Application Note

BQ79600（UART/SPI 至菊花链网桥 IC）的安全手册

Jyothsna Gandham

摘要

本文档是德州仪器 (TI) BQ79600 UART/SPI 至菊花链网桥 IC 的安全手册。本手册提供的信息可帮助开发人员将 BQ79600 器件集成到安全相关系统中。

备注

请注意，在开始开发包含 BQ79600 的安全相关工程之前，除了使用本安全手册之外，您还应该联系当地的 TI 销售人员以获取 TI 的安全文档。

内容

插图清单

表格清单

商标

1 引言

系统和设备制造商或设计人员（作为本文档的用户）负责确保其系统（以及系统中包含的任何 TI 硬件或软件）满足所有适用的安全、法规和系统级性能要求。本文档中的所有应用和安全相关信息（包括应用说明、建议的安全措施、建议的 TI 产品和其他资料）仅供参考。用户了解并同意在安全关键型应用中使用 TI 器件须完全自行承担风险，对于由此类应用引起的任何和全部伤害、索赔、诉讼或成本，用户（作为买方）同意为 TI 提供辩护及赔偿，并保护 TI 免受其害。

本文档是德州仪器 (TI) BQ79600 的安全手册。本文档提供的信息可帮助系统开发人员使用 BQ79600 来创建与安全相关的系统。这个文档包含：

- 产品架构概述
- 用于减少系统故障的开发流程概述
- 用于管理系统集成商在符合 ISO26262 标准的系统中使用该器件时可能会考虑的随机故障和使用假设 (AoU) 的安全架构概述
- 架构划分和实现的安全机制的详细信息

安全分析报告记录了本文档未涵盖的以下信息：

- 故障率估算
- 定性失效分析（设计 FMEA、引脚 FMEA、DFA、FTA）
- 定量失效分析（定量 FMEDA）
- 根据每个系统示例实施的目标标准计算的安全指标

安全案例记录了本文档未涵盖的以下信息：

- 符合目标标准的证据
- 目标标准符合性评估的结果

TI 希望本文档的用户大致熟悉 BQ79600。应将本文档与正在开发的产品的相关数据表和其他文档结合使用。与 IEC 61508:2010 中的安全手册定义相比，该技术内容以简化开发、减少内容重复和避免混淆为目的进行划分。

2 产品概述

BQ79600 是一款网桥 IC，旨在连接微控制器 (MCU) 和 TI 电池监控 IC（例如 bq7961X 和 bq79606）。BQ79600 直接连接到 MCU，并通过变压器或电容器与电池监控 IC 相隔离。

在睡眠/关断模式下，BQ79600 可以支持反向唤醒功能。如果在环形架构中检测到任何未屏蔽的故障，BQ79600 可以唤醒 MCU 或 PMIC。

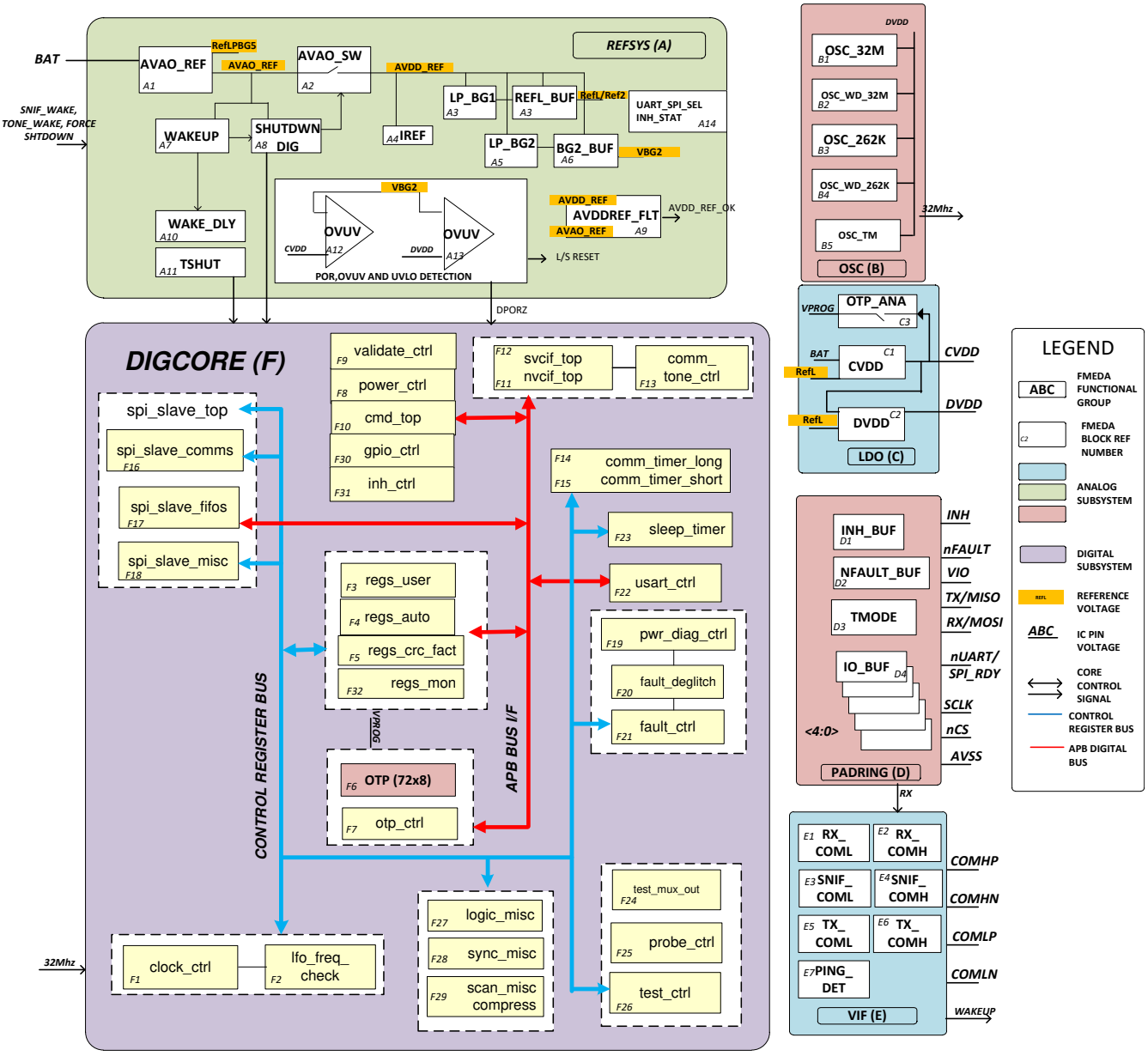

图 2-1. BQ79600-Q1 架构概述

2.1 目标应用

BQ79600 被设计为用作网桥 IC，用于在以下应用中连接微控制器 (MCU) 和 TI 电池监控 IC：

- 纯电动汽车 (EV)、混合动力电动汽车 (HEV) 或插电式混合动力汽车 (PHEV) 动力总成
- 48V 汽车电池系统
- 工业安全应用，尤其是能源存储系统 (ESS)

在概念阶段对多个安全应用的分析支持根据 ISO 26262 – 10 进行独立安全元素 (SEooC) 开发。在设计该器件时，TI 对如何使用该器件做出了各种假设，以便满足电池监控系统的预期行业要求，因为这些安全关键型系统的要求特别高。

尽管 TI 在开发这些器件时考虑了某些应用，但是这不应限制客户实施其它系统。对于所有安全关键型器件，系统集成商必须使器件安全概念合理化，以确认其满足系统安全需求。

在目标系统的要求有所重叠的情况下，TI 已经尝试按照最严格的要求来设计器件。例如，汽车电池应用中的容错响应时间间隔通常约为 1 秒。在这种情况下，TI 已针对假设的包含 96 节电池的应用 100ms 故障检测时间间隔执行了计时器子系统分析。

2.2 产品安全约束

BQ79600 安全分析是在以下系统限制假设下进行的：

- BQ79600 的所有输入都处于器件数据表中定义的建议工作条件范围内，并且不超过其中定义的绝对工作条件。
- BQ79600 的工作温度处于器件数据表中定义的环境温度和最大结温限制范围内。
- BQ79600 的所有外部器件都符合相关器件的器件数据表中定义的电气特性。
- 系统板的布局遵循 BQ79600 数据表中定义的布局指南。
- 微控制器、FPGA 或其他能够作为通信主器件的器件（以下称为主器件）通过 UART 接口直接与 ASIC 进行通信。
- 主机应监测由 ASIC 测量的电池电压和温度，负责根据电池电压和温度信息执行相应的操作，并在适当的情况下将系统置于安全模式。
- 主机应监测是否存在 ASIC 检测到的故障，负责根据 ASIC 检测到的故障执行相应的操作，并在适当的情况下将系统置于安全模式。
- 主机应监测与 ASIC 的通信是否中断，并负责在适当的情况下将系统置于安全模式。
- 主机的 UART 引脚接头和 ASIC 之间的垂直接口通信引脚的连接电路应遵循数据表指南。
- 主机的 SPI 引脚接头和 ASIC 之间的垂直接口通信引脚的连接电路应遵循数据表指南。

3 BQ79600 针对系统故障管理的开发过程

对于安全关键型开发，必须同时管理系统和随机故障。德州仪器 (TI) 为安全关键型半导体创建了开发流程，从而极大地降低了发生系统故障的可能性。该流程建立在作为安全关键型开发基础的标准质量管理开发流程之上。然后第二层开发活动（专门针对符合 IEC 61508 和 ISO 26262 标准的安全关键型应用而开发）增强了该流程。在 BQ79600 的开发过程中管理系统故障的开发活动符合 ASIL-D 标准。

3.1 TI 新产品开发流程

德州仪器 (TI) 为安全关键型和非安全关键型汽车应用开发混合信号汽车 IC 已超过十五年。汽车市场对于质量管理和产品可靠性有着很强的要求。尽管不是明确针对符合功能安全标准进行开发，但 TI 新产品开发流程已经包含了管理系统故障所需的许多要素。

BQ79600 是使用 TI 的新产品开发流程开发的，该流程经 Det Norske Veritas Certification, Inc. 评估，符合 ISO TS 16949 标准。

此标准过程将开发分成以下几个阶段：

- 业务计划
- 验证
- 创建
- 评估
- 投入量产

图 3-1 显示了标准流程。

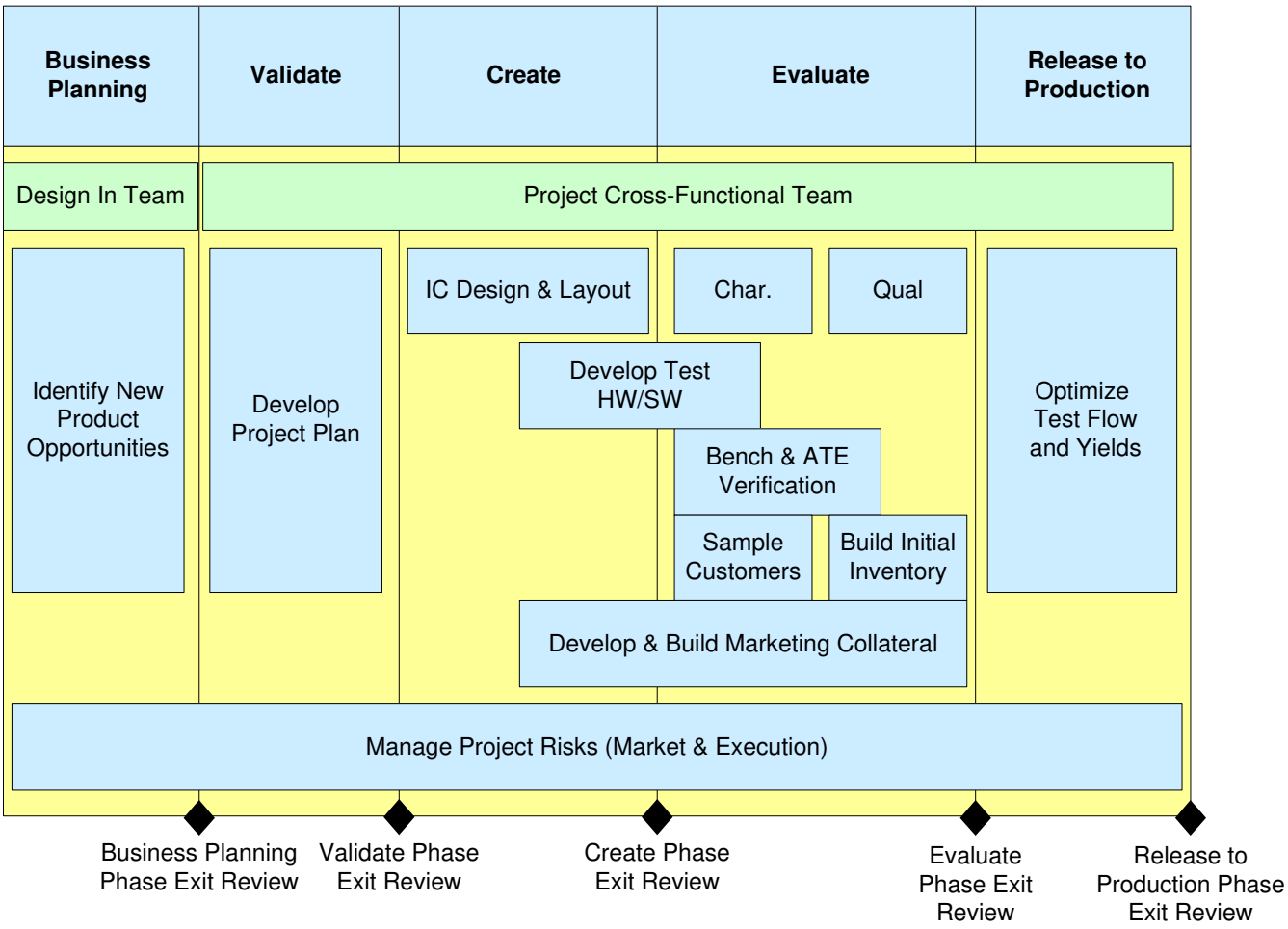

图 3-1. TI 新产品开发流程

3.2 TI 安全开发流程

TI 安全开发流程源自 ISO 26262，这是一组用于混合信号电路安全开发流程的要求和方法。该流程是 TI 新产品开发流程的一个组成部分。该安全开发流程的目标是减少系统故障。

该安全开发流程以符合 IEC 61508 第二版和 ISO 26262 第二版的要求为目标，并且正在不断改进以纳入先进的最佳做法。尽管该安全开发流程不直接针对其他功能安全标准，但 TI 预计许多客户将断定其他功能安全系统应能轻松使用按照行业先进标准开发的产品。

TI 安全开发流程的关键要素为：

- 基于 TI 安全关键型系统开发方面的专业知识在系统级设计、安全概念和要求方面的假设。
- 所结合的定性和定量或者类似的安全分析技术（包含所有器件故障模式和诊断技术）。
- 基于多重工业标准以及 TI 制造数据的故障评估。
- 对通过根据 ISO 26262、IEC 61508 进行多项安全关键型开发以及参与功能安全国际工作组所获得的经验教训的整合。

表 3-1 列出了涵盖标准 QM 开发流程的这些活动。

表 3-1. TI 新产品开发流程

商业机会预先筛选	项目规划	创建	验证、制作样片和确定特征	质量	提升/支持
确定是否需要执行安全流程	定义 SIL/ASIL 等级	执行安全设计	在器件中验证安全设计	安全设计认证	实施支持运营和生产的计划
与主要客户和供应商一同执行开发接口协议 (DIA)	制定安全计划	对设计进行定性分析（FMEA 和 FTA）	发布安全手册	发布安全案例报告	更新安全案例报告（如果需要）
	提交安全案例	将调查结果纳入安全设计	发布安全分析报告	更新安全手册（如果需要）	定期审查确认措施
	分析假设的系统以生成系统级安全假设和要求	开发安全产品预发布版本	确定安全设计的特征	更新安全分析报告（如果需要）	
	制定元件级安全要求	在晶体管、门和 RTL 级别验证混合信号安全设计	审查确认措施	审查确认措施	
	验证组件安全要求是否符合系统安全要求	对设计进行定量分析 (FMEDA)			
	在设计规格中实施安全要求	将调查结果纳入安全设计			
	验证设计规格是否满足元件安全要求	在晶体管/门/物理布局级别验证混合信号安全设计			
	审查确认措施	审查确认措施			

3.3 开发接口协定

开发接口协议 (DIA) 的目的是定义客户和供应商在促进功能安全系统开发方面的责任。

在定制开发中，DIA 是客户和供应商之间在系统和定制 TI 器件开发过程早期阶段执行的关键文档。BQ79600 器件是作为独立安全元素 (SEooC) 开发的商用现货 (COTS) 产品，因此 ISO 26262-8:2018 不要求客户和供应商之间执行 DIA。将定制 DIA 请求提交给您当地的 TI 销售办事处进行处理。

3.4 开发要求

BQ79600 产品是作为独立安全元素 (SEooC) 而开发的，其安全目标是活动模式下的通信符合 ASIL-D 标准，睡眠/关断模式下的通信符合 ASIL-B 标准。使用的安全要求假设基于 TI 对目标安全应用的分析。TI 愿意讨论是否接受针对未来设计的新客户安全要求；请联系您当地的 TI 销售办事处了解更多信息。

3.5 安全文档的可用性

表 3-2 列出了 BQ79600 器件的安全文档，这些文档可以公开或根据保密协议 (NDA) 提供：

表 3-2. 安全文档

可交付使用的名称	内容	机密性
BQ79600 通信网桥接口的安全手册	针对产品安全特性的用户指南，包括系统级使用假定	
BQ79600 通信网桥接口的安全分析报告摘要	按照系统级 ISO 26262 和/或者 IEC 61508 的 FIT 速率和器件安全标准汇总	
BQ79600 通信网桥接口的详细安全分析报告	可用安全分析的全部结果采用允许使用定制标准进行计算的记录格式	需要 NDA

4 BQ79600 用于管理随机故障的产品架构

对于安全关键型开发，必须同时管理系统和随机故障。BQ79600 产品架构集成了多个可以检测和报告随机故障的模块，从而使主机微控制器或其他处理引擎能够将该器件返回到安全状态。

该器件分配了一组核心模块来连续运行硬件安全机制。该器件还提供多个可编程机制，用于在发生系统或随机故障时将器件转换为默认（安全或关断状态）工作模式。

本节介绍 BQ79600 的运行状态和安全状态。

4.1 器件运行状态

BQ79600 具有多种运行状态。系统开发人员应在其软件和系统级设计概念中监测这些运行状态。有关运行状态状态机运行的详细信息，请参阅 BQ79600 的产品数据表。图 4-1 对运行状态状态机进行了概述。

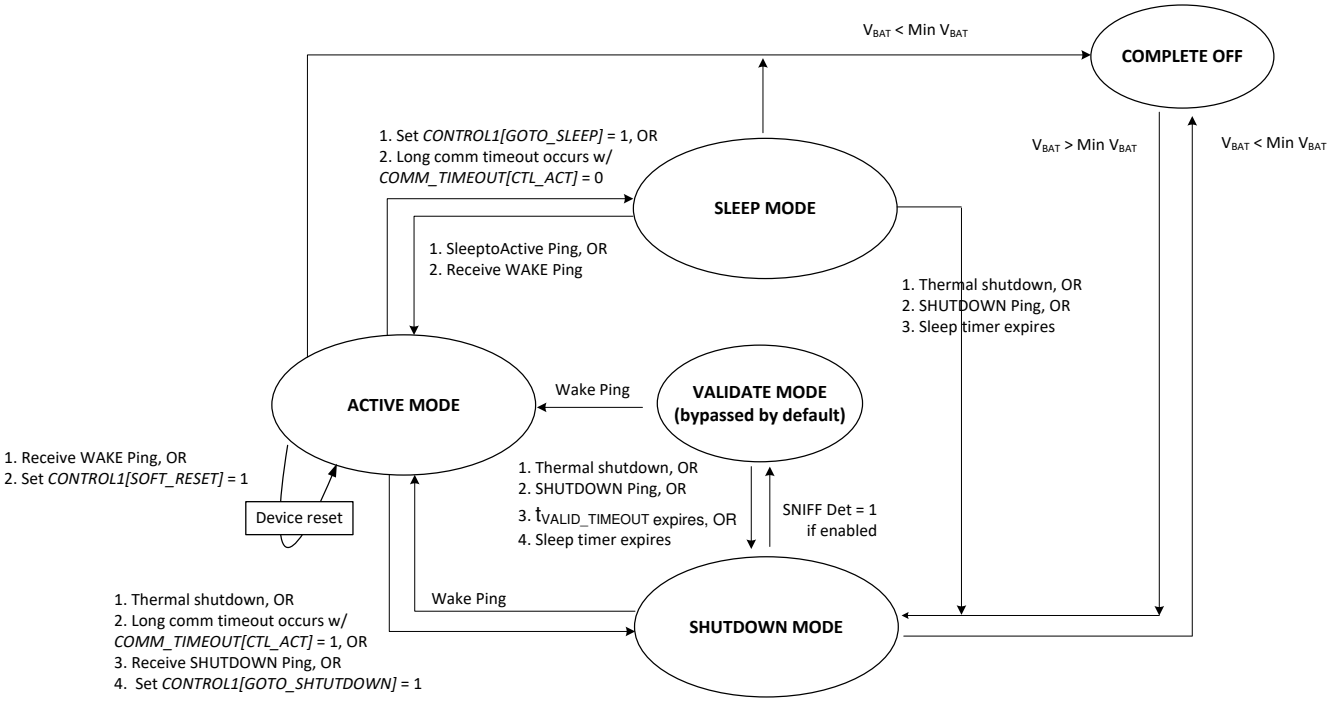

图 4-1. BQ79600 运行状态机

BQ79600 以五种模式之一运行。模式取决于 VBAT 电压和来自主机微控制器的操作命令。下面是对这些模式的概括性说明：

- 关闭 – 电池组的 VBAT 电压低于 VBAT 最小阈值，器件关闭。当 VBAT 引脚上的电压大于 VBAT 最小阈值时，器件转换到关断模式并开始监测是否存在唤醒信号。
- 关断 – 可用的最低功耗状态。为了唤醒至活动模式，器件监测 RX 引脚上是否存在 WAKE ping 输入。可以将 Snif Detector 功能配置为在该模式下开启。
- 活动 – 在活动模式下，器件主动地与主机微控制器和堆栈中的电池监控 ASIC 进行通信。在热关断或命令或通信超时后，器件可以从活动模式进入睡眠模式或关断模式。
- 睡眠 – 在睡眠模式下，器件的功能有限。器件会在检测到 SLEEPtoACTVIE 或 WAKE 信号后转换为活动模式。如果出现睡眠超时信号、关断信号或热关断，则器件转换至关断模式。
- 故障验证 – 故障验证模式的功能有限。该模式仅在启用 Snif Detector 功能后存在。当器件在关断模式下检测到故障音调时，转换至故障验证模式，以验证故障音调。进入该模式时会设置状态位 [VALIDATE_DET]。禁用 Snif Detector 功能后会绕过该模式。

4.2 安全状态

当没有施加电源时，或当器件处于关断模式或当器件在功能齐全且无故障的集成系统中运行时，应将器件视为处于安全状态。在检测到通信故障或支持硬件故障并向主机发送相关信号后，应将器件视为处于安全状态。主机负责监测是否存在来自器件的故障信号通信。主机负责监测与主机的通信是否中断或发生故障。系统/项目的外部主机元素负责故障反应和系统向系统安全状态的转换。

5 BQ79600 架构安全机制和使用假设

本节总结了 BQ79600 架构的每个主要功能块的安全机制，并提供了其使用假设。每个使用假设都由 [AoUx] 表示，其中 *x* 是标识号。安全分析报告指出了这些安全机制的有效性。

系统集成商自然应根据特定最终用途全面评估有效性。

本文档中所述的安全措施可能与表 5-1 中列出的一项或多项安全目标相关。

表 5-1. 假设的安全目标编号

目标编号	说明
1	活动模式下的通信
2	睡眠/关断模式下的通信

每项安全措施的编号不是严格按顺序排列的。表 5-2 说明了所涵盖器件的编号范围和相关功能。

表 5-2. 安全措施编号方案说明

范围	覆盖范围说明
0-99	与电源轨和基准诊断密切相关
100-199	与通信诊断密切相关
200-299	涵盖不属于其他类别的器件功能的安全措施

表 5-3. 安全机制类别

诊断间隔	说明
FDTI	设计用于在每个容错检测间隔内由外部微控制器协助处理的机制或诊断功能
MPFDI	设计用于在多点故障检测间隔内至少一次在外部微控制器协助下执行的机制或诊断功能。
AUTO	属于无源元件或由 ASIC 自动执行的机制
PGM	在器件编程期间使用但在正常运行期间不使用的机制或诊断功能

备注

检测 - 一种频繁或连续运行的测试，目的是防止单点安全目标违反情况（即输出驱动器过压报告）。

诊断 - 定期执行的测试（即每个点火循环一次），目的是防止潜在的安全目标违反情况，例如检测失败（例如注入过压以验证过电压检测是否有效）。

5.1 按设计模块划分的安全机制

表 5-4. 安全机制

用于多个块的按设计块划分的安全机制在该表中仅列出一次，不重复列出				
设计块	**SM 编号**	**安全机制名称**	**诊断间隔**	**诊断/检测**
DVDD_LDO	SM010	DVDD OV 检测	FDTI	检测
DVDD_LDO	SM011	DVDD OC 保护	自动	检测
CVDD_LDO	SM012	CVDD OV 检测	FDTI	检测
CVDD_LDO	SM013	CVDD UV 检测	FDTI	检测
CVDD_LDO	SM014	CVDD OC 保护	自动	检测
REFSYS	SM015	AVDDREF OV 检测	FDTI	检测
REFSYS	SM016	AVDDREF SW 故障检测	FDTI	检测
REFSYS	SM017	电源诊断测试模式	MPFDI	诊断
COMM	SM100	MCU 信号丢失检测	FDTI	检测
COMM	SM101	MCU 异常数据错误检测	FDTI	检测
UART	SM102	UART CRC 错误检测	FDTI	检测
VIF	SM103	菊花链 CRC 错误检测	FDTI	检测
COMM	SM104	短通信超时检测	FDTI	检测
COMM	SM105	长通信超时检测	FDTI	检测
UART	SM106	UART 通信清除检测	FDTI	检测
UART	SM107	UART 停止位错误检测	FDTI	检测
COMM	SM108	帧起始错误检测	FDTI	检测
COMM	SM109	字节错误检测	FDTI	检测
COMM	SM110	异常通信检测	FDTI	检测
COMM	SM112	IERR 检测	FDTI	检测
COMM	SM113	等待错误检测	FDTI	检测
VIF	SM114	菊花链同步 1 错误检测	FDTI	检测
VIF	SM115	菊花链同步 2 错误检测	FDTI	检测
VIF	SM116	菊花链位错误检测	FDTI	检测
VIF	SM117	菊花链字节错误检测	FDTI	检测
VIF	SM118	菊花链故障信号诊断	MPFDI	诊断
COMM	SM119	NFAULT 引脚诊断	FDTI	诊断
VIF	SM120	睡眠模式故障音调	FDTI	检测
VIF	SM121	睡眠模式心跳	FDTI	检测
VIF	SM122	快速心跳检测	FDTI	检测
COMM	SM123	菊花链 CRC 诊断	MPFDI	诊断
COMM	SM124	MCU 通信和故障屏蔽诊断	MPFDI	诊断
COMM	SM125	MCU 器件地址诊断	MPFDI	诊断
COMM	SM126	MCU 通信故障诊断	MPFDI	诊断
COMM	SM127	FMT 错误检测	FDTI	检测
COMM	SM128	SPI 通信清除检测	FDTI	检测
COMM	SM129	TX 数据异常错误检测	FDTI	检测
COMM	SM130	RX 数据异常错误检测	FDTI	检测
COMM	SM131	正确的通信接口检测	FDTI	检测
COMM	SM132	FIFO 寄存器诊断	MPFDI	诊断
COMM	SM133	TXFIFO 下溢检测	FDTI	检测
COMM	SM134	TXFIFO 上溢检测	FDTI	检测

表 5-4. 安全机制 (continued)

用于多个块的按设计块划分的安全机制在该表中仅列出一次，不重复列出				
设计块	**SM 编号**	**安全机制名称**	**诊断间隔**	**诊断/检测**
COMM	SM135	RX FIFO 上溢检测	FDTI	检测
COMM	SM136	MCU SPI 故障诊断	MPFDI	诊断
COMM	SM137	SPI 冲突检测	FDTI	检测
COMM	SM200	Snif 检测器诊断	MPFDI	诊断
COMM	SM201	INH 引脚状态检测	FDTI	检测
COMM	SM202	INH 驱动程序诊断	MPFDI	诊断
LFOSC	SM203	LFOSC 时钟缺失检测	自动	检测
HFOSC	SM204	HFOSC 时钟缺失检测	自动	检测
HFOSC	SM205	LFOSC 频率不匹配检测	FDTI	检测
NVM	SM206	出厂寄存器 CRC 检测	FDTI	检测
NVM	SM207	出厂 CRC 诊断	MPFDI	诊断
NVM	SM208	客户寄存器完整性检测	FDTI	检测
NVM	SM209	客户寄存器完整性诊断	MPFDI	诊断
OTP	SM210	OTP 出厂负载错误	FDTI	检测
TSHUT	SM211	热关断检测	自动	检测
PING	SM212	关断状态	自动	检测
test_ctrl	SM213	出厂测试模式检测	FDTI	检测

5.2 与电源轨和基准电压相关的架构安全机制

接下来的各节介绍了针对电源轨和基准电压的 BQ79600 架构安全机制。

5.2.1 SM010：DVDD OV 检测

BQ79600 自动将 1.8V DVDD LDO 输出电压与过压阈值进行比较。如果故障条件有效，则将设置寄存器 FAULT_PWR 中的 DVDD_OV 位。

[AoU1] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_PWR 位是否为 0。

5.2.2 SM011：DVDD 电流限制

BQ79600 监测 DVDD LDO 输出电流并根据数据表规格对其进行限制。这可以在出现短路或严重瞬态负载的情况下保护电路。

备注

电流限制机制连续工作，没有可监测的状态指示。

5.2.3 SM012：CVDD OV 检测

BQ79600 将 5V CVDD LDO 输出电压与过压阈值进行比较，并设置寄存器 FAULT_PWR 中的 CVDD_OV 位。

[AoU1] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_PWR 位是否为 0。

5.2.4 SM013：CVDD UV DRST 检测

BQ79600 将 5V CVDD LDO 输出电压与欠压阈值进行比较，并设置寄存器 FAULT_PWR 中的 CVDD_UV_DRST 位。该条件将触发器件的数字复位。

[AoU1] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_PWR 位是否为 0。

5.2.5 SM014：CVDD 电流限制

BQ79600 测量 CVDD LDO 输出电流并根据数据表规格对其进行限制。这可以在短路或严重瞬态负载的情况下保护电路。

备注

电流限制机制连续工作，没有可监测的状态指示。

5.2.6 SM015：AVDD_REF OV 检测

BQ79600 将 2.4V 常开型内部 AVDDREF 电压与过压阈值进行比较，并设置寄存器 FAULT_PWR 中的 AVDDREF_OV 位。

[AoU1] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_PWR 位是否为 0。

5.2.7 SM016：AVDDREF SW 故障检测

BQ79600 将 2.4V AVAO_REF 输出电压与 AVDDREF 电压进行比较。这两条电压轨由一个开关连接，该开关应具有非常小的电压降。如果电压降超过数据表中的限值，则会设置寄存器 FAULT_PWR 中的 AVAO_SW_FAIL 位。

[AoU1] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_PWR 位是否为 0。

5.2.8 SM017：电源诊断测试模式

BQ79600 包含电源模式测试模式，可帮助检测 LDO 过压检测电路功能的潜在故障。

该测试模式涵盖 FAULT_PWR 寄存器中的故障位 CVDD_OV、DVDD_OV、AVDDREF_OV。寄存器 FAULT_PWR 中的 CVDD_OV、DVDD_OV、AVDDREF_OV 位指示诊断测试的结果。

[AoU2] - 主机 MCU 在每个 MPDTI 期间执行诊断。

[AoU3] - 主机写入 PWR_DIAG_GO = 1（自行清除位），以启用诊断测试模式。

[AoU4] - 主机等待 PWR_DIAG_RDY = 1，然后读取寄存器 FAULT_PWR 中的 CVDD_OV、DVDD_OV、AVDDREF_OV 位，以验证是否设置了故障。

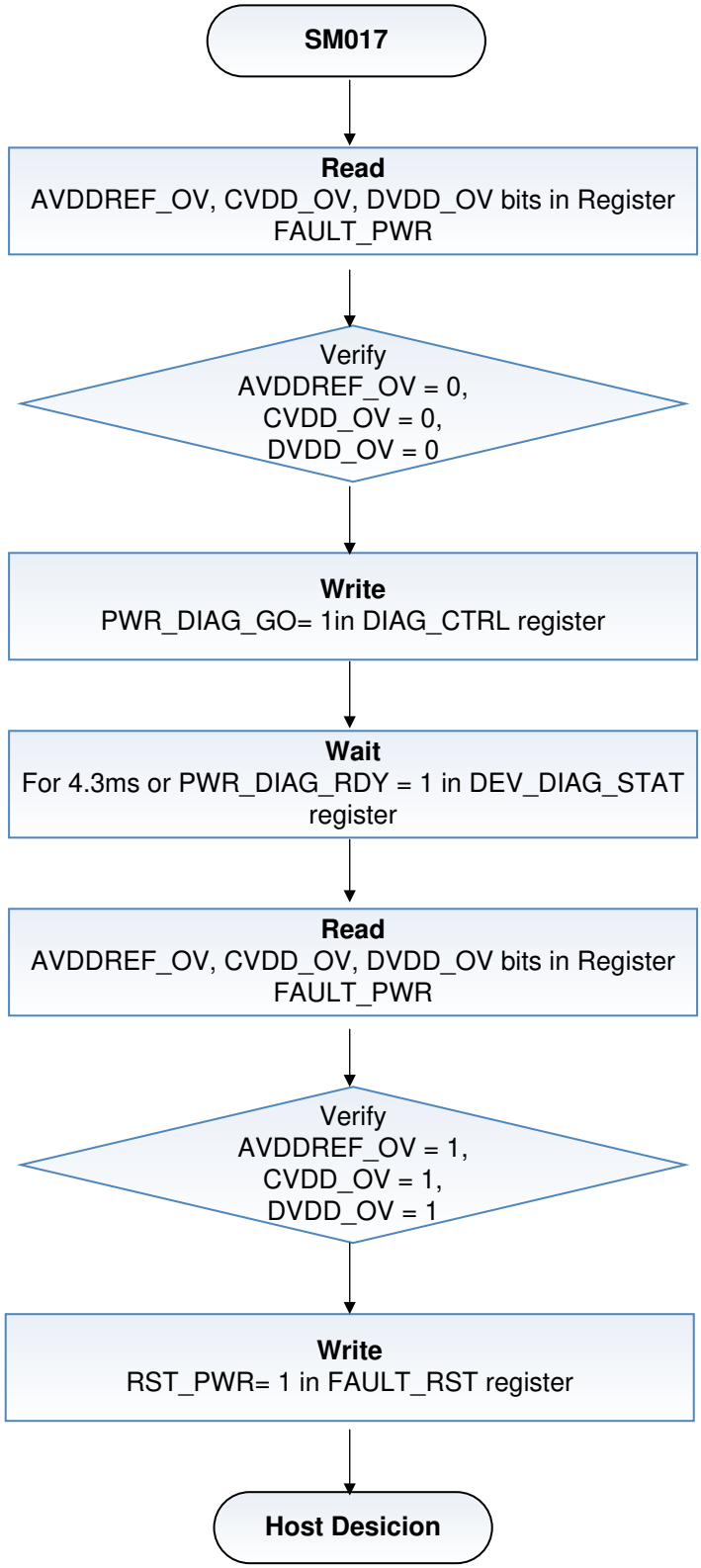

图 5-1. SM017：电源测试模式

5.3 与通信诊断相关的架构安全机制

BQ79600 通信路径具有多种诊断功能，有助于实现器件的安全目标。主机 MCU 应始终监视通信是否产生预期的结果，还应进行通信诊断并监视是否检测到任何通信故障。

5.3.1 SM100：MCU 信号丢失检测

主机 MCU 根据通信类型和预期响应计算每次通信的最大响应时间。如果在分配的时间内没有接收到所有预期的回复，控制器应该识别出通信中断故障。

[AoU5] - 主机 MCU 验证在分配的时间内是否接收到预期的通信响应。

5.3.2 SM101：MCU 异常数据错误检测

主机 MCU 为将从 ASIC 接收的每个预期 UART 帧计算预期帧数据长度、预期器件地址、预期寄存器地址、预期数据字节数以及 CRC。如果 UART 回复与计算的预期值不匹配，控制器应将其识别为接收到异常数据故障。应丢弃不合格的数据传输。

[AoU6] - 主机 MCU 验证接收到的数据是否符合预期。

5.3.3 SM102：UART/SPI CRC 错误检测

BQ79600 计算从主机 MCU 接收的 UART/SPI 数据的 16 位 CRC，并将其与 UART/SPI 帧中发送的 CRC 数据进行比较。如果计算出的 CRC 和接收到的 CRC 不匹配，BQ79600 会设置 RC_CRC 位。如果寄存器 FAULT_COMM1 或 FAULT_COMM2 中的命令帧发生 CRC 错误，则设置 RC_CRC 位。UART_Frame 和 SPI_Frame 具有一对 CRC 故障位。会丢弃不合格的数据传输。

主机 MCU 计算从 UART/SPI 数据接收的 16 位 CRC，并将其与 UART/SPI 帧中发送的 CRC 数据进行比较。如果计算出的 CRC 和发送的 CRC 不匹配，主机 MCU 应将其识别为 CRC 故障。应丢弃不合格的数据传输。

[AoU7] - 主机 MCU 计算一个 16 位 CRC，作为每个发送的 UART/SPI 通信帧的一部分。

[AoU8] - 主机 MCU 验证接收到的 CRC 数据是否正确。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.4 SM103：菊花链 CRC 错误检测

BQ79600 自动为接收到的每个 VIF 菊花链通信帧计算 16 位 CRC，并将其与 VIF 通信帧中发送的 CRC 数据进行比较。如果计算出的 CRC 和发送的 CRC 不匹配，BQ79600 会设置 FAULT_COMM2 寄存器中的 RR_CRC 位。会为读取帧设置 RR_CRC 位。COML_FRAME 和 COMH_FRAME 具有一对 CRC 故障位。会丢弃不合格的数据传输。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.5 SM104：短通信超时检测

在活动模式下，为了帮助检测异常通信延迟，短通信超时会检查是否缺少从 UART/SPI 或菊花链接收到的有效帧。通过设置 COMM_TIMEOUT_CONF 寄存器中的 CTS_TIME[2:0] 位来启用计时器。当从 UART/SPI 或菊花链接收到有效帧时，计时器复位。如果短通信超时到期，则设置 FAULT_SYS 寄存器中的 CTS 位。器件保持在活动模式。可以监测该位以帮助检测与主机 MCU 或电池监控器件堆栈的通信中的异常延迟。

[AoU10] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_SYS 位是否为 0。

5.3.6 SM105：长通信超时检测

如果在活动模式下出现异常通信延迟，BQ79600 长通信超时可自动将器件置于低功耗睡眠模式或将其置于关断模式（可选）。通过设置 COMM_TIMEOUT_CONF 寄存器中的 CTL_TIME[2:0] 位来启用计时器。当从 UART/SPI 或菊花链接收到有效帧时，计时器复位。如果长通信超时到期，则设置 FAULT_SYS 寄存器中的 CTL 位，并将器件置于睡眠模式。在 SLEEPtoACVITE 转换为活动模式后，可以读取 FAULT_SYS 寄存器中的 CTL 位。FAULT_SYS 寄存器中的 CTL 位将通过作为器件唤醒过程一部分的寄存器复位进行复位。

可选择设置 COMM_TIMEOUT_CONF 寄存器中的 CTL_ACT 位，以在长通信超时到期时将器件置于关断模式。FAULT_SYS 寄存器中的 CTL 位将通过作为器件唤醒过程一部分的寄存器复位进行复位。

备注

如果 BQ79600 和主机 MCU 无法通信，则可以配置长通信超时设置以使 BQ79600 保持在活动模式，或转换到睡眠模式，或转换到关断模式。

[AoU10] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_SYS 位是否为 0。

[AoU11] — 当长通信计时器到期时，将器件配置为关断模式。

5.3.7 SM106：UART 通信清除检测

接收器持续监测 RX 线路上是否存在指示所接收下一个字节将是新帧起始的 UART 通信中断条件。当检测到通信清除时，BQ79600 立即终止当前通信，并设置 FAULT_COMM1 寄存器中的 COMMCLR_DET 位。主机必须在通信清除之后至少等待 tUART(RXMIN) 才能开始发送新的通信帧。

备注

还将设置 FAULT_COMM1 寄存器中的 STOP_DET 位，因为通信清除时序违反了典型的字节时序。

RX 引脚上的 SLEEPtoACTIVE ping 也会清除 UART 接收器。在从睡眠模式转换到活动模式时会设置 COMMCLR_DET 位。如果器件处于活动状态，RX 引脚上的 SLEEPtoACTIVE ping 将设置 COMMCLR_DET 和 STOP_DET 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

[AoU12] - 在通信中断并建立正常通信后，主机 MCU 读取 COMMCLR_DET 位并将其复位。

5.3.8 SM107：UART 停止位错误检测

停止位指示 UART 字节传输结束。如果接收到的 UART 数据字节没有停止位，则设置 FAULT_COMM1 寄存器中的 STOP_DET 位。

备注

RX 引脚上的 UART 通信中断将设置 FAULT_COMM1 寄存器中的 STOP_DET 位。RX 引脚上的 SLEEPtoACTIVE ping 将设置 COMMCLR_DET 和 STOP_DET 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

[AoU13] - 在通信中断并建立正常通信后，主机 MCU 读取 STOP_DET 位并将其复位。

5.3.9 SM108：帧起始错误检测

如果在 UART/SPI 或 VIF 堆栈通信中在当前帧完成之前接收到中断或新的帧起始，则会设置 SOF 位。可能会根据接口（UART、SPI、COML 或 COMH）和通信类型（接收命令 (RC)、接收响应 (RR) 或传输数据 (TR)）来设置六个 SOF 位之一。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.10 SM109：字节错误检测

当在 COMH/COML 上接收到的帧中的任何字节发生无效位计数或者在 UART/SPI 上接收到的任何字节上发生停止错误且后续未执行通信清除时，设置 BYTE_ERR 位。可能会根据接口（UART、SPI、COML 或 COMH）和通信类型（接收命令 (RC) 或接收响应 (RR)）来设置四个 BYTE_ERR 位之一。当发生字节错误时，在该接口上接收到的所有其他字节都将被忽略。发生的任何其他帧错误都将被忽略。在 COMH/COMH 上接收到的字节会在堆栈中向上传播，而在 UART/SPI 上接收到的字节不会被传播。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.11 SM110：异常通信检测

如果检测到来自意外接口的通信，则设置异常通信位。例如，接收到的响应方向是错误的。在接收到响应 (RR) 时可能会在 COML 和 COMH 上设置异常位。当发生来自意外接口的通信时，在该接口上接收到的所有其他字节都将被忽略。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.12 SM112：IERR 检测

当接收到无效的帧初始化字节时，设置 IERR 错误位。可能会根据接收无效帧初始化字节的接口（UART、SPI、COML 和 COMH）来设置四个 IERR 位之一。当发生初始化字节错误时，UART/SPI 会忽略通信，不进行转发。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.13 SM113：等待错误检测

如果在前一条命令的所有响应完成之前接收到新命令启动的消息，则设置等待错误位。可能会设置两个等待位，具体取决于接口（UART 或 SPI）。新通信的启动必须始终等待前一条命令的通信回复完成。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.14 SM114：菊花链同步 1 错误检测

当 VIF 通信总线上的同步数据存在错误并且时序可能不正确时，设置同步 1 错误位。该错误表明噪声已破坏了所传输数据前几位中的时序信息。同步 1 位的设置取决于接口 COML 和 COMH。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.15 SM115：菊花链同步 2 错误检测

当从所传输数据前几位中提取的时序数据超出预期窗口时，设置同步 2 错误位。可能是未正确地对数据进行采样，或者噪声破坏了所传输数据前几位中的时序信息。同步 2 位的设置取决于接口 COML 和 COMH。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.16 SM116：菊花链位错误检测

当从由 VIF 传输的数据中提取的电压电平没有足够的样本来检测可靠的逻辑电平时，或者如果某个位由于噪声而损坏，则要设置位错误位。位错误位的设置取决于接口 COML 和 COMH。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.17 SM117：菊花链字节错误检测

当 VIF 通信数据缺少某个位或具有不正确的补充菊花链信号，在无法检测到有效的数据字节通信帧之时，设置 PERR 菊花链字节错误位。PERR 错误位的设置取决于接口 COML 和 COMH。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.18 SM118：菊花链故障信号诊断

主机 MCU 向 BQ79600 发送一条 UART/SPI 命令以发送损坏的 CRC 值，从而设置寄存器 DIAG_CTRL 中的 FLIP_TR_CRC 位。在发送不正确的 CRC 之前和之后，主机应启用并监测 nFAULT 引脚信号。然后主机应将 CRC 故障复位。

[AoU2] - 主机 MCU 在每个 MPDTI 期间执行诊断。

5.3.19 SM119：NFAULT 引脚诊断

主机 MCU 向基底器件发送一条 UART/SPI 命令，该命令的初始字节不正确或具有其他命令错误。主机应启用并监测 nFAULT 引脚信号。然后主机应将故障复位。

[AoU14] - 主机 MCU 在每个 FDTI 期间执行诊断。

5.3.20 SM120：睡眠模式故障音调

在睡眠模式下，如果在堆栈中检测到未屏蔽的故障，堆栈器件会发出故障音调。BQ79600 应设置寄存器 FAULT_COM1 中的 FTONE_DET 位，并且 nFAULT 引脚应被置位。

[AoU15] - 当应用在睡眠模式下包含用于安全相关功能的环网通信选项时，主机 MCU 在睡眠模式之前启用睡眠模式故障音调，然后在堆栈中的器件睡眠时监测 nFAULT 引脚。

5.3.21 SM121：睡眠模式心跳

在睡眠模式下，建立环网通信后，如果未定期检测到心跳音调，则设置寄存器 FAULT_COMM1 中的 HB_FAIL 位，并且 nFAULT 引脚被置位。

[AoU16] - 当应用在睡眠模式下包含用于安全相关功能的环网通信选项时，主机 MCU 在睡眠模式之前启用心跳音调，然后在堆栈中的器件睡眠时监测 nFAULT 引脚。

5.3.22 SM122 快速心跳检测

在睡眠模式下，建立环网通信后，如果检测到心跳音调的频率高于预期值，则设置寄存器 FAULT_COMM1 中的 HB_FAST 位，并且 nFAULT 引脚被置位。该错误表明心跳环网通信的配置出现了问题或者噪声对心跳音调产生干扰。

[AoU17] - 当应用在睡眠模式下包含用于安全相关功能的环网通信选项时，主机 MCU 在睡眠模式之前启用心跳音调，然后在堆栈中的器件睡眠时监测 nFAULT 引脚。

5.3.23 SM123：菊花链 CRC 诊断

BQ79600 具有诊断功能，可在 VIF 菊花链通信传输响应中特意创建不正确的 CRC 值。设置寄存器 DIAG_CTRL 中的 FLIP_TR_CRC 位后，通过反转所有计算得出的 CRC 位来创建不正确的 CRC 值。

[AoU2] - 主机 MCU 在每个 MPDTI 期间执行诊断。

5.3.24 SM124：MCU 通信和故障屏蔽诊断

对客户控制寄存器（地址 0x306 - 0x2030）进行写入操作后，主机 MCU 应向 BQ79600 发送一个命令序列以读回寄存器位设置并验证该设置是否正确。然后主机 MCU 应在多点故障响应时间内定期发送一个命令序列来读回寄存器位设置并验证该设置是否正确。

[AoU18] - 当主机 MCU 更新用于客户控制功能的寄存器内容时，主机 MCU 应读回写入的值以验证寄存器值。主机 MCU 应定期读回寄存器值设置。

[AoU19] - 当应用具有睡眠模式期间的电池平衡或保护功能时，主机 MCU 应在进入睡眠模式之前读回控制寄存器值以验证寄存器值是否正确。

5.3.25 SM125：MCU 器件地址诊断

主机 MCU 应在多点故障响应时间内在 ASIC 处于活动模式时定期发送一个堆栈读取命令序列，以验证响应对于通信配置是否正确，以及 ASIC 编号、器件地址和顺序是否正确。

[AoU2] - 主机 MCU 在每个 MPDTI 期间执行诊断。

5.3.26 SM126：MCU UART 通信故障诊断

如果主机通过 UART 与 ASIC 进行通信，则 MCU 应在多点故障响应时间内定期发送单独的 UART 帧，其中包含：

(1) 不正确的 CRC

(2) 无效的初始字节

(3) 命令之间的无效等待时间

然后 MCU 应验证匹配的错误标志寄存器结果和 nFAULT 引脚状态，清除故障并执行下一个诊断。

[AoU2] - 主机 MCU 在每个 MPDTI 期间执行诊断。

5.3.27 SM127：FMT 错误检测

在 SPI 通信模式下，ASIC 在非读取模式下通过检查 nCS 下降沿之后的第一个数据字节来监视接收命令，并在接收到格式错误的命令时设置寄存器 FAULT_COMM2 中的 SPI_PHY 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.28 SM128：SPI 通信清除检测

在 SPI 通信模式下，ASIC 监测其在通信清除期间接收到的 SCLK 脉冲数，如果其接收的 SCLK 脉冲超过 8 个，则设置寄存器 FAULT_COMM2 中的 SPI_PHY 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.29 SM129：TX 数据异常检测

在 SPI 通信模式下，如果 ASIC 在 COMMCLR 之后从其自身或从堆栈器件接收到异常数据，或者在菊花链超时后从菊花链接收到异常数据，则 ASIC 设置寄存器 FAULT_COMM2 中的 SPI_PHY 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.30 SM130：RX 数据异常检测

在 SPI 通信模式下，如果 MCU 在器件读取模式期间发送除 0xFF 以外的数据或在 SPI_RDY = 0 时启动 SPI 通信，ASIC 设置寄存器 FAULT_COMM2 中的 SPI_PHY 位（例如当 FIFO2 被填满时，主机在 FIFO1 被读出后继续读取 FIFO2。此时，SPI_RDY 为低电平）。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.31 SM131：正确的通信接口诊断

主机应在多点故障响应时间内定期监测通信以验证是否选择了正确的通信协议。

5.3.32 SM132：FIFO 寄存器诊断

BQ79600 包含一种测试模式，可帮助检测 FIFO 寄存器的潜在故障。MCU 应在多点故障响应时间内定期进入 FIFO 诊断测试模式并将 32 个字节写入 RX 缓冲区。ASIC 将针对第一个副本按原样复制 RXFIFO，然后针对后续的每个副本将数据循环左移 1 位。

然后，MCU 应等待 SPI_RDY = 1 以完成事件，然后读取 TX FIFO 以验证数据是否符合预期。然后 MCU 应发送 COMMCLR 以退出 FIFO 诊断测试模式。

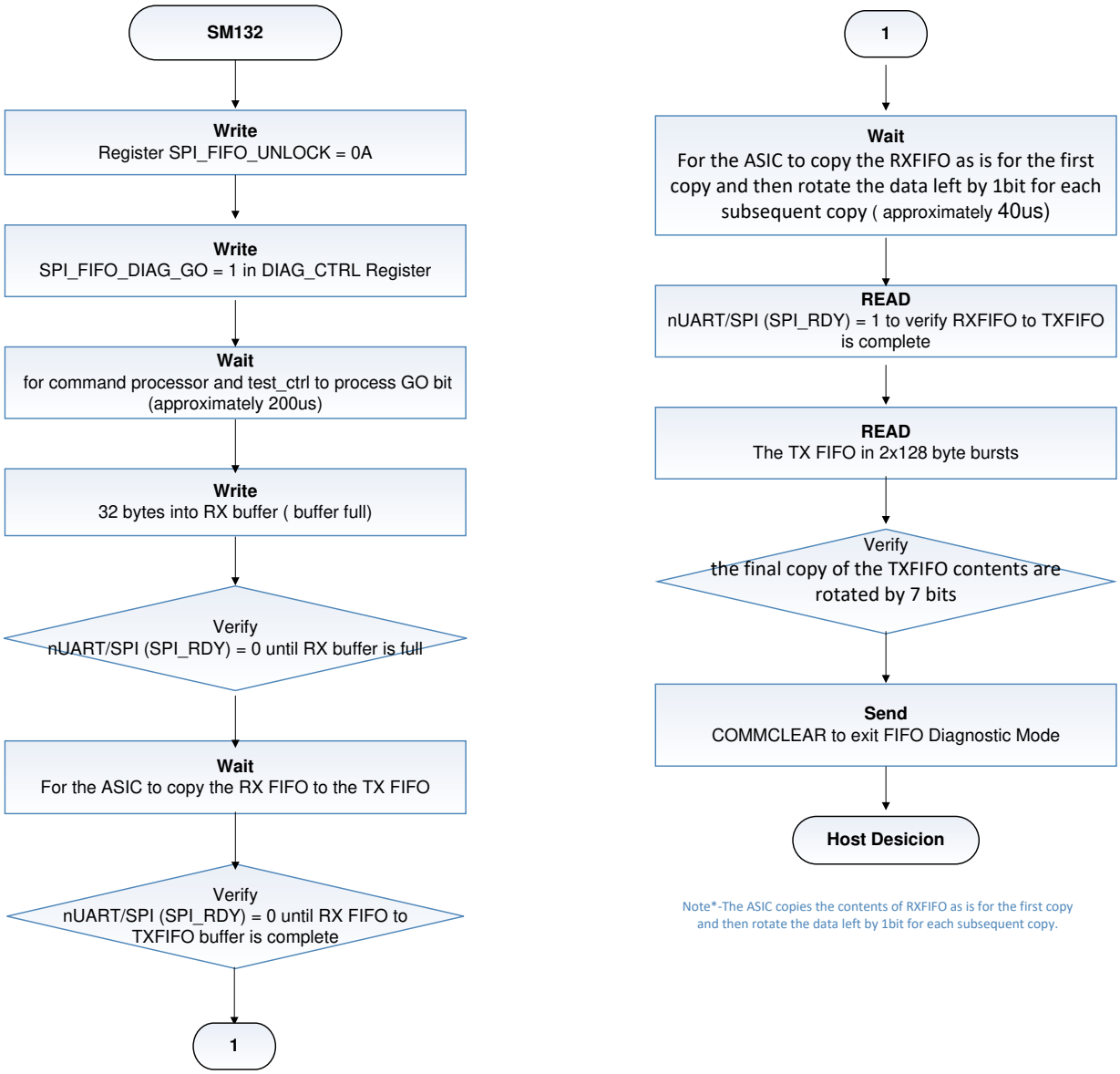

图 5-2. SM132：FIFO 寄存器诊断流程图

备注

RX FIFO 为 32 个字节，TX FIFO 为 256 个字节。ASIC 针对第一个副本按原样复制 RX FIFO 的内容，然后针对后续的每个副本将数据循环左移 1 位，因此 RXFIFO 内容的最终副本将循环移动 7 位。主机可以使用 0x00 (COMM_CLEAR) 以外的任何值来填充模式，并且可以根据需要连续运行 2 次测试。

[AOU2] - 主机 MCU 在每个 MPFDI 期间执行诊断。

[AoU20] - MCU 应将解锁代码 (0x0A) 写入 SPI_FIFO_UNLOCK，然后设置 SPI_FIFO_DIAG_GO = 1 以启动 FIFO 诊断。

[AoU21] - MCU 应在 2 个脉冲下读取 TX FIFO，每次读取 128 个字节（一共 256 个字节）。

[AoU22] - 主机不应使用 0x00 来填充 RX FIFO，否则 ASIC 会将其视为 COMM_CLEAR。

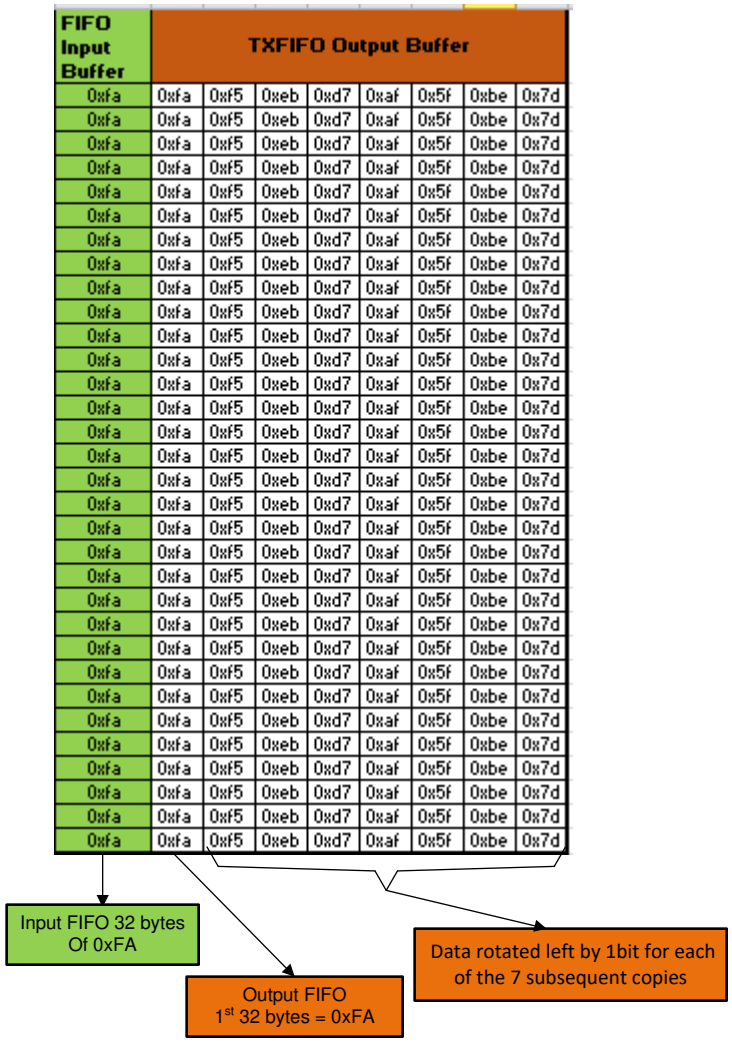

图 5-3. SM132：FIFO 诊断测试模式的示例模式

5.3.33 SM133：TX FIFO 下溢检测

ASIC 在 SPI 通信期间检测 TX FIFO 的下溢。

在读取模式期间，当两个 TX FIFO 都为空时，如果 MCU 继续发送时钟以传输更多数据，ASIC 会设置寄存器 FAULT_COMM2 中的 SPI_PHY 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.34 SM134：TX FIFO 上溢检测

ASIC 在 SPI 通信期间检测 TX FIFO 的下溢。

如果堆栈器件在当前 TX FIFO 已满且另一个 TX FIFO 不为空（MCU 未完成第 2 个 TX FIFO 读取）时发送数据，则 ASIC 设置寄存器 FAULT_COMM2 中的 SPI_PHY 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.35 SM135：RX FIFO 上溢检测

ASIC 在 SPI 通信期间检测 RX FIFO 的上溢。

如果 ASIC 接收到的数据多于其在 RX FIFO 中的可容纳量，则 ASIC 设置寄存器 FAULT_COMM2 中的 SPI_PHY 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.3.36 SM136：MCU SPI 故障诊断

如果主机通过 SPI 与 ASIC 进行通信，则 MCU 应在多点故障响应时间内定期发送单独的 SPI 帧，以测试以下情况：

(1) FMT

(2) TX FIFO 下溢

(3) TX FIFO 上溢

(4) RX FIFO 上溢

然后 MCU 应验证匹配的错误标志寄存器结果和 nFAULT 引脚状态，清除故障并执行下一个诊断。

[AoU2] - 主机 MCU 在每个 MPFDI 期间执行诊断。

5.3.37 SM137：SPI 冲突检测

ASIC 在 SPI 通信期间检测 SPI 冲突。

在读取模式期间，如果 MCU 正在发送命令帧，则 ASIC 设置寄存器 FAULT_COMM2 中的 SPI_PHY 位。

[AoU9] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_COMM 位是否为 0。

5.4 与不属于其他类别的器件功能相关的架构安全机制

5.4.1 SM200：Snif Detector 诊断

为了验证 Snif Detector 的功能，MCU 应定期运行以下诊断测试并监测寄存器 FAULT_SYS 中的 VALIDATE_DET 位。

主机发送一条命令以在堆栈器件顶部设置 CRC 故障。然后堆栈器件的顶部从 COMH 发送故障音调。然后 MCU 将 bq79600 置于关断模式，并在 100ms 之后或检测到 NFAULT 引脚切换为低电平之后（在进入验证模式并且验证了故障音调之后，MCU 就会设置故障），MCU 向 bq79600 发送唤醒 ping。

然后主机验证 VALIDATE_DET 位是否为“1”，以确认 SNIF DET 是否在工作。

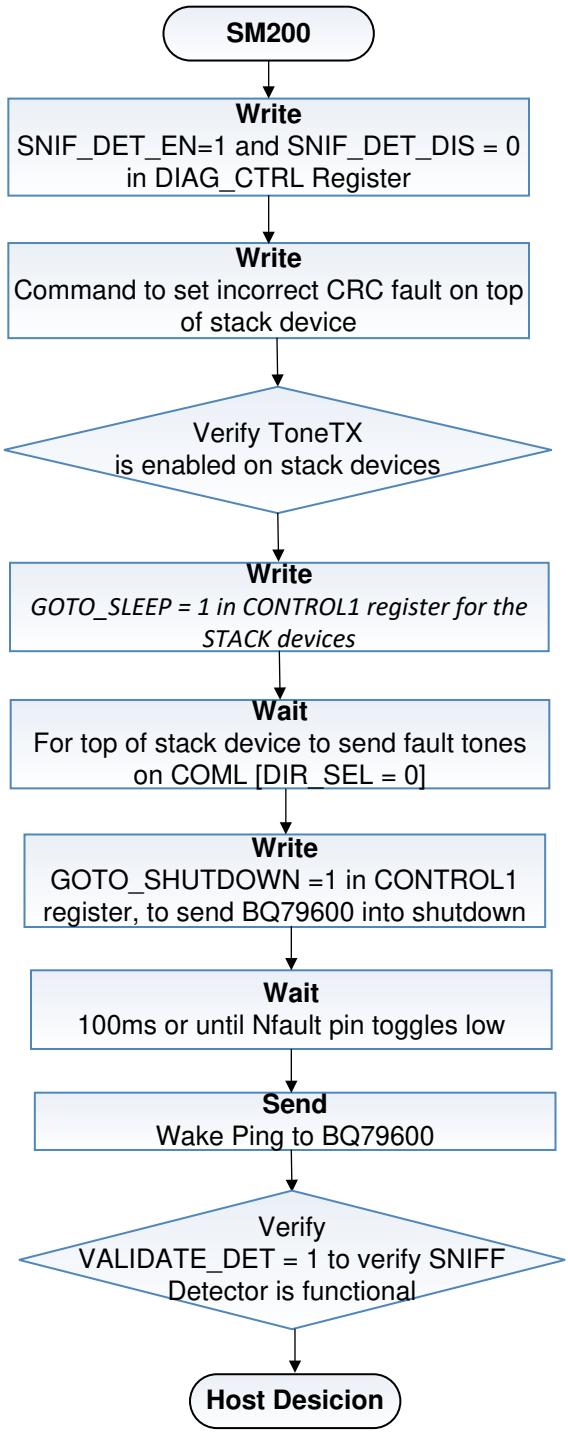

图 5-4. SM200：Snif Detector 诊断流程图

[AoU22] - 仅当在系统中使用了 Snif Detector 功能时，主机才需要运行该诊断。

[AoU23] - Snif Detector 仅在关断模式下有效。若要启用该功能，主机 MCU 需要将 SNIFDET_EN 位设置为 1 并将 SNIFDET_DIS 位设置为 0，然后才能转换为关断模式。

5.4.2 SM201：INH 引脚状态检测

当 INH PMOS 被激活时，ASIC 监测 INH 引脚状态并设置寄存器 FAULT_SYS 中的 INH 位。

5.4.3 SM202：INH 驱动程序诊断

为了检测 INH 驱动程序的潜在故障，MCU 应运行 INH 驱动程序诊断测试。

主机应向寄存器 DIAG_CTRL 中的 INH_SET_GO 位写入 1，然后监测 INH_STAT 位的状态以验证 INH 驱动程序是否在运行。

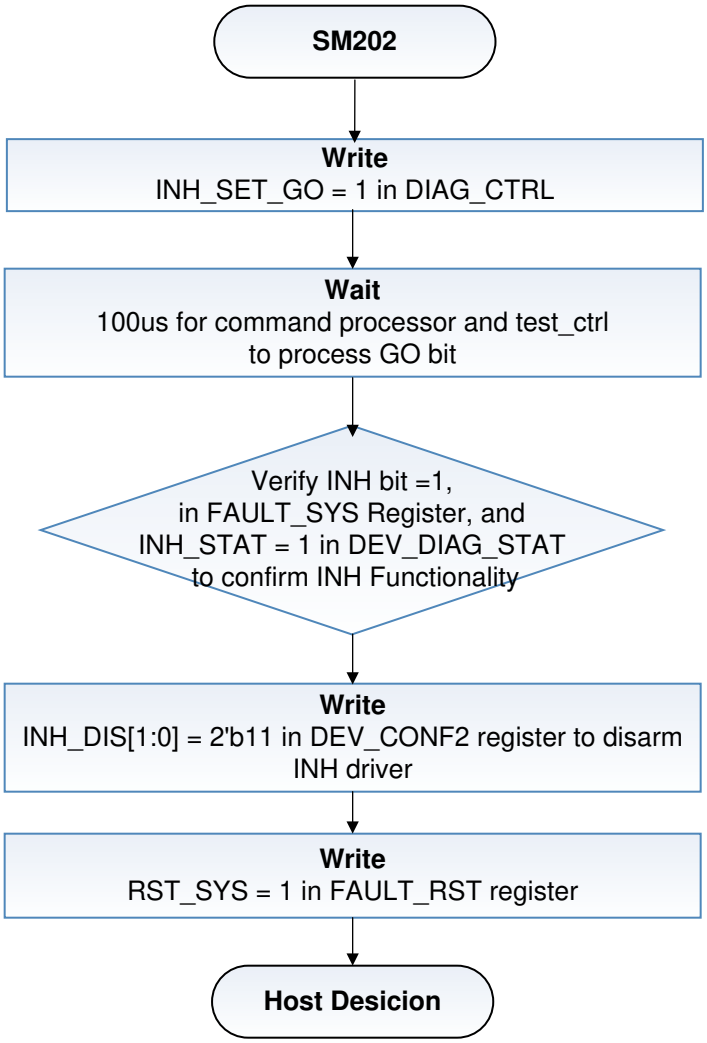

图 5-5. SM202：INH 驱动程序诊断流程图

[AoU24] - 主机 MCU 可以通过设置 INH_DIS[1:0] = 2'b00 来启用 INH 功能，并通过配置位 INH_DIS[1:0] = 2'b11 来禁用 INH 功能。

[AoU25] - 若要清除故障，主机 MCU 需要设置位 INH_DIS[1:0] = 2'b11（解除 INH 驱动器），然后向 RST_SYS 位写入 1。在此之后，若要使用 INH 功能，应设置 INH_DIS[1:0] = 2'b00。

[AoU26] - 如果使用 INH 驱动程序，则在睡眠模式下不应屏蔽通信故障 (hb)、电源故障 (CVDD OVUV)、寄存器故障（位翻转）。

5.4.4 SM203 LFOSC 时钟缺失检测

启用 LFO 后，低频振荡器由一个独立的 LFO 看门狗进行监视，以获知时钟活动情况。如果 LFO 在分配的时间内没有从高电平变为低电平或从低电平变为高电平，则看门狗将使数字内核复位并将数字内核保持在复位状态，直到 LFO 看门狗信号复位。只要 HFO 时钟从高电平变为低电平或从低电平变为高电平，看门狗计时器就会复位并启动新的计时器周期。

备注

LFO 看门狗机制连续工作。当数字内核处于复位状态时，通信和电压监测将停止。

[AoU27] - 主机 MCU 验证在分配的时间内是否接收到预期的通信响应。

5.4.5 SM204：HFOSC 时钟缺失检测

启用 HFO 后，高频振荡器由一个独立的 HFO 看门狗进行监视，以获知时钟活动情况。如果 HFO 在分配的时间内没有从高电平变为低电平或从低电平变为高电平，则看门狗将使数字内核复位并将数字内核保持在复位状态，直到 HFO 看门狗信号复位。只要 HFO 时钟从高电平变为低电平或从低电平变为高电平，看门狗计时器就会复位并启动新的计时器周期。

备注

HFO 看门狗机制连续工作。当数字内核处于复位状态时，通信和电压监测将停止。

[AoU27] - 主机 MCU 验证在分配的时间内是否接收到预期的通信响应。

5.4.6 SM205：LFOSC 频率不匹配检测

BQ79600 使用计数器将 LF 振荡器频率与 HF 振荡器频率进行比较。如果频率差异超出指定的范围，则设置寄存器 FAULT_SYS 中的 LFO 位。

备注

虽然该检测表明两个振荡器之间的频率差异相对于彼此超出规范，但该检测无法确定哪个振荡器发生了漂移。HFO 频率漂移会导致 UART 通信中断。

[AoU10] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_SYS 位是否为 0。

5.4.7 SM206 出厂寄存器 CRC 检测

出厂 NVM 寄存器中的值由 CRC 在后台循环检查。出厂 NVM CRC 逻辑根据出厂寄存器内容计算校验和值，并将其与存储在寄存器中的 CRC 校验和值进行比较。如果存储的 CRC 值和计算出的值不匹配，则设置 FAULT_OTP 寄存器中的 FACT_CRC 位。

备注

如果设置了 FACT_CRC 位，则可以通过器件复位从存储的 NVM 存储器中重新加载出厂 NVM 寄存器值。复位后，FACT_CRC 位应复位，指示瞬态故障已复位。

[AoU28] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_REG 位是否为 0。

5.4.8 SM207：出厂 CRC 诊断

可以专门将一个故障注入出厂 NVM 寄存器 CRC 检查，以诊断 CRC 结果比较和 FACT_CRC 故障位的运行情况。寄存器 DIAG_CTRL 中的 FLIP_FACT_CRC 位控制诊断功能。设置 FLIP_FACT_CRC 后，出厂 CRC 状态位诊断应无法设置 FAULT_REG 寄存器中的 FACT_CRC 位。

[AoU2] - 主机 MCU 在每个 MPFDI 期间执行诊断。

5.4.9 SM208：客户寄存器完整性检测

为了检测客户寄存器中的位翻转，ASIC 会监测寄存器 DEV_CONF1、DEV_CONF2 和 FAULT_MSK。

主机 MCU 应在启动时向 CONF_MON_GO 位写入 1。然后，BQ79600 获取寄存器 DEV_CONF1、DEV_CONF2 和 FAULT_MSK 的快照，并不断将寄存器值与快照值进行比较以检测位翻转。如果 ASIC 检测到位翻转，则设置寄存器 FAULT_REG 中的 CONF_MON_ERR 位。

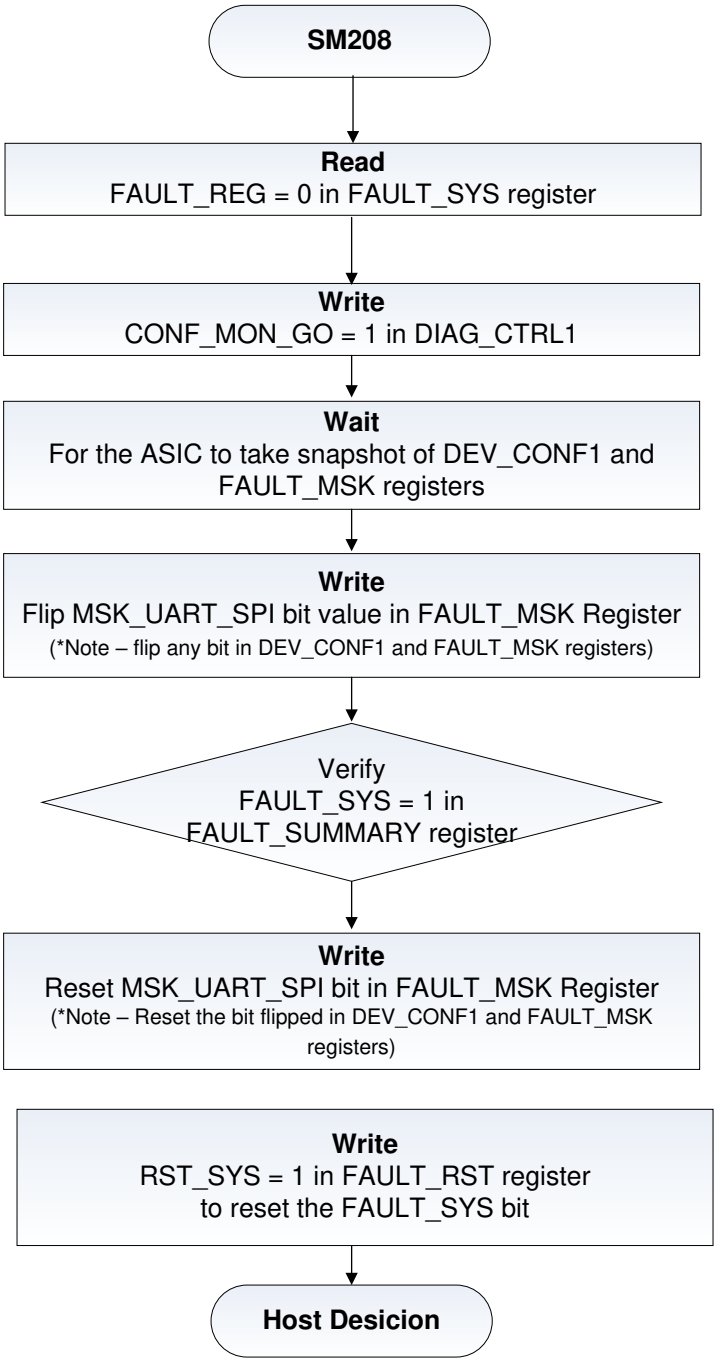

图 5-6. SM208：客户寄存器完整性检测流程图

[AoU28] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_REG 位是否为 0。

[AoU29] - 当主机 MCU 更改 DEV_CONF1、DEV_CONF2 和 FAULT_MSK 寄存器设置或任何寄存器位翻转时，设置故障位 [CONF_MON_ERR]。主机 MCU 更改设置后，需要向 [CONF_MON_GO] 写入 1（重新采样 3 个寄存器值），向 [RST_REG] 写入 1 以清除 [CONF_MON_ERR] 故障。

[AoU30] - 器件复位（接收唤醒 ping 或 SOFT_RESET = 1）后，CONF_MON_ERR] 位 = 0。

5.4.10 SM209：客户寄存器完整性诊断

主机 MCU 应定期将客户寄存器值与其预期的客户寄存器值进行比较，以验证客户寄存器的数据完整性。

[AoU2] - 主机 MCU 在每个 MPFDI 期间执行诊断。

5.4.11 SM210：OTP 出厂负载错误

OTP 出厂负载错误表示将出厂 OTP 复制到寄存器的过程中出现错误。在将出厂 OTP 数据传输到寄存器时，该错误检测自动发生。如果检测到错误，则设置寄存器 FAULT_REG 中的 FACTLDERR 位。

[AoU28] - 主机 MCU 在每个 FDTI 期间读取 FAULT_SUMMARY 寄存器以验证 FAULT_REG 位是否为 0。

5.4.12 SM211：热关断检测

当热关断传感器值大于热关断温度阈值时，器件会自动进入关断模式。发生热关断事件时不会发出故障信号。唤醒后发生热关断事件后，设置寄存器 FAULT_SYS 中的 TSHUT 位，指示热关断导致器件进入关断模式。

[AoU31] - 器件从关断模式转换到活动模式后，主机 MCU 验证 TSHUT 位设置是否为“0”。

[AoU27] - 主机 MCU 验证在分配的时间内是否接收到预期的通信响应。

5.4.13 SM212：关断状态

寄存器 FAULT_SYS 中的 SHUTDOWN_REC 位设置为 1，指示先前的关断是关断 ping 或 TSHUT 引起的，这并非通常的关断方法。

[AoU31] - 器件从关断模式转换到活动模式后，主机 MCU 验证 SHUTDOWN_REC 位设置是否为“0”。

5.4.14 SM213：出厂测试模式检测

在正常工作期间，应始终禁用出厂测试模式。测试模式状态由寄存器地址 0x2601 中的非零值指示。该寄存器中的值 0x00 表示器件处于正常工作模式。

[AoU32] - 主机 MCU 在每个 FDTI 期间执行诊断。

6 BQ79600 作为独立安全元素 (SEooC)

本节包含 BQ79600 的独立安全元素 (SEooC) 原理图。德州仪器 (TI) 已对使用该器件的典型安全系统配置进行了假设。进行系统级安全分析是这些系统的开发人员的责任，而非德州仪器 (TI) 的责任。因此，本节旨在提供相关的信息，说明如何使用 BQ79600 的功能来帮助系统设计人员实现给定的 ASIL 级别。客户负责将该器件置于其系统环境中并分析其中实现的 ASIL 覆盖范围。BQ79600 被设计为按照本安全手册中所述的方式工作/运行，前提是该器件已集成到使用 BQ79600 并按照所述的方式将其与其他器件和元件互连的系统中。请注意，系统设计人员可以选择在其他与安全相关的系统中使用该 BQ79600。

6.1 BQ79600 - 典型应用电路

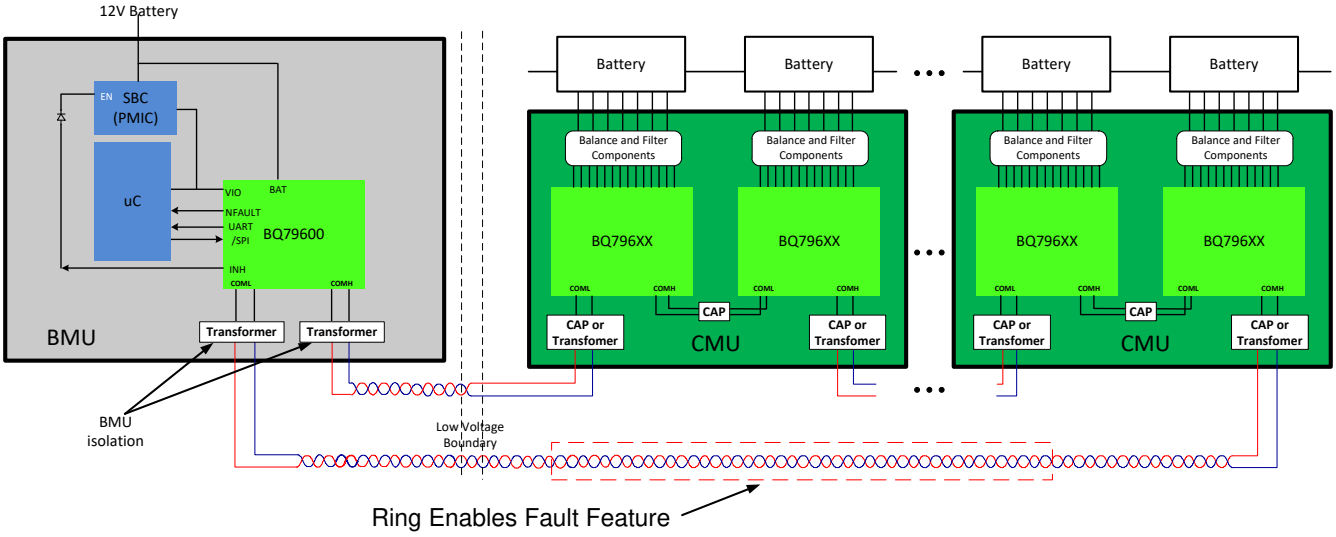

图 6-1. 典型应用电路

7 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision * (June 2020) to Revision A (January 2021)	Page
• 将 SM017 诊断间隔从 FDTI 更改为 MPFDI 并将诊断/检测从检测更改为诊断	10
• 删除了 SM111	10
• 将 SM135 从 MCU SPI 故障检测更改为 RX FIFO 上溢检测	10
• 将 SM136 从 SPI 冲突更改为 MCU SPI 故障诊断，将诊断间隔从 FDTI 更改为 MPFDI 并将诊断/检测从检测更改为诊断	10
• 添加了 SM137	10
• 删除了 SM111 部分	16
• 在 SM125 说明中将广播更改为堆栈	17
• 在 SM213 说明中将 0xE00 更改为 0x2601	27

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