消除 ISO 26262 功能安全认证过程中的各种障碍

Microchip Technology Inc.

功能安全技术工程师

Jacob Lunn Lassen

现今，汽车的各种应用中无不使用数百到数千种半导体和其他组件，例如触摸界面、车载充电器、电池管理系统等等。严格的国际标准化组织（ISO）26262 功能安全规范可确保这些日益复杂和精密的应用安全运行。然而，开发合规设计及获得认证的过程十分耗时且成本高昂。随着半导体行业为汽车原始设备制造商（OEM）和供应商提供完整的功能安全生态系统，这最大限度降低了完成这类认证过程的成本，同时降低了风险并缩短了开发时间，进而使这些挑战得到缓解。

了解 ISO 26262

ISO 26262 标准包含安装在批量生产的道路车辆（轻便摩托车除外）中的电气和/或电子系统的功能安全规范。该 ISO 标准于 2011 年发布，并于 2018 年修订以包含关于半导体的部分，其中规定了从规范到生产发布的开发过程。汽车 OEM 和供应商在对道路车辆内部需要功能安全的运行器件进行认证时，必须遵循并记录此过程。

系统认证需由独立评估员确认其符合 ISO 26262 标准的要求来完成。汽车内应用根据其安全关键性级别“归类”为不同的汽车安全完整性等级（ASIL）。如果电气或电子系统发生故障，则某些应用具有更高的固有安全风险。根据潜在伤害的严重程度和发生概率以及可控程度，分为 A 到 D 四个级别，每个级别都对底层组件有相关的安全要求。ASIL D 表示汽车中安全气囊、防抱死制动系统和动力转向等危险程度最高的应用。尾灯等组件归类为 ASIL-A。头灯和刹车灯通常归类为 ASIL-B。巡航控制等系统归类为 ASIL-C。通常，ASIL 级别越高，对硬件冗余的要求就越多。

组件供应商可通过多种方式帮助加速安全应用的设计及其 ISO 26262 认证过程。这些功能安全资源如图 1 所示。首先，必须仔细选择器件以包含必要的功能安全资源。这些资源包括故障模式影响和诊断分析（FMEDA）报告及安全手册。此外，器件还必须得到有资格创建安全关键型应用的开发生态系统的支持。

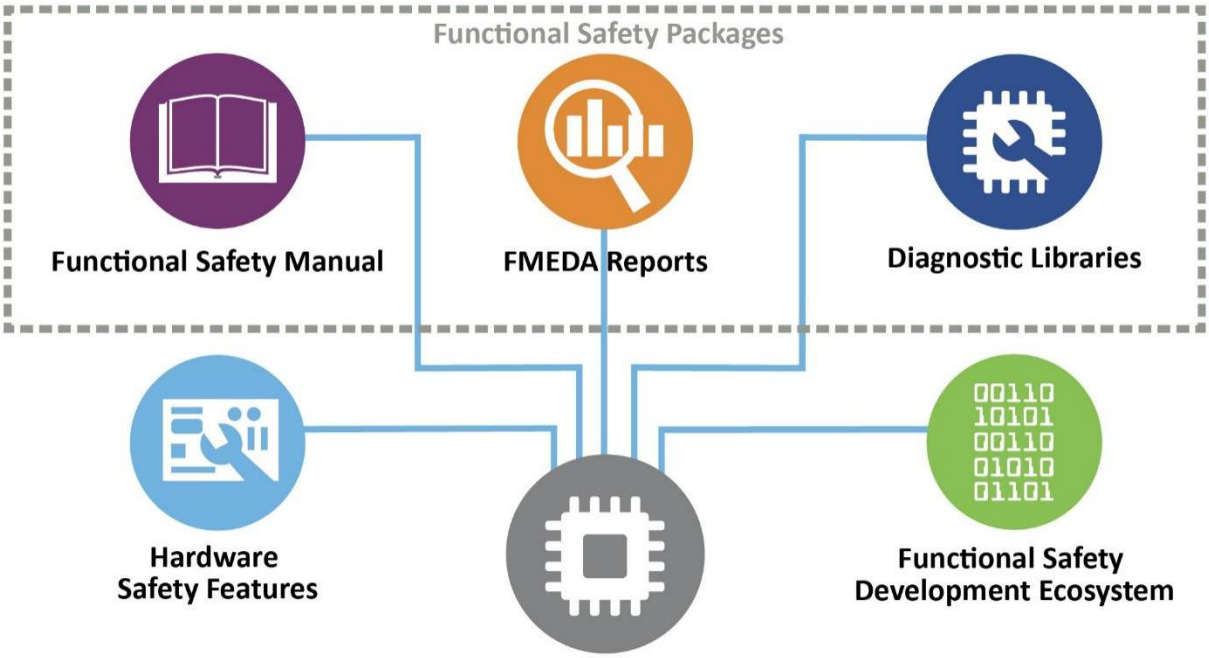

图 1：经过认证的功能安全资源和开发生态系统

功能安全就绪

现今的汽车中使用了各种 IC。尤其是单片机（MCU），它以各种形式普遍存在。所有电子控制单元（ECU）都需要用到单片机，并且全车使用单片机来提供便利功能（例如自动驾驶）和各种其他复杂功能。单片机范围广泛，涵盖针对性能、电源效率和实时控制进行优化并添加基于硬件的触摸界面的 8 位 MCU，到可以运行多线程应用并支持图形、连接和安全功能的 32 位 MCU。此外，还有将 MCU 与 DSP 引擎相结合的数字信号控制器（DSC），可为传感器、电机或电源转换提供可靠且快速的确定性性能。

其中每一个 IC 都必须首先满足汽车电子委员会（AEC）制定的汽车级制造和性能认证标准。AEC-Q100 标准定义了跨温度等级的基于失效机制的压力测试认证过程。根据具体应用，MCU 需要通过 AEC Q100 2 级、1 级或 0 级认证。0 级 = 150℃，1 级 = 125℃，2 级 = 105℃。

除了 AEC 认证之外，还有额外的专用功能安全就绪特性要求，具体取决于器件和应用。例如，8 位 MCU 通常包括用于汽车接口和智能传感器网络的 CAN FD，并且通常用作驾驶室、方向盘、中控台内机械和电容式按钮的用户界面（UI）控制器，或用作无钥匙进入系统的一部分。8 位 MCU 所需的集成硬件安全功能通常适用于存储器、系统复位、安全代码执行、安全通信和通用输入/输出（GPIO）保护。这些功能是通过集成专用的独立于内核的外设（CIP）和其他功能添加的，包括上电复位（POR）、欠压复位（BOR）、窗口看门狗定时器（WWDT）和循环冗余校验（CRC），用于提高操作安全性和可靠性（见图 2）。

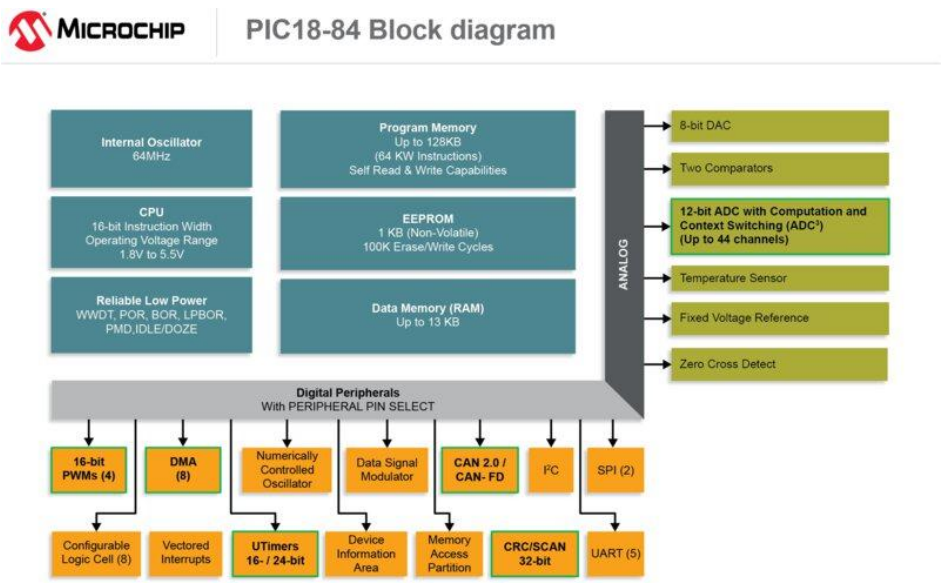

图 2：具有功能安全硬件特性的 8 位 MCU

对于功能安全就绪 16 位 DSC，所需的硬件安全功能通常包括支持错误检测和纠正的存储器、存储器内置自检（MBIST）、时钟监控和冗余振荡器等，这些功能用于故障检测、自诊断和系统诊断以及故障修复。这些功能安全就绪器件支持设计安全关键型高性能嵌入式应用、传感器接口应用、数字电源和电机控制应用。典型应用包括直流/直流系统、车载充电器（OBC）、执行器和传感器（位置和压力）、触摸单元和其他符合 ASIL B 或 ASIL C 标准的控制单元。图 3 显示了功能安全就绪 DSC 的功能示例。

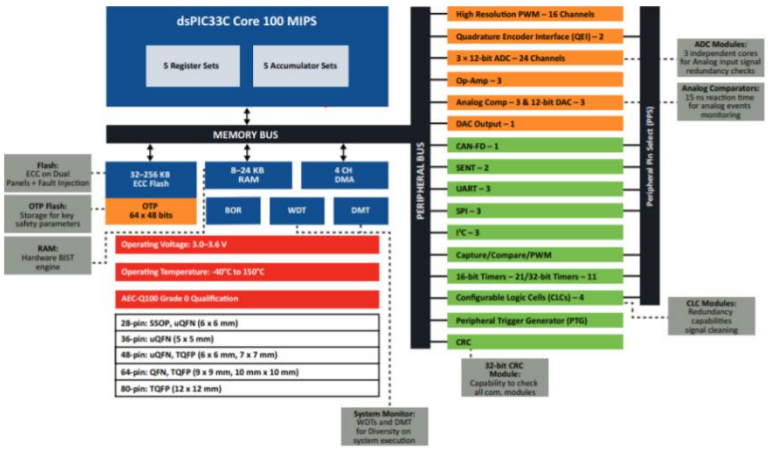

图 3：功能安全就绪 16 位 DSC 示例

与所有功能安全就绪 MCU 一样，32 位 MCU 所需的硬件功能包括支持纠错码（ECC）和错误注入的存储器、存储器内置自检（MBIST）、时钟系统（包含备用振荡器和时钟故障检测）以及具有静电放电（ESD）保护的 GPIO（见图 4）。同样重要的是系统监视器，其中包括 POR、BOR、WDT 和硬件 CRC 功能以及存储器保护单元。32 位 MCU 的适用范围涵盖从驾驶室内部系统到高级驾驶辅助系统（ADAS）等一系列应用，可用于实现功能安全。

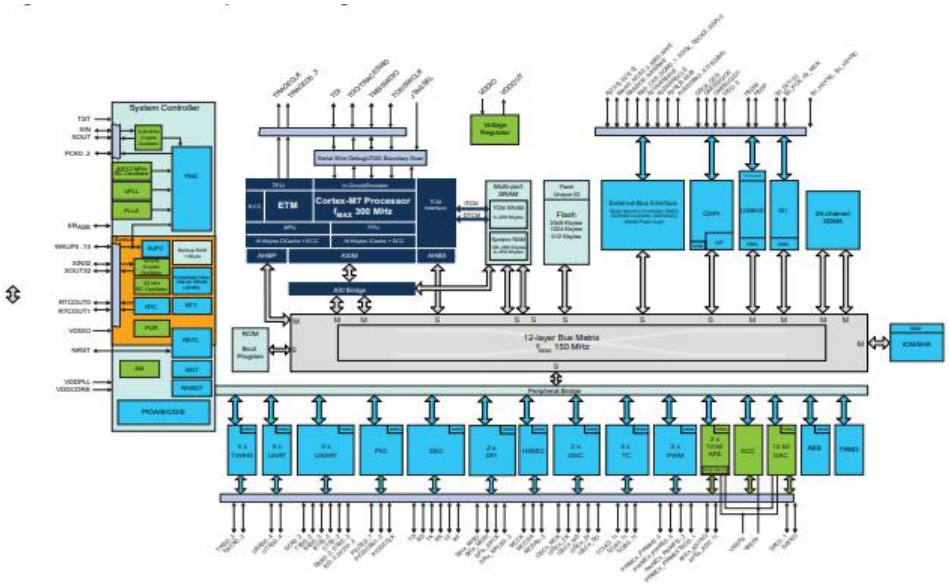

图 4：功能安全就绪 32 位 MCU 示例

通过将主 MCU/DSC 与辅助 MCU/DSC 或安全协处理器相结合，甚至可以使用标准 MCU 和 DSC 达到 ASIL C/D 安全级别。这是通过使用 ASIL 分解原理来实现的：两个符合 ASIL B 标准的子系统组合可用于达到更高的 ASIL，例如 ASIL C/D：

ASIL C = ASIL B (C) + ASIL A (C)
ASIL D = ASIL B (D) + ASIL B (D) = ASIL C (D) + ASIL A (D)

分解是通过划分安全要求与实际器件实现的。

开发工具和认证支持

作为完整开发生态系统的一部分，经过功能安全认证的设计工具包可以更轻松地满足 ISO 26262 标准中规定的验证和确认要求。这一点尤其适用于基于 MCU 和 DSC 的设计。工具供应商与第三方独立评估和认证机构合作，对功能安全编译器进行认证。这通常附带额外的文档，例如编译器、集成开发环境（IDE）以及调试器和编程器的证书、功能安全手册、安全计划及工具分类和资格认证报告。该功能安全文档包简化了工具的资格认证和最终应用认证。

理想情况下，还应该在设计过程中使用代码覆盖率工具来衡量代码的测试效果，并确定软件的哪些部分已经执行或尚未执行。 代码覆盖率工具也应包含在分类和资格认证报告中。寻找一种可以单次运行测试的工具，此工具无需将代码分解为各个模块，也无需对硬件进行大量修改或使用昂贵的软件，同时还能避免在大型数据文件中搜索相关信息的大量工作。应用认证需要代码测试数据，因此单次运行代码覆盖率工具在简化流程和缩短上市时间方面发挥着重要作用。

要开发符合 ISO 26262 标准的汽车应用，除了器件数据手册之外，工程师还需要从半导体供应商处获得一些额外资源。可用的功能安全包为汽车 OEM 和供应商提供了他们在评估和设计周期的各个阶段所需的内容。这些功能安全包应提供经过认证的安全手册、FMEDA 报告，在某些情况下，还应提供诊断软件，例如经过相关 ASIL 认证的自检库。

FMEDA 报告量化了器件的故障模式、其故障率（FIT）分布及相应的检测方法，可帮助制定覆盖率计划。另一个重要资源是安全手册（SM）。它详细介绍了 FMEDA 报告中指定的故障检测方法，并就如何使用器件实现最安全的操作提供了建议。安全手册中包含相关故障以及用于检测系统故障的硬件功能说明，可使用该说明开发诊断库。功能安全诊断库可帮助评估系统在故障条件下的运行状态，检测随机系统故障以及实现功能安全目标。选择提供第三方认证的 FMEDA 报告和安全手册以及诊断库的器件可以简化安全关键型应用的认证工作。

安全关键型应用开发的第一步是定义要实现的安全目标和要达到的目标安全级别。功能安全基础包提供 FMEDA、安全手册和认证等基本资源，帮助用户开始评估目标功能安全级别和设计安全关键型汽车应用。

理想情况下，基于 MCU 的设计的功能安全入门包应包括经过 ASIL B 就绪认证的 FMEDA、安全手册和符合 ASIL B/C 标准的诊断库，以及帮助设计人员了解如何使用这些资源按照 ISO 26262 流程开发安全关键型应用的参考应用。入门包有助于缩短设计周期，并根据 ASIL B 或 C 合规性开发应用。

功能安全完整包可以进行扩展以包含经过认证的诊断库，其中提供用于实现最高 ASIL B/C 级别的设计所需的源代码和相关安全分析报告。鉴于许多最终客户要求对安全关键型应用进行认证，完整包还有助于加快认证过程。

随着汽车的复杂度越来越高，其中的电子元件水平也在不断提高。越来越重要的是，现今，面向汽车应用、以功能安全为重点的产品支持开发生态系统，可提供经过认证的功能安全资源来满足 ISO 26262 要求。IC 供应商还可以帮助汽车客户保护其在这种严密开发和认证过程中的长期投资。他们能够确保只要客户愿意订购，就会持续供应认证系统内使用的器件，从而消除了由于器件意外进入停产（EOL）阶段而导致被迫重新设计的风险。这意味着认证不仅可以快速轻松地完成，而且只需完成一次，因此更加值得客户信赖。

###