简化汽车和工业领域的功能安全认证

Miro Adzan
总经理
工业系统
工厂自动化与控制
德州仪器 (TI)

Arun Vemuri
总经理
汽车系统
车身电子与照明
德州仪器 (TI)

合理的功能安全设计离不开严谨的态度和大量的文档参考，也需要投入一定的时间。无论您从事工厂车间还是公路方面的设计，此白皮书中 **TI** 的集成电路 **(IC)** 设计方法都会为您提供所需的资源，从而简化功能安全设计。

随着工业和汽车领域自动化的出现，人们对功能安全的需求有增无减。所有的工业应用都有功能安全要求，尤其是在工厂自动化和控制系统中。

在汽车行业，尽管安全气囊和制动系统在多年前就具备了功能安全性，但随着电气化水平的提高和自动驾驶功能的出现，系统需要控制电池管理、传感器融合和车辆操作，进而增加了对功能安全设计的需求。

无论是设计工厂机器人系统、家用电器还是未来的汽车，人们对设计工程师提出了更高的要求，即交付的项目应符合应用相关的功能安全标准。

在不要求遵循标准的应用中，设计更安全的系统是在同类竞争产品中脱颖而出的关键因素。

功能安全标准

功能安全是系统整体安全性的一部分，是对某些输入或故障状态做出预测性响应。功能安全标准认为危险总是存在的，因此，所有系统都有一个固有故障率。

功能安全标准对如何开发系统作出了规定，从而将故障率降低到可容忍水平。包含功能安全的系统设计必须能降低由操作不当引发故障的风险，还能检测故障并充分降低故障造成的影响。

为实现功能安全合规性，工程师必须：

- 预测并定义危险状况。
- 确定能应对危险状况的安全功能。
- 评估安全功能的风险降低等级。
- 确保安全功能符合设计初衷。

功能安全标准是由标准组织以及相关行业企业共同制定的，它通过定义系统中的安全功能和建立安全等级评定规范，为设计人员提供了指导。德州仪器 (TI) 加入标准组织，有助于确保其产品开发从始至终都符合功能安全要求。

常见的安全标准包括国际电工委员会 (IEC) 的 61508 标准（针对工业应用）、国际标准化组织 (ISO) 的 26262 标准（针对汽车应用）以及 IEC 60730 标准（针对家用电器）。

各类安全标准都规定了风险降低等级和安全完整性等级 (SIL)。例如，IEC 61508 标准将 SIL 划分为 SIL 1 至 SIL 4 四个等级，其中 SIL 4 的要求最高。SIL 1 要求安全可用性为 90% 至 99%，平均要求失效率 (PFDavg) 为 0.1 至 0.01，风险降低因子 (RRF) 为 10 至 100。SIL 4 要求安全可用性

>99.99%，PFDavg 为 0.0001 至 0.00001，RRF 为 10,000 至 100,000。

ISO 26262 标准的 ASIL 等级与 SIL 类似，即从 ASIL A 至 ASIL D，其中 ASIL D 的要求最高。

功能安全流程

在功能安全开发流程中，通常需要先确定各种危险情况和功能安全目标。然后，工程师开始检查系统架构、模块和 IC。之后，将 IC 作为符合功能安全标准系统的主要构建块进行开发。

为预测系统可能出现的行为，工程师必须量化和预测模块的运行情况。为此，工程师必须在开发流程中对系统进行结构化安全定性分析，从而找出各种失效模式、失效原因及其影响。

功能安全标准规定了工程师需要了解的 IC 相关信息，便于工程师独立进行失效模式、影响和诊断分析 (FMEDA)。由于 IC 的复杂度不同，系统安全分析可能需要有关设计、芯片和封装的信息。

在此过程中，请务必从可靠的供应商处选择合适的器件。无论是用于功能安全设计，还是用于实现差异化竞争的较安全系统中，TI 都能让工程师更轻松地找到并使用合适的产品。

借助功能安全类别简化器件的选择

典型的工业和汽车应用需要复杂度迥异的大量 IC，如一个或多个传感器和传动器，处理传感器数据的微控制器 (MCU) 或处理器，模拟多路复用器，运算或仪表放大器，可能与或未与处理器集成的模数转换器 (ADC) 和数模转换器，直流/直流转换器，低压降稳压器或电源管理 IC (PMIC)，以及 LED 驱动器、电机驱动器、电磁阀驱动器、场效应晶体管 (FET) 和绝缘栅双极晶体管栅极驱动器等驱动器元件，电源开关和负载开关。另外，应用还包括各类通信接口，如 RS-485、控制器区域网 (CAN)、以太网、FPD-Link 和外围组件快速互连 (PCIe) 接口。

表 1 所示是 TI 为功能安全设计提供的产品类别，这也表明了基于标准的 IC 复杂度分类依据。这些类别包括 TI 功能安全型、TI 功能安全质量管理型、TI 功能安全合规型。

功能安全合规型产品

这类产品通常都是系统中相当复杂的器件，如 MCU、处理器或模拟电机驱动器，可能具有集成的安全功能。

TI 使用经 Technischer Überwachungsverein (TÜV) SÜD 等机构认证的功能安全开发流程，开发了这类

		功能 安全型	功能 安全质量管理型	功能 安全合规型
开发流程	TI 质量管理流程	✔	✔	✔
	TI 功能安全流程			✔
分析报告	功能安全时基故障率计算	✔	✔	✔
	失效模式分布 (FMD) 和/或引脚 FMA**	✔	包含在 FMEDA 中	包含在 FMEDA 中
	FMEDA		✔	✔
	失效树分析 (FTA)**			✔
诊断说明	功能安全手册		✔	✔
认证	功能安全产品证书***			✔

表 *1. TI* 用于功能安全设计的产品类别。

** 可能仅适用于模拟电源和信号链产品。

*** 适用于部分产品。

产品。这类认证可确保这一类别的产品是按照功能安全标准（ISO26262 和 IEC61508）规定的规格开发的。

以下列复杂的功能安全合规型器件为例：

- 用于高级驾驶辅助系统、符合汽车电子委员会 (AEC)-100 标准的 Jacinto™ TDAx 片上系统，集成了定点和浮点 TMS320C66x 数字信号处理器 (DSP) 内核、Vision AccelerationPac 嵌入式视觉引擎和双核 ARM® Cortex®-M4 处理器，以及用于低压差分信令环视系统、显示、CAN 和千兆位以太网音频视频桥接的多摄像头接口等外设。这些器件满足广泛的功能安全系统要求，包括具有错误校正码 (ECC) 保护机制的 M4、具有 ECC 保护机制的 32 位双倍数据速率接口、适用于中央处理单元 (CPU) 的专用内存管理单元、内存保护单元、温度监测传感器，以及用于系统监控的八通道 ADC。
- TPS6594-Q1多轨电源管理集成电路（PMIC）支持汽车和工业市场采用的TI Jacinto TDAx 片上系统。PMIC精度高、灵活性强，适合要求功能安全的汽车和工业应用，并会提供功能安全文档。TPS6594-Q1为主域和MCU域提供可扩展的电源管理解决方案，并支持ASIL-D/SIL-3级别的功能安全
- Hercules™ MCU 集成了足够多的安全和诊断功能，可让工程师达到 SIL 3 的目标等级。也就是说，此 MCU 可实现约 99% 的故障覆盖率。例如，在 MCU 上集成两个采用锁步模式的 Cortex-R CPU，可在每个周期对输出进行比较，如出现错误，则会产生非屏蔽中断。在工业应用中，CPU 可在启动时或时间片内进行自检。
- DRV3245E-Q1 是一款适用于三相电机驱动应用的 FET 栅极驱动器 IC。它的三个半桥驱动器可分别驱动高侧和低侧 N 沟道金属-氧化物-半导体 FET。根据 ISO 26262 的适用要求，该栅极驱动器为每个内部时钟集成了诊断和保护功能，还提供了常用系统诊断检查支持，二者皆可通过串行外设接口实现实例化和故障报告。借助灵活的功能，DRV3245E-Q1 可无缝集成到各种安全架构中。
- TPS65381A-Q1多轨PMIC采用双核同步或松散耦合的体系结构，为汽车和工业市场上的TI Hercules TMS570和C2000™ MCU系列产品提供支持。配备内部FET的异步降压开关式电源转换器可将输入电源（电池）电压转换为6-V前置调节器输出电压。然后由6-V的前置调节器为其他调节器供电。它的监控和保护模块，包括电压检测、模拟内建自测、时钟丢失检测、接点温度检测、电源电流限制和MCU误差信号监测等，都能提高诊断覆盖率并降低未检测到的故障率。
- TI 可提供属于这一类别的多种器件，如 C2000 实时控制器和具有板载 DSP、MCU 和雷达加速器的 AWR1843、76GHz 至 81GHz 汽车雷达传感器。所有这些产品都附有专用的功能安全相关文档，以支持系统开发流程：
  - 功能安全时基故障 (FIT) 率计算。
  - 失效模式分布 (FMD)。
  - FMEDA。
  - 失效树分析。
  - 功能安全手册，介绍了 IC 安全功能以及如何使用外部元件实现一定的故障覆盖率和诊断功能。
  - 功能安全产品证书。

功能安全质量管理型产品

第二类产品包含内置诊断功能的复杂产品，且专用于有功能安全要求的系统。但是，这一产品类别在开发时没有按照适用于功能安全合规型产品类别的认证功能安全开发流程，而是使用 TI 的标准质量管理开发流程。

此类别的产品包括但不限于：

- TCAN4550-Q1是业界首创的汽车系统基础芯片（SBC），含集成式CAN FD控制器和收发器。这款高度集成的设备利用现有的SPI端口简化CAN FD总线扩展，这样设计师就可以在升级至

更高宽带CAN FD接口协议时维持当前基于微控制器的结构体系。

- LP87702-Q1是一款双降压和5-V升压转换器，集成符合ASIL的毫米波雷达系统要求的诊断功能，其中包括视窗监控器和一个监控其输出电源的独立参考电压、以及两个外部电源。

对于功能安全合规型器件，我们提供了各种文档，可帮助进行功能安全系统设计。这些文档包括功能安全时基故障率计算、FMEDA 和功能安全手册。非功能安全合规型器件则不包括无故障分析或产品认证。

功能安全型产品

第三类产品包含的 IC 较简单，开发时使用 TI 的标准质量管理开发流程，与功能安全质量管理型产品类别类似。

功能安全型产品通常不具备集成的安全功能，所以通常不会提供内置的监控和诊断功能，这些功能在 TI 其他功能安全产品类别的器件中较常见。

由于这类产品没有集成全面的安全功能，它们不具备其他类别器件常见的内部监控和诊断功能。

但它们仍是功能安全系统中的重要构建块，因此，TI 会提供功能安全时基故障率和 FMD 等重要信息，供设计人员在安全分析中使用。

此类别的产品包括但不限于：

- 小巧的线性热敏电阻TMP61-Q1因长期传感器漂移小于1%且精度优于传统热敏电阻而颇受青睐。我们的热敏电阻替代产品TMP235-Q1是一款精密温度传感器集成电路，无需校准即可达到±1.5°C。
- TPS3840-Q1 电压监控器或复位 IC。这款符合 AEC-Q100 标准的器件可提供 1.5V 至 10V 的宽电压范围，电源电流典型值仅为 350nA，最大值为 700nA。
- 符合 AEC-Q100 标准的 TPS7A16A-Q1 60V、5μA 静态电流、100mA 低压降稳压器，专为需要超低静态电流的连续或断续（备用电源）电池供电应用而设计。此器件非常适合通过多节电池解决方案（如高电池节数电动工具组和汽车应用）生成低电压电源。TPS7A16A-Q1 不仅能提供一个良好稳压的电压轨，还能承受瞬态电压并在电压瞬态期间保持稳压状态。

评估	计划	创建	验证	上市和停产
确定是否要求执行功能安全流程	确定元件的目标 SIL/ASIL 等级	制定元件级功能安全要求	在器件上验证功能安全设计	记录出现的任何问题（如需要）
任命功能安全经理	制定功能安全计划	在设计规格中添加功能安全要求	说明功能安全设计的特色	报告后续操作中出现的事件（如需要）
阶段末审查	验证功能安全案例	验证设计规格	鉴定功能安全设计（根据 AEC-Q100 标准）	更新副产品（如需要）
	提交功能安全案例	开始功能安全设计	敲定功能安全案例	
	分析目标应用，作出系统级功能安全假设	对设计进行定性分析（即失效模式分析）	评估项目	
	阶段末审查	验证定性分析	发布功能安全手册	
		验证功能安全设计	发布功能安全分析报告	
		对设计进行量化分析（即 FMEDA）	发布功能安全报告	
		验证量化分析	阶段末审查	
		重复功能安全设计流程（如需要）		
		阶段末审查		

表 *2.* 功能安全活动在 *TI* 的标准开发流程中具有重要作用。

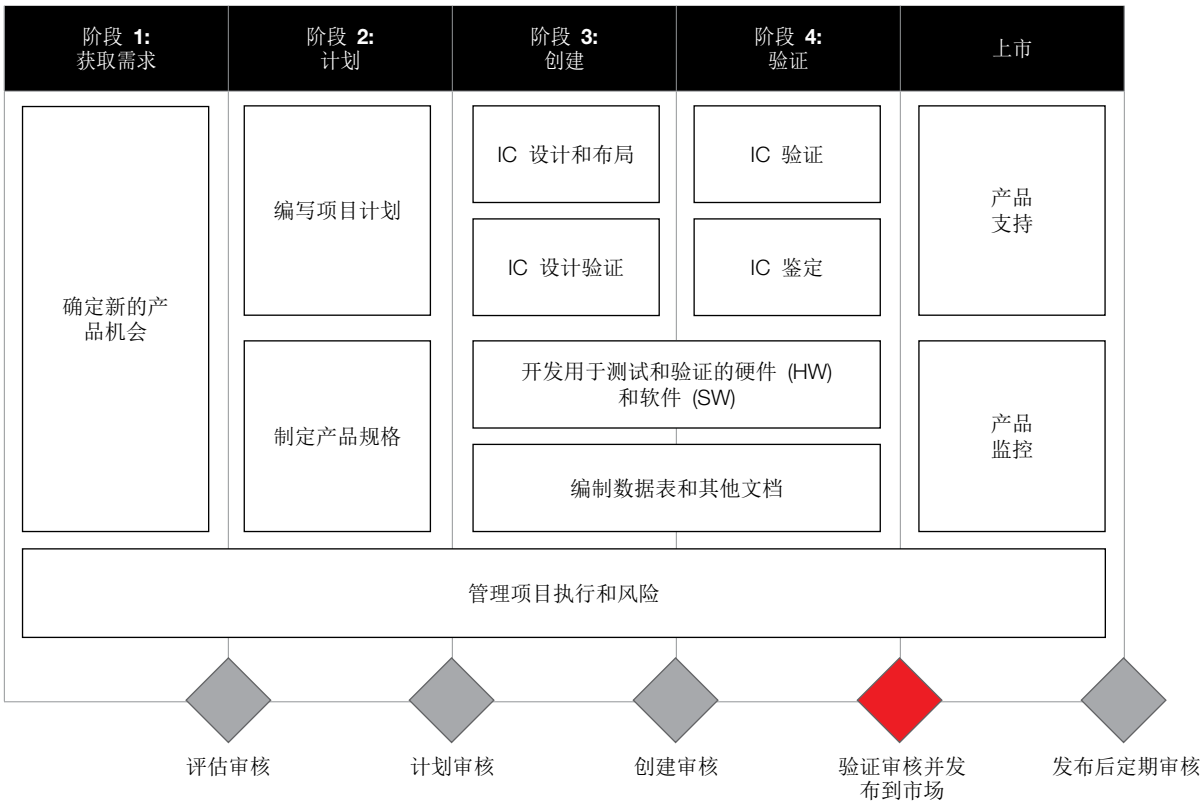

图 *1.* 添加的功能安全活动可能安排在标准质量管理开发流程中。

TI 开发流程

由于功能安全开发流程较复杂，除 TÜV SÜD 认证外，您可能需要了解更多有关公司安全文化和流程的信息。这也是 TI 为管理系统失效和随机失效而创建开发流程的原因所在（见表 2）。

我们的所有产品都遵循质量管理开发流程，从而降低系统失效率。图 1 所示的标准开发流程具有管理系统失效所需的很多要素。此外，这些产品的文档和报告可用于帮助遵循针对最终应用（包括汽车和工业系统）的各种标准（例如 ISO 26262-4 或 IEC 61508-2）。

该流程将开发分为以下几个阶段：

- 评估。
- 计划。
- 创建。
- 验证。

TI 的功能安全开发流程是根据 ISO 26262 和 IEC 61508 制定的。我们向新产品标准开发流程的每个阶段都添加了几项特定的功能安全活动，从而划分出三个基于标准的 IC 复杂度类别。

如 ISO 26262-2:2018 附件 A 所述，TI 的开发流程有利于真正实现功能安全。该开发流程可促进在所有产品开发团队之间共享功能安全类信息。

TI 团队根据适当的标准维护特定组织的功能安全规则，而且其各个流程可确保解决发现的安全异常情况。TI 根据通用标准维护可满足功能安全要求的质量管理系统，从而为客户提供支持。

不断提供功能安全产品系列

功能安全设计侧重在概念阶段就对各类危险、失效和缓解措施作出详尽的计划。这涉及根据标准分析各类系统失效以及所实施诊断方案的有效性。在此期间，需要反复研究用于构建系统的各个器件相关的数据。

TI 不仅持续开发相关产品，还提供这些产品的所有必要数据和文档用于功能安全应用，可帮助满足上述需求。

了解 TI 的功能安全技术

更多资源

- 视频：了解ADC的功能安全及系统级故障检测。
- 视频特辑：C2000™ MCUs的功能安全。
- 视频特辑：TI的功能安全。
- 白皮书：电动汽车和自动驾驶汽车功能安全系统的执行机构设计趋势。
- 白皮书：利用Jacinto™ 7处理器功能安全特性的汽车设计。
- 白皮书：C2000™ MCU SafeTI™控制解决方案：ASIL分解及SIL合成简介。

重要声明和免责声明

TI 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安全、安保或其他要求。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 (https:www.ti.com.cn/zh-cn/legal/termsofsale.html) 或 ti.com.cn 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。

邮寄地址：上海市浦东新区世纪大道 1568 号中建大厦 32 楼，邮政编码：200122