

Application Note

面向牵引逆变器的功能安全：设计方法和元件概述



Yuxin Liu, Sifan You, Lars Lotzenburger

摘要

随着功能安全 (FuSa) 在汽车电气化进程中愈发重要，本文档旨在全面介绍混合动力汽车 (HEV) 与电动汽车 (EV) 牵引逆变器系统中 FuSa 的实现方案。第 1 部分提供基础知识，涵盖牵引逆变器功能安全的重要性、适用的国际与区域性标准，以及 ISO 26262 V 模型开发流程。第 2 节探讨了牵引逆变器应用的系统化 FuSa 需求推导流程，通过安全目标定义、故障树分析 (FTA) 以及失效模式与影响分析 (FMEA) 的实际示例，演示了如何推导出功能安全需求与技术安全需求。第 3 节重点介绍德州仪器面向牵引逆变器及技术安全要求实现的关键器件，涵盖微控制器、栅极驱动器、位置传感器、电流传感器、电源管理 IC 等关键子系统的芯片级安全机制与系统级安全设计策略。本文档旨在为设计人员提供开发 FuSa 设计所需的基本资源。

内容

1 简介.....	2
1.1 终端设备牵引逆变器.....	2
1.2 逆变器为何需要安全性？.....	2
1.3 FuSa 开发流程.....	2
2 牵引逆变器的 FuSa 要求.....	5
2.1 牵引逆变器结构与功能介绍.....	5
2.2 FuSa 要求推导过程.....	5
2.3 安全目标.....	5
2.4 FuSa 概念.....	6
2.5 技术安全概念.....	9
3 逆变器上的安全设计实现方案.....	16
3.1 TI FuSa 产品.....	16
3.2 TSR 如何实现？.....	18
3.3 相关失效注意事项.....	23
3.4 牵引逆变器的详细 FuSa 设计结构.....	24
3.5 借助 TI 安全器件实现 FuSa 要求.....	25
4 总结.....	40
5 参考资料.....	41

商标

所有商标均为其各自所有者的财产。

1 简介

1.1 终端设备牵引逆变器

牵引逆变器是混合动力电动汽车 (HEV) 和电动汽车 (EV) 中的关键系统，根据驾驶员和整车控制单元 (VCU) 发出的命令控制电机以产生牵引扭矩。牵引逆变器还管理再生制动，为高压电池充电。图 1-1 展示了牵引逆变器的结构。

微控制器单元 (MCU) 接收到来自 VCU 的命令并处理测量信号后，执行磁场定向控制 (FOC) 算法，为功率模块生成相应的 PWM 信号。这会将直流输入调制为对称的三相交流电流以驱动电机。扭矩命令来源于两个渠道：一是驾驶员通过加速踏板或制动踏板给出的输入；二是自动驾驶或紧急制动工况下的高级驾驶辅助系统 (ADAS)。

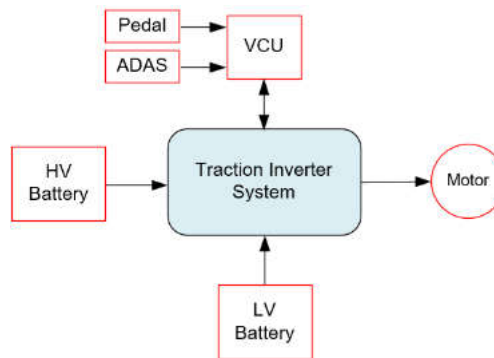


图 1-1. 牵引逆变器的结构

1.2 逆变器为何需要安全性？

随着电气化和自动驾驶技术的不断发展，HEV 与 EV 的安全性问题日益突出。关键故障可能造成危险状况——例如，发生故障的转子位置传感器可能输出错误信号，导致错误的 FOC 调制，并产生非预期的电机扭矩。同样，通信接口故障可能会阻止扭矩命令的正确传输，从而导致电机性能与驾驶员要求不匹配。此类故障对车内乘员构成重大风险。

功能安全 (FuSa) 是整体系统安全的一个关键要素，重点是确保系统以可预测的方式对正常输入和故障状况做出响应。FuSa 的主要目标是通过战略性实施适当的安全机制和设计方法，系统地将风险降至可接受的水平。

因此，FuSa 已被纳入全球国际标准和地方监管框架之中。ISO26262:2018 是道路车辆 FuSa 的国际标准，也是全球汽车 FuSa 最权威的参考。该综合标准定义了适用于汽车电气/电子系统（从概念设计到退役）的完整 FuSa 开发流程，包括安全管理、风险评估、ASIL 分级和验证方法等核心要素。该标准已成为全球汽车市场的强制性合规要求，几乎所有主流 OEM 与供应商都必须严格遵循。在此基础上，多部针对特定地区的标准涉及牵引逆变器 FuSa，包括中国的 GB/T 43254-2023、欧洲的 EU 2019/2144、美国的 SAE J2980 等。这些标准为牵引逆变器的驱动与制动扭矩功能提出了典型安全目标，并正式确立了安全功能的设计与验证要求。此外，为了实现再生制动功能，GB21670-2025 规定了相应的系统结构与安全要求。可以预见，FuSa 正逐步成为逆变器的一项强制性要求。

1.3 FuSa 开发流程

1.3.1 V 模型开发

经典 FuSa 开发流程称为 V 模型，是众多安全关键系统的核心框架。图 1-2 展示了 ISO26262:2018 中的汽车级 FuSa V 模型。这种结构化方法将整个开发生命周期划分为两个主要阶段：左臂（需求分析与设计）和右臂（集成与验证）。

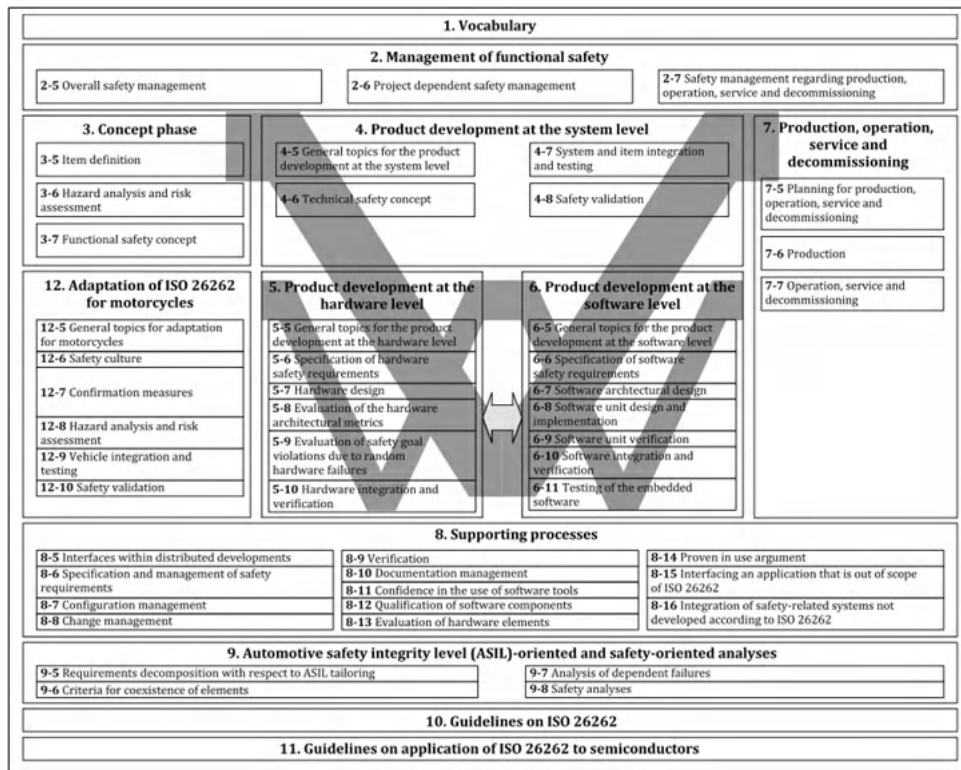


图 1-2. ISO26262:2018 中的 V 模型流程

V 模型的左臂显示了 FuSa 开发中的分解和设计阶段，包括以下详细活动：

- **项目定义**：确定项目范围和边界。
- **危害分析和风险评估**：确定项目的潜在危险，并根据严重度、暴露度和可控性因素进行评估，最终确定安全目标 (SG) 并分配汽车安全完整性等级 (ASIL)。
- **FuSa 概念**：制定高层级安全策略，在系统各功能之间分配安全责任，并确立界定所需安全功能的 FuSa 要求 (FSR)。
- **技术安全概念**：将功能要求转换为具体的技术安全要求 (TSR)，详细规定安全设计如何在系统架构中落地实现。
- **硬件/软件安全要求**：将技术需求进一步细化为硬件安全需求 (HSR) 和软件安全需求 (SSR)，用以指导实际实施。
- **设计实现方案**：根据 HSR 和 SSR 实现具体的安全功能

V 模型的右臂显示了 FuSa 开发中的集成和验证阶段，其中包含以下详细活动：

- **软件测试和验证**：验证最小的软件可测试单元。
- **硬件测试和验证**：验证最小的硬件可测试单元。
- **集成测试**：验证组件之间的交互。
- **系统测试**：验证完整的系统功能。
- **车辆集成测试**：验证实际车辆环境中的性能。
- **安全确认**：确认安全目标的实现。
- **FuSa 评估**：提供最终安全确认。
- **量产版本**：批准系统投入生产。

V 模型强调，每个开发阶段都有相应的验证活动，以验证安全需求在整个开发过程中得到有效传递与验证，从而满足汽车 FuSa 标准的严格要求。

1.3.2 逆变器安全生命周期

若要实现具备功能安全的牵引逆变器系统，TI 与系统集成商除 FuSa 开发流程外，还必须遵循 ISO26262:2018 安全生命周期。该完整方案可验证从概念阶段至退役阶段的系统性风险消减。

该流程始于安全规划与管理，用于确定项目目标。通过危害分析和风险评估，确定并建立适当的汽车安全完整性等级 (ASIL)。随后将安全目标细化为详细安全要求规范，用于指导全部后续开发工作。

在设计与实现阶段落实技术安全概念，并通过集成测试完成验证。安全要求被有条不紊地完善到特定的硬件安全设计和软件安全设计中，这些设计是根据硬件和软件 FuSa 流程独立开发与验证。

最后，定义生产与运行阶段的质量控制，同时规划从销售结束到使用寿命终结的维护和退役机制，以确保牵引逆变器在整个生命周期内维持 FuSa 能力。

2 牵引逆变器的 FuSa 要求

2.1 牵引逆变器结构与功能介绍

牵引系统的主要目标是以高控制带宽高效驱动牵引电机，这类电机通常为永磁同步电机 (PMSM)。在微控制器单元 (MCU) 中实施磁场定向控制 (FOC) 算法以生成相应的 PWM 信号，这些信号控制栅极驱动器精确地切换功率模块，将来自高压 (HV) 电池的直流输入电压转换为三相对称交流电电流，以驱动 PMSM。图 2-1 所示为牵引逆变器的方框图。

对于 FOC 算法，系统需要实时测量相电流、转子位置和直流链路输入电压。这就要求牵引逆变器内部配置高精度、低延迟传感器。此外，高可靠性电源管理器件是为系统全部元件供电的关键。

由于高压侧和低压 (LV) 侧之间需要电气隔离，因此带可靠隔离式电源电路的隔离栅极驱动器为必备器件。牵引逆变器通过 CAN 收发器精准接收驱动扭矩命令，并向整车控制单元 (VCU) 上报所有潜在故障信息。在制动操作期间，牵引逆变器可以在再生模式下运行，在为电池充电的同时产生制动扭矩。

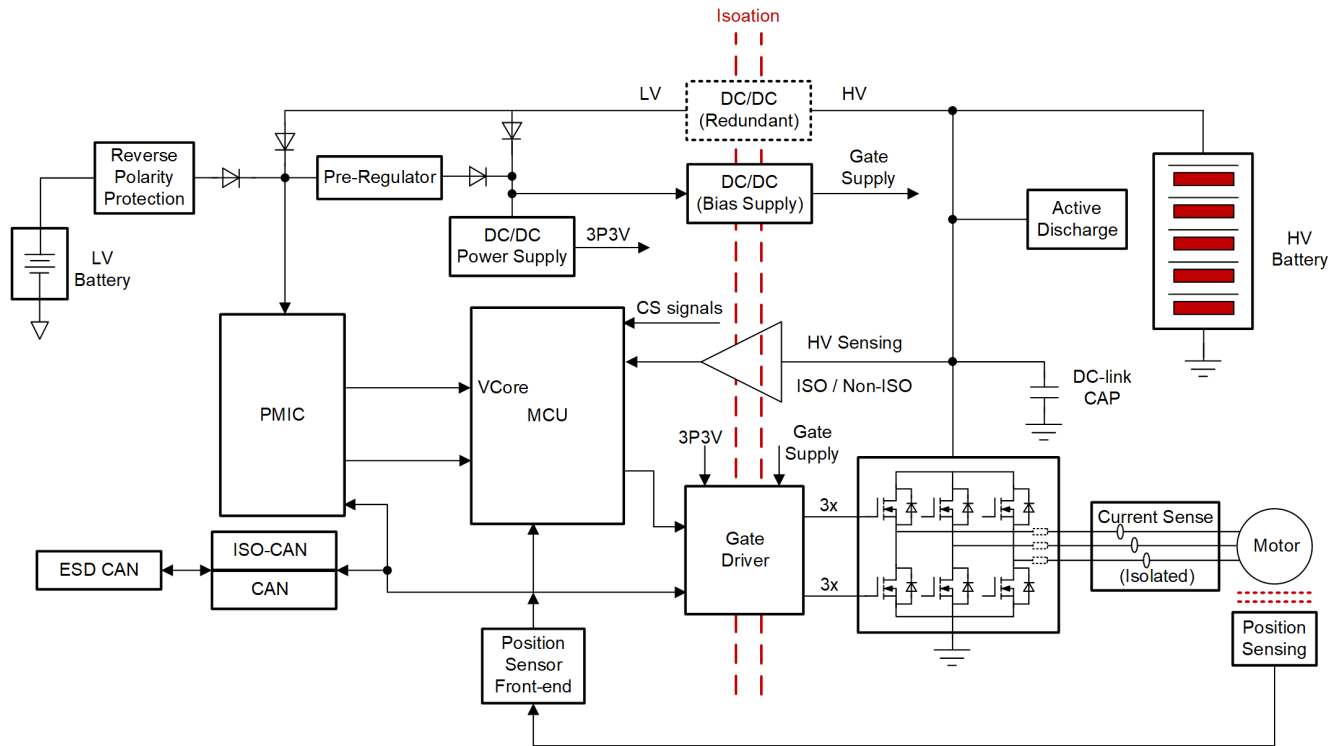


图 2-1. 牵引逆变器的方框图

2.2 FuSa 要求推导过程

以下系统安全设计基于 TI 牵引逆变器参考设计 TIDM-02014 进行应用，所有安全要求均按照第 1.3 节所述顺序推导得出。有关更多系统 FuSa 要求分析步骤，请参阅车充充电器中针对 FuSa：设计方法和元件概述。

在下文分析中，我们汇总了客户通用安全要求以及第 1.2 节所列标准中的规范性安全要求，作为牵引逆变器安全设计的安全目标。我们考虑了逆变器在驱动和制动功能对应的系统资源并相应地提出了系统的安全目标。

本文档以安全目标 1 (SG1) 为例，详细演示了如何根据此顶层安全目标构建故障树分析 (FTA)。推导得到的 FSR 1.6 将作为新安全目标，输入至失效模式与影响分析 (FMEA)。我们针对位置检测系统进行了 FMEA 分析，作为 TSR 推导流程示例。

2.3 安全目标

牵引逆变器的安全目标是针对整车系统的整车级安全要求。制定安全目标时应考虑各类非预期危险事件，以及危急情况发生后的安全状态。表 2-1 中展示了本分析中推导出的安全目标。容错时间间隔 (FTTI) 值应由 OEM 或法

规要求规定，取决于具体系统运行需求。ASIL 等级反映安全流程所需的严格程度，其中 ASIL-D 表示最高安全关键性等级。

表 2-1. 牵引逆变器的示例 FuSa 目标

ID	安全目标	ASIL	安全状态	FTTI
SG1	避免产生超出预期的非预期加速扭矩。	ASIL-C/D	1.发出警报并报告故障。	750ms (由用户指定)
SG2	避免产生超出预期的非预期制动扭矩。	ASIL-C	2.阻止扭矩输出。	
SG3	避免无法输出驱动扭矩。	ASIL-A	发出警报并报告故障。	

2.4 FuSa 概念

确立安全目标后，需制定 FuSa 概念 (FSC)，其中包含各子功能元件对应的安全要求。ISO26262:2018 建议采用演绎分析、归纳分析等安全分析方法识别失效，并转化为安全要求。本章采用典型的演绎分析方法 FTA，由安全目标推导 FuSa 要求。以 SG1 — 避免产生超出预期的非预期加速扭矩 为例，本文档演示了构建 FTA 以推导 FSR 的过程。

FTA 是一种自上而下的演绎分析方法，通过逻辑推理识别系统失效的全部诱因及失效组合。该方法采用布尔逻辑描述各事件间的因果关系。借助 FTA 可识别所有可直接引发顶事件的诱因。基于这些基本事件与逻辑门制定安全要求，即 FSR 的推导流程。

FTA 方法使用户能够将高层级安全目标系统性拆解为更具体的功能要求，用于应对各个失效模式。通过分析可引发非预期加速扭矩的事件逻辑组合，能够识别需要配置安全机制的关键环节，并制定对应的功能要求以降低风险。

2.4.1 FSC 设计架构

图 2-2 展示了 FSC 级牵引逆变器系统方框图。根据此图中所示的系统架构执行 FTA。表 2-2 中列出了每个元件的功能。

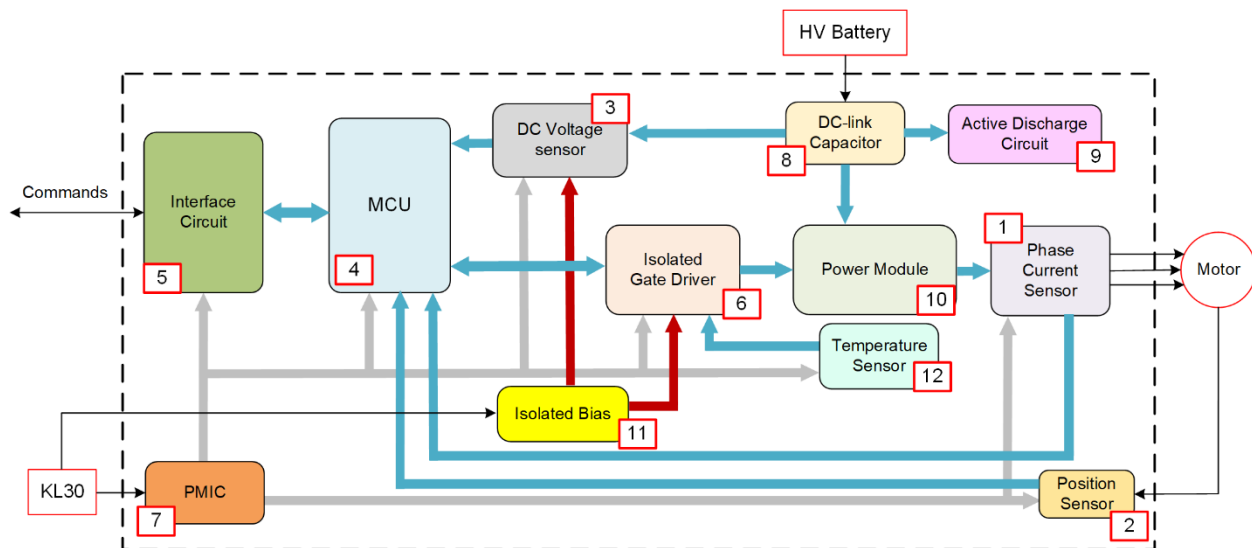


图 2-2. FSR 层级牵引逆变器系统方框图

表 2-2. 牵引逆变器中的关键元件

元件 ID	元件名称	说明
E1	电机相电流测量电路	测量功率级的逆变器相电流，然后传输到 MCU 进行 FOC 和运行状态监控。
E2	转子位置测量电路	测量电机转子位置，并发送至 MCU，用于 FOC 及运行状态监控。
E3	直流电压传感器	测量功率级上的逆变器电源，用于 FOC 和运行状态监控。
E4	微控制器电路	执行 FOC 算法、监控传感器数据、生成 PWM 信号并与外部系统通信。
E5	接口电路	提供逆变器和外部系统之间的通信收发器功能。

表 2-2. 牵引逆变器中的关键元件（续）

元件 ID	元件名称	说明
E6	栅极驱动器电路	根据输入 PWM 信号，为功率模块提供所需的电压和驱动电流
E7	电源管理电路	为逆变器低压侧的关键器件供电，并为 MCU 提供外部看门狗与故障监测。
E8	直流链路电容器	功率级电容，用于稳定并维持 HVDC 输入电压。
E9	有源放电电路	在断电或维修操作时，对直流母线电容执行有源放电。
E10	功率模块	在栅极驱动器电路的控制下，利用高压电池生成所需的调制电机相电流
E11	隔离辅助电源	为栅极驱动器电路与电压检测电路提供高压侧隔离式电源。
E12	温度测量电路	测量功率级温度，用于运行状态监控。

2.4.2 故障树分析

图 2-3 展示了 SG1 的 FTA。顶事件定义为车辆行驶工况下，逆变器产生非预期加速扭矩。随后对系统内功能元件结构开展系统性分析，确定各组件导致该顶事件发生的路径。这些故障事件与故障树图中的不同逻辑门相关，表示潜在失效模式之间的 AND 或 OR 关系。

针对 FTA 中的基本事件或逻辑门开展割集分析。该分析旨在识别割集内可引发顶事件的元件或元件组合，并确定每个割集内的元件数量。割集包含的事件数量越少，其直接造成 SG 违背的概率越高。因此，针对一阶和二阶割集制定 FSR，避免直接违背安全目标。该方法对应 ISO26262 标准中对单点故障与多点故障的处理思路：2018.对于三阶及更高阶割集，视作安全故障。此类故障组合发生概率极低，无需在低阶割集已制定的安全要求之外新增额外安全要求。

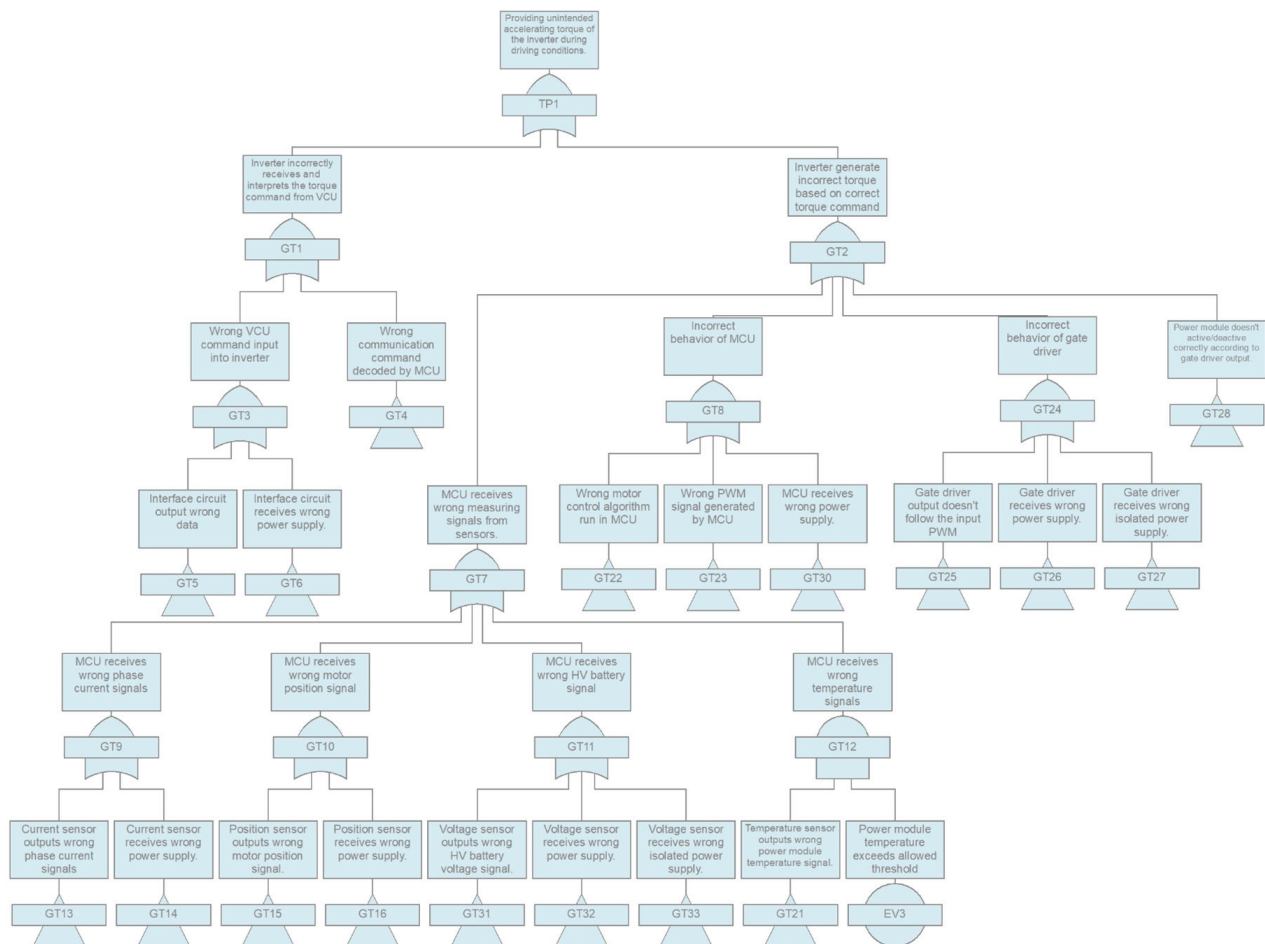


图 2-3. SG1 的 FTA 树示例

2.4.3 FuSa 要求

根据 FTA 结果，某些故障被确定为直接违反顶层安全目标的一阶割集，引发意外扭矩并造成潜在损坏。例如，如果 GT15 — 电机位置传感器输出错误的位置信号成立，MCU 将从传感器接收错误位置信号用于 FOC 控制，并触发事件 GT10 与 GT7。该故障会造成 FOC 算法输出错误 PWM 信号，生成错误交流电流与扭矩，最终导致顶事件 TP1 产生超出预期的意外加速扭矩。

根据此分析，用户可以提出一个 FSR，例如逆变器应通过位置传感器正确测量转子位置并将此要求分配给电机位置传感器实现。采用该系统化方法，基于安全目标避免产生超出预期的意外加速扭矩，已将全部一阶、二阶割集转化为 FSR，如表 2-3 中所列。

表 2-3. SG1 的示例 FSR

FSR ID	FuSa 要求	安全状态	分配	ASIL	FTTI	跟踪至
1.1	逆变器应借助接口电路，将通信数据从 VCU 正确传输至 MCU。	对 MCU 生成警报。进入 0 扭矩控制。	硬件、E5 软件、E4 硬件及软件	D	FTTI	GT5
1.2	逆变器应为接口电路提供正确供电。	进入 0 扭矩控制。	硬件、E7、E5 软件、E4 硬件及软件	D	FTTI	GT6
1.3	逆变器应通过 MCU 正确执行来自 VCU 的通信命令解码。	丢弃扭矩命令并进入 0 扭矩控制。	硬件、E4、E5 软件、E4 硬件及软件	D	FTTI	GT4
1.4	逆变器应通过电流传感器正确测量电机相电流。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E1 软件、E4 硬件及软件	D	FTTI	GT13
1.5	逆变器应为电流传感器提供正确供电。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E7 软件、E4 硬件及软件	D	FTTI	GT14
1.6	逆变器应通过位置传感器正确测量转子位置。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E2 软件、E4 硬件及软件	D	FTTI	GT15
1.7	逆变器应为位置传感器提供正确供电。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E7 软件、E4 硬件及软件	D	FTTI	GT16
1.8	逆变器应通过电压传感器正确采集高压电池电压。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E3 软件、E4 硬件及软件	D	FTTI	GT18
1.9	逆变器应为电压传感器提供正确供电。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E7 软件、E4 硬件及软件	D	FTTI	GT19
1.10	逆变器应正确为电压传感器提供隔离电源。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E7、E11 软件、E4 硬件及软件	D	FTTI	GT20
1.11	逆变器应正确测量功率模块温度。	对 MCU 生成警报。限制最大扭矩。	硬件、E12 软件、E4 硬件及软件	D	MPFDTI	GT21
1.12	逆变器应正确支持 MCU 中运行的电机控制软件算法。	阻止 MCU 输出。进入 ASC 或续流。	硬件、E4、E5 软件、E4 硬件及软件	D	FTTI	GT22
1.13	逆变器应正确提供来自 MCU 的 PWM 控制信号输出。	阻止 MCU PWM 输出。进入 ASC 或续流。	硬件、E4、E5 软件、E4 硬件及软件	D	FTTI	GT23
1.14	逆变器应为 MCU 提供正确供电。	复位 MCU。进入 ASC 或续流。	硬件、E7、E5 软件、E4 硬件及软件	D	FTTI	GT30
1.15	逆变器应在栅极驱动器中正确地将 PWM 信号放大为驱动信号。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E6 软件、E4 硬件及软件	D	FTTI	GT25

表 2-3. SG1 的示例 FSR (续)

FSR ID	FuSa 要求	安全状态	分配	ASIL	FTTI	跟踪至
1.16	逆变器应正确地栅极驱动器供电。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E7、E6 软件、E4 硬件及软件	D	FTTI	GT26
1.17	逆变器应正确栅极驱动器高压侧提供隔离电源。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E7、E6 软件、E4 硬件及软件	D	FTTI	GT27
1.18	逆变器应正确执行功率级的激活/停用控制。	对 MCU 生成警报。进入 ASC 或续流。	硬件、E6、E10 软件、E4 硬件及软件	D	FTTI	GT28

如表 2-3 所示，存在多种直接违背顶层安全目标的失效模式。失效发生后，系统必须强制进入安全状态。对于搭载 PMSM 的牵引逆变器，电机高速运行时会产生幅值较高的反电动势。我们定义了四种可能的安全状态：

• 降级为 0 扭矩模式

该安全状态适用于牵引逆变器仍可完整执行电机控制与检测功能的场景。MCU 继续根据检测信号运行 FOC 算法，令 $I_q = 0$ ，实现零扭矩输出。此安全状态适用于通信故障，例如接收不正确的 VCU 命令或线束断开。由于逆变器的其他器件仍可正常运行，因此故障解决后可便捷恢复正常功能。

• 续流

该安全状态适用于牵引逆变器低速工况下，无法按命令生成正确交流电流及扭矩的场景。在此安全状态下，所有电源开关均关断，以断开所有三个相位。在低电机转速下，PMSM 将仅产生低于高压电池电压的反电动势。

• 主动短路 (ASC)

该安全状态适用于牵引逆变器高速工况下，无法按命令生成正确交流电流及扭矩的场景。高速工况下，PMSM 产生的反电动势高于高压电池电压，会产生较大回馈电流、过大制动扭矩，存在电池损坏风险。因此，在高速工况下，逆变器应通过导通全部三个高侧功率开关或全部三个低侧功率开关来短接三相，从而进入 ASC。该方式将相电流限制为恒定值，产生的制动扭矩较低。

• 限制扭矩输出

该降级失效可运行策略用于功率模块温度超出告警阈值的场景。若在该降级模式下温度仍持续升高，超过关断阈值，则牵引逆变器进入 ASC 或续流模式。

2.5 技术安全概念

一旦 FSC 建立，下一阶段将创建技术安全概念 (TSC)。TSC 将 FSC 转换为具体的 TSR。FuSa 分析用于从 FSR 得出这些技术安全要求。

本文档在上一章中介绍了如何对牵引逆变器系统执行 FTA。本章以 FMEA 这一代表性归纳分析方法为例，说明安全分析流程及 TSR 的推导方法。本章使用 **FSR1.6** — 逆变器应通过位置传感器正确测量转子位置 作为演示示例。

FMEA 是一种系统性方法，用于识别产品设计中可能的失效模式，评估其影响与成因，并针对每一种特定失效制定相应的预防与控制措施。与从既定危害出发自上而下分析的 FTA 不同，FMEA 采用自下而上方式，检查各元器件及其潜在失效模式，再逐级追溯至系统级影响。

2.5.1 TSC 设计体系结构

图 2-4 展示了 TSC 级牵引逆变器系统方框图和 FSR1.6 的安全路径，其层级比 FSC 层级方框图深一级。对于关键器件，该分析的目标是：

- 为不受相关失效影响的安全违规失效模式提出有效的安全机制
- 为系统创建可满足检测/反应时间间隔要求的安全状态进入路径。
- 在不过度设计的前提下提供具备适当诊断覆盖率的安全机制。
- 将 TSR 转化为硬件/软件级实现。

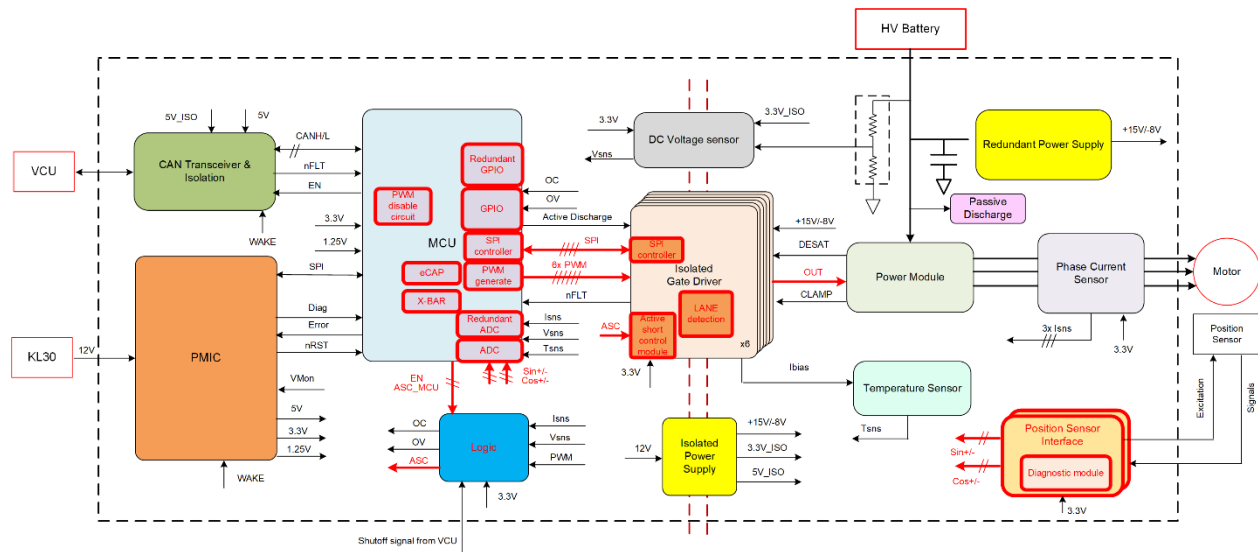


图 2-4. 采用 FSR1.6 安全路径的 TSR 级牵引逆变器系统方框图

2.5.2 失效模式和影响分析

对于每个 FSR，必须构建 FMEA 以识别故障模式、故障影响及故障原因。对于失效模式，必须根据安全目标违规类型对每种失效模式进行分类，共分为三类：

- **单点故障 (SPF)**：直接违反 FuSa 目标的故障。
- **多点故障 (MPF)**：仅当与另一独立故障叠加，才会导致 FuSa 目标被违背的故障。
- **安全故障 (SF)**：不会导致 FuSa 目标被违背的故障，可分为可检测型或本质安全型。

此外，部分元件属于非安全相关元件，其功能不会对安全目标产生影响。

对于所有可能违背 FSR 的故障（含 SPF 单点故障与 MPF 多点故障），均需设计对应的安全机制。这些安全机制可从以下维度进行设计，但不限于：

- **检测机制**（参考 ISO26262 — 第 5 部分/第 11 部分：2018）：
 - 合理性检查：值范围、变化率、信号相关性
 - 冗余监控：冗余通道之间的比较
 - 诊断测试：内置自检、周期性功能测试
 - 看门狗监测：程序流、时序监视
- **控制机制**（参考 ISO26262 — 第 5 部分/第 11 部分：2018）：
 - 安全状态切换：平稳降级以确保安全运行
 - 故障反应：对检出故障立即做出响应
 - 生成警告：向用户上报系统状态
 - 系统关闭：受控系统停用

表 2-4 显示了 FSR1.6 的 FMEA 部分。（逆变器必须通过位置传感器正确测量转子位置）。

表 2-4. FMEA 表节选示例

系统元件	系统子元件	主函数	失效模式	失效影响	SG 违规类型	故障原因	安全机制
转子位置测量电路 (E2)	转子位置测量传感器	测量 FOC 算法的转子位置，以实现电机转速和扭矩控制	无法提供电机位置测量	无法测量电机位置，这会导致错误的电机转速和扭矩控制	SPF	位置传感器输出短路/开路	1.三态输出与运行输出超出范围检查。 2.位置传感器输出超出范围检查。 3.冗余位置传感器测量电路。
					SPF	位置传感器激励电路无输出或输出漂移。	1.激励电路输出合理性检查。 2.三态输出与运行输出超出范围检查。 3.冗余位置传感器测量电路。
					SPF	位置传感器输入短路/开路	1.输入信号合理性检查。 2.三态输出与运行输出超出范围检查。 3.冗余位置传感器测量电路。
			提供的电机位置与实际位置不匹配。	测量的电机位置有误，导致错误的电机转速和扭矩控制	SPF	位置传感器输出漂移	1.输出相位和增益不平衡检查。 2.三态输出与运行输出超出范围检查。 3.冗余位置传感器测量电路。
	转子位置测量传感器冗余电路	向 MCU 提供冗余转子位置，供 FOC 使用	无法提供电机位置测量	MCU 输入值不正确/无输入值，当主转子位置传感器无故障时意外进入安全状态	MPF	激励/AFE/放大器电路的位置传感器输出开路/短路或无输出。	冗余位置传感器测量电路。
			提供的电机位置与实际位置不匹配。	MCU 的输入值不准确，无法检测到主转子位置传感器故障	MPF	位置传感器输出漂移	1.三态输出与运行输出超出范围检查。 2.冗余位置传感器测量电路。

表 2-4. FMEA 表节选示例 (续)

系统元件	系统子元件	主函数	失效模式	失效影响	SG 违规类型	故障原因	安全机制
MCU (E4)	PWM 生成电路	根据 FOC 生成 PWM 信号。	非预期 PWM 信号生成	非预期 PWM 会导致产生意外的扭矩，并且无法进入安全状态。	SPF	非预期 PWM 信号生成。	PWM 跳闸区电路，可禁用 PWM 输出，或编程 PWM 以实现对应响应。用于 PWM 电平检测的 eCAP。
	eCAP 电路	捕获上升沿或下降沿	无法捕获边沿。	无法正确捕获 ePWM 边沿，无法完成 ePWM 诊断	MPF	无法捕获边沿。	BIST
	PWM 跳闸区电路	发生故障时禁用 PWM 或对其进行编程	无法按要求运行	无法禁用 PWM 或将 PWM 编程为安全状态。	MPF	触发电路故障。	BIST
			无跳闸需求时发生非预期运行。	非预期触发并进入安全状态	SF	无触发信号时发生非预期触发	不适用
	ADC 电路	检测用模数转换器	无法正确测量模拟输入信号	无法获得正确的位置传感器输出信号。	SPF	ADC 转换器故障或引脚开路	具有硬件比较器机制的冗余 ADC。
	冗余 ADC 电路	冗余模数转换器。	无法正确测量模拟输入信号	无法获得正确的位置传感器输出信号。	MPF	ADC 转换器故障或引脚开路	具有硬件比较器机制的冗余 ADC。
	GPIO 电路	生成 ASC 相关信号，以帮助系统进入安全状态	非预期触发 GPIO 输出。	非预期触发安全状态。	SF	GPIO 输出错误	不适用
				进入错误的安全状态。	SPF	GPIO 输出错误	GPIO 回读和比较。回读比对异常时，阻止 GPIO 输出，并依靠外部逻辑电路进入安全状态。
	GPIO 回读和比较	读取 GPIO 状态以检测安全状态输出是否正确。	非预期触发错误信号	无 GPIO 输出错误，但非预期进入安全状态。	SF	GPIO 回读电路错误	不适用
栅极驱动器电路 (E6)	主动短路部件	执行 ASC，使电机进入对应安全状态。	无法使用相关 ASC 命令阻止 PWM 输出。	发生故障时无法进入安全状态。	MPF	ASC 逻辑电路或传输电路出现故障。	BIST 隔离通道诊断
			在发出相关 ASC 命令时输出错误的安全状态。	进入不安全的错误状态。	MPF	ASC 逻辑电路或传输电路翻转。	BIST 隔离通道诊断
	隔离通道检测电路	检测到隔离通道上的错误信号。	无法检测到隔离通道错误。	发生故障时无法进入安全状态。	MPF	隔离通道检测电路故障。	BIST
			非预期报告隔离通道故障。	非预期触发安全状态。	SF	隔离通道检测电路故障。	不适用

2.5.3 技术安全要求

根据 FMEA 结果，拟定的安全机制直接以技术安全要求 (TSR) 的形式提出。对于部分 SPF/MPF 故障，若系统层面无法提出可行安全机制，则将安全要求下派至软硬件层级，在半导体元件内部实现。根据表 2-4，FSR1.6 的相关 TSR 详见表 2-5。

表 2-5. FSR1.6 的 TSR

TSR ID	技术安全要求	分配	ASIL	安全状态	FTTI (由用户指定)
1.6.1	转子位置检测电路应正确测量转子位置。	位置传感器 ADC	ASIL B(D)	位置传感器三态输出。MCU 阻止位置传感器信号并路由冗余位置传感器信号。	FTTI_PS
1.6.2	转子位置检测电路应正确运行输入和输出振幅以及相位合理性检查。	位置传感器 ADC	ASIL B(D)	位置传感器三态输出。MCU 阻止位置传感器信号并路由冗余位置传感器信号。	FTTI_PS
1.6.3	转子位置检测电路应正确运行激励振幅和频率合理性检查。	位置传感器 ADC	ASIL B(D)	位置传感器三态输出。MCU 阻止位置传感器信号并路由冗余位置传感器信号。	FTTI_PS
1.6.4	传感器合理性检查失效时，转子位置检测电路应将输出置为三态。	位置传感器 ADC	ASIL B(D)	MCU 阻止位置传感器信号并路由冗余位置传感器信号。	FTTI_PS
1.6.5	冗余转子位置检测电路应进行合理性检查，如果出现故障，则进入三态。	位置传感器 ADC	ASIL B(D)	MCU 放弃冗余位置传感器信号。	FTTI_PS
1.6.6	当两路位置传感器输出有效但不匹配时，MCU 应强制逆变器进入安全状态。	ADC 软件 MCU CPU 位置传感器	ASIL-D	MCU 进入 ASC 或续流。	FTTI_MCU
1.6.7	传感器三态输出时，MCU 应正确执行传感器输出范围合理性检测。	ADC 软件 MCU CPU 位置传感器	ASIL D	MCU 放弃传感器信号并读取冗余传感器信号	FTTI_MCU
1.6.8	MCU 应检查 PWM 输出是否与预期逻辑匹配。	PWM eCAP	ASIL-D	MCU 阻止输出并进入 ASC 或续流	FTTI_MCU
1.6.9	MCU 应检查 ADC 比较器输出。	ADC 冗余 ADC ADC 硬件检查	ASIL-D	MCU 阻止输出并进入 ASC 或续流	FTTI_MCU
1.6.10	栅极驱动器应通过 ASC 信号输入来阻止 PWM 输出。	PWM 禁用电路 PWM 通道检查 ASC 电路 输出级 MCU CPU	ASIL-D	栅极驱动器切断输出级，借助其他 5 个栅极驱动器进入安全状态	FTTI_GD

表 2-5. FSR1.6 的 TSR (续)

TSR ID	技术安全要求	分配	ASIL	安全状态	FTTI (由用户指定)
1.6.11	栅极驱动器应输出正确的安全状态电压电平。	ASC 电路 隔离通道检查 输出级	ASIL-D	栅极驱动器切断输出级，借助其他 5 个栅极驱动器进入安全状态	FTTI_GD
1.6.12	栅极驱动应检查在隔离通道上传输的信号是否正确。	隔离通道检查	ASIL-D	栅极驱动器将阻止 PWM 输出并进入 ASC 或续流。	FTTI_GD

这些技术安全要求定义了具体的措施，以确保转子位置检测功能正常安全地运行。这些要求涵盖测量精度、合理性检查、冗余管理、故障检测和安全状态转换等多个方面。每项要求都分配给特定的元件，分配适当的 ASIL 等级，并链接到定义的安全状态和故障容忍时间区间。

3 逆变器上的安全设计实现方案

3.1 TI FuSa 产品

德州仪器提供各种分立式器件选型，客户可搭建适配自身特定应用需求的安全系统。TI 同时提供全面、灵活的 FuSa 解决方案，完全满足 ISO26262: 2018 要求，帮助客户在汽车电子产品和安全关键型应用中实现 FuSa 目标。此外，TI 还提供完整的产品 FuSa 文档和技术支持，以帮助集成商完成其设计流程并简化安全认证程序。

TI 的产品分为“支持 FuSa”、“FuSa 质量管理型”和“符合 FuSa 标准”三类，以满足不同的 ASIL 要求。详细的开发流程和交付成果如图 3-1 所示。

		Functional Safety-Capable	Functional Safety Quality-Managed	Functional Safety-Compliant
		Low-complexity products that can be evaluated for use in a functionally safe system	Previously-released, complex products that have had additional documentation developed to enable their use in functional safety applications.	Products specifically developed to be compliant to functional safety standards that can be used in functional safety applications
Development process	TI quality-managed process	✓	✓	✓
	TI functional safety process			✓
Analysis report	Functional safety FIT rate calculation	✓	✓	✓
	Failure mode distribution (FMD) and/or pin FMA*	✓	Included in FMEDA	Included in FMEDA
	FMEDA		✓	✓
	Fault-tree analysis (FTA)*			✓
Diagnostics description	Functional safety manual		✓	✓
Certification	Functional safety product certificate**			✓

* May only be available for analog power and signal chain products. ** Available for select products.

图 3-1. TI 在 FuSa 设计中的产品类别

• 支持 FuSa 的产品

这些产品不符合 FuSa 标准，但按照 TI 的质量管理流程开发。TI 提供包括“失效模式分布 (FMD)”和/或“引脚 FMA”在内的帮助文档，协助客户在安全应用中使用该类产品时完成硬件要素评估。TI 还为系统级 FMEDA (失效模式，影响和诊断分析) 提供支持 FuSa 的器件故障率信息。这些产品适用于中低安全完整性等级应用或作为汽车环境中高水平安全系统的辅助元件。

• FuSa 质量管理型产品

这些产品也不符合 FuSa 标准，但按照 TI 的质量管理流程开发。TI 提供详细的故障模式类型、分布和故障率信息。这些信息收录于器件 FMEDA 中，可帮助客户在安全应用中使用这些产品时完成硬件要素的硬件评估。这些产品随附安全手册，系统集成商可以根据其特定需求启用或禁用嵌入式安全机制。它们适用于中低安全完整性等级应用或作为汽车环境中高水平安全系统的辅助元件。

• 符合 FuSa 标准的产品

这些产品是唯一符合 FuSa 标准的类型。它们是按照 TI 的质量管理流程和 TI 的 FuSa 流程开发。TI 拥有适用于硬件和软件且通过 FuSa 认证的 FuSa 开发流程。TI 针对此类产品提供了完整的 FMEDA 和安全手册。系统集成商可以根据需求启用/禁用嵌入式安全机制。这些产品适用于直接用于安全相关应用，可以满足汽车环境中的安全目标。TI 还提供 FuSa 证书或评估报告，以帮助集成商获得系统级 FuSa 认证。

有关 TI FuSa 器件的信息，客户可以在 www.ti.com/technologies/functional-safety/overview.html 中轻松找到相关资料。通过选择 FuSa 类别，即可筛选出所有与安全相关的器件，如 图 3-2 所示。在 图 3-3 中显示的器件详细信息页面中，用户可以通过简单的流程访问关键 FuSa 文档。通过点击技术文档部分，可以直接下载 FuSa 报告，其中提供有关该器件的基本安全相关信息。FMEDA 等更详细的分析文档受保密协议 (NDA) 限制，须单独申请获取。

Hide filters Columns Reset table 44 of 1,148 total products

Search filters...	Product number	Images	Description	Category	Subcategory	TI functional safety category	Rating
▼ Description ▼ Category ▼ Subcategory ^ TI functional safety category Search... OR AND ☒ Select All ☒ Functional Safety Quality-Managed ☒ Functional Safety-Capable ☒ Functional Safety-Compliant Reset filter ▼ Rating ▼ Operating temperature range (°C) ▼ Package type ▼ Pin count ▼ Package area (mm²)	▼ ☐ LP87725-Q1 – NEW Data sheet: PDF HTML ▼ ☐ TPS65224-Q1 – NEW Data sheet: PDF HTML ▼ ☐ TPS653860-Q1 – NEW Data sheet: PDF HTML ▼ ☐ BQ79718-Q1 – NEW Data sheet: PDF HTML View alternates ▼ ☐ ADS131B24-Q1 – NEW Data sheet: PDF HTML ▼ ☐ ADS131B23-Q1 – NEW Data sheet: PDF HTML ▼ ☐ ADS131B26-Q1 – NEW Data sheet: PDF HTML ▼ ☐ BQ79731-Q1 Data sheet: PDF HTML OR view alternates		Automotive, three 3-A low-noise buck converters, 10 LDO and load switch PMIC for radar MMICs 5.5-V PMIC with 4 buck converters and 3 LDOs for ADAS processors up to ASIL-B Automotive 2.3-V to 36-V, 2.8-A power management IC (PMIC) for safety-relevant applications Automotive 18-s precise battery monitor, balancer and integrated protector compliant to ASIL-D Automotive high-voltage battery-pack monitor with four ADC channels for current and voltage sensing Automotive high-voltage battery-pack monitor with three ADC channels for current and voltage sensing Automotive high-voltage battery-pack monitor with six ADC channels for current and voltage sensing Automotive battery junction box voltage monitor, current sensor and isolation interface controller	Power management Power management Power management Power management Power management, Data converters Power management, Data converters Power management, Data converters	Multi-channel ICs (PMICs) Multi-channel ICs (PMICs) Multi-channel ICs (PMICs) Battery monitors & balancers Battery monitors & balancers, Precision ADCs Battery monitors & balancers, Precision ADCs Battery monitors & balancers	Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant	Automotive Automotive Automotive Automotive Automotive Automotive Automotive

图 3-2. TI.com 上的 TI 器件 FuSa 类别

Functional Safety Information

Technical documentation

★ = Top documentation for this product selected by TI

Type	Title	Date
All	Filter title by keyword	
★ Data sheet	TPS3704-Q1 Automotive Quad, Triple, Dual, Single Window or Standard Voltage Supervisor datasheet (Rev. B)	14 Aug 2023
Functional safety information	TPS3704 Functional Safety Analysis Report Summary (FMEDA) (Rev. A)	26 May 2022
Functional safety information	TPS3704 Functional Safety Report Summary (Rev. A)	26 May 2022
Functional safety information	TPS3704x-Q1 Functional Safety Manual (Rev. A)	26 May 2022

Request more information

The full failure modes, effects, and diagnostic analysis (FMEDA) is available. [Request now](#)

Require FMEDA under NDA

图 3-3. 从 TI.com 申请 FuSa 相关文档

3.2 TSR 如何实现？

以第 2.5.3 节中的 TSR 为例，本部分展示了基于 TI 安全位置传感器 AFE LDC5072/3-Q1、安全 MCU F29H859-Q1、智能栅极驱动器 UCC5881-Q1 和 TI 可编程逻辑器件 TPLD1201-Q1 的针对位置传感器输出失效场景的 TSR 实现方案。图 3-4 展示了相关器件的详细安全路径。

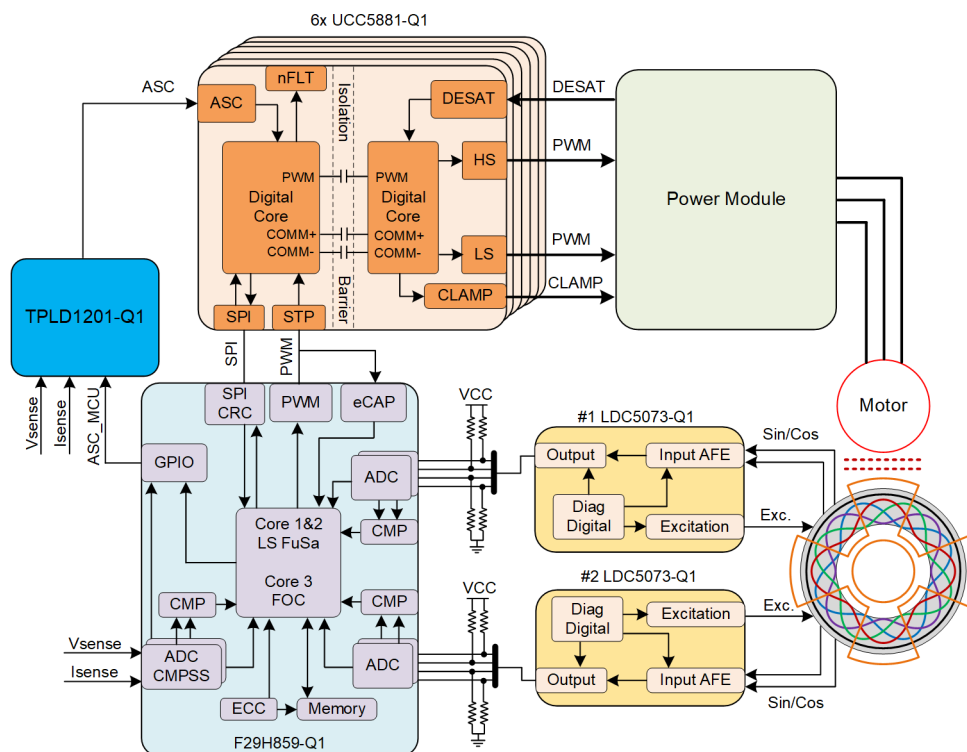


图 3-4. 位置传感器输出失效场景下对应 TSR 的安全路径

3.2.1 位置传感器

LDC5073-Q1 是一款用于电机位置检测的电感式旋转变压器模拟前端，依据 ISO26262: 2018 开发，硬件能力最高可达 ASIL-C 合规等级。该电感式传感器采用 PCB 工艺制作，与 LDC5073-Q1 共用同一块 PCB，由定子线圈和导电靶标构成。靶标安装于电机转子，位于 PCB 走线制成的定子线圈上方。LDC5073-Q1 驱动激励线圈，在靶标上生成涡流，继而在定子感应线圈中感应出电压。线束端 MCU 利用该两路信号估算转子角度。LDC5073-Q1 会生成激励信号，然后对 COS 和 SIN 信号进行滤波、解调和放大。图 3-5 展示了搭载 LDC5073-Q1 的电感式位置传感器方框图。

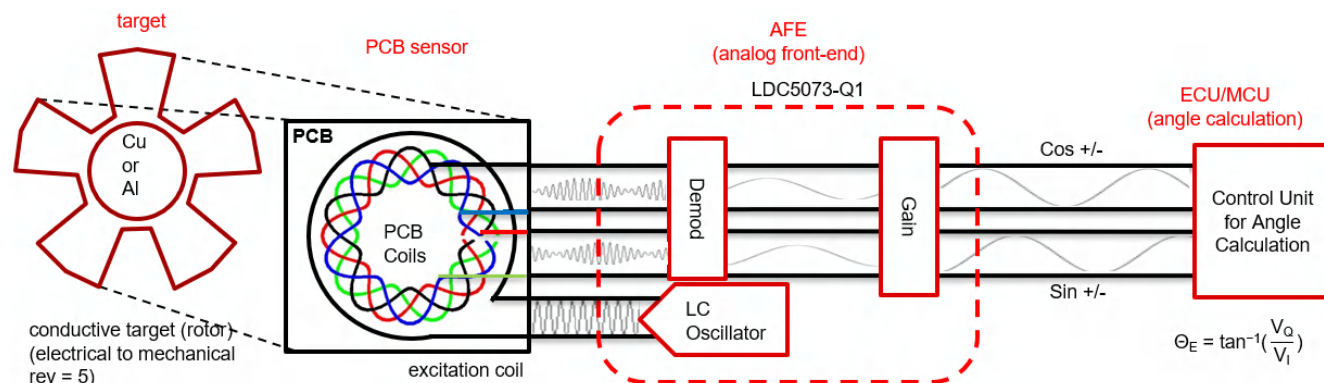


图 3-5. 搭载 LDC5073-Q1 的电感式位置传感器方框图

LDC5073-Q1 全面支持车载诊断 II (OBD2)，让控制器能够区分传感器和线束故障。该器件通过在输出端强制施加故障状态电压，无需传感器板上的额外上拉或下拉电阻即可将故障条件传达给控制器。通过使用下线 (EOL) 编程，可根据控制器板上拉和下拉配置来配置故障状态电压。当出现任何传感器故障或线束故障时，MCU ADC 会读取到引脚电压超出范围并直接检测到故障。OBD2 可与 MCU 协同，支持配置失效可运行模式与失效防护模式。在遇到激励信号故障、传感器输入信号故障、LDC5073-Q1 内部增益/失调故障或 LDC5073-Q1 输出级故障时，LDC5073-Q1 将进入诊断模式，并且 MCU 将根据 ADC 上的 OBD2 电压读取失效模式。同时，失效可运行模式可在发生安全故障期间持续上报角度信息，维持车辆运行，并提示用户进行维修。

LDC5073-Q1 还具备多重诊断功能，能够检测、监控并上报上电前或运行过程中发生的各类故障。诊断包括 UV/OV 监控、BIST、EEPROM ECC 校验、激励/检测输入输出完整性校验、热关断等。LDC5073-Q1 的可配置输出模式支持在 5.0V 电源供电时输出 3.3V SIN/COS 信号，也支持传统 SIN/COS 输出（输出电平跟随 5.0V/3.3V 电源），可将 MCU/ADC 改为 3.3V，传感器板卡仍使用 5V 运行。LDC5073-Q1 是市场上一款可预测性更强的高速角度传感器，延迟不确定度小于 100ns，3 sigma 可重复性为 0.05 度。

为覆盖传感器输出角度错误但信号仍有效的工况，同时满足系统性 ASIL-D 级设计要求，可采用两个搭载冗余检测线圈的 LDC507x-Q1 器件，PCB 尺寸不会显著增加，如图 3-6 所示。如果两个传感器输出不匹配，MCU 将放弃两个传感器输出，并强制系统进入安全状态。此外，当一个传感器输出超出范围时，系统可在失效可运行模式下运行。采用该方案，每个 LDC5073-Q1 可配置更少安全机制；两套 ASIL-B 设计可通过安全分解实现系统 ASIL-D。

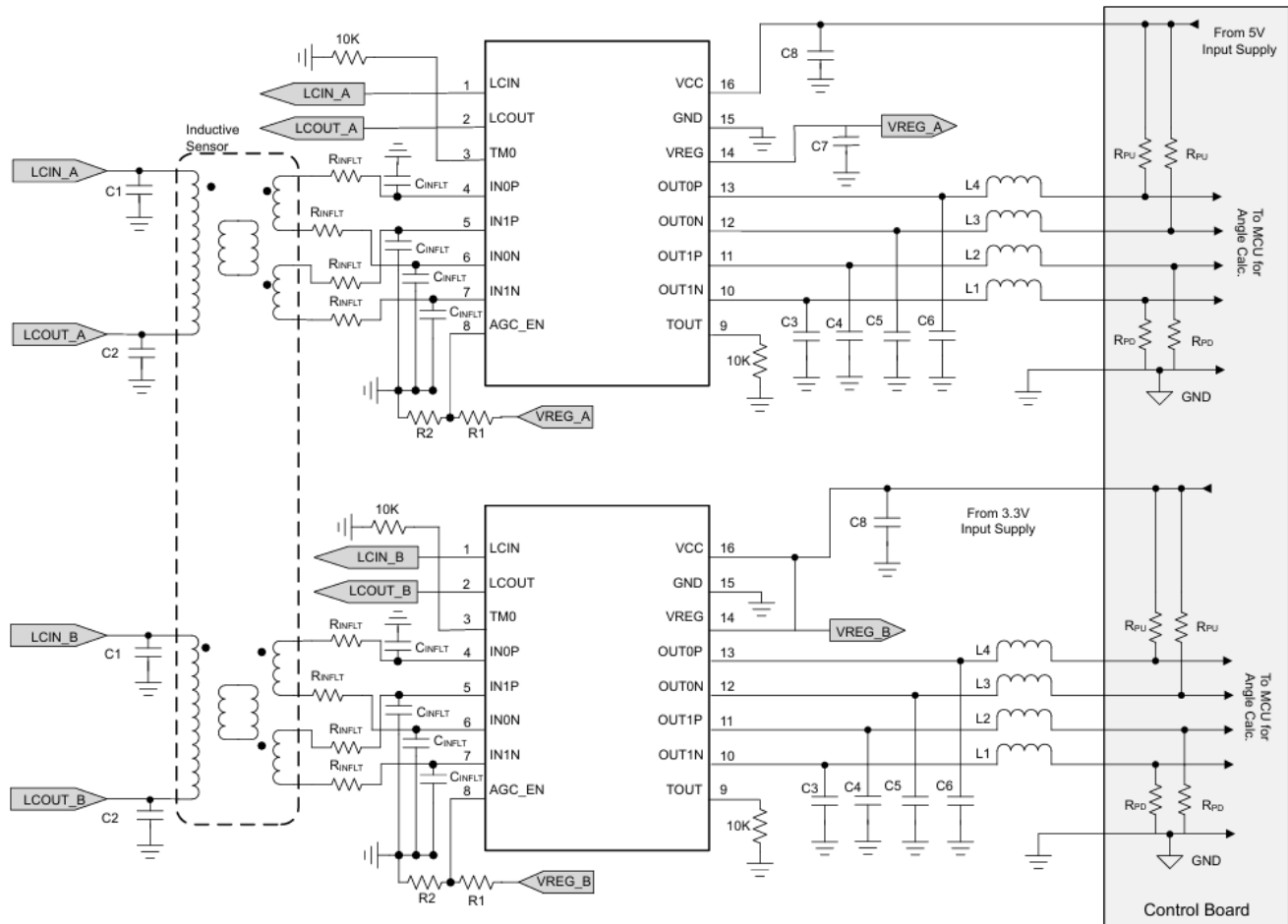


图 3-6. 2 个 LDC507x-Q1 路径作为冗余，以实现系统级 ASIL-D

3.2.2 MCU

F29H859TU-Q1 微控制器属于高性能 C2000™ 实时微控制器系列。C2000 产品线采用适用于汽车和工业应用中多种产品的通用安全架构。它拥有三个 C29x CPU（支持锁步功能），运行频率为 200Mhz，配备 4000kByte 闪

存、452kByte RAM，支持 5 个 SAR ADC、多达 36 个通道 PWM 输出，以及 QFP-144/QFP-176/BGA 256 封装。其符合 ISO26262 与 IEC61508 标准，最高可满足 ASIL-D/SIL3 等级的安全要求，同时支持用于网络安全 HSM。它具有先进的功能和丰富的连接选项，可提供一套完整解决方案。

在牵引逆变器应用中，一对锁步 (LS) 内核可专用于 FuSa 运算，另一个内核则可用于主 FOC 电机控制算法。LS 内核运行完全一致的 FuSa 代码，以检测程序执行或存储器完整性中的所有故障。如果 MCU 检测到来自 ADC 的超出范围信号，它会将位置传感器标记为故障并自动切换到读取冗余位置传感器输出。如果 MCU 检测到两个位置传感器的输出不匹配，它将通过 GPIO 向外部逻辑电路发送 ASC 命令，然后触发智能隔离式栅极驱动器中的 ASC 功能。MCU 还将通过 SPI 传输相应的状态信息，以便为 ASC 模式正确配置栅极驱动器。

ADC 硬件冗余实现方式：外设多个实例对同一输入进行采样，同步执行相同运算，再对输出结果交叉校验。通过在不同 ADC 实例中同时交叉校验 ADC 转换数据，硬件 ADC 检查电路可以检测并处理 ADC 转换故障。可以通过（增强型捕获）具有交叉开关 (XBAR) 的 eCAP 回读 PWM 输出，以检测 PWM 输出是否正确或是否已在 ASC 命令之后通过 PWM 跳闸区 (TZ) 成功禁用。可以为 ASC (GPIO 输出) 实施类似的安全机制，以验证安全状态命令的输出是否正确。

这些全面的安全功能可确保 MCU 能够可靠地检测传感器故障、处理安全关键型信号并在必要时启动适当的安全状态，从而保持牵引逆变器系统的 FuSa 完整性。

3.2.3 逻辑电路

TPLD1201-Q1 是 TI 的可编程逻辑器件，集成了大量逻辑资源，包括查找表 (LUT)、D 型触发器、计数器、边沿检测器和振荡器。它还包含多个模拟宏单元，包括模拟比较器和电压基准。图 3-7 中展示了 TPLD1201-Q1 的详细资源。

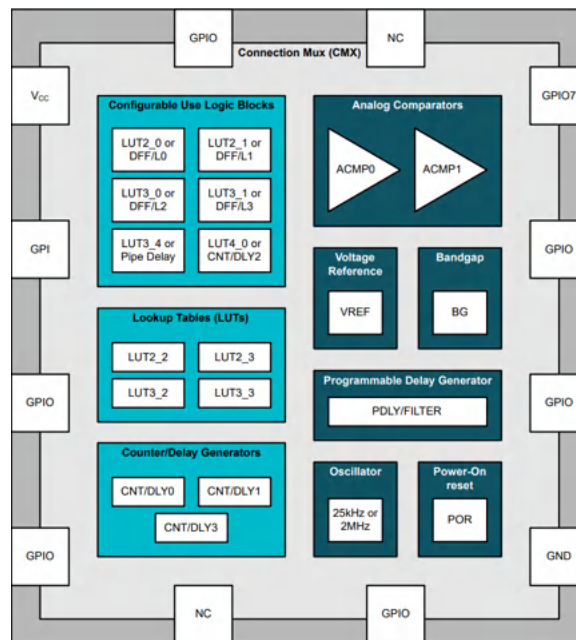


图 3-7. TPLD1201-Q1 中的资源

该器件可通过 TI ICS GUI 轻松配置并且可以永久配置为固定功能器件。借助专用的数字电路设计，TPLD1201-Q1 可用作冗余安全状态进入电路，以帮助系统在 MCU 发生故障时进入正确的安全状态。该实现方案的方框图可见图 3-8。

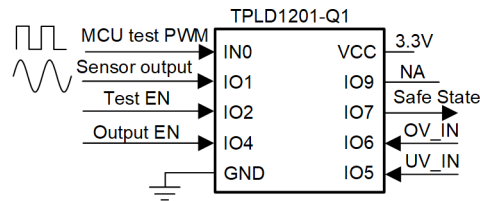


图 3-8. 电机转速检测设计的 TPLD1201-Q1 连接方案

采用该 TPLD1201-Q1 逻辑电路设计，MCU 故障时，PMIC 会向 TPLD1201-Q1 触发 Output_EN 信号，且安全状态输出引脚将根据传感器输出信号频率、OV_IN 和 UV_IN 进行响应。在过压事件期间，TPLD1201-Q1 将输出 ASC 命令、而在欠压事件期间，它将输出续流命令。当电压处于正常范围内时，TPLD1201-Q1 将根据传感器输出频率输出 ASC 命令或续流命令。在配置阶段，可通过修改器件内部的计数器数据来灵活调整阈值频率。

此设计还支持上电内置自检 (BIST)，MCU 会发送 TEST_EN 信号和测试 PWM，从而进一步降低潜在失效指标。如果 MCU 中未检测到故障，TPLD1201-Q1 输出将被屏蔽，并且 MCU 将发出相应的安全状态。用户可以在 ICS GUI 中根据自身需求灵活修改 TPLD1201-Q1 内部的所有功能和安全机制设计。

现已提供 TPLD1201-Q1 的功能安全 FIT 率、FMD 和引脚 FMA 文档。对于任何 FuSa 计算要求，都可参考本文档获取相关数据。

TPLD1201-Q1 是安全架构内的关键器件，提供独立监控与控制通路，即使在 MCU 发生故障时也能保持系统安全性。这种冗余对于在牵引逆变器应用中实现高安全完整性等级至关重要。

3.2.4 智能隔离式栅极驱动器

UCC5881-Q1 是一款隔离式、高度可配置、驱动强度可调的栅极驱动器，专用于驱动大功率 SiC MOSFET 和 IGBT。该器件是一款符合 TI FuSa 标准的器件，根据 ISO26262:2018 开发并完成全面验证。配套文档支持 ISO26262: 2018 系统设计，器件内置大量安全机制，最高可满足 ASIL-D 等级。

UCC5881-Q1 在初级侧和次级侧均具备专用的硬件 ASC 引脚。无论 PWM 输入如何，此主动短路功能都允许系统强制设置功率晶体管的状态。如果主 MCU 由于故障或其他原因而不可用，次级控制电路会将 ASC_EN 输入驱动为高电平，以强制器件的输出处于由 ASC 引脚输入所定义的状态。图 3-9 展示了 UCC5881-Q1 上典型 ASC 实现图。BIST 也会检测 ASC 电路，以确保其正常运行。

表 3-1 展示了安全状态引脚的输入真值表，其中展示不同输入组合如何决定输出状态。除了这些基本功能，ASC 还可以灵活配置为高优先级事件，从而覆盖某些其他故障（例如 DESAT、击穿、SPI 故障等）。无论 UCC5881-Q1 初级侧电源故障和其他与 PWM/通信相关的故障如何，次级侧 ASC 仍可强制系统进入安全状态。更多详情参见 UCC5881-Q1 数据表。

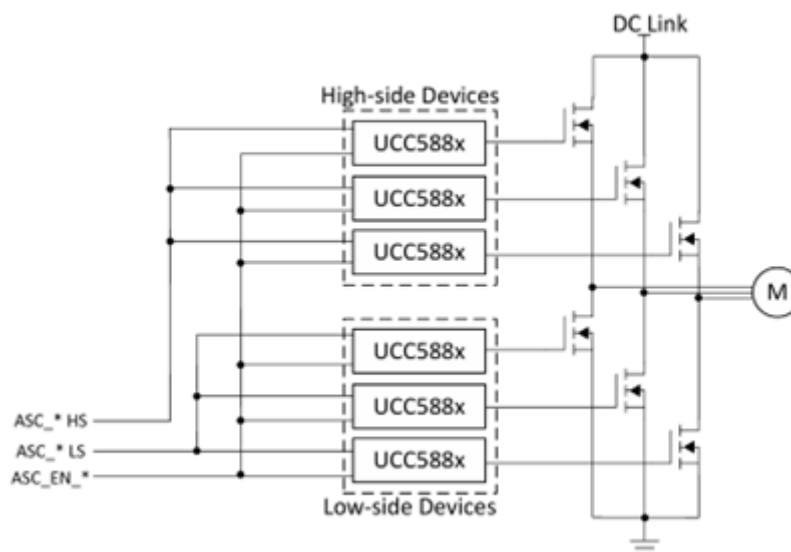


图 3-9. 使用 UCC5881-Q1 的 ASC 实现

表 3-1. UCC5881-Q1 安全状态引脚的真值表

INP	INN	ASC_EN_SEC	ASC_SEC	ASC_EN_PRI	ASC_PRI	输出状态
0	0	0	x	0	x	低
1	0	0	x	0	x	高
x	1	0	x	0	x	低
x	x	1	0	x	x	低
x	x	1	1	x	x	高
x	x	0	x	1	0	低
x	x	0	x	1	1	高

UCC5881-Q1 的击穿保护 (STP) 功能可针对 MCU 发出的错误 PWM 命令导致的击穿情况提供额外防护。若在上述保护生效的情况下仍发生过流或功率模块短路事件，UCC5881-Q1 将通过 DESAT 信号上报此事件，该信号同时由 BIST 监测。

在牵引逆变器安全设计应用中，外部 ASC 信号（来自 MCU 和外部逻辑电路）路由至 UCC5881-Q1 初级侧 ASC 引脚或次级侧 ASC 引脚。该配置可确保必要时栅极驱动器输出独立于 PWM 输入，从而向功率模块生成对应的安全状态输出。PWM 信号和 ASC 信号均通过隔离通道检测安全机制进行保护，以解决潜在的隔离通道故障。基于这些 FuSa 特性，系统可使用 TI 的安全导向器件满足与 FSR 1.6 相关的 TSR 要求。

3.3 相关失效注意事项

相关失效分析 (DFA) 是一种系统安全分析方法，旨在识别和评估可能导致系统内多个元件同时失效的共因失效或级联失效。DFA 的核心原理为分析系统内部耦合依赖关系，识别可导致多项安全功能同时失效的失效触发源，如环境因素、设计缺陷、制造工艺问题、外部干扰等。

DFA 的主要过程遵循四个关键步骤：

- **步骤 1：**列出架构元素并识别依赖对
- **步骤 2：**确定可能导致违反安全目标的相关失效的相关失效触发源 (DFI)
- **步骤 3：**确定必要的安全措施来控制或缓解相关失效。若独立性不满足要求，需补充附加措施
- **步骤 4：**评估控制或避免相关失效的措施的有效性

受篇幅限制，表 3-2 仅展示牵引逆变器系统 DFA 分析的部分内容，分析重点为位置传感器子系统。

表 3-2. 牵引逆变器 DFA 表格示例

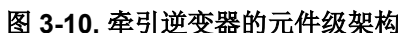
元件	相关元素	DFI 类型	DFI 根本原因	DFI 影响	故障预防措施	故障控制措施
#1 LDC5073-Q1	#2 LDC5073-Q1	共享资源失败	共享电源	3.3V 共享电源失效可能导致 #1 LDC5073-Q1 和 #2 LDC5073-Q1 同时丧失功能	PMIC TPS65386x-Q1 3.3V LDO 嵌入了输出电压监控功能，可用于 UV、OV、SC 事件。	- PMIC IC 级验证和测试 - 由客户开展集成测试
			共享电源元件	PMIC 失效可能导致 #1 LDC5073-Q1 和 #2 LDC5073-Q1 同时丧失功能	TPS65386-Q1 具有 BIST、UVLO、VMON、CRC 等多种安全机制，可覆盖 PMIC 的失效	- PMIC IC 级验证和测试 - 由客户开展集成测试
		单一物理根本原因	串扰	位置传感器的位置可能会受到串扰干扰，导致 #1 LDC5073-Q1 和 #2 LDC5073-Q1 同时丧失功能	不适用	开展仿真与验证测试，验证性能指标。
			局部发热	位置传感器受局部发热影响，可能导致 #1 LDC5073-Q1 和 #2 LDC5073-Q1 同时丧失功能	不适用	- 规格书规定了环境温度范围。本器件针对上述工况完成设计/仿真和测试工作 - 器件已通过 AEC-Q100 高温工作寿命认证。
		环境类故障	EMI	部分应用场景中，#1 LDC5073-Q1 和 #2 LDC5073-Q1 可能会受到影响，同时出现功能丧失	不适用	由客户开展集成测试
			ESD	位置传感器位置可能受静电放电 (ESD) 干扰，导致 #1 LDC5073-Q1 和 #2 LDC5073-Q1 同时丧失功能	针对特定边界的 ESD 保护设计。	规格书明确 ESD 限值，并且所有引脚依据 ESD 标准完成 ESD 测试

在我们的牵引逆变器系统 FuSa 设计中，已全面实施 DFA 分析方法。因此，我们的设计中采用了多样化的冗余、物理隔离、独立监控和其他保护措施，以保证系统发生共因失效时仍可维持所需安全功能。这些措施显著提高了牵引逆变器系统的 FuSa 等级与可靠性。

该系统化相关失效分析方法可在设计早期识别潜在共因失效，并落实相应对策，防止发生危及牵引逆变器系统整体安全的同步失效。

3.4 牵引逆变器的详细 FuSa 设计结构

通过使用第 2 节中讨论的方法，本节概述了牵引逆变器安全设计中所采用的各种 TI FuSa 元件。系统级 FuSa 分析高度依赖具体使用场景和架构。后续章节将先介绍所选元件的基础功能，再逐一介绍各元件的 FuSa 机制。图 3-10 介绍了牵引逆变器的元件级架构。



- **微控制器 (MCU)**。执行电机控制 FOC 算法，监控传感器数据，保护系统并与 VCU 通信。在安全关键型设计中，锁步核以及专用的 MCU 内部看门狗和自诊断能力都是必不可少的。
- **栅极驱动器**。提供功率模块所需的电压和大电流驱动信号。隔离式栅极驱动器还可在低压侧与高压侧之间提供强化电气隔离。为了满足系统的 FuSa 要求，隔离式栅极驱动器包含许多安全机制，例如 BIST、DESAT、钳位电路、ASC、栅极监测器、PWM 通道检测等。
- **隔离式电源**。隔离式偏置电源产生栅极驱动器电压，并在保持电隔离的同时为高压侧检测电路供电。如要驱动 SiC 和 IGBT，需要正与负隔离式偏置电源。为不同栅极驱动器独立配置偏置电源，可支撑更高 FuSa 等级设计。
- **电源管理 IC (PMIC)**。管理和控制多种电源功能，包括带保护的电压转换、电源时序、电压监控与诊断、保护、看门狗及通信。为其他器件提供电源，并对关键电压轨进行电压监控。它还为 MCU 提供外部看门狗及错误引脚监控器。当检测到 MCU 不可恢复故障时，PMIC 可触发 MCU 复位并切断相关控制信号，确保系统进入安全状态。
- **位置传感器**。测量电机转子位置和转速以进行 FOC 控制。牵引逆变器中的典型位置检测解决方案为旋转变压器与电感式传感器。牵引逆变器将生成激励信号并输入到旋转变压器/电感式传感器，同时接收传感器反馈信号进行解码。由于信号线连接到主板外部的传感器，因此需要提供对电池短路/GND 保护。
- **电流传感器**。测量三相交流机电流以进行 FOC 控制并实现过流保护。典型的实现方式包括具有过流引脚的基于霍尔效应的电流传感器，或具有比较器的基于分流器的电流放大器。
- **电压传感器**。测量高压电池直流输入电压以进行 FOC 和调制，并检测过压或欠压事件以提供保护。
- **温度传感器**。监控功率模块结温与电路板环境温度，并上报至 MCU。可实施冗余温度传感器以满足 FuSa 要求。只需通过偏置电流将 NTC 或 PTC 连接到 MCU ADC 或栅极驱动器 ADC，即可进行测量。
- **通信接口**。接收来自 VCU 的扭矩命令和其他命令，并将状态和故障信号报告回 VCU。牵引逆变器一般配置两路 CAN 收发器通道。安全关键消息通过循环冗余校验 (CRC) 和消息计数器检查进行传输，以验证数据完整性。
- **逻辑**。逻辑电路用于 FuSa 设计与保护功能实现，例如 PWM 可行性校验、安全状态进入电路、冗余电机转速检测等。

3.5 借助 TI 安全器件实现 FuSa 要求

如第 2.4 节所述，必须检测或缓解牵引逆变器系统中的所有失效事件，且失效发生时系统必须进入适当的安全状态。本节演示了如何在牵引逆变器中有效实现 TI 器件以满足 FuSa 要求，并特别强调可帮助系统在需要时进入 ASC 或续流状态的设计。

3.5.1 MCU

F29 系列器件是功能强大的 MCU，内置专为汽车与工业应用中的实时控制而设计的 C29x CPU。C29x CPU 采用超长指令字 (VLIW) 架构，具备完全受保护的流水线，并支持多种指令长度。该器件包含多达三个 200MHz 的 C29x 内核，支持 32 位和 64 位浮点与定点信号处理，程序从片上闪存或 RAM 运行。三角函数指令进一步增强了 C29x CPU 的性能，从而加快了对实时控制系统关键的常用算法的速度。

如第 3.2.2 节所述，几个关键特性对于牵引逆变器 FuSa 设计特别有价值、包括锁步功能、纠错码 (ECC) 保护、带交叉校验功能的冗余 ADC，以及 GPIO/PWM 回读特性。除上述安全机制外，F29 MCU 还提供适合 FuSa 系统设计的其他功能、外设和众多安全机制：

- **逻辑上电自检 (LPOST)**。在系统启动期间验证关键逻辑电路的完整性
- **存储器上电自检 (MPOST)**。确存储器内容在系统初始化时有效
- **错误信令模块 (ESM)**。集中整个器件的错误检测和处理
- **双时钟比较器 (DCC)**。监控时钟频率以检测时钟故障
- **通过功能安全与信息安全单元 (SSU) 实现的上下文敏感存储器和外设保护**。支持安全实时固件更新 (LFU) 和 FOTA，用于通过 A/B 切换和回滚控制进行应用固件更新。
- **安全互连 (SIC)**。在安全关键组件之间提供受保护的通信路径
- **用于网络安全、带 ECC 保护的硬件安全模块 (HSM)**。
- **可配置逻辑块 (CLB)**。为定制安全机制提供可编程逻辑功能
- **嵌入式图形发生器 (EPG)**。生成用于诊断目的的测试图形
- **窗口化看门狗计时器模块**
- **丢失时钟检测电路**。识别可能影响系统时序的时钟故障
- **具有存储器保护单元 (MPU) 的实时直接存储器存取 (RTDMA) 控制器**。

这些全面的安全特性使 F29 系列 MCU 尤其适合实现现代牵引逆变器系统复杂的 FuSa 要求，使其能够检测故障并在必要时转换到适当的安全状态。

3.5.2 栅极驱动器

在牵引逆变器系统中，栅极驱动器被分配了高 FuSa 等级，以防止功率模块中出现非预期扭矩和过流/击穿情况。UCC5881-Q1 是一款隔离式、高度可配置、驱动强度可调的栅极驱动器，专为驱动大功率 SiC MOSFET 和 IGBT 而设计。用于进入安全状态的 ASC 功能已在第 3.2.4 节介绍。

除了 ASC 功能外，UCC5881-Q1 还包含多种保护功能，包括栅极驱动器输出状态监控、故障期间的软关断、功率模块阈值电压检测、过压/欠压锁定 (OV/UVLO) 和击穿保护。UCC5881-Q1 还支持有源米勒钳位功能，可防止在高 dv/dt 事件期间功率模块非预期导通。此外，该器件还提供两个外部 ADC 通道来支持多个直流链路电压和功率模块温度检测路径，这有利于在优化系统成本的同时实现测量冗余。

图 3-11 展示了典型牵引逆变器应用中 UCC5881-Q1 的方框图。下面列出了主要保护特性和安全机制。

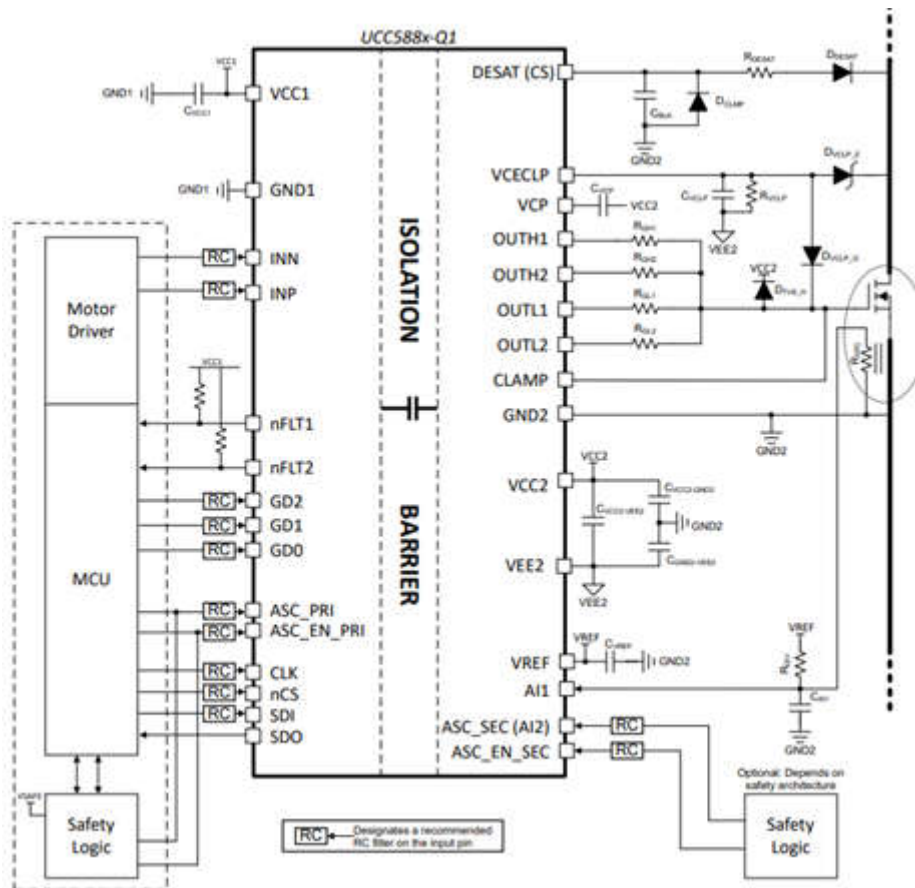


图 3-11. 典型牵引逆变器中使用的 UCC5881-Q1 的方框图

3.5.2.1 栅极监控电路和过流保护

要正确进入 ASC 安全状态，牵引逆变器必须能够可靠地导通全部三个高侧电源开关或全部三个低侧电源开关，同时使另一组桥臂保持关断状态。UCC5881-Q1 集成了一个栅极监控电路，可检测栅极驱动器输出电压电平是否与来自 MCU 的输入 PWM 信号匹配。该电路可快速检测栅极驱动器输出故障或电源开关短路/开路情况。通过监控每个栅极驱动器和电源开关的运行状况，MCU 便可在向安全状态转换期间，据此判断应导通哪些电源桥臂。图 3-12 中展示了栅极监控器电路方框图。

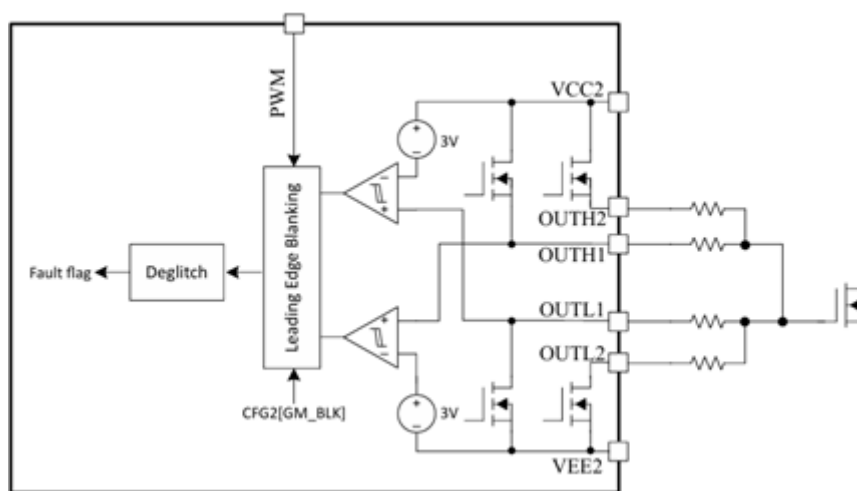


图 3-12. UCC5881-Q1 中的栅极监控器电路

过流保护是牵引逆变器中的一项关键安全功能，若过流状况未得到抑制，且未能在 2 - 3 微秒 (SiC 器件的典型值) 内得到解决，就可能导致严重的器件损坏。UCC5881-Q1 集成了一个 DESAT 电路，可实现快速过流保护。DESAT 输入通过外部电阻器和二极管网络监测 IGBT 的集电极-发射极饱和电压 (VCEsat) 或 MOSFET 的漏-源导通状态电压 (VDSon)，如图 3-13 所示。

当功率 FET 导通时，内部电流源 I_{CHG} 会正向偏置 DESAT 二极管并灌入外部电源开关的集电极/漏极。一旦 DESAT 输入电压充至阈值，便会检测到 DESAT 故障。UCC5881-Q1 上报故障并对功率模块执行软关断，以减小关断过程中的电压尖峰。随后，MCU 根据来自 6 个栅极驱动器的 DESAT 与栅极监控信息，强制系统进入适当的安全状态。

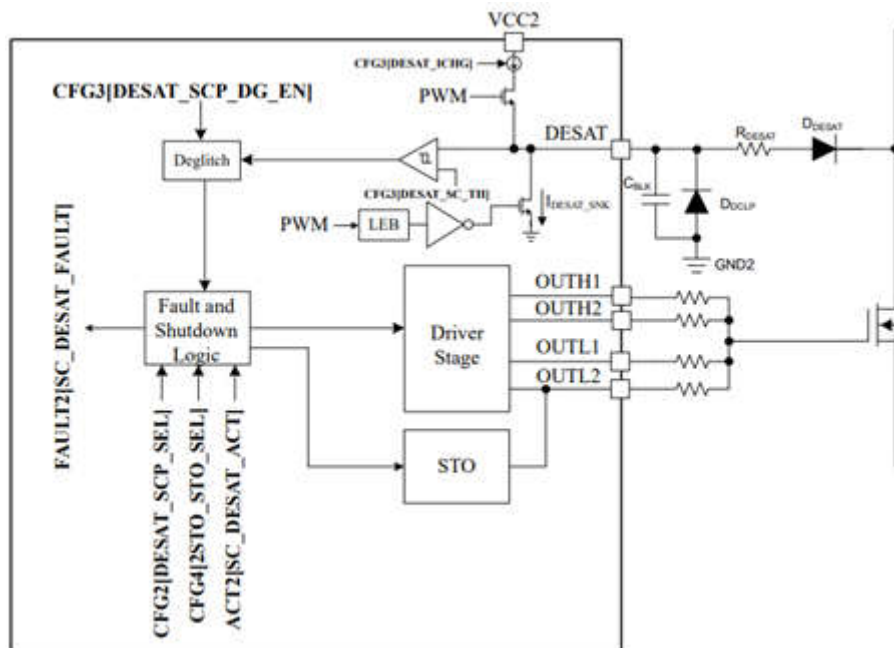


图 3-13. UCC5881-Q1 的 DESAT 电路方框图

栅极监控与快速过流保护的组合，可确保牵引逆变器能够快速检测异常运行状况，并在功率元件受损或电机产生意外扭矩之前转入安全状态。

3.5.2.2 UCC5881-Q1 中的其他安全机制

除了栅极监控和过流保护功能外，UCC5881-Q1 还包含许多旨在增强牵引逆变器保护和故障报告功能的附加安全机制：

- 启动状态下的 $V_{gs(th)}$ 功率模块正常状态检查。
- VCC1、VCC2 和 VEE2 电源上的欠压和过压监控
- 对用于其支持电路的内部电源进行欠压和过压监控
- 逻辑时钟上的时钟监控
- 配置数据循环冗余校验 (CRC)
- SPI CRC
- 内部 NVM (非易失性存储器) CRC
- 针对 VCC1、VCC2、VEE2 和内部稳压器的 UV/OV 监控功能以及主时钟的内置自检 (BIST) 诊断功能
- 功率晶体管高压钳位电路的检测与功能诊断
- 有源米勒钳位诊断。

3.5.3 隔离辅助电源

在牵引逆变器系统，隔离式电源的关键作用是为栅极驱动器提供所需电源，同时在低压控制电路和高压功率级之间保持电气隔离。由于隔离式电源对确保栅极驱动器正常运行至关重要，因此会分配高 FuSa 等级以防止产生非

预期扭矩。依据不同的架构方案，牵引逆变器系统中的隔离式电源结构主要有三种：集中式电源、全分布式电源和半分布式电源。

3.5.3.1 集中式低压隔离式电源架构

图 3-14 展示了牵引逆变器中的集中式电源架构。所有高侧和低侧栅极驱动器均使用单个隔离式偏置电源器件供电。这种方案通过减少元件提供了显著的成本优势。但是，集中式架构会带来关键的安全问题。最值得注意的是，该单一电源器件失效即构成单点故障——如果故障，所有栅极驱动器都会同时断电，可能导致牵引逆变器在故障工况下无法进入所需安全状态。集中式方案的另一重大挑战是设计带六个次级绕组的变压器（初级与次级比率为 1:6）为所有栅极驱动器供电。该设计需要专门的变压器结构，因此导致 PCB 布局复杂、走线冗长，才能覆盖全部栅极驱动器。

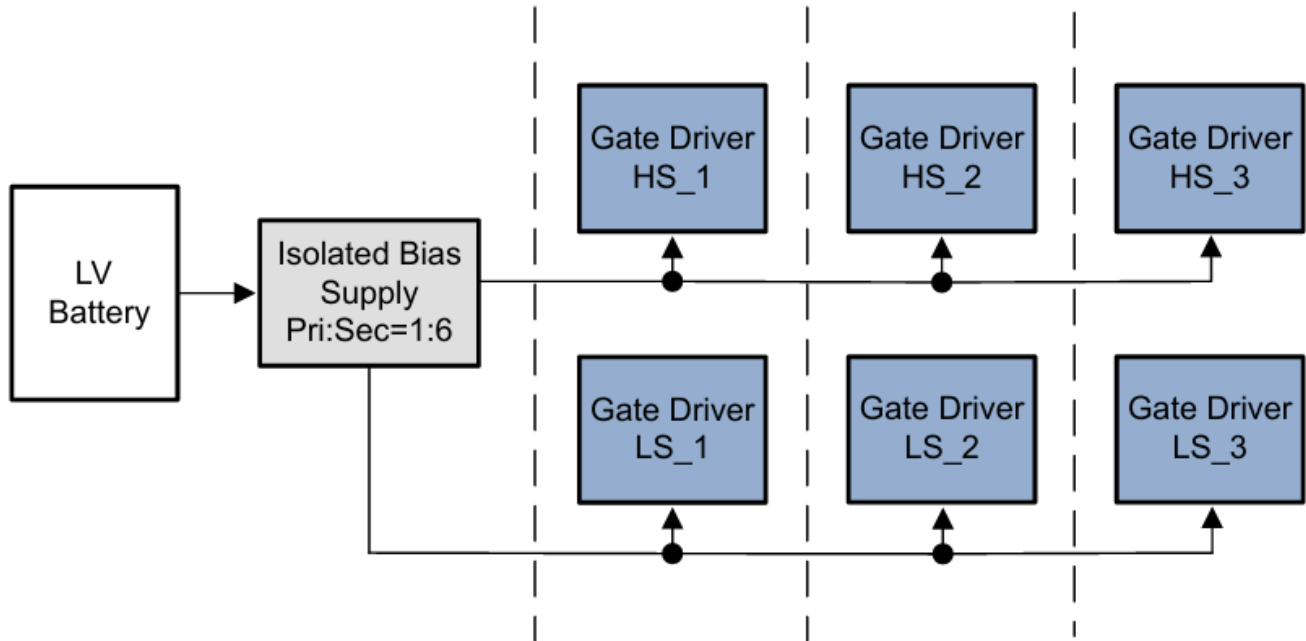


图 3-14. 集中式隔离式电源架构

3.5.3.2 全分布式低压隔离式电源架构

图 3-15 展示了牵引逆变器中的全分布式电源架构。在此配置中，每个栅极驱动器均由其各自的隔离式偏置电源器件供电。这种方法需要六个独立的隔离式偏置电源器件来为三相逆变器中的六个隔离式栅极驱动器供电。这种全冗余方案的主要优势在于其更强的容错能力：即使任何单独的偏置电源电路发生故障，系统仍然可以进入适当的安全状态。这消除了集中式架构中存在的单点故障问题，从而使全分布式方法特别适用于容错至关重要的高 ASIL 应用。

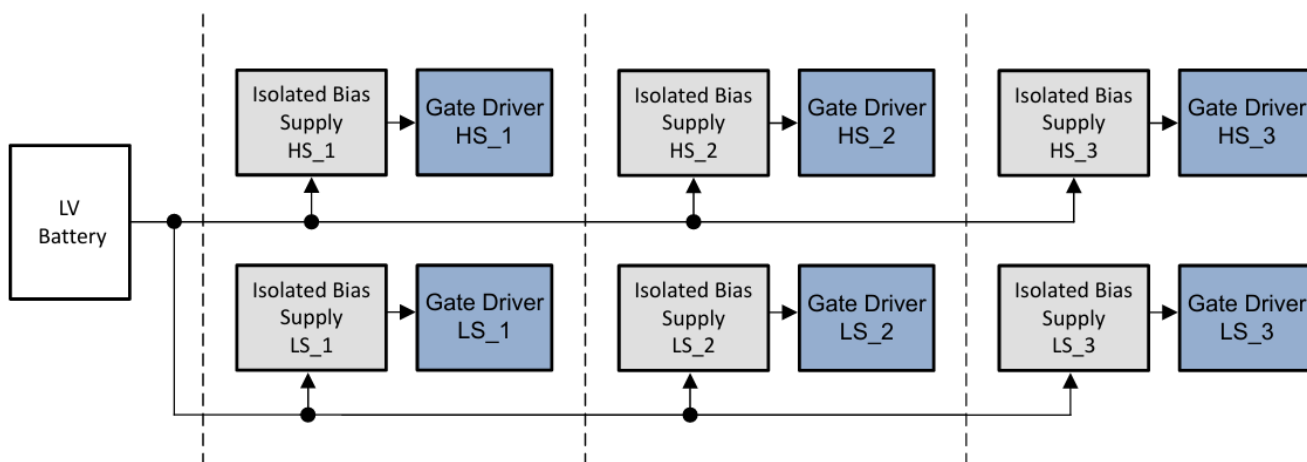


图 3-15. 全分布式隔离式电源架构

3.5.3.3 半分布式低压隔离式电源架构

图 3-16 展示了牵引逆变器中的半分布式电源架构，代表了集中式和全分布式方案之间的战略折衷。在这种配置中，多个栅极驱动器从单个隔离式偏置电源器件共享电力，但系统总体上采用多个电源单元。与全分布式架构相比，这种混合方案可减少所需隔离式电源器件的总数，从而节省成本。它还避免了集中式方案固有的全盘瘫痪风险。如果某一电源出现故障，只有一部分栅极驱动器会断电，而其他栅极驱动器仍正常工作。这种部分冗余可确保逆变器即使在电源故障时仍具备进入安全状态的能力。

这种架构的灵活性使系统设计人员能够根据具体的应用需求与安全目标定制配电策略，因而成为现代牵引逆变器设计的灵活通用方案。

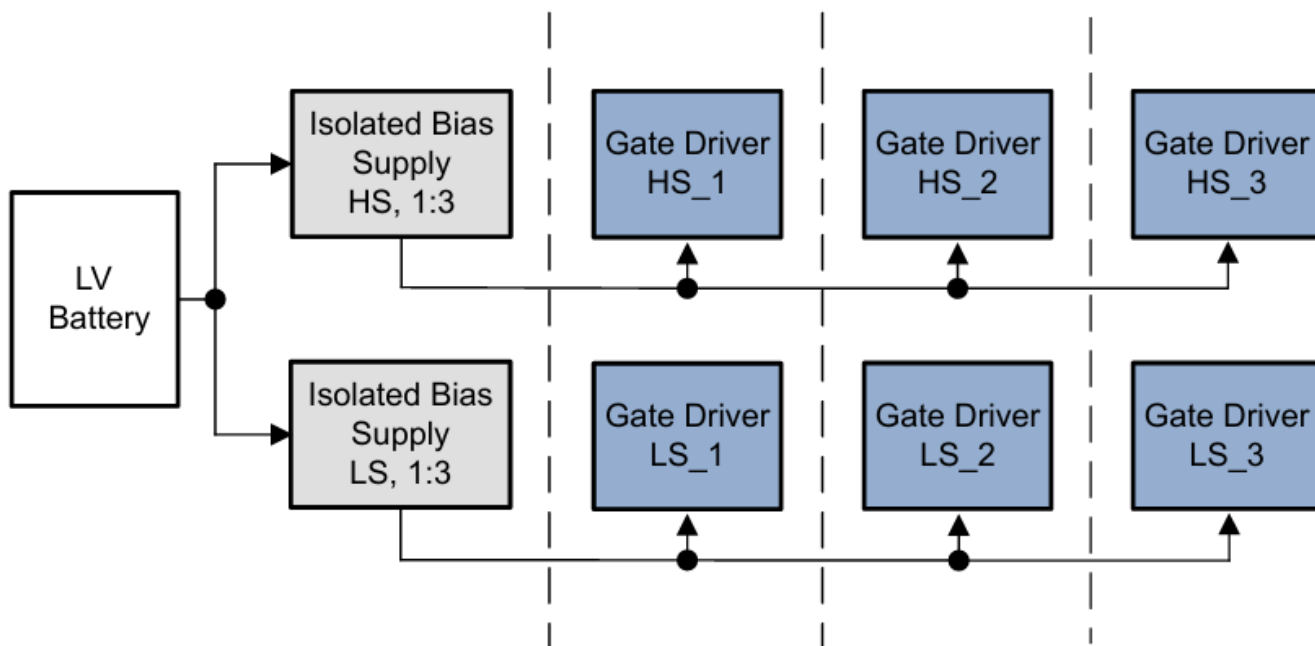


图 3-16. 半分布式隔离式电源架构

3.5.3.4 高压隔离式偏置电源

除了前面讨论的低压隔离式偏置电源架构之外，高压隔离式偏置电源也可在更高 FuSa 等级设计中作为栅极驱动器的冗余电源实现。图 3-17 展示了这种混合结构的示例，其中低侧栅极驱动器同时从低压系统和高压电池获取电力，从而形成冗余电源路径。这一策略性配置验证了，即使低压电源系统完全失效，至少一组驱动器（在本例中为低侧驱动器）仍能保持电源可用性，从而让系统能够进入至少一种可实现的安全状态。

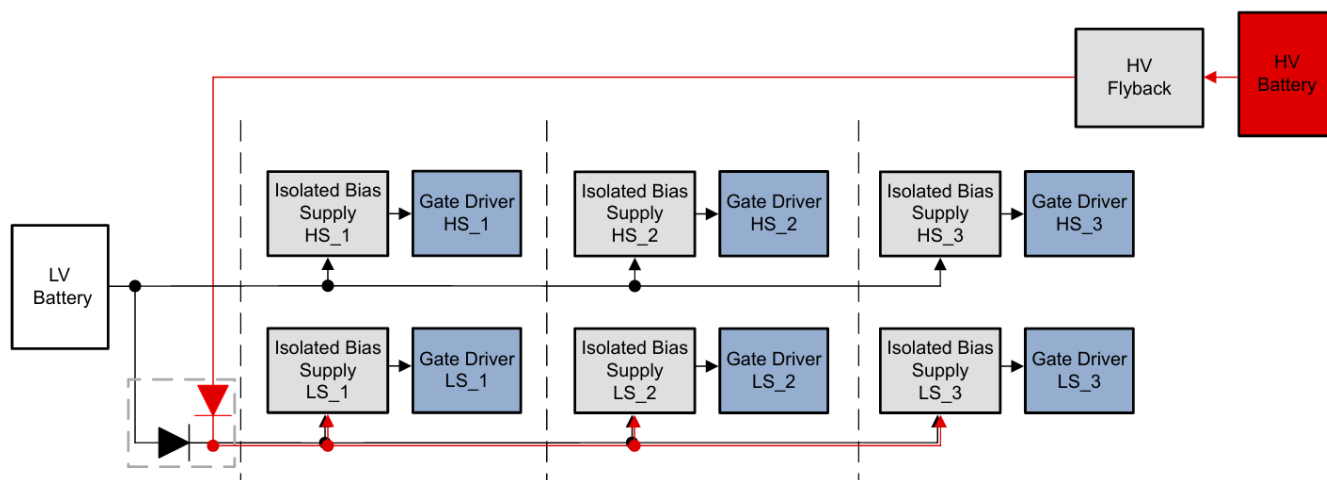


图 3-17. 为 FuSa 设计实现高压和低压隔离式偏置电源

3.5.3.5 TI 的牵引逆变器中隔离式偏置电源设计

TI 可为上文所述全部隔离式偏置电源架构提供完整解决方案，方便设计人员灵活选用最优方案，满足自身特定应用需求。

TI 面向低压隔离式电源应用提供多款集成式直流/直流模块 (UCC34xxx-Q1)，如图 3-18 所示。该系列高性能模块内置集成变压器，采用 H 桥拓扑，工作频率高于 10MHz。该高集成度方案无需外接变压器，可大幅缩减系统体积与高度。这些集成模块的一个主要优势是通过简单的反馈设计简化输出电压配置。该特性可大幅降低隔离式电源设计的工程开发工作量，同时兼具体积紧凑、薄型封装、高性价比优势。图 3-19 直观比较了 TI 的集成式直流/直流模块与传统偏置电源方案，凸显其在外形尺寸与集成度上的显著优势。

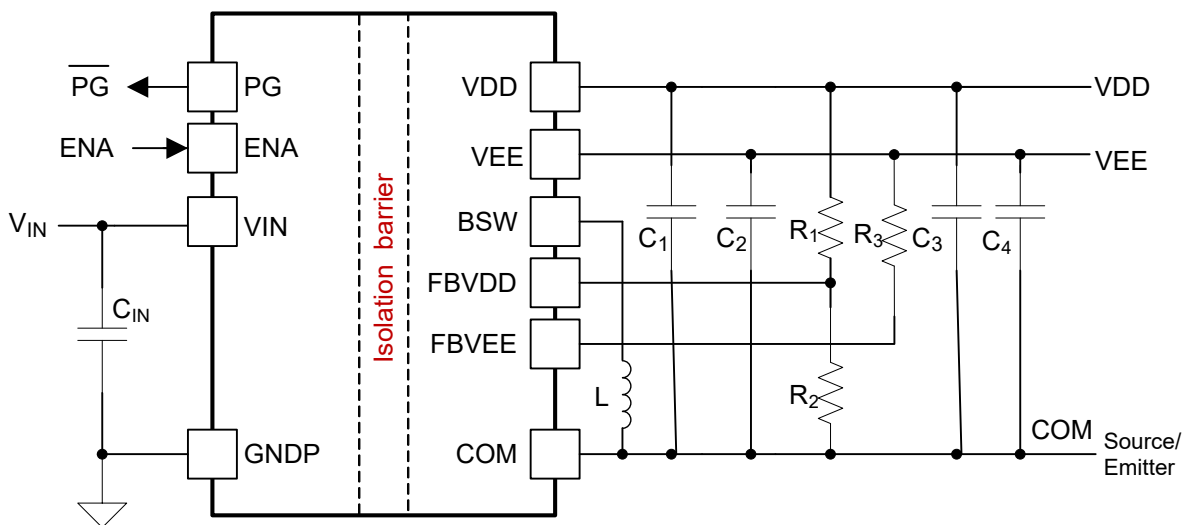


图 3-18. 内置变压器和 FET 的 UCC3414x-Q1 的应用方框图

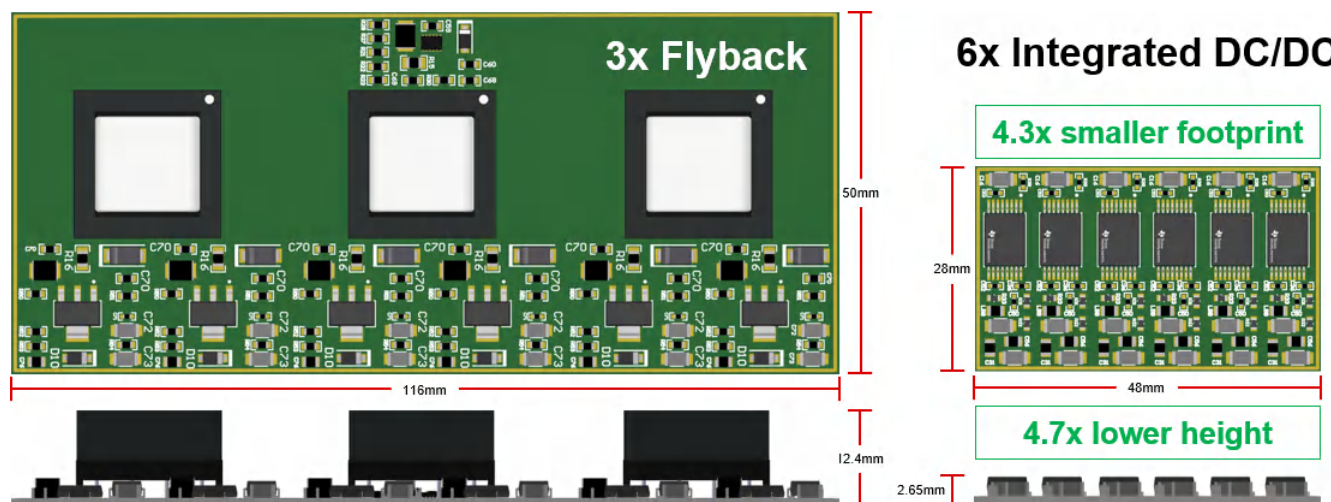


图 3-19. 集成式直流/直流模块 UCC3414x-Q1 与反激式转换器的尺寸比较

除了这些集成模块，TI 还为替代隔离式电源架构和前置稳压器转换器提供解决方案，包括反激式 (LM515x-Q1、LM(2)518x-Q1)、LLC 谐振式 (UCC25800-Q1、UCC259xx-Q1)、推挽式 (SN650x-Q1)、高压反激式设计 (UCC28C5x-Q1、UCC287xx-Q1、UCG288xx) 以及降压-升压转换器 (TPS55287x-Q1、UCC55289x-Q1)。这些方案为设计人员提供更多实现方案选择，可依据具体功率需求、隔离要求以及系统约束条件进行选取。关于 HEV 与 EV 牵引逆变器隔离式偏置电源架构及实现方案的更多详细信息，请参阅 TI 白皮书：用于 HEV 和 EV 牵引逆变器的隔离式偏置电源架构。

3.5.4 电源管理 IC

电源管理 IC 在牵引逆变器系统中承担关键功能，为几乎全部低压器件供电，包括 MCU、传感器、CAN 收发器、栅极驱动器、逻辑电路等。若这些器件无法获得稳定充足的供电，牵引逆变器将无法运行电机正常控制所需的 FOC 算法。图 3-20 中所示的 TPS65386x-Q1 器件是 TI 面向汽车领域的高端电源管理方案。这款高度集成的器件包含一个带内部 FET 的降压-升压转换器，可将输入电池电压转换为可配置的预稳压输出电压。该预稳压输出随后为器件内的其他集成线性稳压器供电，如需额外的电源轨，还可以支持外部稳压器。

TPS65386x-Q1 还具备低功耗模式，非常适合需要在多工况下保持电源效率的 MCU 电源应用。该器件被归类为符合 TI FuSa 标准的产品，按照 ISO 26262:2018 标准开发并针对汽车应用进行了全面验证。配套完整文档，支持基于 ISO 26262:2018、最高至 ASIL-D 等级的系统设计，器件内置大量安全机制。

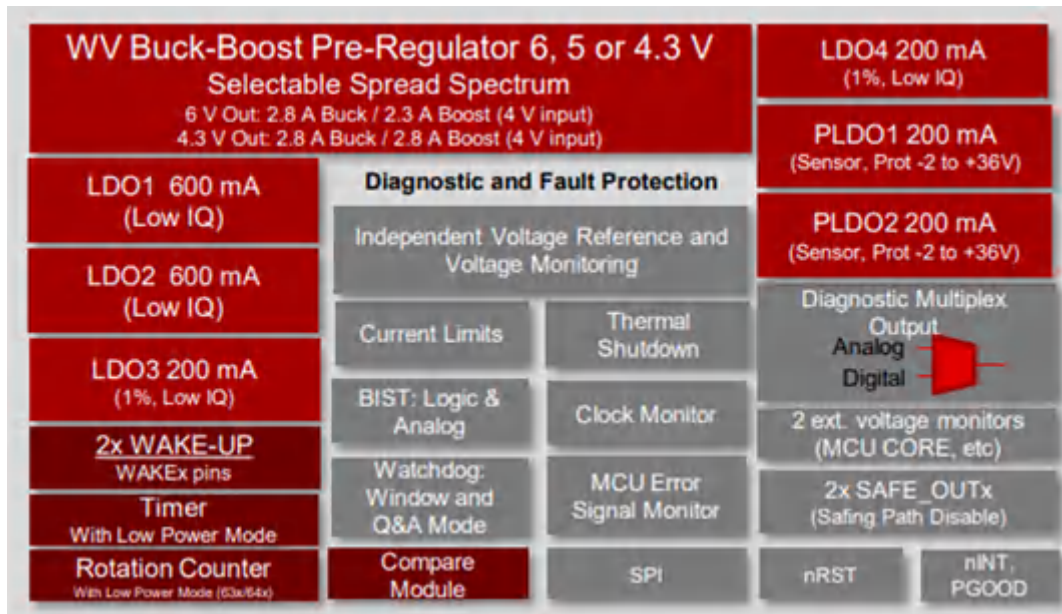


图 3-20. TPS65386x-Q1 的资源

3.5.4.1 具有保护和独立热关断功能的多路径电源轨

TPS65386x-Q1 实现了具有多个受保护电源路径和独立热管理的复杂电源架构，可确保发生部分失效时仍可靠运行。

降压-升压稳压器是该架构的核心，可用作具有集成 FET 的同步直流-直流转换器。这种高效的设计可更大限度地降低器件内的功耗，从而降低热应力。降压-升压转换器将输入电源电压转换为较低电压域 (VOUTBB)，用作 LDO (低压降) 和 PLDO (受保护低压降) 稳压器的电源。该转换器可向所有内部稳压器提供最大输出电流，必要时可额外提供电流余量供给外部稳压器。一项关键的安全特性是集成结温监控系统，可防止功率 MOSFET 中出现过多功率耗散。降压-升压转换器采用数字展频技术，可在宽频率范围内降低 EMI，从而增强系统电磁兼容性。

LDOx 线性稳压器提供 1.0V 至 1.8V (增量为 50mV) 范围内的灵活输出电压选项，同时支持 2.5V、3.0V、3.3V 或 5V 固定电压选项。未使用的 LDOx 稳压器可以改作电压监控器，为系统增加监控功能。每个 LDOx 均自带独立结温监控器，可确保任何单个 LDOx 稳压器发生过热事件时，仅禁用该稳压器，其他稳压器继续运行。根据器件配置，生成的欠压事件可能会根据需要触发额外的状态转换。这种选择性关断功能表明，即使 MCU 内核电源或数字电源丢失，外部器件仍可以通电。图 3-8 中所示的 TPLD1201-Q1 电路可以利用此功能帮助系统在 MCU 发生故障时进入安全状态。

PLDOx 稳压器灵活性更强，支持三种工作模式：跟踪模式、固定输出电压 LDO 模式或电压监控模式。这些稳压器集成了防御电源 (+36V) 和机箱接地 (-2V) 短路的强大保护功能，因此适用于电源可能扩展到 ECU 外部的传感器应用以及位置传感器电源等标准内部应用。PLDO 还可以在跟踪模式下运行，并以 TRACK 输入引脚为基准。为增强可靠性，该器件集成了两个独立的带隙电压基准源，实现交叉校验和冗余，可解决潜在的带隙开路和漂移失效模式。

这种具有多个独立电源路径和保护机制的全面电源架构可确保牵引逆变器在电源系统发生部分失效时，可持续为关键安全器件供电。

3.5.4.2 电源轨电压监控

TPS65386x-Q1 实现了全面的电压监控功能，这对牵引逆变器应用中的 FuSa 至关重要。它持续监测多个电压轨，包括 VBAT 电源电压、所有内部稳压器输出电压、通过专用 EXT_VMONx 引脚实现的外部电源轨以及内部偏置电压。当 VMON 模块在任一受监控电压轨上检测到错误事件时，会立即置位相应的 VMON 错误标志位，从而向系统发出潜在问题警报或关闭故障电源轨。为确保 VMON 基准的精度，主带隙电压基准由第二个独立的带隙基准持续进行交叉校验。此外，模拟内置自检 (ABIST) 会定期对 VMON 模块运行诊断检查，以验证其是否正常运行。每个电源轨上发生的所有故障都会上报，系统可以根据策略进入安全状态。

TPS65386x-Q1 还提供两个外部电压监控器通道，可用于监控关键外部电源轨（例如 MCU 内核输入电压或前置稳压器电压）。这一扩展的监测能力有助于实现更高的系统级 FuSa 覆盖率。图 3-21 展示了使用这些外部监测器，对为 MCU 内核及其他 LDO 供电的外部直流-直流转换器进行监测的实现示例。值得注意的是，在这种布局中，只要这些器件受到 TPS65386x-Q1 的妥善监测，即便是质量管理型 (QM) 器件也可用作直流-直流转换器。该监控关系使得整个电源系统可满足 ASIL-D 安全要求，尽管所使用器件的单项安全等级更低，体现了借助适当监控与故障检测实现安全组合的原理。

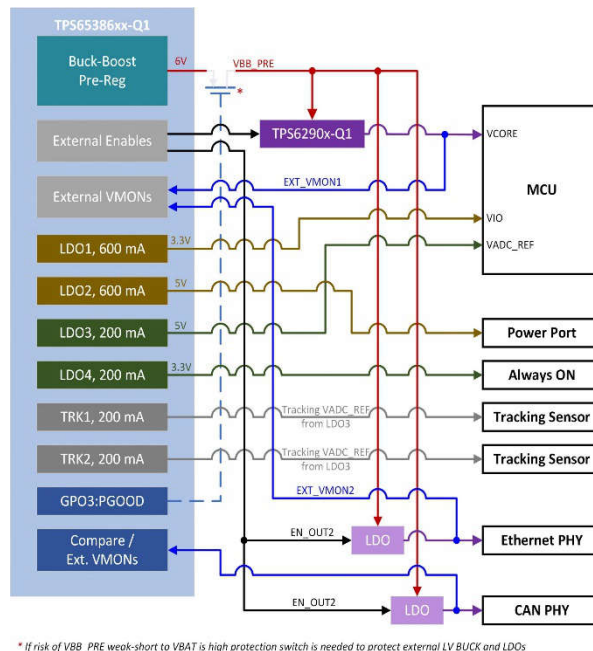


图 3-21. TPS65386x-Q1 监控外部电源轨的示例

3.5.4.3 MCU 故障监控和其他保护机制

TPS65386x-Q1 可监控模块安全 MCU。当安全 MCU 出现硬件和/或软件执行失效模式时，PMIC 将依据严重等级产生的不同后置响应，包括向安全 MCU 触发中断、关断外部功率级和/或模块通信接口；若故障持续超过阈值，则重启安全 MCU。在 MCU 无法正常运行的时段，TPLD1201-Q1 逻辑器件可接管关键安全功能，即便没有 MCU 控制，也能帮助系统进入适当的安全状态。

除了这些关键安全机制外，TPS65386x-Q1 还集成了许多可增强 FuSa 设计的附加安全机制：

- 具备触发和问答 (Q&A) 模式的看门狗。
- MCU 错误信号监控器 (MCU ESM) 用于监控输入至本器件 ESM_IN 引脚的电平或 PWM 信号；该信号来自 MCU 集成的错误诊断功能，其通过 MCU 的输出引脚输出 MCU 故障。
- 内部振荡器的时钟监控（系统时钟和低功耗时钟）
- 非易失性存储器 (NVM) 的 CRC。
- 配置寄存器的 CRC。
- SPI 通信的 CRC。
- 诊断输出引脚允许 MCU 访问器件内部的模拟和数字信号。
- MCU 和系统 (NRST) 的复位输出
- 电源正常输出 (PGOOD)。
- 中断输出 (NINT)。
- 用于在检测到故障时停止功率级或其他系统功能的安全输出。— 专用 SAFE_OUT1 输出 — 多路复用且可配置的 SAFE_OUT2，由多种可配置安全事件触发输出有效。
- 内置自检 (BIST)，在启动时检查器件功能，并可在运行时通过软件命令执行。

- 这些广泛的安全机制可确保电源管理系统能够检测并应对各种潜在故障，即使在复杂的故障场景下也能维持系统安全。TPS65386x-Q1 集 MCU 监控、独立故障响应功能和全面自诊断等特性于一体，因此是在牵引逆变器应用中实现高等级汽车安全完整性的关键器件。

3.5.5 位置传感器

电感式传感器技术作为牵引逆变器电机的位置检测解决方案越来越受欢迎，与传统旋转变压器相比，在成本、重量和高速检测能力方面具备显著优势。LDC5072/3-Q1 是一款适用于牵引电机应用的电感式旋转变压器模拟前端，在提供这些优势的同时满足严格的 FuSa 要求。该器件的功能和安全机制已在第 3.2.1 节中详细介绍。

除了电感式传感器之外，TI 还提供旋转变压器激励解决方案，该解决方案具有采用功率运算放大器 ALM2403/4-Q1 设计的二阶滤波器。图 3-22 中展示了该实现的方框图。这种创新方法可将 MCU 在 10kHz 至 20kHz 的基频下生成的 SPWM 信号转换为干净的正弦波，从而以足够的电压与电流驱动旋转变压器激励。有关详细的设计信息，请参阅 TI 的应用手册：应用 ALM2403-Q1 单芯片旋转变压器解决方案来降低系统成本。

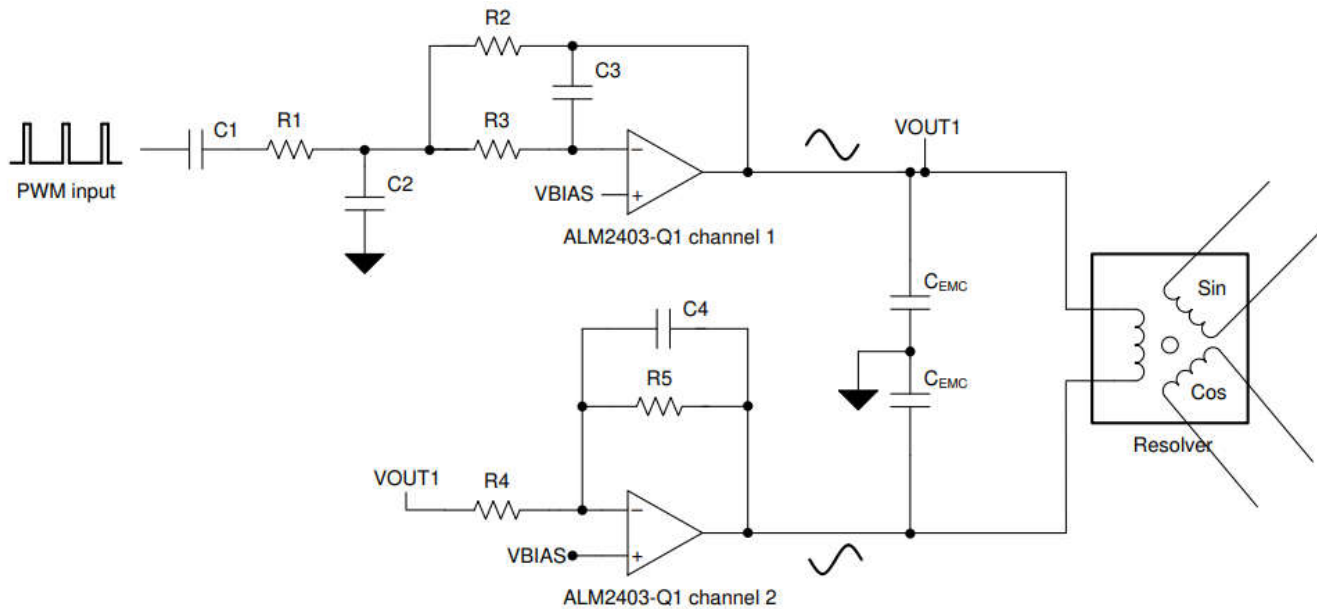


图 3-22. 基于 ALM2403-Q1 的旋转变压器激励二阶滤波器设计

3.5.6 电流传感器

在牵引逆变器系统中，电机相电流检测对于闭环电机转速和扭矩控制以及过流保护至关重要。TMCS2100-Q1 代表了一种非接触式无磁芯霍尔效应电流传感器方案。与需要使用铁氧体材料或将器件插入汇流排的传统电流传感器不同，TMCS2100-Q1 只需安装在位于三相汇流排上方的牵引逆变器控制板上，即可测量相电流引起的磁场。该安装方式具备灵活性，无需复杂机械设计注意事项，可降低工装及制造工艺成本。

通过内部算法和特性标定流程，TMCS2100-Q1 可以选择性地检测其目标汇流排激发的磁场，同时有效屏蔽相邻汇流排的干扰。该特性可将相邻汇流排间距压缩至 5mm，从而减小整体系统尺寸。图 3-23 中展示了该实现方案的原理方框图。

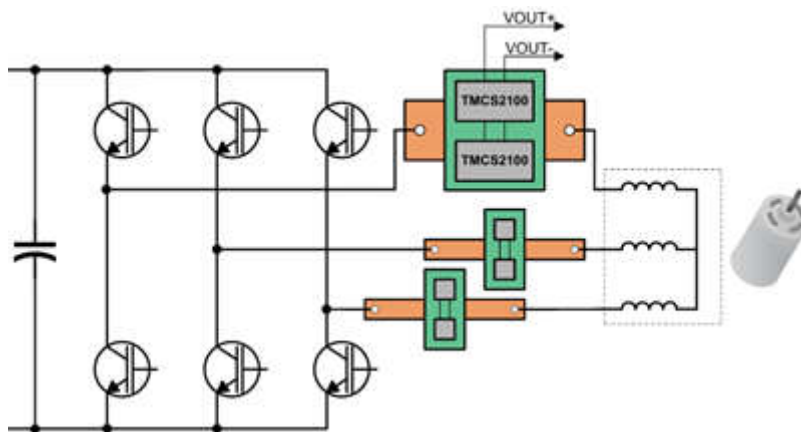


图 3-23. TMCS2100-Q1 测量三相交流电流的方框图

对于 FuSa 设计，可以实施多种系统级安全机制来实现 FuSa 目标：

- 合理性检查

在三相电机控制系统中，由于 $I_a + I_b + I_c = 0$ 的原理，理论上只需要两个电流检测信号。添加第三相电流传感器可在软件中进行合理性检查，是一种有效的安全机制。通过安全分解，可为每个器件分配 ASIL-B 等级来实现系统级 ASIL-D 合规性，也可采用对 A 相和 B 相分配 QM 等级，对 C 相分配 ASIL-D 等级的方案。

- 电流检测范围检测

如果 TMCS2100-Q1 输出超过其满量程阈值，这可能表示实际的过流情况或传感器输出漂移/误差。实施电流检测范围检测可以解决这种失效模式并触发适当的安全状态切换。该方案可实现约 60% 的覆盖率。

- 检查电流传感器输出的扭矩计算

可采用两套独立扭矩计算方法实现交叉校验。第一种方法使用电功率和电机转速计算扭矩，而第二种方法使用三相电流和电机参数进行直接扭矩计算。通过比较这两个计算值，可以验证电流检测精度。

- 使用另一组直流电流检测

增设直流电流传感器检测逆变器直流侧输入电流，用于重构三相电流，为交流电流测量提供额外校验基准。

除了基于霍尔传感器的无芯电流检测外，基于分流器的电流检测在牵引逆变器应用中仍然很受欢迎。该方法在每个汇流排中放置一个精密分流电阻器，连接到外部隔离式运算放大器以进行电流测量。AMC3302-Q1 是一款具有集成隔离式电源的隔离式运算放大器，无需外部隔离式电源。图 3-24 中展示了 AMC3302-Q1 的方框图。TI 还提供常规隔离式放大器 (AMC030x-Q1)，用于基于分流器的电流检测，该器件不带内部电源，支持单端/差分/调制输出模式。除将分流电阻置于汇流排上以外，该电阻也可集成至功率模块内部，在成本、热管理和整机尺寸上更具优势。

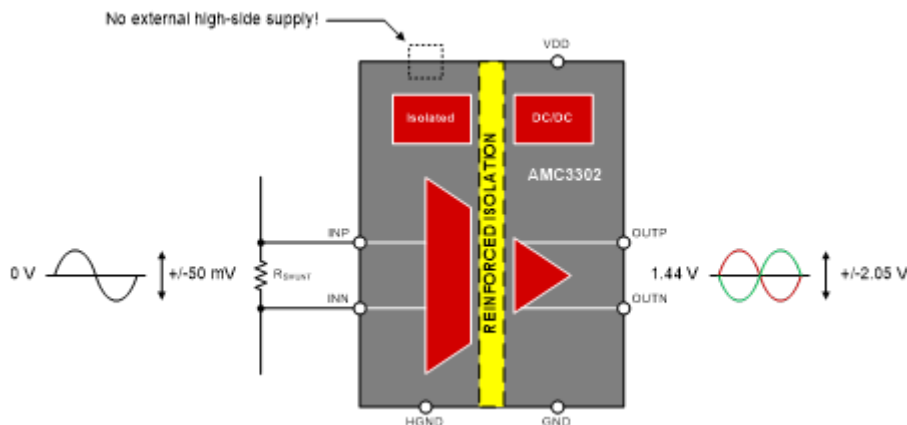


图 3-24. AMC3302-Q1 基于分流器的电流检测方框图

3.5.7 电压传感器

直流电压检测在牵引逆变器系统中发挥着关键作用，承担多项重要功能，包括弱磁控制等控制策略，以及支持 OV/UV 保护。此外，精确的电压检测对闭环有源放电管理以及功率/扭矩计算至关重要。隔离式放大器设计代表牵引逆变器应用中最常用的电压检测方法。这些器件包含一个隔离栅，可有效隔离在不同共模电压电平下运行的系统元件。该隔离对于保护低压控制电路免受高压直流母线影响、防止电气损坏并确保人员安全至关重要。隔离式放大器可提供精确的电压测量，同时保持高压汽车应用中所需的电隔离。隔离栅也可以使用高电阻路径来实现，从而创建非隔离式电压检测设计。

3.5.7.1 隔离式直流电压检测

AMC0311-Q1 是一款隔离式精密放大器，此放大器的输出与输入电路由抗磁干扰性能极强的电容隔离层隔开，器件包含单端输出和差分输出两种版本。高阻抗输入针对与高阻抗电阻分压器或任何其他高阻抗电压信号源的连接进行了优化。出色的直流精度和低温漂支持在闭环系统中进行精确的隔离式电压检测和控制。图 3-25 展示了 AMC0311-Q1 直流电压检测设计的方框图。

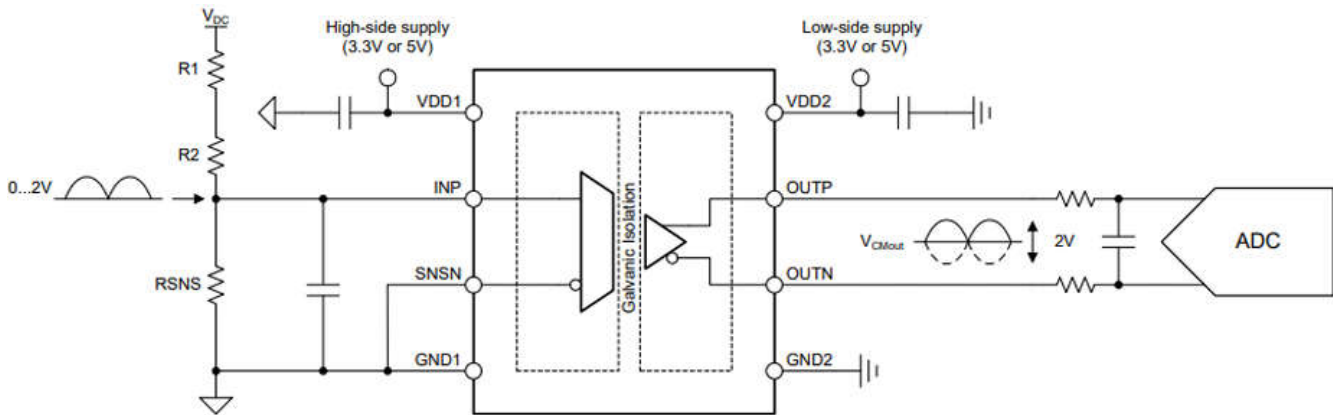


图 3-25. 用于隔离式直流电压检测的 AMC0311-Q1 方框图

为了满足 FuSa 要求，牵引逆变器设计通常采用不同的技术实现冗余直流电压检测路径，以避免潜在的共因失效。图 3-26 显示了典型的双通道电压检测实现方案：

- **通道 1：**传统方案，采用电阻梯、AMC0311-Q1 隔离放大器和 MCU ADC 进行信号转换。
- **通道 2：**采用差异化技术栈，其中包含 RES60A-Q1（集成 12.5MΩ 高电阻梯器件）、UCC5881-Q1 内置 ADC，MCU GPIO 配合 eCAP 或 $\Sigma-\Delta$ 滤波器模块 (SDFM) 或 SPI 完成信号处理。

两路电压检测结果相互交叉校验，实现冗余测量验证，提升系统整体 FuSa。

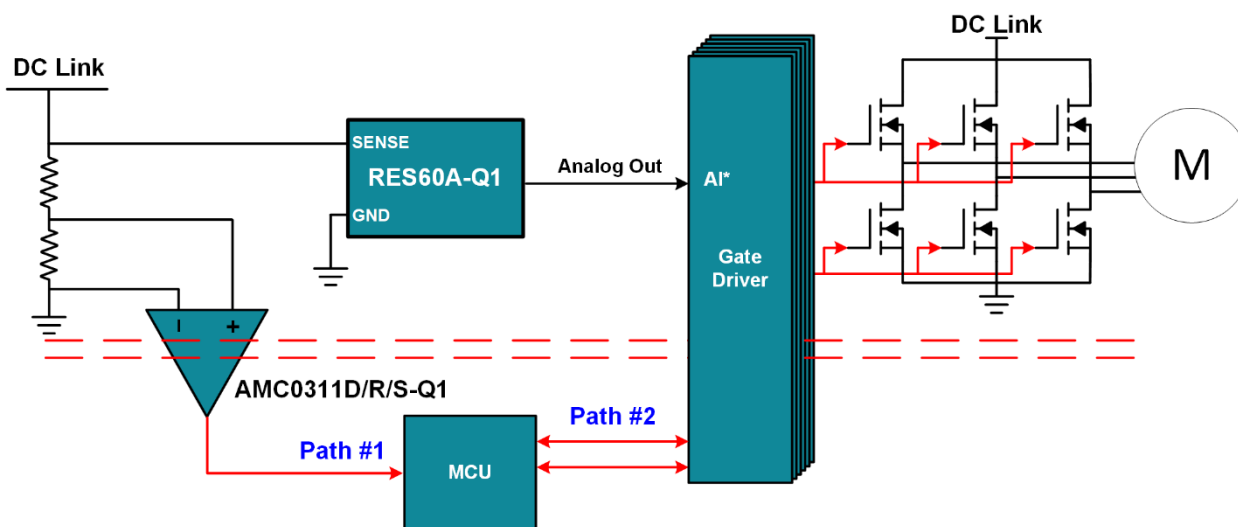


图 3-26. 针对 FuSa 采用不同技术的双通道直流电压检测

除了传统的 AMC0311-Q1 隔离式放大器外，TI 还提供多款先进的电压检测集成设计：

- **AMC038x-Q1** 将电阻梯集成到器件中，可显著减小高压检测所需的 PCB 面积，同时降压精度显著高于传统电阻梯设计。
- **AMC3311-Q1** 将隔离式直流-直流转换器集成到器件中，无需使用外部隔离电源来为高侧电路供电。这种更高水平的集成可减少元件数量，简化设计并提高可靠性。
- **AMC23C1x-Q1** 可以用作隔离比较器，从高压侧直接向 MCU 输出 OV/UV 信号。该方案构建独立监控通路，独立于主直流电压检测电路，满足更高 FuSa 要求的设计。

3.5.7.2 非隔离式直流电压检测

除隔离栅方案外，高阻路径也可在直流电压检测应用中有效地实现隔离。具有高电阻输入电阻器的差分运算放大器是该非隔离式检测方案的典型拓扑。INA160-Q1 和 TPS371K-Q1 是集成差分运算放大器，具有高输入阻抗，可实现极高共模抑制比 (CMRR)，从而实现高精度直流电压检测。这种高输入阻抗使该器件能够直接连接高压电池，同时保持安全运行。这是一种具有成本效益的解决方案，因为它无需使用电容或磁式隔离栅等隔离元件。

3.5.8 温度传感器

在牵引逆变器系统中，温度检测在过热保护和针对降级工作模式的自适应驱动策略管理方面发挥着关键作用。TMP61-Q1 是 TI 推出的具有正温度系数 (PTC) 的硅基热敏电阻。TMP61-Q1 可在其工作范围内提供出色的线性度和始终如一的灵敏度，支持使用简单而准确的温度转换方法。高线性度让用户无需在软件中使用分段拟合或查询表即可计算温度。该传感器在整个温度范围内保持一致的灵敏度，25°C 处的电阻温度系数 (TCR) 为 6400ppm/°C，典型的 TCR 容差仅为 0.2%。图 3-27 展示了典型电阻与环境温度间的关系。

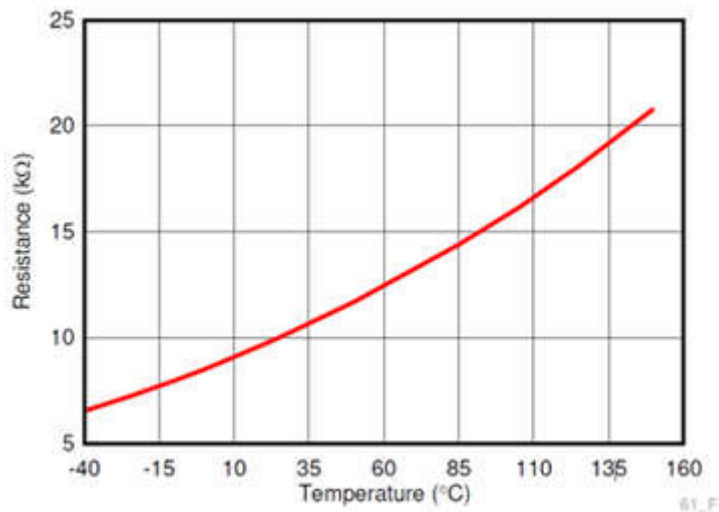


图 3-27. TMP61-Q1 PTC 电阻与温度间的关系

TMP61-Q1 可直接连接到栅极驱动器 ADC 引脚。许多栅极驱动器 (包括前面讨论的 UCC5881-Q1) 内置恒流源, 专门用于在 TMP61-Q1 两端生成测量电压。通过利用六个栅极驱动器中提供的多个 ADC 通道, 系统可以在不同位置监测功率模块的温度。此外, 它还可用作符合 FuSa 要求的冗余测量。

4 总结

本文提供了一套遵循 ISO26262:2018 标准在牵引逆变器系统中实现 FuSa 的完整方案。第 1 节展示了 FuSa 在牵引逆变器中的根本重要性，说明失效如何引发危险工况，并介绍安全关键型汽车系统所需的 V 模型开发流程。第 2 节展示通过 FTA 与 FMEA 系统推导安全要求的过程，确立牵引逆变器的具体安全目标与安全状态，并演示从高层级安全目标向详细技术安全要求的递进。第 3 节介绍了基于 TI FuSa 产品组合的工程实现策略，详述 MCU、智能栅极驱动器、位置传感器、电源管理 IC 等器件如何协同构建可检测故障并切换至相应安全状态的稳健安全架构。本文旨在向系统设计人员提供所需的基本信息与资料，用于开发符合 FuSa 标准、满足所需安全指标的牵引逆变器系统设计。

5 参考资料

1. TÜV SÜD, [了解 ISO 26262 标准：您需要了解的内容 | TÜV SÜD](#), 网页。
2. 德州仪器 (TI), [了解基于 IEC 623801 和 SN 29500 \(版本 A\) 的 FuSa FIT 基本故障率估算](#), 技术白皮书。
3. 德州仪器 (TI), [简化汽车和工业中的 FuSa 认证](#), 功能安全手册。
4. 德州仪器 (TI), [车载充电器系统中的 FuSa 概念](#), 应用手册。
5. 德州仪器 (TI), [汽车类大功率、高性能 SiC 牵引逆变器参考设计](#), 设计指南。
6. 德州仪器 (TI), [适用于 HEV 和 EV 牵引逆变器的隔离式偏置电源架构](#), 技术白皮书。
7. 德州仪器 (TI), [汽车 FuSa 以及 TI 如何通过高精度传感器帮助客户](#), 技术白皮书。

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。

版权所有 © 2026，德州仪器 (TI) 公司

最后更新日期：2025 年 10 月