C2000™ 实时 MCU 安全机制

TEXAS INSTRUMENTS

简介

根据国际电工委员会 (IEC) 的定义，安全是指不存在因财产或环境损害而直接或间接导致人身伤害或健康损害的不可接受的风险。IEC 将功能安全定义为整体安全的一部分，这取决于系统或设备能否对其输入做出正确的响应。

近年来，对于功能安全的重视程度显著提高。因此，开发能够在发生危险故障时确保安全运行的功能安全合规系统已成为各企业和工程师的首要任务。此类功能安全合规系统可以检测潜在的危险故障情况，并部署适当的安全状态以使系统进入已定义的安全状态。

C2000™ SafeTI™ 产品提供了 300 多种安全机制，可用于开发功能安全合规系统，这些系统的最高安全完整性等级可达到国际标准化组织 ISO 26262 所定义的 ASIL D 以及 IEC 61508 标准所定义的 SIL 3。

检测

- **用于检测的冗余外设**
  - 通过让外设的多个实例对相同的输入进行采样并冗余执行相同的操作，然后对输出值进行交叉检查，可以实现在 Σ-Δ 滤波器模块 (SDFM)、模数转换器 (ADC)、增强型捕捉 (eCAP) 和增强型正交编码器脉冲 (EQEP) 等外设上的硬件冗余。
- **ADC 至 DAC 环回检查**
  - 使用 ADC 监控数模转换器 (DAC) 输出，检查 DAC 和 ADC 完整性。在运行时应用此技术可确保从 DAC 驱动适当的电压电平。
- **在线温度监测**
  - 内部温度传感器用于测量器件的结温。ADC 可通过内部连接对传感器输出进行采样，以检测温度变化。
- **ADC PPB（后处理块）**
  - 具有四个 PPB 的每个 ADC 都可以处理 ADC 结果，例如消除偏移和减去参考值。PPB 还可

以标记过零或执行与参考值的高/低比较等等。PPB 的输出可以中断 CPU 或独立于 CPU 生成直接触发以进入安全状态。

- **ADC 结果硬件比较**
  - ADC 结果安全校验器功能可自动比较两个 ADC 转换结果并使用可编程的容差检查它们之间的完整性。这使得不需要在软件中进行结果比较，为每次转换实施 ADC 硬件冗余节省了宝贵的 CPU 周期。
- **具有数字滤波器的 CMP 子系统**
  - 比较器子系统 (CMPSS) 由模拟比较器组成，这些模拟比较器具有用于基准的内置 DAC 和可用于实现电压监测等安全功能的支持电路。针对 CMPSS 输出事件的可配置数字滤波器可以消除报告虚假事件的可能。CMP 模块可以生成 CPU 中断或独立于 CPU 使用 XBAR 架构触发安全状态。

处理

- **“双核锁步”和“与异构处理单元的相互比较”**
  - C28x CPU 内核的双核锁步配置以及锁步比较器模块 (LCM) 根据硬件中的 1oo1D 安全架构实现硬件冗余，以在安全功能运行期间检测 CPU 内部的故障。
  - 通过软件对 C28x 中央处理单元 (CPU) 与控制律加速器 (CLA) 进行相互比较是一种替代 1oo1D 架构，为处理单元提供高诊断覆盖率（根据 ISO 26262-5 的表 D.4）。
  - 交叉检查使硬件和软件具有多样性，因为 C28x CPU 和 CLA 是具有不同的指令集架构 (ISA) 和完全正交工具链的不同处理单元。通过在两个内核中执行算法，可以进一步增加多样性。
- **硬件 BIST**
  - 硬件内置自检 (BIST) 在启动和应用期间对 C28x CPU 提供了高诊断覆盖率。
  - 提供了运行所有测试或根据为硬件 BIST 诊断分配的执行时间只运行这些测试的一个子集的选项。
  - 时间分片测试特性使得硬件 BIST 能够被高效用作运行时诊断，与应用程序并行执行测试。
  - 阅读应用报告“C2000 硬件内置自检”。
- **CLA 软件测试**
  - 借助基于软件的自检库 (STL)，可以测试寄存器组、控制单元和数据路径等各种 CLA 块的完整性。
  - 此测试可以在启动（与密钥开/关周期同步）时或按时间分片执行并在系统内运行，以适应过程安全时间 (PST) 或容错时间间隔 (FTTI)。
- **存储器 BIST**
  - 存储器 BIST 能够识别在系统使用期间降级的嵌入式存储器电路。
  - 这个启动测试（与密钥开/关周期同步）能够防止潜在的存储器故障。
  - 阅读应用报告“C2000 CPU 存储器内置自检”。
- **所有 SRAM 和闪存的 ECC/奇偶校验**
  - 单错校正双错检测 (SECDED) 错误校正码 (ECC) 诊断支持片上闪存。
  - 选定的片上静态随机存取存储器 (SRAM) 支持 SECDED ECC 诊断，并为数据和地址提供单独的 ECC 位，同时通过数据和地址的单独奇偶校验位进行奇偶校验诊断。
  - 阅读应用报告“SRAM 中的错误检测”。
  - C2000 MCU 中实现了奇偶校验检测机制，以针对软错误率 (SER) 提供“高”诊断覆盖率 (DC≥99%)。有关此机制的更多详细信息，请与 TI 联系。
- **针对关键控制寄存器的锁定机制**
  - 配置好控制寄存器后，配置关联的锁定寄存器将锁定写入访问。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。
- **CLA ROM 的背景 CRC**
  - 此安全功能会对 CLA 程序只读存储器 (CLAPROMCRC) 空间中的可配置存储器块执行循环冗余校验 (CRC)。
- **ERAD 模块**
  - 嵌入式实时分析和诊断 (ERAD) 模块提供系统分析功能，这些功能通过配置监测 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，可以检测 CPU 和 MCU 上其他逻辑中出现的故障。
- **ePIE 双 SRAM 硬件比较**
  - 增强型外设中断扩展 (ePIE) 模块可将外设中断连接至 C28x CPU。

- PIE SRAM 地址空间被复制，数据被放置在两个存储器中。
- 在写入操作期间，两个 SRAM 同时更新并在读取时比较两个存储器中的值。
- 如果在比较期间出现错误，CPU 将会分支至一个预定义的位置，此位置将具有用于错误管理的中断服务例程 (ISR)。

驱动

- **采用跳变机制的 ePWM 安全状态置位**
  - 增强型脉宽调制器 (ePWM) 安全状态可使用任何通用输入/输出 (GPIO) 引脚置为有效。
  - 可以灵活地映射这些引脚：跳闸区输入引脚和/或跳闸输入映射到跳闸区子模块和数字比较子模块。
  - 可以为每个 PWM 输出独立配置针对输入跳闸事件（高阻抗、强制进入高阻抗状态或强制进入低阻抗状态）的操作。
- **可配置逻辑块 (CLB)**
  - 可配置逻辑块 (CLB) 是一组可配置的块，这些块可以互连以作为独立于 CPU 的安全机制来触发安全状态，从而实现自定义数字逻辑功能。这样一来，就无需在系统中使用自定义逻辑来实现某些功能安全功能。
  - 数字比较子模块会比较 ePWM 模块外部的信号，从而直接生成 PWM 事件/操作，然后馈送到事件触发器、跳闸区和时基子模块。
  - 消隐窗口功能会滤除来自数字比较事件信号的噪声或不需要的脉冲。
- **用于控制和驱动的冗余外设**
  - GPIO、交叉开关 (XBAR)、PWM、OTTO（高分辨率 PWM）、DAC、比较器子系统 (CMPSS) 和发送中断 (XINT) 等外设上的硬件冗余可通过使用多通道并行输出（在其中独立输出传输信息）来实现。故障检测通过内部或外部比较器或输入比较执行，它们会比较独立输入以确保符合定义的容差。

通信

- **具有内置诊断功能的 100Mbps FSI**
  - 在整个隔离栅内高达 100Mbps 的专有快速串行接口 (FSI) 可提供多种内在诊断功能，例如 CRC 组帧检查、ECC 组帧检查、帧超限检测和帧看门狗超时。
- **冗余通信外设**
  - 在信号接收期间，控制器局域网 (CAN)、串行外设接口 (SPI)、串行通信接口 (SCI) 和内部集成电路 (I^2C) 等外设上的硬件冗余可通过以下方式实现：让外设的多个实例接收相同的数据，然后进行比较以确保数据完整性。
- **嵌入式图形发生器 (EPG)**
  - 嵌入式图形发生器 (EPG) 模块是可定制的图形和时钟发生器，适用于测试和应用场景。
  - 片上图形生成功能可用于测试串行通信外设（如 CAN）是否存在错误条件。这可以增强对 CAN 内部安全机制的错误检测功能的信心，并有助于改进潜在故障指标，而无需在系统中注入复杂的错误。

共因故障和从属故障分析 (CCF/DFA)

- **双振荡器和 MCD**
  - 时钟丢失检测 (MCD) 可以检测锁相环 (PLL) 参考时钟的故障。MCD 使用嵌入式 10MHz 内部振荡器 (INTOSC1)。
- **WWD**
  - 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)。
  - 对于 WWD，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。
  - 在检测到故障时，WWD 能够发出热系统复位或 CPU 可屏蔽中断。
- **专用 ERRORSTS 引脚**
  - ERRORSTS 引脚是“始终输出”引脚并保持低电平，直到在芯片内检测到错误。检测到错误时，ERRORSTS 引脚会变为高电平，直到该错误源的相应内部错误状态标志清除。
- **DCSM**
  - 双代码安全模块 (DCSM) 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。
  - 阅读白皮书“实现 EV/HEV 安全功能共存”
- **存储器访问保护机制**
  - 此机制启用或禁用从各个主器件对各个 RAM 块的特定访问（获取、写入）。

- 始终允许从有权访问该 RAM 块的所有主器件进行读取。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。
- 该功能有助于满足无干扰要求。

要深入了解 C2000™ 汽车功能安全产品，请访问 www.ti.com/cn/lit/swab014

要深入了解 C2000™ 工业功能安全产品，请访问 www.ti.com/cn/lit/swab013

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