Application Note

基于 TI MCU/MPU 的工业功能安全 PLC 架构实现

Zekun Bai, Linjun Meng, Donna Xu

摘要

本应用手册介绍如何使用德州仪器 (TI) Sitara 微控制器 (MCU) 和微处理器 (MPU) 来设计符合 IEC 61508 和 ISO 13849-1 标准的功能安全可编程逻辑控制器 (PLC) 系统。本文档介绍了功能安全的基本概念、系统安全目标分解方法、TI 芯片安全架构特性以及推荐的 PLC 系统设计方法。通过模块化设计原理和灵活的冗余架构，设计工程师可以在降低成本和复杂度的同时，满足 SIL 3/CAT 3 级功能安全要求。目标受众包括工业控制系统设计工程师、功能安全架构师和系统集成商

内容

商标

1 功能安全基础

1.1 什么是功能安全

功能安全是指通过正确运行电气、电子或可编程电子安全相关系统来防止或缓解危险事件的能力。在工业应用中，设备和系统在特定的故障条件下可能会产生危险。功能安全的目标是将此类危险事件的发生概率降低到可接受的水平。

1.2 从故障到伤害的因果链

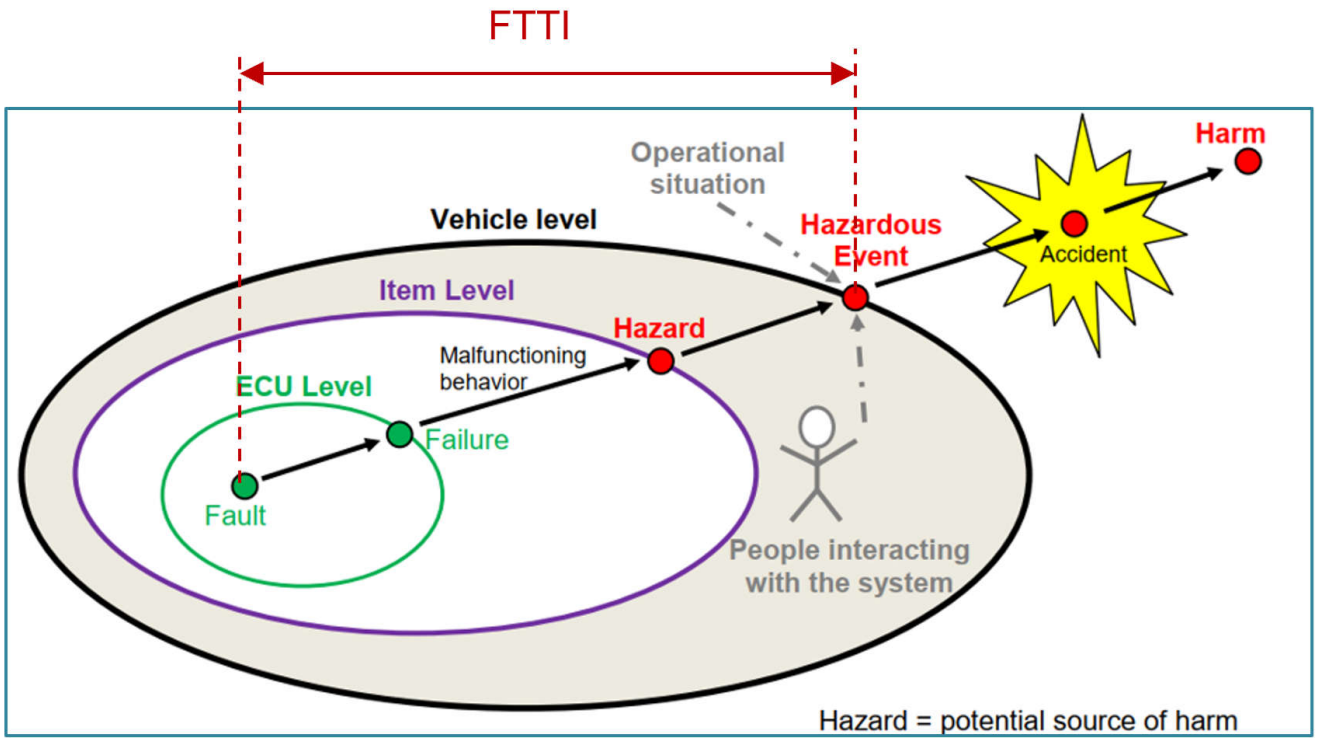

图 1-1. FTTI 可视化

- 1 级：硬件/软件故障 (Fault) → CPU 计算错误、存储器损坏、时序故障等
- 2 级：故障导致失效 (Failure) → 系统功能异常、输出错误、无响应
- 3 级：失效触发危险事件 (Hazardous Event) → 意外设备操作、控制失效、传感器失灵
- 4 级：导致人身伤害的危险事件 (Harm) → 人员受伤、设备损坏、生产停止

根据 IEC 61508 标准定义，从故障到人身伤害的完整过程包括：

Fault → 潜在故障指标

- 系统缺陷，如硬件缺陷、制造工艺偏差、软件缺陷
- 随机失效：由运行应力（温度、电压）和累计使用时间引起
- 系统性失效：由设计不足或工艺不当引起

Failure → 危险失效与安全失效

- 如果未检测到故障或检测到故障的时间过晚，则会导致系统功能丧失
- 危险失效：可能导致安全功能丧失的失效
- 安全失效：导致系统进入安全状态的失效

Hazardous Event → 可预见但无法避免与可预见且可避免

- 失效最终会转化为可能伤害人员或设备的事件
- 示例：机器人意外移动、电梯制动失效、工业设备意外启动

人身伤害 (Harm) → 伤害严重程度的分类

- 如果未及时防止危险事件，将会造成实际伤害

1.3 功能安全解决的核心问题

功能安全设计的目标是在该因果链中建立多条防线：

- **故障检测**：尽快检测是否存在故障
- **故障隔离**：隔离故障影响并防止传播到关键功能
- **安全响应**：当故障导致失效时触发安全功能
- **冗余设计**：单点故障不会导致安全功能丧失
- **可诊断性**：系统能够迅速检测到故障并识别故障

2 安全标准和等级分类

2.1 主要安全标准体系

工业和汽车领域采用不同但相互关联的安全标准。

工业应用基础标准：

- **IEC 61508** - 适用于所有电气/电子/可编程电子安全相关系统的通用安全标准
- **IEC 62061** - 机械安全 - 安全相关电气/电子/可编程控制系统
- **ISO 13849-1** - 机械安全 - 控制系统的安全相关器件（采用性能级别方案）

特定领域的应用标准：

- **IEC 61800-5-2** - 可调速电力驱动系统 - 第 5-2 部分：功能安全要求
- **ISO 10218** - 机器人和机器人器件 - 工业机器人的安全要求
- **IEC 61496** - 机械安全 - 电敏保护设备

工业通信安全标准：

- **IEC 61784-3** - 工业通信网络 - 功能安全
  - 定义 FSoE（以太网功能安全）协议
  - 指定 EtherCAT、PROFINET、EtherNet/IP 和其他协议的安全扩展
  - 定义通信层故障检测与恢复机制
  - 通信故障 PFH 预算通常不超过总系统 PFH 的 1%

汽车应用：

- **ISO 26262** - 道路车辆 - 电气/电子/可编程电子安全相关系统的功能安全

2.2 工业通信中的功能安全 (FSoE)

工业以太网的广泛采用带来了新的挑战：在标准网络上实现确定性和安全性的需求。

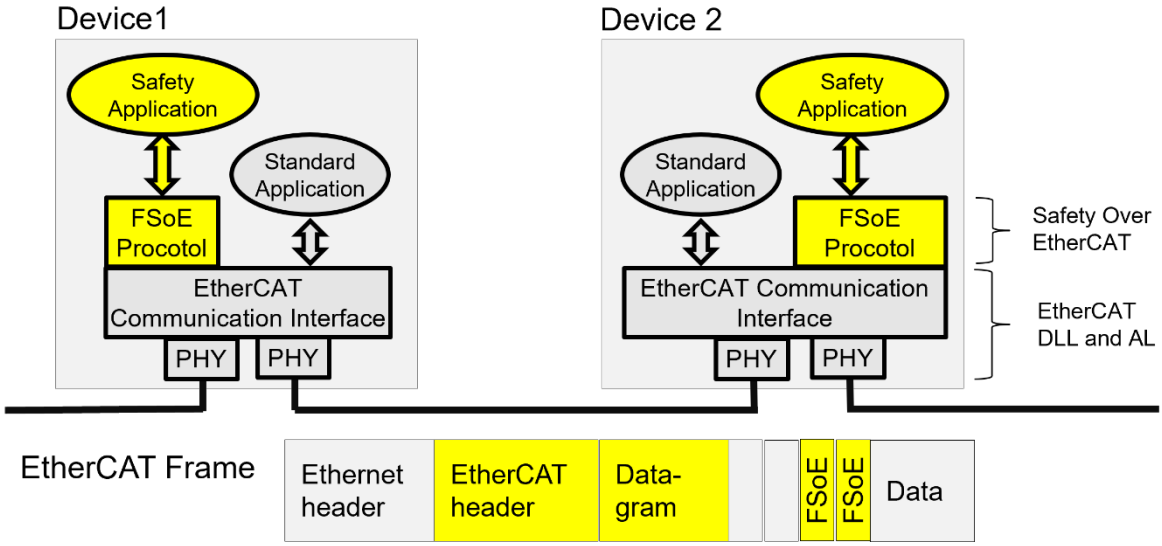

图 2-1. FSoE 协议层次结构

- 应用层：安全相关数据（位置、速度、故障代码等）
- FSoE 协议层：
  - 序列号检测（检测重复、丢失、乱序）
  - CRC 验证（检测数据损坏）
  - 连接 ID（检测错误转发）
  - 看门狗计时器（检测超时延迟）

- 物理层：标准以太网 MAC/PHY

FSoE 不修改底层物理层，它通过应用层协议增强。

图 3 FSoE 与标准 PLC 通信之间的差异

特性	**标准以太网/EtherCAT**	**FSoE 增强**
基本协议	EtherCAT 标准	相同
安全数据	无特殊处理	含 CRC 和序列号
故障检测	数据包丢失检测	完整的 FSoE 诊断
延迟检测	无	看门狗监测
可靠性	中（取决于网络）	高（自动故障转移）
应用复杂度	低	中（协议栈处理）

2.3 安全等级指标系统

2.3.1 IEC 61508 – 安全完整性等级 (SIL)

IEC 61508 根据危险失效概率指标定义了四个安全完整性等级。

图 4 IEC 61508 关键指标

IEC61508						
硬件故障容错						SFF
0	1	2	**0**	1	2	
-	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3	**< 60%**
SIL 1	SIL 2	SIL 3	SIL 2	SIL 3	SIL 4	60% 至 < 90%
SIL 2	SIL 3	SIL 4	SIL 3	SIL 4	SIL 4	90% 至 < 99%
SIL 3	SIL 4	SIL 4	SIL 4	SIL 4	SIL 4	≤ 99%
类型 A			类型 B			

IEC 61508 不需要特定的 HFT，系统可以是 1oo1、1oo2

- A 类子系统：明确定义的失效模式，其中故障条件下的行为已确定，并且有足够的失效数据来声明满足失效率。
- B 类子系统：更复杂的子系统，其中失效模式未完全定义，故障条件无法完全明确定义，并且没有足够的数据来支持满足失效率。

关键指标说明：

- **PFH**（每小时失效概率）：运行 10^9 小时的失效次数（FIT 单位）
- **SFF**（安全失效分数）：非危险失效的比例
- **HFT**（硬件故障容错）：硬件故障容错能力

通信 PFH 预算：根据 IEC 61784-3，通信通道 PFH 不应超过总系统 PFH 的 1%。例如：

- 如果系统目标为 SIL 3 (PFH ≤ 10 FIT)
- 通信允许 PFH ≤ 0.1 FIT（10 FIT 的 1%）
- 这对通信可靠性提出了极高的要求

2.3.2 ISO 13849-1 - 性能级别 (PL) 和类别 (CAT)

ISO 13849-1 使用不同的分级方法，强调架构的抗故障能力。

图 5 性能级别范围 a（最低）至 e（最高）

ISO13849				
DC	类别			
	1	**2**	**3**	**4**
无				
低	c	c	d	
中		d	e	
高				e

ISO13849 类别指定抗故障能力，类似于 HFT（硬件故障容错）。

- Cat1：单通道 + 经过充分验证的元件
- Cat2：单通道 + 测试设备
- Cat3：双通道 + 诊断，无故障累积
- Cat4：双通道 + 诊断，故障累积，对诊断的要求更高

性能级别范围 a（最低）至 e（最高）。主要映射：

- **PL e ≈ SIL 3**：要求 HFT=1 且具有高诊断覆盖率
- **PL d ≈ SIL 2**：要求 HFT=1 且具有中等诊断覆盖率

3 系统安全目标分解

3.1 HARA 流程和安全目标定义

系统安全目标分解从 HARA（危险分析和风险评估）开始

第 1 步：识别所有潜在危险

- 确定系统可能导致的所有非预期事件
- 示例（工业机器人）：机器人意外移动、制动故障、超速
- 示例（PLC 控制系统）：意外输出激活、因通信中断导致的控制故障、传感器读取错误

第 2 步：风险评估与分类

对于工业应用 (IEC 61508)，风险评估基于：

- **后果 (Consequence)**：CA（轻微）→ CB → CC → CD（致命）
- **频率和曝光时间 (Frequency)**：FA（罕见）→ FB（频繁）
- **可避免性（避免的可能性）**：PA（可避免）→ PB（难以避免）

第 3 步：定义安全目标

安全目标应明确阐述：

- 要防止或缓解的危险事件
- 相应的安全完整性等级（SIL 或 ASIL）
- 可接受的故障率 (PFH)
- 诊断覆盖率和故障容错要求

示例：

安全目标 1：“防止意外激活 PLC 控制信号”

- SIL 级别：SIL 2

- PFH 目标：≤100FIT

- 诊断覆盖率：≥90%

- 故障容错要求：HFT=1（单点故障不会导致激活）

安全目标 2：“确保通信通道的可靠性”

- SIL 级别：SIL 2

- PFH 目标：≤1 FIT（通信预算）

- 诊断覆盖率：≥99%（FSoE 机制）

- 故障容错要求：DLR 环形网络冗余

3.2 安全目标分解和 ASIL-SIL 分配

顶级：系统安全目标“PLC 控制系统安全”- SIL 3

二级分解为：

- 子目标 A：“I/O 模块故障不会导致危险输出”- SIL 3
- 子目标 B：“检测并处理通信故障”- SIL 2
- 子目标 C：“处理器故障已隔离”- SIL 2

三级继续分解为具体要求。

ASIL 分解原则 (ISO 26262)

ASIL 分解允许将高级安全目标分配为多个较低级别的子目标。如果满足独立性和多样性要求，该系统仍然可以达到原始 ASIL 级别。

图 6 分解规则：

原始 ASIL	允许的分解组合
ASIL-D	D(D) + QM(D) 或 C(D) + A(D) 或 B(D) + B(D)
ASIL-C	C(C) + QM(C) 或 B(C) + A(C)
ASIL-B	B(B) + QM(B) 或 A(B) + A(B)
ASIL-A	(A) + QM(A)

关键要求：

1. 独立性 (Independence)
   - 分解后的子目标应相互独立
   - 一个子目标失败不应导致另一个子目标失败
   - 示例：使用不同的硬件、不同的电源、不同的时钟
2. 多样性 (Diversity)
   - 采用不同的技术或实现方法
   - 示例：使用不同的处理器供应商、不同的编程语言、不同的算法
3. 可追溯性 (Traceability)
   - 清晰记录分解过程和基础
   - 说明每个子目标如何组合以满足原始目标
   - 维护完整的要求可追溯性矩阵
4. 合理性 (Justification)
   - 需要证明分解后的架构确实达到了原始 ASIL
   - 通常通过故障树分析 (FTA) 或其他定量方法证明

SIL 合成原则 (IEC 61508)

对应于 ASIL 分解，IEC 61508 定义了 SIL 合成方法。SIL 合成本质上允许合成（或组合）两个系统能力为 N 的冗余元素，使其具备 N + 1 的系统能力，前提是 N 小于或等于 SIL 3。根据 IEC 61508，管理 SIL 合成的规则包括：

- SIL 2 + SIL 2 → SIL 3
- SIL 1 + SIL 1 → SIL 2

IEC 61508 不允许递归（多级）合成，但 ISO 26262 允许。例如，SIL 合成

（根据 IEC 61508）不允许以下任一情况：

- SIL 2（支持 SIL 3）+[SIL 1（支持 SIL 2）+ SIL 1（支持 SIL 2）] → SIL 3。
- SIL 2（支持 SIL 3）+ SIL 1（支持 SIL 3）→ SIL 3。

相比之下，ISO 26262 允许多级分解。

IEC 61508 还强制要求 SIL 4 系统必须采用双通道实现（对于 SIL 4 功能，

硬件故障容错必须大于 0）。除此之外，ASIL 分解和 SIL 合成在

ISO 26262 和 IEC 61508 标准中分别是等效的概念。

3.3 系统级分解的具体应用

示例：工业 PLC 系统的 SIL 3 分解

系统级安全目标：SIL 3。分解为三个子系统：

子系统 1 – I/O 故障隔离 (SIL 2)

- 数字输入故障检测
- 数字输出故障检测
- 发生故障时切断输出

- 诊断覆盖率：≥90%

子系统 2 – 双 MCU 故障检测 (SIL 2)

- 看门狗超时检测
- 存储器 ECC 校验
- 内部诊断自检
- 诊断覆盖率：≥90%

子系统 3 — 通信安全 (SIL 2)

- FSoE 协议故障检测
- 网络环冗余 (DLR)
- 消息验证和超时
- 诊断覆盖率：≥99%

组合策略：

- 通过独立的硬件和检测机制实现三个 SIL 2 子系统
- 系统级诊断覆盖率超过 99%
- 单点故障不会导致安全功能丧失 (HFT≥1)
- 结果：整个系统达到 SIL 3 标准

3.4 角色与职责划分

在功能安全项目中，各方之间明确的角色划分至关重要：

客户/系统集成商职责：

- 执行 HARA 并定义系统级安全目标
- 制定安全概念并将安全目标分解为子系统
- 选择合适的 TI 元件
- 开发安全相关软件
- 执行系统级验证和测试
- 准备安全案例文档

TI 职责：

- 使用经认证的开发流程开发功能安全 MCU/MPU
- 提供元件级安全分析 (FMEDA)
- 提供安全手册和诊断库 (SDL)
- 作为 SEooC（独立安全元素）
- 不负责系统集成、应用软件开发和系统评估

独立评估机构（例如 TÜV SÜD）职责：

- 独立评估和认证 TI 元件
- 审核客户系统安全案例
- 颁发功能安全认证证书

4 TI 芯片安全架构

4.1 MCU 级安全架构

下面展示了 TI 功能安全 MCU 架构中的三种常见架构。

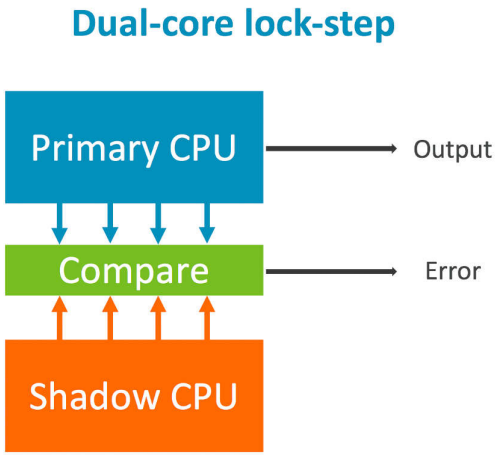

图 4-1. 双核锁步

双核锁步 (DCLS)：两个完全相同的 CPU 内核并行运行，硬件比较器检测不匹配情况，一旦检测到立即中断。

特性：

- 两个 CPU 内核以同步时序执行完全相同的指令
- 硬件比较器持续比较计算结果
- 任何不匹配情况都会立即触发错误处理和系统停止
- 故障检测延时：一个周期（最小值）

优势：

- 低成本、单芯片实现
- 极快的故障检测
- 架构简单

劣势：

- 无法检测共因失效（例如，共享时钟故障）
- 无故障容错，仅具备检测能力
- 如果一个内核出现故障，整个系统将停止

应用：SIL 2 HFT=0 系统

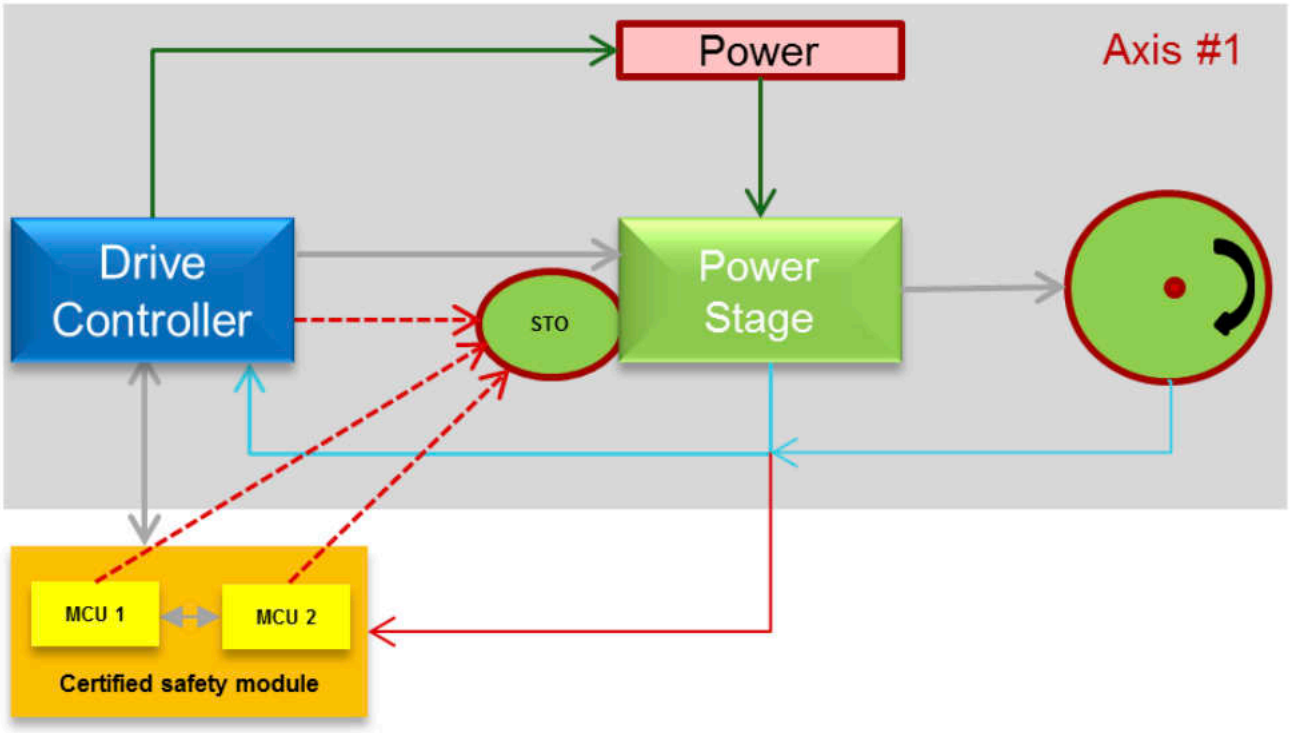

图 4-2. 同构冗余

同构冗余 (HFT=1)：两个完全相同的 MCU 执行独立的任务，通过 SPI/I2C 进行交叉校验，从而消除共因失效 (CCF)。

特性：

- 两个完全相同的 MCU 独立运行并行任务
- 通过 I2C、SPI 或其他隔离式接口进行交叉验证
- 定期比较结果，出现差异会触发安全措施
- 故障检测延时：10-100ms（可配置）

优势：

- 可通过独立设计检测大多数共因失效：
- 硬件故障容错：单个 MCU 失效后，系统仍继续运行
- 两个内核均可独立监测和管理
- 支持复杂的安全逻辑

劣势：

- 需要两个 MCU，成本增加
- 交叉校验通信会增加延时
- 集成更复杂

应用：SIL 3 HFT=1 系统

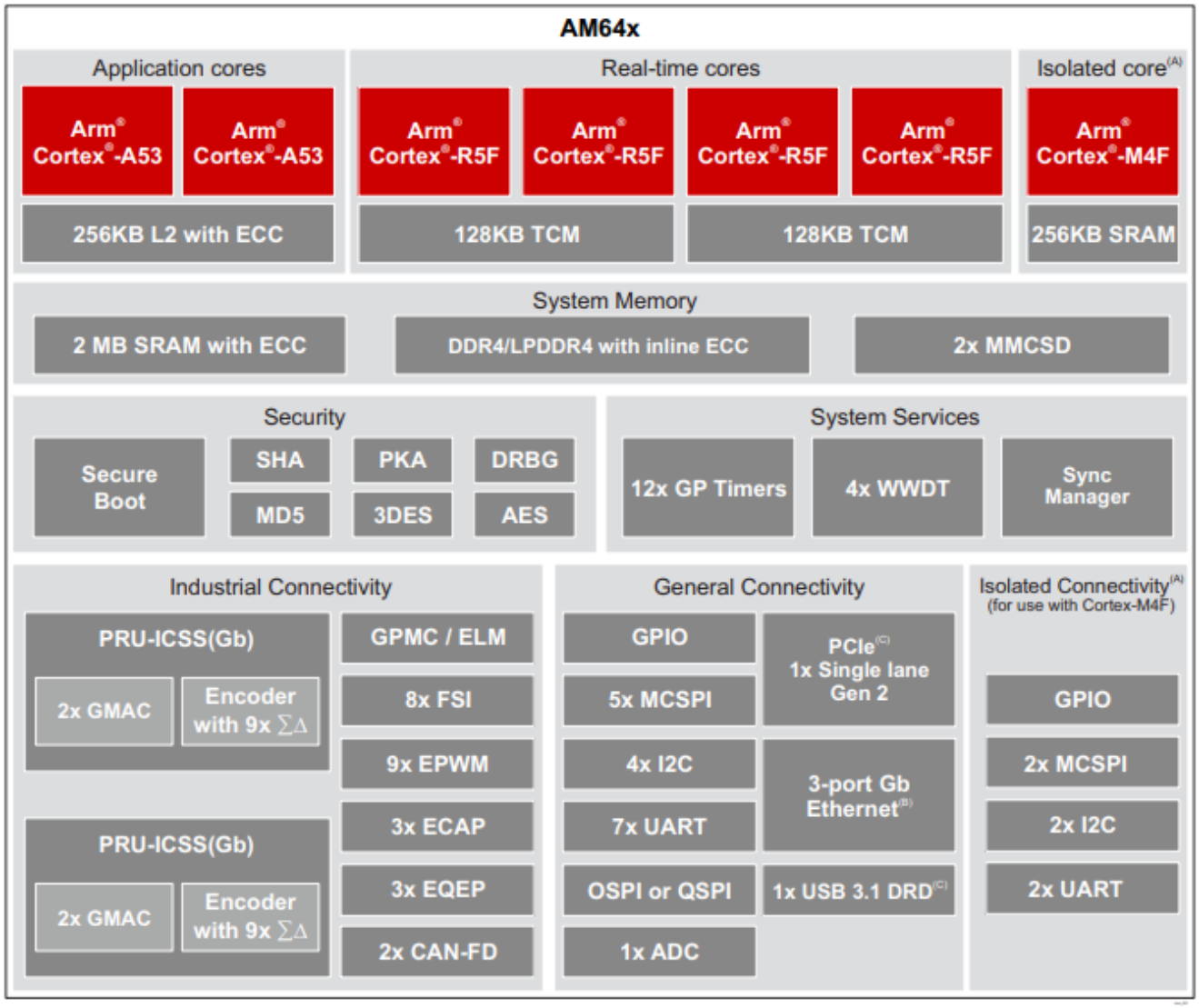

图 4-3. AM64 一页

异构冗余 (HFT=0)：采用不同的 MCU 类型或多样化的软件实现，从而检测系统级失效。

特性：

- 采用 MCU + MPU 组合的处理器架构。
- 根据不同的内核、不同的 SIL 要求实现不同的软件方案。使用高 SIL 内核监测低 SIL 内核任务。
- 内核之间实现硬件隔离，包括外设、电源、存储器。

优势：

- 能够检测某些系统级设计缺陷
- 最大的冗余和故障容错
- 在所有方法中成本较低

劣势：

- 开发复杂度高
- 需要多个平台的深厚专业知识

应用：SIL 2/3 或特殊 ASIL-D 要求

4.2 TI MCU/MPU 中的集成安全机制/技术

TI 为每款功能安全 MCU/MPU 提供经过认证的软件诊断库 (SDL)。

SDL 库典型内容：

- CPU 内核与总线诊断例程
- 存储器测试算法
- 外设内置自检 (P-BIST)
- 逻辑内置自检 (L-BIST)
- 时钟、电压、温度监测
- 中断与异常处理

TÜV 认证说明：SDL 已由评估机构（如 TÜV SÜD）独立评估，能够满足特定的 SIL/ASIL 等级要求。

此外，TI MCU/MPU 还可实现硬件 SIL2 和系统 SIL3 能力，其中集成了如下多项安全措施。

4.2.1 免于扰 (FFI) 设计

FFI 是在单个 SoC 上运行不同安全级别任务时的关键技术。它可以消除

不同 ASIL/SIL 级别元件之间的级联故障和依赖关系，并确保低级别元件故障不会传播到高级别安全岛。

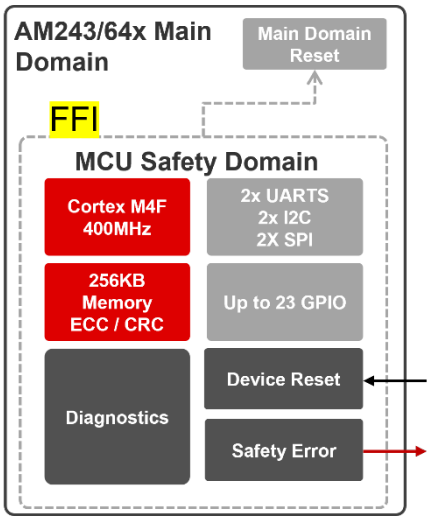

图 4-4. TI MCU/MPU 中的 FFI 实现

FFI 外部侧：非安全域 - 标准应用、通信、非关键任务

FFI 内部侧：安全岛 - 安全关键型任务、独立的 R5F 或 M4F 内核

FFI 隔离机制：

- 防火墙 (Firewall) - 控制总线访问
- 超时 Gasket (Timeout Gasket) - 保护通信路径
- 独立时钟/电源/复位
- 专用中断控制

双向箭头：用于必要通信的受控接口 (SPI/I2C)

状态指示器：安全岛可以独立监测和重新启动非安全域。

FFI 优势

- **成本优化**：在单个 MCU 中集成多个安全级别的功能，从而降低总 BOM
- **集成级别**：无需单独的外部安全 MCU
- **系统复杂度**：降低集成难度并减少测试工作量

4.2.2 存储器保护和 ECC 技术

MCU/MPU 中的数据路径：原始数据 → ECC 编码 → 存储 → ECC 验证 → 纠正/检测

ECC 是保护存储器免受随机故障影响的核心技术。

- 单比特错误 (SBE) 检测与纠正过程
- 多比特错误 (DBE) 检测过程
- 汉明码或 SECDED 码奇偶校验位生成。

以 AM243 /AM64 为例，请参阅下面的 ECC 覆盖范围。

图 11 关键存储器中的 ECC 覆盖范围

内存类型	ECC 类型	范围	注释
L1 I-Cache	奇偶校验	A53 内核	仅检测
L1 D-Cache	ECC SECDED	A53 内核	支持单比特纠正
L2 高速缓存	ECC SECDED	共享 512KB	支持单比特纠正
R5F SRAM	ECC SECDED	每个内核 64KB	覆盖所有 R5F 存储器
MCUSS SRAM	ECC SECDED	512KB 共享	安全岛存储器
DDR EMIF	ECC 可选	主存储器	客户可配置

4.2.3 其他集成安全机制

图 12 TI MCU/MPU 中的其他机制

安全机制	说明	检测到的内容	覆盖率
ECC/EDAC	检错与纠错	存储器中的单比特翻转	高
存储器保护单元 (MPU)	防止未经授权的访问	栈溢出、缓冲区溢出、非法访问	中
看门狗 (WD)	处理器挂起检测	CPU 死循环、系统卡住	高
双时钟比较器 (DCC)	时钟异常检测	时钟频率偏差	高
错误信令模块 (ESM)	集中式故障管理	路由所有诊断故障和响应	非常高
上电复位 (POR/BOR)	电源监测	异常电压条件	中

5 功能安全 PLC 架构设计

5.1 功能安全 PLC 的必要性和应用场景

为什么需要功能安全 PLC

现代工业自动化面临诸多挑战：

1.法规安全要求日益严格

- EU 机械指令强制要求功能安全
- ISO 10218（机器人）要求达到 PL d / SIL 2
- IEC 61800-5-2（变速驱动器）要求进行 SIL 评估

不符合要求的产品无法进入市场

2.人机协作成为趋势

- 协作机器人与人类共存
- 任何故障都可能导致人身伤害
- 传统 PLC 无法提供充分的安全保护

3.系统复杂度增加

- 多个独立的子系统需要协调
- 通信故障可能会导致级联故障
- 需要可靠的故障检测与恢复机制

4.可用性和可维护性要求

- 停产成本高昂（每分钟数万）
- 需要快速故障检测和自动恢复
- 需要详细的诊断信息

5.2 功能安全 PLC 架构设计

功能安全 PLC 的关键概念包括分层、隔离和冗余。

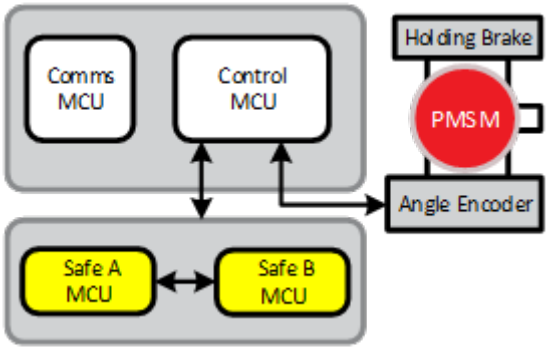

图 5-1. 独立安全 MCU 及标准 MCU 系统概念

控制处理器（中央处理器）

- 高性能 MPU（例如 AM64x 或 AM243x）
- 运行 PLC 扫描周期和用户逻辑
- 处理多种工业通信协议

安全子系统 (Safety Subsystem)

- 两个独立的安全 MCU（AM243x 或 C2000）
- 各自具有单独的 SRAM、ROM 和外设
- 通过 SPI 接口进行交叉校验
- 输出：故障诊断、状态报告

- 隔离式继电器驱动器或直接 GPIO 控制

通信冗余管理（DLR/环形网络）

- AM243x/AM64x 内置 DLR 监控管理器
- 维护两条独立的通信路径
- PRU_ICSSG 执行快速故障检测和传输
- 基于以太网交换机的冗余
- 在工业以太网链路层处理

I/O 模块

- 模块化设计
- 支持各种 I/O 类型 (DI/DO/AI/AO)
- 可选故障检测（高端模块）

5.3 设计实现案例

AM64/AM243 可支持硬件 SIL2、系统 SIL3。请参阅 AM243/AM64 数据表中的详细信息。AM64 和 AM243 为引脚对引脚兼容。

更重要的是，AM64/AM243 集成了两个 PRU_ICSSG 子系统，可通过将不同的固件加载到 PRU_ICSSG 中来实现行业实时通信。

每个 PRU_ICSSG 包括：

- 两个 PRU 内核（可编程逻辑）
- 千兆位以太网 MAC (RGMII/SGMII)
- 实时数据缓冲器 (DPRAM)

下面显示使用两个 AM243 作为 FuSa MCU 模块，并使用另外一个 AM243 作为通信模块。结合上一章中的系统概念，提供 TI FuSa PLC 解决方案。

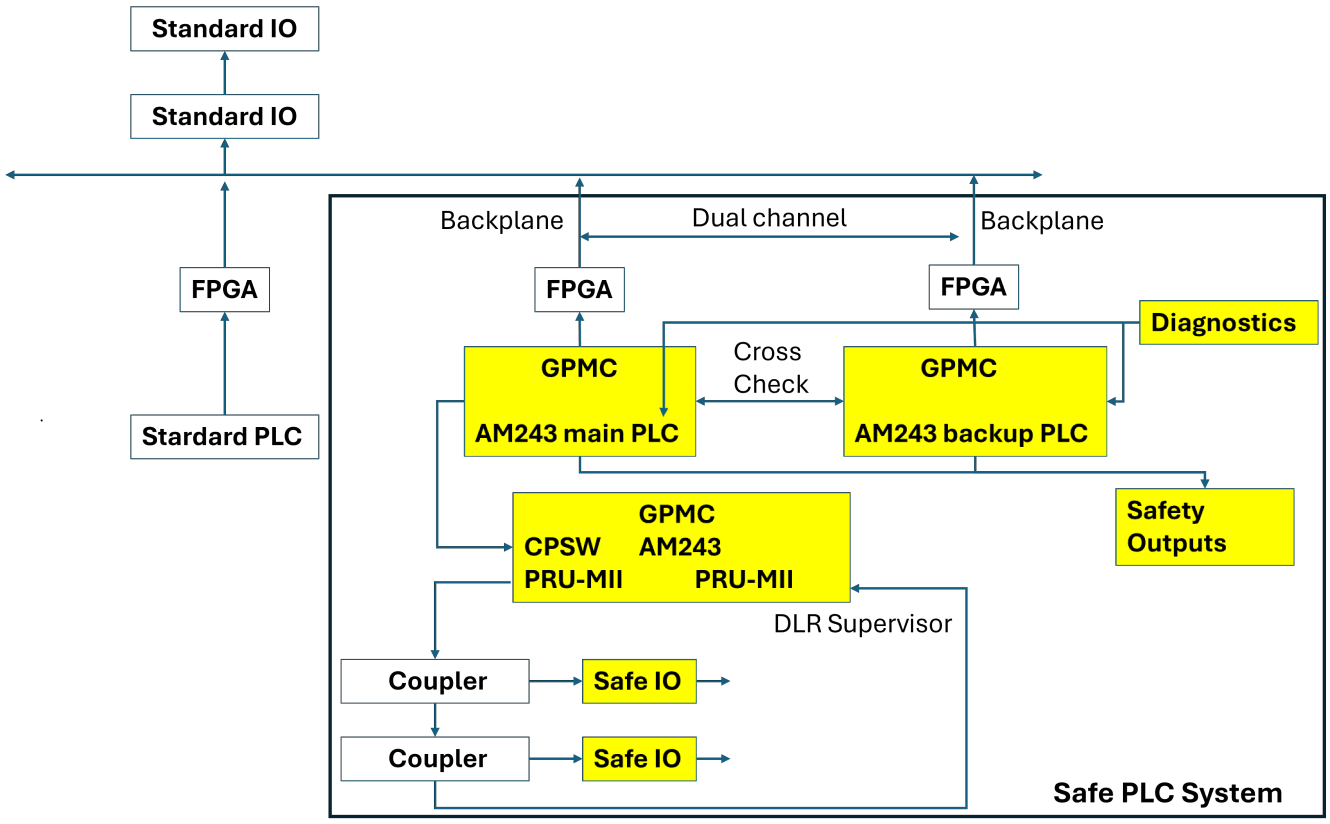

图 5-2. 功能安全 PLC 架构示例

通过与标准 PLC 结合，两个 AM243 用作 FuSa PLC 系统，以实现 SIL3，HFT = 1，CAT 3。使用 SPI 或 I2C 在两个 AM243 之间实现交叉校验。

再使用一个运行的 AM243 作为通信模块来管理通信，并运行与外部耦合器连接的 DLR 监控器，以扩展安全 IO 数量。

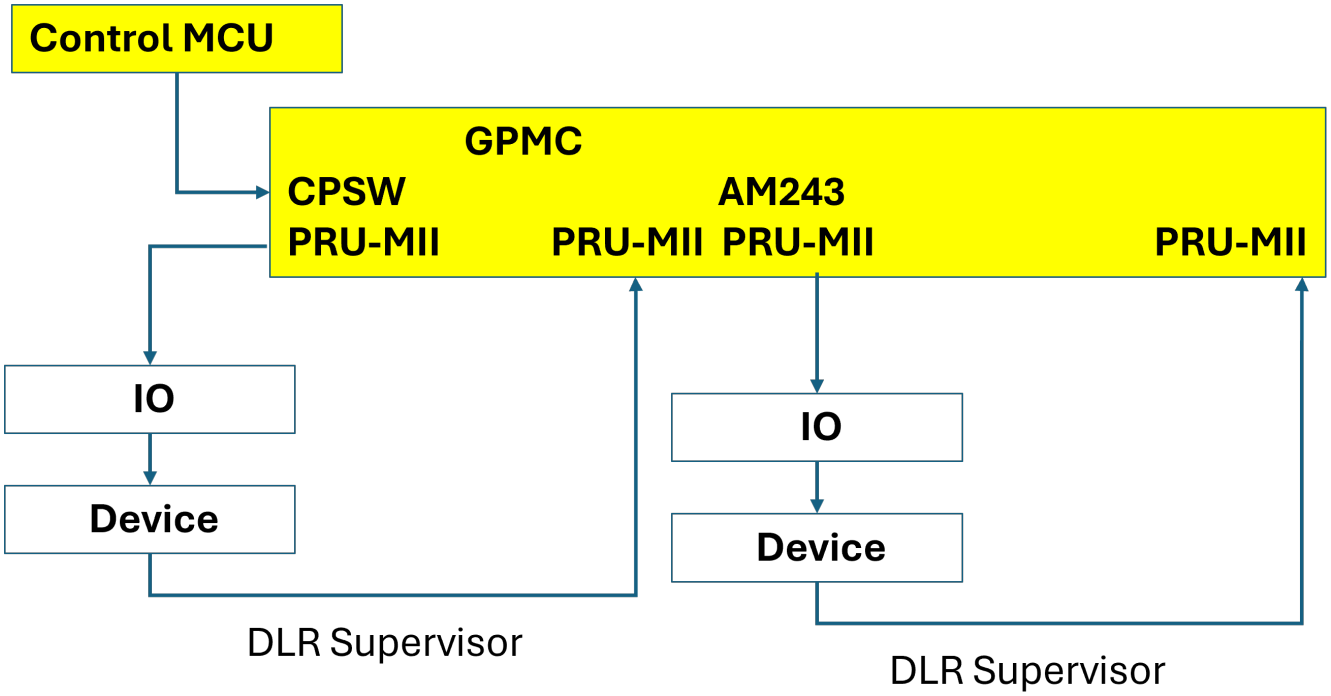

图 5-3. 冗余通信模块示例

AM243 集成了两个 PRU_ICSSG 子系统，可支持最多五个 MAC 端口：PRU_ICSSG 中四个 MAC 端口，CPSW 中一个 MAC 端口。

- 一个 PRU_ICSSG 支持两个 MAC 端口，DLR 监控器在一个 R5F 内核上运行。
- 另一个 PRU_ICSSG 支持两个 MAC 端口，DLR 监控器在一个 R5F 内核上运行。
- CPSW 中有一个 MAC，通过控制 MCU 连接。

关键架构特性

通用硬件接口：

- 所有系列的背板协议完全相同
- I/O 模块外形标准化
- 电源连接器标准化
- 允许混搭不同的模块

优势：

- 客户无需学习多个系统
- 升级成本极低（主要是 CPU 卡）
- 库存管理简单

实现的优势

1.成本优化

- 使用统一的处理器平台
- 共享底层驱动程序和工具链
- 不同的客户需求对应不同的价格点

2.快速产品上市

- 重复使用元件和设计
- 缩短每个新产品的开发周期
- 加快功能安全认证（参考设计已预认证）

3.可维护性

- 统一的代码库和文档
- 更易于技术支持和更新
- 一致的用户培训内容

4.市场覆盖范围

- 小型器件采用低端配置
- 中等器件采用中端配置
- 大型和高风险应用采用高端配置
- 单一产品线覆盖整个市场

5.未来升级能力

- 工业标准演进（新协议支持）时
- 客户可以通过固件升级获得新功能
- 无需更换硬件

5.4 TI 功能安全设计资源

系统级支持

- 参考设计
  - 安全转矩关闭 (STO) 参考设计
  - 安全 I/O 模块参考设计
  - DLR 冗余管理参考设计
  - 经 TÜV 预评估和认证

元件级资源

- 功能安全手册（安全手册）
- FMEDA 分析报告
- 诊断功能检查清单
- 应用手册

软件支持

- 软件诊断库 (SDL)
- 预认证源代码（经 TÜV 批准）
- 完整的 API 文档
- 示例代码和集成指南

工具链支持

- SDK（软件开发套件）
  - 包括 RTOS、驱动程序、协议栈
- SafeTI 编译器资质审核套件
  - 符合 ISO 26262/IEC 61508 编译器验证要求
- 调试工具
- 代码分析工具

文档和指导

- 白皮书和应用手册
- 功能安全最佳实践
- 标准映射指南

- 架构设计指南

6 总结

本应用手册为使用德州仪器 (TI) 微控制器和微处理器设计符合功能安全标准 IEC 61508 和 ISO 13849-1 的工业可编程逻辑控制器 (PLC) 提供了实用指导。它涵盖了从基本概念到实现和实际案例研究的整个安全系统生命周期。

客户价值

对于系统集成商：

- 通过预认证的参考设计，将开发时间缩短 40-60%
- 使用成熟的架构，显著缩短认证周期
- 通过重复使用元件，降低总拥有成本

对于设备制造商：

- 提供明确的路径以符合 ISO 10218（机器人）、IEC 61800-5-2（驱动器）和领域标准
- 全面的故障检测和冗余降低了责任风险
- 灵活的架构支持从简单到复杂的应用

对于最终用户：

- 系统通过适当的冗余实现 99.5% 以上的可用性
- 全面诊断，支持预测性维护
- 具有前瞻性的设计，可通过固件更改升级

重要洞察

架构选择：

- 简单的安全应用使用单个安全 MCU；复杂的系统使用分层 MCU+MPU 方法；网络关键型应用增加 DLR 冗余。

诊断策略：

- 与其实现所有诊断，不如战略性地选择 ECC、看门狗、FSoE 和定期自检，以经济高效地实现目标 SIL/ASIL。

通信可靠性：

- FSoE 协议通过应用层机制在标准以太网上保持安全性；DLR 确保小于 3ms 的网络故障转移，且不会影响安全响应时间。

7 参考资料

1. AM64x Sitara™ 处理器数据手册
2. AM243x Sitara™ 微控制器数据手册

重要通知和免责声明

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、与某特定用途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安全、安保法规或其他要求。

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 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 TI 销售条款)、TI 通用质量指南 或 ti.com 上其他适用条款或 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。 除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

最后更新日期：2025 年 10 月