电池管理模拟前端芯片

BF8915 系列功能安全手册

V1.0

BF8915A

BF8915A-1

2021 年 11 月 11 日

目录

重要声明.....1
版本历史.....3
1. 前言.....4
1.1. 概述.....4
1.2. 假设性说明.....4
1.3. 安全手册指南.....4
1.4. 功能安全标准.....5
1.5. 相关文档.....5
1.6. 其他考虑.....5
2. 产品介绍.....6
3. 应用场景假设.....7
3.1. 假设功能安全.....8
3.1.1. 假设技术安全需求.....8
3.1.2. 假设安全用例.....8
4. BF8915A 安全机制.....10
5. 流程支持.....22
5.1. 设计开发流程.....22
6. 系统诊断指南.....24
6.1. 硬件诊断.....24
6.2. 关于软错误.....25
6.3. 其它支持.....26
6.4. 验证评审流程.....27
6.5. 支持服务流程.....27
7. AECQ100 认证.....28
8. 定量分析结果.....29

重要声明

比亚迪半导体功能安全文档仅用于帮助正在开发使用比亚迪芯片的系统的工程师。工程师需要理解并认可的同时，仍有责任在设计系统和产品时进行独立的分析、评估和判断。安全文档运用标准实验室条件和工程实践经验而创建。比亚迪半导体没有进行任何测试，除了在特定安全文档中公开文件中特别进行描述。比亚迪半导体可能会对安全文档进行更正、优化和其他更改。

由于安全文档部分是基于 SEooC 编写的，因此工程师有权将安全文档与每个特定参考设计中确定的零部件一起使用，并在开发最终产品时修改安全文档。但是，上述内容不授予任何其他比亚迪半导体相关知识产权的明示或默认许可，包括但不限于任何专利权、版权、作品权，也不授予任何第三方技术或知识产权的许可，或与使用比亚迪半导体组件或服务的任何组合、设备或过程有关的其他知识产权。

比亚迪半导体对安全文档或其使用不作任何明示、暗示或法定的保证或陈述，包括准确性或完整性。同时，比亚迪半导体拒绝对安全文档或其使用的适销性、特定用途的适用性、默许或不侵犯任何第三方知识产权作出任何所有权保证和任何默认保证。基于比亚迪半导体安全文档中提供信息，比亚迪半导体不对任何第三方侵权索赔进行负责，也不对产品买方进行辩护或赔偿。对于一些是由比亚迪半导体安全文档或买方使用比亚迪安全文档引起的损害，在任何情况下，比亚迪半导体均不对任何实际的、特殊的、偶然的、后果性的或间接性的损害承担责任，无论这些损害是由任何责任理论引起的，也无论比亚迪半导体是否已被告知此类具有损害的可能性。

比亚迪半导体有权对其半导体产品和服务进行修正、升版、改进和其他更改，停止产品或服务。工程师应在下订单前获得最新相关信息，并应核实信息的完整性和及时性。所有产品均按照比亚迪半导体在订单确认时提供的销售条款和条件进行销售。比亚迪半导体保证其提供产品的性能符合规范和产品销售条款和条件中的保证条款。比亚迪半导体产品的测试和其他质量控制技术在比亚迪半导体认为支持本保修所必需的范围内使用。除非适用法律另有规定，否则不必对每个产品的所有参数进行测试。工程师使用比亚迪半导体产品进行产品和应用开发时，为尽量减少与工程师设计的产品和应用相关的风险，工程师应提供充分的设计和操作保障。

只有在复制时不作更改，并附有所有相关保证、条件、限制和通知时，才允许复制比亚迪

半导体产品的规格书、数据表、参考手册或安全文档中的重要部分。比亚迪半导体不对此类行为的产生的文件负责。第三方的信息可能受到其他限制。

工程师应承认并同意其全权负责的工作遵守与其产品有关的所有法律、法规和安全相关要求。尽管比亚迪半导体可能提供任何与应用相关的信息或支持，但在其应用中使用比亚迪半导体的产品时，工程师需表示并同意其拥有所有必要的专业知识，以建立和执行预防危险故障、监测故障及其后果、降低危险故障的可能性和采取适当的补救措施的保障措施行动。

在某些情况下，比亚迪半导体产品可能会被专门推广，以促进安全相关的应用。比亚迪半导体目标目标是帮助客户设计和创建自己的最终产品解决方案，以满足适用的功能安全标准和要求。除非双方授权官员签署专门管理此类使用的协议，否则比亚迪半导体产品不得用于类似的生命关键型医疗设备、军工设备、航天航空等应用或环境。任何军事或航空用途完全由使用方承担风险。

比亚迪半导体特别指定某些部件符合 ISO/IATF16949 要求，主要用于汽车领域。使用非指定产品，比亚迪半导体不对任何不符合 ISO/IATF16949 的情况负责。

版本历史

版本	修改内容	日期
V1.0	初版	2021-11-11

1. 前言

1.1. 概述

本文档说明了比亚迪半导体 BF8915A 系列 BMS 电池管理模拟前端芯片在安全相关系统中的集成和使用要求。本文旨在支持安全系统开发人员使用芯片的安全机制来构建安全相关系统，并描述为达到所需的系统级功能安全完整性而应实施的系统级硬件或软件安全措施。BF8915A 系列 BMS 电池管理模拟前端芯片是根据 ISO 26262 标准开发的，具有完整的安全概念。

1.2. 假设性说明

本文对 BF8915A 系列 BMS 电池管理模拟前端芯片在系统级的应用进行了假设。在系统级开发过程中，系统开发者需要在具体的安全系统的背景下，确定 BF8915A 系列 BMS 电池管理模拟前端芯片假设的有效性。为了实现这一点，所有相关的假设都在安全手册中进行说明。

安全相关的系统开发人员在决定这些假设是否适用于他们特定的安全相关系统时需要慎重。在假设无效的情况下，安全系统开发人员应该分析其影响，并发起变更管理。例如，如果一个假设没有实现，那么应该寻找另一种替代实现，并证明这种替代实现在满足有关的功能安全需求同样有效（例如，实现了相同水平的诊断覆盖率，相关故障的可能性也同样低等）。如果替代实现被证明不确定有效，则必须进行由于偏差而导致的故障率度量评估（SPFM:单点故障度量，LFM:潜在故障度量），FMEDA 可以用来帮助进行此分析。

1.3. 安全手册指南

本文档需结合《BF8915A 规格书》，确认安全相关系统中如何配置和使用 BF8915A 系列 BMS 电池管理模拟前端芯片。本文档描述了 BF8915A 系列 BMS 电池管理模拟前端芯片的简要介绍、假设的应用场景和功能安全目标、设计验证与支持的流程以及如何结合 BF8915A 系列 BMS 电池管理模拟前端芯片的功能进行系统诊断。安全系统开发人员在决定这些指南是否适用于他们特定的安全系统时，需要慎重。

1.4. 功能安全标准

假设本文的使用者熟悉《ISO 26262 道路车辆功能安全标准》。BF8915A 系列 BMS 电池管理模拟前端芯片是基于 ISO 26262 的一个组件/元素，在这种情况下，它的开发与相关项或系统的开发能够完全分离开。因此，BF8915A 系列 BMS 电池管理模拟前端芯片的开发被认为是一种独立于环境的安全要素(SEooC)的开发，如 ISO 26262-10.9 章节所述。更多具体描述见 ISO 26262-10 章节。

1.5. 相关文档

BF8915A 系列 BMS 电池管理模拟前端芯片是根据 ISO 26262 开发的，并具有完整的安全概念，此安全概念主要针对要求高安全完整性的安全相关系统。为了将 BF8915A 系列 BMS 电池管理模拟前端芯片更好地集成到安全相关系统中，相关应用手册、规格书以及 FMEDA 文档也可供参考。欲了解更多信息，请联系比亚迪半导体业务人员或访问 https://www.bydmicro.com。

1.6. 其他考虑

BMS 电池管理模拟前端芯片是根据 ISO 26262 开发的，并具有完整的安全概念，此在使用 BF8915A 系列 BMS 电池管理模拟前端芯片开发安全相关系统时，以下方面应考虑:

1. 《BF8915A 规格书》中给出的使用条件；
2. 实时留意 BF8915A 系列 BMS 电池管理模拟前端芯片相关文档已发布的勘误表；
3. BF8915A 系列 BMS 电池管理模拟前端芯片质量协议中给出的推荐生产条件；
4. 安全系统开发者需向 BYD 报告 BF8915A 系列 BMS 电池管理模拟前端芯片所有的现场失效；
5. 与任何技术文档一样，读者有义务确保自己使用的是文档的最新版本。

2. 产品介绍

BF8915A 是一款针对高压电池模块的电压及温度数据的采集监视芯片，具有功能诊断、通信隔离、电量均衡等特性。

芯片内置 16 位增量累加型 ADC 和高精度低温漂电压基准源，室温典型条件下具有低于 ±3mV 的电池测量误差。BF8915A 配置了标准四线 SPI 通信接口和双线差分菊花链通信接口，以实现高速率、高抗干扰的局域数据和指令交换。单颗芯片最多同时测量 16 节串联电池模组，芯片间通过菊花链堆叠应用可实现 16 组 BF8915A 通信，支持多达 256 个电压通道和 128 个温度通道的同时检测。芯片电量均衡支持内部和外部电池电荷均衡控制。芯片具备可编程定时器用于电池电荷均衡，均衡电压阈值可配置，配置后可自主均衡。芯片内部 16 个均衡开关可最大支持 4.2V 下 200mA 的内不均衡电流放电。下图 2.1 为 BF8915A 的主要功能框图。

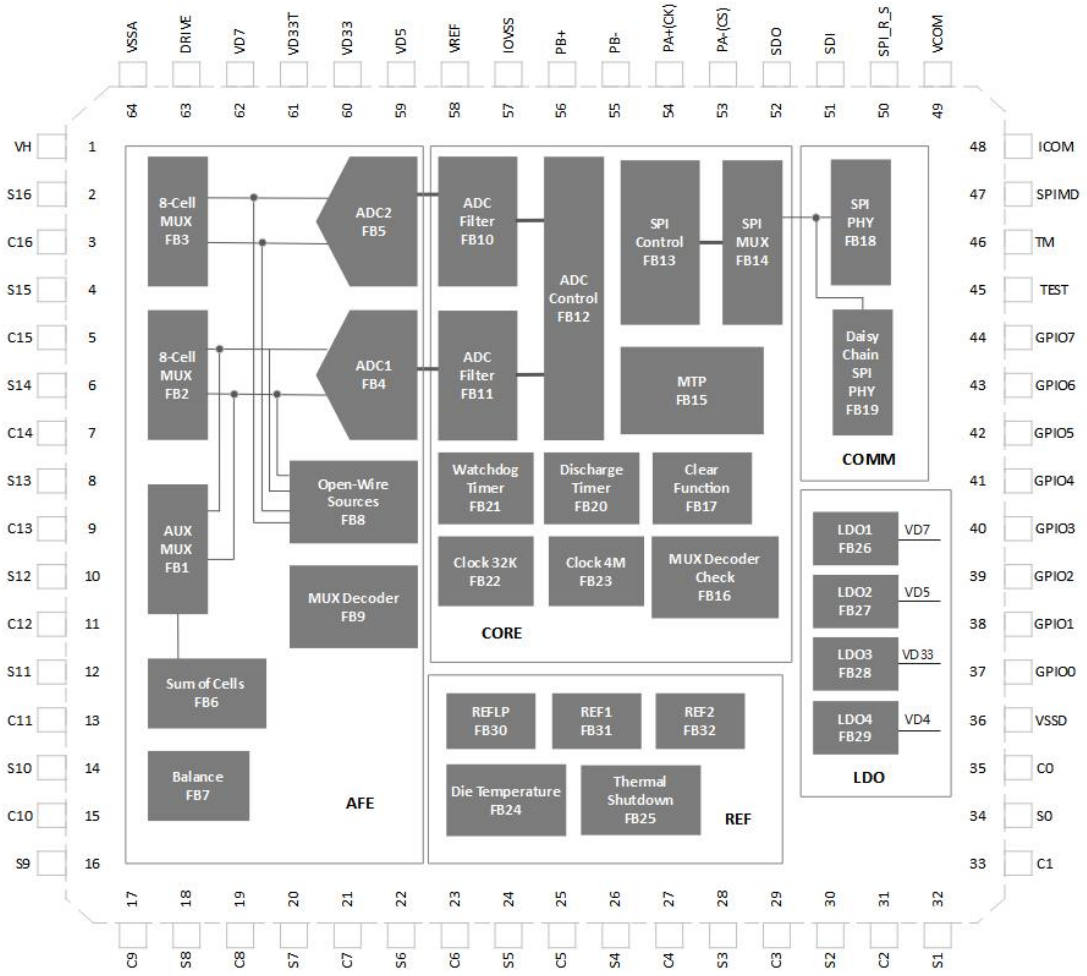

图 2.1　BF8915A 功能框图

3. 应用场景假设

BF8915A 作为车规级产品，该产品是在 ISO 26262 的指导下开发的，是一种脱离上下文的安全元素（SEooC）。SEooC 将假定的项目定义为电力存储系统，由电池组、电池管理、电子和热传感器、执行元件和接触器组成。SEooC 假设 BF8915A 用作传感器设备，它监视电动和混合动力电动汽车中的电池管理单元。下图 3.1 是一个典型应用示意图，BF8915A 由一个单独的微控制器监控的，称为 BMS 控制器。

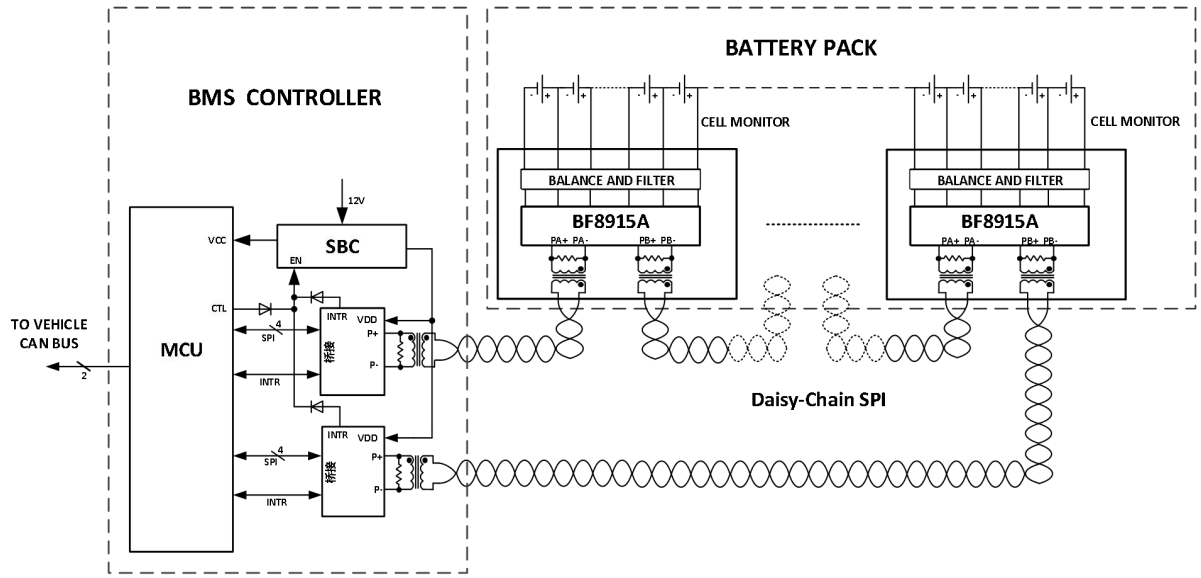

图 3.1 项目应用示意图

BF8915A 作为车规级产品，适用于以下典型应用：

- 电动汽车及混合动力汽车；
- 后备电池系统；
- 电网能量存储；
- 高功率便携式设备；
- 高温（<125˚C）作业环境。

3.1. 功能安全假设

产品 BF8915A 为 BMS 管理芯片，BF8915A 是为符合 ISO26262 标准的系统而设计、开发、生产和测试的，主要功能为监控测量电池参数、执行管理电池主控芯片发出的控制算法和与其他功能性模块单元执行通信任务。此外，BF8915A 还监控其 BMS 功能相关组件的安全性，若系统需要正确操作 BF8915A 从而达到安全目标，则系统的 ASIL 将分配至 BF8915A。

为了使 BF8915A 能够控制电池系统并建立安全状态，车域系统应及时了解电池状态信息。为此，该项目提出了以下两个假设安全目标：

SG1：正确执行电池电压监测，

SG2：正确执行温度监测。

针对上述安全目标，提出了相应的功能安全需求，如表 3.1 所示。

表 3.1 BF8915A 功能安全需求

SG 编号	FSR 编号	描述
SG1	**FSR1**	电池的充电或放电应根据制造商基于电池测量的规格进行调节。
SG2	**FSR2**	电池的充电或放电应根据制造商基于温度测量的规格进行调节。

3.1.1. 技术安全要求的假设

根据上文所述 BF8915A 假设的功能安全要求，为了能正确解决、规避和检测产品功能失效，针对 FSR1、FSR2 提出了对应假设的技术安全需求，分别为：

TSR1：确保电池电压测量根据数据规范正确执行；

TSR2：确保芯片 GPIO 的测量根据数据规范正确执行。

3.1.2. 假设安全用例

假设用例可以被视为在安全使用 BF8915A 的用户在应用时的安全要求。本节中列出的假设用例不包括功能安全以外对设备的操作。

AU01：假设单颗芯片最大测量 16 节串联锂离子电池电压；

AU02：电池通过一个简易 RC 滤波器连接到 C 引脚。假设系统可以容忍任何额外的测量误差；

AU03：电池将通过至少 10Ω的电阻串联放电或外部放电 MOSFET 电路连接到 S 引脚；

AU04：温度测量将使用一个简单的热敏电阻和电阻组合连接到 VD33T 引脚和 GPIO 输入端；

AU05：BF8915A 总是在规格书中规范的表格内的绝对最大值数值内运行；

AU06：放电许可，即 ADCV、ADOL、ADCVGP 等命令代码中的 DISCP，应设置为 0。若使用外部 MOSFET 用于放电，寄生 I*R 压降小于 TSR1 中的电压精度或系统所需精度，则该假设用例可以被忽略；

AU07：所有 DCC 位在电池测量期间都置 0，除非在安全机制的控制中；

AU08：在电池或温度测量之前，应提前配置 REFON 位；

AU09：所列的安全机制应在项目层定义的 FTTI 和 MPFDI 上至少使用一次；

AU10：使用 BF8915A 时，其串联电压的总和不得低于 16V；

AU11：系统假定 FTTI 中的任何一项测量过程中都可能存在由于低概率瞬态故障而损坏，且视为能够容忍此类突发事件。

4. 安全机制

针对上节中所列的技术安全要求，BF8915A 产品制定下列表 4.1 中的安全机制，以应对覆盖和诊断系统功能安全失效，以确保产品符合系统功能安全要求。表 4.1 为结合技术安全需求的安全机制汇总清单。

表 4.1　安全机制汇总

	安全机制编号	安全机制名称	频率
TSR01	SM1	电压测量结果范围检查	FTTI
	SM2	电池重叠检查	FTTI
	SM3	电池采集通路开路检查	FTTI
	SM4	电池电压总和检查	FTTI
	SM5	均衡检查	FTTI
	SM6	确认在电池测量期间，开路电流源未滞留于接通位置	FTTI
TSR01/ TSR02	SM7	内部温度测量	根据系统需求
	SM8	寄存器自测	FTTI
	SM9	清除储存数据结果检查	FTTI
	SM10	内部设备参数检查	FTTI
	SM11	验证寄存器可正常写‘1’和‘0’状态	MPFDI
	SM12	MUX Decoder 检查	FTTI
	SM13	通讯检查	FTTI
	SM14	通信控制器检查	MPFDI
TSR02	SM15	GPIO 相邻引脚短路检查	FTTI
	SM16	GPIO 采集通路开路检查	FTTI
	SM17	冗余热敏电阻电路	FTTI
	SM18	热敏电阻测量结果查看	FTTI
	SM19	确认在 GPIO 测量期间，开路电流源未滞留于 on（接通）或 off（断开）位置	FTTI

以下出现的安全机制用于 2.3 节中所列 2 个技术安全要求：

SM1：检查电池测量结果与有效电池电压范围。

系统根据规格书中规定的阈值内验证电池引脚上的所有 ADC 测量结果。SM1 可检测到以下内部失效：

1. 电池电压寄存器组中的卡滞故障可能导致电池电压超出系统设置的最小和最大边界。
2. V-引脚与 C 或 S 引脚之间短路将导致电池电压低于系统设置的最小值。
3. 由于 ESD 结构故障，一个 C 引脚与其他 C 引脚之间发生短路故障，由此导致电池电压超出系统设置的最小和最大边界。

系统应根据电池类型、硬件配置、用例等设置最小和最大边界的阈值。

SM2：使用 ADOL 命令测量带 ADC1 和 ADC2 的 CELL9。测量结果应在取决于转换模式的公差范围内匹配。

ADOL 指令使用 ADC1 和 ADC2 同时测量 CELL9。主机以比较两个结果，从未诊断是否存在异常。从 ADC2 中检测的 CELL9 的结果放置在电池包电压寄存器组 C 的正常情况下 CELL8 存储的位置。ADC1 的检测结果放置在电池电压寄存器组 C 的正常情况下 CELL9 存储的位置。ADOL 指令测试时序如图 4.1 所示。

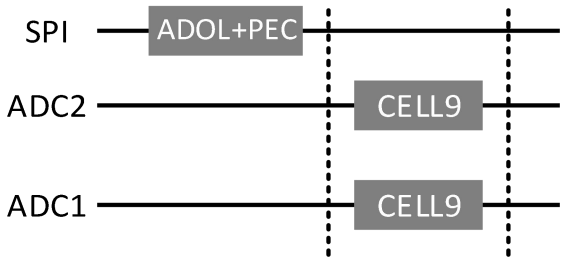

图 4.1　ADOL 指令测试时序

ADC 转换完成后，主机可以读取结果值，使用 CELL9 结果对确认 ADC2 的精度与 ADC1 具有相似的准确性。

由于调制器中存在噪声，2 个 ADC 的测量值应存在可容忍的差异。表 4.2 展示了在 ADC 在 256 采样模式下可允许的最大测量误差。若测量数值误差大于表 4.2 中的数值，视为存在异常。

表 4.2　ADC 最大允许测量差

ADC 采样模式	ADOL 命令下可允许的最大值测量差				
	V_{cell}=0.8V	V_{cell}=2.0V	V_{cell}=3.3V	V_{cell}=4.2V	V_{cell}=5.0V
256	6mV	8mV	9mV	10mV	12mV

SM3：使用 ADCOW 命令，对电池采集通路进行开路检查

ADCOW 命令可用于检查 BF8915A 内部 ADC 输入和外部电池之间的任何 MUX 开关上的开路失效，其简化检测电路如图 4.2 所示。ADCOW 命令对 C 引脚输入执行 ADC 转换，与 ADCV 命令类似，不同的是，在测量两个 C 引脚输入时，导通开路电流源驱动开关。与 ADCV 命令一样，ADCOW 命令指定了一个选项，用于确定要测量的通道数、ADC 模式和过采样率。

主控 MCU 应执行以下算法：

1. 持续执行 ADCOW 至少两次以上，结束后读取 CELL 输入 1~16 引脚的电压数据并将该数据存储在阵列 $CELL_{OW}$ 中；
2. 通过观察、对比测量数据的变化，以判断开路开关电流源中的故障；
3. 若存在某个电池电压测量通道上，执行 ADCOW 命令后读取的电压数值接近 0V，则表示该采集通道存在开路异常。反之，则通道正常。

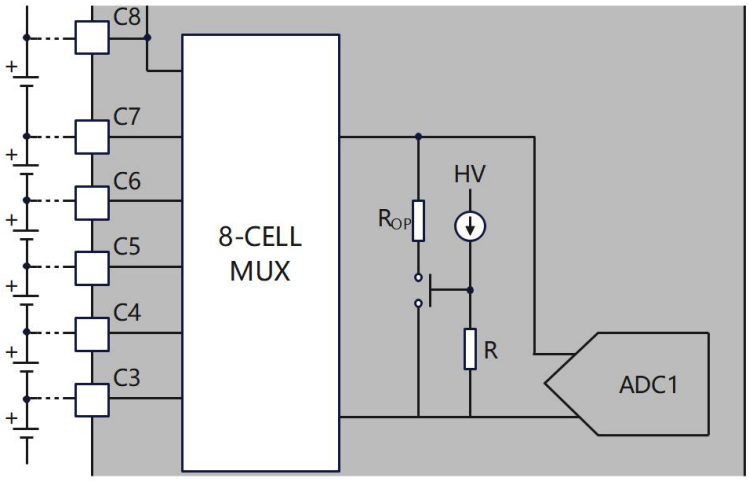

图 4.2　电池电压采样通道开路检测简化电路

SM4：使用 ADCVH 和 ADCV 命令测量电池电压总数。将结果与单个电池测量值进行比较。

ADCVH 命令是一个诊断命令，用于测量总电池电压值。总电池电压（VH）测量值为 C16 和 C0 之间的电压，衰减率为 20：1。VH 测量值是存储在状态寄存器组 A 中的 16 位值。VH 结果表示所有电压电池测量值的总和，由以下公式给出：

总电池电压： VH 电压 =(20*VH*VLSB)μV

为了确认电池电压采集回路的正确运行，可将 VH 值与单个电池测量值的总和进行比较。若整个测量回路运行正确，则这两个数量应在数据表的公差范围内一致，反之亦然。

在环境温度 25˚C 的条件下的单颗电池的总测量误差（TME）和 VH TME 分别处于±0.08%及±0.92%，两次测量之间的差值大于±1%表示 VH 测量路径或单颗电池测量路径故障。随后的电池和 GPIO 采集数值可能存在不准确。

注：测量单颗电池时，所有放电位 DCC 必须设置为 0。

SM5：均衡

BF8915A 有两种均衡方式，分别为自主均衡和指令均衡。使用指令均衡功能时，可以在软件中实现验证放电功能的功能。在使用外部放电 MOSFET 的应用中，可以在电池和放电 MOSFET 之间添加额外的电阻器。这将允许系统检测放电电路中的故障。电路如图 4.3 所示。

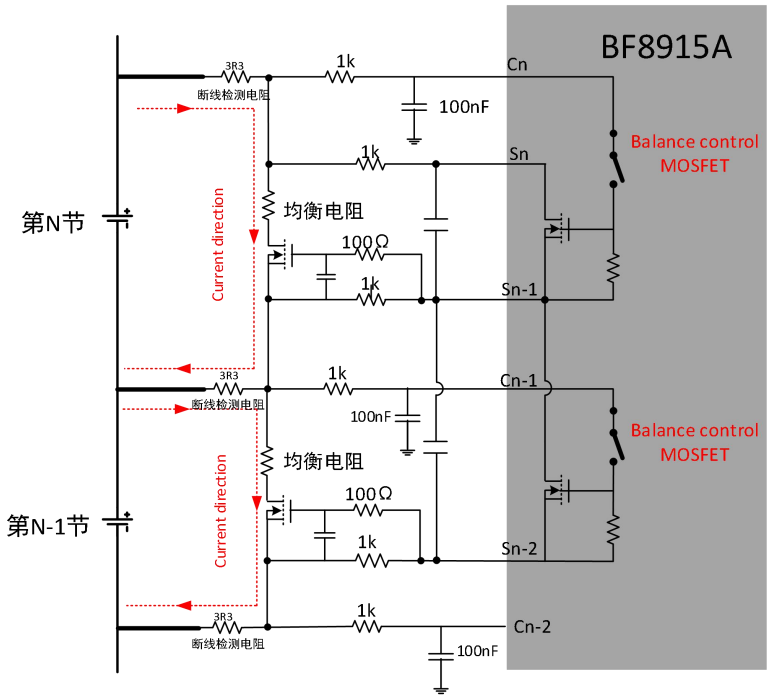

图 4.3 指令均衡电路

放电电路的功能可通过进行电池测量和比较放电关闭时的测量值与放电打开时的测量值来验证。

1. 开始均衡前先对写配置寄存器组 B 的均衡开关 DCC[15:0]，把需要均衡的电池开关打开，相应 DCC 位置 1。
2. 在 STANDBY 模式下使用均衡命令 STRBL 开启均衡，即对命令中的 BL_EN 位置 1。同时，指令 STRBL 通过对其 OESEL 位置位，以对均衡电池奇偶节数的选择，OESEL = 0 选择奇数节进行均衡放电；OESEL = 1 选择偶数节进行均衡放电。奇偶节电池不能同时进行，每次只能是奇数节均衡或者只能是偶数节均衡。
3. 当均衡一段时间，主机可以发送指令停止均衡，可发送 ADCV 电池电压测量指令来检测电池电压，如果放电不满足要求就再次开启均衡。当均衡一段时间，主机也可以不停止均衡，直接发送 ADCV 命令来测量，因为 ADCV 命令中的 DISCP 位有放电允许位。如果电池测量指令中 DISCP = 1，则在电池测量期间 S 引脚放电状态不改变；如果 DISCP = 0，S 引脚的放电状态将关闭，当测量完成后电池可以继续放电。
4. 指令均衡时 WDT 正常计数，如果 WDT 溢出时，放电停止，关闭放电均衡使能。如果芯片温度大于 125℃，关闭均衡开关 DCC，均衡总开关总信号 1 清零，单节电池均衡开关控制信号清零，放电停止，同时需要主机发送带 BL_EN = 0 的 STRBL 均衡指令关闭 BL_EN。

SM6：确认在电池测量期间，开路电流源未滞留于接通位置

为确保电压源未滞留于接通位置，在需要测量的电池回路上发出 ADCOW 命令，并将 ADCOW 结果与 ADCV 结果进行比较。

其算法思路为，在电池 CELL(n)，n 为 1 至 16，上执行 ADCOW 命令。电池 CELL(n)读数将比 ADCV 命令后的数值减少 V_{CN} *R_{OP}/(2*R_{Fiter}+R_{Switch}+R_{OP})，其中，R_{Switch} 为 C 引脚多路复用开关接通电阻，R_{OP} 为 C 引脚开路开关电流源串联电阻，参考图 4.2。

假设 R_{Fiter}=1KΩ ，R_{Switch}=400Ω（标准值），R_{OP}=32KΩ（标准值），主机控制器应执行以下算法，用于检查 C 引脚输入通道中开路电流源开关的闭 CELL(n)状态：

1. 执行 ADCV 命令。结束命令后，读取 CELL(n)，引脚输入的电压数值，并将该数值存储在阵列 $CELL_{CV}$ 中；

2. 执行 ADCOW 命令至少两次。结束命令后，读取 CELL(n)，引脚输入的电压数值，并将该数值存储在阵列 $CELL_{OW}$ 中；
3. 计算在上述步骤中对 CELL 1~16 引脚进行在使用/未使用电流源两种不同情况下的差值 $CELL\Delta(n) = CELL_{CV}(n) – CELL_{OW}(n)$；
4. 对开关导通前的 ADCV 测量电压和导通后的 ADCOW 量结果进行比较，若两者电压差大于 50mv，则表示相关开路电流源开关运行正常；反之，则存在异常。

通过观察、对比数据，以判断开路电流源开关的故障。如果测量数据的处理结果被验证为采集通道存在异常，则不能再依赖 SM3 中描述的开路算法来检查开路。

上述算法除可检测开路电流源开关的闭合状态外，还可用于检测开路、卡断的 MUX 信道和高阻抗大于 4k 的 MUX 信道。该算法要求输入滤波电容（BF8915A 和开路线之间）限制为 10nF 或更小的电容。如果开路 C 引脚输入上有更多的外部电容，则转换需要更多的时间（由于 100μA 内部电流源有限）。为确保产生可测量的电压差，可通过在步骤 1-4 中增加连续 ADCOW 命令的数量。

SM7：使用 ADSTAT 命令测量芯片内部温度。

主机控制器可以使用 ADSTAT 命令作为诊断来监控芯片内部温度。测量值可用于确保满足绝对最高温度额定值。若 VTEMP 对应的温度超过规格书中的最高温度阈值时，将启动过温保护。

SM8：将寄存器自测命令与选项 ST=0b0 和 ST=0b1 一起使用。用于检查 BF8915A 内 ADC 采集数据存储寄存器，且寄存器内容应与规格书中数值匹配。

BF8915A 中有三个自测指令，CVST（电池电压自测试）、GPST（GPIO 输入自测试）、STATST（内部参数自测试），用于测试寄存器状态。

自测试命令诊断数字滤波器和存储器。一位脉冲密度调制器输出由 1Bit 测试信号代替，测试信号通过数字滤波器转换为 16 位 ADC 数据，测试信号和调制器输出的 1 位信号进行相同的数字转换，因此任何自检测命令的转换时间和相应常规的 ADCV 命令完全相同。16 位的 ADC 采集数据存储在和相应常规 ADCV 命令相同的寄存器组中。测试信号被设计成在寄存器中交替写入‘0/1’的模型。

SM9：在任何测量命令之前使用清除命令，这会将使相关寄存器历史数据复位。

BF8915A 有 3 个清除命令，分别为 CLRCELL、CLRGP 和 CLRSTAT。这些命令清除存储所有 ADC 转换结果数据的寄存器。该安全机制旨在转换之前清除寄存器数据，为新的转换数据提供了安全措施。

CLRCELL 命令：清除电池包电压寄存器组 A、B、C、D、E 和 F。这些寄存器所有字节都通过该命令设置为 0xFF。

CLRGP 命令：清除辅助寄存器组寄存器组 A、B、C。这些寄存器所有字节都通过该命令设置为 0xFF。

CLRSTAT 命令：清除状态寄存器组 A、B、C、D。状态寄存器组 A、B、C 所有字节和 D 中的 OV、UV 位由 CLRSTAT 设置为 1 的。

SM10：使用 ADSTAT 命令，以查看内部参数。

ADSTAT 命令是一个诊断命令，用于测量一下内部设备参数：VD33、电池包总电压 VH、VD7、VD5、VD4、芯片内部温度（VTEMP）、VREF_LP 和 VREF2 等。

内部参数通道选择列表如表 4.3 所示。

表 4.3 内部参数通道选择列表

名称	描述	数值描述	
STSEL[3:0]	ADC 转换的内部参数选择	0	所有内部参数 VD33、VH/20、VD7/3、VD5/2、VD4/2、VTEMP、VREF2、VREF_LP
		1	VD33
		2	VH/20
		3	VD7/3
		4	VD5/2
		5	VD4/2
		6	VTEMP
		7	VREF2
		8	VREF_LP

ADSTAT 指令测量所有内部参数时序如图 4.4 所示。

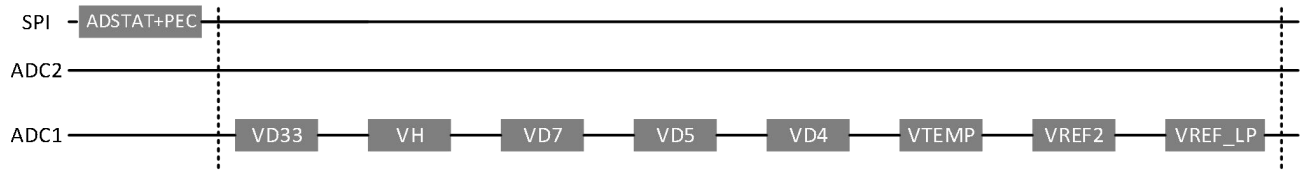

图 4.4　ADSTAT 指令测量所有内部参数时序

ADSTAT 指令测量一个内部参数时序如图 4.5 所示。

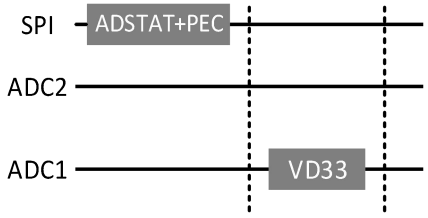

图 4.5　ADSTAT 指令测量一个内部参数时序

表 4.4 为各个内部参数的测量结果。

	最小值	典型值	最大值	单位
VD33	3.27	3.3	3.32	V
VH	16	——	100	V
VD7	6	7	8.5	V
VD5	4.9	5	5.1	V
VD4	3	4	4.7	V
VTEMP	0	3.3	5	V
VREF2	1.1	1.2	1.3	V
VREF_LP	1.1	1.2	1.3	V

表 4.4 内部参数的测量范围

SM11：验证寄存器可正常写‘1’和‘0’状态

验证确认清除命令可以将所有 0 写入 1。每个按键开启周期：执行以下操作以确保清除命令可以写入所有电池电压寄存器、GPIO 寄存器，和状态寄存器位高：

1. 发出 CVST 选项 1 命令，正常模式；发出 GPST 选项 1 命令，正常模式；发出 STATST 选项 1 命令，正常模式。

2. 发出 RDCVA、RDCVB、RDCVC、RDCVD、RDCVE、RDCVF、RDGVA、RDGVB、RDGVC、RDSTATA、RDSTATB、RDSTATC 和 RDSTATD 命令，以验证所有寄存器中的 0x6666 模式。
3. 发出 CLRCELL、CLRGP 和 CLRSTAT 命令。
4. 发出 RDCVA、RDCVB、RDCVC、RDCVD、RDCVE、RDCVF、RDGVA、RDGVB、RDGVC、RDSTATA、RDSTATB、RDSTATC 和 RDSTATD 命令，以验证所有寄存器中的数据位与规格书中的一致。
5. 发出 CVST 选项 2 命令，正常模式； 出 GPST 选项 2 命令，正常模式；发出 STATST 选项 2 命令，正常模式。
6. 发出 RDCVA、RDCVB、RDCVC、RDCVD、RDCVE、RDCVF、RDGVA、RDGVB、RDGVC、RDSTATA、RDSTATB、RDSTATC 和 RDSTATD 命令，以验证所有寄存器中的 0x9999 模式。
7. 发出 CLRCELL、CLRGP 和 CLRSTAT 命令。
8. 发出 RDCVA、RDCVB、RDCVC、RDCVD、RDCVE、RDCVF、RDGVA、RDGVB、RDGVC、RDSTATA、RDSTATB、RDSTATC 和 RDSTATD 命令，以验证所有寄存器中的数据位与规格书中的一致。

SM12：检查 MUX Decoder 的状态。

当发送测量开始测量时，测量开关（Cell/GPIO/Status）时序打开，把输出给模拟的开关时序信号返回数字再进行反译码，如果译码的不一致，则译码检查标志位，即寄存器是状态寄存器组 D 的 MUXFAIL 位会置 1。读 MUXFAIL 位，指令 CLRSTAT 可把这个标志位置 1。所以测量之前如果发送 CLRSTAT 指令，之后要读一下状态寄存器组 D 清零标志位 MUXFAIL，保证测量之前 MUXFAIL=0；

注：当测量完之后读取状态寄存器组 D，判断 MUXFAIL 位是否为 1。

SM13：从 BMS 控制器读取数据，确认通信功能正常。检查从 BF8915A 读取的所有数据的 PEC（数据报文错误代码）。BF8915A 将仅使用正确 CRC 的执行命令时，拥有正确 CRC 的数据才会被写入内存。

数据报文错误码（PEC）是一个 15 位循环冗余校验（CRC）值，该值是按照寄存器组中所位的传递顺序计算的，使用初始 PEC 值为 0000 0000 0010 000，其特征多项式如：$x^{15}+x^{14}+x^{10}+x^{8}+x^{7}+x^{4}+x^{3}+1$.

PEC 可防止有效数据被干扰，并保证安全通信。串行 I/O 端口故障将导致发送错误数据或阻止数据接收。在写入设备的情况下，如果计算出的 PEC 不匹配，则接收到的数据将被丢弃。写入操作后，应从设备读回数据，以确认正确接收了写入操作。如果读回的数据与写入的数据不匹配，则应再次尝试写入。从 BF8915A 读取数据时，如果 MCU 计算的 PEC 与传输的 PEC 不匹配，则数据无效。在这种情况下，应执行额外的读取操作，直到 PEC 匹配为止。上述特征多项式具有 48 位分组数据，汉明距离为 6，意味着 CRC 将检测到 5 位或更少的任何数据损坏。并可以使用测量的误码率来估计未检测到的数据错误的概率。

SM14：发送 CRC 错误的命令或寄存器写 CRC 错误的命令，以验证 BF8915A 是否拒绝这些命令。

系统对 SPI 控制器中的 CRC 引擎进行诊断测试，以确保 SPI 控制器是否存在故障。

SM15：GPIO 相邻引脚短路检查

只有当相邻 GPIO 用作输入或输出时，SM15 才是必需的。任何 GPIO 引脚与热敏电阻和电阻器一起用于温度测量。相邻的 GPIO 常用作输入或输出。如果 GPIO 引脚上的数值超出其有效范围，则可能与相邻 GPIO 短路。要确定是否存在短路，可执行以下操作：

1. 测量 GPIO(n)，n 为 0 至 7，预计在其有效范围内。
2. 对相邻 GPIO 写入低位。GPIO(n-1)和 GPIO(n+1)将被写入低位。如果 GPIO(n-1)或 GPIO(n+1)是数字输入，则系统应将其驱动为低电平，并通过写入配置寄存器将其驱动为低电平。
3. 再次测量 GPIO(n)，将其与之前的结果进行比较。
4. 如果 GPIO(n)结果发生显著变化或接近 0V，则与相邻 GPIO 短路。

SM16：使用 GPOW 命令，对 GPIO 采集通路执行开路检查，已确认 GPIO 输入上是否存在断路。

GPOW 命令用于检查 BF8915A 内部 ADC 输入和 GPIO 之间的开路或任意高阻抗 MUX 开关。GPOW 命令指定了一个选项，用于确定要测量的通道数和 ADC 模式。此外，GPOW 命令的特定位（DOWN）确定当前使用的内部电流源（100μA）为上拉电流源（DOWN=0）或为下拉电流源（DOWN=1）。GPIO 采集通道内部电流源简化示意图如图 4.6 所示。

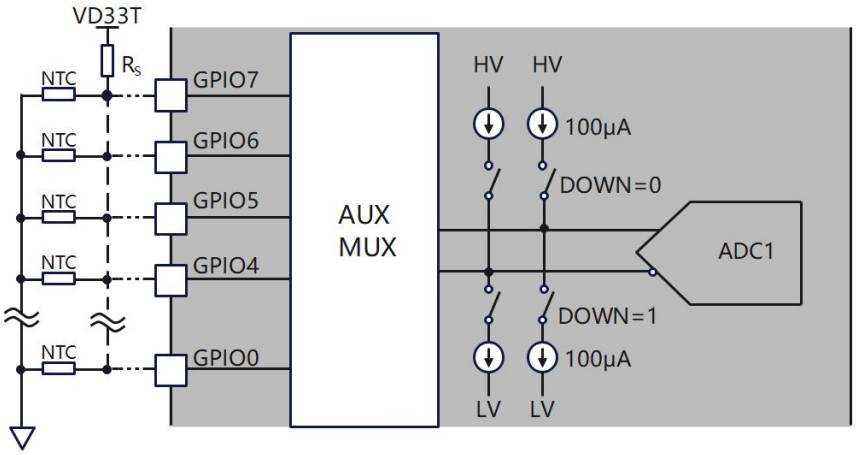

图 4.6　GPIO 采样通道开路检测简化电路

GPIO 开路检测算法在常温 25˚C 下，执行如下步骤：

1. 执行 DOWN=0 的 GPOW 命令。在命令结束后，读取 GPIO（0~7）引脚输入电压一次，并将其存储在阵列 $GPIO_{D0}(n)$中，n=0 到 7，表示 GPIO 输入引脚编号；
2. 执行 DOWN=1 的 GPOW 命令。在命令结束后，读取 GPIO（0~7）引脚输入电压一次，并将其存储在阵列 $GPIO_{D1}(n)$中，n=0 到 7，表示 GPIO 输入引脚编号；
3. 计算在上述步骤中对 GPIO 0~7 引脚比较导通上拉和下拉电流源测量值 $GPIO\Delta(n) = GPIO_{D0}(n)–GPIO_{D1}(n)$；
4. 如果在某个 GPIO 输入引脚上，存在 $GPIO\Delta(n)$ 大于 850mV，则 GPIO(n)通路异常；反之，则 GPIO(n)通路正常。

SM17：使用冗余热敏电阻电路和 GPIO 输入进行冗余温度测量。

GPIO 输入和内部温度由 ADC 测量。ADGP 命令进行 GPIO 输入的测量。其后，再使用 RDGVA,RDGVB 和 RDGVC 命令读取结果。

对于更高的 ASIL 要求，系统可以考虑使用热敏电阻，该冗余热敏电阻在冗余 GPIO 引脚上测量。冗余可缓解 GPIO 引脚泄漏、外部电容泄漏或热敏电阻电路故障导致的潜在单点故障。系统应确保用于冗余温度测量的 GPIO 引脚彼此不相邻，以避免潜在的引脚间短路导致潜在故障。不相似的温度测量表明一条或两条测量路径上存在故障。如果使用冗余 GPIO 进行温度测量，则不需要 SM15（GPIO 相邻短路检查）和 SM16（GPIO 开路检查）。

SM18：检查热敏电阻测量结果是否在有效范围内。

根据规格书中的 VD33T 的电气特性得知，电压值介于于 3.27 和 3.33V 之间。发出 ADGP 命令，以测量 GPIO 引脚输入电压，检查热敏电阻结果是否在有效范围内。

SM19：确认在 GPIO 测量期间，开路电流源未滞留于 on（接通）或 off（断开）位置。

为确保开路电流源未滞留于开/关位置，在 DOWN=1 的任何 GPIO 上发出 GPOW 命令，并将 GPOW 结果与 ADGP 结果进行比较。不考虑 GPIO 采集回路上的滤波阻抗时，具有下拉开路电流源功能的 GPOW 结果将减少 100μA *(R_{NTC}+R_{Switch})，其中 R_{NTC} 是从 GPIO 引脚看到的 NTC 的有效电阻，R_{Switch} 为 GPIO 引脚多路复用开关接通电阻。

假设 R_{NTC}=5kΩ，R_{Switch}=360Ω（标准值），GPOW 结果将比 ADGP 结果低约 536mV。如果电流源滞留于 on（接通）或 off（断开）位置，则两个命令之间存在差异。系统可以设置低于 536mV 的阈值，并具留有足够的余值来检测下拉电流源中的故障。如果检测到故障，则不能再依靠 SM17 中描述的开路算法来检查开路。

类似地，为确保上拉电源未滞留于开/关位置，在 DOWN=0 的任何 GPIO 上发出 GPOW 命令，并将 GPOW 结果与 ADGP 结果进行比较。GPOW 结果应比 ADGP 结果高出下拉电流诊断设置的阈值，因为 100uA 电流流入 GPIO 引脚。

5. 流程支持

5.1. 设计开发流程

比亚迪半导体集成电路开发和制造的质量管理体系由认证的注册机构认证，符合 ISO/IATF16949 和 ISO 9001。比亚迪半导体具有完善的集成电路设计开发管理程序，由一系列的阶段组成，为设计开发活动提供结构化管理规范和审查里程碑。以下是整个过程的主要阶段和关键里程碑描述：

1. E-1：项目立项及准备阶段

- 识别项目所开发的新产品概念
- 确定项目设计开发资源
- 确定项目预算
- 确定项目人员名单及职责确定项目计划
- 立项评审

2. E0：设计定型阶段

- 确定产品定义及产品规格
- 芯片与版图设计
- 芯片与版图的前端及后端仿真验证与评审
- DFMEA 评审
- 设计定型评审

3. E1：产品功能与性能确认阶段

- 确定晶圆及样品制作规范
- 确定 CP、FT 测试方案及评审
- 确定工程样品测试方案及评审
- 测试结果评审
- 设计冻结及评审

4. E2：产品定型阶段

- 第一次可靠性测试结果评审

- 确定产品品质控制计划
- 设计输出评审

5. E3：生产确认阶段

- 第二次、第三次可靠性测试结果评审
- 供应商 PPAP 评审
- 确定客户对样品的承认
- 生产确定评审

6. E4、SOP：量产阶段

- 确认试产与量产导入
- 项目总结

采用 ISO 26262 功能安全标准后，流程中将包括以下主要内容：

- 建立安全团队和任命安全经理
- 将安全关键项目纳入产品追踪系统，成为安全计划
- 对 ISO 26262 进行裁剪分析，以确定哪些可交付成果适用
- 系统级安全使用假设、HARA、功能安全需求分析、技术安全需求分析
- 失效模式影响和诊断分析、FMEDA、FTA、相关失效分析
- 建立安全档案

6. 系统诊断指南

6.1. 硬件诊断

在本文第四章中列出了 BF8915A 所包含的所有安全机制清单，本节将指出上述安全机制在硬件安全模块测量中的诊断和覆盖方式。

表 6.1 硬件诊断覆盖

编号	名称	描述	相关功能块	安全机制覆盖
1	MUXes	复用模块由模拟开关组成，并由译码器控制。复用模块覆盖了产品内所有的采集通道中模拟开关部分，可通过 MUX Decoder 检查、ADCOW、GPOW、ADSTAT、ADCVH 等命令，并开路算法和读取 Muxfail 位进行检查运行状况。	FB1/FB2/FB3/FB9	SM1/SM2/SM3/SM4/SM6/SM7/SM10/SM12/SM16/SM17/SM18/SM19
2	ADC	产品 BF8915A 使用的两个(Δ∑)ADC 确保，采集数据在+25°度的温度下，不大于±3mV 的偏差。可以通过 ADCV、ADCOW、ADOL、ADCVH、ADGP、GPOW 等命令对该模块进行检查。	FB4/FB5	SM1/SM2/SM3/SM4/SM6/SM15/SM16/SM17/SM18/SM19
3	Reference Voltages	工作参考基准电压保证，受控功能模块的正确运行。可通过检查内部参数进行检查参考电压数值。	FB30/FB31/FB32	SM10
4	Serial Communication	产品 BF8915A 的串口通信模块，包含标准 4 线的 SPI 通信接口和双线差分菊花链 SPI 接口，确保产品与外界产品的正确通信。可通过读/写和错误 CRC 报文、命令对该模块进行检查	FB13/FB14/FB18/FB19	SM13/SM14
5	LDOs, Sum of Cells	产品 BF8915A 将总电池电压作用于多个 LDO 功能模块，用于产生所有的工作参考基准电压。可通过内部参数、ADCV、ADGP、ADCVH 和规格书中的规范阈值进行比较，从而诊断该模块。	FB6/FB26/FB27/FB28/FB29	SM4/SM10
6	Logic and MTP	该模块中包含数据寄存器和状态机，用于控制 BF8915A。可通过寄存器自	FB15/FB16/FB17	SM8/SM9/SM11

		测功能，寄存器清除功能和写入‘0/1’等诊断方式，以确保存储正确。		
7	Balance FETs	产品 BF8915A 通过引脚 S1 至 S18 和所连内/外 MOSFET 对电池进行放电。	FB7	SM5
8	Open-Wire Sources	产品 BF8915A 允许 BMS 控制器检擦 ADC 之前的电池和 GPIO 采集回路的开路情况和回路阻抗情况。通过 ADCOW 命令和 GPOW 命令进行检测，亦可叠加 ADCV 命令和 ADGP 命令使用可诊断回路高阻抗。	FB8	SM3/SM6/SM16/SM17/SM19
9	Temperature Measurements	外部温度测量可通过 GPIO 引脚和外部温敏电阻构建。并根据所测温敏阻抗确定温度值。 内部结温可通过内部参数测量获得该数据，并在结温高达 125°时，自动开启过温保护模块	FB24/FB25	SM7/SM18

6.2. 关于软错误

- JEDEC 标准将软错误定义为高能粒子冲击引起的不损害功能性的错误。软错误包括单事件扰动（SEU）、多位扰动（MBU）、单事件功能中断（SEFI）、单事件瞬态（SET）和单事件闩锁（SEL）。
- SEU：由单一高能冲击引起瞬态信号状态变化。通常时序逻辑（如锁存器和 RAM）要针对 SEU 设定目标。
- SEFI：使组件复位、锁定或其它可检测到的但不需要组件电源来恢复可操作性的错误。它通常与控制位或寄存器中的异常有关。SEFI 实际上是 SEU 的一个子集，因为控制位和寄存器中的 SEU 会导致 SEFI。
- SET：由单个高能粒子冲击引起的 IC 节点处的瞬时电压偏移（尖峰）。它会导致组合逻辑、时钟和其他公用功能的错误。
- SEL：由于单个高能粒子通过器件结构的敏感区域而导致器件中的异常高电流状态，并导致器件功能丧失。SEL 在在器件功能丧失而导致硬错误之前不是安全至关重要的。最先进的设计实践和测试应该能够防止这一点。

对于 BF8915A 系列 BMS 电池管理模拟前端芯片的软错误，重点将放 SEU 和 SET 方面。

BF8915A 系列 BMS 电池管理模拟前端芯片中可能导致软错误的能量水平远远大于低于 100nm IC 中的能量水平。因此，BF8915A 系列 BMS 电池管理模拟前端芯片的软错误率（SER）比那些通常具有更大片上存储体的 IC 低多个数量级。

如果带电粒子曾经在 BF8915A 系列 BMS 电池管理模拟前端芯片中以不明显的速率引起软错误，则大多数粒子可以通过系统级的措施来减轻，也可以通过系统级措施来检测。

BF8915A 系列 BMS 电池管理模拟前端芯片的 SER 与先进 CMOS 工艺中的其他集成电路相比微不足道，后者具有更高的逻辑和内存密度以及更低的电源电压。由 SEU 和 SET 引起的极低概率的瞬时故障大多可以通过系统级的安全机制或措施来检测或减轻。

表 6.2　软错误

软错误类型	检测或减轻机制（定性分析举例）
寄存器 SEU	SM_RSEU_1：数据寄存器在每次 ADC 采样转换结束时不断更新。只有那些发生在寄存器被主机控制器读取之前的 SEU 才需注意。主控单元可以拒绝由任何 SEU 导致的不切实际电池电压数据，同时范围内的其他 SEU 可通过从多次测量中获取平均值来减轻影响。 SM_RSEU_2：配置寄存器的 SEU 将显示为错误操作。比如，范围外的配置可以被拒绝，也可以被主控单元通过现有的安全机制（如，读回寄存器）检测。
存储体 SEU	SM_SSEU_1：存储体中的内容直接读取，不用影子寄存器操作。
公用资源 SET	SM_SET_1：公用资源 SET 可能导致模块状态机故障，如 ADC 提前终止或执行错误命令。例如：读回寄存器校验或每次运行开始前复位状态机。又例如：可能导致 ADC 滤波器和 ADC 控制器的故障。ADC 滤波器中的故障可通过冗余滤波机制来检测。ADC 控制器中的故障将导致与状态机中的故障模式类似，因此可以检测到它们。

6.3. 其它支持

除本安全手册外，客户还可通过签订保密协议获得 BF8915A 系列 BMS 电池管理模拟前端

芯片其它功能安全相关文件，包括 FMEDA、PPAP 等。有关本产品 ISO 26262 的更多信息，请联系比亚迪半导体在当地的销售办事处或销售代表人员。

6.4. 验证评审流程

对于验证评审工作，都遵循一个综合的评估计划。产品设计开发流程详细说明了如何制定评审计划、设计、验证、FMEA、工艺研究以及证明有效质量体系的质量认证。

评审过程在设计开发流程中进行了描述。在适当的情况下，通过将产品置于各种测试模式来验证安全机制。测试模式包括在产品的设计阶段的测试验证。在评审过程中，保留了评审调查结果和描述评审方法的文件。

同时，实施定期安排评审会议，以审查任何发现的问题。在整个评审过程中，保留了勘误表和修订表。完整的评审清单和总结作为评审过程的工作成果。

BF8915A 系列 BMS 电池管理模拟前端芯片验证和确认报告中总结了安全相关功能的测试，用于识别产品对 ISO26262 合规性。

6.5. 支持服务流程

在 ISO 26262 的范围内，BF8915A 系列 BMS 电池管理模拟前端芯片是脱离上下文的的硬件单元安全元素（SEooC）。安全相关特性设计开发流程中定义，并通过我们的质量体系在制造和测试中得到保证。

作为设计开发流程的输出，安全要求输入给测试组件和测试流程。所有电气测试要求在设计开发流程确定，并作为测试团队测试测试开发流程的输入，并根据测试开发流程完成测试组件的开发和鉴定。

产品验证措施和验收标准基于设计开发流程的输出。所有支持服务流程的要求作为产品和 ISO/IATF16949 认证质量体系的一部分进行实施和维护。

7. AECQ100 测试鉴定

BF8915A 系列 BMS 电池管理模拟前端芯片根据 AECQ-100 标准进行可靠性测试鉴定。BF8915A 系列 BMS 电池管理模拟前端芯片通过进行额外的组件和封装级应力测试，保证本产品满足或超过当前 AEC-Q100 的要求。这些附加试验可能包括但不限于：AC、TC、HAST、HTSL、HTOL、ELFR、EDR、ESD、LU 等试验。

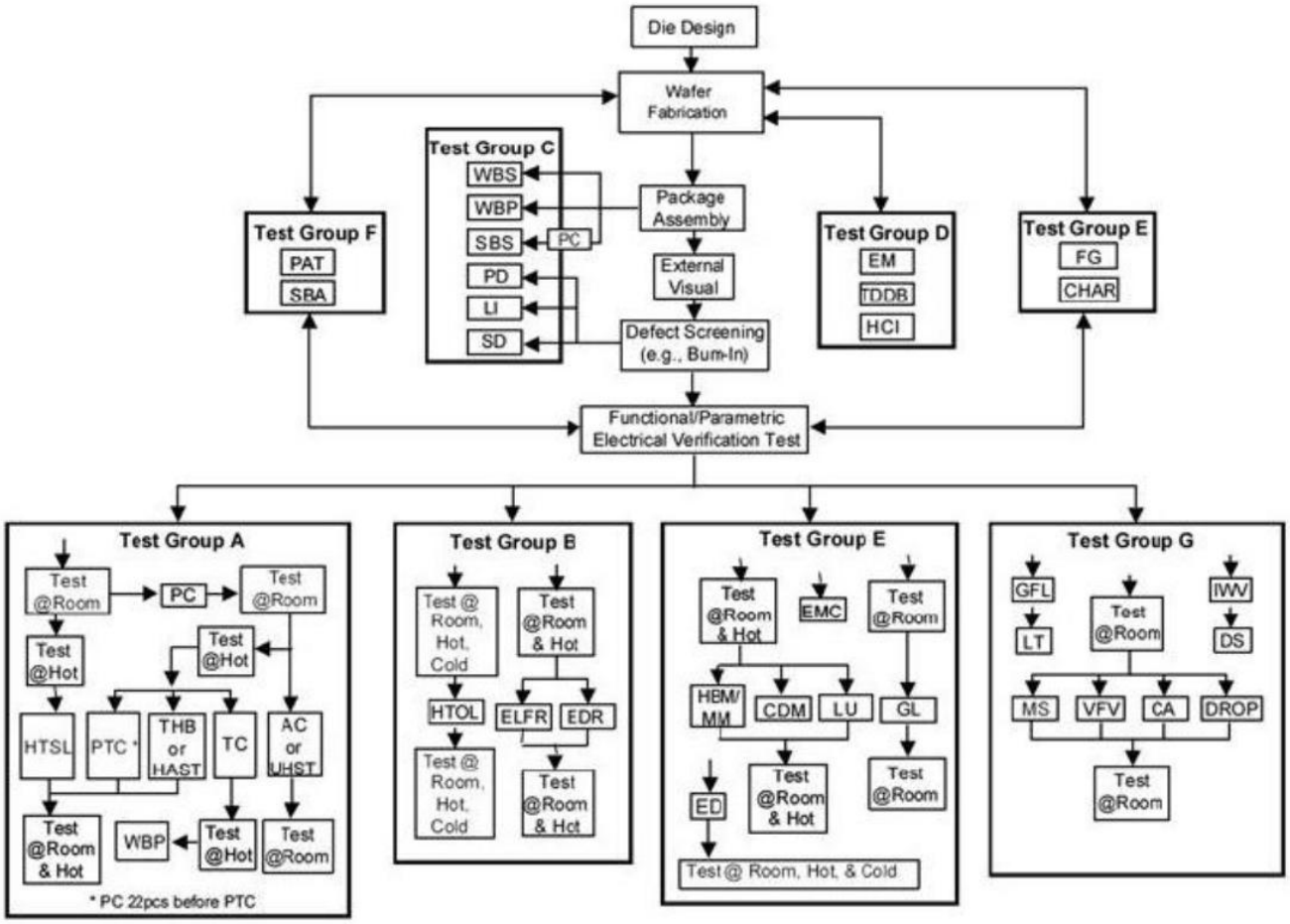

图 8.1　可靠性鉴定

比亚迪半导体在产品发布之前通过这些测试验证了 BF8915A 系列 BMS 电池管理模拟前端芯片产品的健壮性，旨在消除测试逃逸和早期失效。比亚迪半导体车规级设计开发流程提供额外的筛选检查和更严格的标准用于晶圆制造、封装、电气和可靠性测试中。

8. 定量分析结果

随机硬件失效分析假设 BF8915A 是在上述假设范围内使用。系统必须利用 BF8915A 的诊断特性，以确保报告的测量结果并非异常。可采用 FMEDA 进行定量分析。根据 3.1 节中的功能安全假设，并综合考虑所有功能块，计算得出以下 ASIL 等级，如表 8.1 所示。

表 8.1　BF8915 定量分析结果

	TSR1	TSR2
Total FIT(Raw FTI)	4.5768	4.0634
Total Safety Related FIT	4.3624	3.8653
Single Point Fault Metric/SPFM[%]	97.1119	97.4643
Latent Fault Metric/LFM[%]	99.4138	99.1769
Probabilistic Metrics for Random Hardware Failures/PMHF(in FIT, Lifetime = 10 years)	0.6677	0.6973