Application Note

面向车载充电器中的功能安全：设计方法和元件概述

Forest Fu, Sifan You, Harvey Chen, Mingrui Zhu

摘要

随着功能安全 (FuSa) 在汽车应用中日益关键，本文档旨在全面介绍在车载充电器 (OBC) 系统中实现 FuSa 的情况。第 1 部分提供涵盖背景信息、适用标准及 TI 功能安全工具的基础知识。第 2 节探讨适用于 OBC 应用的一般 FuSa 设计原理，并演示了系统设计方法的实用示例。第 3 节重点介绍用于 OBC FuSa 实现的关键 TI 元件，这些元件具有芯片级安全特性和系统级安全机制。本文档旨在为设计人员提供开发 FuSa 设计所需的基本资源。

免责声明

本文档中介绍的系统级 FuSa 分析示例及安全机制仅用于教育目的。它们不应取代合格系统设计人员做出的适当工程分析及设计决策。系统集成商必须在特定系统设计实现的背景下重新评估所介绍的所有安全措施，以验证有效性。

内容

商标

1 简介

1.1 背景

近年来，由于环保效益（包括零排放和对化石燃料的依赖减少），电动汽车数量迅速增长。随着电气化和自动驾驶技术的不断发展，电动汽车的安全问题变得越来越重要。

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。

ISO 26262：2018 年是道路车辆中电气及电子 (E/E) 系统功能安全的国际标准。它调整了通用 IEC 61508：2010 安全-生命周期框架迁移至汽车领域。它提供了一种结构化、基于风险的方法来验证故障不会导致不安全的情况。

这些故障可以分为系统故障和随机硬件故障。系统故障在硬件设计和软件设计中都存在，可通过严格的开发流程或独立评估来管理和缓解。随机硬件故障仅限于硬件，此类故障无法消除，但可以通过实施安全机制来检测和预防。表 1-1 总结了系统故障和随机硬件故障之间的差异。

表 1-1. 系统故障与随机硬件故障

方面	系统故障	随机硬件故障
定义	在特定条件下表现一致的设计、规范、实施或者操作所固有的确定性故障	在硬件运行期间因物理现象、老化、应力或者环境因素而不可预测地发生的物理缺陷或故障
根本原因	例如设计错误、规格错误、实施错误	例如物理性能劣化、电应力、元件老化
可预测性	确定且可重现，可消除并永久修复	概率性和统计性发生，不能消除和重现
目标	在发布前消除缺陷。	在故障发生时，检测和缓解故障。
措施	在整个生命周期内进行功能安全管理、开发、测试、验证、确认活动。	安全机制设计及验证。
典型指标	未发现的安全要求数量、检查覆盖范围、工具可信度。	故障率、诊断覆盖率。

由于可以通过确保高质量的开发流程来防止和消除系统故障，因此本白皮书将重点介绍随机硬件故障分析。硬件指标 — 单点故障指标 (SPFM)、潜在故障指标 (LFM) 及随机硬件失效概率指标 (PMHF) — 用于定量评估随机硬件失效并确定符合汽车安全完整性要求。

汽车安全完整性等级 (ASIL) 从 ASIL A 到 ASIL D 不等，其中 ASIL D 最为严格。表 1-2 列出了依据 ISO 26262 与每个 ASIL 级别关联的随机硬件故障指标的可接受值。

表 1-2. 依据 ISO 26262 的硬件故障指标

ASIL 级别	SPFM	LFM	PMHF（以 FIT 为单位；时基故障）
ASIL-A	不相关	不相关	不相关
ASIL-B	≥ 90%	≥ 60 %	≤ 100 FIT
ASIL-C	≥ 97%	≥ 80 %	≤ 100 FIT
ASIL-D	≥ 99%	≥ 90%	≤ 10 FIT

1.2 硬件/软件 FuSa 分析流程

ISO26262：2018 年将从初始风险评估到设计、实施、生产和现场操作指导制造商，确保在车辆的整个生命周期中实现并记录安全目标。图 1-1 是符合 ISO26262:2018 的通用硬件/软件安全分析流程。[1]

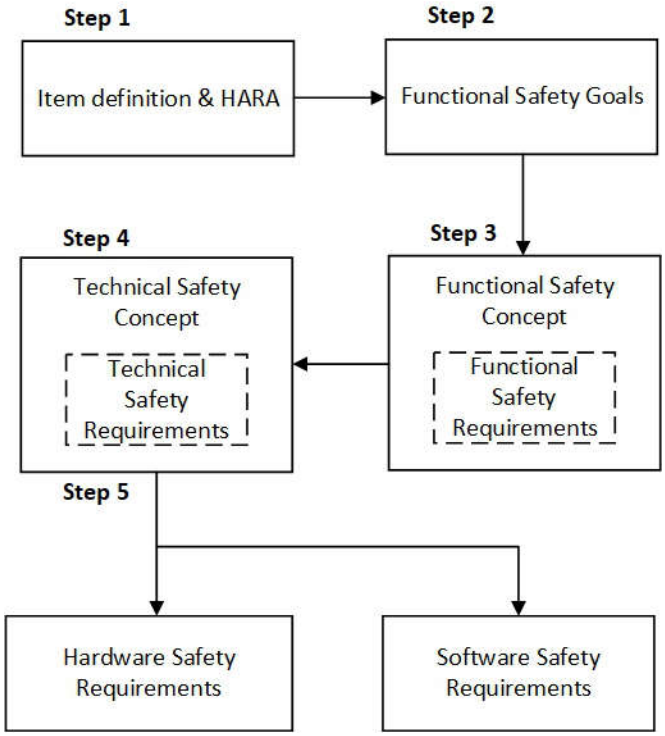

图 1-1. 制定软件/硬件要求

1.2.1 项目定义

FuSa 设计的第一步是项目定义。该项目是将进行功能安全分析的顶级车辆功能或子系统。项目定义的目标为：

- 定义和描述项目及其对环境和其他项目的依赖关系，以及与环境和其他项目的交互。
- 帮助充分了解该项目，以便后续阶段的活动可以执行。

此步骤包含危险分析和风险评估 (HARA)，这是一种将确定的功能危险转换为量化的汽车安全完整性等级 (ASIL) 和相应的安全目标的系统方法。HARA 流程为项目定义建立了明确的可追溯性，同时为所有后续安全活动提供基于风险的基础。HARA 的主要目标包括：

- 识别该项目可能导致的全部潜在危险事件。
- 通过详细分析每种危险的严重性、暴露概率和可控性因素，进行严格的风险评估。
- 根据评估结果分配适当的 ASIL 分级。

可以使用失效模式和影响分析 (FMEA)、危险及可操作性研究 (HAZOP) 等技术或从过去的质量问题中吸取的经验教训来进行危险识别。然后，评估确定的每个危险事件的严重性 (S)、暴露程度 (E) 和可控性 (C)，再分配 ASIL。每个事件的相应 ASIL 可以从表 1-3 中所示的矩阵推导。

表 1-3. 依据 ISO 26262 的 ASIL 等级

严重程度	暴露	可控性		
		C1（简单）	C2（正常）	C3（困难，无法控制）
S1（轻伤及中度伤害）	E1（极低）	QM	QM	QM
	E2（低电平）	QM	QM	QM
	E3（中等值）	QM	QM	A
	E4（高电平）	QM	A	B
S2（严重和危及生命的伤害 — 可能存活）	E1（极低）	QM	QM	QM
	E2（低电平）	QM	QM	A
	E3（中等值）	QM	A	B
	E4（高电平）	A	B	C
S3（危及生命的伤害 – 致命伤害）	E1（极低）	QM	QM	A
	E2（低电平）	QM	A	B
	E3（中等值）	A	B	C
	E4（高电平）	B	C	D

1.2.2 功能安全目标

第二步是制定 FuSa 目标和相应危险事件安全状态。FuSa 目标是一项高级别安全要求，必须满足该要求才能防止发生在 HARA 期间发现的危险。它源自对元件或系统所有可能失效模式的全面分析。对于每个 FuSa 目标，必须指定相应的安全状态；只要发生相关的危险事件，系统就必须转换到该安全状态。

根据表 1-3，从 A 到 D 分配 ASIL 的每种危险都至少需要一个 FuSa 目标，而归类为 QM 的危险不需要安全目标。当多种危险导致相似的安全目标但具有不同的 ASIL 时，可以使用其中最高的 ASIL 将它们整合到一个目标中。

1.2.3 功能安全概念

第三步是开发功能安全概念 (FSC)。FSC 提供了一个基于风险的高级描述，说明车辆功能或子系统将如何达到可接受的安全水平，这是 FuSa 目标和安全机制具体设计之间的桥梁。FSC 的目标是：

- 推导功能安全要求 (FSR)。
- 将每个 FSR 分配给相关子系统或者必须添加到架构中的外部安全措施。

作为安全目标的一个属性，ASIL 会被后续的每个安全要求继承。如果难以直接满足单个 FSR，ISO 26262 允许将其 ASIL 分解为多个冗余的 FSR，并分布在足够独立的设计元素中。这种分解通常会在主要功能元件和外部措施元件之间分配要求 — 额外的安全机制，例如冗余实现、监控电路或故障检测系统。

如果应用了 ASIL 分解，则此活动应遵循 ISO 26262-9 中允许的 ASIL 分解模式，如表 1-4 所示。

表 1-4. ASIL 分解方案

分解	原始要求			
	ASIL D	ASIL C	ASIL B	ASIL A
选项 1	ASIL B(D)+ ASIL B(D)	ASIL A(C)+ ASIL B(C)	ASIL A(B)+ ASIL A(B)	QM(A)+ ASIL A(A)
选项 2	ASIL A(D)+ ASIL C(D)	QM(C)+ ASIL C(C)	QM(B)+ ASIL B(B)	-
选项 3	QM(D)+ ASIL D(D)	-	-	-

对于每个 FSR，还必须指定故障-容差时间间隔 (FTTI)。FTTI 是发生故障与系统在发生不可接受危险之前达到安全状态之间的最长时间。

1.2.4 技术安全概念

第四步是制定技术安全概念 (TSC)，这是 FSC 更详细实施层面的对应步骤。TSC 的目标是：

- 推导技术安全要求 (TSR)。
- 证明 TSR 符合相应 FSR。

从 FSC 迁移到 TSC 涉及将 FSC 中定义的功能块分配至具体的物理架构。换言之，TSC 将高级安全目标和 FSR 细化为产品的特定硬件和软件开发要求。

故障处理时间间隔 (FHTI) 包括检测时间和反应时间，表示安全系统响应故障的总时间，如图 1-2 所示。[2]

- 故障检测时间间隔 (FDTI)：从发生故障到通过诊断措施检测故障之间的时间段。它表示系统能够以多快的速度识别出发生了故障。
- 故障反应时间间隔 (FRTI)：从检测到故障到启动指定对该故障的指定反应之间的时间段。这表示系统在检测到故障后的响应速度。

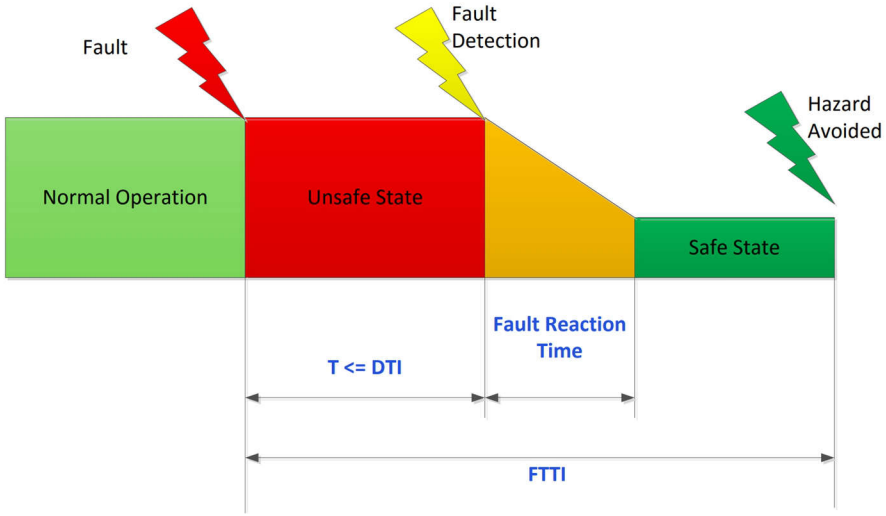

图 1-2. FDTI、FRTI 和 FTTI 之间的关系

TSR 可以通过故障树分析 (FTA) 或故障模式影响分析 (FMEA) 获得。

- FTA 是一种自上而下的方法，从不希望发生的顶层事件开始，将其分解为根本原因，提供关键故障路径的系统视图。通常采用这种自上而下的方法来系统地评估严重故障。
- FMEA 是一种自下而上的方法，用于检查单个元件，识别其可能的故障模式，并评估这些故障对整个系统的影响。通常采用这种自下而上的方法来评估潜在故障。

1.2.5 硬件/软件安全要求

第五步是推导硬件安全要求 (HSR) 及软件安全要求 (SSR) 的规格。这两组要求都可以从原始的功能安全要求中追溯，具有相同的 ASIL，共同构成具体的、可验证的安全特征。

HSR 是指定硬件元素必须如何表现以满足分配给它的 FSR 的 TSR。这是通过使用 FTA、FMEDA 或 FMEA 分析 FSR 而在 TSC 中获得的。HSR 始终追溯到单个 FSR 并继承 ASIL。

SSR 是定义软件单元必须满足的行为、质量和验证标准以满足分配的 FSR 的那些 TSR。这是通过在 TSC 中将每个 FSR 映射到软件功能，然后分析可能的软件故障模式来实现的。SSR 继承关联 FSR 的 ASIL。

硬件软件接口 (HSI) 是一组安全关键连接，用于指定跨越硬件软件边界的信息。HSI 在 TSC 中引入，然后在 HSR 和 SSR 中实现，这对于证明硬件-软件边界是明确的、确定性的和可独立验证的非常重要。

1.2.6 依赖性故障分析

依赖性故障分析 (DFA) 是一种系统性方法，用于识别和缓解由于应独立的系统或元件之间的依赖关系 (包括级联失效 (CF) 和共因失效 (CCF)) 而产生的故障。

- CF 是一个元件中的故障，该故障引发另一个元件的故障，这两个故障都由相同的根本原因引起。CF 在故障树中表示成与门。
- CCF 是一个根本原因，它同时禁用两个或多个与安全相关的项目。

DFA 在整个 FuSa 设计中应用。它在概念阶段进行，并将通过系统、硬件和软件开发加以完善。DFA 的目标是：

- 确认设计中充分实现了所需的独立性或者不受干扰性。
- 为潜在相关故障制定安全措施。

1.3 TI 配套资料

1.3.1 TI 元件类别

尽管系统集成商最终负责执行系统级功能安全分析和合规流程，但选择合适的元件对于成功至关重要。德州仪器 (TI) 将产品整理到明确的功能安全类别中来简化这一任务。

如图 1-3 所示，TI 器件分为功能安全型、功能安全质量管理型或功能安全兼容型，使工程师更容易为安全关键设计确定合适的产品。

- 功能安全型产品：
  - 使用 TI 标准质量管理型开发流程开发的更简单 IC。
  - 内部监控和诊断等安全功能并非总是集成在一起。
  - TI 提供了 FuSa 时基故障率 (FIT) 计算、FMD 及引脚 FMA。
- 功能安全质量管理型产品：
  - 具有内部诊断功能的复杂产品。
  - 使用 TI 的标准质量管理开发流程开发而成。
  - 大量文档：FMEDA 分析、FuSa 手册。
- 功能安全合规型产品：
  - 最复杂的产品，可以是系统本身。
  - 根据 ISO 26262:2018 中规定的经认证 FuSa 开发流程开发。
  - 更多详尽的文档：故障树分析、FuSa 产品证书。

		Functional Safety-Capable	Functional Safety Quality-Managed	Functional Safety-Compliant
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***			✓

图 1-3. TI 在 FuSa 设计中的产品类别

** *可能仅适用于模拟电源和信号链产品。*

*** *适用于部分产品。*

功能安全手册 [3] 介绍了安全功能，并示出了如何采用外部元件来获得所需的故障覆盖范围和诊断功能。TI 的标准质量管理开发流程，如上所述，是该公司处理系统性和随机故障的过程。有关此过程的更详细说明，请参见 [3]。

1.3.2 用于安全 MCU 的 FuSa 配套资料

TI 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，可帮助用户打造需要确保功能安全的汽车应用。除了图 1-3 中符合功能安全标准的配套资料外，还提供了更多文档和软件库，以简化和加快 FuSa 设计。可以在 [4] 中找到 C2000 安全配套资料。

- 开发流程证书。QRAS-AP00210 的 TUV-SUD 证书。适用于符合 IEC 61508-2 和 ISO 26262-5 标准的元件的 FuSa 开发流程。
- C2000 安全包。应要求提供并需要签订保密协议。包内含有关于随机硬件功能的技术报告、有关系统功能的技术报告、FMEDA、器件概念评估、安全分析报告和器件特定的自检库包。
- 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。
- FuSa 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。
- 安全认证的 RTOS。预先认证的安全实时操作系统。
- 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。

2 OBC 系统的 FuSa 概念

本节概述了适用于板载充电器 (OBC) 应用的总体 FuSa 设计，并演示了 ISO 26262: 2018 年的开发流程如何在系统级别应用。讨论遵循在第 1.2 节中介绍的步骤顺序。

系统级 FuSa 分析在很大程度上取决于特定的使用场景和架构，由系统集成商负责。此次所示的示例仅用于培训目的，不得替代完整的生产级系统设计。

2.1 项目定义

2.1.1 项目功能

项目 是指经历安全生命周期的最高级别实体。在定义 OBC 时，说明必须指定 OBC 是什么，OBC 如何工作以及 OBC 如何与其他项目进行交互。OBC 用于从交流电网为高压 (HV) 电池充电，同时满足汽车标准定义的性能、安全和通信要求。

OBC 架构经过几代发展：

- 早期的设计是低功率 (≤ 3.3kW) 单向转换器，使用二极管整流器和升压转换器作为功率因数校正 (PFC) 级，然后是单独的 DC-DC 级。
- 下一代设计采用了图腾柱 PFC 级和双向 DC-DC 转换器级，将额定功率提高到 6.6kW，并增加了双向能力。图 2-1 所示为典型的单相双级 OBC 拓扑（左侧）和三相双级 OBC 拓扑（右侧），这些拓扑是当前市场中的主流拓扑。
- 最近的趋势是单级 OBC 拓扑，它减少了元件数量和成本，同时提供了更高的功率密度。该架构将 PFC 级和 DCDC 级合并成一个高频转换级。单级 OBC 拓扑也有众多不同的型号。图 2-2 示出了两种典型的单级 OBC 拓扑。左侧是交错式图腾柱单级拓扑，右侧是准单级拓扑。

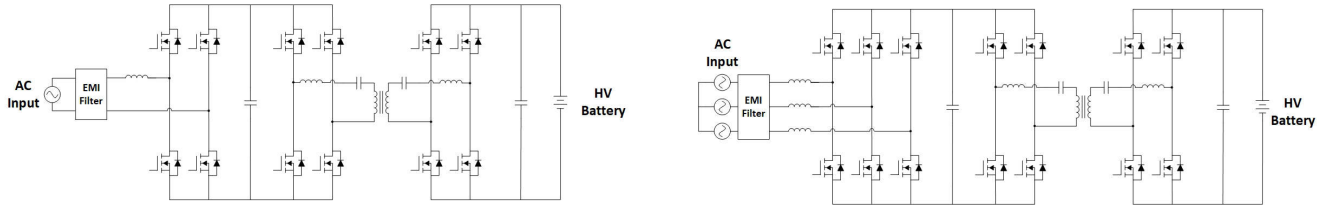

图 2-1. 双级 OBC 的方框图

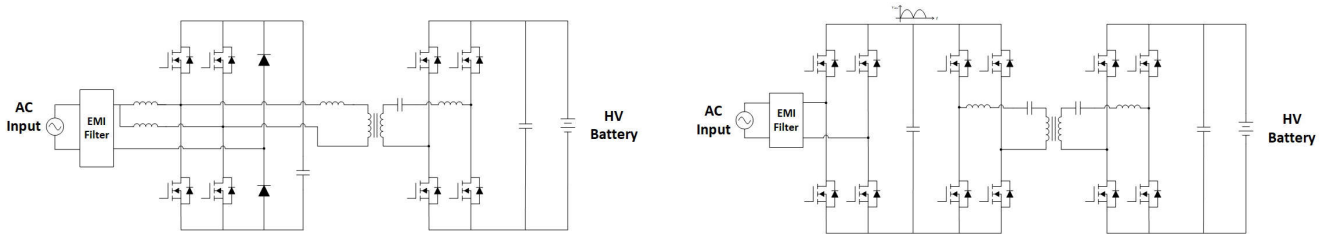

图 2-2. 单级 OBC 的方框图

尽管图 2-2 中的单级拓扑在市场上越来越受关注，但矩阵转换器目前被视为最出色的单级拓扑。图 2-3 示出了裕度调节电路的方框图。本应用手册以矩阵转换器为例进行进一步 FuSa 分析；但是，大多数分析也适用于单相和三相双级拓扑或其他单级拓扑。

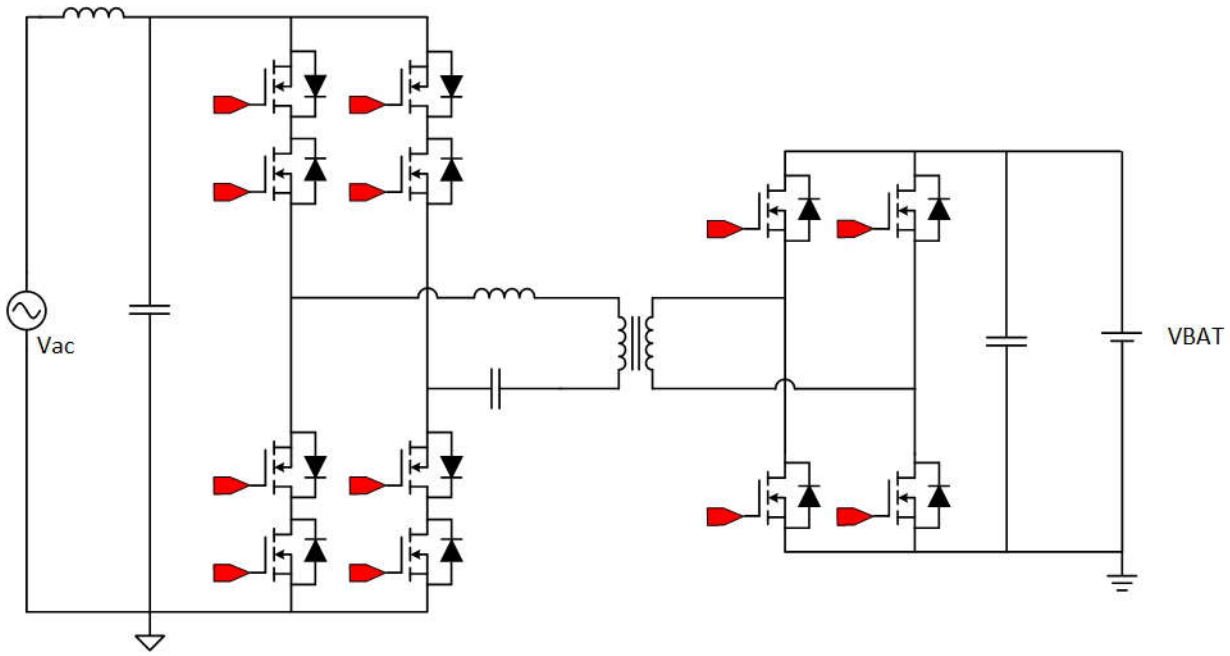

图 2-3. 矩阵转换器的方框图

总之，OBC 执行以下主要功能：

- 电源转换：OBC 执行电源转换时的功率级别符合充电站、电缆及电池的要求。
- 功率因数校正：OBC 将输入电流整形为正弦波形，使输入电流与电网电压对齐，并更大限度地减少输入电流的谐波。
- 输出调节：OBC 根据 BMS 设定点、温度限制和充电状态限制对电池充电电压和电流进行实时控制。
- 车联网 (V2X)：V2X 是 OBC 在反向模式下运行的统称，X 表示通信网络中的不同端点。车辆到负载 (V2L) 允许将车辆用作负载的移动电源。车辆到电网 (V2G) 允许车辆将电力返回至电网。车辆到车辆 (V2V) 支持将车辆用作移动电源来为其他车辆充电。车辆到住宅 (V2H) 使电动汽车能够在停电或电费较高期间为住宅供电。
- 电隔离：交流侧和高压直流母线之间的隔离。
- 保护：提供全面的电气故障、热故障及隔离故障保护。
- 通信：交流电源插座处的 CC/CP 信号。用于充电指令、模式选择及状态报告的 CAN 通信。
- 诊断：监控系统状态并报告任何故障情况。

由于拓扑是矩阵转换器，因此用于此安全目标的 FSC 具有几个独特的特性，有别于传统的两级 OBC。

- OBC 输出端的过流问题无法通过简单地关闭所有功率器件来解决。由于没有可用的续流路径，同时关闭每个电源开关会产生巨大的电压尖峰，这可能会损坏电源开关。因此，需要电源开关具有精密的关闭顺序。
- 交流侧电流可用做合理性检查。由于矩阵转换器不包含直流链路电容器，因此瞬态直流输出电流直接反映在交流侧电流中。相比之下，传统的两级 OBC 依靠直流链路电容器来提供瞬态直流电流。
- 更短的 FTTI。矩阵变压器拓扑以高得多的开关频率运行，因此通常需要使用 SiC 或 GaN 器件。与传统的硅开关相比，SiC/GaN 晶体管需要明显更快的电流保护响应，从而缩短允许的故障-容差时间间隔。
- 对于栅极驱动器，必须禁用两个通道之间的互锁功能，因为可以控制背对背电源开关来同时导通。不得错误触发栅极驱动器的 UVLO 功能，因为这也会导致没有续流路径的问题。

2.1.2 系统边界

系统边界定义了执行安全生命周期的*项目*的确切范围。这将属于安全相关系统（范围内）的所有内容与周围的车辆、基础设施或环境（范围外）区分开来。表 2-1 总结了系统边界。

表 2-1. 项目定义中的系统边界

系统边界	范围内	超出范围
电源转换	矩阵转换器 关键模拟元件	电网侧基础设施 外部连接器及保险丝
通信	与 AC 入口通信 连接到 BMS/VCU 的 CAN 接线	VCU 中的更高级车辆网络。BMS、电子锁、高压互锁（HVAC、HVDC）
环境	环境温度 冷却液温度	机械部件（冷板，接地）、湿度、EMC

2.1.3 外部接口

GBT 18487.1 — 2023 等多项标准定义了高压电池的整个充电过程。本章介绍了高压电池充电系统与 OBC 边界以外的其他系统之间的接口，该接口可作为 HARA 分析的输入。

在系统边界，接口还可以分为电源接口、通信接口和环境接口、如表 2-2、表 2-3 和表 2-4 所示。

表 2-2. 电源接口

电源接口	连接器	用途
交流输入	火线、零线、PE	提供主电压。规格：85V 至 265V，50Hz，最大 7kW
HV 直流输出	HV+、HV-	向电池组提供稳定的直流充电电压（250V 至 460V）和电流（典型值为 22A）。
电源	KL30	永久蓄电池正极端子/连接。

表 2-3. 通信接口

通信接口	连接器	用途
交流入口	CC、CP、充电枪温度	CP 承载 1kHz PWM *导频*，指示插入状态、最大电流能力和车辆就绪状态。 CC 承载用于充电器就绪和误差的低电平直流电流。
点火	KL15	开关式点火电源端子/连接。
BMS	CAN-H、CAN-L	交换蓄电池状态、充电限制及故障代码。
VCU	CAN-H、CAN-L	高级充电模式命令、充电设定点命令、安全状态请求、诊断请求。
测试引脚	硬接线，JTAG	调试期间使用的密钥。

表 2-4. 环境接口

环境接口	连接器	用途
散热接口	冷却液温度、环境温度	为电源开关、磁性元件、关键模拟器件及其他无源器件提供热管理。冷却液温度：-40°C 至 85°C 环境温度：-40°C 至 85°C

2.1.4 操作模式

单级 OBC 的行为被划分为若干种操作模式，这些模式由车辆液位控制器 (VCU/BMS) 或在检测到故障时通过内部逻辑进行选择。表 2-5 列出了单级 OBC 的主要操作模式。

表 2-5. 单级 OBC 的主要操作模式

操作模式	用例	状态
待机	正常驾驶，车辆待机	已禁用电源转换器。等待唤醒。
降额充电	蓄电池深度放电、蓄电池低温、蓄电池高温	根据电压和温度将充电电流限制为安全值。
AC 充电	标准充电。	将电池组电压和电流调节到 BMS 设定点。
再生	V2G、V2L、V2V、V2H	反向功率级运行。
维护	出厂诊断、固件更新	运行预定义测试模式。
紧急	检测到安全关键故障，通信中断	停止电源转换。向 VCU/BMS 报告故障代码。

操作模式还包含 OBC 的使用概况，不同客户的使用情况有很大差异。这包括充电频率、典型充电持续时间、特定充电场景及平均充电功率等因素。评估循环寿命对 HARA 至关重要。表 2-6 中示出了一个说明性的任务概况示例。

表 2-6. 单级 OBC 的说明性的任务概况示例

配置	值	理由
每日充电事件	1.5	家庭充电和工作场所充电。
平均充电时间	6h	隔夜或工作时间充电平均值。
平均功耗	7kW	单相充电桩的典型功率
使用寿命	8 年	更新车辆的典型频率
总计周期数	4380 个周期	对 5000 个周期进行四舍五入以进行安全评估

基于上述分析，图 2-4 给出了系统级方框图，其中包括主要元件和接口。

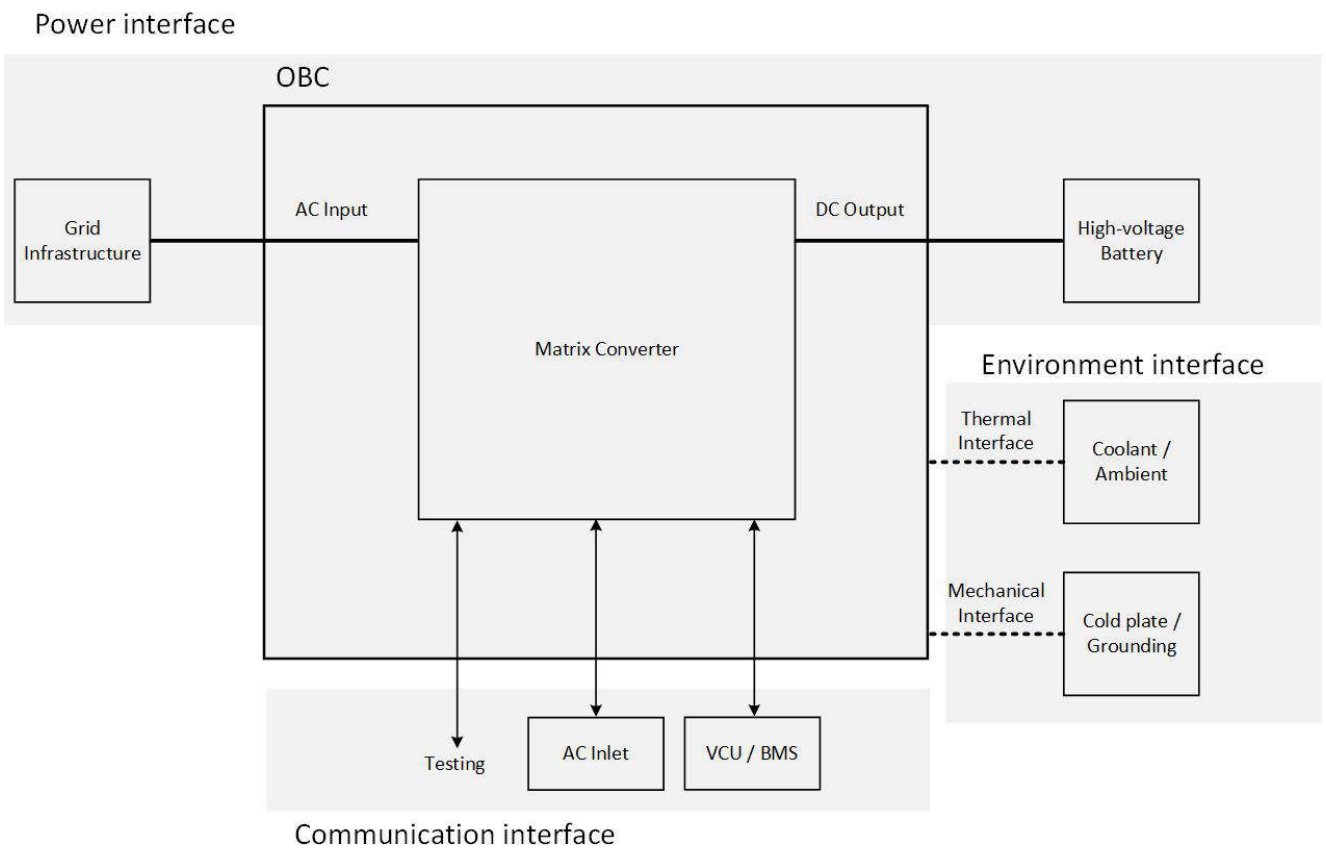

图 2-4. 项目定义级别系统方框图

2.2 功能安全目标

在进行 HARA 之前，采用以下简化假设来限制分析范围：

- 项目功能（第 2.1.1 节）：OBC 采用单级矩阵转换器拓扑，主要功能包括功率转换、电压调节、电隔离、保护、通信和诊断。
- 系统边界（第 2.1.2 节）：仅 OBC 系统在范围内；不包括 HV-LV DC-DC 转换器、PDU 和任何其他电子控制单元。
- 外部接口（第 2.1.3 节）：单个 MCU 控制 OBC。此 MCU 专用于 OBC 控制以及接合交流电源插座及 BMS/VCU。
- 操作模式（第 2.1.4 节）：主要功能是为高压电池充电，分析仅关注快速充电操作模式。

定义每一项的功能、流程和交互后，下一个阶段是 HARA。根据已建立的假设和分析，每个子系统中的任何错误行为都可能导致潜在的危险事件，例如直流过压、直流母线过流和热故障。

必须使用 ISO 26262 分别评估每种危险：2018 年严重性 (S)、暴露程度 (E) 及可控性 (C) 标准。以热故障为例：

- 严重程度：热故障的最严重后果是车辆起火，这可能会导致危及生命或致命伤害。因此，该事件被分配给 S3。
- 暴露程度：在 OBC 使用曲线中，充电器在车辆总运行时间的适度部分内处于活动状态。这对应于暴露等级 E3。
- 可控性：当车辆在充电过程中处于静止状态时，驾驶员可以立即中断充电电路（例如，断开充电器或打开接触器）。因此，该事件被视为 C2。

根据表 1-3，组合 S3 – E3 – C2 对应于 ASIL-B，因此热故障风险被指定为 ASIL-B。

关于直流母线过流，这不会对高压电池产生重大影响，因为高压电池的最大充电电流远高于交流充电的电流。但是，过流会导致 OBC 输出侧的功率器件过热并因短路而发生故障。短路故障后，高压电池会形成一条通过 OBC 的低阻抗路径，从而可能导致严重的系统过热，在极端情况下可能导致车辆火灾。暴露程度及可控性水平与热失效相同。根据表 1-3，组合 S3 – E3 – C2 对应于 ASIL-B，因此直流母线过流危险被指定为 ASIL-B。

对于直流母线过压，它会导致 OBC 输出侧的功率器件出现过压击穿，并且过压也会对高压电池上的锂离子电池造成危险，这会进一步导致系统过热，甚至导致车辆起火。暴露程度及可控性水平与热失效相同。根据表 1-3，组合 S3 – E3 – C2 对应于 ASIL-B，因此直流母线过压危险被指定为 ASIL-B。

需要分析所有危险事件。由于该评估通常由系统集成商执行，因此此处不介绍每种危险的详细评估。HAZOP 是一种系统危险分析方法，可提供 7 个指导词。表 2-7 示出了 HARA 分析的示例。HAZOP 引导词用于故障行为。

表 2-7. 单级 OBC 的 HARA 分析示例

ID	故障行为	潜在的车辆级别危险	S	E	C	ASIL
H1	热量超出预期	过热导致车辆起火	S3	E3	C2	B
H2	直流母线电流超出请求值	OBC 短路导致的车辆火灾	S3	E3	C2	B
H3	直流母线电压超出请求值	OBC 短路导致的车辆火灾	S3	E3	C2	B
H4	电气干扰更多	杂散控制信号	S1	E3	C2	QM

对于表 2-7 中从 ASIL A 到 ASIL D 的危险事件，必须至少确定一个安全目标。功能安全目标是满足安全状态要求的高层级、技术无关性陈述。

表 2-8 是 FuSa 目标的一个示例条目。FTTI 值必须得自危险分析和监管要求。以 SG1 为例，工作温度为 65°C，热故障临界温度为 155°C。对于一般温度上升速率 15°C / s，达到临界温度的时间为 6s。500ms FTTI 时间对于早期检测是保守的，以允许在级联故障之前进行早期干预。

表 2-8. 单级 OBC 的 FuSa 目标示例

ID	安全目标	ASIL	安全状态	FTTI
SG1	避免车辆因热故障而起火。	B	OBC 关断并切换至紧急操作模式。	由用户指定
SG2	避免由于直流母线过流而导致车辆起火。	B		
SG3	避免由于直流母线过压而导致车辆起火。	B		

安全状态要求规定了发生危险时必须触发的全系统响应。例如，SG1 至 SG3 的安全状态是 OBC 应切换到紧急操作模式，其中关键操作如下所示。与双级 OBC 不同，该架构不包含直流链路电容器，因此没有对直流链路电容器放电的操作。

- 按顺序禁用栅极驱动器。
- 打开所有接触器。
- 将 OBC 输出总线放电至安全电压。
- 记录故障状况。

2.3 功能安全概念

在制定 FuSa 目标后，下一阶段是开发 FSC。系统方框图如图 2-5 所示，它比项定义中的方框图深一级。目标是在初步架构图上定义子功能元素及互连。

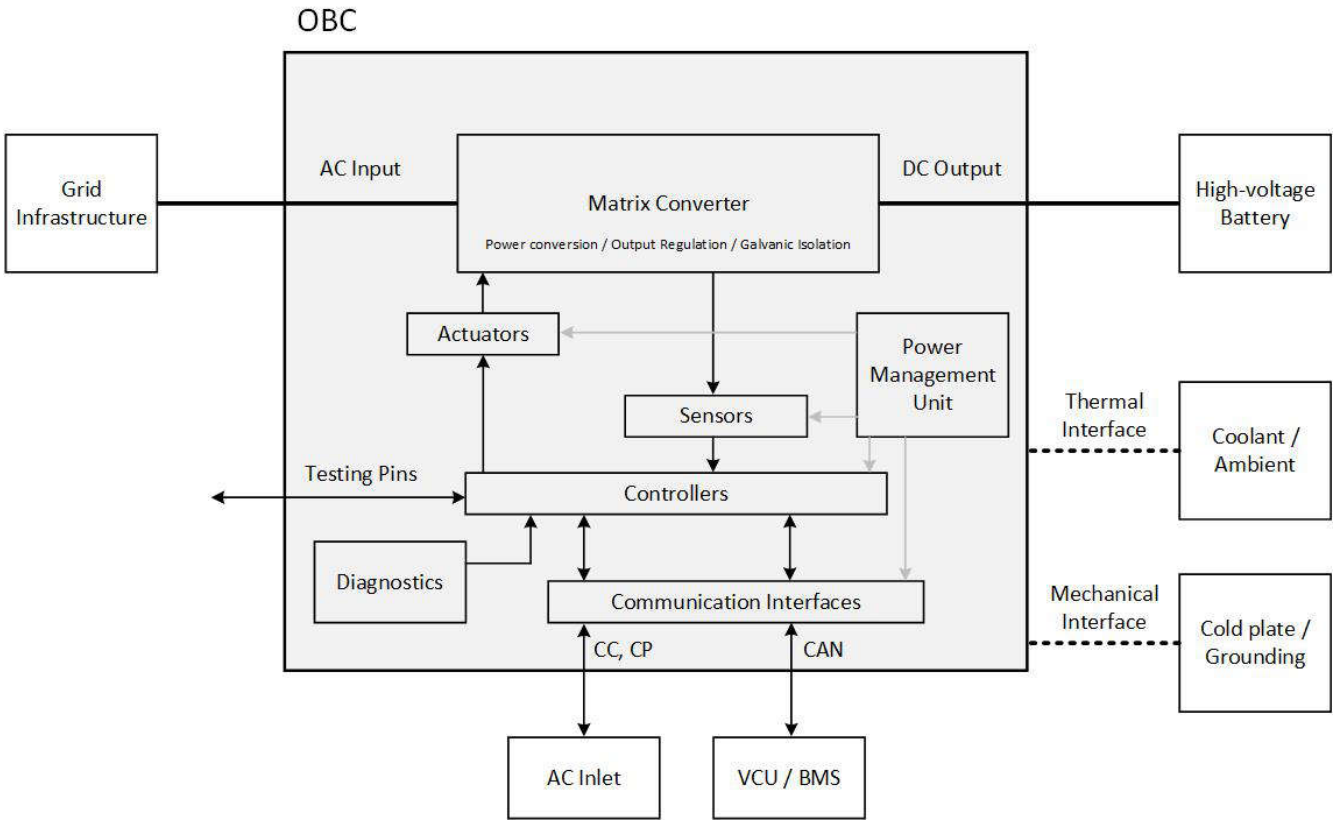

图 2-5. FSR 级系统方框图

为了简化分析，选择 SG2 作为示例。图 2-6 是与 SG2 相关的更深一级的方框图，相关子功能元素和交互在表 2-9 中进行了定义。

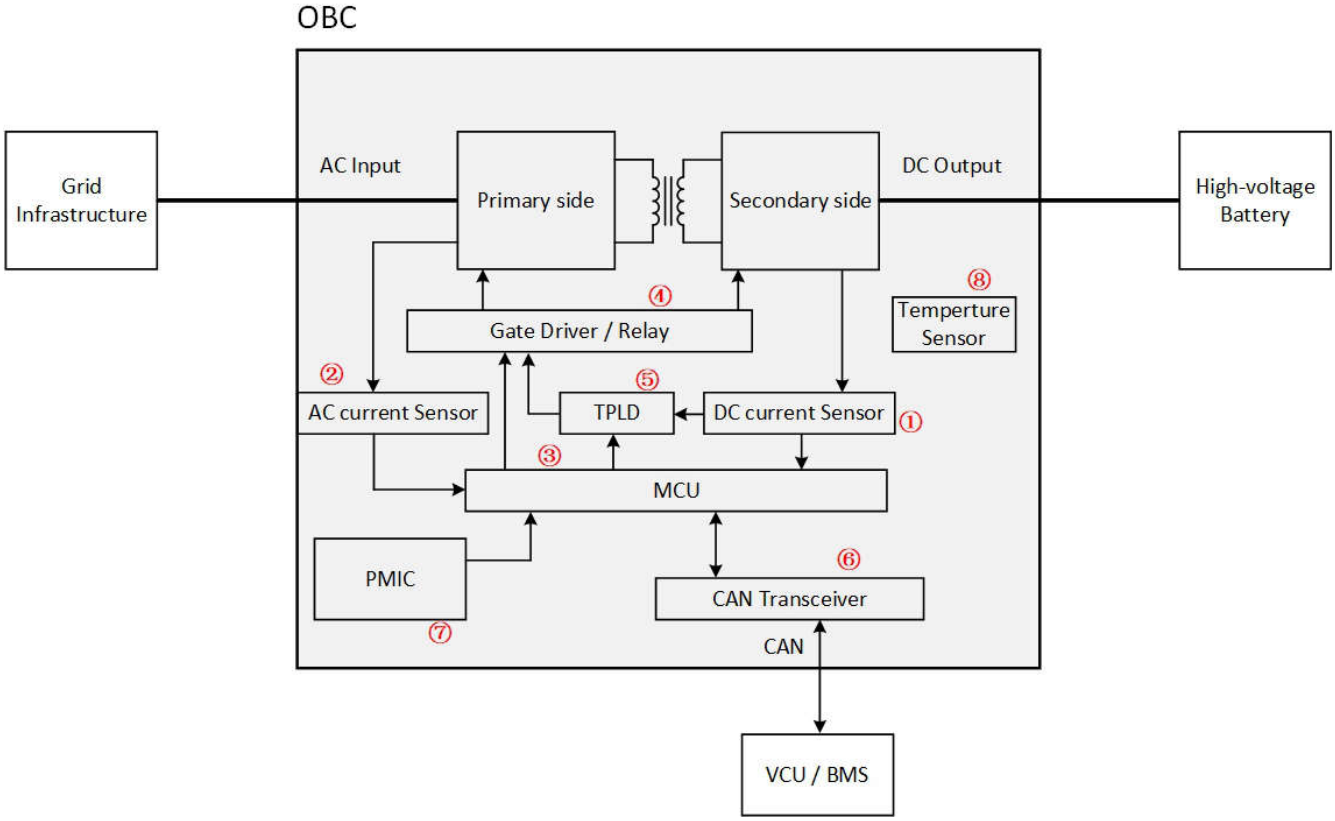

图 2-6. SG2 的 FSR 级系统方框图

表 2-9. SG2 的子功能元素及交互

元素 ID	元素名称	说明
E1	直流输出电流测量电路	测量用于恒流控制及过流保护的 OBC 输出电流。
E2	交流输入电流测量电路	测量 OBC 输入电流以进行交流电流控制及过流保护。
E3	微控制器电路	执行充电器控制算法、监控传感器数据、生成 PWM 信号并且与车辆的 BMS/VCU 通信。
E4	栅极驱动器电路	提供电源开关所需的电压和大电流驱动信号。
E5	TPLD 电路	可编程逻辑器件，其特征是具有组合逻辑的电源开关关闭序列。
E6	CAN 收发器电路	与 BMS/VCU 交换状态和诊断信息。
E7	PMIC 电路	为关键器件提供电源，并对关键电压轨进行电压监控。这也为 MCU 提供了外部看门狗及错误引脚监控器。
E8	温度测量电路	监测电源开关的结温、变压器温度及转换器的环境温度。

执行 FTA 以生成 SG2 的 FSR。FTA 分析分成三个步骤。第一步是创建将 SG2 违例作为顶部事件的故障树，然后第二步是推导定义的子功能元件的每个潜在故障，这些故障会导致顶部事件发生，接着第三步是使用逻辑门来表示事件之间的关系。

按照上述步骤，FTA 树如图 2-7 所示。必须确定关键故障路径以进行割集分析。如果 SPF 直接违反 FuSa 目标，则必须设计 FSR；如果 SPF 未直接违反 FuSa 目标，则有必要确定双点失效系统是否可接受并分析两点失效的独立性。

对于 SG 的 FTA 分析，在 FSR 级别，其可以在部件处终止，同时必须在 TSR 级别进行更详细的分析。如图 2-7 所示，如果存在电流检测异常、控制故障或电源问题，则违反 SG2。然后可以将其细分为不同的元件。

- 电流传感器故障或者用于过流保护的分立式比较器上的任何故障可能会导致电流检测不正确。

- 错误的控制命令可能会由许多元件引起。它可能是由于与 VCU 通信（充电命令不正确或无法报告故障状态）所导致。它可能由 MCU 发出的错误控制信号引起。它可能由栅极驱动器的驱动波形不正确造成。它可能由故障反应路径中分立式逻辑元件上的任何故障引起。
- 电源故障会导致关键元件发生故障，包括 MCU、栅极驱动器、传感器、电压基准。

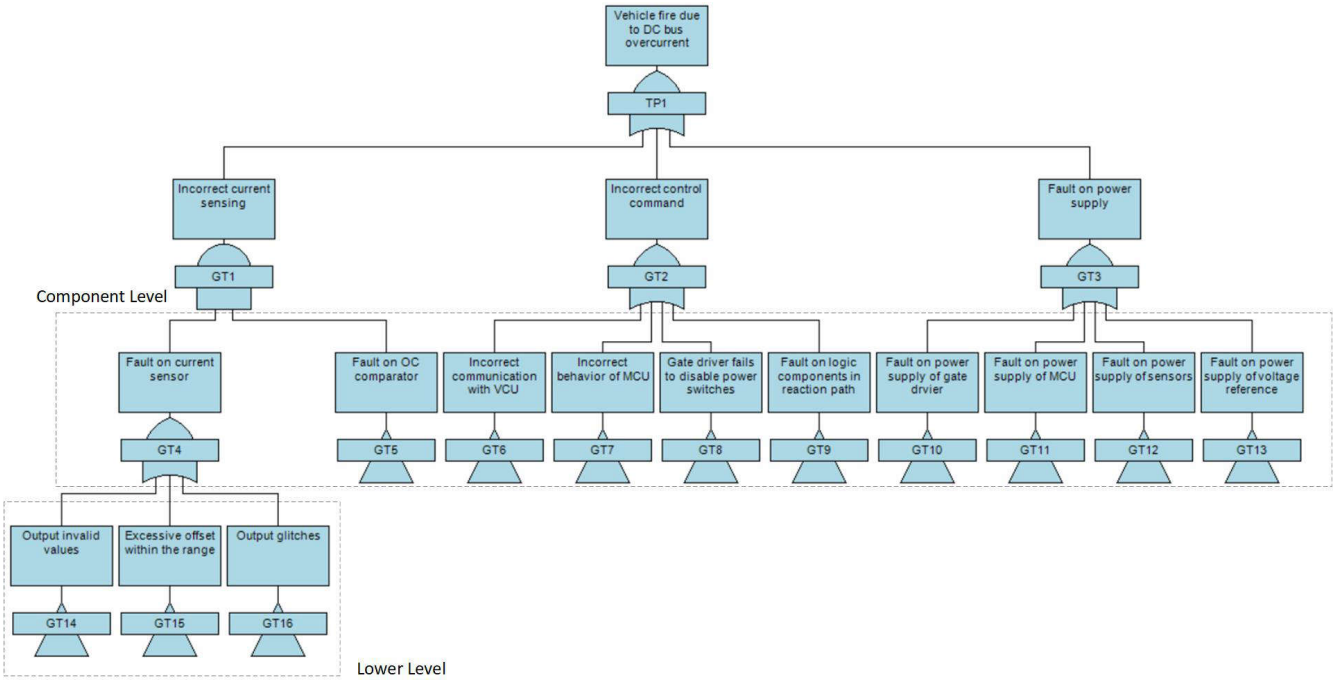

图 2-7. SG2 的 FTA 树示例

割集是一种逻辑分析，于确定导致顶部栅极条件失败的栅极/事件组合集。

- 1 阶割集。只有一个事件可以导致顶部事件发生。这些事件转换为具有 FTTI 要求的 FSR。
- 2 阶割集。同时发生的两个事件可能会导致最重要的事件发生。这些事件将转换成符合 MPFHTI 要求的 FSR。
- 2 阶以上割集。同时发生两个以上的事件可能导致最重要的事件发生。这些事件不会转换成 FSR。

每个 FSR 都必须分配至负责实现的逻辑块。如果 FSR 跨越多个块，则必须列出所有相关子系统。表 2-10 列出了一组简明的用于支持目标的 FSR，该目标即*避免由于直流母线过流而导致车辆起火*。

表 2-10. SG2 的示例 FSR

SG2：避免由于直流母线过流而导致车辆起火。					
ID	**FSR**	**安全状态**	**分配**	**ASIL**	**跟踪至**
FSR 2.1	直流总线电流检测系统应执行精确的电流测量。	将 OC 标志置为有效以发送至 MCU。	E1 及 SW	B	GT4
FSR 2.2	TCAN 应在 OBC 与 VCU 之间执行正确的通信。	将 OC 状态发送至 VCU。	E6 及 SW	B	GT6
FSR 2.3	MCU 应执行正确的控制方案。	切换到紧急操作模式。	E3 及 SW	B	GT7
FSR 2.4	栅极驱动器应当正确驱动电源开关。	禁用电源开关。	E4	B	GT8
FSR 2.5	辅助电源应向关键元件提供可靠电压。	提供可靠电压轨。	E7	B	GT3

2.4 技术安全概念

一旦 FSC 建立，下一阶段将创建 TSC。TSC 将 FSC 转换为具体的 TSR。建议执行 FMEA 来生成 TSR。对于关键元件，分析确认：

- 必须通过安全机制检测失效模式。

- 故障检测和安全状态转换的响应时间就已足够。
- 诊断覆盖率满足 ASIL 要求。

SG2 的 TSR 级别系统方框图如图 2-8 所示，比 FSC 架构更深一级。在图 2-8 中，设计了子功能元素的设计和互连。基本保护路径以红色表示。当发生过流时，来自电流传感器的 OC 标志会馈送到 MCU。在检测到 OC 标志时，MCU 会执行特定的关断序列，并会触发 PWM 以验证可靠关断。

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。故障路径可以分为三类：

- 单点故障 (SPF)：故障直接违反 FuSa 目标。
- 两点故障 (DPF)：当与另一个独立故障结合使用时，故障违反 FuSa 目标。
- 安全故障 (SF)：故障不能违反 FuSa 目标，该目标既可以被检测到，也可能在本质上安全。

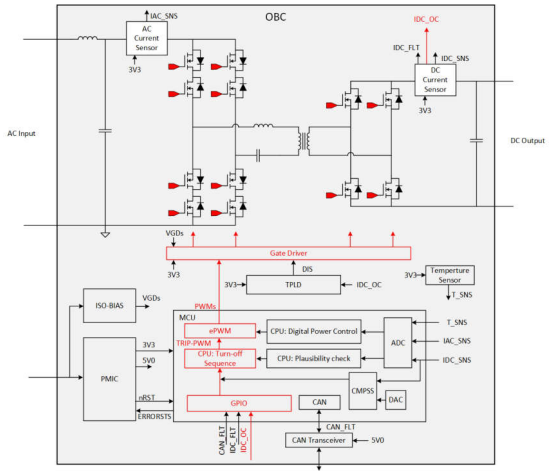

图 2-8. SG2 的 TSR 级系统方框图

对于可能违反 FuSa 目标（包括 SPF 和 DPF）的每个故障，都设计了一种安全机制。表 2-11 中列出了 FMEA 表。

表 2-11. FMEA 表的示例

系统子元件	主函数	失效模式	失效影响	SG 违规	故障原因	安全机制
直流输出电流测量电路 (E1)	OC 检测	OC 标志置为有效不正确	无法识别 OC 故障	SPF	OC 阈值设置或者 OC 信号链故障	来自 MCU CMPSS 模块的冗余 OC 标志。
		电流检测不正确	无法识别 OC 故障	DPF	VOUT 信号链故障。在这种情况下，前一个 SM 发生故障	交流侧电流传感器的合理性检查
CAN 收发器电路 (E6)	报告故障状态	通信故障	无法报告 OC 故障	SPF	CAN 总线故障或局部故障	TCAN 指示器标志
栅极驱动器电路 (E4)	驱动电源开关	无法禁用电源开关	直流总线短路	SPF	栅极驱动器或信号链故障	切断接触器
微控制器电路 (E3)	执行控制和保护	关闭顺序不匹配	电压应力会导致电源开关出现故障	SPF	CPU 延迟的 ISR 执行	用于禁用栅极驱动器的独立 TLPD 电路
微控制器电路 (E3)	执行控制和保护	数字输出或 PWM 信号不正确。	无法关闭电源开关	DPF	PWM 输出故障	PWM 输出冗余；PWM 环回检查
微控制器电路 (E3)	执行控制和保护	MCU 无法执行控制算法。	系统故障	SPF	CPU 延迟的 ISR 执行	PMIC 错误引脚监控和复位
PMIC 电路 (E7)	电压电源	电压误差	系统故障	SPF	降压/LDO 输出误差	过压和欠压监控

在表 2-11 中，安全机制一般可分为检测机制和控制机制。检测机制包括但不限于合理性检查、冗余检测、诊断测试及监测。控制机制涉及但不限于安全状态转换、故障反应、警告生成及系统关断。

对于 SG2 – *避免车辆因直流母线过流而起火*，以系统子元件直流输出电流测量电路为例。对于电流测量电路，电流传感器应具有 OC 输出功能，可在检测到过流时将 OC 标志置为有效。传感器必须有足够的带宽或者响应时间来捕获快速故障瞬变。

对于电流传感器 OC 功能上的 SPF，它可能会导致 OC 无法正确触发。最直接的方法是使用冗余过流检测电路。外部隔离式比较器可以用作第二个信号链。隔离式比较器的输出可以与电流传感器的 OC 输出进行逻辑或运算，因此可以覆盖电流检测电路上的 SPF。

但是，额外的元件会导致成本增加。MCU 中的比较器子系统 (CMPSS) 模块可以用作冗余 OC 检测。CMPSS 通过数字滤波选项来提供模拟比较功能。电流传感器的模拟输出被馈送到 CMPSS 模块，在与 MCU 内部的电压阈值进行比较后，这可以确定系统是否处于过流状态。在电流测量电路上，这种安全机制被定义为 SPF 的 SM1。

SM1 的前提是电流传感器的模拟输出是准确的，因此应监测电流传感器模拟输出的精度。这可通过合理性检查来实现。根据矩阵转换器输入和输出之间的瞬态功率平衡，可以将直流输出电流测量值与 OBC 交流输入上现有的电流测量值进行比较。考虑到交流电压下降或电池电压过低，合理性检查时必须比较输入和输出功率，而不是比较电流。在确定合理性检查的阈值时，还必须考虑无功功率和效率。交流侧传感器的读数提供了一个二次验证路径，而无需添加额外的直流总线传感器。在电流测量电路上，这种安全机制被定义为 DPF 的 SM2。

电流测量电路的安全机制如图 2-9 所示。

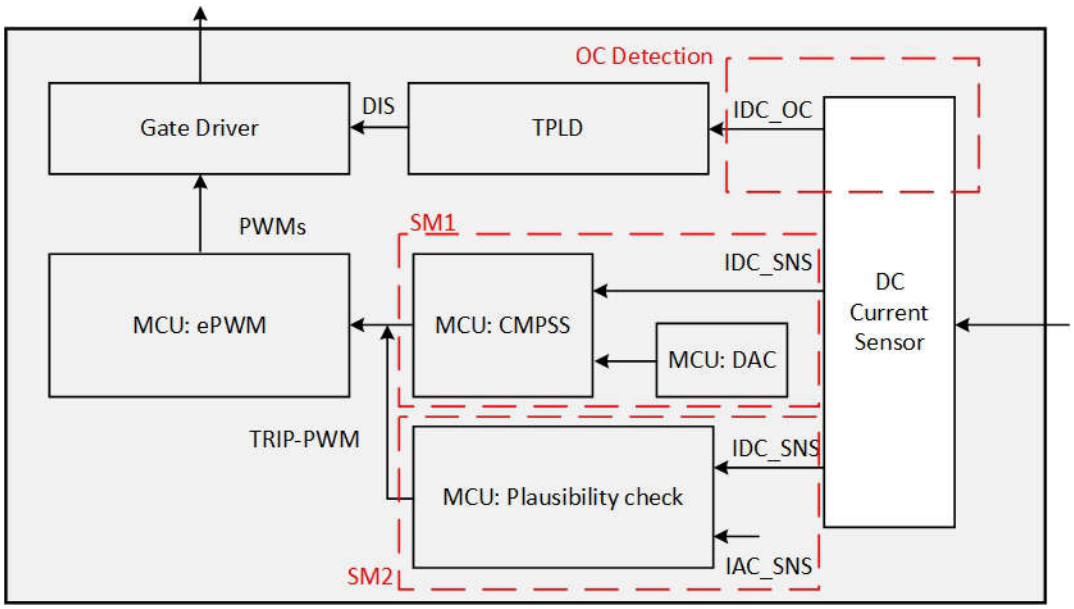

图 2-9. 电流测量电路上的功能机制

对于表 2-11 中的其他系统子要素，此处不详细分析；仅列出了一些功能安全机制。

- CAN 与 VCU 通信。对于 CAN 收发器，它应在 OBC 和 VCU 之间建立并保持可靠的双向通信。这个关键接口使 VCU 能够向 OBC 传输充电参数和命令，同时允许 OBC 向 VCU 报告运行状态和故障状态。
  - SM1：集成 CAN 收发器诊断。它使微控制器能够持续评估 CAN 收发器的运行状况及系统完整性。这些集成式诊断功能包括欠压检测、CAN 总线故障识别、软件看门狗计时器监控、电池连接检测、热保护、驱动器显性状态超时及全面的总线故障保护功能。
  - SM2：高级端到端 (E2E) 保护功能。它们在协议级别实现以检测潜在通信故障。这些技术包括通过 CRC 校验和进行的消息完整性验证、用于检测缺失消息的序列计数器，以及用于识别通信时序异常的时间戳。即使硬件级诊断无法直接检测某些故障情况，这种分层方法也会验证可靠的信息交换。
- 驱动器电源开关。对于栅极驱动器，它应在检测到故障时关闭电源开关，并且系统必须进入安全状态。通常对于 OBC 应用，使用没有自诊断功能的标准隔离式栅极驱动器。如果同时关闭电源开关，由于单级 OBC 没有续流路径，这可能会导致电源开关中出现明显的电压尖峰。

  - SM1：用于禁用栅极驱动器的独立 TLPD 电路。对于使用 PWM 关断的方法，如果信号链或输入引脚中有 SPF，电源开关关闭将违反指定的序列。TPLD 是一款可编程逻辑器件，具有电源开关和组合逻辑关闭序列。这种纯硬件路径独立于任何软件执行。TPLD 电路的输出端连接到栅极驱动器的 EN 引脚，因此可以涵盖 PWM 信号链上的 SPF。
  - SM2：切断接触器，作为独立的故障反应。如果驱动器的次级侧有 SPF，则无法可靠地关断电源开关。对于这种情况，通过关闭 OBC 输入和输出上的接触器，OBC 可以与输入和输出接口断开连接。
- 电压电源。PMIC 为关键元件提供电压电源。由于 PMIC 已经是符合 FuSa 标准的元件，因此安全手册中详细说明了 FuSa 机制。下面列出了一些和电压电源相关的典型 FuSa 机制。

- SM1：VSYS 上的冗余 OVLO/OVP 电压监控器。
- SM2：输出电压监测。
- SM3：残余电压检测。
- SM4：上电序列期间的 ABIST。
- SM5：VREG 和 VDD_1P8 上的冗余 UV/OVP 电压监控器。
- SM6：寄存器映射上的 CRC。
- MCU 执行控制和保护。由于 MCU 已经是符合 FuSa 标准的元件，因此安全手册中详细说明了 FuSa 机制。本应用手册的第 3.2 节将介绍一些相关安全机制。除了 MCU 的安全机制外，PMIC 还对 MCU 发挥监控作用。下面列出了一些典型的 MCU 监控相关 FuSa 机制。
  - SM1：MCU 错误监控器。
  - SM2：数字输出引脚回读（nINT/GPIO 和 GPIO）
  - SM3：实现独立的看门狗功能，以检测软件执行故障。

总之，采用多层安全机制来验证是否不违反这一安全目标。执行合理性检查和冗余，以提供可靠的故障识别。独立的保护路径为任何过电流事件提供纠正措施。全面的诊断验证在潜在故障成为安全关键故障之前的早期检测能力。

SPF 的安全机制必须转换为具有 FHTI 要求的 TSR，DPF 的安全机制必须转换为具有 MPFHTI 要求的 TSR。表 2-12 示出了与电流传感器相关的 FSR 的 TSR 示例。当多个 FSR 要求相同的硬件或软件功能时，相关要求将合并到一个 TSR 中。每个 TSR 都会继承源 FSR 的 ASIL-B，并且需要 FTTI 满足分组 FSR 中最严格的时序限制。

表 2-12. FSR 2.1 的 TSR 示例

FSR 2.1：直流母线电流检测系统应该执行精确的电流测量					
ID	TSR	分配	ASIL	安全状态	跟踪至
TSR-CS-1	直流母线电流传感器检测到的电流精度应在 2%以内（用于 SW OCP 及合理性检查）	电流传感器 Vout 引脚。	B	输入用户处理 SW	FSR2.1 - 电流检测
TSR-CS-2	直流母线电流传感器应执行自检，并在测试失败时报告故障。	电流传感器 FLT 引脚。	B	向 MCU 报告 FLT	FSR2.1 — 电流检测，OC 检测
TSR-CS-3	当电流比过流阈值高 20%时，直流母线电流传感器应将 OC 引脚置为有效。	电流传感器 OC 引脚。	B	向 MCU 报告 OC	FSR2.1 — OC 检测
TSR-CS-4	MCU 应对两个独立的电流传感器读数进行合理性检查，并在出现 >20% 的误差时标记故障。	MCU ADC 模块。	B	停止充电	FSR2.1 电流检测
TSR-CS-5	如果检测到 OC，MCU 应执行软件 OC 保护并禁用 PWM 输出。	MCU CMPSS 模块。	B	停止充电	FSR2.1 — OC 检测

所有 TSR 均可追溯至原 FSR，携带相同的 ASIL-B 分类，并遵循安全目标*避免由于直流母线过流而导致车辆起火*所要求的 FTTI。

2.5 硬件/软件安全要求

TSR 建立后，下一个阶段是将其转换为 HSR 和 FSR。每个 HSR/SSR 均继承其父 TSR 的 ASIL-B，并遵循组中限制性最高的 FSR 规定的 FTTI。HSR 定义了必须内置于电流检测前端的硬件特性；SSR 定义了必须对所测量信号执行的软件操作，以满足时序和检测标准。

依据表 2-12，电流传感器必须能够以足够的带宽或响应时间指示短路情况，并且还包括自我诊断功能。出于这些原因，在 OBC 应用中选择了 TMCS1133-Q1 作为电流传感器，并将其放置在 PFC 级的输入侧和 DCDC 级的输出侧。引脚图如图 2-10 所示。也可以使用另一种基于分流器的电流检测方法，但在这种情况下，HSR 和 FSR 是不同的，本文档不对此进行介绍。

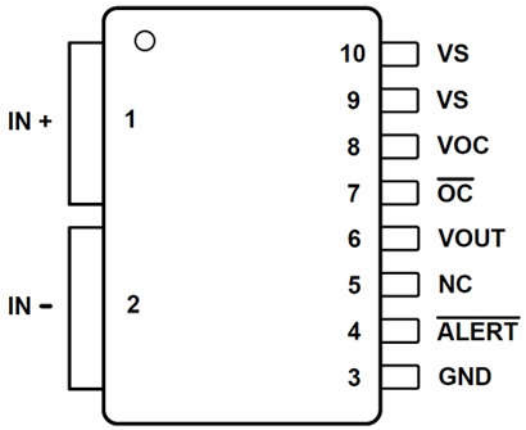

图 2-10. TMCS1133-Q1 引脚图

在表 2-12 中，TSR-CS-1、TSR-CS-2 和 TSR-CS-3 分配给电流传感器，TSR-CS-4 和 TSR-CS-5 分配给 MCU。表 2-13 和表 2-14 是实现这些追溯到 FSR 2.1 的 TSR 的 HSR 及 SSR 示例。

表 2-13. 追溯到 FSR 2.1 的 TSR 的 HSR 示例

ID	HSR	ASIL	跟踪至
HSR-CS-1A	霍尔传感器的带宽应大于 200kHz，VOUT 滤波器的截止频率也应大于 200kHz。	B	TSR-CS-1
HSR-CS-1B	霍尔传感器应具有至少 40A 的检测范围。	B	TSR-CS-1
HSR-CS-2A	霍尔传感器应具有用于自检的 FLT 引脚，并在 100ms 内向 MCU 报告故障。	B	TSR-CS-2
HSR-CS-2B	霍尔传感器 FLT 引脚应连接至 DSP 以报告故障。	B	TSR-CS-2
HSR-CS-3A	霍尔传感器 VOC 引脚应将 OC 阈值设置为比最大电流高 20%。	B	TSR-CS-3
HSR-CS-3B	当检测到过流时，霍尔传感器 OC 引脚应在 0.5us 内将 OC 标志置为有效。	B	TSR-CS-3
HSR-CS-3C	霍尔传感器 OC 滤波器的截止频率应该大于 1MHz	B	TSR-CS-3
HSR-CS-4A	交流侧电流传感器的 VOUT 应连接到独立 MCU ADC 通道。	B	TSR-CS-4

表 2-14. 追溯到 FSR 2.1 的 TSR 的 SSR 示例

ID	SSR	ASIL	跟踪至
SSR-CS-1A	MCU 应该以 100kHz 的频率对霍尔传感器输出进行采样。	B	TSR-CS-1
SSR-CS-1B	MCU 应该实现加电霍尔传感器偏移校准。	B	TSR-CS-1
SSR-CS-2A	MCU 应该根据 FLT 的占空比识别不同类型的警报。	B	TSR-CS-2
SSR-CS-2B	如果检测到传感器警报，MCU 应进行合理性检查	B	TSR-CS-2
SSR-CS-4A	MCU 应该以 10kHz 的频率执行合理性检查算法，以计算两个传感器读数的绝对差值	B	TSR-CS-4
SSR-CS-4B	如果连续三次采样的差值大于 20%，MCU 应该在 2ms 内将硬件故障置为有效	B	TSR-CS-4

表 2-14. 追溯到 FSR 2.1 的 TSR 的 SSR 示例（续）

ID	SSR	ASIL	跟踪至
SSR-CS-5A	MCU 应该将软件 OC 阈值设置为比最大电流高 10%	B	TSR-CS-5
SSR-CS-5B	MCU 应该根据 ADC 值使用 CMPSS 模块执行 OC 检测。	B	TSR-CS-5
SSR-CS-5C	如果检测到 OC，MCU 应该按特定顺序禁用 PWM 输出。	B	TSR-CS-5

这些只是一小部分说明性案例。在实际的 OBC 工程中，系统集成商必须对每个 TSR 进行全面分析，然后继续执行后续步骤。

- 设计分配。将每个 HSR 和 SSR 分配给相应的团队。
- 可追溯性矩阵。整合 FTA 或 FMEA 方框图，将 FuSa 目标链接到 FSR、TSR，然后链接到 HSR 和 SSR。每个 HSR 和 SSR 都应当与其验证证据相关联。
- 验证计划。HSR 及 SSR 的验证和确认。提供表明已满足相关要求并证明符合 ASIL-B 安全目标的测试报告。

在 OBC 系统中，一些模拟元件的 ASIL 等级为 QM。在 ASIL-B 系统中使用 QM 元件是可行的，但需要硬件元件评估。硬件要素评估表明 QM 元件不能干扰安全目标，或者额外的安全机制提供足够的诊断覆盖率来实现所需的 ASIL。

例如，TMCS1133-Q1 是一款支持 FuSa 的元件，选择该元件是为了满足 ASIL-B 要求。假设在直流输出侧将它用于电流检测和过流保护。TI 可提供以下内容来方便客户进行硬件元件评估。

- 所有失效模式。
- 每种失效模式的概率。
- 对于系统安全的影响。

所有上述信息都可在 TMCS1133-Q1 的 FuSa 文档中找到。客户应进行设计验证，包括分析和测试。所有故障模式均包括芯片失效模式与引脚失效模式。元件总时基故障率为 62，包括裸片时基故障率 (FIT) 26 和引脚时基故障率 (FIT) 36。表 2-15 中列出了所有芯片失效模式和分布。

表 2-15. TMCS1133-Q1 裸片失效模式及分布

裸片失效模式	失效模式分布 (%)
VOUT 开路（高阻态）	5
VOUT 卡滞（高电平或低电平）	30
VOUT 功能不在规格范围内	30
OC 误跳闸，跳闸失败	15
ALERT 误跳闸，跳闸失败	20

引脚故障模式主要包括典型的逐引脚故障场景：

- 引脚对地短路。
- 引脚开路。
- 引脚对邻近引脚短路。
- 引脚对电源短路。

以引脚对地短路为例，对潜在失效影响的说明如表 2-16 所示。失效影响类别指示这些引脚状况如何影响器件：

- A 类：器件可能会损坏，并使功能受损。
- B 类：器件未损坏，但功能丧失。
- C 类：器件未损坏，但性能下降。
- D 类：器件未损坏，功能和性能也未受到影响。

表 2-16. 器件引脚对地短路的引脚 FMA

引脚名称	引脚编号	对潜在故障影响的说明	失效影响类别
IN+	1	对于正向电流，绕过霍尔传感器，不会检测和放大信号。如果 IN+ 引脚具有高于 GND 的大电势，此状态会导致大量电流灌入。这可能会损坏输入电流系统电源、负载器件或实际器件，具体取决于布局和配置。	A
IN-	2	对于反向电流，绕过霍尔传感器，不会检测和放大信号。如果 IN-引脚处于高于 GND 的大电势，则此状态会导致大量电流灌入。这可能会损坏输入电流系统电源、负载器件或实际器件，具体取决于布局和配置	A
GND	3	正常运行。	D
ALERT	4	由于 ALERT 短接至 GND，因此无法触发警报	B
NC	5	正常运行	D
VOUT	6	输出被拉至 GND，并且输出电流受到短路限制。当处于此配置时，当 VS 连接到支持高负载的电源，并且在某些高负载条件下通过 IN+ 和 IN- 引脚时，芯片温度可能接近或超过 150°C。	A
OC	7	由于 OC 短接至 GND，因此无法触发警报。	B
VOC	8	GND 处的阈值意味着所有电压都触发警报。因此，警报卡在工作模式下。	B
VS	9	电源对地短路。	B
VS	10	电源对地短路。	B

应根据安全机制进行诊断覆盖率计算，以显示 >90% 的检测。此评估确定此硬件元件可充分支持分配给它的安全要求。

最后，开发团队有一套完整、可追溯和可验证的具体安全要求，可以在单阶段 OBC 中实施，并在 ISO 26262:2018 审核期间接受审查。

2.6 依赖性故障分析

应执行 DFA 来识别可能影响冗余的级联故障及共因故障。通过 DFA 分析确认了独立要求的其他 TSR。一般而言，DFA 分析确认：

- 物理分离。冗余元件具有足够的物理分离，冗余信号路径具有不同的路由，并且关键元件之间具有热隔离。
- 多元化。用于冗余功能的技术不同，关键元件的供应商不同，硬件和软件保护的实现方法不同。
- 独立。用于冗余电路的独立电源，用于冗余功能的独立处理，以及用于安全机制的独立激活路径。

例如，如果 MCU 的辅助电源对地短路，合理性检查将无法检测到故障，软件相关的安全机制也将失去其功能。在这种情况下，电压监测是验证 OBC 进入安全状态的关键安全机制。

3 OBC 系统的 FuSa 元件

本节旨在概述 OBC 系统中的各种 TI 功能安全元件，而不是设计满足特定功能安全目标所需的最低级别系统。因此，在下面介绍的元件中，并非所有元件都将在同一 OBC 系统中同时使用。

系统级 FuSa 分析在很大程度上依赖于特定的使用场景和架构。在以下各节中，将首先介绍所选元件的基本功能，然后介绍元件的安全特性。

3.1 元件概述

图 3-1 介绍了单级矩阵转换器的元件级架构。该图采用颜色编码，使不同的设计方面易于识别。

- 红色文本。硬件项的示例器件型号，通常在详细设计阶段选择。这些标识符仅为占位符；必须根据技术要求、尺寸及成本选择实际器件型号。
- 蓝色文本。蓝色标签突出显示了携带安全信号的引脚、冗余元件（双电压传感器）和诊断接口（自检、看门狗、奇偶校验）。通过标记这些引脚，利用该图可以直接将安全相关信号追溯到相应的 FSR。

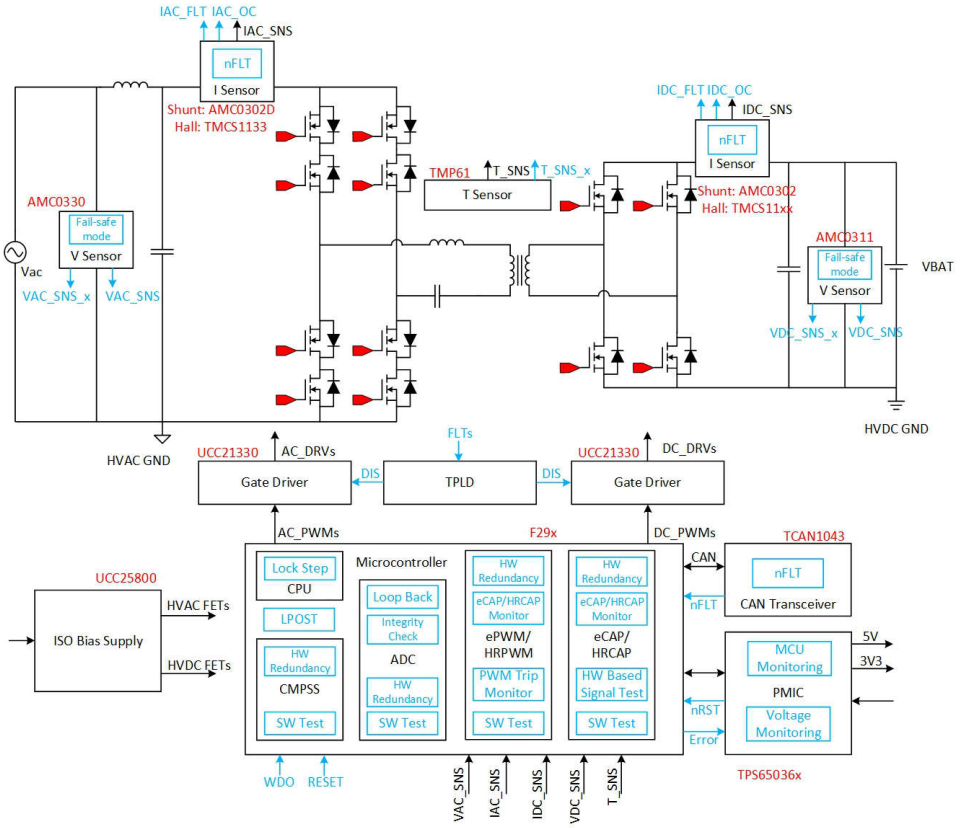

图 3-1. 单级矩阵转换器的元件级架构

在 OBC 应用中，除了电源开关和无源元件外，主要功能块还有微控制器、PMIC、栅极驱动器、电压传感器、电流传感器、温度传感器、隔离式和非隔离式辅助电源以及通信。

- 微控制器 (MCU)。执行充电器控制算法、监控传感器数据并同车辆上的 BMS/VCU 进行通信。在安全关键设计中，MCU 通常是一个双核器件，具有专用的 MCU 内部看门狗和自诊断功能。
- 电源管理 IC (PMIC)。管理和控制多种电源功能，包括电压转换、电源时序、监控、保护和通信。PMIC 为其他器件供电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。在检测到 MCU 发生不可恢复的故障时，PMIC 可以触发 MCU 复位并切断相关控制，从而使系统保持在安全状态。
- 系统基础芯片。与 BMS/VCU 交换状态和诊断信息。安全关键消息通过 CRC 和消息计数器检查进行传输，以验证完整性。
- 电源和监控器。隔离式辅助电源产生栅极驱动器电压，并在保持电隔离的同时为检测电路的高压侧供电。在无需电隔离的情况下，非隔离式辅助电源为低电压元件供电。

- 栅极驱动器。提供电源开关所需的电压和大电流驱动信号。对于隔离式栅极驱动器，此项还提供低压信号和高压侧之间的电隔离。驱动器的内置保护功能用于满足系统的 FuSa 要求。
- 电压传感器。以足够的分辨率测量交流输入电压和直流母线电压，以检测过压或欠压事件。传感器输出可以路由到 MCU 和安全监控逻辑。
- 电流传感器。检测交流输入电流和直流总线电流，并实现过流保护。典型的实现方式包括具有 OC 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。
- 温度传感器。监测电源开关的结温、变压器温度及转换器的环境温度。可实施冗余温度传感器以满足 FuSa 要求。

3.2 微控制器

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 3 个 C29x CPU（支持锁步功能），在 200MHz、4000kByte 闪存、452kByte RAM 上运行，支持 5 个 SAR ADC、多达 36 个通道 PWM 输出和 QFP-144/QFP-176/BGA-256 封装。它符合 ISO 2626 **2** 和 IEC61508 标准，可确保符合高达 ASIL-D/SIL3 的安全要求。它具有先进的功能和丰富的连接选项，可提供全面的设计。用于 OBC 应用的 MCU 中的主要安全特性包括以下方面。

3.2.1 CPU

嵌入式 CPU 支持多种指令大小（16/32/48 位）。CPU 还支持可变指令包大小，每个指令包可包含多达 8 条并行执行的指令。例如，CPU 架构能够并行执行多达 8 条 16 位指令。这由 CPU 内可以同时执行的多个功能单元实现。内核 1 及内核 2 能够在分离锁定模式或锁定步进模式下独立执行。

- 使用锁步比较模块 (LCM) 的硬件冗余。锁步比较模块 (LCM) 用于实现锁步比较功能并指示误差。
- LCM 的自检逻辑。LCM 自检逻辑专为锁步比较器而设计。比较器的自检有两种不同的模式：匹配测试及失配测试。启动自检时，会依次在两个比较器上执行两种不同的测试模式。
- 内部看门狗 (WD)。提供两种模式选择的看门狗功能，即普通看门狗 (WD) 和窗口式看门狗 (WWD)。
- 逻辑开机自检。LPOST（逻辑开机自检）在启动及应用期间在晶体管级为器件提供高诊断覆盖率。为了快速执行高质量的制造测试，LPOST 采用插入器件的可测性设计 (DFT) 结构，但是使用的是一个内部测试引擎而非外部自动测试设备 (ATE)。LPOST 测试由 BootROM 根据 SECCFG 用户输入触发。

3.2.2 ADC 采样

F29H859TU-Q1 MCU 上集成了高性能模拟块，可进一步支持系统整合。三个独立的 12 位 SAR ADC 和两个独立的 16 位/12 位可选 SAR ADC 可以准确、高效地管理多个模拟信号，最终提高系统吞吐量。四个模拟比较器模块可以针对跳闸情况对输入电压电平进行持续监控。对于 ADC 支持的主要安全机制如下。

- DAC 至 ADC 环回检查。可以使用 ADC 监测 DAC 输出来检查 ADC 的完整性。DAC 可以配置并输出一组预先确定的电压电平。这些电压电平可由 ADC 测量，并对照预期值进行交叉检查，以验证 ADC 是否正常工作。
- ADC 输入信号完整性检查。可以对 ADC 转换混合使用硬件和软件运行时诊断来检查 ADC 输入信号的完整性。可以借助内置硬件机制及软件可配置阈值来验证输入信号的合理性检查。可以使用 ADC 后处理块对转换结果进行合理性检查。
- 使用 ADC 安全校验器实现硬件冗余。使用 ADC 的多个实例来对同一输入进行采样并同时执行相同的操作，然后对输出值进行交叉检查。基于硬件的结果安全校验器模块，在两个结果都可用时自动比较主 ADC 和冗余 ADC 的结果。
- 包括错误测试在内的功能软件测试。支持在 ADC 模块及后处理块上运行功能测试或故障注入测试。可以由外部电路或内部 DAC 在 ADC 输入引脚上提供一组预定的电压电平。可以将转换结果与预期值进行比较，以检查 ADC 模块和后处理块的功能正确性。
- 逻辑开机自检。LPOST（逻辑开机自检）在启动及应用期间在晶体管级为器件提供高诊断覆盖率。为了快速执行高质量的制造测试，LPOST 采用插入器件的可测性设计 (DFT) 结构，但是使用的是一个内部测试引擎而非外部自动测试设备 (ATE)。LPOST 测试由 BootROM 根据 SECCFG 用户输入触发。

3.2.3 PWM 生成

F29H859TU-Q1 器件包含先进的控制外设，这些外设具有 36 个增强型脉宽调制器 (ePWM) 通道，所有这些通道都具有高分辨率功能 (HRPWM)。增强型捕捉 (eCAP) 模块可实现对于系统的出色控制。内置的 Σ-Δ 滤波器模块 (SDFM) 允许在隔离层上无缝集成过采样 Σ-Δ 调制器。

- 硬件冗余。对于 PWM，可以通过多通道并联并通过内部或外部比较器比较输出来实现硬件冗余。对于 eCAP、SDFM，可以让外设的多个实例对相同的输入进行采样并同时执行相同的操作，然后对输出值进行交叉检查，以此来实现硬件冗余。
- 通过 eCAP/HRCAP 监控 ePWM/HRPWM。可以通过输入捕捉外设（如 eCAP/HRCAP）来监测 ePWM/HRPWM 输出是否正常运行。捕获的脉冲宽度可用于构建附加诊断，供用户实施以检测 PWM 的上升沿和下降沿以及时间戳信息。当 eCAP/HRCAP 用作 PWM 诊断时，可通过定期测量 ePWM/HRPWM 脉冲宽度来测试。
- 在线 MINMAX 监测跳闸事件。支持在配置的时间窗口内检测跳闸事件的发生。该窗口由 XMINMAX 寄存器组中配置的 MIN 和 MAX 值配置。
- 使用最小死区逻辑避免故障。最小死区逻辑可配置成验证两个 PWM 通道的有源脉冲相位和跨 PWM 实例之间的最小无源间隙（死区）。
- 硬件冗余以及使用 WADI 的输出比较。波形分析仪和诊断 (WADI) 外设包含许多有用的内置信号分析支持，同时为信号提供安全机制。WADI 能够对单个信号执行以下检查，或在两个信号之间执行检查：脉宽测量、频率测量、相位重叠测量、死区测量。
- 包括错误测试在内的功能软件测试。支持在 ePWM 模块上运行功能测试或者故障注入测试。可以通过使用 PWM 提供适当的激励并使用其中一个捕获（时间戳）模块 (eCAP) 观察响应来测试各个子模块，以检查 eCAP 或 ePWM 模块的功能正确性。
- 使用信号监控进行错误检测。基于硬件的信号监控单元能够测量 eCAP 输入信号的边沿、脉宽和周期，以检查此事件是否发生在可编程预期范围内。
- 逻辑开机自检。LPOST（逻辑开机自检）在启动及应用期间在晶体管级为器件提供高诊断覆盖率。为了快速执行高质量的制造测试，LPOST 采用插入器件的可测性设计 (DFT) 结构，但是使用的是一个内部测试引擎而非外部自动测试设备 (ATE)。LPOST 测试由 BootROM 根据 SECCFG 用户输入触发。

3.2.4 CMPSS

CMPSS 由模拟比较器和配套元件组成，它们组合成一种拓扑结构，可用于峰值电流模式控制、开关模式电源、功率因数校正和电压跳变监测等电源应用。使用 ePWM 进行有源同步整流，有源同步整流可实现更高的效率。

- 硬件冗余。对于 CMPSS，可以通过使用多通道并行输出或输入比较来实现硬件冗余。
- 包括错误测试在内的功能软件测试。支持在 CMPSS 关键寄存器或者关键特性上运行功能测试或故障注入测试。在用户读回寄存器值并与预期值进行比较后，可以将一组预先确定的模式写入寄存器。通过调整滤波器阈值，检查输出是否跟随滤波器变化，从而实现关键 CMPSS 功能检测。
- 逻辑开机自检。LPOST（逻辑开机自检）在启动及应用期间在晶体管级为器件提供高诊断覆盖率。为了快速执行高质量的制造测试，LPOST 采用插入器件的可测性设计 (DFT) 结构，但是使用的是一个内部测试引擎而非外部自动测试设备 (ATE)。LPOST 测试由 BootROM 根据 SECCFG 用户输入触发。

3.2.5 数据传输

通过各种业界通用通信端口（例如串行外设接口 (SPI)、串行通信接口 (SCI)、集成电路总线 (I2C) 和控制器局域网 (CAN)）支持数据传输，并提供了多个多路复用选项，可在各种应用中实现出色的信号布局。

- 包括端到端安全状态恢复的信息冗余技术。模块通信收发器或物理层被视为“黑盒”，任何通信收发器或物理层相关故障都可通过通信协议 E2E 保护（包括附加消息校验和、序列计数器和时间戳等）间接检测。信息冗余技术可使用软件提供附加的运行时诊断。软件可以应用许多技术，例如回读写入值和多次读取同一目标数据并比较结果。
- 逻辑开机自检。LPOST（逻辑开机自检）在启动及应用期间在晶体管级为器件提供高诊断覆盖率。为了快速执行高质量的制造测试，LPOST 采用插入器件的可测性设计 (DFT) 结构，但是使用的是一个内部测试引擎而非外部自动测试设备 (ATE)。LPOST 测试由 BootROM 根据 SECCFG 用户输入触发。

3.2.6 故障信号监控及安全状态控制

安全 MCU 检查远程传感器数据的完整性，控制电池电量。当检测到异常情况时，系统将进入安全状态。

3.3 电源管理 IC

TPS650365-Q1 器件是一款高度集成的电源管理 IC。此器件包含三个降压转换器和一个低压降 (LDO) 稳压器。所有转换器都可以在强制固定频率 PWM 模式或自动 PFM 模式下运行，并支持可选的展频调制 (SSM) 以降低

EMI。TPS650365-Q1 还支持低功耗模式。这些灵活的功能适合 MCU 电源应用。符合 ISO 26262: 2018 和 IEC61508: 2010 标准，确保符合高达 ASIL-B/SIL2 的安全要求。采用 VQFN-24 封装。用于 OBC 应用的 PMIC 中的主要安全特性包括以下方面。

3.3.1 MCU 监测器

TPS650365-Q1 元件可监控模块安全 MCU 的硬件及软件操作。对于安全 MCU 硬件和/或软件执行失败模式，PMIC 会根据所检测到故障的严重等级产生不同的反应，包括中断 MCU、关闭外部功率级和模块通信接口，如果故障仍然超过阈值，则会重新启动安全 MCU。

- 看门狗。通过三种可选模式提供外部看门狗功能：输入触发模式、软件触发模式及问答 (Q&A) 模式。
- 错误信号监测器 (ESM)。在 MCU 配置 ESM 后，TPS650365-Q1 器件可以通过 nERR 输入引脚监控 MCU 错误输出信号，并使用起始位启用此项。ESM 支持两种操作模式：电平模式和 PWM 模式。

3.3.2 关断序列

在检测到 PMIC 或 MCU 中不可恢复的故障时，TPS650365-Q1 元件可以提供关断序列。该元件进入 RESET-MCU 状态并将 RESET 引脚输出驱动到 MCU，然后控制处于复位状态的安全 MCU。相应地切断 MCU 输出控制。

3.3.3 电源

TPS650365-Q1 元件可监控 PMIC 内部电压、输入和输出电压，并提供内部诊断功能。

- 电压监控器。通过与基准电压进行比较，持续监控 TPS650365-Q1 的输入电源电压和内部稳压输出电压是否发生欠压和过压事件。当电压超出范围时，稳压器关断，状态机跳至故障处理状态。注意：所有稳压器都具有限流电路，可保护内部功率 MOSFET 免受过流事件的影响。
- ABIST。在上电时以及按需为所有稳压电源提供模拟内置自检 (ABIST) (如果启用) 。

如电源管理 IC 中所述，PMIC 代表了一种完全集成的设计，可为 OBC 系统提供电源和电压监控功能。或者，可以在不使用 PMIC 的情况下实施分立式方法。在分立式配置中，系统基础芯片或单个 LDO 稳压器为 MCU 供电，而单独的监控电路或看门狗器件负责系统监控功能。第 3.4 节介绍系统基础芯片，第 3.5 节将讨论电源单元和监控电路。

3.4 系统基础芯片

TCAN1164-Q1 是一款高速控制器局域网 (CAN) 系统基础芯片 (SBC)，符合 ISO 11898-2:2016 CAN 灵活数据速率 (FD) 规范对物理层的要求。该收发器支持传统 CAN 和 CAN FD 网络 (数据速率高达八兆位/秒 (Mbps)) 。TCAN1164-Q1 支持宽输入电源电压范围，并且集成了 5V LDO 输出。5V LDO 输出 (VCCOUT) 可在内部为 CAN 收发器提供电压，并在外部提供额外电流。

TCAN1164-Q1 使用德州仪器 (TI) 公司质量管理型产品开发流程开发而成，符合 AEC Q100 1 级标准。该流程属于 TI 的功能安全质量管理型产品类别。TI 建议通过*硬件元件评估*策略将该元件集成到系统中 (ISO 26262-8：2018，第 13 条) 。

TCAN1164-Q1 与系统连接，如下所述：

- TCAN1164-Q1 从 VSUP 引脚上的非 ISO 辅助电源接收 5V 电源。
- TCAN1164-Q1 集成了一个 5V LDO (VCCOUT)，为内部 CAN 收发器和外部器件供电。
- TCAN1164-Q1 通过四个 SPI 引脚连接至 MCU。主机 MCU 使用这些引脚来配置 TCAN1164-Q1 并定期为看门狗提供服务。
- TCAN1164-Q1 通过 CANH 及 CANL 引脚连接到外部 CAN 总线，并通过 TXD 和 RXD 引脚连接到 MCU 以实现 CAN 总线通信。

因此，潜在故障点和安全机制侧重于 CAN 通信、电源电压轨监控、SPI/处理器通信以及内部存储器，从而满足功能安全应用的要求。

3.4.1 CAN 通信

以下是涵盖 CAN 通信的功能安全机制。

- CAN 协议：在 MCU 中实现了 CRC 校验和的 CAN 协议可以检测并处理任何通信错误

- CAN 总线故障诊断：TCAN1164-Q1 提供先进的总线故障检测电路，用于监测 CANH 和 CANL 引脚，并确定是否存在对电池短路、对地短路、相互短路或开路故障。
- TSD：TCAN1164-Q1 具有热关断警告和热关断 (TSD) 保护功能，可禁用 CAN 收发器。
- CAN 总线短路限制器：该器件在 CAN 总线的线路短路时限制短路电流。

CAN TXD 引脚显性状态超时：该器件支持主导状态超时 (DTO)；该器件防止本地节点在硬件或软件故障的情况下阻止网络通信，其中 TXD 保持主导（低电平）的时间长于超时时间。

3.4.2 电源电压轨监控

TCAN1164-Q1 中监测了两个电压轨：VSUP 及 VCCOUT。VSUP 是 TCAN1164-Q1 的输入源，VCCOUT 是用于 CAN 收发器和外部电源的 LDO 输出。一旦检测到电源故障，器件就会进入待机模式或失效防护状态。涵盖电源电压轨的安全机制包括：

- VCCOUT LDO 短路电流保护
- VSUP 电源欠压检测 (UVSUP)
- VCCOUT 欠压检测 (UVCCOUT)
- VCC 过压检测 (OVCCOUT)

3.4.3 SPI/处理器通信

TCAN1164-Q1 通过多种方法来确定处理器和器件之间的通信是否正常运行。

- 看门狗：器件提供基于默认窗口的看门狗以及使用 SPI 接口的可选超时和问答 (Q&A) 看门狗。
- SPI 通信错误指示符：如果在一个 SPI 事务期间没有移入正确数量的时钟周期和数据，则会在专用寄存器处设置中断。
- 暂存区写入/读取：该器件提供了一个专用寄存器，可以对其进行写和读回，以验证与寄存器空间的 SPI 接口。

3.4.4 器件内部 EEPROM

TCAN1164-Q1 使用内部 EEPROM 进行特定性能修整。加电时，器件会从 EEPROM 加载内部寄存器并执行 CRC 校验。当用于修整的内部 EEPROM 存在 CRC 错误时，便会设置 CRC_EEPROM 中断。

3.5 电源和监控器

本节介绍了采用两款 TI 功能安全型器件（组合 TPS3850-Q1 监控器的 LM5155-Q1 升压控制器）来满足系统 ASIL-B 要求的 TI 设计。

LM5155-Q1 用于为安全 MCU 输出 3.3V 电源。将 MCU 的电源保持在推荐的工作范围内对于防止 MCU 进入不安全状态至关重要。因此，需要监控 3.3V 电源输出是否存在电源欠压或过压等故障。如果发生 OV 或 UV，则需要重置 MCU 以关闭系统并将系统转换为安全状态。

为了检测 3.3V 电源 OV/UV 故障模式，建议的设计使用外部监控器来监测电源输出。监控器与电源输出无关，因此不会出现共因失效。鉴于监控器的高性能和准确性，电源过压和欠压的诊断覆盖率很高。

在此 OBC 系统中，TPS3850-Q1 是一款带有集成式窗口看门狗的窗口电压监控器，可用于监控 3.3V 电源轨。检测到电源故障时这会将安全 MCU 复位至安全状态。

3.6 栅极驱动器

在典型的 OBC 应用中，栅极驱动器需要用于防止意外的导通事件以及高侧和低侧开关中的直接击穿。UCC21330-Q1 是一款隔离的双沟道栅极驱动器，具有 4A 峰值源极和 6A 峰值吸收电流，用于驱动功率 MOSFET、SiC、GaN 和 IGBT 晶体管。

UCC21330-Q1 的保护功能包括：电阻器可编程死区时间、同时关闭两个输出的禁用功能以及可抑制短于 5ns 的输入瞬态的集成抗尖峰脉冲滤波器。所有电源都有 UVLO 保护。INA 及 INB 引脚上的内部弱下拉可验证输出在默认情况下是否为安全状态低电平。设置为高电平时 DIS 引脚会同时禁用两个驱动器输出，而设置为低电平时则会启用两个输出。如果检测到故障状态，微控制器或其他模拟比较器置位的全局 DIS 将同时禁用所有驱动器。

为了防止在动态开关期间高侧和低侧 FET 直接击穿，可以通过将 0Ω 放置到 150Ω 电阻器或将 DT 引脚短接至 GND 以让两个输出互锁来启用互锁功能。如果两个输入同时都处于高电平，则两个输出都将立即被设为低电平。图 3-2 可说明该功能。

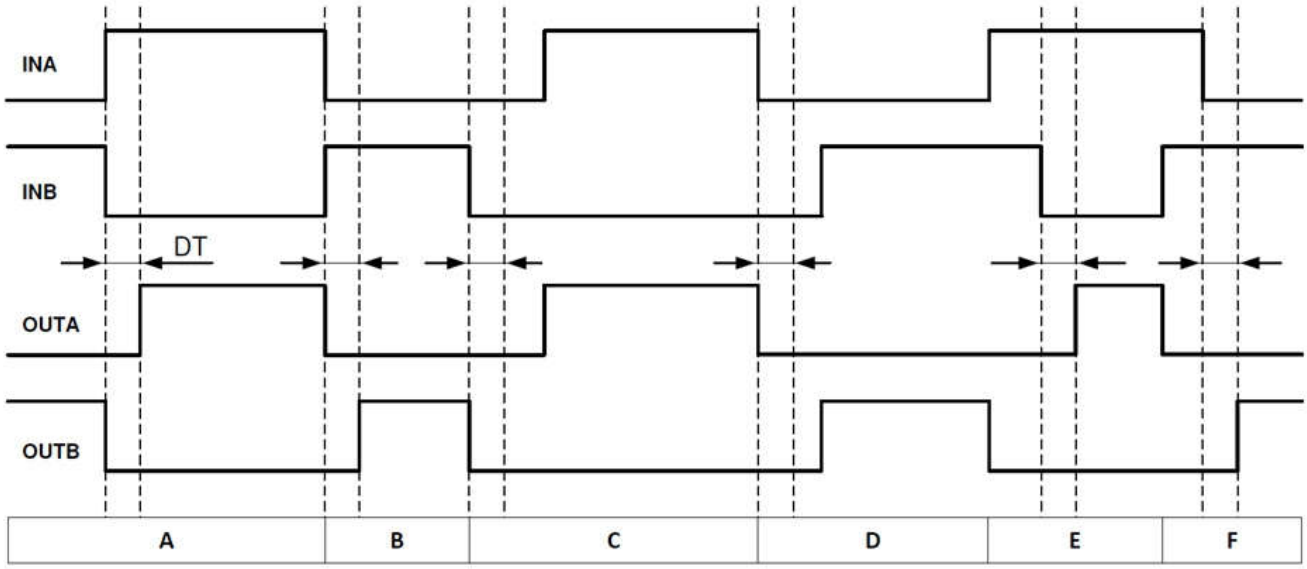

图 3-2. 各种输入信号条件下输入与输出逻辑之间的关系

条件 A：INB 变为低电平，INA 变为高电平。INB 立即将 OUTB 设为低电平并将已编程设定的死区时间分配给 OUTA。在已编程设定的死区时间后，OUTA 能够变为高电平。

条件 B：INB 变为高电平，INA 变为低电平。INA 现在立即将 OUTA 设为低电平并将已编程设定的死区时间分配给 OUTB。在已编程设定的死区时间后，OUTB 能够变为高电平。

条件 C：INB 变为低电平，INA 仍为低电平。INB 立即将 OUTB 设为低电平并将已编程设定的死区时间分配给 OUTA。在这种情况下，输入信号的死区时间比编程设定的死区时间长。因此，当 INA 变为高电平时，会立即将 OUTA 设为高电平。

条件 D：INA 变为低电平，INB 仍为低电平。INA 立即将 OUTA 设为低电平并将已编程设定的死区时间分配给 OUTB。INB 的自身死区时间长于已编程设定的死区时间。因此，当 INB 变为高电平时，会立即将 OUTB 设为高电平。

条件 E：INA 变为高电平，而 INB 和 OUTB 仍为高电平。为了避免过冲，INA 立即将 OUTB 拉为低电平并使 OUTA 保持低电平状态。一段时间后，OUTB 变为低电平并将已编程设定的死区时间分配给 OUTA。OUTB 已经为低电平。在已编程设定的死区时间后，OUTA 能够变为高电平。

条件 F：INB 变为高电平，而 INA 和 OUTA 仍为高电平。为了避免过冲，INB 立即将

OUTA 拉为低电平并使 OUTB 保持低电平状态。一段时间后，OUTA 变为低电平并将已编程设定的死区时间分配给

OUTB。OUTA 已经为低电平。在已编程设定的死区时间后，OUTB 能够变为高电平。

为了确认栅极驱动器稳健可靠地运行，请特别注意最小脉冲宽度。最小输入脉冲宽度由驱动器 IC 中存在的抗尖峰脉冲滤波器决定，该滤波器确定在空载驱动器中传输到输出的最短脉冲。

在栅极驱动器中实现欠压锁定 (UVLO)，以监控栅极电压并防止其降至指定阈值以下。在使用 Si 和 SiC MOSFET 或 IGBT 的高功率应用中，UVLO 等级是一个重要的考虑因素。

- UVLO 是验证系统在偏置电源故障时是否受到保护的关键功能。
- 由于器件特性和大功率系统，高功率应用中的 SiC MOSFET 和 IGBT 需要高 UVLO。高效开关这些器件对于防止损坏或寿命缩短至关重要。

对于高开关频率或硬开关应用，为了防止栅极驱动器误导通，优先选择米勒钳位以提高整体系统稳健性。UCC5350-Q1 是一款单通道隔离式栅极驱动器，具有 10A 典型峰值拉电流和 10A 典型峰值灌电流，其具有米勒钳位或分流输出的选项。

- Vds dv/dt 会导致电流通过 Cgd，也称为米勒电容。该米勒电流会在栅极处产生电压
- 米勒钳位引入了一条低阻抗路径来绕过米勒电流，并防止栅极驱动器关断时误导通。

这款单通道栅极驱动器集成了特定逻辑，可防止击穿。只需将 IN+ 和 IN- 分别连接到单通道器件，即可实现互锁。如果高侧和低侧栅极驱动器同时发送输入高电平，驱动器将禁用输出以防止击穿。表 3-1 中列出了逻辑表。

表 3-1. 器件功能状态

IN+	IN-	OUTH/OUTL	功能状态
0	0	LO	系统关闭
0	1	LO	正常低电平
1	0	HI	正常高电平
1	1	LO	防止击穿

如果需要额外的高级保护功能，可以考虑 UCC218200-Q1，它是一款隔离式栅极驱动器，具有过流和短路检测、故障后受控软关断、故障报告、有源米勒钳位、输入和输出侧电源 UVLO（用于优化 SiC 和 IGBT 开关行为和稳健性）、输出电压栅极监控以及启动期间的内置自检。

输出电压栅极监控器进行检查，确保 PWM 为高电平时栅极电压大于 VDD - 3V，而 PWM 为低电平时栅极电压小于 VEE + 3V。

- 当检测到栅极监控器故障时，RDY 被拉至低电平。
- 低压侧的 OUT_FB 提供实时反馈输出。

在初始启动期间，驱动器会运行一系列检查，以验证以下比较器是否卡在高电平还是低电平：

- DESAT/OC。
- VCC、VDD 及 VEE UVLO。
- VDD-3V 和 VEE+3V 栅极监控器。
- 米勒钳位阈值。

3.7 电压传感器

在 OBC 应用中，电压检测对于闭环控制、故障检测和后续保护至关重要。隔离式放大器是使用隔离栅进行电压检测的常用设计。该隔离层可将系统中以不同共模电压电平运行的各器件隔开，防止高电压冲击导致低压侧器件电气损坏或对操作员造成伤害。

AMC0311D-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电磁干扰性能极强的电容隔离层隔开。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 3-3 显示了方框图。

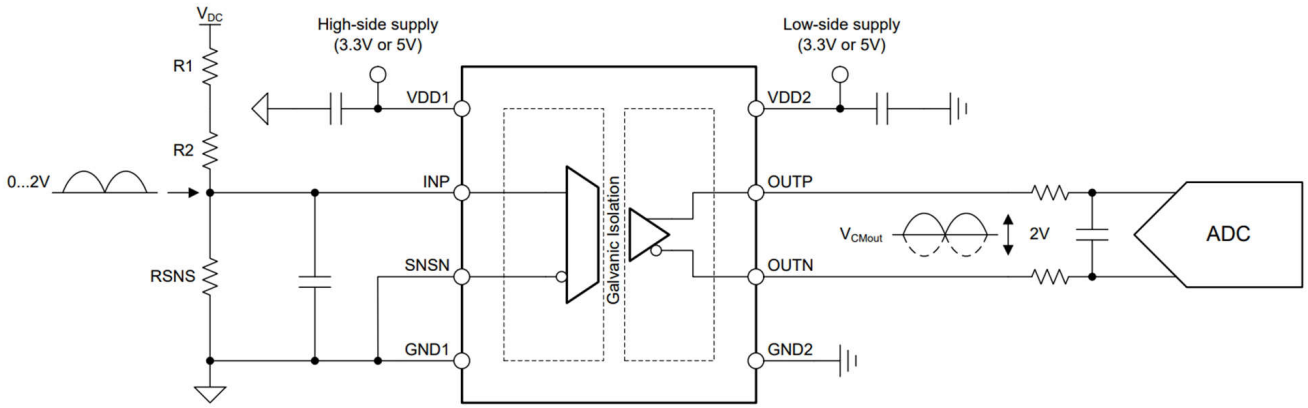

图 3-3. AMC0311D-Q1 的方框图

集成的高侧电源电压缺失检测功能可简化系统级设计和诊断。图 3-4 示出了失效防护模式，其中 AMC0311D-Q1 输出在正常工作条件下不会出现的负差分输出电压。

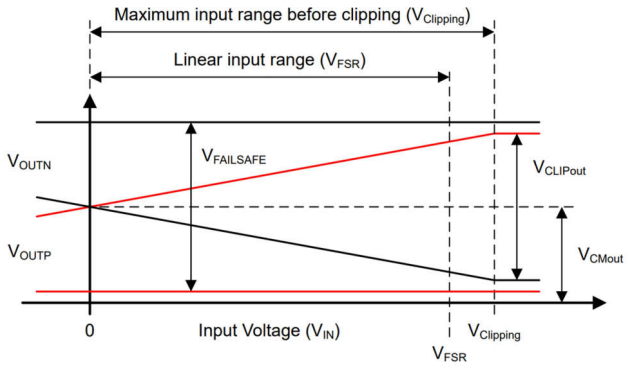

图 3-4. AMC0311D-Q1 的输出行为

使用最大故障安全电压作为系统级故障安全检测的参考值。在以下三种情况下，失效防护输出处于活动状态：

- 当 AMC0311D-Q1 器件的高侧电源 VDD1 缺失时。
- 当高侧电源 VDD1 降至低于欠压阈值 VDD1 UVLO 时。

在实际应用中，可以使用两个独立的采样通道进行冗余电压检测，以验证 MCU 是否拥有可靠的电压信息。

3.8 电流传感器

在典型的 OBC 应用中，需要使用电流传感器来实现闭环控制以及过流或短路保护。一种选择是基于霍尔效应的元件，可用于交流和直流电流测量。基于霍尔效应的元件具有低电阻引线框架路径，可降低功耗，并且不需要任何外部无源元件、隔离式电源或高压侧的控制信号。

TMCS1133-Q1 是一种电隔离霍尔效应电流传感器，提供高水平的可靠加强隔离工作电压、环境磁场抑制和高载流能力。在 25° C 时，工厂修整的灵敏度误差为 0.4%，在整个工作温度下，灵敏度误差为 0.5%，实现了行业领先的精度。功能方框图如图 3-5 所示。

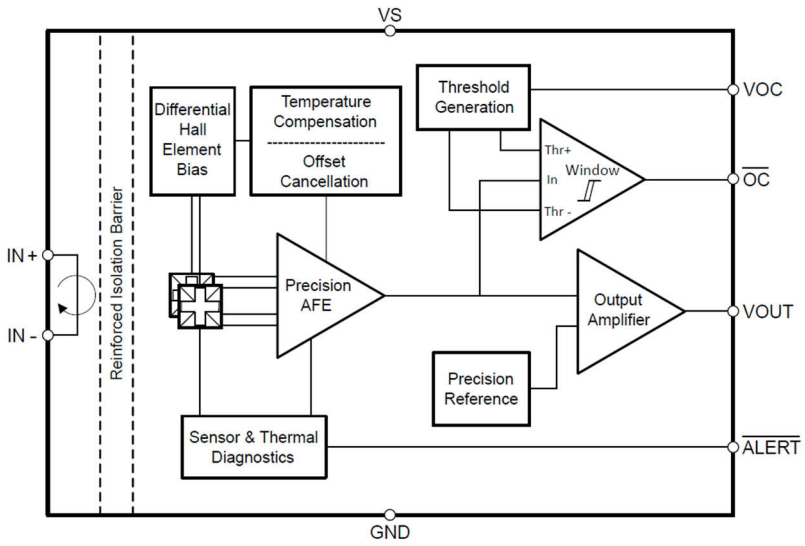

图 3-5. TMCS1133-Q1 的功能方框图

TMCS1133-Q1 提供快速数字过流检测响应。这可用于触发警告或发起系统关断，以防止由短路或其他意外系统状况引起的电流过大而造成的损坏。OC 阈值可在双向和单向器件上配置为根据满量程模拟测量范围的一半至两倍以上之间的信号进行置位。

使用 OC 输出而不是 VOUT 来检测过流事件的好处是更高的动态范围、更高的灵敏度和更低的模拟信号带宽，由此带来更低的总体信号噪声。但是，VOUT 引脚也可以通过使用 MCU 的 CMPSS 模块用作冗余 OC 保护功能。为了实现 VOUT 引脚 OC 保护，可以设置较低的 OC 阈值，以在电流较小但持续时间较长的情况下覆盖该事件。当 OC 引脚路径中出现 SPF 时，该引脚还可以覆盖 OC 事件。

TMCS1133-Q1 中加入了内置自诊断功能，以便在运行条件使电流传感器测量无效时发出警告。受监控的两个关键条件是传感器温度和灵敏度。

- 高输入电流，加上环境温度和印刷电路板热设计的升高，会导致 TMCS1133-Q1 过热，并因超过允许的最大结温而损坏。当内部温度接近允许的最高结温时，会发生热警报。
- TMCS1133-Q1 内部会持续监测传感器灵敏度及偏移。如果霍尔传感器灵敏度或偏移量超出工厂设置的限制范围（这种情况不太可能发生），则会出现传感器警报。

低电平有效 ALERT 输出信号可用于辨别 TMCS1133-Q1 处于四个诊断状态中的哪一个状态。8kHz PWM 输出信号的占空比指示过热运行条件警告和传感器运行条件警告哪一个存在、两者都不存在或者两者都存在。

基于分流电阻器的设计是电流检测的替代方案。AMC0302D-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电磁干扰性能极强的隔离层隔开。AMC0302D-Q1 的输入经优化，可直接连接低阻抗分流电阻器或其他具有低信号电平的低阻抗电压源。通过出色的直流精度和低温度漂移，支持在 OBC 应用中进行精确的电流控制。图 3-6 显示了方框图。

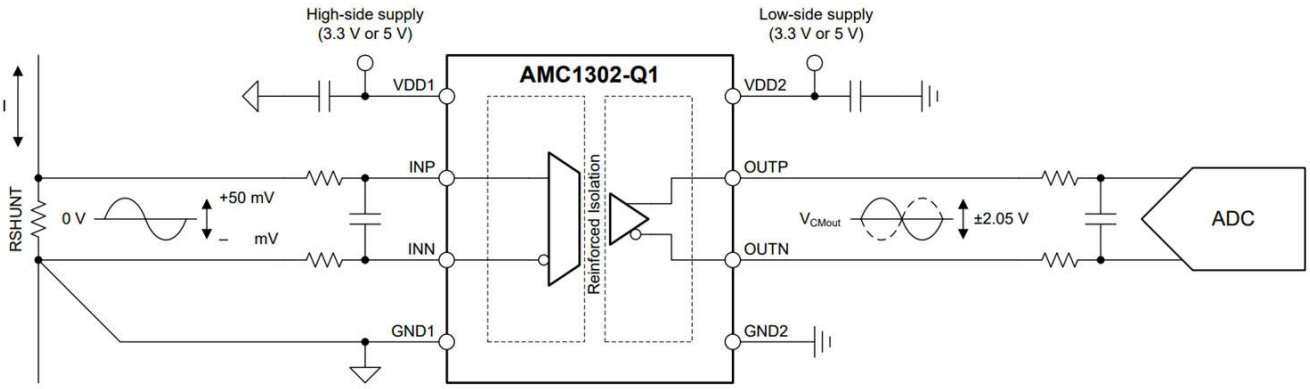

图 3-6. AMC0302D-Q1 的方框图

集成的无分流器和无高侧电源检测功能可简化系统级设计和诊断。图 3-7 示出了失效防护模式，其中 AMC0302D-Q1 输出在正常工作条件下不会出现的负差分输出电压。

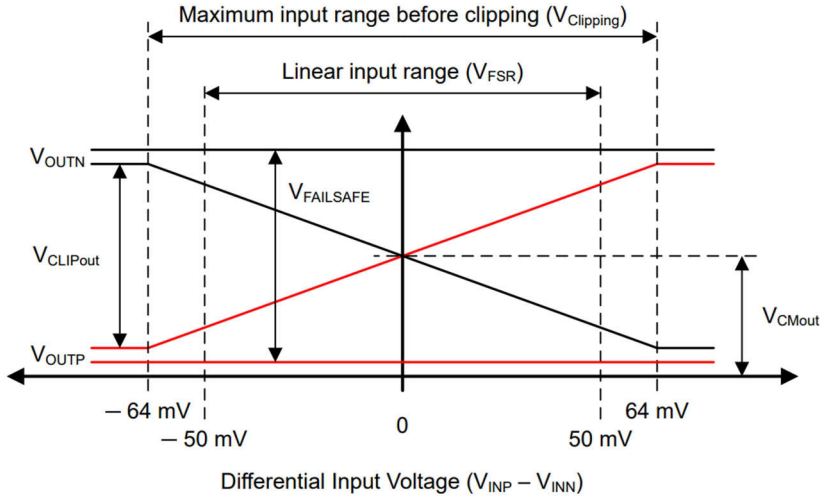

图 3-7. AMC0302D-Q1 的输出行为

使用最大故障安全电压作为系统级故障安全检测的参考值。在以下两种情况下，失效防护输出处于活动状态：

- 当高压侧电源缺失或低于 VDD1 UVLO 阈值时。
- 当共模输入电压（即 VCM =(VINP + VINN)/2）超过共模过压检测水平时。

如果电流检测电路仅用于过流保护而不用于电流控制，则隔离式比较器是一种非常合适的解决方案。通常，它可被视为 FuSa 的第二个冗余检测链。AMC23C12-Q1 是一款响应时间较短的隔离式窗口比较器。比较器的窗口电压以 0V 为中心，这表示如果输入电压的绝对值超出跳变阈值，则比较器就会跳变。其框图如图 3-8 所示。

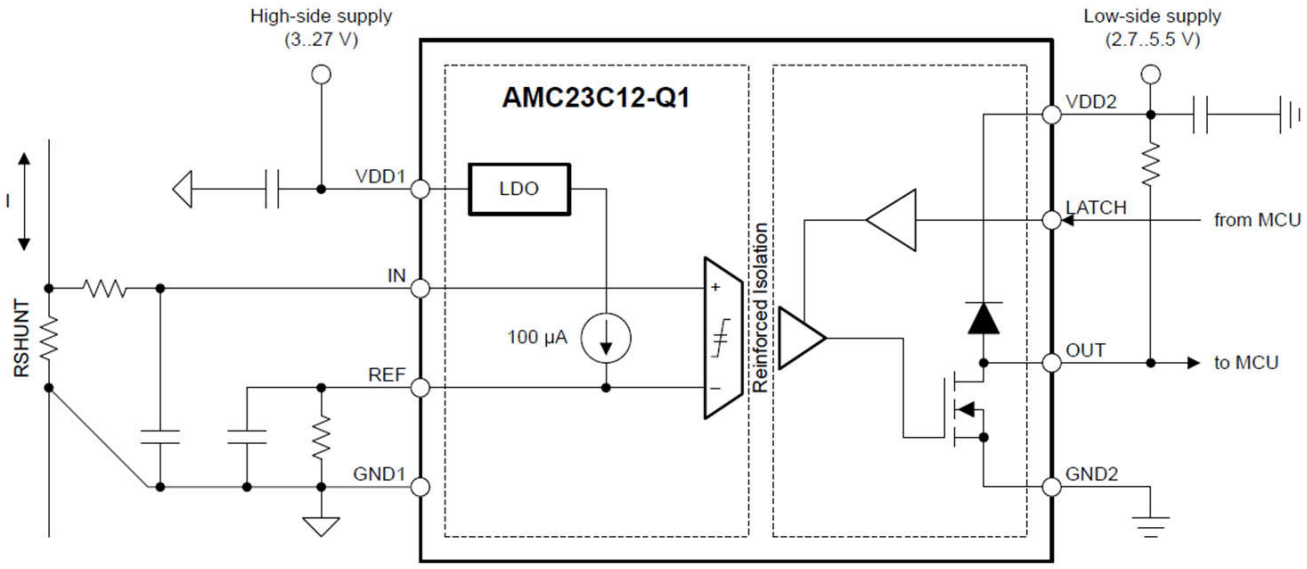

图 3-8. AMC23C12-Q1 的方框图

3.9 温度传感器

在 OBC 系统中，温度传感器对于控制和安全监控也至关重要，因此也需要仔细考虑这一点。这通常由模拟器件实现，例如负温度系数 (NTC) 电阻器。TMP61-Q1 是具有正温度系数 (PTC) 的硅基热敏电阻。

精度是温度传感器的最关键因素。TMP61-Q1 可在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 3-9 示出了典型电阻与环境温度间的关系。

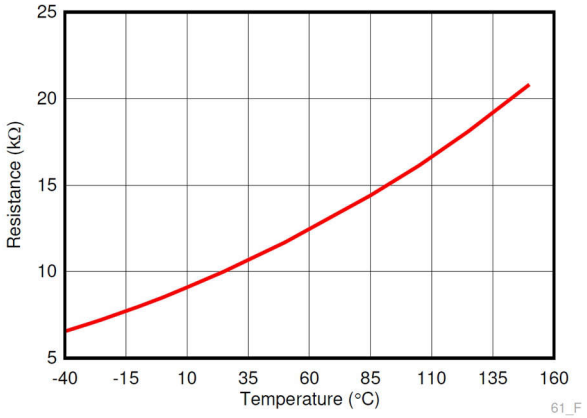

图 3-9. TMP61-Q1 典型电阻与环境温度间的关系

TMP61-Q1 专门为长使用寿命和高性能而设计。它内置了在高温下发生短路故障时的失效防护行为。凭借出色的抗环境波动能力，可保持典型的传感器长期漂移仅为 0.5%。该器件可快速响应温度变化，热响应时间短，仅为 0.6 秒。

TMP61-Q1 采用紧凑型 0402 封装，可靠近热源放置，并可直接替代传统 NTC 电阻器。对于需要更高温度容差的应用，ELPG 封装选项可将工作范围扩展至 170°C。

温度检测的可靠性不仅取决于热敏电阻，还取决于上拉电阻和电源。TMP23x-Q1 器件是汽车级高精度 CMOS 集成电路线性模拟温度传感器系列，其输出电压与温度成比例。图 3-10 显示了方框图。

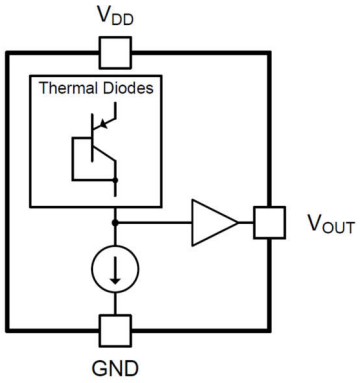

图 3-10. TMP23x-Q1 的方框图

TMP235-Q1 器件在 -40°C 至 +150°C 的整个温度范围内提供 10mV/°C 的正斜率输出，电源范围为 2.3V 至 5.5V。更高增益的 TMP236-Q1 传感器在 -10°C 至 +125°C 的范围内提供 19.5mV/°C 的正斜率输出，电源范围从 3.1V 至 5.5V。通过消除对外部上拉电阻器的需求，实现了更高的可靠性。此外，它还为下游元件提供内置保护，当暴露于电源过压情况时，该器件可以防止这些异常高的电压按比例传输到后端 ADC，从而有效地保护 MCU 免受潜在的损害。

如果热敏电阻不能靠近热点放置（例如 FET /变压器/分流电阻器），则精度和响应时间通常会受到影响。对于 OBC 应用，由于需要考虑电气间隙和爬电距离，有时放置热敏电阻来进行权衡。为了解决这个问题，ISOTMP35-Q1 是业界先进的隔离温度传感器 IC，集成了隔离栅，可承受高达 3000VRMS 的电压，具有一个模拟温度传感器，可在 –40°C 至 150°C 范围内实现 10mV/°C 的斜率。图 3-11 示出了方框图。

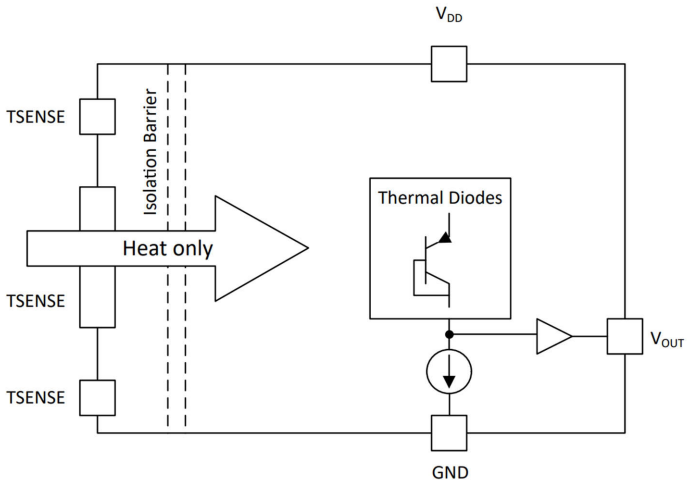

图 3-11. ISOTMP35-Q1 的方框图

这种集成使得传感器能够与高压热源并置，无需昂贵的隔离电路。与通过将传感器放置在较远位置来满足隔离要求的方法相比，直接接触高压热源还可提供更高的精度和更快的热响应。

除了上述器件级设计外，冗余温度传感器和合理性检查也是提升系统功能安全性的常见方法。

4 总结

本文介绍针对 OBC 的 FuSa 分析。第 1 节概述 FuSa 基础知识、一般 ISO 26262: 2018 工作流程以及支持 FuSa 开发的 TI 工具。第 2 节介绍单级 OBC 的 FuSa 分析示例，首先是项目定义、推导安全目标，然后是开发 FSR、TSR，最后是 HSR 和 SSR。第 3 节概述关键 OBC 元件和安全功能，包括 MCU、栅极驱动器、传感器和辅助电源。本文档旨在为设计人员提供使用 FuSa 创建 OBC 设计所需的基本信息及资源。

5 参考资料

1. TUV SUD，*了解 ISO 26262 标准：您需要了解的内容 | TÜV SÜD PSB*
2. 德州仪器 (TI)，*了解符合 IEC 623801 和 SN 29500 的功能安全 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功能安全认证功能安全手册*，功能安全手册。
4. 德州仪器 (TI)，*为安全 MCU 设计电源以满足功能安全 ASIL B 要求*，技术白皮书。
5. 德州仪器 (TI)，*TMCS1123-Q1、TMCS1126-Q1、TMCS1127-Q1 和 TMCS1133-Q1 功能安全 FIT、FMD 和引脚 FMA* 功能安全信息。
6. 德州仪器 (TI)，*C2000™ 实时微控制器的汽车功能安全（修订版 F）*，功能安全手册。
7. 德州仪器 (TI)，*C2000™ 安全机构（修订版 B）*，功能安全手册。

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