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

本白皮书介绍功能安全概念，例如危害分析和风险评估、随机故障和系统性故障、独立安全元素以及 IEC 61508 SIL 和 ISO 26262 ASIL 等级。提供了有关 AM243x MCU 和 AM64x 处理器系列如何通过使用片上安全 MCU 和安全诊断来帮助系统集成商实现功能安全目标的示例。

内容

插图清单

表格清单

1 功能安全目标和安全概念

功能安全目标是在设计过程开始时定义的系统级目标，重点是降低潜在危险事件的风险。伤害风险不能通过设计完全消除，但通过适当的设计技术，可以将危害风险降低到可接受的水平。根据最终应用、潜在危害的程度以及发生危险的可能性，功能安全目标会有所不同。以可接受的伤害风险水平实现安全目标的方法称为安全概念。

为了更好地了解功能安全目标和安全概念，剖析一家现代制造工厂可能会有所帮助。在制造车间，自动化和非自动化流程和机械与许多操作、监控和维修保养设备的人员共存。制造设备各不相同，从快速移动的机械臂到简单的测试和测量站，在适当的条件下全都可能对个人造成潜在危害。

为了降低制造车间中的危害风险，我们在设计过程的早期就为制造设备和工厂工艺制定了安全目标。为了应对人被机械臂击中的潜在危险，我们定义了一个安全目标，以将这种危险的发生率降低到每运行 10 亿个小时少于 1 次。然后定义安全概念来支持这一安全目标；安全目标使用基于激光的光幕在机械臂周围创建禁止区域，这是一种基于机器学习 (ML) 的视觉系统，用于跟踪操作员相对于禁止区域的位置，以及在检测到操作员进入禁止区域时停止机械臂的失效防护方法。安全转矩关闭 (STO) 和安全制动控制 (SBC) 安全功能用于实现机械臂的紧急停止。

STO 会切断电机的电源，而 SBC 会向电机施加外部制动。STO 和 SBC（以及其他特定于电机的安全功能）通常在电机控制应用中用于支持安全概念。下一节（节 2）详细介绍了系统集成商用于定义安全目标和安全概念的过程。

2 HARA 和安全概念评估阶段

危害分析和风险评估 (HARA)是定义系统级安全目标的一个广为接受的过程。HARA 流程的第一步是识别系统中的所有潜在危险，然后根据危害风险对每种危险进行分类。用于对危险进行分类的条件因所使用的标准而异，但通常包括诸如以下因素：危险程度（严重性）、发生的可能性（暴露）和危险的可控程度（可控性）。本白皮书重点介绍安全完整性等级 (SIL) 和汽车安全完整性等级 (ASIL) 危险分类技术和级别。

在确定系统级危险并指定 SIL 或 ASIL 等级后，可以定义安全目标来降低危险。为了在终端系统中实现安全目标，需要安全概念，这些概念在安全概念评估阶段定义。在这个阶段中，会确定支持安全概念所需的各个组件，并为其分配适当的 SIL 或 ASIL 等级。例如，在这个阶段中，系统集成商会确定 MCU 或处理器对于实现安全概念是否至关重要，如果是，则分配适当的 SIL 或 ASIL 等级。可以使用符合安全标准的分解技术来降低基于系统架构的某些组件的安全完整性等级，而不会降低最终的系统安全完整性等级。

图 2-1 以图形方式显示了 HARA 和安全概念阶段。

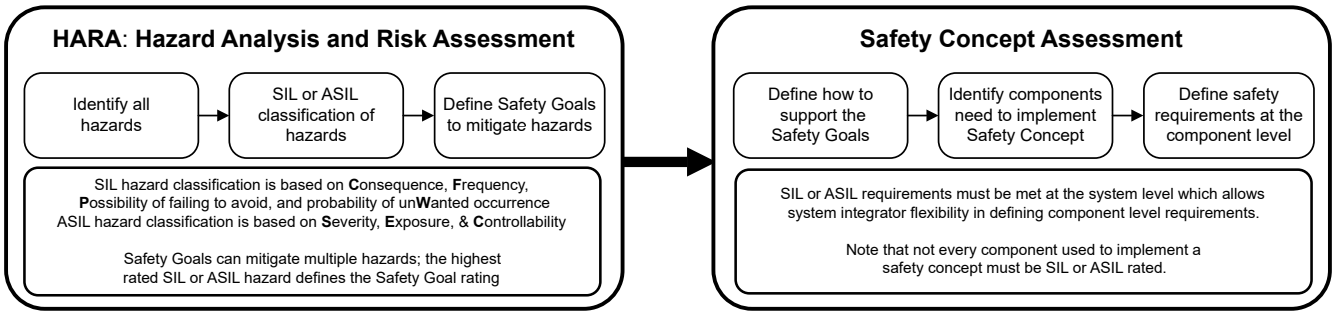

图 2-1. HARA 和安全概念评估阶段

3 SIL 和 ASIL 分级

对于很多工业应用，SIL 等级用于对危险进行分级并定义安全概念元件的可接受故障率。国际电工委员会 (IEC) 61508 功能安全标准中定义了分配 SIL 等级的条件。IEC 61508 广泛应用于许多行业，涵盖了包含电气、电子或可编程电子器件（或这三种功能的任意组合）的安全相关系统。

在 IEC 61508 中，根据后果、频率和暴露时间、未能避免特定危害的可能性和意外事件的可能性这几个方面对每个危害进行了分类。

图 3-1 展示了用于将每种危害分类为 SIL 1 至 SIL 4（SIL 1 的伤害风险最低）的矩阵。

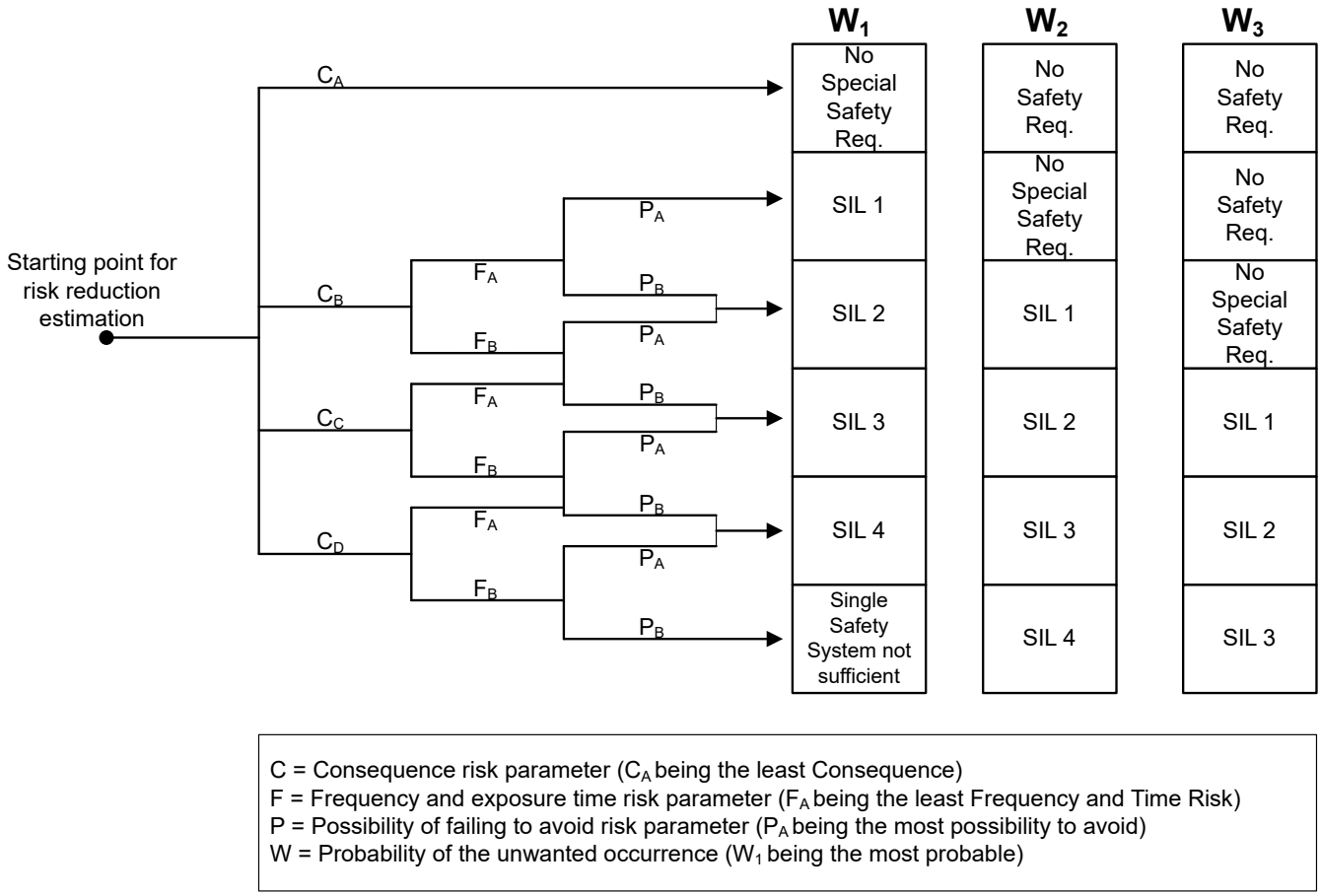

图 3-1. IEC 61508 风险图、危害分级矩阵

对于汽车应用，使用 ASIL 等级对危险进行分级和定义安全概念元件的可接受故障率。国际标准化组织 (ISO) 26262 标准中定义了分配 ASIL 等级的条件。IEC 61508 与 ISO 26262 的目标相似，但使用了不同的方法和安全度量指标

ISO 26262 使用 **S** 严重性或危害、**E** 暴露的可能性以及 **C** 可控性（可以避免危害的程度）对每个危害进行分级。通过使用图 3-2 所示的矩阵，每个危害被归类为质量管理 (QM) 或从 ASIL A 到 ASIL D 的 4 个等级之一。QM 等级表示识别的危害不需要专门的安全目标来降低风险，而 ASIL D 等级表示最高的潜在危害风险。

备注

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

时基故障率是用于定义 IEC 61508 和 ISO 26262 中可接受风险等级的关键合规性指标。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。原因很明显，最关键的类别是未检测出的危险故障。其他故障类别不会产生严重的安全问题，或者可以通过诊断来检测，从而得以减轻来消除任何潜在的危害。元件级别的时基故障率定义随着时间的推移可能发生的最大未检测出的危险故障数。

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 标准使用每小时失效概率 (PFH, **P**robability of **F**ailure per **H**our) 来表示每小时***未检测出的危险故障***总数。安全失效分数 (SFF, **S**afe **F**ailure **F**raction) 表示不属于未检测出的危险故障的故障所占的百分比。

与 PFH 度量指标类似，ISO 26262 使用硬件随机失效度量指标 (PMHF, **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 SFF。

ISO 26262 添加了一种用于 IEC 61508 中没有的诊断硬件的附加故障度量，称为潜在故障度量指标 (LFM, **L**atent **F**ault **M**etric)。诊断硬件故障被视为潜在故障，因为在正常运行期间无法检测到故障，只有在未检测到可检测到的故障时才会发现故障。为了减少 LFM 故障的数量，诊断硬件的设计必须具有较高的测试覆盖率，并在现场部署之前进行广泛的测试。

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。系统性故障是由设计、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 或 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。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 TI 的功能安全主页。

与系统性故障不同，随机故障不可能减少到零，因此必须通过使用不同的技术将其控制在可接受的水平。对于 IC，通过使用系统级设计技术，采用低时基故障率器件工艺制造并实施硬件和软件安全诊断，可以将随机硬件故障的数量降至可接受的 SIL 或 ASIL 等级。节 5 介绍了安全诊断的含义，并提供了 AM243x 和 AM64x 器件中的使用示例。

5 AM243x 和 AM64x：安全诊断和示例

TI 的 AM243x 微控制器和 AM64x 处理器是专用于在各种应用（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 的未检测出的危险故障）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。

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. 安全诊断类别

单错校正双错检测 (SECDED, **S**ingle-**E**rror **C**orrecting **D**ouble-**E**rror **D**etecting) 是一种用于检测内存错误的常见硬件诊断。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。AM243x 和 AM64x 在所有片上存储器上都有 SECDED。

循环冗余校验 (CRC, **C**yclic **R**eduction **C**heck) 是一种用于检测数据传输错误的软件诊断。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和实现软件。

内部看门狗计时器就是硬件 + 软件诊断的一个示例。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。如果看门狗达到零，则假定处理器已锁定并置于安全状态，或者需要复位*并*置于安全状态。

所有安全故障都路由到 AM64x 和 AM243x 错误信令模块 (ESM)，并提供一个集中式故障管理和报告系统。ESM 模块根据严重性对错误进行分类，并允许系统集成商对每个错误的响应进行编程。响应选项包括将安全错误引脚（图 6-3）置为有效并生成高优先级或低优先级中断，或者将安全错误引脚置为有效并生成中断。

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。

6 AM243x 和 AM64x：具有 FFI 支持的安全 MCU

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 时，可以使用 M4F 来监控主处理域，以支持 SIL 等级。

当与第二个安全 MCU 结合使用时，AM243x 和 AM64x 有助于支持最高等级为 SIL-3 HFT = 1 的系统。增加第二个安全 MCU 可以为系统增加硬件容错能力。两个安全 MCU 相互执行交叉校验计算。如果结果不匹配，可以使用其中一个处理器将系统置于安全状态。

与使用两个外部安全 MCU 相比，集成安全 MCU 可降低系统成本和减小布板空间。图 6-1 展示了带两个外部安全 MCU 的 SIL-3 HFT = 1 系统。图 6-2 展示了相同的系统，但其中一个安全 MCU 集成到 AM243x 或 AM64x 控制器中。

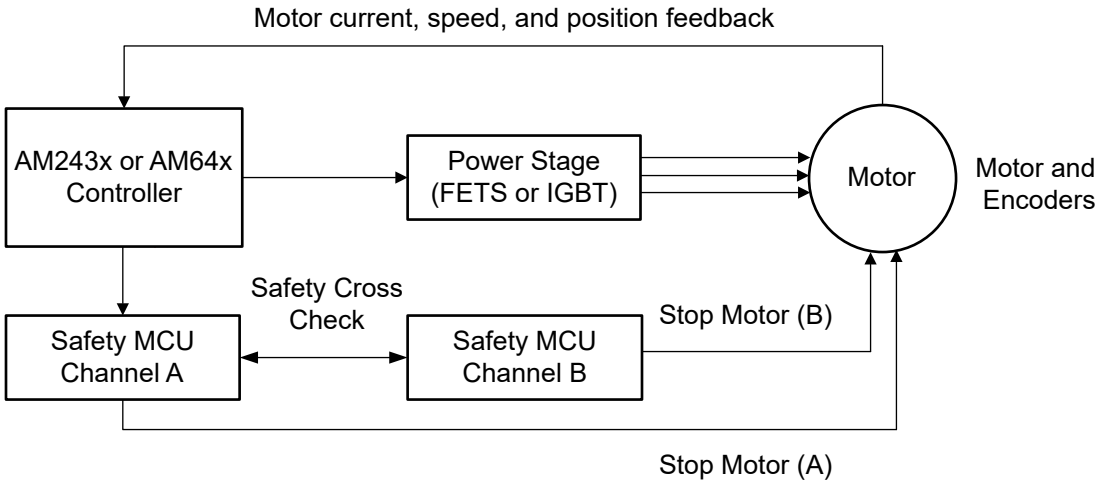

图 6-1. 带两个外部安全 MCU 的 SIL-3 HFT = 1 系统

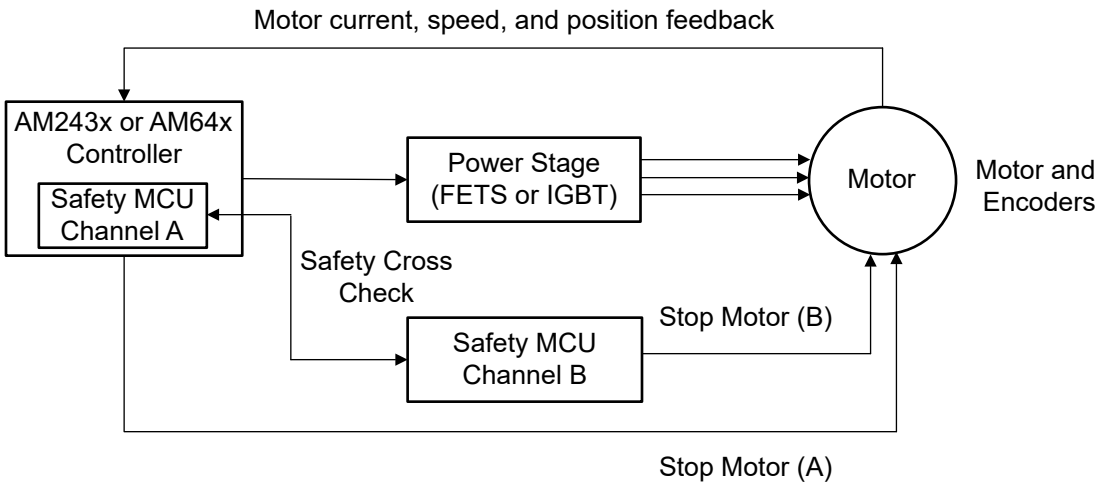

图 6-2. 带集成和外部安全 MCU 的 SIL-3 HFT = 1 系统

集成安全 MCU 需要使用无干扰 (FFI, **F**reedom **F**rom **I**nterference) 技术将安全 MCU 域与主处理域隔离。FFI 定义为系统中两个或多个元件之间不存在级联故障和相关性；FFI 是一种隔离形式。

防火墙和超时垫用于隔离 AM243x 和 AM64x 安全域，确保主域中发生的事件不会影响安全域。超时垫可在域间通信期间保护安全域不受主域故障的影响。当安全域发起与主域的事务时，会设置看门狗计时器。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，从而防止安全域锁定。在主域无响应的情况下，安全域能够在保持活动状态的同时复位主域。

除了防火墙和安全垫之外，安全域中的其他安全特性包括时钟丢失检测电路、用于检测不正确时钟频率的双时钟比较器、总线事务奇偶校验、专用 I/O 电源轨和内置自检 (BIST) 支持。

图 6-3 展示了 AM243x 和 AM64x 安全域、主域复位、安全错误标志和器件复位引脚。发生灾难性错误时，此错误标志会向系统电源管理 IC (PMIC) 或其他器件发送信号，来启动 AM243x|AM64x 的复位。

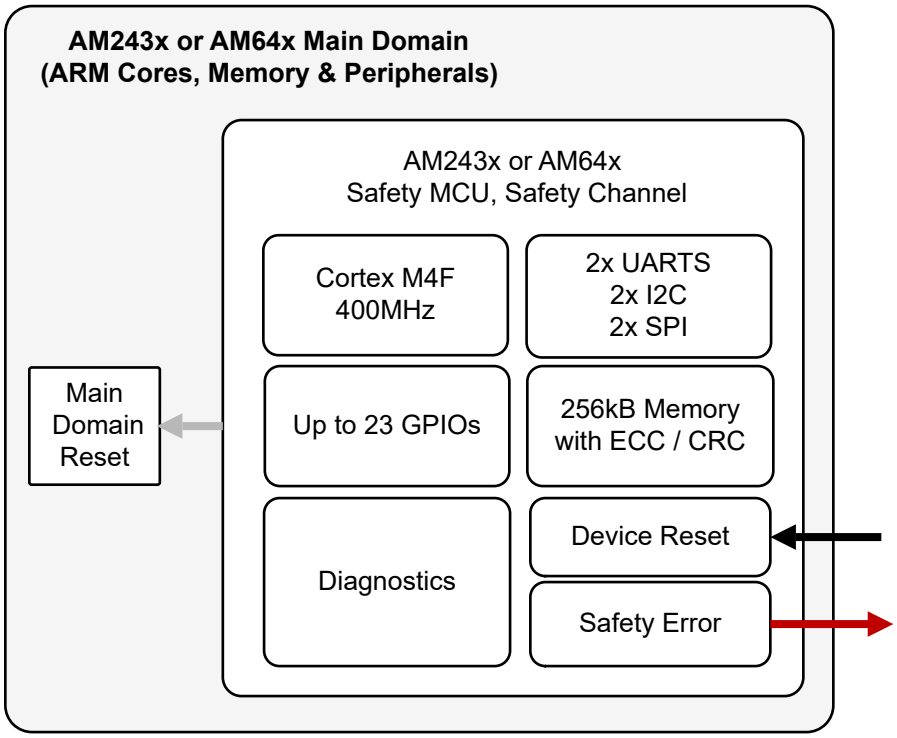

图 6-3. AM64x 和 AM243x 片上安全 MCU

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 是一种无需事先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。

要设计 IC 以支持独立于终端应用的功能安全，必须作出多个系统级假设并在系统级提供支持，以满足器件的额定 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处理器，从而检测处理器是否无响应。带有片上看门狗计时器的 PMIC 是满足此要求的常用方法。

AM243x 和 AM64x 安全手册中提供了系统假设的完整列表。安全手册提供了大量诊断建议列表和支持的诊断类型的详细信息。根据系统集成商的安全目标，系统集成商可以选择可用硬件和软件诊断的子集来支持功能安全目标；也就是说，并非所有可用安全诊断都必须在给定系统中使用。

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。作为示例，表 8-1 列出了 AM243x 和 AM64x 功能安全资源。

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器件诊断功能、建议和实施指南。还定义了 TI 和最终客户责任以及 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 SIL 或 ASIL 计算假设。支持基于器件寿命、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以及客户定义的诊断对时基故障率和诊断覆盖范围进行建模。
安全分析报告	安全分析报告定义了在 FMEDA 中作出的假设，还定义了有助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 TI 的功能安全主页。

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