C2000™ 实时微控制器的汽车功能安全

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 ISO 26262 认证流程。我们的 C2000™ 实时 MCU 经过 TÜV SÜD 独立评估和认证，系统功能高达 ASIL D 等级，可帮助您打造需要确保功能安全的汽车应用。C2000 实时 MCU 还有助于实现工业功能安全。

C2000 功能安全产品的亮点是：

- 器件架构针对功能安全进行了调整
- 文档支持使得客户可轻松在系统级别进行安全评估
- 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进而帮助将系统置于安全状态，在系统的整体安全性中发挥着关键作用。凭借 TÜV SÜD 定义并独立评估有效性的 300 多种内置多种安全机制，C2000 MCU 提供所需的诊断覆盖范围，以满足元件级 ASIL B 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，以及实现元件之间不干扰和避免相关故障的技术，以帮助客户开发符合高达 ASIL D 等级要求的合规系统。可调的 FMEDA 提供了更高的灵活性，支持使用封装 FIT 估算、产品功能定制、安全机制定制和定制诊断等功能来定制和计算硬件指标，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 的主要安全特性

主要安全特性		F2838x	F2837x F2807x	F28004x	F28003x	F28002x	F280015x	F28P65x
硬件	符合 ASIL D 标准的开发流程	✓	✓	✓	✓	✓	✓	✓
	随机硬件功能	ASIL B	ASIL B	ASIL B	ASIL B	QM	ASIL B	ASIL B
	系统功能	ASIL D	ASIL D	ASIL D	ASIL D	ASIL D	ASIL D	ASIL D
	CPU 的单点故障覆盖 (SPFM)	相互比较	相互比较	相互比较	相互比较	不适用	锁步 C28x	相互比较 (CPU1 + CLA) 锁步 C28x (CPU2)
	存储器奇偶校验	✓	✓	✓	X	X	✓	✓
	存储器 ECC	✓	✓	✓	✓	✓	✓	仅闪存 ECC
	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	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	✓	不适用	不适用	✓	即将推出
	STL（软件测试库）：CLA 的永久性故障覆盖率达到 60%	✓	✓	✓	✓	不适用	不适用	即将推出
	功能安全质量 (FSQ) 闪存 API	X	X	X	✓	不适用	✓	即将推出
文档	安全手册：详细的产品概述、功能和限制、TI 开发流程、安全元件和安全诊断。	SFFS022	SPRUI78	SPRUID8	SFFS277	SPRUIT5	SFFS222	提供 Beta 版本 - 请联系 TI
	器件认证	SSZQQM2	SWAQ009	SPRQ004	SFFS610	不适用	SFFS748	即将推出

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 标准的硬件组件的功能安全开发流程
C2000 安全包*	应要求提供并需要签订保密协议。该包具有以下内容： • **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。
软件诊断库	演示安全特性和机制的模块和示例库。示例包括 CPU、存储器、时钟/看门狗、HWBIST 等。 通过此库支持 F2837x/07x。 通过 C2000Ware 中发布的库支持所有其他 F28x 系列。
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。
C28x CPU 自检库 (C28x-STL)*	用于针对 C28x 逻辑完整性执行启动的库
CLA 协处理器自检库*	用于针对 CLA 逻辑完整性执行启动和定期测试的库
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

*未公开提供的配套资料。请联系您当地的 TI 代表以申请这些配套资料。

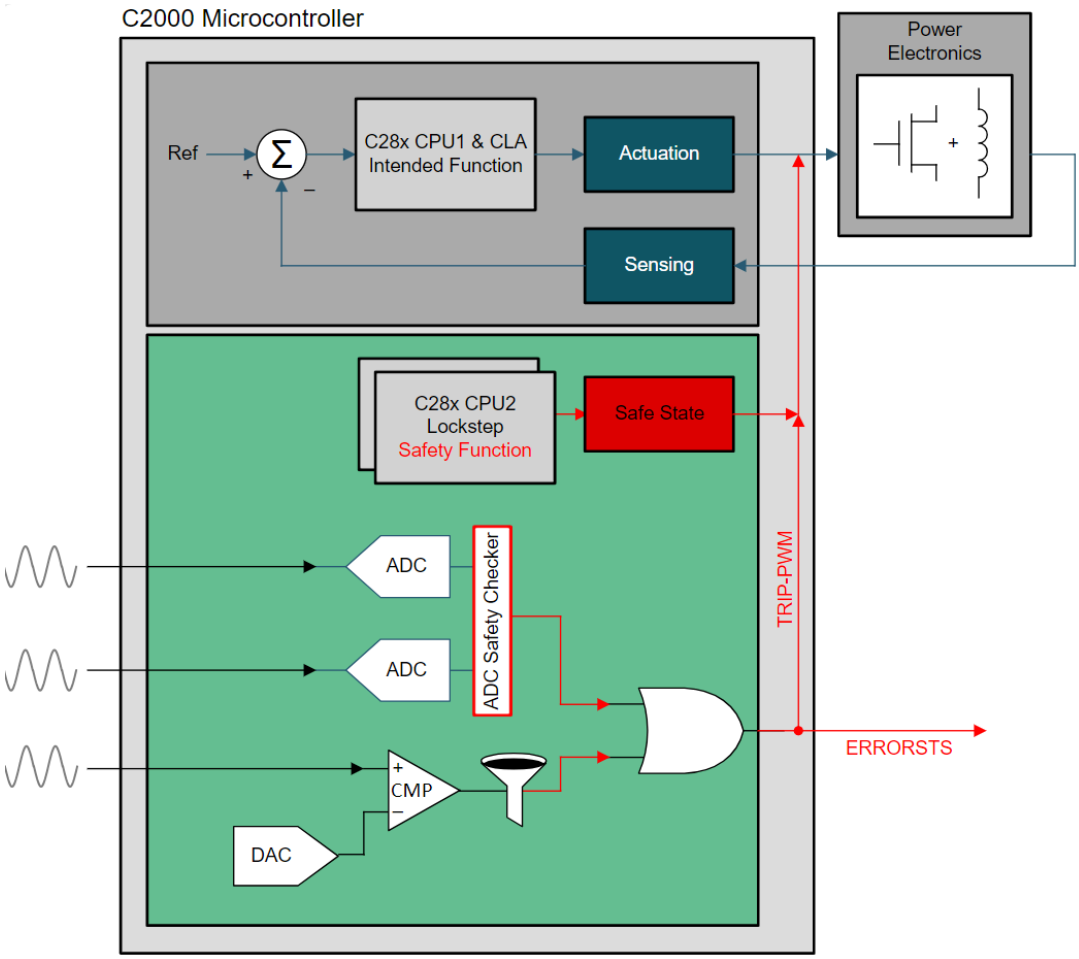

图 1.汽车功能安全应用示例：采用 F28P65x-Q1 的车载充电器 (OBC)。

- 预期功能：可在 C28x CPU1 和 CLA 上实现。
  - 在上面的示例中：车载充电器 (OBC) 数字电源控制的控制功能
- 安全功能：使用 C28x CPU2 和 ADC、CMPSS、SDFM 次级滤波器、CLB 等其他硬件模块实现。
  - 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、**使用锁步比较模块 (LCM) 的硬件冗余**、**使用 ADC 安全校验器的硬件冗余**、**静态配置寄存器的定期软件读回**等来满足。
- 诊断功能：使用 C28x CPU 和 LCM、ADC、CMPSS、SDFM 次级滤波器、CLB 等其他硬件模块实现
  - LFM 可通过 **CPU 的软件测试**、**LCM 的自检逻辑**、**功能软件测试（包括误差测试）**等来满足。
- 有关上述安全机制的更多详细信息，请参阅 F28P65x 安全手册。

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