软件表决

TIMER 模块包含三个用于提供操作系统时基的计数器。当一个计数器用作操作系统时基时，可以使用另外两个计数器中的任一个来诊断第一个计数器，即通过软件对两个计时器中的计数器值进行定期检查。可以将不同的时钟源用于 CPU Timer2，并选择不同的预分频配置以避免共模错误。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.4.2 DMA 溢出中断

DMA 支持锁存一个额外的触发事件。在 DMA 处理该锁存事件之前，如果发生其他事件，则会生成 DMA 溢出中断，从而设置 CONTROL_REG.PERINTFLG 并发生另一个中断事件。设置的 CONTROL_REG.PERINTFLG 表示先前的外设事件已被锁存且尚未由 DMA 进行处理

6.4.3 为未使用的中断维护中断处理程序

TMS320F28004x MCU 器件包含大量中断；一个典型应用只使用所有可用中断中的一小部分。对于未使用的中断，可以进行多种配置。这包括禁用未使用的中断、启用未使用的中断以及返回到中断服务例程 (ISR) 中的应用，等等。接收到应用中未使用的中断可能是 TMS320F28004x MCU 中某些故障场景的早期迹象。因此，强烈建议启用所有中断并将 ISR 配置为用于日志记录或错误处理的通用例程。

6.4.4 上电预运行安全检查

器件启动期间，它会经历如图 4-9 所示的各个阶段。在预运行阶段（启动应用之前），应用代码应执行一组检查以确保正确初始化器件安全性，包括检查以确认正确的链路指针设置、CRC 锁定设置、安全 RAM 块和闪存扇区（抓取位）的正确分区、安全 RAM 块和闪存扇区的仅执行保护设置、CLA 和闪存组 2 的正确分区，以及引导配置的正确设置。在开始执行下载的代码之前，用户应使用 CRC 功能检查代码的完整性。一旦预运行检查成功完成并获得预期结果，器件就可以进入应用阶段。

6.4.5 链路指针的多数表决和错误检测

链路指针 OTP 位置不受 ECC 保护。为了给客户代码提供更好的安全性并实现应用安全，实现了基于多数表决和数据一致性的错误检测。OTP 中区域选择部分的位置由各区域 OTP 中已编程的三个 29 位链路指针 (Zx-LINKPOINTERx) 的值决定。当通过比较所有三个值（按位表决逻辑）以向所有链路指针发出虚拟读取时，将在硬件中解析链路指针的最终值。最终链路指针值解析中的任何错误都会设置 Zx_LINKPOINTERERR 寄存器。

6.4.6 PIE 双 SRAM 硬件比较

PIE SRAM 地址空间被复制，数据被放置在两个存储器中。在向量获取期间，ePIE 对两个向量表输出进行硬件比较。如果两个向量表不匹配，CPU 会跳转到 PIEVERRADDR 寄存器中的地址，并且 ePIE 会向 PWM 发送跳变信号。如果 PIEVERRADDR 寄存器值尚未设置，则使用地址 0x003FFFBE 处的默认引导 ROM 处理程序。

6.4.7 PIE 双 SRAM 比较检查

为了检查 PIE 双 SRAM 比较特性和故障处理，可以通过等待冗余向量地址来向两个 SRAM 注入不同的数据。SRAM 中不匹配的 PIE 向量对应的中断需要通过软件触发。然后，软件需要验证 CPU 是否跳转到 PIEVERRADDR 寄存器中的地址，并且 ePIE 会向 PWM 发送跳变信号。有关执行该检查的详细信息，请参阅 *TMS320F28004x 微控制器技术参考手册* 中的*向量地址有效性检查*一节。

6.4.8 X-BAR 标志的软件检查

X-BAR 标志寄存器用于标记 ePWM 的输入和输出 X-Bar，以提供有关被触发的输入源的软件知识。可以定期读取该标志寄存器，以确定没有缺失 ePWM 跳匣区域、ePWM 同步或 GPIO 输出信号。

6.4.9 包括错误测试在内的 ePIE 运行软件测试

可以实施用于测试基本功能以及失效模式（如连续中断、无中断和交叉中断）的软件测试。这种测试可以基于从外设生成中断，并确保中断得到维护且按正确的顺序进行维护。可以使用软件强制功能（如 ECAP_REGS.ECFRC.CTROVF）生成中断，也可以在功能上创建中断场景，例如在 eCAP 中创建计数器溢出条件。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.4.10 禁用未使用的 DMA 触发源

DMA 传输的意外触发可能会使关键数据受损，这可能是安全关键型应用的一个潜在干扰源。为避免启动意外的 DMA 传输，建议在源端或通过配置 DMACHSRCSELx 寄存器禁用未使用的 DMA 通道和 DMA 触发源。

6.5 数字 I/O

6.5.1 eCAP 应用级安全机制

可以根据应用要求，检查 eCAP 模块输出是否饱和、宽度是否为零或超出范围。在测量旋转机械的速度时，应用可以根据工作型材设置测量速度的界限。类似的界限设置可用于其他应用场景，如周期和占空比测量、通过已编码电流或电压传感器的占空比解码电流或电压等。还可以根据应用规范对周期性中断进行在线监测，以提高诊断覆盖率。

6.5.2 ePWM 应用级安全机制

在电动汽车牵引、直流/直流和工业驱动器等闭环控制应用中，ePWM 通常用作输出信号。在此类应用中，ePWM 输出失效（例如固定故障，或频率/占空比变化）会对控制环路参数或变量造成干扰，从而导致过压、过流或过热等情况。通过监测在应用级实现的这些控制环路参数的特性，可以检测到 ePWM 模块中出现的故障。

6.5.3 使用 X-BAR 进行 ePWM 故障检测

ePWM 输出到输入 X-BAR 的反馈、GPIO 反转逻辑和 ePWM 数字比较 (DC) 子模块的组合可用于对 PWM 输出实现简单（例如信号交叉）但有效的异常检查。如果检测到任何异常，该特性可用于跳变 PWM 并进入安全状态。

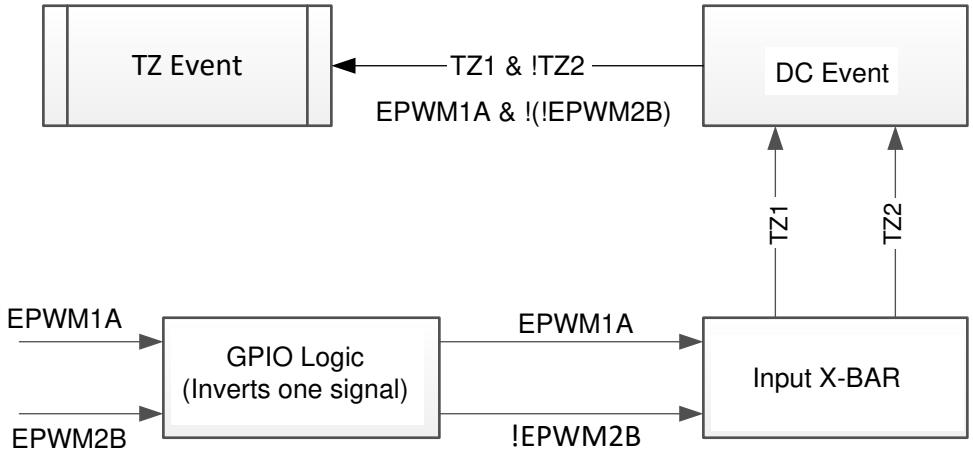


图 6-4. 使用 X-BAR 进行 ePWM 故障检测

6.5.4 ePWM 同步检查

ePWM 模块可通过时钟同步方案链接在一起，该方案使这些模块能够在需要时作为单个系统运行。在同步操作模式下，务必要确保各 PWM 实例正确同步从而避免灾难性情况。可通过读取 ePWM 模块的 TBSTS.SYNCI 位来检查各 PWM 的同步情况。可通过比较 TBCTR 寄存器值来交叉检查作为同步操作结果的相位关系是否正确。

6.5.5 eQEP 应用级安全机制

eQEP 通常用于闭环控制应用，与线性或旋转增量编码器直接连接，以便从高性能运动和位置控制系统所用的旋转机器中获得位置、方向和速度信息。在此类应用中，可以根据应用要求检测 eQEP 输出是否饱和、为零值或超出范围。在估算旋转机械的速度/位置时，应用可以根据工作型材设置测量速度/位置的界限。还可以根据应用规范对来自 eQEP 的周期性中断进行在线监测，以提高诊断覆盖率。

6.5.6 eQEP 正交看门狗

eQEP 外设包含了 16 位看门狗计时器，用于监测正交时钟，以指示运动控制系统执行正确的操作。eQEP 看门狗计时器从 SYSCLKOUT/64 计时，并且正交时钟事件（脉冲）会使看门狗计时器复位。如果在周期匹配之前未检测到正交时钟事件，看门狗计时器将超时，并且系统将设置看门狗中断标志。可通过看门狗周期寄存器对超时值进行编程。

6.5.7 正交看门狗功能的 eQEP 软件测试

软件测试可用于测试正交看门狗的基本功能，以及用于引入诊断错误并检查错误响应是否正确。这种测试可在启动时执行，或者定期执行。必要的软件需求由系统集成商执行的软件定义。

6.5.8 硬件冗余

硬件冗余技术可通过硬件或作为硬件和软件的组合来提供运行时诊断。在该实现中，利用冗余硬件资源为 TMS320F28004x MCU 内部和外部要素（线束、连接器、收发器）提供诊断覆盖。

对于 GPIO、X-BAR、ePWM、OTTO、DAC、CMPSS 和 XINT 等外设，可以通过多通道并行输出（采用独立输出传输信息，通过内部或外部比较器进行失效检测）或输入比较或表决（对独立输入进行比较，以确保在时间和

数值上符合规定的容差范围）来实现硬件冗余。在这些情况下，系统可以设计成一个输入/输出的失效不会导致系统进入危险状态。在为错误条件（如冗余条件）提供服务（如在两个冗余源中使 PWM 跳变）时，始终读回状态标志并确保两个源在跳变时均处于运行状态，从而为跳变逻辑提供潜在故障覆盖。

对于 ADC、PGA、eCAP、HRCAP 和 eQEP 等外设，可以让外设的多个实例对相同的输入进行采样并同时执行相同的操作，然后对输出值进行交叉检查，以此来实现硬件冗余。

对于 SDFM，可以让多个通道对相同的输入进行采样，然后对输出值进行交叉检查，以此来实现硬件冗余。

对于 DCAN、SPI 和 SCI 等通信外设，可以通过让外设的多个实例接收相同的数据然后进行比较来实现信号接收期间的硬件冗余，以确保数据完整性。可以通过从发射器到接收器的完整冗余信号路径（线束、连接器、收发器）或通过冗余外设实例对传输的数据进行采样，然后进行数据完整性检查，以此来实现传输期间的硬件冗余。

可以通过由独立处理单元进行冗余数据存储/传输，然后对计算结果进行比较，以此来实现器件互连 (INC) 的硬件冗余。

可以通过将中断并行连接到 CLA 作为触发源来实现外设中断 (PIE) 的硬件冗余。可以在 CPU 和 CLA 之间实现互惠式比较，以检测错误的 PIE 行为。

对于双代码安全模块 (DCSM)，C28x CPU 和 CLA 可以配置为通过独立区域访问其资源。可以在 CPU 和 CLA 之间实现互惠式比较，以检测 DCSM 模块中的故障。

在为 ADC 和 DAC 模块实现硬件冗余时，还需要注意确保共因失效不会以相同的方式影响两个实例。为冗余模块实例配置的基准电压源应是独立电压源。此外，用于冗余 ADC 实例的 ADC SOC 触发源应配置为不同的 ePWM 模块实例。对于 DAC，可以使用外部器件来实现比较器。

在为 ePWM 模块实现硬件冗余时，建议将所用的 ePWM 模块实例作为单独同步链的一部分。这是为了避免同步信号的共因失效以相同的方式影响两个 ePWM 模块。

在为 GPIO 模块实现硬件冗余时，建议使用来自不同 GPIO 组的 GPIO 引脚，以避免共因失效。

6.5.9 HRPWM 内置自检和诊断功能

HRPWM 中的微边沿定位器 (MEP) 逻辑能够在 255 个离散时间阶跃之一中放置边沿。这些阶跃的精度约为 150ps。有关典型的 MEP 步长，请参阅器件特定数据表。MEP 步长根据最坏情况下的工艺参数、工作温度和电压而变化。MEP 步长随着电压降低和温度升高而增大，随着电压升高和温度降低而减小。使用 HRPWM 特性的应用应使用 TI 提供的 MEP 比例因子优化 (SFO) 软件功能。SFO 功能有助于在 HRPWM 运行时动态地确定每个 EPWMCLK 周期的 MEP 步数。

HRPWM 模块具有内置自检和诊断功能，可用于确定任何操作条件下的理想 MEP 比例因子值。TI 提供了一个可调用 C 语言程序的库，库中包含一个 SFO 函数，该函数利用此硬件并确定理想 MEP 比例因子。对于给定温度下的给定系统时钟频率，SFO 确定函数返回一个已知的 MEP 比例因子值。通过将返回的 MEP 比例因子值与预期值进行比较来验证系统时钟频率操作是否正确。

6.5.10 信息冗余技术

信息冗余技术可通过软件提供附加的运行时诊断。为了提供对于 TMS320F28004x MCU 之外的网络要素的诊断覆盖（线束、连接器、收发器），必须采用端到端安全状态恢复机制。这些机制也可提供 TMS320F28004x MCU 内部的诊断覆盖。

对于处理要素（CPU 和 CLA），这是指多次执行代码和基于软件的交叉检查，以确保正确性。多次执行和结果比较可以基于多次执行的相同代码或实现的不同软件代码。有关实现的详细信息，请参阅 ISO 26262-5:2018 的 D.2.3.4。

对于 DMA，信息冗余技术是指除数据有效载荷之外的可确保数据完整性的附加信息。例如，SECDED 码、奇偶校验码、CRC 等都可以实现信息冗余。

典型的控制应用包括测量三相电压和电流。这些值要么使用片上 ADC 直接采样，要么使用 eCAP、SDFM 等进行捕捉并由传感器发送至 TMS320F28004x MCU。在这些情况下，输入信号之间的相关性可用于检查完整性（例如，如果测量三相电压 V_1、V_2 和 V_3，则函数 $V_1 + V_2 + V_3 = 0$ 可用于提供诊断覆盖以确保输入信号完整性）。

对于 SRAM 和闪存，关键数据、程序、变量等可以冗余存储，并在使用之前进行比较。切勿用编译器来优化包含冗余数据/程序的代码。闪存中的安全程序可以复制到 SRAM，并在针对预先计算的黄金 CRC 值执行 CRC 检查后执行。

6.5.11 eCAP 对 ePWM 的监测

可以通过输入捕捉外设（如 eCAP）来监测 ePWM 输出是否正常运行。ePWM 输出和 eCAP 输入之间的连接可在电路板外部进行，也可在内部使用 X-BAR 进行。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。同样，作为诊断用测试，可通过测量 ePWM 脉冲宽度来测试 eCAP。XINTxCTR（XINT 模块的计数器）、eQEP 的捕捉模式和 DCCAP（PWM 事件过滤器单元）也可用于检测 PWM 的上升沿/下降沿并提取时间戳信息。该信息可进一步用于构建附加诊断。

6.5.12 ADC 对 ePWM 的监测

ADC 可以根据板级反馈来监测 ePWM 输出是否正常运行，如图 6-5 所示。链接 [9] 中提供了实现此类环回（如信号分辨率等）的技术详细信息。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

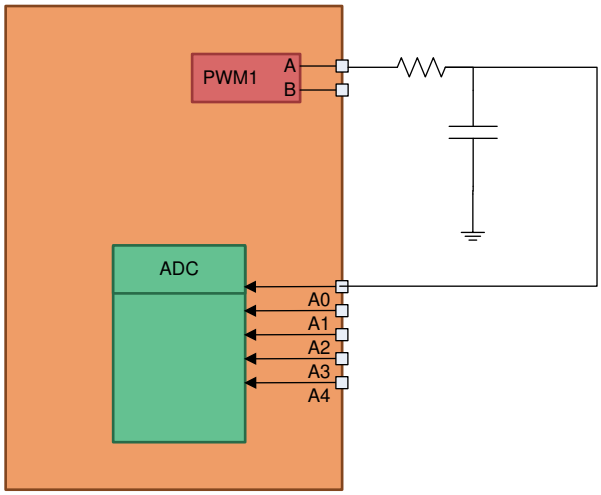


图 6-5. ADC 对 ePWM 的监测

6.5.13 在线监测周期性中断和事件

对于中断和事件，可以使用有关系统时间行为的信息来检测故障。所监测的信号可以是周期性的，也可以是非周期性的。

对于典型的闭环控制应用，大多数关键事件本质上是周期性的，可以监测这些周期性事件，并且事件中的不一致性可用于故障检测。可以使用 ERAD 等外设在线监测周期性中断和事件的几种情况包括：

- 在线监测周期性中断的发生，例如 ePWM、ADC 转换结束 (EOC)、eCAP 和 eQEP 中断
- 在线监测周期性事件：
  - ADC 转换启动 (SOC) 的周期性生成：ADC SOC 信号可用于借助 X-BAR 生成外部中断 (XINT)。可以监测周期性中断的发生。
  - 周期性 DMA 触发：某些 DMA 事件在本质上也可能是周期性的（例如，复制 ADC 结果、更新 CMPA 寄存器，等等）。DMA 支持在 DMA 操作完成时生成中断，该功能可用于在线监测。

监测在正常运行期间通常不会发生的中断和事件也有助于提高诊断覆盖率（例如 ECC 可校正错误中断）。

6.5.14 用于在线监测的 SDFM 比较器滤波器 - 0 类

SDFM 的比较器单元可用于在线监测初级滤波器的运行。比较器滤波器具有一个可配置的 Sinc 滤波器，其输出与三个编程阈值电平进行比较，以检测超过阈值和低于阈值的情况以及过零事件。如果比较器滤波器的数据输出超过阈值上限或低于阈值下限，它将向 CPU 发出中断。比较器滤波器的输出还可用于验证初级滤波器输出是否具有适当的缩放比例。

6.5.15 SD 调制器时钟故障检测机制

当 SD 调制器时钟在 256 个连续系统时钟周期内出现故障或丢失时，SD 调制器输入控制单元中的时钟故障检测子模块会检测到该故障并向 CPU 生成中断。该机制可用于检测丢失的调制器时钟故障或与调制器时钟相连的数字 I/O 中的任何故障。

6.5.16 包括错误测试在内的功能软件测试

软件测试可用于测试模块的基本功能，引入诊断错误并检查错误响应是否正确。这种测试可在启动时执行，或者定期执行。必要的软件需求由系统集成商执行的软件定义。

下面给出了创建一些特定于模块的测试功能和错误测试的思路：

- 可以通过向 TMS320F28004x MCU 发送一个已知的输入测试序列来检查 SDFM 功能，再使用数字抽取滤波器对其进行处理，并对照已知值对该值进行交叉检查。为了检测比较器中断生成逻辑中的故障，可以创建一个测试模式，用于将高、低阈值寄存器值分别配置为最小值和最大值。应始终使用这样的配置来生成中断。
- 可以通过将已知良好的数据从源存储器传输到目标存储器并在传输后检查数据完整性来检查 DMA 功能。使用提供的软件触发器 (CONTROL.PERINTFRC) 可以启动传输。片上计时器可用于评测此类数据传输所需的时间。
- 使用输入和输出 X-BAR 创建一个循环（输出 X-BAR 可用作输入 X-BAR 的激励信号），在输入端发送一个已知测试序列，并在最终输出端观察，从而执行输入和输出 X-BAR 模块的软件测试。可通过发送测试激励信号并使用 ePWM 跳变或同步功能来观察响应，从而检查 ePWM X-BAR 的完整性。
- 可通过配置输入 X-BAR 并强制相应的 GPIO 寄存器生成中断来检查针对 XINT 功能的软件测试。通过执行极性检查 (XINTxCR.POLARITY) 和使能 (XINTxCR.ENABLE) 功能，可以提高诊断覆盖率。
- 可通过将 PWM、HRPWM 或 GPIO 输出环回到各自的模块输入，提供模块所需的已知良好序列并观察模块输出来检查 eCAP、HRCAP 和 eQEP 功能。对于 eCAP 和 HRCAP，可以借助输入 X-BAR 在内部进行测试。
- 可以使用节 6.3.7 中给出的类似技术检查 ROM 预取功能。
- ePWM 模块由时基 (TB)、计数器比较 (CC)、动作限定器 (AQ)、死区发生器 (DB)、PWM 斩波器 (PC)、跳变区 (TZ)、事件触发器 (ET) 和数字比较 (DC) 子模块组成。使用 ePWM 提供合适的激励信号并使用其中一个捕捉（时间戳）模块（eCAP、XINT、eQEP 等）观察响应，从而测试各个子模块。建议在执行软件测试时覆盖与应用配置相关的各种寄存器值。由于各种子模块的正则线性特性，使用软件测试可以获得高覆盖率。
- SRAM 包装程序逻辑电路的软件测试应提供诊断覆盖，以便在访问特定 SRAM 的各种主器件之间进行仲裁，并确保访问保护正常运行。这对用于提供 SRAM 位单元覆盖的测试进行了补充（请参阅节 6.3.12）。

- 可通过从 CPU 和 CLA 的处理单元写入互补数据模式（如 0xA5A5、0x5A5A 等），并从通过不同网桥连接的 IP 寄存器读回来测试互连 (INC) 功能。可将读回数据与预期黄金值进行比较，以确保无故障互连操作。可以使用 CPU 和 CLA 对不同数据宽度类型的访问（16 位和 32 位）和宽地址范围（如适用）重复该练习。对于连接到各种网桥的应用中使用的不同外设实例，可以重复 CPU 访问，如图 4-1 所示。
- 为了测试 ADC 模块和后处理块 (PPB) 的核心功能，可通过外部电路或内部 DAC 在 ADC 输入引脚上提供一组预定的电压电平。由此获得的 ADC/PPB 结果可以对照预期值进行交叉检查，以确保正常运行。可以运用和测试应用中使用的 ADC 极端拐角值来检查工作范围内的转换是否成功。可通过写入互补数据模式、读回并与预期值进行比较来检查 ADC 配置寄存器。
- DAC 包含一组控制寄存器，可通过在 16 位访问模式下写入互补数据模式（如 0xA5A5、0x5A5A 等）来进行检查。可以读回所有寄存器并与预期值进行比较。可通过将寄存器配置为 0xA5A5 模式、置位 DAC 的软复位、读回寄存器并将读回值与预期复位值进行比较来检查寄存器的复位特性。可以检查锁定寄存器，以确保其只需设置一次。此外，被锁定的寄存器在写入时不得更新。若要测试 DAC 模块的核心功能，可以使用软件对其进行配置，以提供一组预定的电压电平。这些电压电平可由外部或内部 ADC 测量，由此获得的结果可以对照预期值进行交叉检查，以确保正常运行。根据应用对 DAC 的极端拐角值进行编程和测试，以检查在有效范围内数字到模拟模块的转换是否成功。
- 比较器子系统 (CMPSS) 包含一组寄存器，可通过在 16 位和 32 位访问模式下写入互补数据模式（如 0xA5A5、0x5A5A 等）来检查这些寄存器。可以读回这些寄存器并与预期值进行比较。可由适用的主器件（即 DMA、CLA 和 CPU）覆盖这些访问。在通过上升的 PWMSYNC 信号从 RAMPDLYS 加载 RAMPDLYA 后，可以检查 CMPSS 模块的特性（如斜坡递减），以进行 RAMPDLYA 的倒计时。应确保减量器减少到零并保持不变，直到下一次从 RAMPDLYS 重新加载。可在倒计时之前配置 RAMPDLYS 的极值。可通过将数字滤波器 CTRIPHFILCTL/CTRIPLFILCTL 寄存器配置为各种 SAMPWIN（采样窗口）和 THRESH（多数表决阈值）值，然后根据滤波器输出的变化验证 COMPHSTS/COMPLSTS 的变化，从而检查数字滤波器 CTRIPHFILCTL/CTRIPLFILCTL 寄存器。可以使用滤波器时钟预分频器值 (CTRIPLFILCLKCTL) 的适用范围来确保滤波器正确采样。
- 可通过软件测试来测试 CPU 计时器的一般操作，方法是从周期寄存器 PRDH 加载 32 位计数器寄存器 TIMH，在每个时钟周期开始递减计数器。当计数器达到零时，计时器中断输出会生成一个中断脉冲。在测试计时器功能时，通过选择时钟源 SYSCLK、INTOSC1、INTOSC2 或 XTAL 来改变计时器预分频计数器 (TPR) 值，并改变输入时钟。在计时器计数结束时测试中断生成功能。检查 TCR 寄存器中的时间溢出标志和计时器重新加载 (TRB) 功能是否正常运行。
- 可以在 zone1、zone2 和非安全区域中独立实现 DCSM 中的软件测试功能，以检查 DCSM 功能。在器件启动阶段，器件安全配置从 OTP 加载到 DCSM。测试功能可用于对属于同一区域和不同区域的 RAM 和闪存扇区进行访问过滤检查（读写和执行权限）。另外，还可以对 RAM 和闪存扇区进行 EXEONLY 配置检查，以确保阻止除执行访问之外的所有访问。

6.5.17 HRCAP 对 HRPWM 的监测

可以通过输入捕捉外设（如 HRCAP）来监测 HRPWM 输出是否正常运行。HRPWM 输出和 HRCAP 输入之间的连接可在电路板外部进行，也可在内部使用 X-BAR 进行。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。同样，作为诊断用测试，可通过测量 HRPWM 脉冲宽度来测试 HRCAP。XINTxCTR（XINT 模块的计数器）、eQEP 的捕捉模式和 DCCAP（PWM 事件过滤器单元）也可用于检测 PWM 的上升沿/下降沿并提取时间戳信息。该信息可进一步用于构建附加诊断。

6.5.18 HRCAP 校准逻辑测试特性

该校准逻辑由两个自由运行的计数器组成；一个由 HRCLK(HRCLKCTR) 计时，另一个由 SYSCLK(HRSYSCLKCTR) 计时。当 HRSYSCLKCTR 等于 HRCALIBPERIOD 时，校准块将捕捉并复位两个计数器值，然后触发一个中断，表明已准备好计算新的比例因子。将 HRSYSCLKCAP 除以 HRCLKCAP 可得到该比例因子，请参阅方程式 1。该比例因子的计算应在校准中断服务例程内完成。计算比例因子后，可以应用方程式 2 以从原始计数中获取已捕获值的实际测量值。

图 6-6 中描述了校准块的完整详细信息。

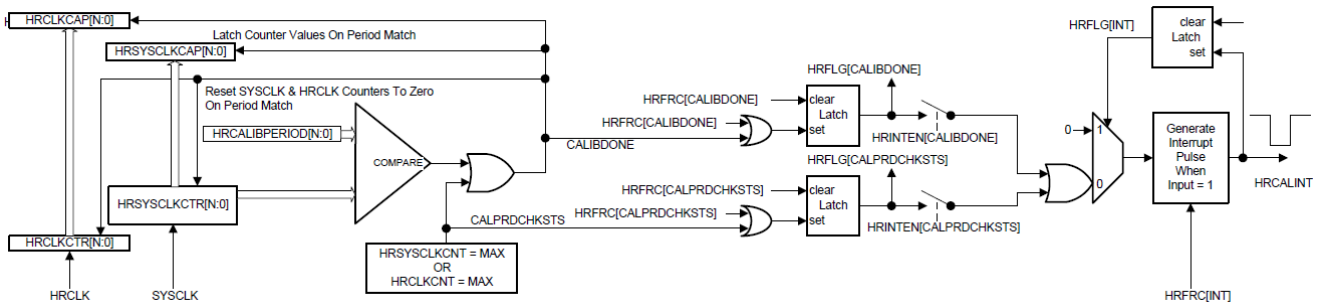


图 6-6. HRCAP 校准

$$ScaleFactor = \frac{HRSYSCLKCAP}{HRCLKCAP} \quad (1)$$

$$Measurement(ns) = \frac{RawCount \times scaleFactor}{128} * SysClk\,Prd(ns) \quad (2)$$

备注

即使经过校准，1.2V VDD 电源上的噪声也会对 HRCAP 子模块的标准偏差产生负面影响。应注意确保 1.2V 电源是清洁的，并且在使用 HRCAP 时已最大限度地减少了干扰性内部事件（例如启用和禁用时钟树）。

6.5.19 QMA 错误检测逻辑

QEP 模式适配器 (QMA) 旨在扩展 C2000 eQEP 模块功能，以支持 *TMS320F28004x 微控制器技术参考手册* 中的 *QMA 模块* 部分所述的其他模式。QMA 模块具有错误检测逻辑，可检测 EQEPA 和 EQEPB 输入信号上发生的非法转换。QMA 模块的错误和中断集成在 eQEP 模块中。

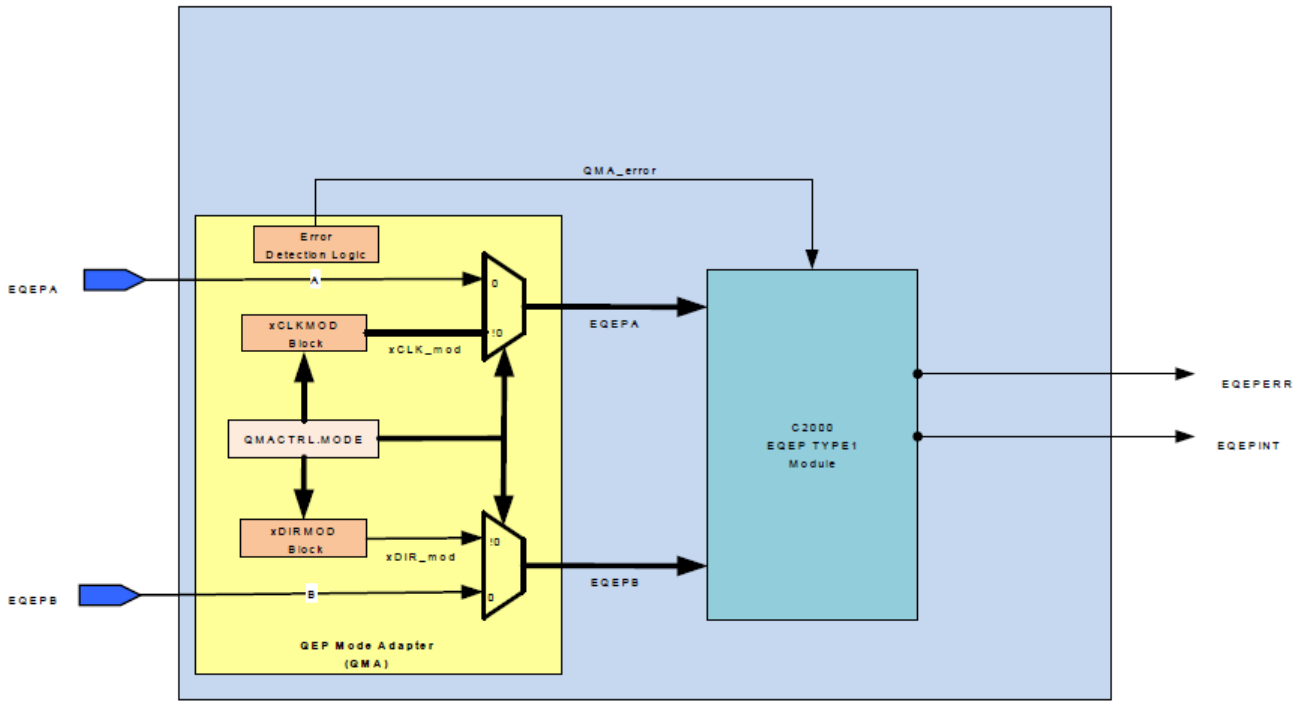


图 6-7. QMA 模块方框图

6.6 模拟 I/O

6.6.1 ADC 信息冗余技术

可以通过软件应用信息冗余技术，以提供有关 ADC 转换的运行时诊断覆盖。可以应用时间冗余技术，在同一 ADC 上进行多次转换，然后在软件中比较结果。此外，输入信号之间的相关性可用于检查完整性（例如，如果使用 ADC 测量三相电压 V_1、V_2 和 V_3，则函数 $V_1 + V_2 + V_3 = 0$ 可用于提供诊断覆盖以确保输入信号完整性和 ADC 转换）。

错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.6.2 ADC 输入信号完整性检查

可以对 ADC 转换混合使用硬件和软件运行时诊断来检查 ADC 输入信号的完整性。可以使用器件内可用的一些内置硬件机制对转换后的值进行过滤或合理性检查（例如，检查这些值是否在预期范围内）。通过设置适当的上限和下限阈值，可以借助比较器对输入信号进行合理性检查。可以使用 ADC 后处理块对转换结果进行合理性检查。

6.6.3 通过改变采集窗口来检查 ADC 信号质量

外部信号源在快速有效地驱动模拟信号方面的能力各不相同。为了达到额定分辨率，信号源需要将 ADC 内核中的采样电容器充电至信号电压的 0.5LSB 以内。采集窗口是允许采样电容器进行充电的时间量，可通过 ADCSOCxCTL.ACQPS 寄存器针对 SOCx 进行配置。该可配置参数还可用于为输入信号路径和 ADC 采样电容器逻辑提供诊断覆盖。可通过 ADC 使用预设的 ACQPS 配置和高于预设配置的 ACQPS 配置，对相同的输入信号进行冗余转换来完成该测试。由此获得的结果必须在由应用和 ADC 规格参数确定的预定义范围内。

6.6.4 CMPSS 斜坡发生器功能检查

CMPSS 斜坡生成功能用于某些控制应用（例如峰值电流模式控制）。通过读回 DACHVALA 寄存器的内容并确保根据 RAMPDLY、RAMPDECVAL 和 RAMPMAXREF 定期更新寄存器值，可以检查斜坡发生器的功能。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

6.6.5 DAC 至 ADC 环回检查

可以使用 ADC 来监测 DAC 输出以检查 DAC 和 ADC 的完整性。可以使用软件来配置 DAC，以提供一组预定的电压电平。这些电压电平可由 ADC 测量，可以对照预期值对由此获得的结果进行交叉检查，以确保 DAC 和 ADC 正常运行。也可以在运行期间应用这项技术，以确保从 DAC 驱动适当的电压电平。

更多有关无需外部板级连接即可由 ADC 采样的 DAC 通道的信息，请参阅器件特定数据表或技术参考手册。在对 12 位差分输入模式执行环回检查时，应使用两个 DAC 为 ADC 提供输入。为避免共因失效，建议在执行测试时保持 ADC 和 DAC 的基准电压不同。此外，在执行测试时，ADC 的输入信号不应由任何其他源驱动。

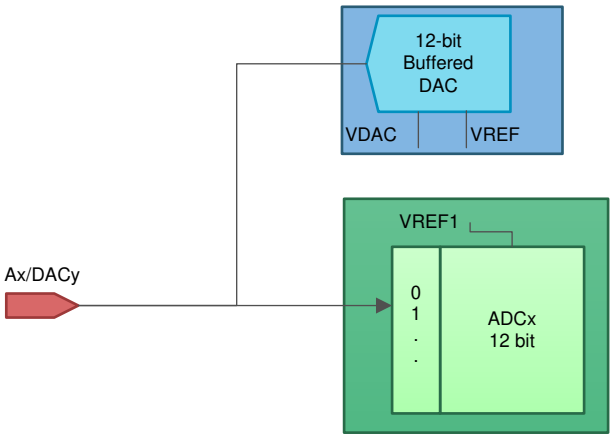


图 6-8. DAC 至 ADC 环回

6.6.6 DAC 至比较器环回检查

DAC 输出可以环回到比较器输入，以检查被驱动的输出是否处于适当的电压电平。需要在电路板上提供外部连接才能进行这项检查。通过对比较器设置更严格的限制条件，可以获得更高的诊断覆盖率。这项技术还可用于检测导致 DAC 输出被设置为超出应用安全工作范围值的控制流错误。

6.6.7 PGA 至 ADC 环回测试

可以通过一组已知值驱动 PGAx_IN 输入来检查 PGA 的完整性，并在使用片上 ADC 转换后监测输出。可以使用软件来配置 DAC，以提供一组预定的电压电平。借助外部连接，DAC 的输出可以连接到 PGAx_IN。ADC 可以对 PGAx_OUT 进行转换，SW 可以对 ADC 输出进行比较，以测试 PGA 是否将输入信号放大到适当的比例。

图 6-9 表示使用 DAC 和 ADC 来设置 PGA 测试的两种可能方案。

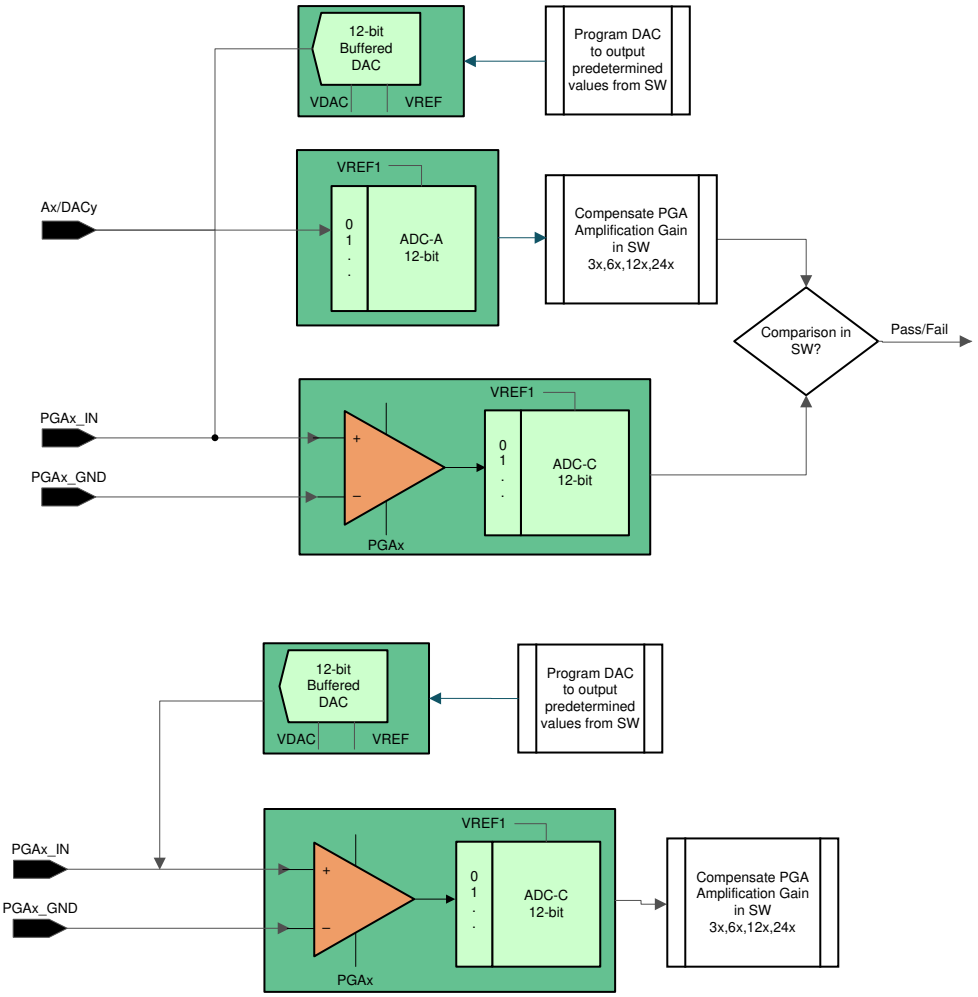


图 6-9. 使用 ADC 和 DAC 来测试 PGA

6.6.8 ADC 的开路/短路检测电路

开路/短路检测电路 (OSDETECT) 可用于检测系统中的 ADC 输入通道故障。该电路在通道选择多路复用器之后、S+H 电路之前连接到 ADC 输入端，如图 6-10 所示。错误响应、诊断的可测试性以及任何必要的软件要求由系统集成商所实现的软件来定义。

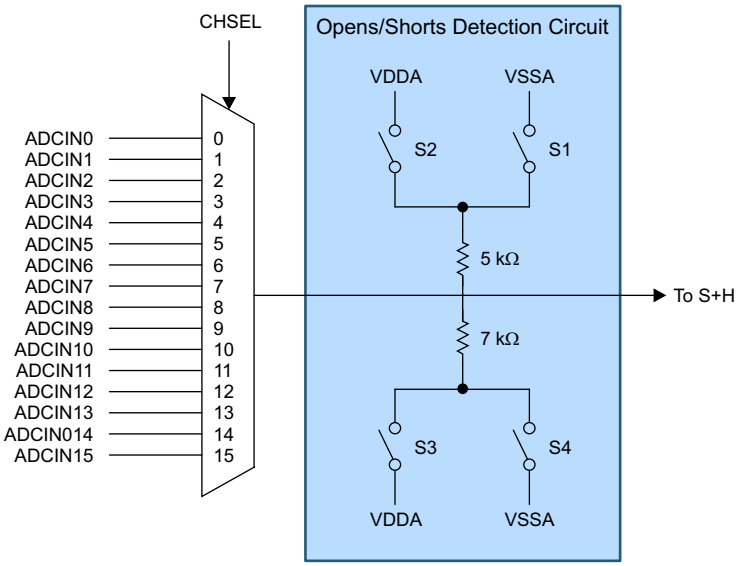


图 6-10. ADC 开路/短路检测电路

可通过向 ADCOSDETECT 寄存器中的 DETECTCFG 字段写入一个值来操作该电路。这将导致电路在任意转换的 S+H 阶段向输入端提供电压。表 6-1 中给出了采用不同 DETECTCFG 设置的 OSDETECT 电路的电压和驱动强度。有关实现该诊断的更多详细信息，请参阅 *TMS320F28004x 微控制器技术参考手册*中的*开路/短路检测电路 (OSDETECT)* 一节。

表 6-1. ADC 开路/短路检测电路真值表

ADCOSDETECT.DETECTCFG	源极电压	S4	S3	S2	S1	驱动阻抗
0	关闭	开路	开路	开路	开路	开路
1	零标度	闭合	开路	开路	闭合	5K || 7K
2	满标度	开路	闭合	闭合	开路	5K || 7K
3	5/12 VDDA	开路	闭合	开路	闭合	5K || 7K
4	7/12 VDDA	闭合	开路	闭合	开路	5K || 7K
5	零标度	开路	开路	开路	闭合	5K
6	满标度	开路	开路	闭合	开路	5K
7	零标度	闭合	开路	开路	开路	7K

6.6.9 通过 ADC 进行 VDAC 转换

COMPDAC (VDAC) 的基准电压输入与 ADCB 输入实现双键合。为了检测 VDAC 电源和相应模拟 I/O 中的故障，可以通过 ADC 进行转换。可以对照预期输出对 ADC 结果输出进行交叉检查，以识别任何故障。程序编入的错误响应和任何必要的软件要求由系统集成商定义。

6.6.10 禁用 ADC 未使用的 SOC 输入源

ADC 模块的 ADC SOC（转换启动）信号输入可由多个源触发，包括软件、CPU 计时器、GPIO 和 ePWM 模块实例等。为避免因源自未用于实现安全功能和级联到 ADC 的外设的故障而产生干扰，建议应用仅启用所需的 SOC 触发器。这是一种避免源自外部源的故障影响 ADC 功能的方法。

6.7 数据传输

6.7.1 包括端到端安全状态恢复的信息冗余技术

信息冗余技术可通过软件提供附加的运行时诊断。可应用很多技术，例如已写入值的读回和与结果相比较的同一目标数据的多次读取。

为了提供对于 TMS320F28004x MCU 之外的网络要素的诊断覆盖（线束、连接器、收发器），必须采用端到端安全状态恢复机制。这些机制也可提供 TMS320F28004x MCU 内部的诊断覆盖。可采用多种不同的机制，例如附加消息校验和、冗余传输、传输中的时间多样性等等。大多数通用校验和被添加到一个传输的有效载荷部分以确保传输的正确性。除了任何协议级奇偶校验与校验和之外，还会应用这些校验和、序列计数器和超时预期（或时间戳）。由于这些都是由通信任一端的软件生成和评估的，整个通信路径是安全的，实现了端到端安全状态恢复。

实施的任何端到端通信诊断都应考虑 IEC 61784-3:2016 中描述并在 IEC 61784-3:2016 表 1 中总结的失效模式和潜在的缓解安全措施。

6.7.2 位错误检测

当 CAN 模块将信息传输到其总线上时，它还可以监测总线，以确保传输的信息如预期的那样显示在总线上。如果没有从总线读回预期值，硬件会标记错误并向 CPU 发出中断信号。必须在软件中启用和配置该特性。

LIN 模块支持检测位错误情况。当 TED（TXRX Error Detector 子模块）中的位监测器检测到位错误时，会设置错误标志位。位错误表示 LIN 总线上发生了冲突，例如，监测到的位值与发送的位值不同。当检测到位错误时，应在不迟于下一个字节的情况下中止传输

6.7.3 消息中的 CRC

CAN 模块在消息中附加一个 CRC 字。CRC 值由发送器计算并发送，然后由接收器重新计算。如果接收器计算出的 CRC 值与发送的 CRC 值不匹配，则会标记 CRC 错误。错误响应和任何必要的软件要求由系统集成商定义。

6.7.4 DCAN 确认错误检测

当 CAN 网络上的节点接收到发送的消息时，它会发送一个确认，表明已成功接收该消息。当接收节点未确认发送的消息时，发送 DCAN 将会标记一个确认错误。错误响应和任何必要的软件要求由系统集成商定义。

6.7.5 DCAN 格式错误检测

根据 CAN 协议，DCAN 中某些类型的帧具有固定格式。当接收器在其中一个违反协议的帧中接收到一个位时，该模块将标记一个格式错误。错误响应和任何必要的软件要求由系统集成商定义。

6.7.6 DCAN 填充错误检测

在 CAN 消息协议中，通过位填充对多个帧段进行编码。每当发送器在待发送的位流中检测到 5 个具有相同值的连续位时，它就会自动将一个互补位插入到实际发送的位流中。如果在应通过位填充进行编码的接收段中检测到第 6 个连续相等位，则 DCAN 模块将标记填充错误。错误响应和任何必要的软件要求由系统集成商定义。

6.7.7 使用片上计时器进行 I2C 访问延迟性能评测

每个 I2C 消息都需要固定数量的系统时钟周期来完成事务。主器件可以根据从器件发送的消息确认信号来检测事务是否完成。片上计时器模块可用于对完成每个事务所需的时间进行评测。

6.7.8 I2C 数据确认检查

当 I2C 网络上的节点接收到一个字节（地址或数据）时，它会发送一个确认，表明已确认地址或成功接收数据字节。当接收 I2C 未确认发送的消息时，发送 I2C 将会标记 NACK。必要的软件要求由系统集成商定义。例如，一个需要传输 4 字节数据并可将 CRC 作为第 5 个字节发送的函数。器件软件可以这样设计：如果数据和 CRC 不匹配，则不提供确认。

PMBus 支持使用确认握手机制来检测错误，可以将其配置为在自动或手动模式下工作（PMBSC.MAN_SLAVE_ACK 位）。这种确认握手机制可由固件有效地实现，以检测通信故障，例如，如果接收到的地址不等于从器件地址，则通过置位 NACK 来伪装故障，或确认 PMBus 从器件接收字节确认信号所接收的每个字节，或确认接收到的命令字节，等等。如需了解更多详细信息，请参阅 *UCD3138 监控与通信程序员手册*。

6.7.9 消息中的奇偶校验

该模块支持在由硬件发出的每个消息的数据有效载荷中插入一个奇偶校验位。硬件也支持对传入消息进行奇偶校验评估。检测到的错误生成一个到 CPU 的中断。

6.7.10 SCI 中断错误检测

当 SCIRXD 在缺失停止位后的 10 位周期内处于低电平时，会出现 SCI 中断检测情况。该操作设置 BRKDT 标志位（SCIRXST，位 5）并启动中断。

仅当 LIN 在 SCI 模式下工作时，该特性才适用。当 LINRX 在缺失停止位后的 10 位周期内处于低电平时，会出现 SCI 中断检测情况。该操作设置 BRKDT 标志位并启动中断。

6.7.11 帧错误检测

接收串行数据时，SCI 上的每字节信息都有一种预期格式。如果接收到的消息与之不匹配，SCI 硬件会标记错误并向 CPU 生成中断。必须在软件中启用和配置该特性。

LIN 模块支持检测成帧错误情况。当未找到预期的停止位时，将设置错误标志位。在 SCI 兼容模式下，只检查第一个停止位。缺失的停止位表示与起始位的同步已丢失，并且字符成帧不正确。如果设置了 RXERR INT ENA 位，则检测到一个成帧错误时会生成一个错误中断。LIN 模块支持可验证有效同步字段的特性。它通过比较波特率并在波特率不同时进行调整来帮助自动调整波特率。如果在给定的容差范围内未检测到同步字段，则将设置不一致同步字段错误 (ISFE) 标志并生成一个 ISFE 中断。

6.7.12 超限错误检测

如果 SCI RX 缓冲区在读取以前的数据之前接收到新的数据，则现有的数据将被覆盖并丢失。如果出现这种情况，SCI 硬件可以标记该错误并向 CPU 生成中断。必须在软件中启用和配置该特性。

LIN 模块支持检测数据超限情况。当从接收移位寄存器到接收器数据缓冲区寄存器的数据传输将已接收数据寄存器中已经存在的未读数据覆盖时，系统会设置一个错误标志位。如果 SET OE INT 位 = 1，则检测到超限错误也会导致 LIN 生成错误中断。

6.7.13 使用 I/O 环回的功能软件测试

大多数通信模块支持 I/O 的数字或模拟环回功能。若要确认模块实现的环回功能，请参阅器件特定技术参考手册。数字环回测试到模块边界的信号路径。模拟环回在启用输出驱动器的情况下测试从模块到 I/O 单元的信号路径。为获得最佳效果，任何功能测试都应采用 I/O 环回设计。

6.7.14 SPI 数据超限检测

如果 SPI RX 缓冲区在读取以前的数据之前接收到新的数据，则现有的数据将被覆盖并丢失。如果出现这种情况，SPI 硬件可以标记该错误并向 CPU 生成中断。必须在软件中启用和配置该特性。

6.7.15 传输冗余

使用同一个模块实例按顺序多次传输信息，并进行比较。当同一个数据路径用于重复传输时，传输冗余将仅在检测瞬态故障时有用。通过在冗余传输期间发送反相数据，可以提高诊断覆盖率。

为了提供对器件互连和 EMIF 的诊断覆盖，可以对写入的数据进行读回（在写入数据时）并对信息进行多次读回（在读取数据时）。

6.7.16 FSI 数据超限/欠载检测

FSI 模块支持检测数据超限或欠载情况。

- 接收缓冲区超限 - 该事件表明从接收移位寄存器到接收器数据缓冲区寄存器的数据传输将覆盖已接收数据中已经存在的未读数据。
- 接收缓冲区欠载 – 该事件表明软件在缓冲区为空时读取缓冲区
- 发送缓冲区超限 – 如果在传输之前覆盖了一条数据，则会发生该事件。
- 发送缓冲区欠载 – 当发送器尝试从尚未写入的位置读取数据时，会发生该事件。

当发生数据超限/欠载错误并启用了相应的寄存器位时，系统将设置一个标志位并生成中断。

6.7.17 FSI 帧超限检测

FSI 模块支持检测帧超限事件。该事件表明在仍设置 FRAME_DONE 标志时已接收到新帧。如果启用了相应的寄存器位，则会设置标志并生成中断。

6.7.18 FSI CRC 成帧检查

FSI 模块支持检测 CRC 成帧错误情况。当接收到的预期 CRC 值与计算出的 CRC 值不匹配时，将生成 CRC 错误。如果启用，则会设置标志并生成中断。

6.7.19 FSI ECC 成帧检查

FSI 模块支持检测 ECC 成帧错误情况。它在发送器和接收器模式下都支持 16 位或 32 位 ECC 计算模块。在发送模式下，软件可以配置 FSI 寄存器以计算发送缓冲区中数据的 ECC 值，并在接收模式下将其纳入发送帧。软件可以将接收到的数据和 ECC 值反馈给 ECC 模块，以检测并自动校正数据中的单一位错误，或者检测已接收数据中的多位错误并使已接收数据无效。

备注

FSI 模块中支持的 ECC 检查需要借助软件来完成。FSI 模块中的硬件支持 ECC 计算，但写入数据和检查 ECC 错误的任务必须在软件中执行。

6.7.20 FSI 帧看门狗

FSI 模块支持检测帧看门狗超时事件。该事件表明帧看门狗计时器已超时。该超时情况使用 RX_FRAME_WD_CTRL 寄存器进行设置。一旦检测到帧相位的开始，帧看门狗计数器将从 0 开始计数。在看门狗计数器达到基准值之前，帧相位的结束必须完成。如果没有发生这种情况，看门狗将超时，并将生成该事件。如果发生该事件，接收器必须进行软复位和随后的重新同步，以确保正常运行。发生这种情况时，如果启用，则会设置标志并生成中断。

6.7.21 FSI RX Ping 看门狗

FSI 模块支持检测 RX Ping 看门狗超时事件。该事件表明 Ping 看门狗计时器已超时。接收器未在 RX_PING_WD_REF 寄存器中指定的时间段内接收到有效帧。当触发了 Ping 帧并且启用了相应的寄存器位时，会生成 Ping 帧触发的中断。当 Ping 计数器超时时，将设置该位。如果启用了相应的寄存器位，则会生成中断。在发送器上，无需任何进一步的软件或 DMA 干预即可设置和发送 Ping 帧。可通过自动 Ping 计时器、软件或外部触发器来传输 Ping 帧。

6.7.22 FSI 标签监控器

FSI 模块支持传输帧中的标签字段。它包含最后成功接收的帧的 4 位 FRAME_TAG 字段。FSI 标签监控器检查必须在软件中实现。接收端每个帧的标签字段均可通过软件进行监测，并根据预期值进行验证。除了 FRAME_TAG 之外，FSI 模块还支持将用户数据作为用户完全可配置的数据字段，用于数据帧中。通过写入 TX_FRAME_TAG_UDATA.USER_DATA 来设置要传输的用户数据。接收到的用户数据存储在 RX_FRAME_TAG_UDATA.USER_DATA 中。

6.7.23 FSI 帧类型错误检测

FSI 模块支持检测帧类型错误。该错误表明已接收到无效的帧类型。如果发生该错误，接收器必须进行软复位和随后的重新同步，以确保正常运行。如果启用了相应的寄存器位，则会生成中断。

6.7.24 FSI 帧结束错误检测

该错误表明已接收到无效的帧结束位模式。如果发生该错误，接收器必须进行软复位和随后的重新同步，以确保正常运行。如果启用了相应的寄存器位，则会生成中断。

6.7.25 FSI 寄存器保护机制

作为 FSI 模块密钥寄存器的故障避免安全措施，寄存器受到 EALLOW 特权、寄存器密钥和主寄存器锁的保护。这些保护功能确保不会对这些寄存器进行虚假写入或无意修改。FSI 寄存器中的某些位受密钥保护。为了写入这些位，必须同时写入密钥。

控制寄存器锁将阻止对控制寄存器的任何写入，直到锁被释放。若要设置控制寄存器锁，请将 0xA501 分别写入接收器的 RX_LOCK_CTRL 和发送器的 TX_LOCK_CTRL。

6.7.26 LIN 物理总线错误检测

LIN 模块支持检测物理总线错误情况，将设置错误标志并生成中断。如果总线上无法生成有效消息（总线对 GND 或 VBAT 短路），则主器件检测到物理总线错误 (PBE)。如果没有生成同步间隔（例如，总线对 VBAT 短路造成的），或者没有生成同步间隔界定符（例如，总线对 GND 短路造成的），位监测器在报头传输期间检测到 PBE。

6.7.27 LIN 无响应错误检测

LIN 模块支持检测无响应错误情况。当在 TFRAME_MAX（允许响应的最大时间长度）内没有对主器件的标头做出响应时，系统会设置一个错误标志位并生成中断。通过读取 SCIINTVECT0/1 寄存器中相应的中断偏移量来清除无响应错误标志。

6.7.28 LIN 校验和错误检测

LIN 模块支持检测接收到的数据中的校验和错误。当接收节点检测到校验和错误时，系统会设置错误标志位并生成中断。要使用的校验和类型取决于 CIGCR1.CTYPE 位（经典校验和 - 与 LIN 1.3 从节点兼容，或增强校验和 - 与 LIN 2.0 和更新的从节点兼容）。通过读取 SCIINTVECT0/1 寄存器中相应的中断偏移量来清除校验和错误标志。

6.7.29 数据奇偶校验错误检测

LIN 模块支持检测接收到的数据中的奇偶校验错误。当在接收到的数据中检测到奇偶校验错误时，系统会设置错误标志位。在地址位模式下，根据接收到的帧的数据和地址位字段来计算奇偶校验。在空闲线模式下，只使用数据来计算奇偶校验。当接收到的字符中 1 的个数与其奇偶校验位不匹配时，会生成错误。如果奇偶校验功能被禁用（即 SCIGCR1.2 = 0），则 PE 标志被禁用并读为 0。如果 SCISETINT.SETPEINT 位 = 1，则检测到奇偶校验错误会导致 LIN 生成错误中断。

6.7.30 LIN ID 奇偶校验错误检测

LIN 模块支持检测 ID 字段中的奇偶校验错误。如果启用了奇偶校验，当发送的 ID 字节的两个奇偶校验位（偶数/奇数）中的任何一个不等于接收器节点上计算出的奇偶校验位时，将会检测到 ID 奇偶校验错误 (PE)。使用混合奇偶校验算法生成两个奇偶校验位（偶数/奇数）。如果检测到 ID 奇偶校验错误，则标记 ID 奇偶校验错误，并且接收到的 ID 无效

6.7.31 消息中的 PMBus 协议 CRC

PMBus 模块支持使用数据包误差校验 (PEC) 值特性来检测传输期间的数据损坏。当启用该特性时，它会强制 PMBus 发送器接口将 PEC 字节附加到消息末尾。接收器硬件会检查消息中的最后一个字节是否包含与消息中字节数相对应的有效数据包误差校验值。

6.7.32 时钟超时

PMBus 模块支持检测串行时钟 (SCL) 引脚上的卡滞故障。如果 SCL 引脚在通信期间卡滞在高电平或低电平值，且持续时间超过编程值（在 PMBTIMHIGHTIMOUT 和 PMBTIMLOWTIMOUT 寄存器中），则会生成中断并在 PMBSTS 状态寄存器中设置相应的标志。

6.7.33 使用片上计时器进行通信访问延迟性能评测

每个通信消息都需要固定数量的系统时钟周期来完成事务。主器件可以根据从器件发送的消息确认信号来检测事务是否完成。片上计时器模块可用于对完成每个事务所需的时间进行评测。

7 参考文献

1. 德州仪器 (TI)：*计算嵌入式处理器的有效使用寿命*
2. *Moisture/Reflow Sensitivity Classification for Nonhermetic Solid State Surface Mount Devices*, https://www.jedec.org/standards-documents/docs/jesd-22-a112
3. *Handling, Packing, Shipping and Use of Moisture/Reflow Sensitive Surface Mount Devices*, https://www.jedec.org/sites/default/files/docs/jstd033b01.pdf
4. *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, International Electrotechnical Commission, Edition 2.0 2010.
5. *ISO 26262 – Road Vehicles-Functional Safety*, International Standard ISO, vol. 26262, 2018.
6. Standardized E-Gas Monitoring Concept for Gasoline and Diesel Engine Control Units
7. J. Astruc and N. Becker, *Toward the Application of ISO 26262 for Real-Life Embedded Mechatronic Systems*, in International Conference on Embedded Real Time Software and Systems.ERTS2, 2010.
8. 德州仪器 (TI)：*在 TMS320F280x 数字信号控制器上将 PWM 输出用作数模转换器*
9. W. M. Goble and H. Cheddie, Safety Instrumented Systems Verification: Practical Probabilistic Calculations.Isa, 2004.
10. 德州仪器 (TI)：*TMS320C28x FPU 入门*
11. 德州仪器 (TI)：*在 TMS320C28x DSP 上进行在线堆栈溢出检测*
12. IEC-61784 官方网站。可在线获取：https://www.iec.ch。
13. 德州仪器 (TI)：*TMS320F28004x 微控制器技术参考手册*
14. 德州仪器 (TI)：*TMS320F28004x 微控制器数据手册*
15. 德州仪器 (TI)：*UCD3138 监控与通信程序员手册*
16. 德州仪器 (TI)：*加速器：增强 C2000™ MCU 系列的功能*

A 安全架构配置

表 A-1 中列出了安全仪表系统可能采用的各种冗余架构。如需了解更多信息，请参阅 [10]。

表 A-1. 安全架构配置

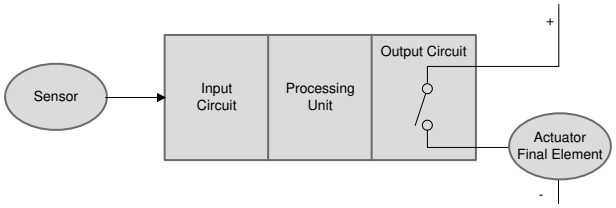
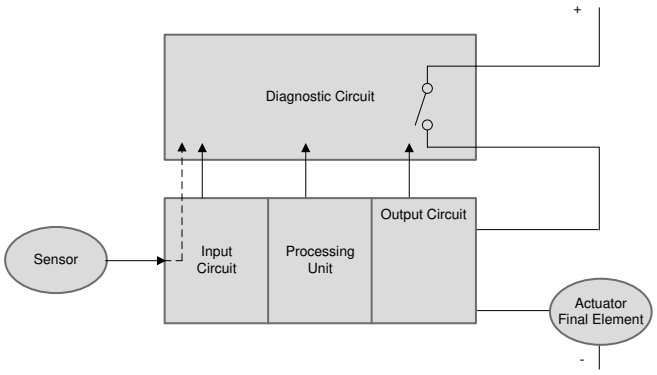
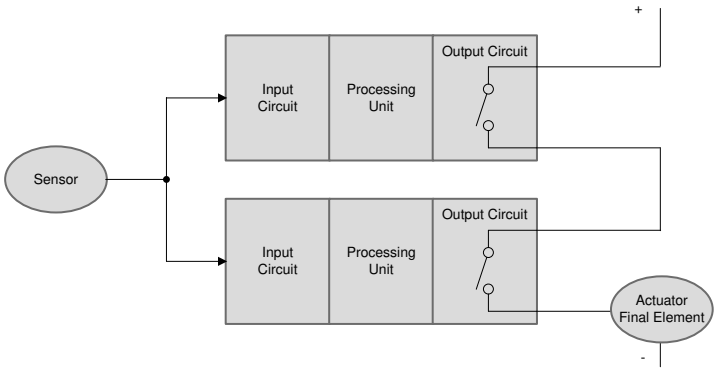
		诊断实现
1	1oo1 架构 	无。
2	1oo1D 	诊断通道是使用各种硬件诊断特性（如看门狗）实现的。
3	1oo1D 与上图相同。	诊断通道是使用互惠式比较（使用两个处理单元来实现互惠式比较）和其他硬件诊断特性实现的。
4	1oo2 	两个不同的处理单元用于实现一个通道。

表 A-1. 安全架构配置 (continued)

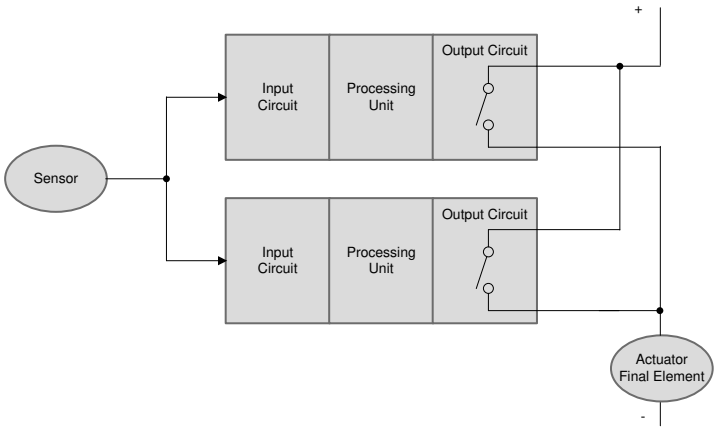
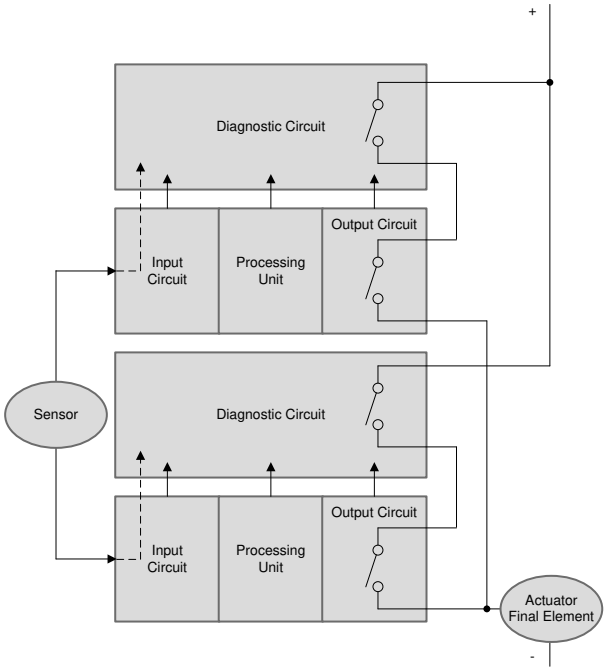
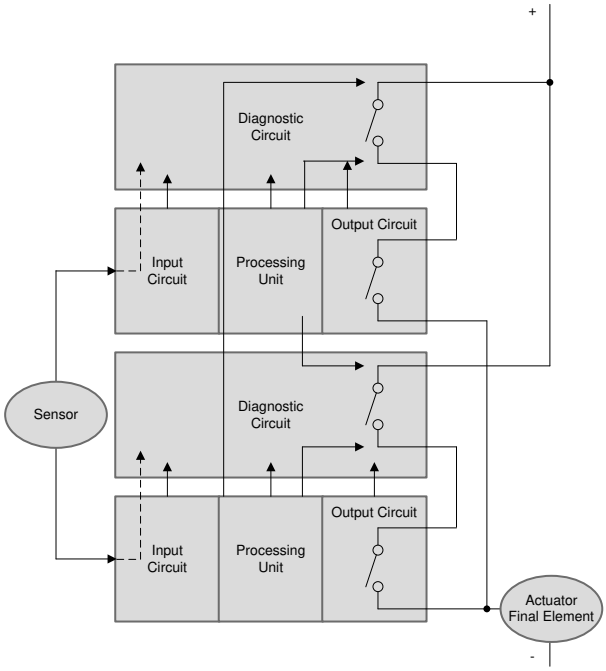
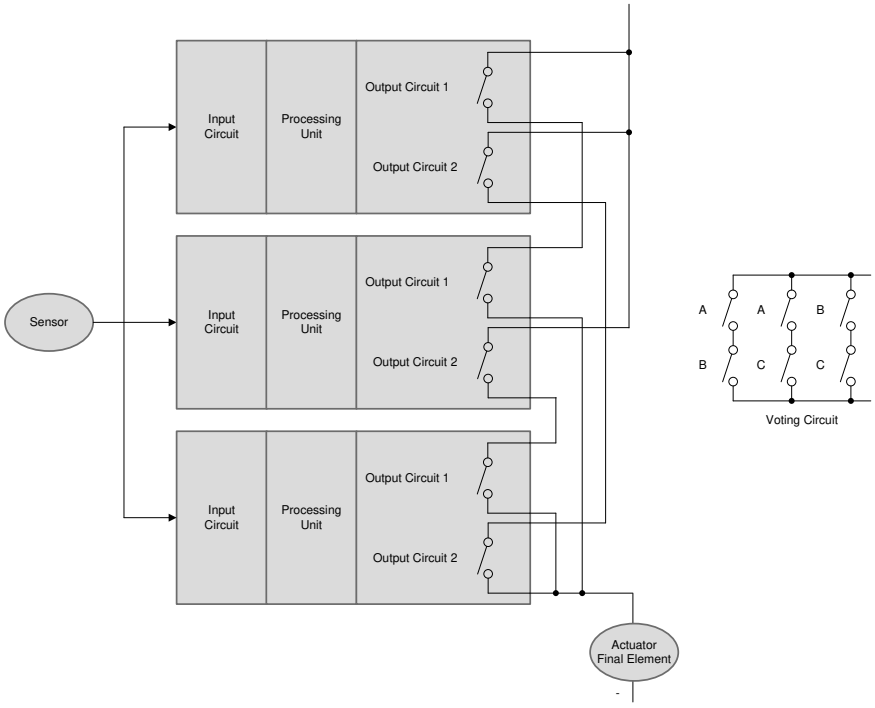
		诊断实现
5	2oo2 	两个不同的处理单元用于实现一个通道。
6	2oo2D 	#2 的两个 1oo1D 结构通过导线连接在一起以实现一个安全通道。
7	2oo2D 与上图相同。	#3 的两个 1oo1D 结构通过导线连接在一起。

表 A-1. 安全架构配置 (continued)

		诊断实现
8	1oo2D 	类似于 #6 的 2oo2D 实现，带有额外的控制线路（通过导线连接）以使用另一个单元控制一组单元
9	1oo2D 与上图相同。	类似于 #7 的 2oo2D 实现，带有额外的控制线路（通过导线连接）以使用另一个单元控制一组单元。
10	2oo3 	使用三个不同的处理单元来实现多数表决。第四个通道可以单独使用，也可以与硬件诊断特性一同使用。

B 分布式开发

开发接口协议 (DIA) 旨在让双方就管理与功能安全系统开发相关的各方责任达成协议。功能安全合规型组件通常设计用于许多不同的系统，并视为独立安全要素 (SEooC) 硬件组件。然后，系统集成商负责使用硬件组件功能安全手册、功能安全分析报告和功能安全报告中提供的信息来执行系统集成活动。由于没有分配开发活动，TI 不接受与系统集成商签订 DIA。

“符合功能安全标准”的组件是 TI 所代表、推广或营销的产品，可帮助客户降低最终应用中的功能安全相关风险和/或符合行业功能安全标准。更多有关功能安全合规型组件的信息，请转至此处。

B.1 功能安全生命周期如何应用于功能安全合规型产品

TI 已经按需修改了 ISO 26262:2018 和 IEC 61508:2010 的功能安全生命周期，以更好地满足独立功能安全要素 (SEooC) 开发的需求。功能安全标准是在功能安全系统的环境中编写的，这意味着某些要求仅适用于系统级。功能安全合规型组件是硬件或软件组件，因此，TI 已经按需修改了功能安全活动，以创建新的硬件和软件产品开发流程，确保适当地应用先进的技术和措施。这些新产品开发流程已通过第三方功能安全专家的认证。若要查找这些认证，请转至此处。

B.2 德州仪器 (TI) 执行的活动

功能安全合规型集成电路 (IC) 产品是作为独立功能安全要素而开发的硬件组件。如此一来，TI 的功能安全活动集中在那些与围绕硬件组件开发的功能安全管理相关的方面。系统级架构、设计和功能安全分析不在 TI 活动的范围之内，而是由系统集成商负责。ISO 26262-11:2018 中提供了一些将该硬件组件的 SEooC 安全分析集成到系统级的技术。

表 B-1. 德州仪器 (TI) 执行的活动与客户执行的活动

功能安全生命周期活动	TI 执行	系统集成商执行
功能安全的管理	是	是
终端设备和相关项的定义	否	是
终端设备/相关项的危害分析和风险评估	否	是
终端设备功能安全概念的创建	否。做出假设以进行内部开发。	是
子系统、硬件组件和软件组件的终端设备要求分配	否。做出假设以进行内部开发。	是
硬件组件安全要求定义	是	否
硬件组件架构和设计执行	是	否
硬件组件功能安全分析	是	否
硬件组件验证和确认 (V&V)	执行 V&V 以支持内部开发。	是
将硬件组件集成到终端设备中	否	是
验证终端设备中的 IC 性能	否	是
选择应用于 IC 的安全机制	否	是
终端设备级验证和确认	否	是
终端设备级功能安全分析	否	是
终端设备级功能安全评估	否	是
终端设备批量生产	否	是
生产中功能安全问题管理	根据需要提供支持	是

B.3 提供的信息

德州仪器 (TI) 总结了其认为客户可以公开或根据保密协议 (NDA) 获得的关键功能安全工作产品。为了保护在特定功能安全文档中披露的专有和敏感信息，必需签署 NDA。

表 B-2. 产品功能安全文档

交付物名称	内容
功能安全产品预发布	概述了产品开发和产品架构的功能安全考量。在公开发布产品之前提供。

表 B-2. 产品功能安全文档 (continued)

交付物名称	内容
功能安全手册	针对产品功能安全特性的用户指南，包括系统级使用假定。
功能安全分析报告	以允许计算定制指标的格式记录可提供的功能安全分析所有结果。
功能安全报告(1)	汇总了符合功能安全标准的理由和证据。引用已分析的特定组件、组件系列或 TI 流程。
评估证书(1)	符合功能安全标准的证据。引用已分析的特定组件、组件系列或 TI 流程。由第三方功能安全评估机构提供。

(1) 当功能安全合规型产品获得评估证书时，可能不会提供功能安全报告。提供功能安全报告时，可能不会提供评估证书。这两个文档满足相同的功能安全要求，并将根据功能安全合规型产品互换使用。

C 术语和定义

- IEC 61508：E/E/PE 安全相关系统的功能安全标准，旨在作为适用于各行各业的基本功能安全标准。它将功能安全定义为：“与 EUC（受控设备）和 EUC 控制系统相关的整体安全的一部分，依赖于 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施的正常运行”[4]。
- ISO 13849：为控制系统安全相关部分 (SRP/CS) 的设计和集成提供安全要求和指南，包括软件设计。
- N 取 M (MooN) 架构：一种安全仪表系统，需要“N”个通道中的最少“M”个通道才能实现安全功能运行（例如三取二 (2oo3) 架构，其中多数表决用于实现安全功能）。

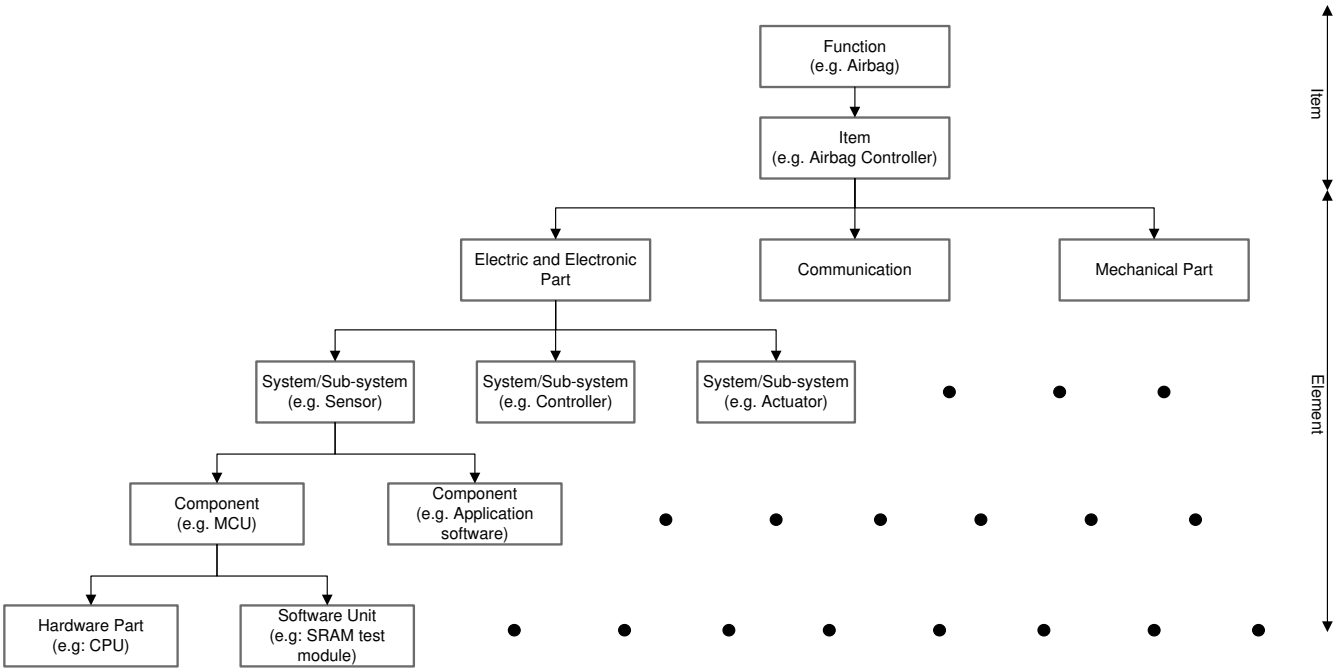


图 C-1. ISO 26262 相关项、系统、组件、硬件元器件和软件单元的说明

- 具有诊断功能的 N 取 M 通道架构 (MooND)。
- 功能安全：与 EUC 和 EUC 控制系统相关的整体安全的一部分，依赖于 E/E/PE 安全相关系统和其他风险降低措施的正常运行
- 相关项：一个系统或多个系统的组合，能够实现整车级功能，采用 ISO 26262:2018 标准（例如，汽车的动力转向）。

- 要素：系统或系统的一部分，包括组件、硬件、软件、硬件元器件和软件单元。
- 系统：一组与至少一个传感器、一个控制器和一个执行器相关联的要素
- 组件：在逻辑上和技术上可分离的非系统级要素，由硬件元器件和软件单元组成。
- 硬件元器件：无法细分的硬件（例如 CPU）。
- 软件单元：软件架构中可进行独立测试的原子级软件组件（例如，SRAM 测试模块）。
- 失效：要素按要求执行功能的能力的终止。
- 失效模式：要素或相关项发生故障的方式。
- 单点故障：安全机制未涵盖的要素故障，会直接导致违反安全目标。
- 单点失效：单点故障导致的失效，会直接导致违反安全目标。
- 多点故障：与其他独立故障一同导致多点失效的单个故障。
- 多点失效：由多个独立故障组合导致的失效，会直接导致违反安全目标。对于直接违反安全目标的多点失效，必须同时出现所有独立故障。
- 多点故障检测间隔：在多点故障导致多点失效之前检测多点故障的时间跨度。
- 潜在故障：在多点故障检测间隔内既没有被安全机制检测到，也没有被驱动器感知到的多点故障。
- 功能安全评估：基于证据的调查，以判断一个或多个 E/E/PE 安全相关系统和/或其他风险降低措施实现的功能安全。
- 功能安全审计：系统性的独立检查，以确定符合计划安排的功能安全要求的特定程序是否得到有效实现，以及是否适合实现规定的目标。
- 危害和风险分析 (IEC 61508:2010)/危害分析和风险评估 (ISO 26262:2018)：用于识别安全功能和/或功能安全目标的终端设备级功能安全分析。该过程还确立了 SIL (IEC 61508:2010) 或 ASIL (ISO 26262:2018) 等级，定义了每个安全功能和/或功能安全目标所需的风险降低等级。
- 流程定制：更改开发流程或功能安全生命周期以满足企业参与需求的行为。要求可以从一个阶段移动到另一个阶段或由其他开发人员执行，但不允许删除流程要求。
- 质量管理：指按照适用的质量标准而不是功能安全标准开发的设计要素。根据功能安全认证的结果，可以在特定功能安全设计中使用质量管理型设计要素。
- 安全要求分解：安全要求分解是将安全要求分解为一系列较低抽象级冗余安全要求的过程，以支持定制较低抽象级设计要素的 SIL (ISO 26262:2018)/ASIL (ISO 26262:2018) 合规要求。例如，可通过具有较低安全完整性的外设的冗余实例来满足具有高安全完整性的外设功能的要求。
- 有关 ISO 26262 的适用术语及其定义的完整列表，请参阅 ISO 26262-1:2018，道路车辆 — 功能安全 — 第 1 部分：词汇表。
- 有关 IEC 61508 的适用术语及其定义的完整列表，请参阅 IEC 61508:2010，电气/电子/可编程电子安全相关系统的功能安全 — 第 4 部分：定义和缩写。

D 安全特性和诊断汇总

表 D-1. 汇总表图例

唯一标识符	用于引用内容的标识符
安全特性或诊断	安全特性
用途	此图表中列出的每个测试可以是以下两种类型之一：“诊断”测试或“诊断用测试”。 诊断：覆盖器件主要功能发生的故障。此外，它还可以提供其他诊断的故障覆盖范围，因此在某些情况下也可以用作诊断用测试 仅诊断用测试：不覆盖器件主要功能发生的故障。它仅用于提供其他诊断的故障覆盖范围
诊断类型	硬件 - 由 TI 在器件中实现的诊断，可在检测到失效时传达错误状态。它可能需要软件来启用诊断和/或在检测到失效时采取行动。 软件 - TI 推荐的测试，必须由软件实现者创建。此测试可能会使用 TI 在器件上实施的其他硬件。 硬件/软件 - TI 推荐的测试，既需要 TI 在器件中实施的诊断硬件，也需要必须由软件实现者创建的软件。 系统 - 在微控制器外部实施的诊断
诊断操作	可以是以下情况之一： (i) 启动（默认启用） (ii) 连续 - 复位时启用：复位时默认启用的硬件安全机制。 (iii) 连续 - 由软件启用：需要由软件启用的硬件安全机制。 (iv) 按需（软件定义）：在诊断测试间隔内由软件激活的软件或硬件-软件安全机制 (v) 系统定义：由系统实现。
测试执行时间	此列列出了完成此诊断所需的时间。
针对所检测故障执行的操作	检测到错误时此诊断所采取的响应措施。 对于软件驱动的测试，此操作通常取决于软件实现。
错误报告时间	用于向系统指示所检测故障的诊断所需的典型时间。对于故障检测时间已知的安全机制，将指示该值。对于软件驱动的测试，此时间通常取决于软件实现。

表 D-2. 安全特性和诊断汇总

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
电源	PWR1	外部电压监控器	诊断	系统	系统定义	系统定义	系统定义	系统定义
	PWR2	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	PWR4	欠压复位 (BOR)	诊断	硬件	连续 - 复位时启用	零或超低开销	器件复位	通常小于 1us
时钟	CLK1	时钟丢失检测 (MCD)	诊断	硬件	连续 - 复位时启用	零或超低开销	带有 ERRORSTS 断言和 PLL 参考时钟的 NMI 切换到 INTOSC1	0.82ms
	CLK2	使用 CPU 计时器进行时钟完整性检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLK3	使用 HRPWM 进行时钟完整性检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLK4	双路时钟比较器 (DCC) - 0 类	诊断	硬件 - 软件	按需（软件定义）	软件定义	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	CLK5	通过 XCLKOUT 对时钟进行外部监测	诊断	系统	系统定义	系统定义	系统定义	系统定义
	CLK6	内部看门狗 (WD)	诊断	硬件	连续 - 复位时启用	零或超低开销	根据配置进行器件复位或中断	软件定义
	CLK7	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	CLK8	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLK9	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLK10	看门狗 (WD) 操作的软件测试	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLK12	时钟丢失检测功能的软件测试	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLK13	使用片上计时器进行 PLL 锁定性能评测	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLK14	外设时钟门控 (PCLKCR)	故障避免	硬件 - 软件	按需（软件定义）	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
复位	RST1	热复位的外部监测 (XRSn)	诊断	系统	系统定义	系统定义	系统定义	系统定义
	RST2	复位原因信息	故障避免	硬件 - 软件	按需（软件定义）	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	RST3	复位的软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	RST4	复位引脚上的干扰滤波	故障避免	硬件	连续 - 复位时启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	RST5	NMIWD 影子寄存器	故障避免	硬件 - 软件	按需（软件定义）	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	RST6	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	RST7	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	RST8	NMIWD 复位功能	诊断	硬件	连续 - 复位时启用	零或超低开销	器件复位	软件定义
	RST9	外设软复位 (SOFTPRES)	故障避免	硬件 - 软件	按需（软件定义）	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
系统控制模块和配置寄存器	SYS1	控制寄存器的多位使能键	故障避免	硬件	连续 - 复位时启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	SYS2	针对控制寄存器的锁定机制	故障避免	硬件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	SYS3	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SYS4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SYS5	在线监测温度	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	SYS8	关键寄存器的 EALLOW 和 MEALLOW 保护功能	故障避免	硬件	连续 - 复位时启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
系统控制模块和配置寄存器（续）	SYS9	ERRORSTS 功能的软件测试	诊断	软件	按需（软件定义）	软件定义	系统定义	系统定义
	SYS10	外设访问保护 - 0 类	故障避免	硬件 - 软件	按需（软件定义）	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
电子保险丝	EFUSE1	电子保险丝自动负载自检	诊断	硬件	启动（默认启用）	零或超低开销	器件复位	<400 个 CPU 周期
	EFUSE2	电子保险丝 ECC	诊断	硬件	启动（默认启用）	零或超低开销	器件复位	<400 个 CPU 周期
	EFUSE4	电子保险丝 ECC 逻辑自检	诊断用测试	硬件	启动（默认启用）	零或超低开销	器件复位	<400 个 CPU 周期
调试逻辑	JTAG1	JTAG 端口的硬件禁用	故障避免	系统	连续 - 复位时启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	JTAG3	内部看门狗 (WD)	诊断	硬件	连续 - 复位时启用	零或超低开销	根据配置进行器件复位或中断	软件定义
	JTAG4	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
C28x 中央处理单元	CPU1	软件互惠式比较	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CPU3	CPU 的软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CPU4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CPU5	存储器访问保护机制	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	CPU7	CPU 对于非法操作、非法结果和指令陷入的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
C28x 中央处理单元（续）	CPU8	内部看门狗 (WD)	诊断	硬件	连续 - 复位时启用	零或超低开销	根据配置进行器件复位或中断	软件定义
	CPU9	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	CPU10	信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CPU14	栈溢出检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	CPU15	VCU CRC 自动覆盖	诊断用测试	硬件	连续 - 复位时启用	零或超低开销	软件定义	软件定义
	CPU18	嵌入式实时分析和诊断 (ERAD) - 0 类	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
控制律加速器 (CLA)	CLA1	软件互惠式比较	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLA2	CLA 的软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLA3	CLA 对于非法操作和非法结果的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	CLA4	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLA5	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLA7	信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLA8	使用 CPU 进行 CLA 活跃度检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CLA9	存储器访问保护机制	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
控制律加速器 (CLA)（续）	CLA11	禁用未使用的 CLA 触发源	故障避免	软件	连续 - 由软件启用	零或超低开销	NA（故障避免技术）	NA（故障避免技术）
闪存	FLASH1	闪存 ECC	诊断	硬件	连续 - 复位时启用	零或超低开销	基于错误严重性的带有 ERRORSTS 断言或 CPU 中断的 NMI	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	FLASH2	静态存储器内容的 VCU CRC 检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	FLASH3	闪存阵列中的位多路复用	故障避免	硬件	连续 - 复位时启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	FLASH4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	FLASH5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	FLASH6	ECC 逻辑的软件测试	诊断用测试	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	FLASH7	闪存程序验证和擦除验证检查	故障避免	软件	按需（软件定义）	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	FLASH8	闪存预取、数据缓存和等待状态的软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	FLASH9	内部看门狗 (WD)	诊断	硬件	连续 - 复位时启用	零或超低开销	根据配置进行器件复位或中断	软件定义
	FLASH10	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	FLASH12	CPU 对于非法操作、非法结果和指令陷入的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	FLASH14	信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
SRAM	SRAM1	SRAM ECC	诊断	硬件	连续 - 复位时启用	零或超低开销	基于错误严重性的带有 ERRORSTS 断言或 CPU 中断的 NMI	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	SRAM2	SRAM 奇偶校验	诊断	硬件	连续 - 复位时启用	零或超低开销	带有 ERRORSTS 断言的 NMI	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	SRAM3	SRAM 的软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SRAM4	SRAM 存储器阵列中的位多路复用	故障避免	硬件	连续 - 复位时启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	SRAM5	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SRAM6	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SRAM7	清理数据以检测/校正存储器错误	故障避免	软件	按需（软件定义）	软件定义	基于错误严重性的带有 ERRORSTS 断言或 CPU 中断的 NMI	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	SRAM8	静态存储器内容的 VCU CRC 检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SRAM10	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SRAM11	存储器访问保护机制	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	SRAM12	针对控制寄存器的锁定机制	故障避免	硬件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	SRAM13	ECC 逻辑的软件测试	诊断用测试	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
SRAM（续）	SRAM14	奇偶校验逻辑的软件测试	诊断用测试	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	SRAM16	信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SRAM17	CPU 对于非法操作、非法结果和指令陷入的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	SRAM18	内部看门狗 (WD)	诊断	硬件	连续 - 复位时启用	零或超低开销	根据配置进行器件复位或中断	软件定义
	SRAM19	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	SRAM20	CLA 对于非法操作和非法结果的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	SRAM21	存储器开机自检 (MPOST)	诊断	硬件	启动（默认启用）	软件定义	软件定义	软件定义
ROM	ROM1	静态存储器内容的 VCU CRC 检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ROM2	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ROM3	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ROM4	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ROM5	CPU 对于非法操作、非法结果和指令陷入的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S*（中断处理时间取决于系统负载和软件）
	ROM6	内部看门狗 (WD)	诊断	硬件	连续 - 复位时启用	零或超低开销	根据配置进行器件复位或中断	软件定义
	ROM7	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	ROM8	上电预运行安全检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
ROM（续）	ROM9	CLA-PROM 的背景 CRC (CLAPROMCRC)	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	ROM10	存储器开机自检 (MPOST)	诊断	硬件	启动（默认启用）	零或超低开销	软件定义	软件定义
器件互连	INC1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	INC2	内部看门狗 (WD)	诊断	硬件	连续 - 复位时启用	零或超低开销	根据配置进行器件复位或中断	软件定义
	INC3	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	INC4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	INC5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	INC6	CPU 对于非法操作、非法结果和指令陷入的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	INC7	CLA 对于非法操作和非法结果的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	INC8	传输冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	INC9	硬件冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
直接存储器访问 (DMA)	DMA2	信息冗余技术	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DMA3	传输冗余	诊断	软件	按需 (软件定义)	软件定义	系统定义	软件定义
	DMA4	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DMA5	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DMA6	包括错误测试在内的功能软件测试	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
直接存储器访问 (DMA) (续)	DMA7	DMA 溢出中断	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	DMA8	存储器访问保护机制	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	DMA9	禁用未使用的 DMA 触发源	故障避免	软件	连续 - 由软件启用	NA (故障避免)	NA (故障避免技术)	NA (故障避免技术)
增强型外设中断扩展器 (ePIE)	PIE1	PIE 双 SRAM 硬件比较	诊断	硬件	连续 - 复位时启用	零或超低开销	单核器件：CPU 异常，双核器件：带有 ERRORSTS 断言的 NMI	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	PIE2	SRAM 的软件测试	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	PIE3	包括错误测试在内的 ePIE 运行软件测试	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	PIE4	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	PIE5	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	PIE6	PIE 双 SRAM 比较检查	诊断用测试	软件	按需 (软件定义)	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	PIE7	为未使用的中断维护中断处理程序	诊断	软件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	PIE8	在线监测中断和事件	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	PIE9	硬件冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
双区域代码安全模块 (DCSM)	DCSM1	控制寄存器的多位使能键	故障避免	硬件	连续 - 复位时启用	NA (故障避免)	NA (故障避免技术)	NA (故障避免技术)
	DCSM2	链路指针的多数表决和错误检测	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DCSM3	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DCSM4	包括错误测试在内的功能软件测试	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DCSM5	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DCSM6	CPU 对于非法操作、非法结果和指令陷入的处理	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	DCSM8	静态存储器内容的 VCU CRC 检查	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	DCSM9	外部看门狗	诊断	系统	系统定义	系统定义	系统定义	系统定义
	DCSM11	硬件冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
交叉开关 (X-BAR)	XBAR1	包括错误测试在内的功能软件测试	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	XBAR2	硬件冗余	诊断	软件	连续 - 由软件启用	零或超低开销	软件定义	软件定义
	XBAR3	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	XBAR4	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	XBAR5	X-BAR 标志的软件检查	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
计时器	TIM1	使用次级自由运行计数器进行 1oo2 软件表决	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	TIM2	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	TIM3	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
计时器 (续)	TIM4	包括错误测试在内的功能软件测试	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
通用 I/O 和多路复用 (GPIO 和 PINMUX)	GPIO1	针对控制寄存器的锁定机制	故障避免	硬件	连续 - 由软件启用	NA (故障避免)	NA (故障避免技术)	NA (故障避免技术)
	GPIO2	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	GPIO3	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	GPIO4	使用 I/O 环回的功能软件测试	诊断	硬件 - 软件	按需 (软件定义)	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	GPIO5	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
增强型脉宽调制器 (ePWM)	PWM1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PWM2	硬件冗余	诊断	软件	连续 - 由软件启用	零或超低开销	软件定义	软件定义
	PWM3	eCAP 对 ePWM 的监测	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PWM4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PWM5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PWM6	针对控制寄存器的锁定机制	故障避免	硬件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	PWM8	使用 XBAR 进行 ePWM 故障检测	诊断	软件	连续 - 由软件启用	零或超低开销	软件定义	软件定义
	PWM9	ePWM 同步检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PWM11	ePWM 应用级安全机制	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PWM12	在线监测周期性中断和事件	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PWM13	ADC 对 ePWM 的监测	诊断	系统	按需（软件定义）	软件定义	软件定义	软件定义
高分辨率捕捉 (HRCAP)	HRCAP1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	HRCAP2	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	HRCAP3	HRCAP 对 HRPWM 的监测	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
	HRCAP4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	HRCAP5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	HRCAP7	HRCAP 校准逻辑测试特性	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
高分辨率脉宽调制器 (HRPWM)	OTTO1	HRPWM 内置自检和诊断功能	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	OTTO2	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	OTTO3	eCAP 对 ePWM 的监测	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	OTTO4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	OTTO5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
增强型捕捉 (eCAP)	CAP1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAP2	信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAP3	eCAP 对 ePWM 的监测	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAP4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAP5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	CAP6	eCAP 应用级安全机制	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAP7	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
增强型正交编码器脉冲 (eQEP)	QEP1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	QEP2	eQEP 正交看门狗	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	QEP3	信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	QEP4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	QEP5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	QEP6	eQEP 应用级安全机制	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	QEP7	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	QEP8	QMA 错误检测逻辑	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	QEP9	正交看门狗功能的 eQEP 软件测试	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
可编程增益放大器 (PGA)	PGA1	PGA 至 ADC 环回测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PGA2	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PGA3	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PGA4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PGA6	针对控制寄存器的锁定机制	故障避免	硬件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
本地互连网络 (LIN)	LIN1	使用 I/O 环回的功能软件测试	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	LIN2	包括端到端安全状态恢复的信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	LIN3	传输冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	LIN4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	LIN5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	LIN6	数据奇偶校验错误检测	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	LIN7	超限错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	LIN8	帧错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	LIN9	LIN 物理总线错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	LIN10	LIN 无响应错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	LIN11	位错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
本地互连网络 (LIN)（续）	LIN12	LIN 校验和错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	LIN13	LIN ID 奇偶校验错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	LIN15	SCI 中断错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	LIN16	使用片上计时器进行通信访问延迟性能评测	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
快速串行接口 (FSI)	FSI1	使用 I/O 环回的功能软件测试	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	FSI2	包括端到端安全状态恢复的信息冗余技术	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	FSI3	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	FSI4	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	FSI5	传输冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	FSI6	FSI 数据超限/欠载检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	FSI7	FSI 帧超限检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
快速串行接口 (FSI)（续）	FSI8	FSI CRC 成帧检查	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	FSI9	FSI ECC 成帧检查	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	FSI10	FSI 帧看门狗	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	FSI11	FSI RX Ping 看门狗	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	FSI12	FSI 标签监控器	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	FSI13	FSI 帧类型错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	FSI14	FSI 帧结束错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	FSI15	FSI 寄存器保护机制	故障避免	硬件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
电源管理总线模块 (PMBus)	PMBUS2	I2C 数据确认检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PMBUS3	包括端到端安全状态恢复的信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
电源管理总线模块 (PMBus)（续）	PMBUS4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PMBUS5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PMBUS6	传输冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	PMBUS7	消息中的 PMBus 协议 CRC	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	PMBUS8	时钟超时	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
Σ-Δ 滤波器模块 (SDFM)	SDFM1	用于在线监测的 SDFM 比较器滤波器 - 0 类	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	SDFM2	信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SDFM3	SD 调制器时钟故障检测机制	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	SDFM4	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SDFM5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SDFM6	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SDFM7	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
XINT	XINT1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	XINT2	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
XINT（续）	XINT3	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	XINT4	硬件冗余	诊断	软件	连续 - 由软件启用	零或超低开销	软件定义	软件定义
模数转换器 (ADC)	ADC1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ADC2	DAC 至 ADC 环回检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ADC3	ADC 信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ADC4	ADC 的开路/短路检测电路	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	ADC5	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ADC6	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ADC7	通过改变采集窗口来检查 ADC 信号质量	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ADC8	ADC 输入信号完整性检查	诊断	硬件	连续 - 由软件启用	零或超低开销	软件定义	软件定义
	ADC9	ADC 对 ePWM 的监测	诊断	系统	按需（软件定义）	软件定义	软件定义	软件定义
	ADC10	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	ADC11	禁用 ADC 未使用的 SOC 输入源	故障避免	软件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
BUFDAC	DAC1	包括错误测试在内的功能软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	DAC2	DAC 至 ADC 环回检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	DAC3	针对控制寄存器的锁定机制	故障避免	硬件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	DAC4	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	DAC5	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
BUFDAC（续）	DAC6	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	DAC7	DAC 至比较器环回检查	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
CMPSS	CMPSS1	包括错误测试在内的功能软件测试	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CMPSS3	硬件冗余	诊断	软件	连续 - 由软件启用	软件定义	软件定义	软件定义
	CMPSS4	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CMPSS5	静态配置寄存器的定期软件读回	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CMPSS6	针对控制寄存器的锁定机制	故障避免	硬件	连续 - 由软件启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	CMPSS7	通过 ADC 进行 VDAC 转换	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CMPSS8	CMPSS 斜坡发生器功能检查	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
控制器局域网 (DCAN)	CAN1	使用 I/O 环回的功能软件测试	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAN2	包括端到端安全状态恢复的信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAN3	SRAM 奇偶校验	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	CAN4	SRAM 的软件测试	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	CAN5	SRAM 存储器阵列中的位多路复用	故障避免	硬件	连续 - 复位时启用	NA（故障避免）	NA（故障避免技术）	NA（故障避免技术）
	CAN7	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAN8	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
控制器局域网 (DCAN)（续）	CAN9	传输冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAN10	DCAN 填充错误检测	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	CAN11	DCAN 格式错误检测	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	CAN12	DCAN 确认错误检测	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	CAN13	位错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	CAN14	消息中的 CRC	诊断	硬件	连续 - 复位时启用	零或超低开销	CPU 中断	通知时间通常小于 1 µS*（中断处理时间取决于系统负载和软件）
	CAN15	奇偶校验逻辑的软件测试	诊断用测试	软件	按需（软件定义）	软件定义	软件定义	软件定义
	CAN16	硬件冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
串行外设接口 (SPI)	SPI1	使用 I/O 环回的功能软件测试	诊断	硬件 - 软件	按需（软件定义）	软件定义	软件定义	软件定义
	SPI2	包括端到端安全状态恢复的信息冗余技术	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SPI3	静态配置寄存器的定期软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
串行外设接口 (SPI)（续）	SPI4	写入配置的软件读回	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义
	SPI5	传输冗余	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	SPI6	SPI 数据超限检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	SPI7	硬件冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
串行通信接口 (SCI)	SCI1	使用 I/O 环回的功能软件测试	诊断	硬件 - 软件	按需 (软件定义)	软件定义	软件定义	软件定义
	SCI2	消息中的奇偶校验	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	SCI3	包括端到端安全状态恢复的信息冗余技术	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	SCI4	超限错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	SCI5	SCI 中断错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
	SCI6	帧错误检测	诊断	硬件	连续 - 由软件启用	零或超低开销	CPU 中断	通知时间通常小于 1 µ S* (中断处理时间取决于系统负载和软件)
串行通信接口 (SCI) (续)	SCI7	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	SCI8	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	SCI9	传输冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	SCI10	硬件冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
内部集成电路 (I2C)	I2C1	使用 I/O 环回的功能软件测试	诊断	硬件 - 软件	按需 (软件定义)	软件定义	软件定义	软件定义
	I2C2	I2C 数据确认检查	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	I2C3	包括端到端安全状态恢复的信息冗余技术	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	I2C4	静态配置寄存器的定期软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	I2C5	写入配置的软件读回	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义
	I2C6	传输冗余	诊断	软件	按需 (软件定义)	软件定义	软件定义	软件定义

表 D-2. 安全特性和诊断汇总 (continued)

器件分区	唯一标识符	安全特性或诊断	用途	诊断类型	诊断操作	测试执行时间	针对所检测故障执行的操作	错误报告时间
	I2C7	使用片上计时器进行 I2C 访问延迟性能评测	诊断	软件	按需（软件定义）	软件定义	软件定义	软件定义

E 术语表

本文档中使用的定义术语列于表 E-1 中。

表 E-1. 术语表

首字母缩写词	全称
ADC	模数转换器
ASIL	汽车安全完整性等级 (ISO 26262:2018)
CLA	控制律加速器
CPU	中央处理单元
CRC	循环冗余校验
CSP	合规性支持包
DAC	数模转换器
DC	诊断覆盖
DTI	诊断测试间隔
E/E/PE	电气/电子/可编程电子
E2E	端到端协议
ePIE	增强型外设中断扩展
ePWM	增强型脉宽调制器
eQEP	增强型正交编码器脉冲
ERAD	嵌入式实时分析和诊断
EUC	受控设备
FMEDA	失效模式影响和诊断分析
FPU	浮点单元
FSA	功能安全评估
FSI	快速串行接口
FTA	故障树分析
FTTI	容错时间间隔
HARA	危害分析和风险评估
HFT	硬件故障容错
HRCAP	高分辨率捕捉
IEC	国际电工委员会
ISO	国际标准化组织
LIN	本地互连网络
MCU	微控制器单元
MTBF	故障间隔平均时间
OTP	一次性可配置
PGA	可编程增益放大器
PMBus	电源管理总线模块
PWM	脉宽调制器
SECDED	单错校正双错检测
SIL	安全完整性等级
SOC	转换开始
SPS	软件产品规格
TI	德州仪器 (TI) 公司
TMU	三角函数加速器
VCU	Viterbi、复杂数学和 CRC 单元

修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision C (September 2020) to Revision D (January 2022)	Page
• 更新了整个文档中的表格、图和交叉参考的编号格式。	3
• 对节 4.3 进行了更新。	19
• 对节 4.3.4 进行了更新。	22

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265