

Application Note

针对 MSPM0 MCU 的系统级 ASIL B 合规性



Lars Lotzenburger

摘要

本应用手册介绍了针对 TI MSPM0 微控制器系列 ASIL B 版本器件的内核电压监控实现方案。根据 ISO 26262 的要求，所述设计支持在汽车应用中实现 ASIL B 功能安全完整性。

此设计适合许多汽车应用，这些应用需要为大型系统提供辅助控制或数据聚合，并且需要 ASIL B 车身电子装置和照明系统。所提议的方法专为功能安全工程师而设计，可提供可靠的电压异常检测、稳健的故障处理机制以及可量化的诊断覆盖率指标。借助随附的实现指南，工程师能够在满足汽车安全标准的同时，将内核电压监测高效集成到基于 MSPM0 的设计中。

内容

1 简介.....	2
2 详细说明.....	3
2.1 项目定义.....	3
2.2 假设.....	3
2.3 危害分析和风险评估 (HARA).....	3
2.4 功能安全概念.....	3
2.5 技术安全概念.....	4
2.6 技术安全要求.....	11
3 总结.....	14
4 参考资料.....	15

商标

Arm® and Cortex® are registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere.

所有商标均为其各自所有者的财产。

1 简介

MSPM0 微控制器集成了一个 LDO，用于生成内核电压。然而，由于缺少对 LDO 输出电压进行内部监测，因此需要外部监测机制来支持汽车应用中的功能安全合规性 (ASIL B)。本文档介绍了一种经济高效的外部监测实现方法，首先从子系统的安全目标定义开始。该方法介绍了功能安全概念的开发和架构设计，以满足功能和技术安全要求。详细的实现指南阐述了用于电压监测、故障检测和系统响应策略的具体安全机制。本文档最后介绍了失效模式和影响分析 (FMEA) 以及失效模式、影响和诊断分析 (FMEDA)，并提供了定量安全指标，以证明是否符合目标 ASIL B 要求。

2 详细说明

2.1 项目定义

该项目包含一个完整的 ASIL B 安全相关系统，由三个主要功能要素组成：传感器子系统、处理子系统和驱动子系统。这种架构代表了一种通用安全功能实现方案，适用于需要达到 ASIL B 完整性等级的各种汽车应用。特定系统的 ASIL B 合规性取决于整个系统的设计。

2.2 假设

已作出以下假设：

- 提供了一路标称电压为 3.3V 的电源导轨 V_{IN} ，并且
 - 未对该电源导轨进行欠压 (UV) 与过压 (OV) 故障保护，
 - 还用于直接与 MCU 对接的传感器和执行器电路。
- 连接到电源导轨的所有电路，其推荐最大供电电压均不低于 3.6V
- V_{IN} 不超过 42V

2.3 危害分析和风险评估 (HARA)

本文档不涉及危害分析和风险评估。以下安全目标要求假定为 HARA 的结果。

2.3.1 安全目标定义

安全目标 ID	安全目标	ASIL	安全状态	FTTI
SG_01	避免执行错误的 MCU 计划	B	微控制器电源周期	10ms

ASIL B 应用必须满足以下 ISO 26262 要求：

- SPFM $\geq 90\%$
- LFM $\geq 60\%$
- PMHF ≤ 100 FIT。

已为该安全机制分配 10ms 的 FTTI。如果系统级时序要求需要较低的值，则可以减小该值；但是，窗口看门狗刷新周期决定了 FTTI 的实际最小值。

2.3.2 安全状态“微控制器电源循环”

将微控制器电源循环作为故障反应执行，会在更大系统中引起级联安全状态转换，例如与监控系统层的通信暂时中断。初始故障排除后，MCU 能够自行恢复，上层实例可独立检测并确认该恢复，然后再恢复正常运行。

2.4 功能安全概念

过压事件可由电磁干扰 (EMI)、负载突卸或感性开关的瞬态响应不足、地电位偏移或线路故障引发。

当电压超出工作限值时，后果从暂时性故障到永久性损坏不等。MCU I/O 引脚有可能超出绝对最大额定值，造成器件不可逆损坏。如果输入输出压差过大，嵌入式 LDO 可能承受热应力或稳压失效，从而导致 V_{CORE} 不受稳压以及工作不稳定。在内核级别，过压可引发门锁效应、Flash/EEPROM 数据损坏、存储器过早损耗，甚至导致芯片彻底失效。未检测到的过压会导致系统行为失控，从而带来功能和安全隐患。

2.4.1 系统架构

该 MCU 用作系统的中央处理单元。所有传感器和执行器电路均直接连接到 MCU。车辆电池为系统供电。DC/DC 转换器将电池电压降至 3.3V 稳压电源导轨 (V_{IN})。这个统一电源为 MCU 供电，并为所有连接的传感器和执行器提供逻辑电源。

使用一个统一的电源导轨意味着所有元件始终在相同的电压电平下运行。在相同电压电平下运行可消除元件之间的逻辑电平不匹配，并防止系统中已通电和未通电元件之间出现漏电流。

图 2-1 展示了本文档范围内的应用子系统，用虚线表示。

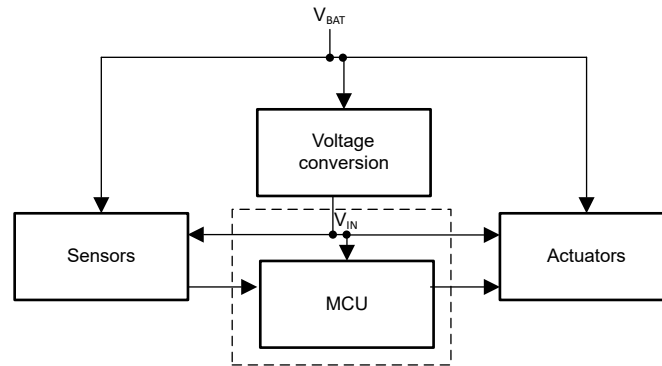


图 2-1. 系统架构设计

2.4.2 安全架构

为了满足安全目标 SG_01，MCU 必须在条件良好的环境中运行，以降低潜在危险。该系统必须防范高达 V_{BAT} 的危险电压条件，从而防止硬件损坏或错误运行，同时还必须保持经过良好调节的 V_{DD} 以实现可靠的 MCU 运行。此外，应提供正确驱动和受监测复位信号，以实现正确的 MCU 初始化和恢复行为。此外，应使用窗口看门狗机制来检测错误程序执行，其可能由各种底层故障导致。

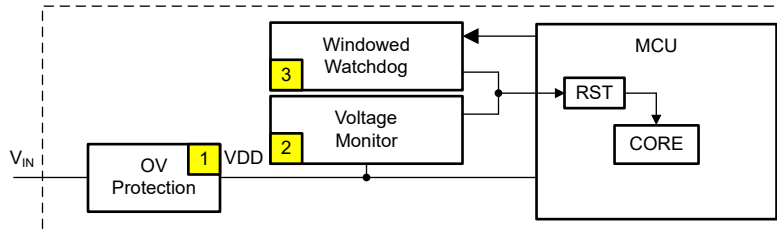


图 2-2. 安全架构设计

2.5 技术安全概念

本文介绍的方案仅是多种可行方案之一。在用于满足 ASIL B 要求的 MSPM0 外部 VCore 监测应用手册中探讨了采用并联基准、电阻梯和比较器的分立式替代方案。

2.5.1 器件描述

该设计的关键元件是使用 MSPM0G3107-Q1 实现的 MCU。以下各节将介绍该器件以及实现 ASIL B 合规性所需的所有支持元件。

2.5.1.1 MSPM0G3107-Q1

MSPM0G3107-Q1 是 TI MSPM0G 系列中符合 AEC-Q100 1 级标准的汽车级微控制器，专为汽车功能安全应用而设计。该器件已通过高达 ASIL B 等级的 ISO 26262 系统和硬件合规性认证。该器件将运行频率高达 80MHz 的 32 位 Arm® Cortex®-M0+ 内核与受 ECC 保护的闪存和受奇偶校验保护的 SRAM 相结合，以确保存储器完整性。连接功能包括一个集成式 CAN-FD 控制器和四个具有硬件流控制功能的 UART。两个采样速率为 4MSPS 且支持同步采样的 12 位 ADC 和一个采样速率为 1MSPS 的 12 位 DAC 可提供高精度模拟功能。具有故障处理、死区插入和 QEI/霍尔传感器支持的高级计时器可实现稳健的电机和照明驱动控制。硬件 AES-128/256、TRNG 和 CRC 引擎以及两个看门狗增强了安全关键完整性。该器件采用具有 5V 容限开路 I/O 的 64 引脚 LQFP 封装。

可在[功能安全](#)网页上查看所有符合 ISO26262 标准的 MSPM0 产品列表。

2.5.1.2 TPS388R0x-Q1

TPS388R0x-Q1 器件系列包括 2 通道、4 通道和 6 通道窗口监控器 IC，采用 16 引脚 3 × 3mm WQFN 封装设计，专为在低电压电源导轨上运行且电源容差裕度非常小的系统而设计。每个通道均可配置为 OV、UV 或窗口配置中的两者，故障输出可选择性地映射到 NRST/NIRQ 引脚。该器件通过 AEC-Q100 认证，并具有高达 ASIL B（硬件）和 ASIL D（系统性）的功能安全合规性，且启动时内置自检。该器件可提供 ±6mV 的阈值精度，检测输

入电压范围为 0.2V 至 5.5V，且无需外部电阻。所有参数均可通过 I2C 进行配置或在工厂进行编程。其他特性包括内部干扰滤波、CRC 和数据包错误检查 (PEC) 以及序列日志记录。

另一个版本 TPS388C0x-Q1 系列包括窗口看门狗。

2.5.1.3 TPS3842C011-Q1

TPS3842C011-Q1 是一款汽车级电压监控器，属于 TPS3842-Q1 系列，已通过 AEC-Q100 认证，适用于严苛汽车环境。该器件可监测电源导轨上的过压 (OV) 情况，并在 SENSE 引脚电压超过定义的阈值时置位 RESET 信号。该器件支持 1.9V 至 42V 的宽输入电压范围，从而可以直接连接到 12V 汽车电池。该器件具有 850nA 的超低静态电流和高阈值精度，可支持安全关键应用。该器件经评定具备功能安全能力，这意味着它提供基本 FIT 率、故障模式和分布。

2.5.1.4 TPS22919-Q1

TPS22919-Q1 是一款高性能负载开关，专为需要低损耗配电的汽车应用而设计。该器件由 5.5V 电源供电，可处理高达 1.5A 的持续电流，导通电阻为 100mΩ。这些规格可最大限度降低开关上的功率耗散和压降。该器件采用稳健运行封装，并内置限流和热关断保护，可在故障条件下安全运行。

2.5.2 实现详情

该应用基于 MSPM0G3107-Q1 微控制器而构建。根据 ISO 26262，该器件支持高达 ASIL B 的系统和随机硬件安全能力。

此类 MCU 的一个常见特性是集成低压降稳压器 (LDO)，它生成内核电压 (V_{CORE}) 电源导轨。由于该电压通常不在内部监测，因此必须在系统级实施外部措施。如果在 V_{CORE} 电源导轨上检测到 UV 或 OV 故障，则需要对 MCU 进行完整电源循环，因为复位逻辑取决于该电源导轨。

还必须持续监测 V_{DD} 是否存在 UV 和 OV 情形。MCU 集成了欠压锁定 (UVLO) 功能，可通过触发内部复位来应对 UV 故障。为了防止 MCU 和连接元件上的 V_{DD} 超过 4.1V (MCU 绝对最大值)，可以使用两种方法：电压钳位 (需要大型无源组件来耗散功率) 或断开电源。该设计采用断电方法。

MSPM0G3107-Q1 集成了两个内部看门狗计时器：一个窗口看门狗和一个独立看门狗，可用于程序流监测。独立看门狗由备用时钟源驱动，能够充分独立于主系统时钟。

图 2-3 显示了考虑这些因素的实现框图。

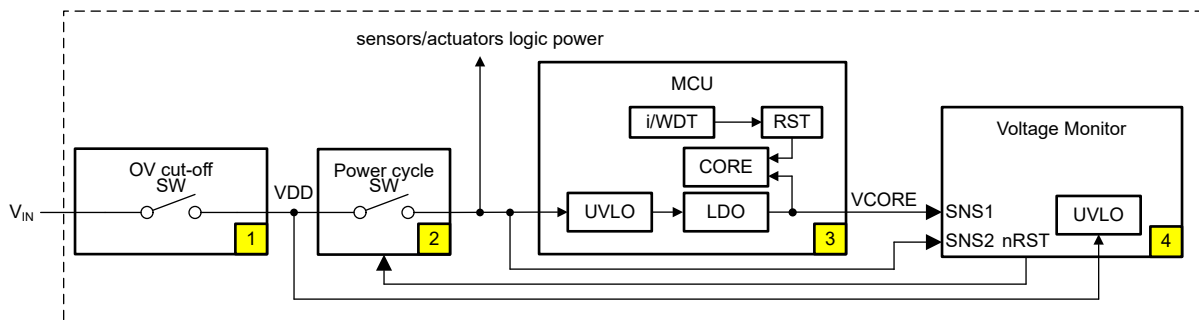


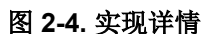
图 2-3. 实现方框图

下表说明了架构设计要素。

组件 ID	组件名称	说明
1	OVP 切断	带切断功能的过压监测，用于断开电源
2	电源周期切断	通过对 MCU 执行电源周期复位，响应 V_{CORE} 欠压/过压故障
3	MCU	运行程序代码的微控制器
4	电压监控器	监测 MCU 内核电压

表 2-1 显示了应用子系统的设计参数。

设计参数	参数值
电压输入范围 (V _{IN})	3.3V ± 约 3%
输入电流	10mA + 传感器或执行器电路
过压保护电路	
过压保护电压阈值	3.9V ± 约 5%
故障输入电压 (最大值)	42V
故障响应时间 (最大值)	7 μs
复位延时时间 (标称值)	250 μs
MCU 电压监控 (V _{DD} 和 V _{CORE})	
故障响应时间 (V _{CORE} 和 V _{DD}) , 最大值	750ns
V _{CORE} 过压阈值	1.40V ± 7.5mV
V _{CORE} 欠压阈值	1.29V ± 7.5mV
V _{DD} 过压阈值	3.50V ± 0.5%
V _{DD} 欠压阈值	2.65V ± 0.5%
微处理器	
集成式 LDO 输出电压范围 (最大值)	1.30V 至 1.39V
VCORE 工作范围 (最大值)	1.27V 至 1.42V



如果不需要过压保护，可移除 **OVP** 级，因为该级与电路其余部分相互独立。虽然 **TPS388R02-Q1** 可以检测并响应高达 **5.5V** 的过压情况，但任何超过此电平的电压都可能损坏负载开关、电压监控器和 MCU。

2.5.2.3 应用加电和断电

加电时，TPS388R02-Q1 开始在 1.65V 电压下工作并置位 *NRST*，从而使 MCU 保持未通电状态。TPS388R02-Q1 在 2.81V 时达到完全运行，然后执行内部内置自检 (BIST)。在此过程中检测到的任何内部故障都会使 *NRST* 保持置位，从而使应用保持在安全状态。成功完成 BIST 后，*NRST* 将置为无效。由于 *NRST* 和 *ACT* 相连，此事件会同时激活 TPS388R02-Q1 并使能 TPS22919-Q1 负载开关，然后为 MSPM0G3107-Q1 供电。

断电时，MCU 可以在低至 1.62V 的电压下运行；但当低于 2.6V 时，TPS388R02-Q1 将不再监测 V_{CORE} 并相应置位 *NRST*，从而将 MCU 置于安全状态。如果相邻电路要求 V_{DD} 保持在 2.6V 以上，请使用 TPS388R02-Q1 的第二个监测通道 (*MON2*) 将 *NRST* 置为更高电压阈值。

2.5.2.4 TPS388R02-Q1 无软件操作

TPS388R02-Q1 经过预编程，可简化系统集成并且无需启动软件配置。即使是低订购量，也可直接从德州仪器 (TI) 申请预编程器件。I2C 通信保持可用，并可与预编程配置一起使用以进一步提高灵活性。

2.5.2.5 V_{CORE} 和 V_{DD} 监控

根据 [MSPM0G3x0x-Q1 功能安全手册](#)，必须通过 *VCORE* 引脚在外部监测 V_{CORE} 。MSPM0G3107-Q1 *VCORE* 引脚在 RUN、SLEEP 和 RESET 模式下可提供高达 100 μA 的电流，并在 STOP 和 STANDBY 模式下可提供高达 20 μA 的电流。*VCORE* 引脚无灌电流能力。标称 V_{CORE} 电压为 1.35V，绝对最大范围为 1.27V 至 1.42V。内部 LDO 可提供 1.3V 至 1.39V 的输出范围，为 UV 和 OV 检测提供 30mV 的阈值裕量。

TPS388R02-Q1 监控器提供 $\pm 7.5mV$ 的精度，并在检测到 UV 或 OV 故障时触发 MCU 断电事件 (*NRST* 低电平)，并保持该状态，直至 V_{CORE} 恢复到有效范围。该器件支持两种工作模式：模式 1X 覆盖 0.2V 至 1.475V 范围，步长为 5mV，在整个温度范围内的最大输入漏电流为 75nA；模式 4X 覆盖 0.8V 至 5.5V，步长为 20mV，在整个温度范围内 1.35V 时最大漏电流为 4.3 μA 。

使用模式 1X 测量 V_{CORE} ，因为该模式具有更精细的阈值粒度，可提供 1.28V、1.285V 和 1.29V 的 UV 选项，以及 1.40V、1.405V 和 1.41V 的 OV 选项。此外，模式 1X 的漏电流较低，可在整个产品生命周期内为其他漏电源（例如旁路电容器和 PCB 效应）预留更大余量。相比之下，模式 4X 提供 1.28V 的 UV 阈值和 1.40V 的 OV 阈值。

VCORE 旁路电容的典型值为 470nF（请参阅 [MSPM0G310x-Q1 数据表](#)）。更大的电容值可提升抗干扰能力，但同时会影响 V_{DD} 旁路要求、启动时间以及 UV/OV 检测时间，详见下表。

V_{CORE} 引脚电容 (C4)	引导时间	V_{DD} 引脚电容 (C3)	UV 和 OV 检测时间
470nF	300 μs	10 μF	1 μs
2.34 μF	450 μs	50 μF	5 μs
4.7 μF	600 μs	100 μF	10 μs

更大的旁路电容与设置在接近 LDO 输出电压范围的监控阈值 (UV 为 1.29V、OV 为 1.40V) 组合，有助于缩短 UV 和 OV 故障检测时间，从而更快地响应受监控电源导轨上的电压异常。

如果 V_{CORE} 超出允许范围，必须对 MSPM0G3107-Q1 执行完整电源周期。在此事件期间，*NRST* 置为有效 (低电平)、TPS22919-Q1 断开 MCU 的电源。*NRST* 为低电平也会停用 TPS388R02-Q1，因为 *NRST* 和 *ACT* 连接在一起。

然后，TPS388R02-Q1 等待预设 *NRST* 延时时间，然后将 *NRST* 置为无效 (高电平)。此转换会重新激活 TPS388R02-Q1 (*ACT* 为高电平)。在 TOUT_SEQ 时间之后（请参阅 [TPS38800-Q1](#) 和 [TPS388R0-Q1 数据表](#)），器件恢复正常运行。

当 V_{DD} 降至 0.9V 以下且持续时间至少为 100 μs 时，即实现有效的 MCU 电源循环。根据为 *VCORE* (C5) 和 *VDD* (C4) 选择的电容值，相应调整 TPS388R02-Q1 的复位延时时间和放电电阻 R6，以实现正确的电源循环行为。

该电路未包含用于检测电源循环事件期间 V_{DD} 下降至低电平的专用措施。如果需要此功能，可通过防止 *NRST* 节点在 TPS22919-Q1 输出仍保持高电平期间转换为高电平，来解决该多点故障。

2.5.3 监测机制

2.5.3.1 监测 VIN 电源导轨是否存在 OV 故障 (包括保护)

采用 OVP 电路来监测 V_{IN} 电源导轨。当输入电压超过定义的 3.9V 阈值时，OVP 电路会自动断开应用与电源的连接，从而防止因出现过压而造成损坏。

2.5.3.2 监控 MCU 电源电压的 UV 或 OV 故障

TPS388R02-Q1 器件可为 MCU V_{DD} 和 V_{CORE} 电源导轨提供持续的 UV/OV 监控。如果该器件在任一电源导轨上检测到 UV 或 OV 故障，该器件会转换到安全状态，以在异常电压条件下保持系统完整性。

2.5.3.3 监测 CPU 处理单元程序流

程序流监测通过两个嵌入式看门狗计时器实现：窗口看门狗计时器 (WWDT) 和独立看门狗计时器 (IWDT)。IWDT 由专用的独立时钟源驱动，可实现独立于主 CPU 时钟的时钟，并扩大故障检测覆盖范围。如果需要在 MCU 和看门狗计时器之间进行物理隔离，请使用 TPS388C02-Q1 版本。该器件将窗口看门狗集成到外部器件中。

2.5.4 FMEA

元件	子元件	子元件功能	失效模式	失效影响	SGV	失效原因	控制或检测故障的措施
MCU	CPU	软件执行	指令流未执行， 非预期指令流， 指令流时序错误	非预期程序执行	SPF	α 粒子或 内部故障	(独立的) 片内或外部窗口看门狗计 时器
MCU	CPU	软件执行	指令流结果错误	计算错误、程序顺序错误、 堆栈指针 (SP) 错误等	SPF	α 粒子或 内部故障	合理性校验、软件测试功能、内置自 检功能
MCU	看门狗	监控 MCU 程序序列	时序异常时看门狗未触发复位	程序执行错误	MPF	看门狗故障	无
MCU	看门狗	监控 MCU 程序序列	时序正常时看门狗触发复位	转换至安全状态	SF	看门狗故障	-
MCU	LDO	内核电压生成电路	电压超出规格 (欠压或过压)	内核电压超出范围	SPF	基准电压漂移、PFET 短路/ 开路	外部电压监控器
MCU	欠压锁定电路	如果 V_{DD} 低于 UVLO 电压， 则对 MCU 进行复位	MCU 未复位	MCU 在 V_{DD} (和 V_{CORE}) 无 效的情况下运行	MPF	内部故障	电压监控器内的冗余 UVLO 电路与 V_{DD} 检测
过压切断	电压监控器	对 VIN 进行过压监测	监控单元未检测出过压/未置位信号	后端器件出现过压	MPF	电阻器或基准源发生漂移/开 路/短路	无
过压切断	电压监控器	对 VIN 进行过压监测	监控器误检测出过压/误置位信号	转换至安全状态	SF	电阻器或基准源发生漂移/开 路/短路	-
过压切断	开关元件	断开电源与应用电路之间的 连接	开关无法断开	后端器件出现过压	MPF	电阻器漂移/开路/短路，BJT 短路失效	无
过压切断	开关元件	断开电源与应用电路之间的 连接	开关无法闭合	转换至安全状态	SF	电阻器漂移/开路/短路，BJT 开路失效	-
电压监控器	VMON 通道	V_{CORE} 电源监测器	监测器在发生欠压或过压故障时，不 会置位 NRST 复位信号。	V_{CORE} 超出范围	MPF	内部故障，基准漂移	BIST
电压监控器	VMON 通道	V_{CORE} 电源监测器	监测器误检出欠压或过压故障	MCU 电源周期	SF	内部故障，基准漂移	-
电压监控器	VMON 通道	V_{DD} 电源监测器	监测器在发生欠压或过压故障时，不 会置位 NRST 复位信号。	V_{DD} 超出范围	MPF	内部故障，基准漂移	BIST
电压监控器	VMON 通道	V_{DD} 电源监测器	监测器误检出欠压或过压故障	MCU 电源周期	SF	内部故障，基准漂移	-
电压监控器	欠压锁定电路	如果 V_{DD} 低于 UVLO 电压， 则对 MCU 进行复位	NRST 未复位	MCU 在无 V_{CORE} 监控条件 下运行	MPF	内部故障	MCU 内部与 V_{DD} 检测通路的冗余 UVLO 电路
电压监控器	I/O 电路	置位 NRST，激活电路	NRST 未置位，ACT 引脚开路	器件不执行监控 (旁路)	MPF	内部故障，ACT 引脚开路	无
负载开关	开关元件	将 V_{DD} 连接到 MCU	收到指令后开关未断开	MCU 未断电	MPF	固定电平失效，控制引脚开 路	无
负载开关	开关元件	将 V_{DD} 连接到 MCU	收到指令后开关未闭合	MCU 无法加电	SF	固定电平失效，控制引脚开 路	-

2.5.4.1 安全机制

系统内实施了多项安全机制，以检测随机硬件故障并做出响应。以下各个小节将详细地介绍每项机制。

2.5.4.1.1 SM1 : MSPM0G3107-Q1 BIST 和软件测试

MSPM0G3107-Q1 内置多项安全机制，其中包括但不限于循环冗余校验 (CRC)、纠错码 (ECC)、窗口看门狗计时器 (WWDT) 和独立窗口看门狗计时器 (IWDT)。此外，软件例程在容错时间间隔 (FTTI) 内定期执行，以测试安全相关的应用元件并检测其他内部故障。有关更多详细信息，请参阅 [MSPM0G3x0x-Q1 功能安全手册](#)。

2.5.4.1.2 SM2 : TPS388R02-Q1 BIST 和内部故障检测

启动时，TPS388R02-Q1 会自动执行 BIST 以验证内部功能完整性。根据 BIST 机制，诊断可采用连续、定期或一次性执行方式。检测到故障后，TPS388R02-Q1 会置位 NRST 信号以复位 MCU，并进入安全状态。有关更多详细信息，请参阅 [TPS388 功能安全信息](#) (可应要求提供)。

2.5.4.1.3 SM3 : MSPM0G3107-Q1 V_{CORE} 监控

TPS388R02-Q1 可持续监控 MSPM0G3107-Q1 的 V_{CORE} 电源导轨的 UV/OV 条件，以使 MCU 内核电压保持在定义的安全工作范围内。该安全机制通过 TPS22919-Q1 启动一次电源循环。

2.5.4.1.4 SM4 : MSPM0G3107-Q1 V_{DD} 监测

TPS388R02-Q1 持续监测 MSPM0G3107-Q1 的 V_{DD} 电源导轨是否存在 UV/OV 故障。该安全机制通过 TPS22919-Q1 启动一次电源循环。

此外，如果 V_{DD} 电压低于定义的阈值，MSPM0G3107-Q1 集成式欠压复位 (BOR) 电路会将 MCU 置于复位状态，从而提供次级保护。

2.5.4.1.5 SM5 : 过压保护

VIN 电源导轨的过压保护分两个工作范围实现：

高于 3.5V 时：TPS388R02-Q1 与 TPS22919-Q1 负载开关配合，可切断 MSPM0G3107-Q1 供电，以防止其在定义的安全电压窗口之外运行。

高于 3.9V 时：TPS3842C011-Q1 监控 V_{IN} 电源导轨，并在输入电压达到或超过 3.9V 标称值时自动断开电源与应用的连接。

2.6 技术安全要求

2.6.1 针对安全目标 SG_01 的 FMEDA

组件名称	故障率/FIT	安全相关元件？	失效模式 (FM)	FM 分布	如果没有安全机制 (SM)，FM 是否可能违反 SG？	SM 可防止 FM 违反 SG？	针对安全目标违反场景的失效模式诊断覆盖率	残余失效率与单点故障 (SPF) 失效率/FIT	导致违反 SG 的 FM 是否与另一个元件的独立失效组合在一起？	检测方法？SM 可防止潜在 FM？	与潜在失效相关的失效模式覆盖率	潜在多点故障失效率/FIT
M0G3107QRGZRQ1	受限	是	永久性	100%	X	SM1、SM3-5	>90%	受限	X	SM1	> 90%	受限
	受限		瞬态	100%	X	SM1、SM3-5	> 99%	受限	X	SM1	100%	0
TPS388R02001RTERQ1	受限	是	永久性	100%					X	SM2	99.71%	受限
	受限		瞬态	100%					X	SM2	100%	0
TPS3842C011-Q1	3	是	复位未能触发	35%					X	-	0%	1.05
			复位误触发	25%								
			复位触发点超出规格范围	30%					X	-	50%	0.45
			复位延时超出规格范围	10%						-		
TPS22919-Q1	3	是	VOUT 输出粘滞导通	25%					X	-	0%	0.75
			VOUT 开路或高阻态	25%								
			VOUT 超出规格范围	35%	X	SM4	99%	0.011				
			QOD 输出粘滞导通	5%								
			QOD 输出粘滞断开	5%					X	-	0%	0.15
			引脚之间短路	5%					X	SM2	100%	0
Q1	4	是	短路	80%					X	-	0%	3.2
			开路	20%								
R1	0.2	是	开路	40%					X	-	0%	0.08
			漂移	60%					X	-	50%	0.06
R2	0.2	是	开路	40%								
			漂移	60%					X	-	50%	0.06
R3	0.2	是	开路	40%					X	-	0%	0.08
			漂移	60%								
R4	0.2	是	开路	40%								
			漂移	60%								
R5	0.2	是	开路	40%								
			漂移	60%								
R6	0.2	是	开路	40%					X	-	0%	0.08
			漂移	60%								

组件名称	故障率/FIT	安全相关元件？	失效模式 (FM)	FM 分布	如果没有安全机制 (SM)，FM 是否可能违反 SG？	SM 可防止 FM 违反 SG？	针对安全目标违反场景的失效模式诊断覆盖率	残余失效率与单点故障 (SPF) 失效率/FIT	导致违反 SG 的 FM 是否与另一个元件的独立失效组合在一起？	检测方法？SM 可防止潜在 FM？	与潜在失效相关的失效模式覆盖率	潜在多点故障失效率/FIT
C1	2	是	短路	65%								
			开路	10%					X	SM4	99%	0.002
			漂移	25%								
C2	2	是	短路	65%								
			开路	10%					X	SM4	99%	0.002
			漂移	25%								
C3	2	是	短路	65%								
			开路	10%								
			漂移	25%								
C4	2	是	短路	65%								
			开路	10%	X	SM4	99%	0.002	X	SM4	100%	0
			漂移	25%								
C5	2	是	短路	65%								
			开路	10%	X	SM4	99%	0.002	X	SM4	100%	0
			漂移	25%								

2.6.1.1 注释

FMEDA 表格结构参考 ISO 26262-5:2018 附录 E 给出的计算示例。

MSPM0G3107-Q1 与 TPS388R02-Q1 为符合 ISO 26262 要求的器件，可按需提供完整 FMEDA 报告。上述系统级 FMEDA 已纳入两款器件的芯片内核级 FMEDA 结果。

TPS3842C011-Q1 归类为具备功能安全能力的器件。有关更多相关功能安全文档，请参阅 [TPS3842-Q1 功能安全 FIT 率、FMD 和引脚 FMA](#)。

电阻、电容、晶体管的 FIT 率以及失效模式分布数据来源于 Birolini (2017) *可靠性工程*。

OVP 电路的触发前提是所连接电源产生过压事件，该过压事件构成双故障场景中的第一重故障。由于 OVP 电路仅在该故障条件下才会动作，并且未实现测试电路，因此在系统正常运行期间无法验证其是否正确工作。该情形符合 ISO 26262 功能安全标准中对潜在故障的定义。

对于无专用检测机制的通用失效模式（例如参数漂移），采用 50% 的诊断覆盖率。针对该类失效模式，假设 50% 为安全故障、50% 为危险故障，二者占比均等。

FMEDA 范围仅限定于芯片内核级 (Die FMEDA)。引脚 FMEDA 必须针对每个器件单独执行，具体取决于系统实现。

2.6.2 定量结果

上方的 FMEDA 表提供了该子系统的以下功能安全结果。

基于 IEC/TR 62380	芯片	
	永久性	瞬态
单点故障指标 - SPFM	>99%	>99%
潜在故障指标 - LFM	>70%	不适用

3 总结

建议设计满足基于 MSPM0G3107-Q1 实现最高 ASIL-B 等级、符合 ISO 26262 所必需的系统级功能安全要求。具体系统是否满足 ASIL-B 合规性，取决于系统设计本身。本文档提供的 FMEDA 结果需要集成到更高层级的系统级 FMEDA 中，为最终应用产品的功能安全评估提供支持。

4 参考资料

1. 德州仪器 (TI), [MSPM0 MCU 在汽车应用中的优势](#), 技术白皮书
2. 德州仪器 (TI), [MSPM0G3x0x-Q1 功能安全手册](#), 功能安全手册
3. 德州仪器 (TI), [MSPM0 G 系列 80MHz 微控制器技术参考手册](#), 用户指南
4. 德州仪器 (TI), TPS388 功能安全信息 (可应要求提供)
5. 德州仪器 (TI), [TPS3842-Q1 功能安全时基故障率、FMD 和引脚 FMA 功能安全信息](#)
6. Alessandro Birolini, Reliable Engineering, 8th Edition, ISBN 978-3-662-54208-8
7. 德州仪器 (TI), [带 CAN-FD 接口的 MSPM0G310x-Q1 汽车混合信号微控制器](#), 数据表
8. 德州仪器 (TI), [TPS38800-Q1/TPS388R0-Q1 多通道过压和欠压 I2C 可编程电压监控器](#), 数据表
9. 德州仪器 (TI), [符合 ISO26262 标准的 MSPM0x 器件预筛选列表](#), 网页
10. 德州仪器 (TI), [用于满足 ASIL B 要求的 MSPM0 外部 VCore 监控](#), 应用手册

重要通知和免责声明

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任何明示或暗示的担保，包括但不限于对适销性、与某特定用途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安全、安保法规或其他要求。

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 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 [TI 销售条款](#)、[TI 通用质量指南](#) 或 [ti.com](#) 上其他适用条款或 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。除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

版权所有 © 2026，德州仪器 (TI) 公司

最后更新日期：2025 年 10 月