新能源汽车三电系统功能安全技术要点分析

董蕾蕾　千煜晗　陈新宇
陕西重型汽车有限公司　陕西　西安　710200

摘　要：新能源汽车三电系统功能安全技术是保障整车安全运行的核心支撑，涉及电池、电机、电控三大部件的全流程安全防护。本文从底层逻辑与架构体系、分域功能安全技术要点、全流程技术管控三个维度展开分析，涵盖硬件层安全设计、软件层安全设计、系统层协同设计等关键环节，并提出需求拆解、方案验证、异常识别、体系升级等全流程管控策略，为新能源汽车三电系统功能安全技术发展提供理论参考。

关键词：新能源汽车；三电系统；功能安全技术

引言：新能源汽车作为汽车产业电动化转型的核心载体，其三电系统（电池、电机、电控）的功能安全直接关系到整车运行可靠性。随着新能源汽车市场渗透率持续提升，三电系统功能安全技术已成为行业关注的焦点。聚焦三电系统功能安全技术要点，从架构设计逻辑、分域技术实现、跨域协同机制、全流程管控路径等方面展开系统性分析，旨在为行业提供可落地的技术参考。

1 新能源汽车三电系统功能安全技术底层逻辑与架构体系

1.1 三电系统功能安全的技术内涵与核心定位

新能源汽车三电系统功能安全技术，以ISO 26262-1:2018第4章、GB/T 34590.1-2022第4章为顶层核心标准体系，配套GB 38031-2020第5章、GB/T 18488-2024第5章、GB 18384-2020第5章等行业核心标准为合规依据，搭建全流程技术合规框架。功能安全核心是规避系统故障非预期行为引发的人身与车辆危害，聚焦故障全生命周期管控与安全完整性等级落地；电气安全聚焦绝缘防护与电气回路可靠性，防范直接电气接触危害；热安全聚焦温度场管控与热失控主动抑制，防范热累积引发的连锁危害，三者边界清晰、范畴独立、互为支撑，不可混淆等同。三电系统是新能源汽车核心动力来源，功能安全技术依托ISO 26262-3:2018第6章规定的危害分析和风险评估（HARA）方法完成整车级安全目标拆解，围绕三大部件搭建全维度防护体系，通过故障诊断、冗余设计、应急控制，规避单一部件故障连锁风险，贯穿研发测试全流程，是整车安全运行的核心技术支撑。

1.2 三电系统功能安全的整体架构设计逻辑

三电系统功能安全架构设计，依托AIAG&VDA FMEA:2019规定的设计失效模式与影响分析（DFMEA）方法，完成全链路风险预判与架构优化，行动优先级（AP）为高的风险项100%制定优化方案，严格匹配ISO 26262-4:2018第5章顶层功能安全标准。设计聚焦系统级安全目标，推动三大系统联动，形成完整防护链。硬件层强化关键硬件抗干扰与稳定性，关键传感器、微控制器单元（MCU）实现100%冗余备份，满足ISO 26262-5:2018第9章硬件随机失效概率要求。软件层优化控制算法与故障识别逻辑，搭建多层级容错机制，代码静态测试覆盖率100%，符合ISO 26262-6:2018第9章要求。系统层明确各部件安全职责边界，建立高效信息交互机制，故障传递延迟 ≤ 10ms。某车型初期架构未设置独立安全监控芯片，主微控制器单元（MCU）锁死时无法触发安全停机，经DFMEA识别为AP高风险项后，新增独立ASIL D级安全监控芯片，采用“主MCU+安全MCU”双核锁步架构，主MCU异常时3ms内接管控制权，触发高压下电与制动，累计规避12起潜在失控事故[1]。

2 新能源汽车三电系统分域功能安全技术要点核心分析

2.1 动力电池系统功能安全技术实现路径

动力电池系统功能安全技术落地，严格遵循GB 38031-2020第5.1条、第6.2条核心要求，以HARA分析方法为核心，针对BMS故障导致的过充、过放、热失控触发等功能失效场景，完成严重度、暴露率、可控性量化分析，确定汽车安全完整性等级（ASIL）D最高安全等级并拆解安全目标，同步通过DFMEA完成电芯、电池管理系统（BMS）、热管理系统全链路失效识别。电芯层级优化正负极材料与工艺，提升热稳定性与电化学一致性，直流内阻偏差 ≤ 3%。BMS优化核心参数监测精度与诊断算法，提升异常识别与响应速度。热管理系统控温精度±2℃，电芯间温差 ≤ 5℃。某车型曾发生3起因BMS单通道采样失效导致的电芯过充热失控事故，经HARA评定为ASIL D级最高风险后，采用“电芯级独立电压采样+主从双MCU冗余架构+三级过充保护”方案，每节电芯独立采

样，主从MCU交叉校验数据，整改后同类事故发生率降至0，累计完成100万+公里实车验证无异常。

2.2 驱动电机系统功能安全运行保障

驱动电机系统的功能安全保障，严格遵循GB/T 18488-2024第5.3条、第5.4条核心要求，依托DFMEA分析方法，完成全工况失效识别与风险分级，针对绕组短路、位置传感器失效、控制器过流等高风险模式，通过HARA分析量化危害等级，匹配ASIL B至ASIL D防护策略，实现全流程管控。电机本体选用高稳定性绝缘材料，提升绕组绝缘性能，绝缘电阻 ≥ 100MΩ，规避绝缘老化短路风险，同步强化定转子结构，降低振动磨损。电机控制策略优化精度与响应速度，转速控制精度±0.5%，扭矩控制精度±3%，规避指令偏差引发的过载、堵转异常。运行状态监测体系实现关键参数全时段捕捉，绕组温度监测精度±2℃，控制器故障响应时间 ≤ 5ms。某SUV车型在高速行驶时曾出现旋转变压器信号丢失导致的非预期失速问题，经DFMEA发现单路旋变信号无冗余[2]。整改后采用“旋转变压器硬件信号+无传感器算法软件冗余”双路监测方案，主信号异常时1ms内无缝切换，维持扭矩输出偏差 ≤ 5%，该方案已应用于全系12款车型。

2.3 整车电控系统功能安全控制策略

整车电控系统作为三电系统控制中枢，其功能安全控制策略严格遵循GB/T 34590.4-2022第5章、GB 18384-2020第5.1条核心要求，以HARA分析方法为基础，针对非预期加速、非预期制动、高压意外下电等整车级危害事件，完成安全等级评定与目标拆解，同步通过DFMEA完成软硬件全链路失效分析，优化控制策略。控制架构采用分布式与集中式结合，明确各模块职责边界，降低运行干扰，控制指令传输延迟 ≤ 5ms，执行准确率100%。搭建全流程故障诊断与容错控制体系，故障诊断覆盖率 ≥ 99%，轻微故障切换时间 ≤ 20ms维持基础运行，严重故障触发安全停机。某轿车曾发生2起因控制器局域网（CAN）总线干扰导致的非预期加速事故，经HARA评定为ASIL D级风险后，采用“CAN FD双通道冗余通信+扭矩安全监控”方案，关键扭矩指令通过两条独立物理通道传输，整车控制器（VCU）与电机控制器（MCU）交叉校验指令一致性，当两条通道指令偏差超过5%且持续10ms以上时，立即触发扭矩限制与安全停机，整改后完成1000小时电磁兼容测试与50万公里实车验证，未再发生同类问题。

2.4 三电系统跨域协同功能安全技术实现逻辑

三电系统的安全稳定运行，依赖各域之间的高效协同。跨域协同功能安全技术体系严格遵循GB/T 34590.6-2022第6章核心要求，依托DFMEA失效模式与影响分析方法，完成跨域故障传导路径全链路识别与风险管控，配合HARA分析量化协同失效危害，匹配对应安全等级，形成严谨的技术逻辑。优化跨域数据交互协议，传输延迟 ≤ 10ms，误码率 ≤ 10^{-9}，保障三电各域信息传递精准高效。跨域协同控制打破壁垒，结合工况统筹调配参数，实现三电系统性能优化与安全防护联动。建立跨域故障联动机制，实现故障信息全域同步，联动响应时间 ≤ 20ms。某纯电货车曾发生1起因BMS过温信号未同步至电机控制器导致的热失控事故，当时电池温度达65℃但电机仍满功率放电[3]。经DFMEA识别为跨域通信失效高风险后，搭建全域故障信息共享总线，建立“故障等级-联动动作”映射表，BMS一级过温信号15ms内同步至三电全系统，电机立即降功率至50%，电控限制最大放电电流，热管理系统全功率制冷，整改后同类风险完全消除。

3 新能源汽车三电系统功能安全全流程技术管控与能力提升

3.1 安全技术需求的层级拆解与转化

安全技术需求的层级拆解与转化，是三电功能安全管控的核心前提，遵循GB/T 34590.3-2022第6章自上而下拆解原则，依托HARA分析方法，完成整车级危害识别与ASIL等级评定，确定安全目标并全链路落地，保障管控有据可依。需求拆解遵循层级逻辑，从整车级安全目标拆解至系统级，再细化至部件软硬件需求。拆解全程可追溯，保障下一层级需求100%覆盖上一层级目标，无脱节、无冲突。需求转化将抽象安全要求转化为可落地的量化指标、设计规范与验证标准，为研发生产提供依据，例如将避免非预期加速的ASIL D目标，转化为扭矩控制精度±3%、监控周期 ≤ 1ms的指标。转化结合三电特性，配合DFMEA验证覆盖度，保障技术适配工况，从源头规避系统性风险。

3.2 安全技术方案的验证与闭环确认

三电功能安全技术方案的可靠性，需通过系统化验证与闭环确认保障，严格遵循GB/T 34590.8-2022第5章核心要求，依托DFMEA方法，针对高风险失效模式制定专项验证方案，实现场景全维度覆盖与方案全流程优化。验证场景贴合实际工况，覆盖正常与极限异常，100%覆盖核心安全要点。验证流程遵循模型在环（MIL）、软件在环（SIL）、处理器在环（PIL）、硬件在环（HIL）、实车测试层级逻辑，ASIL D项目故障注入测试覆盖率 ≥ 99%。某BMS过充保护功能验证项目，通过DFMEA识别出低温环境下采样精度不足、过充判定延迟、保护

动作执行卡滞、通信中断四类高风险，制定了包含256种故障场景的验证矩阵[4]。SIL测试注入128种软件故障，定位-30℃下采样漂移导致过充判定延迟25ms；PIL测试发现执行器驱动延迟12ms。优化温度补偿算法与驱动电路后，过充判定延迟降至8ms，保护动作执行准确率100%，完全匹配ASIL D安全目标。

3.3 安全异常状态的识别与防控

三电运行中安全异常的精准识别与防控，严格遵循GB 18384-2020第5.2条要求，依托HARA完成异常分级，配合DFMEA分析失效诱因，优化识别逻辑与防控策略。异常识别依托各域监测模块，实时捕捉核心参数波动，搭建多维度判定逻辑，识别准确率 ≥ 99.9%，误报率 ≤ 0.01%，区分工况波动与隐患信号，规避误判漏判。针对不同等级异常，制定差异化防控措施，结合严重程度触发预警、降功率、安全停机，轻微异常响应 ≤ 50ms，严重异常 ≤ 10ms。某车型曾频繁出现高压绝缘监测误报警问题，经DFMEA发现原单路绝缘监测易受电机载波与湿度影响，误报率达0.5%。整改后采用“双路独立绝缘监测+多参数融合判定”方案，两路监测模块采用不同测量原理，结合环境湿度、高压电流、电池电压等参数综合判定，当两路监测结果偏差超过20%且持续50ms以上时才触发预警，误报率降至0.005%以下，同时保持了10ms内的严重异常响应速度。

3.4 安全技术体系的升级与完善路径

三电功能安全水平的持续提升，依赖安全技术体系迭代完善，立足行业标准迭代与三电技术发展趋势，以HARA、DFMEA常态化应用为核心，明确升级路径，区分功能、电气、热安全边界，实现三者协同优化。体系优化立足三电特性，梳理薄弱环节，针对性迭代核心方案，弥补管控短板，保障100%覆盖三电全生命周期。体系完善注重各域技术协同，打破壁垒，推动三电安全技术深度融合，形成协同防护效应[5]。同步强化标准化建设，搭建全生命周期失效数据库，固化成熟技术与管控规范，每年完成1次全体系DFMEA复盘，失效案例闭环率100%。体系迭代聚焦行业趋势，融入AI故障预测、数字孪生等技术，优化安全架构，迭代后安全目标验证通过率100%，适配技术发展需求，为整车安全提供坚实技术支撑。

结束语：未来，随着新能源汽车智能化、网联化趋势加速，三电系统功能安全技术将面临更复杂的应用场景和更高的安全要求。需持续深化硬件抗干扰设计、软件容错算法、系统协同控制等核心技术研发，完善全流程验证与闭环确认机制，推动安全技术体系向智能化、自适应方向升级，为新能源汽车产业高质量发展筑牢安全基石。

参考文献：

[1]张治国.新能源汽车三电系统功能安全技术要点分析[J].汽车电器,2025(6):21-22+25.

[2]邓建明,龚循飞,于勤,等.新能源汽车电驱动系统关键技术及其发展趋势分析[J].汽车文摘,2025(2):18-22.

[3]吴飞,宋文艳,王佳俊.新能源汽车“三电”系统功能安全技术分析[J].汽车周刊,2022(11):22-24.

[4]姚日煌,鹿洵.汽车电子系统功能安全策略与ISO 26262应用分析[J].机器人产业,2024(5):21-31.

[5]马丕军.智能网联背景下新能源汽车三电系统检测维修研究[J].汽车维护与修理,2025(9):112-114.