C2000™ 实时微控制器的工业功能安全概述

借助我们的功能安全合规型产品、文档、软件以及我们知识渊博的专家提供的支持，简化和加快 IEC 61508 (SIL) 和 ISO13849 (PL) 认证流程。我们的 C2000™ 实时 MCU 经过 TUV SUD 独立评估和认证，系统功能高达 SIL 3 等级，可帮助您打造需要功能安全的工业应用。C2000 实时 MCU 还满足汽车功能安全要求。

C2000 功能安全产品的亮点有

- 器件架构助力实现功能安全
- 文档支持客户轻松进行系统级安全评估
- 软件库助力实施安全机制

C2000 关键安全机制

安全机制通过检测潜在的危险故障，可帮助将系统置于安全状态，在确保系统的整体安全方面发挥着关键作用。凭借由 TUV SUD 定义并独立评估其有效性的 300 多种安全机制，C2000 MCU 可提供所需的诊断覆盖范围，从而满足元件级 SIL 2 的随机硬件功能。功能安全手册提供了有关安全机制的详细信息，以及避免元件之间干扰和相关失效的技术，可帮助客户开发符合 SIL 3 要求的合规系统。可调的 FMEDA 提供了更高的灵活性，支持使用封装时基故障 (FIT) 估算、产品功能定制、安全机制定制和定制诊断等功能来自定义和计算硬件指标，从而使客户能够根据自己的应用特定需求**调整 FMEDA**。

详细了解 C2000 实时 MCU 安全机制

	主要安全特性	F2838x	F28P65x	F2837x F2807x	F28P55x	F28003x	F28002x	F280015x
硬件	符合 SIL 3 标准的开发流程	✓	✓	✓	✓	✓	✓	✓
	随机硬件功能	SIL 2	SIL 2	SIL 2	SIL 2	SIL 2	QM	SIL 2
	系统功能	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3
	CPU 的单点故障覆盖 (SPFM)	相互比较	相互比较 (CPU1 + CLA) 锁步 C28x (CPU2)	相互比较	相互比较	相互比较	不适用	锁步 C28x
	存储器奇偶校验	✓	✓	✓	✓	X	X	✓
	存储器 ECC	✓	仅闪存	✓	✓	✓	✓	✓
	存储器 BIST (MPOST)	✓	✓	X	✓	✓	✓	✓
	双核安全模块 (DCSM) 实现软件元素之间不干扰	✓	✓	✓	✓	✓	✓	✓
	具有独立时钟的窗口化看门狗计时器	✓	✓	✓	✓	✓	✓	✓
	硬件 CRC 加速	✓	✓	✓	✓	✓	✓	✓
	硬件 BIST (HWBIST)：C28x CPU 的永久性故障覆盖率超过 90%	✓	✓	✓	X	✓	✓	X
	冗余且独立的 ADC/PWM 模块	✓	✓	✓	✓	✓	✓	✓
	在硬件中自动比较 ADC 转换结果	X	✓	X	✓	X	X	X
	冗余可配置逻辑块 (CLB) 选项	✓	✓	✓	✓	✓	✓	不适用
软件	STL（软件测试库）：C28x CPU 的永久性故障覆盖率超过 60%	不适用	✓	不适用	即将推出	不适用	不适用	✓
	STL（软件测试库）：CLA 的永久性故障覆盖率达到 60%	✓	✓	✓	即将推出	✓	不适用	不适用
	功能安全质量 (FSQ) 闪存 API	X	✓	X	✓	✓	不适用	✓
文档	安全手册：详细的产品概述、功能和限制、TI 开发流程、安全元素和安全诊断。	SFFS022	SFFS700	SPRUI78	Beta	SFFS277	SPRUIT5	SFFS222
	器件认证	SSZQQM2	SFFS901	SWAQ009	即将推出	SFFS610	**不适用**	SFFS748

安全配套资料	
开发流程证书 硬件 | 软件	QRAS-AP00210 的 TUV-SUD 证书。适用于符合 IEC 61508-2 和 ISO 26262-5 标准元件的功能安全开发流程
C2000 安全包* *未公开提供的配套资料。 请联系您当地的 TI 代表申请获取。	应要求提供并需要签订保密协议。安全包具有以下内容： **适用于汽车和工业 MCU 的 C2000 安全包** • **关于随机硬件功能的技术报告** • **关于系统功能的技术报告** • **FMEDA**：失效模式、影响和诊断分析 (FMEDA) 用于在开发阶段提供对不同失效模式、失效模式相关影响、诊断以及任何实施的诊断/安全机制对诊断覆盖率的影响的详细分析。由五部分组成的 FMEDA 培训视频系列。 • **器件概念评估** • **SAR（安全分析报告）**：包含根据目标功能安全标准进行安全分析的结果。 **特定于器件的自检库包** • **C28x_STL（C28x 自检库）**：C28x CPU 软件测试库 • **CLA_STL（CLA 自检库）**：CLA 软件测试库
软件诊断库	演示安全特性和机制的模块和示例库。CPU、存储器、时钟/看门狗、HWBIST 等。 通过此库为 F2837x/07x 提供支持。 通过 C2000Ware 中发布的库为所有其他 F28x 系列提供支持。
功能安全闪存 API	库在 C2000Ware 中提供。如需进一步了解合规性支持包产品/服务，请联系当地的 TI 代表。
编译器鉴定套件	将客户用例的编译器覆盖率与 TI 编译器版本验证的覆盖率进行比较
已获得安全认证的 RTOS (SafeRTOS)	预先认证的安全实时操作系统 (RTOS)
MathWorks 仿真和代码生成	IEC 认证套件可帮助您鉴定 MathWorks 代码生成和验证工具，从而简化嵌入式系统的认证

机械应用中常见的**工业安全架构**通常需要双通道安全方法（硬件故障容错 = 1）。C2000 器件具有独特的功能和可扩展性，可针对 SIL-2（或 cat 3 PL d）和 SIL-3（或 cat 3 或 cat 4 PL e）系统实现两种不同的架构：即在单个器件中，两个安全通道各使用一个 C2000 MCU（图 1），或一个 C2000 MCU 用于一个安全通道，一个 C2000 MCU 用于另一个安全通道，同时兼具控制器功能负责系统的控制逻辑（图 2）。

但是，对于移动机器人等多种工业应用，**单**通道架构可用于满足安全要求（硬件故障容错 = 0）。C2000 器件与外部测试设备一起可实现出色的架构，从而实现所需的 SIL-2（或 cat 2 PL d）等级；C2000 MCU 可用作电机控制器和测试设备以及用于诊断，还可使用带有诊断功能的外部电源来诊断和确保 C2000 MCU 的正常运行（图 3）。 详细了解简化机器人电机驱动安全评估。

此外，与用于安全功能的通用 MCU 相比，C2000 器件具有更出色的计算性能和器件功能，可用于实现复杂的安全运动功能，而不仅仅是需要实时监控 SLS（安全限速）、安全制动控制 (SBC)、安全方向 (SDI)、安全速度监控 (SSM) 等参数和快速启动安全状态的安全扭矩关闭 (STO)。

有关更多详细信息，包括有关这些概念和架构的 TUV 报告，请查阅 C2000 安全包，需遵守保密协议。

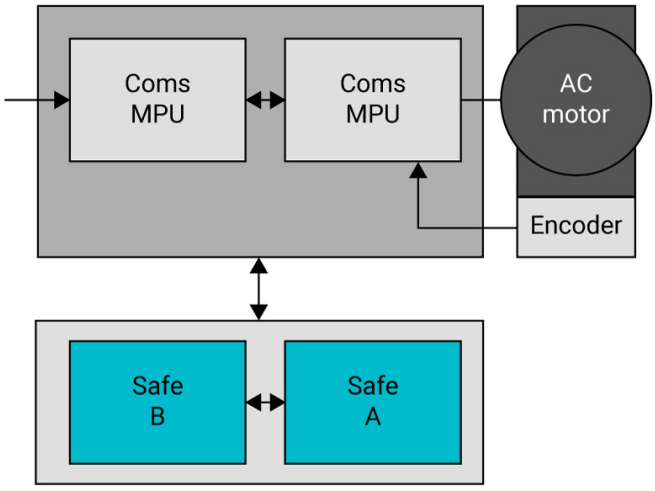

图 1：架构 1，具有双安全 MCU（HFT=1，SIL 2 或 SIL 3）

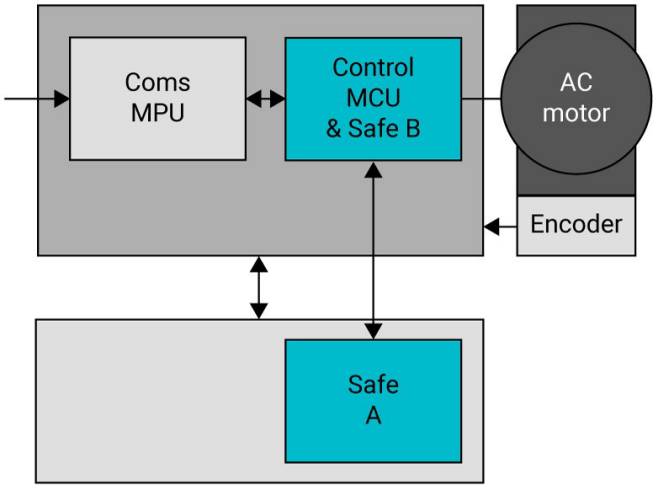

图 2：架构 2，具有单个安全 MCU 和集成到驱动 MCU 中的安全功能（HFT=1，SIL 2 或 SIL 3）

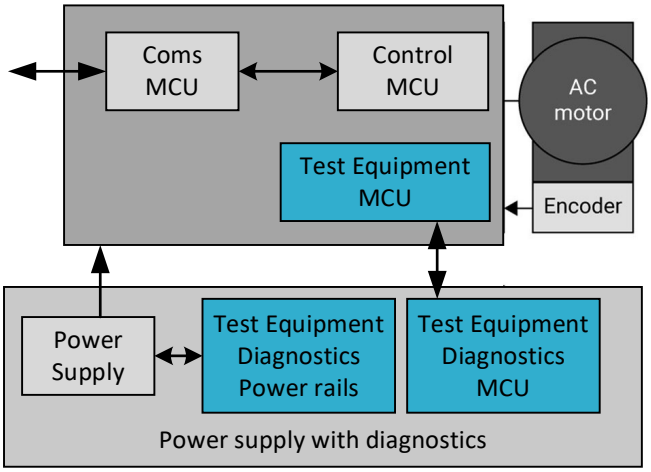

图 3：架构 3，具有单个安全 MCU 和 PMIC（HFT=0，SIL 2）

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