Technical White Paper

基于 Arm® 的微控制器和处理器功能安全支持

Neelima Muralidharan, Michael Firth, Kathryn Kalouf *Catalog Processors*

摘要

本白皮书介绍了功能安全概念，例如危害分析和风险评估、SIL 和 ASIL 等级、随机故障与系统性故障以及独立安全元素。该白皮书还举例说明了 AM243x MCU 和 AM64x 处理器系列如何通过集成安全 MCU 和使用安全诊断来支持功能安全。

内容

插图清单

表格清单

1 功能安全目标

功能安全目标是一个系统级目标，旨在降低潜在危险事件的风险。这里的关键词是*降低*。无论何时何地都会存在一定程度的风险，安全目标的目的是将伤害风险降低到可接受的水平。

根据终端应用、设备的使用方式以及操作人员与设备的交互方式来定义安全目标。例如，工厂车间有许多设备可能会伤害工人。衣服可能会被机器夹住，如果机器没有立即停止，工人会受伤。本例中的安全目标是在机器的预设距离内检测到人员时立即停止机器，从而防止对操作人员造成伤害。系统集成商实施和支持此安全目标的方式称为安全概念。用于停止电机或机器的常见安全概念称为安全转矩关闭 (STO)，在本例中，可以实施此安全概念来支持安全目标。（有关详细信息，请参阅表 8-1 中的 STO 概念与评估报告。）

2 危害分析和风险评估

定义安全目标的第一步是让系统集成商执行危害分析和风险评估 (HARA)。HARA 首先要确定系统中可能发生的所有潜在危害。然后，根据一组预定义的标准对这些危害进行分类，这些标准为每项危害指定一个安全完整性等级 (SIL) 或汽车安全完整性等级 (ASIL)。指定的 SIL 或 ASIL 等级定义了每种危害的最大可接受发生率。然后定义安全目标和安全概念，来减轻危害并将危害发生情况限制在目标 SIL 或 ASIL 等级。

图 2-1 以图形方式显示了 HARA 和安全概念阶段。

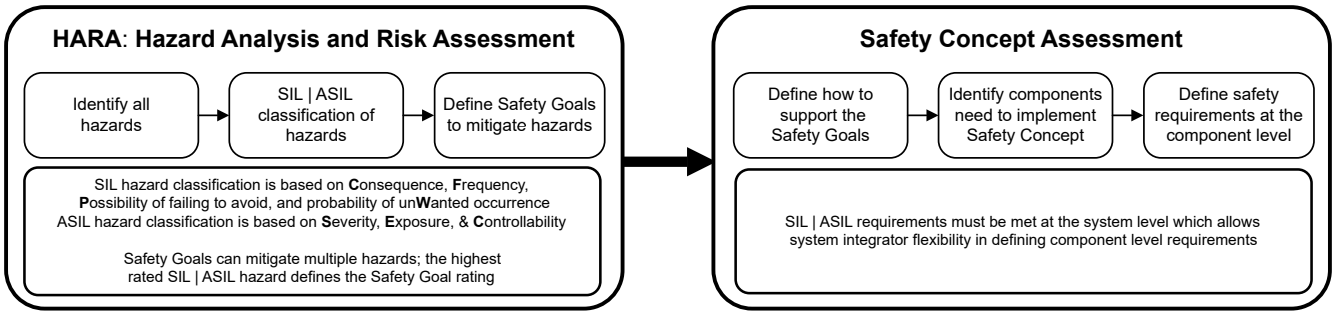

图 2-1. HARA 和安全概念评估阶段

3 SIL 和 ASIL 等级

在 HARA 分析过程中，识别的每个危害都会归为 SIL | ASIL 的四个等级之一。SIL | ASIL 等级越高，危害风险越大，因此安全要求也越高。IEC 61508 是一个适用于许多行业（包括工业应用）的功能安全标准，该标准定义了 SIL 等级。ISO 26262 标准定义了 ASIL 等级，该等级特定于汽车行业。国际电工委员会 (IEC) 61508 与 ISO 26262 标准的目标相似，但使用了不同的方法和安全度量指标。

在 IEC 61508 中，根据 **C** 后果（4 个等级）、**F** 频率和暴露时间（2 个等级）、**P** 未能避免特定危害的可能性（2 个等级）和 **W** 意外事件的可能性（3 个等级）这几个方面对每个危害进行了分类。基于此，使用图 3-1 中的以下风险矩阵将每种危害分类为 SIL 1 至 SIL 4（SIL 1 的伤害风险最低）。

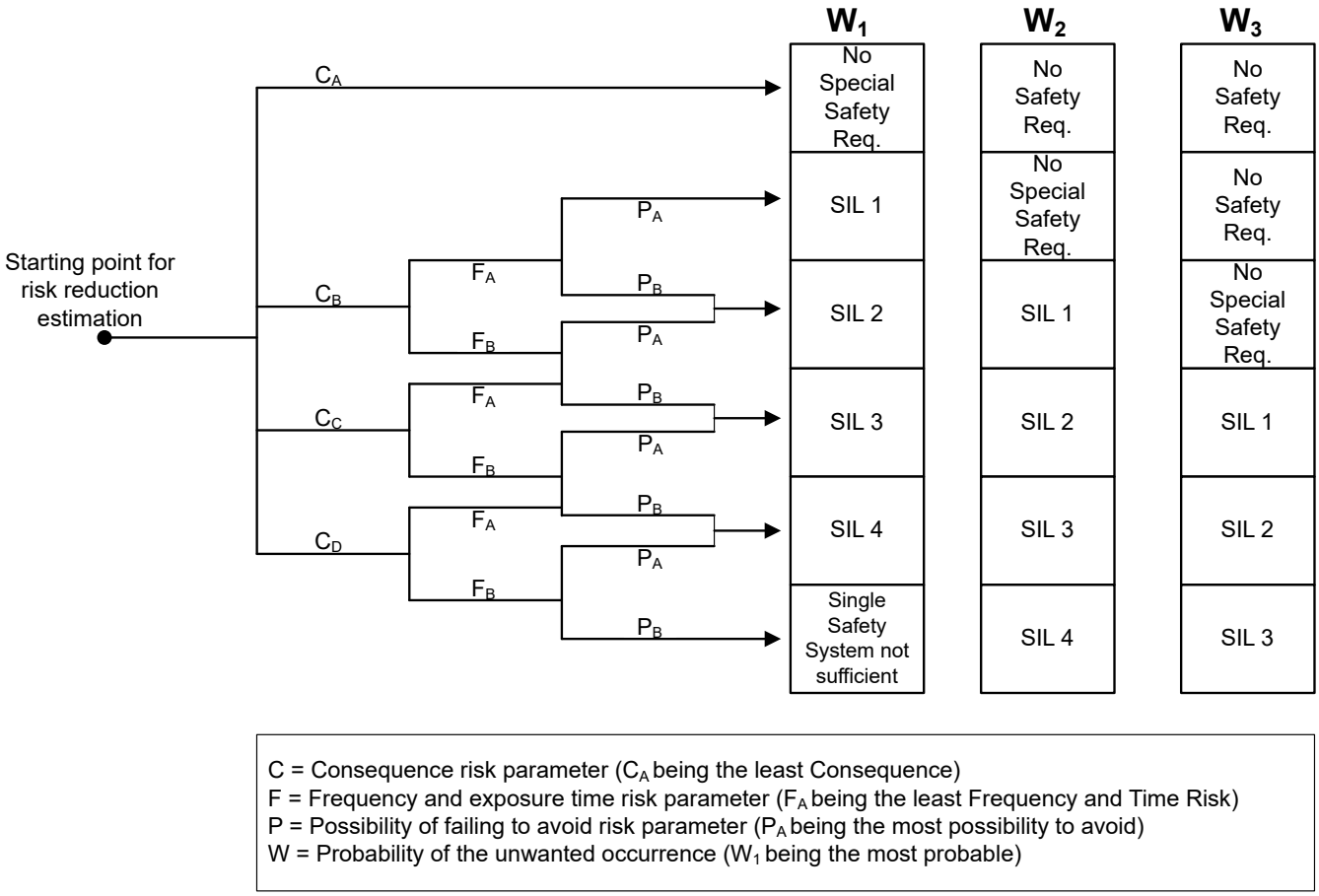

图 3-1. IEC 61508 风险图、危害分级矩阵

ISO 26262 标准使用 **S**、**E**、**C**（严重度、暴露度、可控性）对每种危害进行分类。伤害的**严重度**评估分为三个等级。**暴露度**于潜在危险情况下的概率评估分为四个等级。**可控性**（即可以避免危害的程度）评估分为三个等级。基于此，每个危害可在质量管理 (QM) 到 ASIL D 范围内进行分级，如图 3-2 所示。QM 等级表示该危害风险不需要专门的安全目标。对于集成电路 (IC)，标准半导体质量管理型设计和制造工艺足以满足 QM 等级。

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL-A
	E4	QM	ASIL-A	ASIL-B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL-A
	E3	QM	ASIL-A	ASIL-B
	E4	ASIL-A	ASIL-B	ASIL-C
S3	E1	QM	QM	ASIL-A
	E2	QM	ASIL-A	ASIL-B
	E3	ASIL-A	ASIL-B	ASIL-C
	E4	ASIL-B	ASIL-C	ASIL-D

S = Severity: How severe is the injury due to the hazard (S1 being the least severe)
E = Exposure: How likely is the hazard to occur (E1 being the least likely)
C = Controllability: How much can the driver do to prevent injury (C1 being the least controllable)

图 3-2. ISO 26262 危害分级矩阵

为危害指定 SIL | ASIL 等级后，定义安全目标，将危害降低到 SIL | ASIL 度量指标定义的可接受水平。IEC 61508 和 ISO 26262 都将**时基故障率**作为定义可接受风险级别的一个关键合规性度量指标。时基故障（FIT，**F**ailures **I**n **T**ime）定义为运行 10^9 小时（即运行 10 亿个小时）间隔内的时基故障数。

并非所有故障都具有相同的潜在危害，因此故障分为不同的类别，例如非安全相关故障、检测出的安全故障、未检测出的安全故障、检测出的危险故障和未检测出的危险故障。最关键的故障类别是未检测出的危险故障，原因显而易见。其他故障类别不会产生安全问题，或者可以通过硬件诊断和软件诊断来检测，从而得以减轻来消除任何潜在的损害。

表 3-1 和表 3-2 列出了 IEC 61508 SIL 和 ISO 26262 ASIL 度量指标。

表 3-1. IEC 61508 SIL 度量指标

	HFT = 0		HFT = 1	
SIL 等级（B 类系统）	**PFH**	**SFF**	**PFH**	**SFF**
SIL 1	⩽ 1000 FIT	⩾60%	⩽ 1000 FIT	< 60%
SIL 2	⩽ 100 FIT	⩾ 90%	⩽ 100 FIT	⩾ 60%
SIL 3	⩽ 10 FIT	⩾ 99%	⩽ 10 FIT	⩾ 90%
SIL 4	无法达到		⩽ 1 FIT	⩾ 99%

表 3-2. ISO 26262 ASIL 度量指标

ASIL 等级	PMHF	SPFM	LFM
ASIL A	⩽ 1000 FIT	未指定	未指定
ASIL B	⩽ 100 FIT	⩾ 90%	⩾ 60%
ASIL C	⩽ 100 FIT	⩾ 97%	⩾ 80%
ASIL D	⩽ 10 FIT	⩾ 99%	⩾ 90%

IEC 61508 标准使用 PFH (**P**robability of **F**ailure per **H**our)，即每小时失效概率，是每小时***未检测出的危险故障*** 总数。SFF 是安全失效分数 (**S**afe **F**ailure **F**raction)，表示未分类为未检测出的危险故障在所有故障类型中所占的百分比。

与 PFH 度量指标类似，ISO 26262 使用 PMHF（硬件随机失效度量指标，**P**robabilistic **M**etric for random **H**ardware **F**ailures）表示***未检测出的危险故障*** 总数。单点故障指标（SPFM，**S**ingle **P**oint **F**ault **M**etric）类似于 IEC 的 61508 SFF。IEC 61508 和 ISO 26262 之间的主要区别之一是，ISO 26262 标准添加了潜在故障度量指标（LFM，**L**atent **F**ault **M**etric）。LFM 是与诊断硬件相关的故障，且可视为一种隐藏的故障，因为在正常运行期间无法检测出 LFM，其仅在未检测出可检测的故障时才会出现。为了改进 LFM 度量指标，必须将硬件诊断设计为在现场部署之前对诊断进行广泛测试。

4 随机故障和系统性故障

可能会发生两种类型的故障：随机故障和系统性故障。随机故障的发生受许多因素的影响，包括工作温度、通电时间、工作电压和中子通量因子。因此，解决随机硬件故障的能力仅限于在运行时执行期间检测并尽可能防止故障并将系统置于安全状态。系统故障是由设计、开发或制造流程中存在的某种不足引起的，并且通常源于开发流程中的缺陷。因为可以在开发的设计验证阶段检测到器件错误，所以该错误是系统性故障。

理论上，通过严格控制并遵守开发和制造流程，可以将系统性故障减少到零。SIL | ASIL 系统等级不会像随机故障那样指定时基故障率，而是定义必须遵守的不同级别的程序和流程，从而防止出现系统性故障。为了满足 IEC 61508 和 ISO 26262 的系统能力要求，TI 开发了一个内部安全 IC 开发标准，此标准已经通过独立第三方评估商 TÜV SÜD 的认证。有关 TI 安全硬件和软件开发认证的信息，请参阅功能安全主页。

与系统性故障不同，随机故障不可能减少到零，但可以显著减少。通过使用系统级设计技术、安全诊断和采用稳健的低时基故障率器件工艺来设计 IC，可以减少未检出的危险随机硬件故障的数量，从而满足 SIL 和 ASIL 要求。

5 AM243x、AM64x：安全诊断和示例

TI 的 AM243x MCU 和 AM64x 处理器系列是专用于在各种工厂自动化应用（包括可编程逻辑控制器 (PLC)、电机控制、工业通信网关和机器人）中支持功能安全的器件示例。AM243x 和 AM64x 系列具有多种器件选项，旨在实现 SIL-2 随机故障能力（≤100 FIT 未检出的危险故障）和 SIL-3 系统功能。在系统级别，当与外部安全处理器结合使用时，AM243x 和 AM64x 可协助系统集成商实现高达 SIL-3 HFT = 1 的等级。硬件容错 (HFT) = 1 表示，即使在单点硬件故障的情况下，系统也可以保持安全概念和安全功能。

为了符合 SIL-2 随机故障度量指标，AM243x 和 AM64x 广泛使用安全诊断。器件级安全诊断分为 3 类，如图 5-1 所示。

Safety Diagnostics		
Hardware Diagnostics Diagnostics supported in hardware. Software may or may not be needed for initial configuration, but not required after configuration.	**Software Diagnostics** Diagnostics supported by software. Require CPU support and often need to meet critical timing requirements.	**Hardware + Software Diagnostics** Diagnostics require hardware and software support. Minimal CPU support requirements.

图 5-1. 安全诊断的类型

AM243x 和 AM64x 广泛使用的一个硬件诊断示例是单错校正双错检测（SECDED，**S**ingle-**E**rror **C**orrecting **D**ouble-**E**rror **D**etecting）错误校正，用于所有 AM243x 和 AM64x 片上存储器。顾名思义，这种诊断用于校正 1 位存储器错误，并检测 2 位甚至某些 3 位存储器错误。通过 AM64x、AM243x 错误信令模块 (ESM) 聚合所有硬件诊断故障，提供一个集中式故障管理和报告系统。ESM 模块按照严重度对错误进行分类，并且其对每个错误的响应可由系统集成商进行编程。错误响应选项包括将安全错误引脚 (图 6-3) 置为有效，向 CPU 生成高优先级和/或低优先级中断。

循环冗余校验（CRC，**C**yclic **R**eduction **C**heck）是软件诊断的一个示例。CRC 通常用于数字通信网络来检测数据传输错误。根据传输前的数据包计算 CRC 值，然后在接收端重新计算该值。如果计算结果不匹配，则数据在传输过程中损坏。系统集成商负责在软件中完成两次计算。

此外，AM243x 和 AM64x 具有硬件 + 软件诊断功能。内部看门狗计时器就是这种诊断类型的一个示例。看门狗计时器是在器件中实施的计数器，从初始值开始倒数到零。待监控的处理器运行一个程序，此程序定期复位看门狗计时器，从而防止计时器达到零。如果看门狗未复位并达到零，则假定处理器已锁定，需要复位并置于安全状态。

以上示例只是 TI 为确保器件符合 SIL 和 ASIL 标准而提供的众多诊断中的一小部分。有关 AM243x 和 AM64x 支持的硬件和软件诊断的完整列表，请参阅功能安全手册。请注意，系统集成商必须实施建议的软件诊断，如果未实施，则器件无法达到目标 SIL | ASIL 等级。

6 AM243x、AM64x 片上安全 MCU 和 FFI 支持

AM243x 和 AM64x 均配备具有专用存储器和外设的片上隔离式 Arm® Cortex®-M4F 处理器。当配置为安全 MCU 和安全通道时，此 MCU 可用于监控主处理域，从而满足系统的功能安全目标和目标 SIL 等级。与使用外部安全 MCU 相比，集成安全 MCU 可降低系统成本和减小布板空间。

当与第二个安全 MCU 结合使用时，AM243x、AM64x 有助于系统集成商支持最高等级为 SIL-3 HFT = 1 的系统。增加第二个安全 MCU 可以为系统增加一定程度的硬件容错能力。两个安全 MCU 执行相同的功能，相互交叉校验结果。如果其中一个安全通道发生故障，则交叉校验计算会不同，且另一个冗余安全通道会检测到该故障并使系统置于安全状态。

图 6-1 显示了一种通过两个外部安全 MCU 实现 SIL-3 HFT = 1 的传统方法。图 6-2 显示了相同的系统，但其中一个安全 MCU 集成到 AM243x、AM64x 电机控制器中。

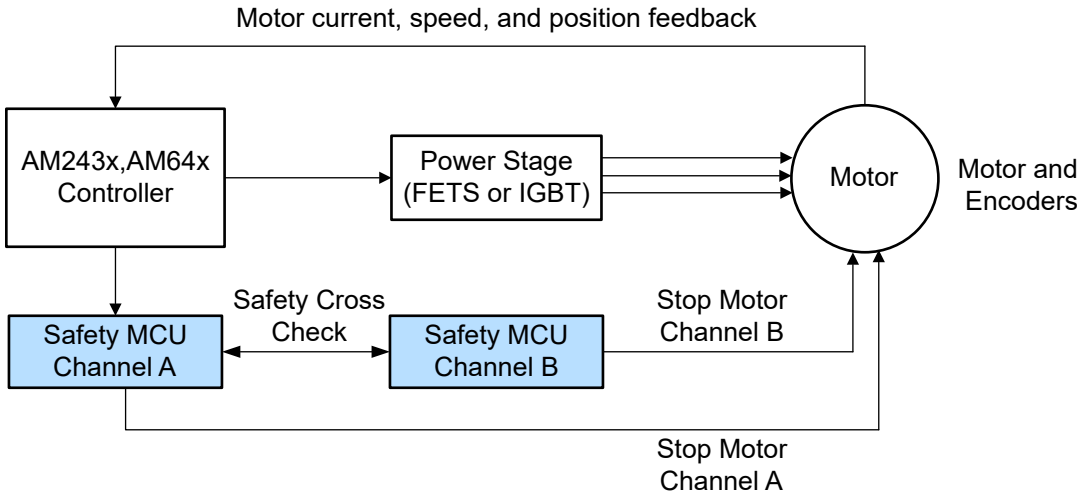

图 6-1. 带两个外部安全 MCU 的 SIL-3 HFT = 1 系统

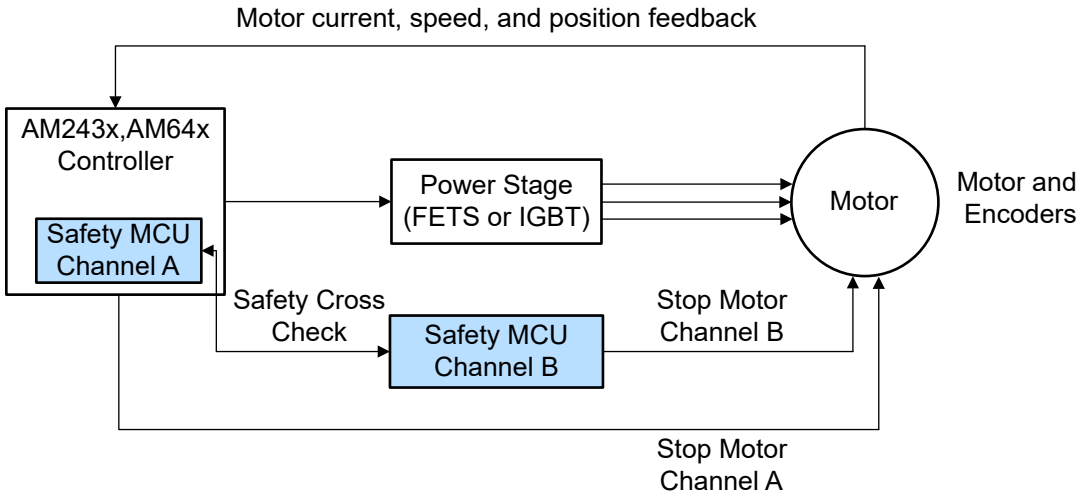

图 6-2. 带有集成和外部安全 MCU 的 SIL-3 HFT = 1 系统

借助外部安全 MCU，安全 MCU 会与待监控的处理器在物理上进行隔离。集成安全 MCU 需要使用几种无干扰（FFI，**F**reedom **F**rom **I**nterference）技术将安全 MCU 与主处理域隔离。FFI 是指系统中两个或多个元件之间没有可能存在级联故障和级联相关性；FFI 是一种隔离形式。

AM243x 和 AM64x 使用防火墙隔离片上安全 MCU，确保主域中发生的事件不会影响安全 MCU 的运行。除了防火墙之外，还使用超时垫来保护安全 MCU 和主域之间的通信通道。当安全 MCU 发起与主域的事务时，会设置计

时器。如果计时器在事务完成之前到期（由于主域中的问题），则取消总线事务，从而防止安全域挂起或锁定。如果安全 MCU 确定主域未正常运行，则 MCU 能够在保持运行状态的同时使主域复位。

图 6-3 显示了集成式 AM243x、AM64x 安全 MCU 以及关联的主域复位和安全错误标志。发生灾难性错误时，可以使用此错误标志向系统电源管理 IC (PMIC) 或其他器件发送信号，来启动 AM243x、AM64x 器件的完全断电复位。

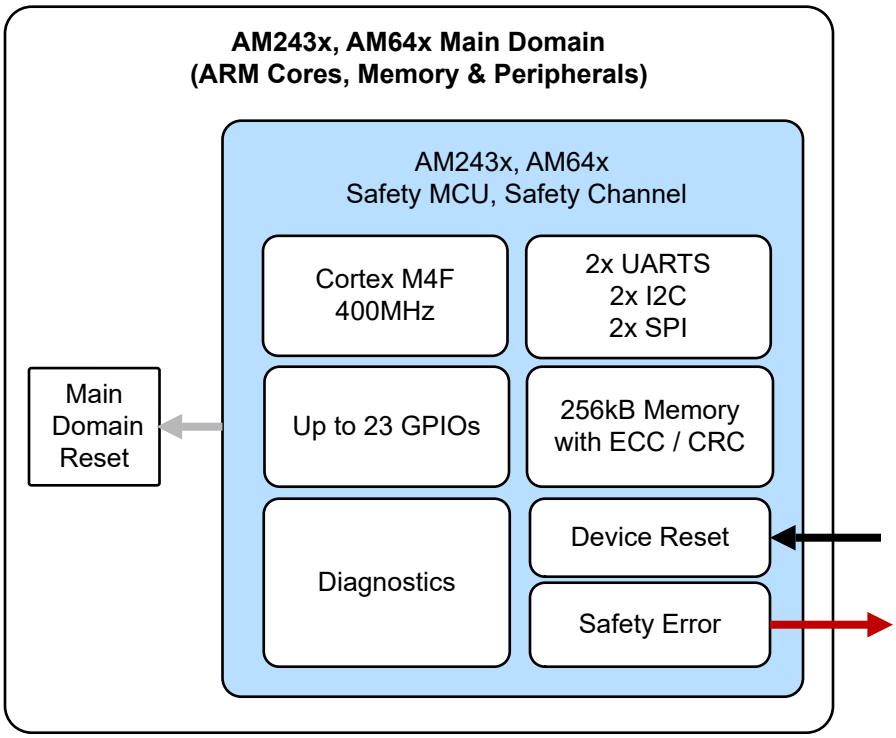

图 6-3. AM64x、AM243x 片上安全 MCU

7 独立安全元素

AM243x 和 AM64x 系列作为独立安全元素（SEooC，**S**afety **E**lements **o**ut **o**f **C**ontext）来开发。SEooC 是一种无需了解终端系统安全目标或系统运行方式就能支持功能安全的器件。开发一个 SEooC 器件可以高效利用资源和资金，因为这样可让单个器件支持许多不同的应用和安全目标。由于 AM243x 和 AM64x 旨在支持独立于终端应用的功能安全，因此必须作出多个系统级假设并在系统级提供支持，从而满足器件的额定 SIL 等级。例如，AM243x 和 AM64x 的一个系统级假设是，电源或其他外部监控器件可以监控 MCU，从而检测 MCU 是否无响应。带有片上看门狗计时器的 PMIC 是实现这种可用性监控的常用方法。

AM243x、AM64x 安全手册中提供了系统假设的完整列表。该安全手册提供了详尽的诊断建议列表。根据系统集成商的安全目标，并不需要实施所有软件和硬件诊断建议，而可以进行定制来满足最终目标并简化整个开发周期。

8 功能安全资源和示例

TI 提供大量文档和指导来协助客户实现功能安全目标。表 8-1 列出了 AM243x、AM64x 功能安全资源，并且这也是 TI 提供的功能安全配套资料类型的示例。

表 8-1. 配套资料中的功能安全设计

安全手册	功能安全手册详细列出了诊断功能、要求、建议和实施指南。还定义了 TI 和客户责任以及 SEooC 系统级设计假设和设计要求。
FMEDA	失效模式、影响和诊断分析 (FMEDA) 记录了 SIL	ASIL 计算假设，并让系统集成商可以基于许多变量（包括器件寿命、由于宇宙辐射造成的软误差、工作温度曲线、特定器件功能和引脚用途）对时基故障率和诊断覆盖进行建模，以及添加客户定义的诊断。
安全分析报告	安全分析报告定义了在 FMEDA 中作出的假设以及用于根据特定应用定制 FMEDA 的变量。
功能安全诊断库	安全诊断库 (SDL) 为配置和使用安全诊断功能提供了软件和 API 接口。该库提供了片上诊断的示例配置代码以及不同的故障检测选项。AM243x、AM64x SDL 代码已通过 TÜV SÜD 的 SIL-3 认证。
安全转矩关闭安全概念和评估报告	SIL-3，HFT = 1 安全转矩关闭安全概念和 TÜV SÜD 评估报告

使用以下链接申请访问上述信息。AM243x、AM64x 完成功能安全认证后，所有非 NDA 材料都将在 AM243x 和 AM64x 产品文件夹中提供。

- AM243x：MySecure 功能安全访问申请
- AM64x：MySecure 功能安全访问申请

有关 TI 的功能安全产品和相关功能安全资源的概括介绍，请参阅功能安全主页。

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