电动汽车电池管理系统(BMS)功能安全标准研究

李 波，付 越，周 荣

(中国汽车技术研究中心有限公司，天津 300300)

摘要：电动汽车三大核心之一是电池，而电池的核心在于电池管理系统(BMS)。BMS 作为电池大脑，时刻对电池充电、放电状态进行管理，其功能安全技术水平决定了电池的安全性能，并直接影响整车安全。国家标准 GB/T《电动汽车用电池管理系统功能安全要求及试验方法》将从电池管理系统(BMS)的正向设计、开发、验证、确认的源头规避安全风险，进而规范 BMS 行业技术发展，提升电动汽车整车安全水平。基于国家标准 GB/T 34590-2017《道路车辆 功能安全》中给出的电控系统功能安全技术分析方法，结合典型的电动汽车用电池管理系统(BMS)架构，为国家标准 GB/T《电动汽车用电池管理系统功能安全要求及试验方法》的制定以及规范和提升电池管理系统行业技术水平，促进电动汽车整车安全提供了参考借鉴。

关键词：电池管理系统；功能安全；标准；危害分析与风险评估；安全目标；ASIL 等级

Research on functional safety standard for battery management system (BMS) of electric vehicles

LI Bo, FU Yue, ZHOU Rong

(China Automotive Technology and Research Center Co., Ltd, Tianjin 300300, China)

Abstract: The battery is one of three most important components in electric vehicle, and the core of the battery is the Battery Management System (BMS). As the brain of battery, BMS manages the charging and discharge state of the battery all the time. Its functional safety technology determines the safety performance of the battery, and affects the safety of the vehicle. The national standard of GB/T "Functional safety requirements and testing methods for battery management system of electric vehicles" aims to avoid the safety risks from the design, development, verification and validation of BMS, standardize the development of BMS industry technology, and improve the safety level of electric vehicles. This paper is based on the analysis method of functional safety given in the national standard GB/T 34590-2017 "Road Vehicles-Functional Safety" and combined with the typical BMS architecture of electric vehicles. It provides reference for developing the national standard GB/T "Functional safety requirements and testing methods for battery management system of electric vehicles", as well as standardizing and improving the technology of BMS industry, and promoting the safety of electric vehicles.

Key words: battery management system (BMS); functional safety; hazard analysis and risk assessment; safety goal; ASIL

0 引言

近年来，我国电动汽车产业发展迅猛，市场份额位居世界前列。在市场形成规模的形势下，各项技术发展迅速。动力电池能量密度迅速提高，接近世界先进水平；电机功率密度等指标大幅提高，电动空调、电动助力转向已形成规模市场，成本明显下降；整车续驶里程显著提高；充电基础设施发展迅速，商业模式不断创新。但是，伴随而来的安全事故频发、车企召回，安全问题已凸显，并受到行业、消费者、政府部门的高度关注，安全性已成为制约我国电动汽车发展的短板。

电动汽车三大核心之一是电池，而电池的核心在于电池管理系统(BMS)。电池管理系统作为实时监控、自动均衡、智能充放电的电子部件，也是动力和储能电池组中不可或缺的重要部件，起到保障充/放电安全、延长寿命、估算剩余电量等重要功能，它通过一系列的管理和控制，从而保障电动汽车的正常运行，因此，没有电池管理的电池包就是一枚炸弹。

电动汽车用锂离子电池单体、电池包或系统存在的风险包括其作为大质量车载能源对整车结构、乘员及第三方造成的机械危害、泄漏(如挤压、短路，可能导致高压安全、绝缘失效间接造成电击、起火等危险)、起火(如短路，直接烧伤人体)、爆炸(如挤压、短路，直接危害人体)、电击(由于电流流过人

体而引起的伤害)。

为了确保安全，相关国际和国内的标准法规正在加快制定中，例如，国际上近期发布的由中国作为副主席国牵头起草制定的全球技术法规 GTR 20(电动汽车安全 EVS)、我国正在开展制定的强制性国家标准 GB《电动汽车用锂离子动力蓄电池安全要求》提出了电动汽车整车、车用锂离子电池单体、电池包或系统最基本的安全要求以提供对人身的安全保护。标准中提到，基于行业共识，车企在确定电动汽车用锂离子电池单体、电池包或系统采用何种设计方案时，首先，如有可能，优先选择安全性高的材料，尽量避免使用容易出现绝缘失效、热失控或燃烧起火的材料；同时，如果无法实行以上原则，那么需制定保护措施，减少或消除危险发生的可能性。

因此，除了需要解决电池单体、电池包在设计过程中的结构工艺安全、化学安全、机械安全外，电池管理系统(BMS)，作为电池大脑，时刻对电池充电、放电状态进行管理，其决定了电池性能，并影响整车系统，其安全可靠的设计、运行是避免事故隐患发生的关键因素。

锂离子电池管理系统(BMS)发生故障、功能失效将会引起电池发生过充、过放、过流、过温的风险，进而使电池内部出现放热连锁反应，引起电池温升速率急剧变化的过热现象，即热失控，导致电动汽车的自燃或爆炸，对车内外人员造成伤害，属于电控系统功能安全领域范畴，应遵循 GB/T 34590《道路车辆 功能安全》给出的方法，制定相应的安全措施以避免危害的发生。

在国内，BMS 厂商众多，呈现出激烈的竞争态势。在技术层面上，由于生产企业流程开发体系、技术积累经验不同，存在严重的两极分化和良莠不齐，在当前电池系统安全隐患越来越突出的情况下，对于电动汽车整车安全已构成严重威胁。

为提升我国电池管理系统产业的安全技术水平，增强新能源汽车产品的核心竞争力和安全性能，遵循升级一批、规范一批、淘汰一批的原则，国家标准化管理委员会于 2017 年下达了国家标准 GB/T《电动汽车用电池管理系统功能安全要求及试验方法》的制定计划，旨在从电池管理系统(BMS)的正向设计、开发、验证、确认的源头规避安全风险，提升整车安全水平。

1 电池管理系统(BMS)的功能

按照国家标准 GB/T 34590《道路车辆 功能安全》给出的方法论，从整车层面出发，电池管理系统指的是实现车辆层面功能的系统，这里重点强调的是功能，即该功能可以由电池管理系统 BMS 实现，也可以由整车控制系统实现。GB/T《电动汽车用电池管理系统功能安全要求及试验方法》将给出两种方法描述电池管理系统的功能。举例来说，电池管理系统实现整车层面的功能包括充电管理和放电管理。

充电管理指的是该功能旨在通过 BMS 的控制管理，使得动力电池在充电过程中处于安全状态。BMS 在电池充电过程中对充电电压、充电电流、可检测到的电池温度等进行控制优化，确保电池在放电过程中的安全。充电管理包括正常充电管理和能量回收管理。

放电管理指的是该功能旨在通过 BMS 的控制管理，使得动力电池在放电过程中处于安全状态。BMS 在电池放电过程中对电池的放电电压、放电电流、可检测到的电池温度等参数进行控制优化，确保电池在放电过程中的安全。

基于典型的电动汽车用电池管理系统(BMS)架构，利用 HAZOP 分析方法以及国家标准 GB/T 34590-2017《道路车辆 功能安全》给出的方法论，开展电池管理系统危害分析与风险评估，提出电池管理系统的功能安全目标和功能安全要求。

2 电池管理系统的危害分析与风险评估

2.1 电池管理系统典型架构

锂离子动力蓄电池由于其能量密度和功率密度高的优点成为电动汽车主流，但随之而来的是显著的安全问题。由上节的功能定义，锂离子动力蓄电池在使用的过程中可能会产生起火、爆炸、冒烟、高压触电等危害，对于导致这些危害的原因有很多，主要有电芯过充、过流、过温等引发锂枝晶或者产生大量热，使得 SEI 膜刺破或者分解，进而发生一系列负反应，即电芯内短路。其他电芯本身的设计也会是影响锂离子动力蓄电池系统安全的重要因素，如杂质的影响。

这些失效主要分为电化学、机械结构、电力电子、制造工艺类等，都是电动汽车动力蓄电池系统的开发设计过程中应认真考虑的，并在整个开发流程中，根据相应安全分析制定相应的安全要求，落实安全要求，最终在零部件级、系统级和整车级测试验证这些安全要求的正确实现。

除了动力蓄电池系统本身的机械结构设计、电化学性能、制造质量，电池管理系统(BMS)可以通过合理的控制策略，避免动力蓄电池系统产生过压、过放后再充电、过流以及过温。假设不考虑动力蓄

电池系统本身在防止过充、过温、过流失效上面的机械结构类措施，重点讨论电池管理系统的功能安全设计，即关注电子电气类故障导致的动力蓄电池在整车系统中产生的危害。

在进行安全分析的初期，需要定义相关项与其他相关项的功能边界及相互接口。在现有的电动汽车和混动汽车中，各企业有不同的高压架构和控制架构，导致电池管理系统功能具有多样性以及功能实现方式有很多途径。

图 1 为 BMS 相关项的边界和接口参考示例。其他相关项如：可充电储能系统(REESS)、整车低压蓄电池、整车动力控制系统(整车控制器、电机控制器等)、高压部件(服务开关等)、充电接口(对于具有可外接充电功能的电动汽车)。

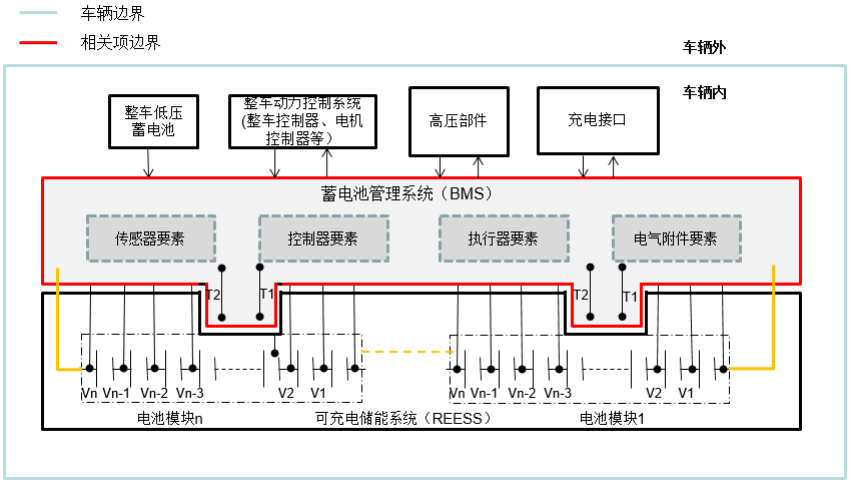

图 1 典型电池管理系统 BMS 的边界和接口

Fig. 1 Boundaries and interfaces of typical BMS

2.2 电池管理系统危害识别

常用的安全分析方法主要分为三大类：

1) 推论型，如故障树分析 FTA，开始于已知的影响，推导可能的原因。

2) 诱导型，如失效模式与影响分析 FMEA，故障注入分析等，开始于已知的原因，分析可能的影响。

3) 探索型，例如 HAZOP 分析。它是一种利用引导词进行失效原因以及风险影响的分析。

这些分析方法都是分析失效原因和影响的有效手段，帮助我们进行系统化、条理化的研究，避免遗漏、重复。本文将电池管理系统的本质功能进行抽象，即分为充电管理和放电管理，并以动力蓄电池的充电管理为例进行 HAZOP 分析，HAZOP 的引导词主要分为四类，即功能丧失、在有需求时，提供错误的功能、非预期的功能以及功能卡滞。

表 1 为应用 HAZOP 方法识别出充电管理、放电管理功能的异常表现。

表 1 充电管理、放电管理功能的 HAZOP 分析-识别功能的异常表现

Table 1 Abnormity of HAZOP Analyze-identify functions of charging/discharge management functions

功能关键字		功能丧失	在有需求时，提供错误的功能			非预期的功能(在无需求时，提供功能)	输出卡滞在固定值上(功能不能按照需求更新)
			错误的功能(多于预期)	错误的功能(少于预期)	错误的功能(方向相反)		
充电管理	充电电压管理	充电管理失效	充电过压(过充管理失效)	N/A	N/A	N/A	卡滞在固定单体电压
	充电电流管理	充电管理失效	充电过流(过流管理失效)	充电电流不足	预期充电，实际为放电	非预期充电	卡滞在固定电流
	充电温度管理	充电管理失效	充电过温(过温管理失效)	N/A	N/A	N/A	卡滞在固定温度值
放电管理	放电电压管理	放电管理失效	放电过放(过放管理失效)	N/A	N/A	N/A	卡滞在固定单体电压
	放电电流管理	放电管理失效	放电过流(过流管理失效)	放电电流不足	N/A	非预期放电	卡滞在固定电流
	放电温度管理	放电管理失效	放电过温(过温管理失效)	N/A	N/A	N/A	卡滞在固定温度值

表 2 功能异常表现导致的整车层面的危害

Table 2 Damage on the vehicle level caused by function abnormity

功能异常表现	整车层面的危害(最严重的情况)
充电时电流超出预期，造成电池过流时无保护或保护不及时，引发热失控—过流	冒烟、起火、爆炸、产生的高温气体烧伤人或毒性气体使人中毒
充电时充电电压超出预期，造成电池过充时无保护或保护不及时，引发热失控—过充	冒烟、起火、爆炸、产生的高温气体烧伤人或毒性气体使人中毒
充电时电池温度超出预期，造成电池过温时无保护或保护不及时，引发热失控—过温	冒烟、起火、爆炸、产生的高温气体烧伤人或毒性气体使人中毒
放电时放电电流超出预期，造成电池过流时无保护或保护不及时，引发热失控—过流	冒烟、起火、爆炸、产生的高温气体烧伤人或毒性气体使人中毒
放电时电池温度超出预期，造成电池过温时无保护或者保护不及时，引发热失控—过温	冒烟、起火、爆炸、产生的高温气体烧伤人或毒性气体使人中毒
放电时放电电压超出预期，若进行在充电，造成电池过放后再充时无保护或保护不及时，引发热失控—过放后再充	冒烟、起火、爆炸、产生的高温气体烧伤人或毒性气体使人中毒

2.3 电池管理系统危害分析和风险评估

危害是针对整车层面来说的，危害需要结合特定的场景才能形成危害事件。电动汽车车辆典型的使用场景有正常行驶(高速行驶，城市路况，转弯)、车辆静止无人看管充电、车辆静止无人看管放电、车辆长期静置、碰撞(发生碰撞，碰撞之后)、维修。在不同场景下进行危害分析和风险评估，例如，车辆在行驶过程、慢充和快充甚至发生碰撞后，都有可能由于控制系统失效导致电池系统过充、过温、过流，造成电池包产生热失控或者热扩散，引发起火的危害。但在不同场景下，危害发生的严重度 S、驾驶员对于危害的可控性 C 以及场景的暴露概率 E 都是不同的，需要逐条分析讨论。

这里以非预期的释放热能导致燃烧或明火为例，进行电池管理系统的危害分析与风险评估，需要指出的是该示例仅作为参考，具体安全要求应根据企业在开发过程中的实际情况而定。

如果电动汽车发生起火的危害，会危及驾驶员以及乘员的生命，因此，严重度定义为 S3。对于暴露概率 E，不是指发生功能失效的概率，而是对于危害事件，每个运行场景在驾驶过程中出现的暴露概率。车辆正常行驶在高速路况或者城市路况以及进行车辆充电(包括慢充和快充)，对于一般的驾驶员来说，是几乎每次驾驶都会发生的，所以将正常行驶和车辆充电的暴露概率定义为 E4。对于碰撞和维修场景，可保守定义为 E2。暴露概率的评定，不同国家和不同的驾驶员习惯有很大的不同，需要按照实际情况进行分析与判断。

车辆在高速公路上正常行驶的场景在生活中很常见，如果在该场景中电池系统起火对于驾驶员以及乘客有致命的威胁，但是驾驶员或者乘客闻到燃烧的气味或者看到冒烟，及时将车辆停靠旁边，离开车辆，是可以避免人身伤害的，所以在该场景中驾驶者对于此危害有一定的可控性。严重度、暴露度和可控性的判断如表 3 所示。

表 3 电池管理系统危害分析与风险评估示例

Table 3 Example of BMS hazard analysis and risk assessment

整车层面危害	系统层面的影响	可能的原因	危害场景	严重度 S	暴露概率 E	可控性 C	ASIL 等级
非预期的释放热能导致燃烧或明火	电池包释放热能导致燃烧或明火	电芯电压升高直至过充，电芯或者电池高阻抗引起过温，导致热失控甚至热扩散以及排气，引起电池包冒烟、起火以及化学物质泄露 电池包过流甚至短路导致热失控或者热扩散以及排气，引起电池包冒烟、起火以及化学物质泄露 其他电芯设计失效或者缺陷导致的电芯内短路引起热失控或者热扩散，引起电池包冒烟。起火以及化学物质泄漏	车辆正常行驶在高速公路时	S3	E4	C2	C
			晚上在住所或者住所附近进行无人看管的充电	S3	E4	C3	D/C
			高速行驶时发生碰撞	S3	E2	C3	B
			车辆进行高压系统维修时	S3	E2	C3	B

对于纯电动汽车晚上在住所或者住所附近进行无人看管的充电是经常会发生的情形，此时如果在住所或者附近充电导致起火，人员在熟睡的过程中，可能无法对该危害进行回避，即评判为 ASIL D，但是考虑到中国国情，车库与住所连在一起的住房情

况并不多见，城市中大多位于地下车库或者路面停车位，即整车级危害起火最高等级可定义为 ASIL C。

2.4 电池管理系统安全目标

根据上述电池管理系统危害分析与风险评估，电池管理系统应该在车辆正常行驶、充电时、发生车辆碰撞和维修时都应该对电池系统进行合理的充电管理，以避免出现电池过充、过流和过温，导致起火的危害。根据不同场景，归纳电池管理系统的安全目标如下，其中 ASIL 等级取分析的危害事件中最高的 ASIL 等级，表 4 给出了电池管理系统安全目标的示例。

表 4 电池管理系统安全目标示例

Table 4 Security objectives example of BMS

No.	系统层面失效	安全目标	ASIL
1	过充	防止电池过充,导致热失控	C
2	过放后再充电	防止电池过放后再充电,导致热失控	C
3	过温	防止电池过温,导致热失控	C
4	过流	防止电池过流,导致热失控	C

3 电池管理系统功能安全要求

根据上节中电池管理系统安全目标得出 BMS 功能安全要求，并且将这些安全要求分配给 BMS 初始架构中不同要素。

3.1 电池管理系统安全要求

对于电池管理系统来说，为了避免电池系统过充、过放后再充电、过流、过温，对动力蓄电池进行合理的充放电管理是主要的安全要求，针对电池系统安全目标，不考虑控制系统以外的独立的保护措施。

根据电池管理系统架构，提出电池管理系统功能安全要求。对于电池管理系统的功能安全要求考虑如下几个要素：故障探测或者失效减轻；故障或者失效的仲裁逻辑；系统的安全状态；系统故障容错时间。表 5 给出了电池管理系统安全要求的示例。

表 5 电池管理系统功能安全要求示例

Table 5 Example of BMS functional safety requirement

No.	系统层面失效	安全目标	ASIL	安全要求
1	过充	防止电池过充，导致热失控	C	BMS 应监测电芯电压，当电芯电压值超过安全阀值时，使电池系统在 FTTI 时间内进入安全状态
2	过放后再充电	防止电池过放后再充电，导致热失控	C	BMS 应监测电芯电压，当电芯电压值低于安全阀值时，使电池系统在 FTTI 时间内进入安全状态
3	过温	防止电池过温，导致热失控	C	BMS 应监测电芯温度，当电芯温度值超过安全阀值时，使电池系统在 FTTI 时间内进入安全状态
4	过流	防止电池过流，导致热失控	C	BMS 应监测电池系统电流，当电流值超过安全阀值时，使电池系统在 FTTI 时间内进入安全状态

4 总结与展望

电动汽车保有量快速增长所带来的电动汽车安全事故受到了国内外广泛关注，为确保安全，国际和国内分别从标准和法规角度针对车辆电控系统提出了功能安全要求。本文基于典型的电动汽车用电池管理系统(BMS)架构，利用 HAZOP 分析方法以及国家标准 GB/T 34590-2017《道路车辆 功能安全》给出的方法论，开展电池管理系统危害分析与风险评估，提出了电池管理系统的功能安全目标和功能安全要求，为国家标准 GB/T《电动汽车用电池管理系统功能安全要求及试验方法》的制定以及规范和提升电池管理系统行业技术水平，促进电动汽车整车安全提供了参考借鉴。

参考文献

[1] GB/T 34590-2017《道路车辆 功能安全》[S].

收稿日期：2018-11-21

作者简介：

李　波，男，博士，高级工程师，研究方向为汽车电子标准化;

付　越，男，硕士，工程师，研究方向为汽车电子标准化;

周　荣，男，硕士，教授级高级工程师，研究方向为电动汽车标准化。