参考文献

避免电机控制设计流程中的功能安全合规性缺陷

Texas Instruments

Bharat Rajaram
Systems Engineering Manager
Arm-Based Microcontrollers

系统设计和功能安全合规性不应该依次进行。遗憾的是，传统设计方法以及许多组织都将设计流程中的这些步骤视为单独的孤立活动，这往往会导致设计成本增加和产品面市延误。

内容概览

在设计功能安全的电机控制应用时，您是否应该从一开始就将功能安全合规性作为初始设计要求？或者，您是否应该将功能安全视为融入设计最终阶段的附加功能？

功能安全应纳入初始设计要求中，与电机驱动器的预期功能交织在一起。这并不是准则，因为传统的系统设计工作流程不会协同处理安全合规性。但是，如果不一开始就考虑如何满足安全完整性合规要求，则可能会导致将系统推向市场时出现延误，而这种延误成本高昂。

随着工业 4.0 的兴起以及车辆电气化和连接技术的发展，我们需要改变功能安全合规性方法。简而言之，现在我们在更多的应用中拥有更多的电机系统，并且在符合功能安全标准方面达到了很高的水准。

定义功能安全合规性

诸如国际电工委员会 (IEC) 61508 和国际标准化组织 (ISO) 26262 等功能安全标准的目标是管理和缓解系统故障，同时还能够检测和防止随机硬件故障，或至少确保排除其风险。

采用具有独立验证和确认的严格开发流程有助于针对系统故障进行管理。

可以通过以下方式检测、防止随机硬件故障或排除其风险：

- 全面了解所控制的设备。
- 分析情境性风险的可能来源及其属性，例如发生概率、影响的严重性和事件的可控性。

然后，将安全机制与情境性风险配对，有助于设计人员满足 IEC 61508 所要求的量化指标，例如安全失效分数 (SFF) 和每小时故障概率 (PFH)。例如，安全完整性等级 (SIL) 为 2 的系统在超过 10 亿小时的运行中必须满足 SFF≥90% 且 PFH ≤1000 时基故障。

功能安全系统设计的两个属性

功能安全标准假设所有系统都将发生故障（不是会不会发生故障，而是何时发生故障），不存在零风险的情况。

功能安全系统设计的两个属性分别是：开发一个系统来提供预期功能，以及开发同一个系统来满足特定 SIL 或汽车 SIL (ASIL) 等安全功能要求。

设计人员经常以不同的方式或按顺序处理这两个方面。为大容量应用设计功能安全的系统，同时保持设计预算要求是一项挑战。**表 1** 概述了控制和驱动应用中预期功能和安全功能的示例。

为了更好地理解此概念，请查看**表 1** 中的电梯电机示例。

电梯的预期功能是根据用户输入上下运送乘客。如果您按下到达五楼的按钮，电梯应该会停在五楼。

电梯的安全功能则更进一步，可能包括：

- 将您从一个楼层平稳地运送到另一个楼层。
- 停在与每层楼平台齐平的位置。
- 如果电梯超过安全速度，则自动应用制动器。

功能安全应用	预期功能示例	安全功能示例（以及相应的 SIL 或 ASIL 目标）
工业：电梯电机	根据用户请求上下移动电梯	• 安全启动或停止电梯（避免急冲）(SIL 2) • 电梯行驶速度过快时应用自动制动 (SIL 3)
汽车：电动汽车 (EV) 牵引电机	通过加速器或制动器，根据驾驶员指令前后移动电动汽车	• 防止加速时扭矩不足或过大 (ASIL C) • 防止制动过猛（避免追尾）(ASIL D)
工业：钢压机	控制伺服驱动系统，该系统可在不降低工厂生产率的情况下操作钢压机	• 安全扭矩关闭 (STO) 会在发生超扭矩或超速度时切断驱动控制器的电源 (SIL 3) • 安全限速 (SLS) 可在操作人员接近时将电机转速保持在可接受的限值内 (SIL 2) • 如果 SLS 超出界限检查的范畴，则触发 STO（用以平衡生产力和安全性，从而实现更高的 SIL，例如 SIL-3）

表 1. *控制和驱动应用中的预期和安全功能示例。*

为了更好地理解预期功能和安全功能如何协同工作，假设一栋建筑物中有 20 个楼层，里面的电梯有一个按钮电路（请参阅**图 1**），电梯电机控制器将故障解释为让电梯抵达第 25 或第 30 层（即，建筑物内不存在的楼层）。界限检查会尽早发现故障，以免其导致错误或最终导致失效。这是功能安全方面的公认进展：“故障”会导致“错误”，而某些错误可能会导致“失效”。

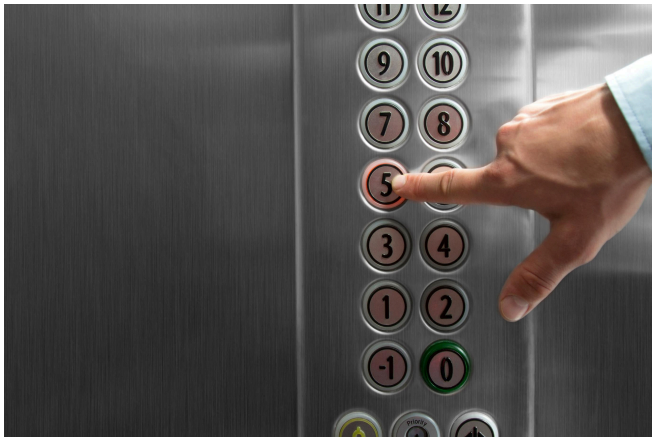

图 1. *现代电梯按钮示例。*

我们来回顾一下预期功能设计和安全功能设计的流程。

在电机驱动器的预期功能设计流程中，系统工程师选择微控制器 (MCU) 来满足预期功能的要求。随后，他们分配检测功能（例如集成模数转换器 (ADC) 通道），以监控转子位置、线路电流、相电压和系统温度。然后，系统工程师继续使用 MCU 的可用处理能力（例如 CPU 的每秒百万条指令 (MIPS)）来运行电机控制算法，以及可用的驱动外设（例如脉宽调制器 (PWM)）来驱动电机驱动器电路。此过程通常需要几个月，还涉及设计印刷电路板 (PCB)、开发电机控制算法以及开发和调试所有嵌入式软件。

在由一个独立的、有些孤立的团队负责处理安全功能设计流程的组织中，会有一名单独的功能安全专家负责检查系统工程师最初选择的 MCU 的功能安全手册。在某些情况下，功能安全专家可能会发现独立安全元素 (SEooC) 安全概念需要使用软件测试功能，包括错误测试、硬件冗余、数模转换器 (DAC) 至 ADC 环回检查或通过增强型捕捉监控增强型 PWM。回顾之前的电梯示例，可能有必要使用多个 ADC 通道来监控每个楼层上的水平传感器，以防止 MCU ADC 中出现“卡住”故障。

如果 ADC 和 PWM 通道不足或 CPU MIPS 不足，无法实现功能安全，可能需要返回到制图板并选择另一个 MCU

来实现功能安全系统，这可能会使独立系统设计团队迄今为止完成的工作付诸东流。

即使设计步骤不是按顺序进行，它们也经常在独立的组织孤岛中进行；也就是说，系统工程师通常不具备任何功能安全专业知识，而功能安全专家也不是系统工程师。这种孤立的方法最终会带来同样的问题：系统成本增加和面市时间延误数月。

设计功能安全电机控制和驱动系统的推荐方法

设计功能安全系统的系统工程师的最终目标是在设计流程的一开始就着手处理功能安全合规性。

设计和提供符合设计预算的功能安全系统需要对安全合规性和预期功能进行协同分析。独立或依次处理工程可能会带来挑战，甚至无法满足系统设计目标。考虑到之前的由团队管理安全功能设计流程的示例，尽早开展协作或许可以避免选择新 MCU 和重新配置 PCB。

实际上，另一个示例可能说明了建议的方法。人类同时利用左脑（逻辑）和右脑（创造性）来全面解决问题，如**图 2** 所示。

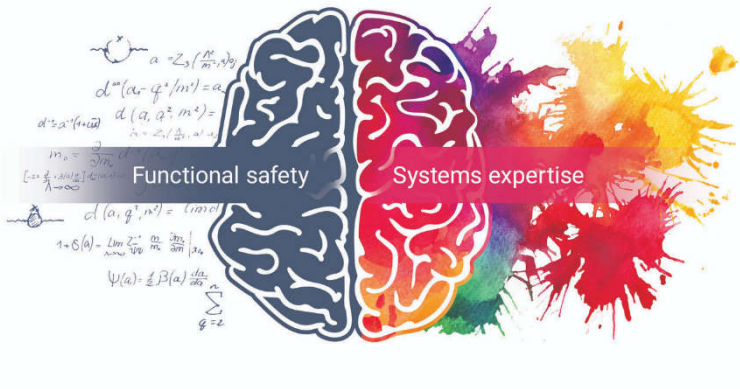

***图 2.** 整个大脑在系统设计和功能安全合规性方面拥有统一的专业知识。*

将大脑想象成一个组织，其中每一半代表不同的团队或内部设计资源，能够在设计流程中提出特定学科的观点。他们可以在设计工作流程中作为一个单元协同工作，从专业角度处理设计，同时保持清晰持续的沟通。

同样，有效的设计工程需要系统设计人员和功能安全专家团队协同工作来实现功能安全系统。

为了帮助缩短产品面市时间，系统工程师需要合适的设计资源。例如，TI 提出了子系统级和系统级功能安全概念，并由第三方独立评估。

TI 如何帮助您设计功能安全系统

TI 的产品系列种类繁多，涵盖电机驱动器和栅极驱动器到基于专有 CPU 架构的 MCU，包括基于 C2000™ 和基于 Arm® Cortex® 的 MCU，例如 AM2434BSDFHIALVR。这些产品具有高级诊断功能和片上感应外设，能够快速检测故障并对其做出反应，同时更大限度地减少系统停机时间（在工业环境中，可提高工厂生产力）。

为了帮助您找到更有效的器件来进行功能安全设计，TI 定义了三个适合在功能安全应用中使用的产品类别：TI 功能安全型、TI 功能安全质量管理型和 TI 功能安全合规型。（我们的电机驱动器、栅极驱动器和 MCU 通常是 TI 功能安全合规型产品。）

TI 设计和构建这些产品来满足 IEC 61508 和 ISO 26262 的系统功能合规性建议，使您能够构建安全可靠的电机控制和驱动系统。我们为每个器件提供失效模式、影响和诊断分析 (FMEDA)、功能安全手册以及（若适用）安全诊断库，系统和子系统功能安全概念报告可在 TI.com 上找到或通过申请获得。TI MCU 的功能安全手册包括 SEooC 的背景介绍，并概述了示例应用可能的故障组。

我们的设计资源示例包括适用于工业驱动器且经过 TÜV SÜD 评估的 STO 模块，如***适用于工业驱动器且经过 TUEV 评估的安全转矩关闭 (STO) 参考设计 (IEC 61800-5-2)*** 中所述。请访问 **www.ti.com.cn/zh-cn/technologies/functional-safety.html**，详细了解我们的功能安全产品并查看设计资源。

TI 在符合 ISO 26262 SEooC 和 IEC 61508 标准的部件，以及使用 TI 产品的功能安全型系统的类型方面拥有丰富的经验。当然，实现这些优势需要平衡开发预期功能和安全功能的复杂需求。

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