Technical White Paper

简化机器人电机驱动器安全评估

Ester Vicario, Kristen Mogensen *Systems Engineering and Marketing*

摘要

随着机器人系统在工业环境中的应用越来越广泛，行业安全要求以及国家/地区和国际安全法规需要不断更新，确保人类在靠近机器的位置工作时拥有安全的环境。需要进行功能安全评估以证明器件满足安全要求，可以负责任地将其推向市场。

安全评估可能是一个漫长的过程，会延迟产品上市时间并增加产品的总体设计成本。本文档介绍了如何简化评估流程。本文档以面向自主移动机器人 (AMR) 的电机驱动器为例，介绍了在选择合适的器件、满足安全要求并缩减总体物料清单 (BOM) 尺寸和成本时需要考虑的事项。本白皮书通过描述满足安全要求所需遵循的步骤，阐述了如何加快安全评估和降低设计成本。

内容

插图清单

表格清单

商标

1 引言

工业依赖自动化来提高生产率和整体效率。为了提高生产率，公司正在工厂中部署机器人，工人继续与这些机器一起工作。因此，员工会面临新型危险，这就需要对这类危险进行监管以确保人身安全。

为了证明机器人符合安全要求，在投放市场之前，每件产品都必须经过安全评估。评估必须表明机器符合最低和规定的安全要求。确保产品符合安全标准通常是一个漫长而复杂的过程，这会增加总体设计成本、机器人尺寸和上市时间。

本白皮书简要说明了对电机驱动器进行安全评估所需遵循的流程。介绍了使用的主要标准、架构类型和器件选型，有助于加快系统设计过程。

对于此特定文档，将单通道电机驱动器设计的新安全概念用作基准。此安全概念提供了块级概念，说明如何根据 ISO 13849 实现 2 类、性能级别 2（2 类、PLd），或根据 IEC 61508 标准实现安全完整性级别 2 和硬件容错 = 0（SIL 2、HFT = 0），此类概念旨在帮助读者以具有成本效益的方式满足安全要求。例如，本白皮书参考了 ISO 3691-4 标准，该标准侧重于工业卡车，例如自主移动机器人 (AMR)；但是，相同的程序可用于需要 2 类、PLd 的任何其他机器。

此概念使用了 TI 全新的高性能电机控制 C2000™ 实时控制器和 PMIC，它们都包含片上安全功能。通过使用此产品系列、设计概念和其他 TI 可用的安全资源，设计可以实现整个系统的较低 BOM 实现并缩短上市时间。

2 了解 2 类、PLd 安全要求

了解所需的产品安全标准是产品设计过程中至关重要的第一步。因为本白皮书以移动机器人电机驱动器为例，因此必须满足 ISO 3691-4 产品安全标准要求。

2.1 符合 ISO 3691-4 的安全要求

ISO 3691-4 标准定义了无人驾驶工业卡车的安全要求和验证，包括自主移动机器人 (AMR) 等工业移动机器人。该标准描述了整个机器的安全要求；因此，设计人员负责确定安全功能在工业叉车模块内的位置，如图 2-1 所示。

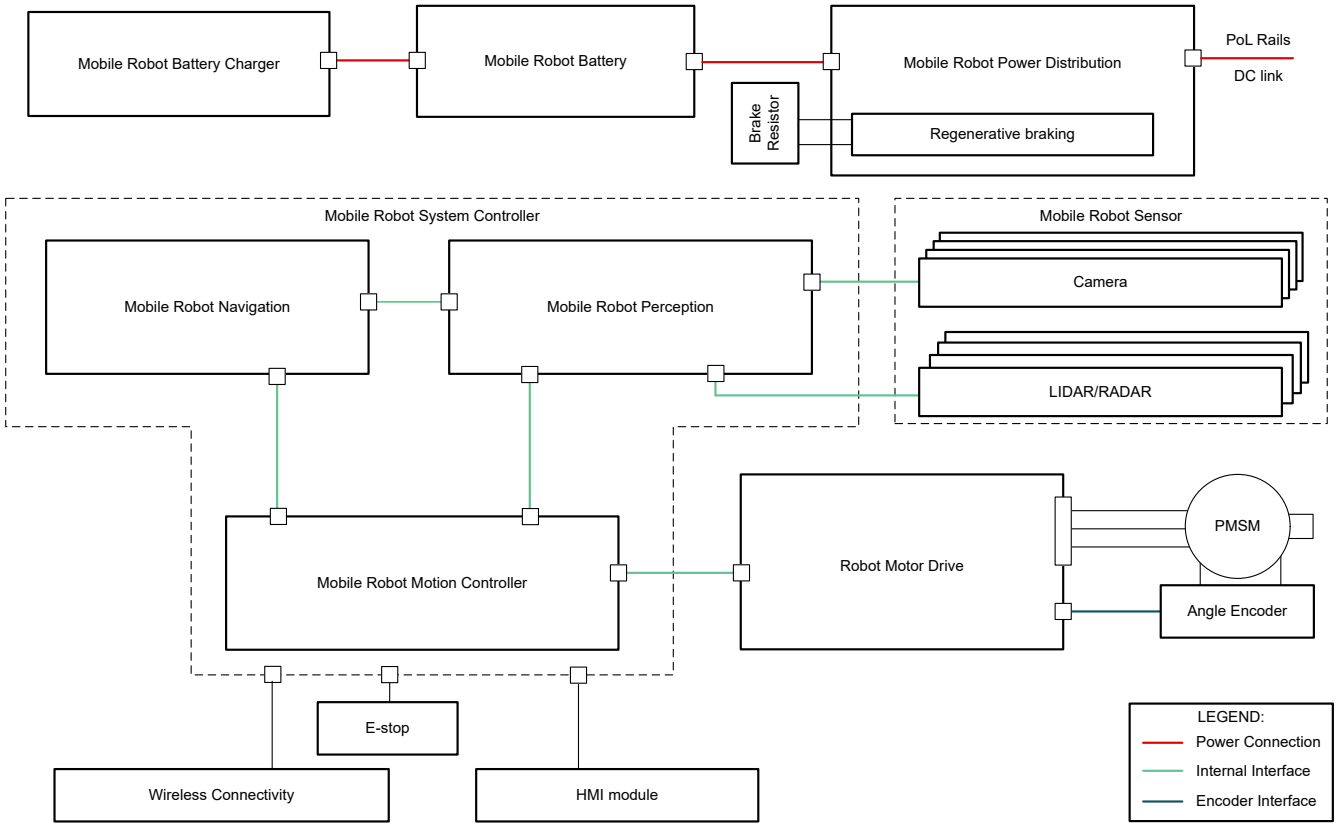


图 2-1. 简化的移动机器人方框图

安全标准 ISO 3691-4 描述了在存在危险情况时必须实施的安全注意事项，旨在满足必要的风险降低要求。对于所述的每种风险情况，ISO 3691-4 标准根据 ISO 13849-1 分配所需的最低性能级别 (PL)。PL 是一个通常用于实现每个安全功能所需风险降低的值，并在机械标准 ISO 13849-1 中进行定义。

与 PL 类似，多个标准使用 IEC 61508 中定义的安全完整性等级 (SIL) 参数来衡量系统安全性能。表 2-1 中显示了 PL 和 SIL 级别之间的关系。

表 2-1. IEC 61508 和 ISO 13849 SIL 和 PL 关系

硬件故障容错 (HFT)								类别			
IEC 61508 标准							ISO 13849				
0	1	2	0	1	2	SFF	直流	1	2	3	4
-	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3	< 60%	无				
SIL 1	SIL 2	SIL 3	SIL 2	SIL 3	SIL 4	60% 至 < 90%	低	c	c	d	
SIL 2	SIL 3	SIL 4	SIL 3	SIL 4	SIL 4	90% 至 < 99%	中		d	e	
	SIL 4	SIL 4	SIL 4	SIL 4	SIL 4	⩽ 99%	高				e
类型 B			类型 A								

SIL 和 PL 都是用于确保安全性能的离散级别，这些级别通过使用不同的参数来量化诊断能力。SIL 使用安全失效分数 (SFF) 作为参数来量化系统的安全故障与总故障之间的比率。同样，PL 将 DC 参数称为系统中实施的诊断有效性的度量。但是，SIL 和 PL 通过两个成反比的主要参数相关：MTTF（平均危险失效时间）和 PFH（每小时危险失效概率），前者在 ISO 标准中使用，后者在 IEC 标准中使用。通过使用此关系，可以在评估系统安全性时同时使用 PL 和 SIL 级别。

表 2-2. 通过 PFH 和 MTTF 参数建立的 PL 和 SIL 关系

PL (ISO 13849)	PFH 目标值 [PFH = 1/MTTF]	SIL（IEC 61508、IEC 62061）
a	⩾ 10^{-5} 至 < 10^{-4}	无对应关系
b	⩾ 3 x 10^{-6} 至 <10^{-5}	1
c	⩾ 10^{-6} 至 < 3 x 10^{-6}	1
d	⩾ 10^{-7} 至 < 10^{-6}	2
e	⩾ 10^{-8} 至 < 10^{-7}	3

尽管 PL 或 SIL 适用于完整的安全功能（通常由传感器、数据处理和执行器组成），但这些功能子系统中的每一个都需要满足最低 PL 或 SIL 要求。每个子系统都有不同的标准来描述如何满足安全级别。例如，对于电机驱动器和执行器实施，子系统特定的标准 IEC 61800-5-2 用于指定安全要求。

IEC 61800-5-2 通过描述安全转矩关闭 (STO)、安全限速 (SLS)、安全制动控制 (SBC) 等指定的安全子功能，定义了电机驱动器的设计和开发要求。

在该标准中，IEC 61800-5-2 指的是 ISO 13849-1，其中描述了每个子功能实现最低 PL 所需的要求。此外，上文提到的两个标准都讨论了系统之间的独立性、冗余和处理时间等方面，在实施系统时必须加以考虑。

因此，在开始系统实施之前，务必了解每个应用的安全要求、需要实施的安全子功能和每个子功能所需的风险降低级别（SIL 或 PL）之间的主要关系。

如 ISO 3691-4 的表 1 所示，对于这种特定情况，需要最低 PLd 级别。着眼于电机驱动子系统，使用 IEC 61800-5-2 中定义的安全子功能，以满足 PLd 要求。表 2-3 总结了这三个标准之间的主要关系。

表 2-3. 符合 ISO 3691-4 的安全要求

符合 EN ISO 3691-4 的安全功能	符合 EN ISO 3691-4 的最低要求 PL	符合 IEC 61800-5-2 的相关安全子功能
制动系统	d/b	SBC、SS1、STO

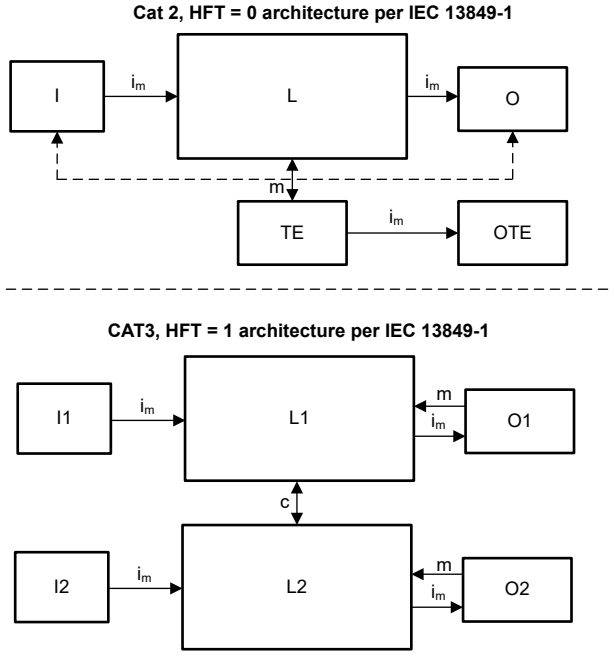
表 2-3. 符合 ISO 3691-4 的安全要求 (continued)

符合 EN ISO 3691-4 的安全功能	符合 EN ISO 3691-4 的最低要求 PL	符合 IEC 61800-5-2 的相关安全子功能
速度控制	d/c	SLS、SOS、STO
电池自动充电	b	NR(1)
负载处理	b	NR(1)
转向	-	SLS
稳定性	c	NR(1)
紧急停止功能	d	STO
人员检测系统	d/c	SLS、SOS、SS1、STO SDI
自动、手动和维护模式	d/c	SLS、SOS、STO
警告系统	a	NR(1)
进入受限区域	d	SOS、STO

(1) NR：实现与机器人电机驱动器无关

2.2 系统架构选择

ISO 13849-1 标准定义了所需诊断覆盖率和与系统的冗余量相关的架构类别之间的关系。如前所述，ISO 3691-4 标准要求最低 PLd 安全级别，这可通过使用 IEC 13849-1 标准中定义的 2 类、HFT = 0 或 3 类、HFT=1 架构来实现。此选项会影响系统中所需的冗余量和诊断覆盖率，如图 2-2 所示。



I= 输入，L= 逻辑，O= 输出，TE= 测试设备，OTE= 输出测试设备，m= 监控，c= 比较

图 2-2. 符合 IEC 13849-1 标准的 2 类和 3 类的指定架构

如表 2.1 的 2 类、HFT = 0 所示，系统实现需要较少的冗余，以换取更高的 90% 诊断覆盖率 (DCavg = 90%)。为满足所需的 DCavg 要求，需要在定义的时间间隔内执行诊断功能，以确保按时达到安全状态。相反，3 类架构需要双通道设计，以换取较低的诊断覆盖率和更宽松的时序约束。

对于 AMR，关键的限制因素之一是系统的整体尺寸和重量。因此，更紧凑的 2 类架构适用于这些类型的应用程序。但是，在优先选择 3 类实施的情况下，TI 还提供了 *C2000™ 实时微控制器的工业功能安全* 产品概述和有关如何实施此类系统的指导。

2.3 基于过程安全时间的器件选择

了解了初始安全要求以及要实施的架构后，就需要进行器件选择。作为一个常见的起点，MCU 或处理器的选择优先于其他器件，而安全特性或处理能力等方面是选择过程中的关键结果。

在安全标准中，ISO 13849-1 描述不同的时序要求，以确保系统能够检测到故障并在规定的过程安全时间内达到安全状态。图 2-3 显示了用于定义时间间隔的典型命名规则。

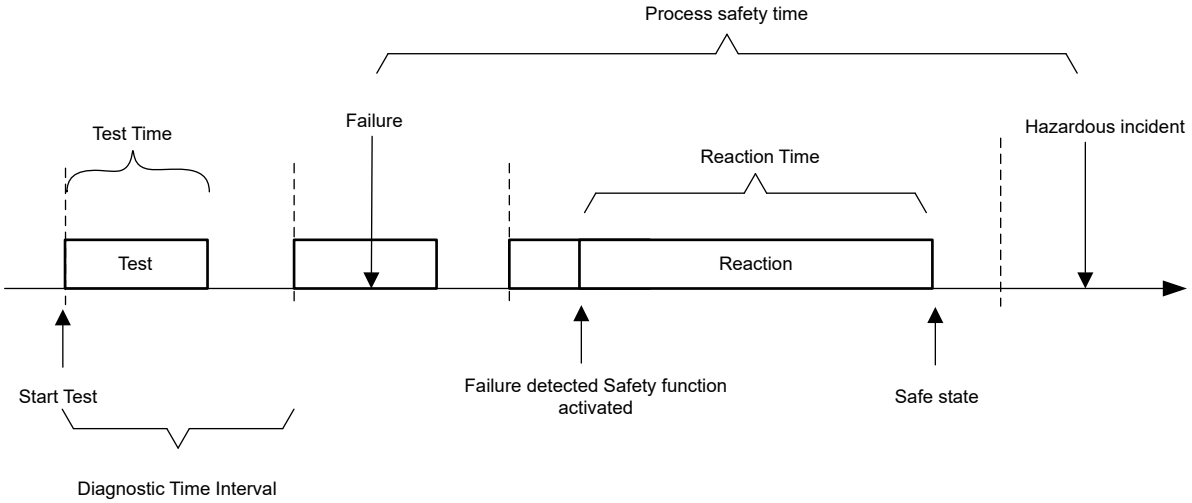


图 2-3. 与功能安全相关的时序注意事项

诊断时间间隔包括可用于执行诊断功能和处理从这些功能接收到的输入的时间量。在给定定义的诊断时间间隔时，诊断覆盖率越高，则意味着需要功能越强大的处理器。

由于危害的不可预测性，在 AMR 中，诊断需要持续运行。通过持续运行，可瞬时检测到故障，并可在所需的过程安全时间内使器件进入安全状态。

此外，ISO 3691-4 还通过根据与物体的距离定义 AMR 的最大速度，进一步限制了此测试时间间隔。通过考虑最坏的情况，设计人员必须计算规避风险所需的过程安全时间，并确保在物体碰撞之前达到安全状态。

根据 ISO 3691-4 表 A.1 中规定的最大速度以及与物体的距离，估计安全过程时间需要小于 415ms。在此时序内，必须完成 MCU 的诊断功能，如果检测到故障，则必须达到安全状态。为了留出足够的反应时间，诊断时间间隔必须小于整个过程安全时间的 10%。这意味着，在系统功能运行期间，允许进行完整诊断扫描的最长时间为 41.5ms。

由于这些时序限制和 2 类架构选择，务必拥有功能强大的实时 MCU 以及集成的安全机制，此类机制可以同时满足电机控制和安全要求。TI C2000 实时控制器和 PMIC 器件是确保同时满足过程安全时间和诊断覆盖率的理想之选，可实现 PLd。

3 实施移动机器人电机驱动器安全要求

了解系统的安全要求和架构类别后，设计人员必须选择其余器件并实施完整的电机驱动器，以确保满足安全要求。

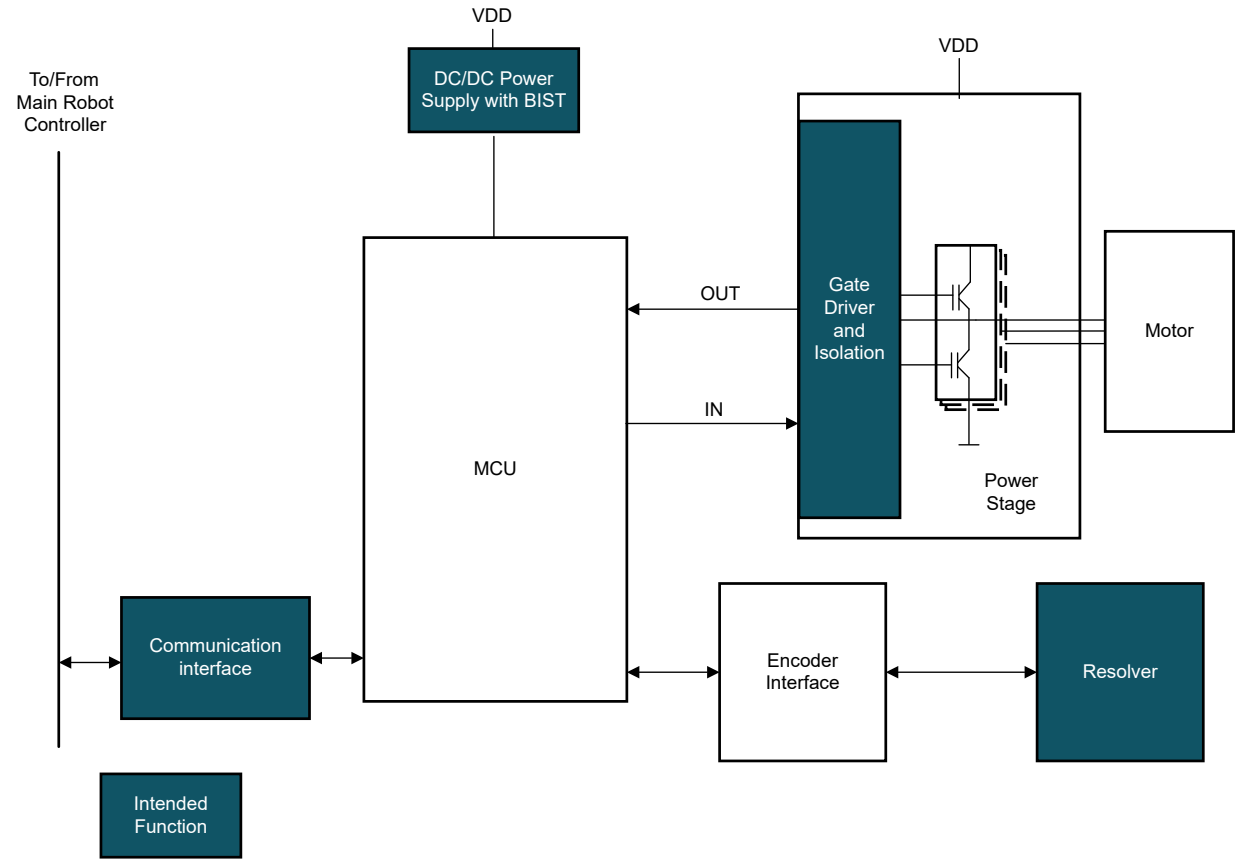


图 3-1. 电机驱动系统方框图

如图 3-1 所示，电机驱动系统通常由 MCU 组成，MCU 是一个可集成模拟前端、编码器和电源的功率级。

在 IEC 61508 中，所需的安全失效分数 (SFF) 取决于器件的类型（可以是 A 类或 B 类）。根据 IEC 61508，A 类子系统具有明确定义的故障模式，其中确定了故障条件下的行为并且有足够的故障数据来声明故障率得以满足。相反，B 类子系统是更复杂的子系统，其中故障模式没有完全定义，故障条件无法完全确定，并且没有足够的数据来支持故障率得以满足。IEC61508 标准的第 7.4.4 节提供了这两种类型的子系统的完整定义。

此外，IEC61508 标准的 CNB-M-11.059 修订版规定，诊断子系统只需达到这样一个安全级别：低于达到最低安全级别所需的系统 SIL 级别。尽管该修订版是 IEC61508 标准的一部分，但在分析诊断子系统时，将其与 ISO 13849-2 机械标准一起使用更符合目前的趋势。

因此，对于这种特定情况，由于需要 SIL 2 系统，因此诊断相关模块必须至少满足 SIL 1 且最低 SFF = 0%，才能满足 SIL 2 系统要求。但是，安全和非诊断功能仍必须满足 SIL 2 要求，且最低 SFF 为 60%。

通过了解哪些子系统是 A 类和 B 类，可以根据可用的安全文档或诊断功能等特性轻松选择器件本身。

由于 MCU 是 B 类器件且用于实现安全功能，因此 MCU 要求最低 SFF = 60%。这意味着，必须使用诊断功能对器件使用的每个子系统进行监控，以达到所需的 60% 覆盖率。

第一步，需要选择需使用的器件功能以及每项功能所需的诊断覆盖率。一旦定义，安全文档就成为关键，旨在证明是否有足够的诊断可用于每个预期功能或是否需要外部诊断器件。

TI 全新的 C2000™ 实时控制器在设计时将功能安全考虑在内。通过利用所提供的安全特性和文档，可以简化和加速安全评估。 C2000™ 实时微控制器的工业功能安全产品概述中介绍了一些主要的 C2000™ 安全特性和器件。

此外，对于不太复杂的器件，具有安全文档也很重要。如前所述，考虑采用 A 类器件的条件之一是必须明确定义器件功能和故障模式。为此，TI 安全文档结果有利于证明采用相应器件类型的合理性，以及因此满足所需的最低 SFF 要求。

TI 多通道 IC (PMIC) 器件十分有助于缩减电机控制模块的总体 BOM 和尺寸，同时确保满足安全要求。凭借内置 LDO、监控器、BIST、看门狗和直流/直流稳压器等集成功能，这些 IC 有助于简化设计，同时提供监控 MCU 和需要的电源轨所需的诊断功能。

根据 ISO 13849 第 6.1 节，鉴于无法定期执行安全功能，诊断和安全功能无法在同一个 IC 中，因而无法实现这一 60% 的诊断覆盖率。ISO 13849 认为，IC 中的单一故障会导致该 IC 的功能完全丧失，对于类别 2，应通过诊断功能来检测这类功能丧失问题。因此，为确保这一功能丧失不会导致诊断功能丧失，不可能在同一 IC 内使用电压监控和看门狗问答。在本例中，使用了外部电压监控器和 PMIC 器件的内部问答 (Q&A) 看门狗。监控器和复位 IC 电源管理文件夹详细介绍了 TI 广泛的支持功能安全的电压监控器产品系列。

图 3-2 显示了可用于实现 SIL 2 的一些诊断功能的
高度简化示例。

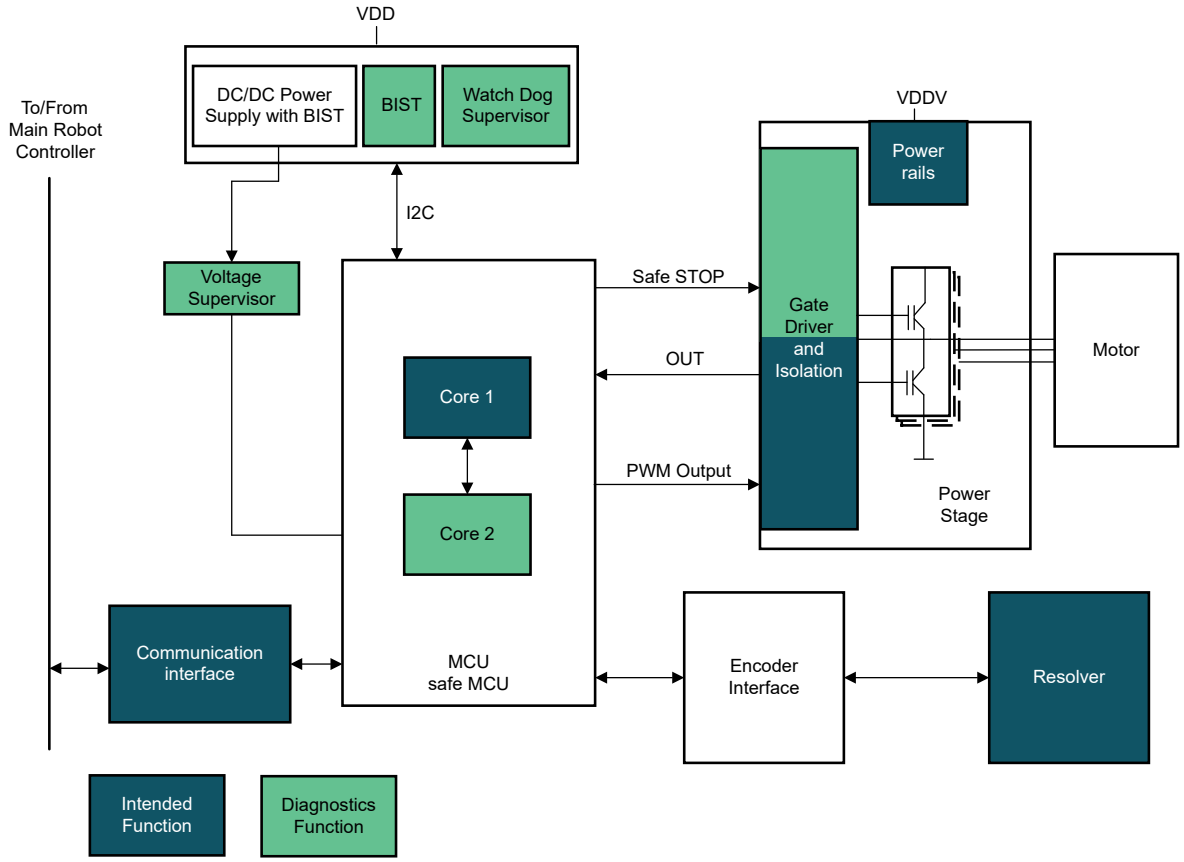


图 3-2. 包含安全特性的简化电机驱动系统

一旦在系统级定义了安全功能，就需要进行块级分析，以证明每个子系统都满足所需的安全要求。

在这种情况下，安全子系统划分为安全功能和诊断功能。诊断功能用于确保安全功能符合依据子系统类型定义的最低 SFF。表 3-1 总结了详细信息。

表 3-1. 每个器件类型所需的诊断覆盖率示例

参数	A 类	A 类	B 类	B 类
安全功能 (S)、诊断功能 (D)	S	D	S	D
SIL	2	1	2	1
HFT	0	0	0	0

表 3-1. 每个器件类型所需的诊断覆盖率示例 (continued)

参数	A 类	A 类	B 类	B 类
所需的最低 SFF | DC	60%	0%	90%	60%

通过正确定义和证明每个预期功能均可达到所需的最小诊断覆盖率，这表明系统能够达到所需的 PL 和 SIL 并可获得安全认证。

4 结论

本文档介绍了实现安全认证系统应遵循的过程。清晰的产品设计和开发策略可进一步缩短上市时间。此外，通过正确地了解确保满足安全级别所需的要求，可以通过更大限度地利用器件的内部特性来减少总 BOM。因此，TI 在功能安全方面的专业知识可以在产品开发过程中发挥巨大优势。

TI 提供了广泛的以功能安全为中心的器件和资源产品系列。TI 功能安全页面提供了有关配套资料和产品的信息，可供您选择更佳器件并了解更多安全相关知识。

从 TI 销售团队获取本文档中示例的完整安全概念。总体概念极大地简化了移动机器人的安全认证过程，也可用于任何需要 HFT = 0、PLD 的电机驱动器。

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265