白皮书

集成了安全性的硬件解决方案，为ASIL-D应用提供支持

作者：
Valerie Bernon-Enjalbert
Mathieu Blazy-Winning
Regis Gubian
David Lopez
Jean-Philippe Meunier
Mark O'Donnell

摘要

对安全性至关重要的应用进行实时控制一直是工程师所面临的挑战。应用功能变得越来越复杂，并且，在汽车和工业市场中，行业标准要求更加全面的功能安全概念。对一个系统的功能安全性的评估需要大量参与和验证工作。为此，飞思卡尔推出了SafeAssure计划，目的是帮助系统制造商简化评估，从而更轻松地满足国际标准化组织(ISO)的标准。本白皮书涵盖了各种安全架构的实施，以及简化系统级功能安全设计，并符合ISO 26262标准的创新型集成安全解决方案的详细信息。

目录

2 介绍

2 什么是功能安全?

3 安全开发管理：SafeAssure流程

3 量化剩余风险 – 架构指标

4 ASIL-D解决方案及安全架构的影响

8 结束语

介绍

在汽车应用中，人体与电气电子系统之间的交互大大增加了，特别是在进行安全性至关重要的决策时尤为如此，因为此类决策会对驾驶员的人身安全造成严重影响。随着这些先进的系统从被动安全趋向更多的主动安全（包括预测安全直至自动驾驶概念），汽车行业一如既往的需要满足严格的功能安全要求。

这些安全性至关重要的决策管理会变得更加复杂，安全系统中会出现更多的软件内容。由于复杂性的提高，系统性和/或随机硬件故障的风险也相应地增加了。为了帮助确保最高的安全标准并推动汽车安全系统的开发，汽车业已经发布了最新的汽车安全标准：ISO 26262。

本文讨论了各种安全架构的实施，并介绍了一种创新的、综合性安全解决方案，该解决方案能够简化系统级功能安全设计，包括符合ISO 26262标准的要求。

什么是功能安全?

根据定义，功能安全意味着不存在由于系统故障而造成的风险。要大幅降低发生故障的风险，关键是了解并评估可能发生的故障类型。这些故障可分为两类：

1. 系统故障，可归因于某个原因，只能通过变更制造过程、操作流程、文档的设计或其它相关因素消除。借助强大的开发流程可降低发生系统故障的概率。

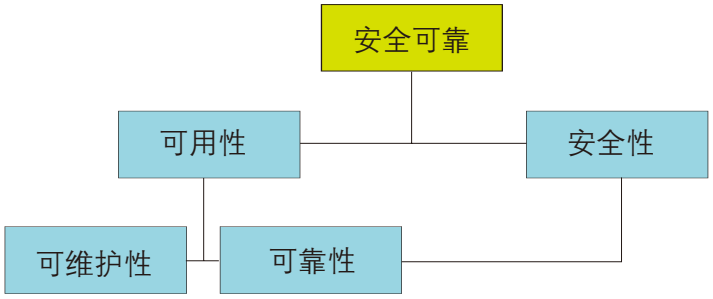
2. 随机故障，这表示在硬件元件的生命周期内发生的不可预知的故障，按照概率分布。这些故障可能是由于永久性或短暂的干扰环境，也可能是在系统的生命周期中，由内部技术的性能而导致。可通过专用架构和IC策略降低随机故障的风险。

2011年11月15日，汽车行业发布了ISO 26262:2011(E) 。该标准专为“道路车辆 – 功能安全”而制定，为汽车电气电子 (E/E) 系统，根据功能安全标准 IEC 61508进行修订。

为了确保车辆的道路行驶安全，所有应用必须保证运行正常、可靠。为了实现安全可靠目标，E/E 系统的设计应实现安全性和可用性的最佳平衡。

可用性是可维护性与可靠性之间的良好平衡点，而安全性主要取决于系统可靠性。这种交互如下图所示。

功能安全可靠性的平衡



飞思卡尔SafeAssure产品的目标是通过将可用性、安全性及可靠性有效地结合在一起，实现安全可靠。

安全开发管理：SafeAssure流程

评估一个系统的功能安全需要进行大量的参与和验证。简化这种评估是飞思卡尔SafeAssure计划的一个主要目标，该计划在2011年9月份制定和启动，适用于汽车和工业应用。

SafeAssure产品的目的是降低功能安全系统的复杂性，这也是系统制造商的一个重要目标。该计划的制定注重故障模式和效应分析(FMEA)、持续流程改进(CPI)和零缺陷。对新产品开发(NPD)流程、工具和指标也进行了修改，整合并满足功能安全要求。具体而言，产品定义阶段现在包括系统级假设，作为描述系统环境的组成部分。对于半导体设备来说，这些假设基于Safety Element out of Context (SEooC)。由于MCU和模拟配套芯片是作为标准解决方案而开发的，其目的是满足多个行业的多种应用，因此SEooC 是作为安全元素，并不针对特定的系统或特定的汽车平台而开发。

量化剩余风险 – 架构指标

架构指标用于评估IC在与安全故障有关方面的性能，用于推动架构选择（包括检测和保护），并支持用户选择自我检查机制。

ISO 26262:2011(E) 根据原始设备制造商 (OEM) 的汽车安全完整性等级 (ASIL) 定义了要实现的安全目标。该标准还提供了评估度量指南。

评估方法之一包括单独检查每个单点故障的残差，以及导致违反特定安全要求的各个双点故障。

在IC设计过程中必须以迭代方式进行评估。为了达到预期系统要求，可采用拥有不同集成度的多个架构。

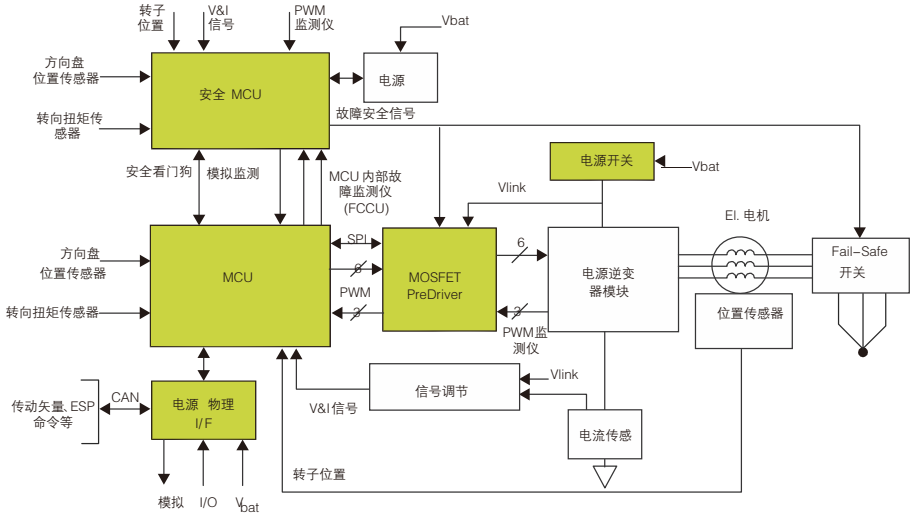
ASIL–D 解决方案和安全架构的影响

电动助力转向(EPS)是要求高级安全性的众多汽车应用之一，其目标是确保汽车的转向系统是可预测、确定性的。

根据特定应用中为满足ASIL–D要求而采用的硬件和软件交互组合，可采用多种方法或系统架构。

第一种方法是使用两个MCU来执行安全输出的外部比较。

基于单内核和安全MCU的EPS



飞思卡尔技术

这种架构的优势是物理复制安全相关和非安全相关的功能与特性。

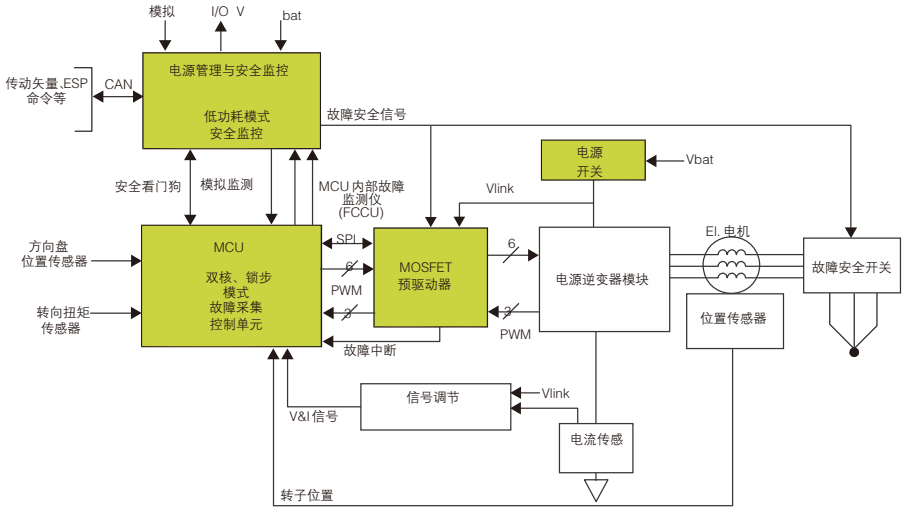
然而，这种配置非常复杂，再加上软件同步及PCB空间增加等因素，会给这种方法带来巨大的挑战和障碍。随着终端设备数量不断增加，系统功能的可靠性和可用性降低了。

这种配置可能会引入如单事件诱因的瞬时故障，在这方面不会实现良好的容限。

飞思卡尔开发的另一种替代方法使用在锁步模式下运行的最新一代多核MCU。该设计包含一个结合了内部自检和高级模拟电源管理的解决方案，能够监控MCU并控制故障安全状态。

第二种方法提高了集成度，减少了电路板的大小，降低了系统复杂性。采用锁步模式，并将监测功能集成到电源装置提高了可用性，实现了更高的安全性。此外，与第一种方法相比，第二种方法降低了软件开发的复杂性。

飞思卡尔面向ASIL-D EPS系统的集成安全架构



飞思卡尔技术

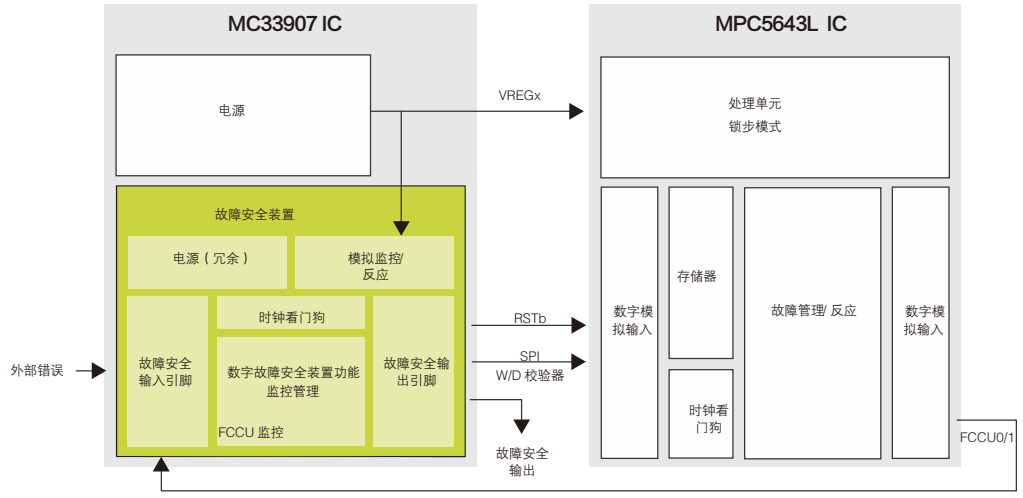
飞思卡尔面向新一代功能安全的硬件系统概念由MPC5643L和MC33907构成，这是最新一代系统基础芯片(SBC)，目的是满足ISO 26262标准的安全要求。

MC33907包含一个能源管理单元 (EMU)，基于可切换到低功耗模式的高效的DC/ DC电源。MC33907的主要功能包括：为MPC5643L MCU供电并对其进行监控。其电源管理与多种安全机制相关联，与 MPC5643L结合开发，以避免应用发生导致可怕事件的故障。在一个系统中使用这两个器件可减少实现ASIL-D系统级解决方案所需的工作量。

MPC5643L是一款双核锁步MCU，采用集成安全架构，为内核、存储器、内部总线、通信模块和外设等提供嵌入式自测试 (BIST) 机制。此外，该器件还进行了优化，可防止时钟或电源电压问题引起的常见故障。MPC564xL系列提供用于检测时钟偏差的硬件模块，以及面向内部内核电压和闪存电源电压等电源电压的硬件监测。双核MPC564xL除了内核外，其它关键硬件模块同样实现冗余，包括内部总线、内存保护单元、中断控制器、DMA和软件看门狗定时器。这种大规模冗余的主要好处是让MCU能够检测内核及主要子模块中经常以软错误出现的单点失效。

下图显示了MPC5643L和MC33907及其有助于确保系统级安全的交叉检验机制。

飞思卡尔面向ASIL-D EPS系统的集成安全架构



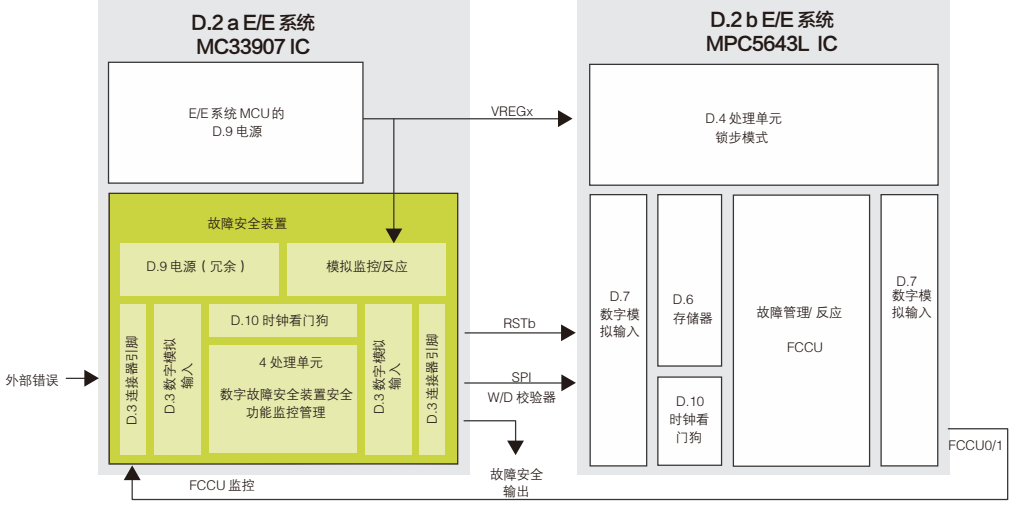
主IC中独立、分离、强大的故障安全装置

飞思卡尔致力于为客户提供能够满足ISO 26262-5:2011(E) 附录D所述要求的硬件解决方案。

飞思卡尔功能安全方法符合ISO 26262-5:2011(E) 附录D所定义的嵌入式系统的通用硬件，其中每个组件（MCU和模拟模块）都作为系统环境外的安全元件而开发。该解决方案包含一个D.2b E/E 系统IC (MPC5643L MCU) 和一个 D.2a E/E 系统 IC (MC33907 MCU)，是一款SBC模拟解决方案（参见下图）。

这两种系统IC中使用的特定的半导体元件可以表示为ISO 26262-5:2011(E) 附录D中的D.1至D.10（参见下图）。 这有利于分解各个元件，指明诊断覆盖范围。

功能安全系统解决方案，包括 ISO 26262 附录D的措施



主 IC 中独立、分离、强大的故障安全装置

下表对以下各项进行了汇总：

- 飞思卡尔安全系统硬件元件列表
- 各个元件实施的安全机制/措施
- 根据ISO 26262-5:2011(E) 附录D的定义，认为各个安全机制/措施能够实现的典型诊断覆盖范围

MC33907和MPC5643L的组合值，目的是满足ASILD要求

元件	安全机制/措施	可实现的典型诊断覆盖范围	飞思卡尔硬件解决方案注释	
D.3连接器引脚	通过在线监控实现故障检测	高	√	短路检测
D.4 处理单元	硬件冗余	高	√	双核锁步
D.5 ROM	借助错误检测校正代码实现存储器监控	高	√	完整性校验和ECC
D.6 RAM	借助错误检测校正代码实现存储器监控	高	√	BIST和 ECC
D.7 模拟和数字I/O	测试模式	高	√	BIST、错误注入校验
	监控输出	高	√	短路检测（包括物理层）
D.8 通信总线	将信息冗余、帧计数器和超时监控相结合	高	√	SPI协议校验器
D.9 电源	电压控制（输出）	高	√	输出欠压(UV)和过压 (OV) 检测
D.10程序序列监控/时钟	将程序序列的时间和逻辑监控与时间相关性相结合	高	√	集成看门狗

此表是ISO 26262 标准实施摘要：集成式硬件架构具有较高的诊断覆盖范围，目的是大大降低危险故障的概率并对各个故障情况采取确定性行为，满足ASIL-D 要求。

信息来源：参考了ISO 26262-5:2011(E) 附录D及飞思卡尔硬件解决方案（MPC5643L 和 MC33907）。

SEooC 的设计结合了 SafeAssure MCU 和模拟系统基础芯片，有利于评估系统的安全性。开发这些器件的目的是满足 ISO 26262 标准的要求，并提供一种可扩展的方法来简化需要符合功能安全标准的系统的开发工作。各个元件之间实现了最佳交互，使系统更简单、更强大。此外，该架构可减少系统级元件的数量，满足功能安全要求，并提高可靠性。

在MC33907里，电源管理单元与故障安全装置相结合，与MCU进行交互。采取了4种安全措施，以确保MCU和SBC之间的交互，分别是不间断供电、监控关键信号的故障安全输入、推动故障安全

状态的故障安全输出以及用于高级时钟监控的看门狗。与MPC5643L MCU结合后，各种安全措施都实现了优化，能够达到最高的安全性能水平。

在组件开发过程中，制定了一套完整的故障模式、影响和诊断分析(FMEDA) 流程，以检测单点失效、潜在失效和共因失效(CCF) 等方面的安全性能。这种安全分析是SafeAssure产品的支持服务交付项目，也是为确定系统安全性而进行的混合器件故障模式分析后的结果。为了降低FMEDA风险，已经实施了器件架构。

例如，通过分离主要功能（电源和通信）和故障安全装置（一组独立的安全功能，如监控、检测和安全状态控制等）来减少CCF。已经采取了这种措施来减少CCF，此外，还与模拟和数字BIST相结合，以减少潜在失效。

在系统层，可以通过故障采集控制单元(FCCU) 的双向稳定协议，由MC33907监控MPC5643L的安全检查机制。这种IC交叉检验类似于监控定时的问询功能，提供系统外部检测，并提供了进一步保证故障检测的另一冗余。

冗余路径与系统基础芯片系列的安全架构相同，要激活安全状态时，通过专用的故障安全输出切换到冗余路径。这些输出是MCU故障安全输出的补充，它们在发生故障时将应用设置在确定性状态。

这些硬件实施方法有助于软件工程师简化软件架构，并实施借助单MCU方法专注于安全性的软件开发战略。

最后，飞思卡尔提供了详细的文档，对功能安全、安全目标及各个组件的安全实施方法进行了描述，支持用户使用标准的半导体器件来管理各种安全应用。

结束语

从评测及架构角度来说，在芯片级实施安全相关功能的新ISO 26262标准尚不成熟。必须要在冗余和简便性之间找到最佳平衡点，才是开发经济高效、安全的解决方案的关键。

采用各种不同的架构均可实现ASIL–D级状态，但是，就目前来说，正确地实施MCU和SBC可让系统变得更简单、速度更快、更加可靠、更经济。MC33907 SBC和MPC5643L MCU的结合使设计人员只需将我们的SafeAssure流程融合到硬件、软件和支持中，便可轻松地将功能安全添加到关键系统中。除了将器件进行组合外，还提供全面的文档（如FMEDA和安全手册），目的是简化硬件架构，并加快任何ISO 26262应用的上市速度。请参见应用说明**“为安全应用集成MPC5643L和 MC33907/08”**。

飞思卡尔独特方法的目的是简化功能安全，降低风险，并降低开发过程的成本。在开发流程的早期阶段（即投入生产前）预测风险并减少潜在故障的影响，有助于提高驾驶员和乘客的安全，并降低制造商的质量成本。

支持

请访问freescale.com/support，获取您所在地区的电话号码清单。

如需了解更多信息，请访问 freescale.com

文档编号：FUNCSAFTASILDWP REV 1