# MCU实现汽车功能安全合规性

## Freescale Microcontrollers for Functional Safety Compliance

Arun Mishra　Markus Baumeister　飞思卡尔半导体公司 首席设计工程师 安全架构师

**摘要**：汽车正在不断加强安全措施，关键汽车操作所使用的安全MCU 都需要遵循 ISO26262 (ASIL-D) 或 IEC61508 (SIL3) 标准。本文讨论了MPC574x等飞思卡尔公司 32 位 Qorivva 微控制器（MCU）提供的主要设计功能。这些功能可帮助最终客户满足汽车 (ISO26262)/工业 (IEC61508) 标准提出的安全要求。稍后我们将讨论飞思卡尔SafeAssure功能安全项目，飞思卡尔将为寻求实现产品功能安全合规的客户提供综合支持。

**关键词**：微控制器；汽车；安全；SafeAssure
DOI: 10.3969/j.issn.1005-5517.2013.3.004

### 功能安全要求

功能安全与最大限度地减少系统故障引起的危险有关。系统故障可能由于硬件/软件错误引起，可能是永久性的，也可能是瞬时性的。下面描述了发生错误时可能出现的反应：

- 故障－危险：发生故障时可能造成危险；
- 故障－不一致：发生故障时提供的结果可能明显不一致；
- 故障－停止运行：发生故障时完全停止运行；
- 故障－安全：发生故障时返回或保持安全状态；
- 故障－可以运行：发生故障时继续正常工作；
- 故障－静音：发生故障时不打扰任何人；
- 故障－指示：向环境指示发生了故障。

在系统中实施功能安全通常意味着将故障映射到能被整个系统或伺机处理的预期反应，从而确保最大限度地减少系统故障引起的危险。

下一节讨论了飞思卡尔片上系统实现的各种功能安全，在发生系统故障时，执行此类映射。

### 飞思卡尔MCU设计提供的主要功能安全

现在深入讨论针对汽车安全应用的飞思卡尔设备的主要安全特性。

#### 核心锁步

确保 SoC 中的内核能够安全运行是功能安全的主要要求之一，这是因为几乎所有的操作都以其为中心。在Qorivva微控制器MPC574x中，通过采用一个与主内核锁步运行的检查内核来实现安全运行。这意味着，检

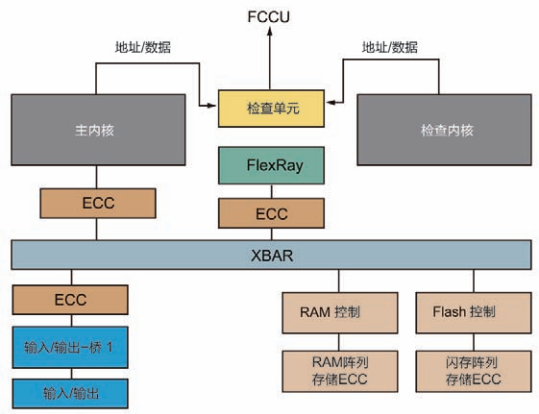


图1　实施 Checker Core（检查内核）和 E2EECC

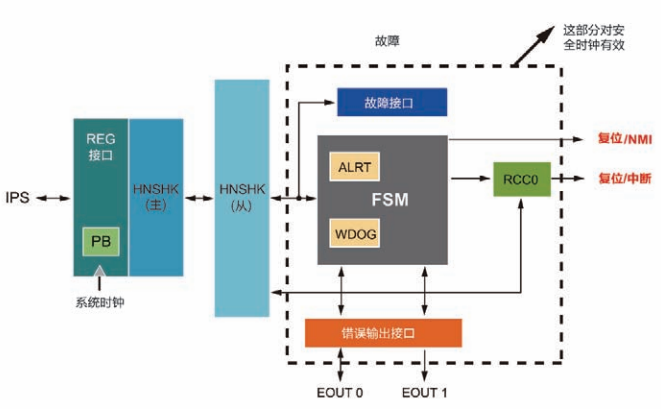


图2　FCCU框图

查内核执行与主内核相同的指令，内核的地址和数据总线在检查单元进行对比，以检测运行偏差。将检测到的错误报告给错误收集和应对模块(见下文)。由于锁步，从软件的角度来看，两个内核作为一个单独的内核运行，减少软件实施。查看下面的图 1 所示的框图。

除了内核，eDMA、中断控制器、缓存等其他安全相关模块可在系统中进行复制。所有此类复制必须在芯片上保持物理隔离，这样，常见故障(CCF) 便不会影响两个实例的运行。

**存储器中提供的端到端 ECC (E2EECC) 保护**

在海明间距为 4 的情况下实现 ECC(纠错码)和 SECDED(单纠错和双纠错)，可保护所有的存储器存储操作。ECC 在数据、地址信号上实现，并通过写操作与数据一起存储在存储器中。发起读操作时，ECC 在检索到的数据和请求的地址上重新进行计算，并通过已存储的 ECC 进行验证。

在Qorivva MPC574x器件中，没有仅用于存储器的ECC，但它提供了E2EECC，可检测总线主设备和总线客户端之间的所有数据路径上的数据损坏，提供至少99%的覆盖率。该机制如下所示。

1)来自主设备的数据通过 ECC-SECDED 代码进行编码。该数据编码包括寻址信息覆盖。

2)路径的各个模块包括本地机制，如确保控制数据的正确发送和正确地址解码。

上述方法可确保数据路径上没有数据损坏。然后主设备提供的ECC被用于RAM和闪存，因此存储器不需要额外的ECC计算，ECC从一端(总线主设备)传到另一端(存储器)。

系统中有一个中央存储器错误管理单元，负责采集和报告与在SRAM、外设系统RAM及闪存上所使用的ECC 逻辑相关的错误事件。 每当发生可纠正(单位)或不可纠正(多位)的错误时，MEMU 都会收到一个错误信号，然后记录错误地址，设置相应的错误标记并报告给FCCU。在需要特殊更正数时或进一步分析软件中这样的错误时，可以使用。

**故障收集和控制单元(FCCU)**

FCCU是一个可编程的单元，监控MCU的完整性状态，提供灵活的安全状态控制，在设备发生故障时通过可控的方式使设备处于安全状态。 收集和控制操作不需要 CPU 的干预。FCCU简易框图如图 2 所示。

FCCU提供一个有限状态机，根据系统中发生的错误以及对这些错误采取的行动/无为，从一个状态迁移到另一个状态。根据故障配置，FCCU可能会触发复位、屏蔽/非屏蔽中断、外部故障指示、或不反应。该SoC 还提供两个外部指示引脚(EOUT0/1)，可以就系统中发生的故障与外部环境进行通信，并遵循各类静态或切换协议。

**自我测试控制单元**

这是针对在启动/关机时运行的设备的自我诊断措施，以确保在应用运行过程中设备不会出现延时/休眠故障而破坏其运行。通常来说，自我检测根据数字逻辑(称为 LBIST)在嵌入式存储器( 称为 MBIST)上执行，有足够的覆盖率，可满足所要求的系统安全完整性等级(SIL)。

1. 在 STCU 重置事件后，SSCM 检测到设备自我检测尚未运行。

2. SSCM 从非易失性闪存存储器(NVM) 读取自我检测参数。

3. SSCM 将自我检测参数加载到 STCU 中，并将控制传送到 STCU。

4. STCU 管理 MBIST 并更新其内部状态。

5. STCU 管理 LBIST 并更新其内部状态(可能有其他LBIST和MBIST的顺序或并行执行)。

6. 如果检测到故障，STCU 便将测试故障报告给 FCCU 或重置设备。

7. 在完成自我测试后，STCU 便

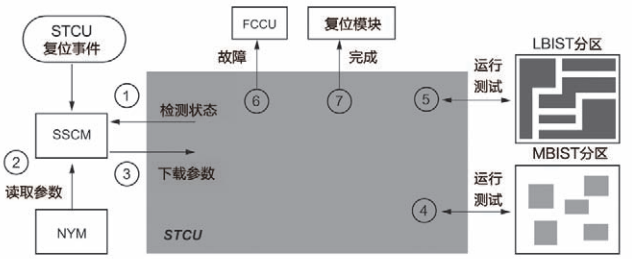


图3 系统启动过程中 STCU 的运行

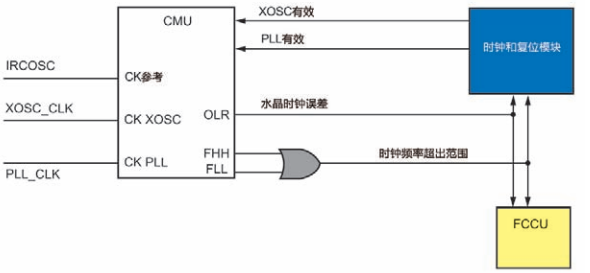


图4 CMU简易框图

示意重置模块，引导顺序推进到下一阶段。

**时钟监控和辅助时钟**

为了检测安全运行中内外部时钟电路故障，基于辅助时钟监控(见下文)其主时钟。该辅助时钟由内部 RC 振荡器提供，只要器件重置便可使用。有了辅助时钟，即使内部 PLL 由于某些原因而发生故障，也能保证系统有时钟可以运行许多安全机制，确保继续运行。该 IRC 振荡器可进行微调，使时钟在不同的 PVT(流程、电压和温度)下保持一致。

**时钟监控单元**

CMU 是监控系统 PLL 输出频率的模块，如果发生时钟丢失或被监控的时钟超出低频或高频边界时，便会显示故障、重置或中断。CMU将辅助时钟(见上文)作为参考来对时钟进行监控，同时根据外部晶体振荡器监控辅助时钟。 CMU 简易框图如图 4 所示。

如图4所示，如果发生振荡器时钟丢失事件或被监控时钟发生低频/高频事件，CMU 会向重置和FCCU模块提供信号。 只有当一段时间内FCCU未反应的情况下，才激活重置模块路径。因此，重置和FCCU的信号路径在MCU内组成了冗余故障指示路径，以确保FCCU的故障无法阻止所有的故障报告。FCCU 模块的配置决定事件是否会造成中断或重置。

## 电源管理控制器

Qorivva MCU 提供的 PMC 采用电压监控电路和 BIST。有两种电压监控器，即低压检测 (LVD) 和高压检测 (HVD) 监控器。所有与安全相关的电压都受到内部监控，防止电压超出这些范围。

PMC 中实施的 BIST 在启动时或通过软件检测 PMC 中关键的带隙电压/其他功能。

由于安全相关电压故障可能导致MCU故障指示机制(例如 FCCU和错误输出板)在反应前关闭，其电压错误指示将直接导致设备跳变到故障安全状态(执行重置)，而无需FCCU干预。

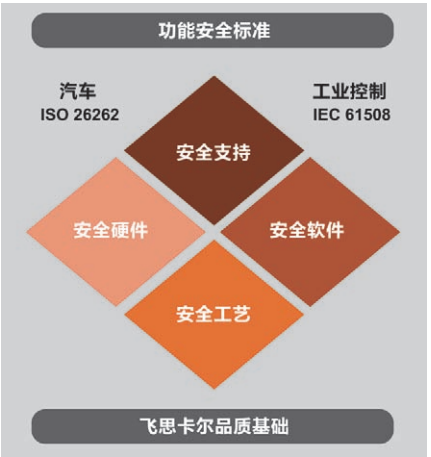


图5 飞思卡尔质量基础

## 飞思卡尔 SafeAssure 计划

飞思卡尔SafeAssure功能安全计划旨在帮助系统制造商更轻松符合国际标准组织(ISO)26262和国际电工委员会(IEC)61508功能安全标准。 该计划强调飞思卡尔解决方案(硬件和软件)，优化了设计，支持功能安全实施，同时集成了丰富的支持。飞思卡尔方案包含四个支持领域，可使客户大大减少产品上市周期。这四个领域如下所示。

1)安全硬件：上述各节所讨论的在硬件中部署的各种主要功能安全特性是 SafeAssure 计划的一大要素。

2)安全支持：该部分确保提供完整的文档支持，包括产品的安全应用说明、安全手册和 FMEA/FMEDA 分析。除了提供支持以外，飞思卡尔还为系统开发人员提供了一个选项，可与区域安全专家密切合作以加快其开发工作。

3)安全软件：对安全产品的软件支持包括驱动程序开发、移植操作系统和自检软件，确保器件在其整个生命周期内都正常运行。

4)安全流程：飞思卡尔内部随后的流程确保从要求管理到设计实施的安全遵从，以及在验证/确认/生产阶段的功能覆盖。通过保持全面的可追溯性矩阵来实现，并构成“SafeAssure”计划的第四个要素。

这四个方面对于系统开发人员保证顺利进行产品功能安全合规认证来说至关重要。

## 总结

设备实施功能安全特性需要 MCU 提供冗余，可能增加功耗和芯片尺寸。但是，如果与强大的硬件系统连接(MCU能够提供故障安全、故障静音或故障指示状态)，带来的好处非常多，尤其在减少软件复杂性方面。本文讨论了飞思卡尔 Qorivva MCU 所实施的各种安全设计。 在器件中实施这些安全特性是飞思卡尔 SafeAssure 计划的四大要素之一，使客户的应用能够符合 ASIL/SILx 。

EW

**参考文献：**

[1]Chalupa L.新一代汽车电机控制：趋势与解决方案
[2]Freescale.MPC574x 参考手册
[3]飞思卡尔SafeAssure计划[R/OL].www.freescale.com/safeassure