储能储能标准与规范

编者按：储能技术的大发展亟需各种相关标准和规范，但是我国在这方面的工作还需发展和完善，鉴于此，本刊自2019年设立了“储能标准与规范”栏目，目的是改善我国储能技术研究实验和数据分析不规范的问题，栏目主编为中国科学院物理研究所李泓研究员。该栏目内容包括“基础科学实验规范”和“产业技术标准与规范”。“基础科学实验规范”方面，将介绍实验原理，推荐实验流程，样品准备条件，推荐实验设备，数据分析方法，数据可能获得的结论和意义；“产业技术标准与规范”方面，将介绍我国在锂电池及其它储能技术方面制定的标准和规范方面的具体内容、要点。文章以约稿为主，接受自由来稿，期待您的参与！**本栏目得到北京卫蓝新能源科技有限公司及天目湖先进储能技术研究院的大力支持！**

锂离子电池储能系统BMS的功能安全分析与设计

朱伟杰[1]，史尤杰[2]，雷 博[2]

（[1]深圳市科陆电子科技股份有限公司储能研发中心，广东 深圳 518057；[2]直流输电技术国家重点实验室（南方电网科学研究院），广东 广州 510663）

摘 要：近两年，中国储能产业迎来爆发式增长。相较于其他储能技术，由于生产技术的快速进步、制造成本的逐步下降等因素，锂离子电池具备更显著的竞争力，在储能领域的市场渗透率越来越高。作为对电池进行监控和管理的电子装置，电池管理系统（battery management system，BMS）是储能系统的核心部件之一，其功能安全关系到整个锂离子储能电站的安全稳定运行。为了正确高效地实现储能系统的电池管理系统功能安全设计和验证，针对锂电池储能系统BMS的产品特点，本工作从系统的危险识别和风险分析、整体安全要求确定和安全功能分配、安全完整性实现及验证3个主要分析步骤，参照IEC 61508、IEC 60730-1等相关参考标准梳理了电池储能系统BMS功能安全的分析与设计过程。分析结果表明，选择失效模式影响和诊断分析（FMEDA）以及风险矩阵法（RM），可靠性框图法（RBD），适合于储能系统电池管理系统BMS的功能安全分析和设计。依照IEC 61508、IEC 60730-1等相关标准，结合储能系统产品的特点，选择正确的分析设计路径，可以确保储能系统BMS的功能安全完整性等级（SIL）有效达成，为储能电站设计开发者提供参考。

关键词：电池储能系统；电池管理系统；功能安全；功能安全完整性等级

doi：10.19799/j.cnki.2095-4239.2019.0177

中图分类号：X 956 **文献标志码：**A **文章编号：**2095-4239（2020）01-271-08

Functional safety analysis and design of BMS for lithium-ion battery energy storage system

ZHU Weijie[1], *SHI Youjie*[2], *LEI Bo*[2]

([1]Energy Storage R&D center of Shenzhen Clou Electronics Co., Ltd., Shenzhen 518057, Gunagdong, China; [2]State Key Laboratory of HVDC (Electric Power Research Institute, China Southern Power Grid), Guangzhou 510663, Gunagdong, China)

Abstract: During the previous two years, China's energy storage industry has witnessed explosive growth. Compared with other energy storage technologies, lithium-ion batteries are more competitive

收稿日期：2019-08-02；**修改稿日期：**2019-08-27。
基金项目：国家重点研发计划项目（2018YFB0905300）。

第一作者及联系人：朱伟杰（1977—），男，工程师，研究方向为储能技术，E-mail：zhuweijie@szclou.com。

due to rapid advances in production technology and a gradual decline in manufacturing costs, and the market penetration rate in the field of energy storage is continuously increasing. As an electronic device for monitoring and managing a battery, the battery management system (BMS) is the core component of an energy storage system. Its functional safety is related to the safe and stable operation of an entire lithium-ion battery power station. To accurately and efficiently implement the design and verification of function safety in the BMS of the energy storage system, the analysis and design of a BMS to achieve functional safety, which is primarily described through system hazard identification and risk analysis, overall safety requirements and safety function allocation, and safety integrity verification, are outlined by incorporating the characteristics of a lithium-ion battery energy storage system BMS according to IEC 61508, GB/T 20438, and other related reference standards. The analysis shows that the failure mode effects and diagnostic analysis, the risk matrix, and the reliability block diagram are suitable for the functional safety analysis and design of the BMS of the energy storage system. Based on the IEC 61508 and IEC 60730-1 standards, combined with the characteristics of the energy storage system, an accurate analysis design ensures that the functional safety integrity level of the energy storage system BMS is effectively achieved. These provide a reference for the design and development of the energy storage power stations.

Key words: battery energy storage system; battery management system; functional safety; functional safety integrity level

近年来全球储能行业迅猛发展，由于具有放电倍率大、能量密度和体积密度高等优势，相较于其他种类的电化学储能技术，锂离子电池的累计装机规模最大，在全球电化学储能中的占比为86.3%[1]。然而，伴随着锂离子储能应用的爆发式增长，其暴露出的储能安全问题也日益突出，安全已成为行业发展最受关注的指标。2018～2019年期间，仅韩国就发生了23起储能电站起火事件，根据韩国政府公布的事故调查结果，电池系统缺陷、针对电冲击的保护体系不周以及储能集成系统管理欠缺是造成事故的三个重要原因[2]。作为对电池进行监控和管理的电子装置，电池管理系统（battery management system，BMS）被公认为是储能系统的核心部件之一，也与上述造成韩国储能电站火灾事故的三个原因息息相关，因此BMS的功能安全设计对锂离子储能系统的安全至关重要。

IEC 61508是出台最早、应用最广泛的功能安全国际标准，为电气/电子/可编程电子部件（E/E/PE）构成的安全相关系统规定了功能安全周期和基础评价方法。随后国际标准化组织基于IEC 61508制定了道路车辆功能安全国际标准ISO 26262，目前已有不少厂家和国内外学者基于ISO 26262标准充分研究了电动汽车BMS中的功能安全概念设计、评估和验证[3-8]，但由于汽车产品的运行环境和安全需求与储能电站领域的相差甚远，所以ISO 26262国际标准以及上述相关研究成果并不适用于储能系统BMS功能安全分析设计。另外，国际储能标准IEC 62619及ANSI/CAN/UL-1973均明确要求储能BMS需参照进行功能安全评估[9-10]，然而需要厂家根据产品自身特性从中选择合适的方法来实现功能安全设计与评估，所以上述标准在储能BMS的应用仍有一定难度。在储能系统功能安全领域，国外已有UL（Underwriter Laboratories Inc.）、CSA（Canadian Standards Association）、TUV（Technischer überwachüngs Verein）等几家相关认证机构，哥伦比亚的Bureau Veritas已对工业应用的电池进行功能安全认证工作[11]，但罕有系统性研究成果报道。而国内目前仍缺乏储能系统功能安全的认证机构，鉴于锂离子电池储能电站的消防安全风险也是最近几年才集中突现并受到关注，其研究工作更是相对落后。

针对锂离子电池储能系统BMS产品特点，本文依照相关参考标准梳理了BMS功能安全的分析与设计过程，为储能电站设计开发者提供参考。

1 BMS功能安全要求简述

根据IEC 61508-4的定义，功能安全（functional safety）是指整体安全中与受控设备

（equipment under control，EUC）和EUC控制系统相关的部分，它取决于E/E/PE安全相关系统和其他风险降低措施正确执行其功能[12]。要实现特定的安全相关系统，就必须有相应的安全功能（safety function）实现。所谓安全功能，是指针对特定的危险事件，为实现或保持EUC的安全状态，由E/E/PE安全相关系统或其他风险降低措施实现的功能。对于储能电池系统，充放电控制或保护设备是EUC，电池管理系统BMS是E/E/PE安全相关系统，需要对电池系统进行安全保护。

IEC 61508所规定的安全生命周期大致可分为分析、设计、实现和操作维护几个阶段[13]。本文主要研究储能BMS安全相关系统的分析和设计，这两个阶段主要包括以下内容：

（1） 系统分析，即确定系统的功能、结构和范围；

（2） 危险识别和风险分析，即对每个可能出现的危险事件进行分析和评估；

（3） 确定整体安全要求，并对必要的危险事件进行安全功能的分配；

（4） 安全完整性实现并验证。

实现和操作维护两阶段具体包括整体安装调试、整体安全确认、整体运行维护和修理、退役或处置、整体修改和改型等过程，由于不是本文重点，下文将不再重点介绍。

2　系统分析

尽管IEC 61508并没有明确要求必须将安全相关系统的设计与非安全相关系统的设计分开，但出于独立性要求以及便于评估等方面考虑，在实施过程中一般尽量将上述两个过程分开。

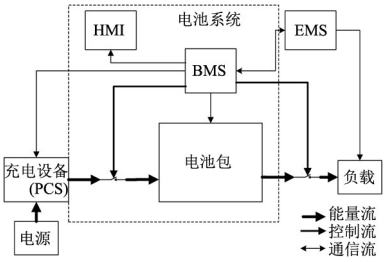

图1　电池系统-BMS监控的交互模块框图

Fig.1　Interactive block diagram with battery system -BMS monitoring

本阶段的目的是说明目标产品的控制功能、应用环境、可能出现的危害和危险以及需要遵守的安全法规。本阶段可明确储能系统BMS的控制范围、实际包含设备、外部事件、事件类型和其他相关设备系统等，可得出如图1所示的电池系统BMS的交互模块框图，其中HMI是人机接口，EMS是能量管理系统。

3　危险识别和风险分析

系统分析工作完成后，可根据输出的系统分析文档和确定的系统范围，开展BMS危险识别和风险评估工作。在本阶段，失效模式及影响分析（failure mode and effect analysis，FMEA）是一种较为有效和常用的风险分析方法。另外，当需考虑BMS对风险的侦查能力时，也可采用失效模式、影响及其诊断分析（failure modes effects and diagnostic analysis，FMEDA）方法完成对最终数据

表1　电池系统可能的危险事件

Table 1　Potentially hazardous events in battery system

序号	危险事件名称	来源	相关安全功能
1	释放可燃、有毒或爆炸性气体	电池化学反应	有害气体监测功能 报警功能 通风控制功能
2	流出可燃、有毒或腐蚀性液体	电池化学反应	流出液体监测 报警功能
3	热失控	电池化学反应	通过结构设计进行防护
4	电芯着火或爆炸	电池化学反应	消防启动功能
5	电芯过热	电池化学反应	过温保护功能
6	电池内短路	电池	电流监测功能
7	电池内阻超出	电池	在线内阻监测功能 报警功能

续表

序号	危险事件名称	来源	相关安全功能
8	外短路	PCS 或线缆	过流保护 +熔断器(不属于功能安全)
9	地震事件	外部环境	固定、机械强度(不属于功能安全)
10	外部火灾	外部环境	外壳防护(不属于功能安全)
11	滴水	外部环境	外壳防护(不属于功能安全)
12	跌落	外部环境/人为	外壳防护(不属于功能安全)
13	电池由于电池架倒塌受到挤压	外部环境或人为因素	固定(不属于功能安全)
14	操作人员失误	人员	输入防错功能
15	其他人为故意行为	人员	输入安全密码控制功能
16	失去温度控制	BMS	过温保护功能
17	失去电池电压控制功能	BMS	过压保护功能
18	由于失去控制功能或接地故障发生的过放电	BMS	绝缘故障检测功能 状态监测功能 主接触器控制功能
19	由于失去控制功能或数据漂移或软件错误发生的过充电	BMS	状态监测功能 主接触器控制
20	过放后充电	外部指令或人为误操作	状态监测功能 主接触器控制功能
21	BMS 控制线故障	BMS/外部环境	状态监测功能 主接触器控制功能
22	BMS 通信中断、错误	BMS/EMS	通讯监测功能
23	电击	外部环境/绝缘故障	接地保护 绝缘故障监测功能 报警功能

表 2 FMEA 分析表格

Table 2 FMEA analysis

组件名称			电池管理单元 BMU					
元件编号	元件名称	功能	失效率(单位：fit)(10^{-9})	失效模式	占比	影响	失效类型	诊断覆盖率
R8	薄膜贴片电阻	8.5 V 电源输出电压调节	0.21485524	开路	100%	无影响	S	
R10	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R12	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R13	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R14	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R16	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R35	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R40	薄膜贴片电阻		0.002933952	开路	100%	主电源失效，BMU	D	60%
R109	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R110	薄膜贴片电阻		0.002933952	开路	100%	无影响	S	
R111	薄膜贴片电阻		0.002933952	开路	100%	主电源失效，BMU	D	90%
R117	薄膜贴片电阻		0.002933952	开路	100%	主电源失效，BMU	D	60%
R118	薄膜贴片电阻		0.002933952	开路	100%	主电源失效，BMU	D	90%

续表

组件名称		电池管理单元BMU					
R142	薄膜贴片电阻	0.002933952	开路	100%	主电源失效，BMU	D	60%
R145	薄膜贴片电阻	0.002933952	开路	100%	主电源失效，BMU	D	60%
R108	薄膜贴片电阻	0.002859009	开路	100%	主电源失效，BMU	D	60%
R155	薄膜贴片电阻	0.002859009	开路	100%	主电源失效，BMU	D	60%
填写依据或说明		MIL-HDBK-217F-Notice2及实际电路影响因子分析		IEC 61709附录A		S：安全失效，失效导致；D：危险失效	高：99% 中：90% 低：60%

的整理分析。

FMEA的基本步骤为：

（1） 列出所有部件；

（2） 对每个部件，列出所有已知失效模式；

（3） 对每个部件/失效模式，列出对更高层面上的影响；

（4） 对每个部件/失效模式，列出影响的严重性/危险程度。

IEC 60812规定了FMEA详细的设计过程，其附录Table F.9提供了FMEA在一个安全相关控制系统中的应用实例[14]。需要注意的是，该方法可以分层分子系统进行套用，使用时需按照系统的复杂度对分层分子系统进行逐个自下而上地完成分析。

元器件的失效模式和失效率数据可以从器件手册、用户现场反馈可信数据、先验手册等来源获取，本文更加推荐前两种数据来源。此外，目前较常见的先验手册有以下几种：

（1） MIL-HDBK-217F：美军电子设备可靠性预计手册，由美国国防部发布，主要针对军用等级元器件[15]；

（2） Telcordia Bellcore SR-332：可靠性测试标准，由Telcordia Technologies的Bellcore（贝尔通信实验室）发布，在电信设备、医疗设备、电源灯商用电子产品中广泛应用[16]；

（3） IEC 61709：该标准提供了电子元器件可靠性预计的公式方法、失效模式及其分配比例等[17]；

（4） Siemens SN 29500：由Siemens发布的电子和机电元件可靠性预测的标准，可视为对IEC 61709的补充。

针对固定式储能系统，本文给出如表1所示的电池系统可能发生的危险事件列表。

针对识别的风险对每个功能安全相关部件进行FMEA分析，输出分析结果，见表2。

4　整体安全要求确定及安全功能分配

整体安全要求确定环节是指为达到所要求的功能安全，根据整体安全功能要求和整体安全完整性要求，为每一个危险件建立起对应的安全功能，并对每个安全功能规定安全完整性等级要求SIL，形成整体安全要求规范。安全功能分配环节是指将整体安全要求规范中的安全功能分配至E/E/PE安全相关系统和其他风险降低措施中。IEC 61508-1的7.5和7.6章节提供了整体安全要求和分配的详细执行要求[13]。

对各个安全功能进行安全完整性等级SIL目标确定是本阶段的一个核心工作。IEC 61508-5附录B提供多种危害分析方法，如常用的有风险图法、危险事件严重性矩阵、保护层分析（layer of protection analysis，LOPA）等[18]。下文以防电击安全功能为例，采用危险事件严重性矩阵，说明如何进行安全完整性等级SIL的确定。由表1可知，防电击安全系统由两部分：①BMS安全功能部分，具体分为绝缘故障监测和报警两个子功能，分别记为SF1-1、SF1-2；②电气安全措施部分，将电池包外壳进行接地保护。由于上述两部分安全措施是相对独立的，互不影响其功能的执行结果，因此独立的安全功能数量为2。假设项目团队对此危险事件的出现概率评估为中等可能性，严重性等级评估为严重的，则根据图2所示的危险事件严重性矩阵（摘自IEC 61508-5附录G）[18]，BMS安全功能SF1

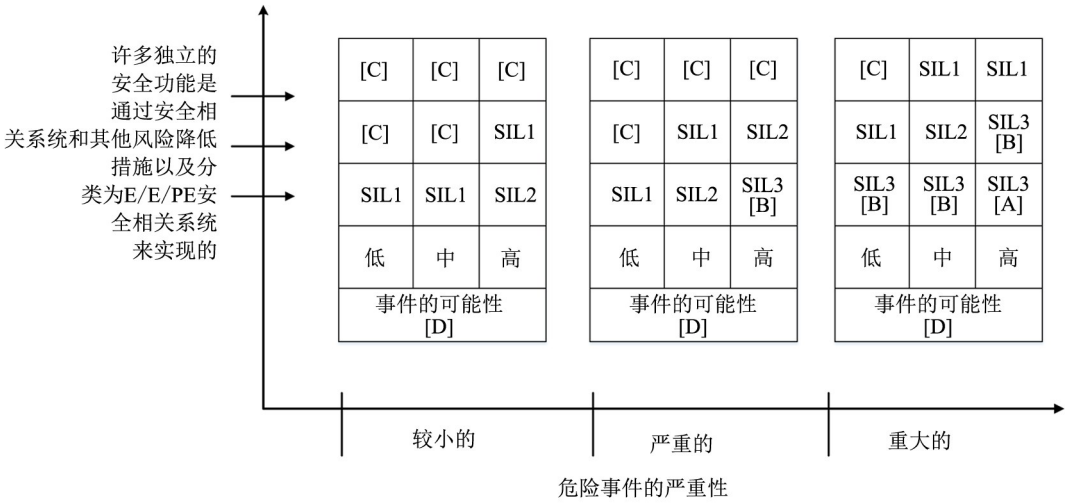

图 2 危险事件严重性矩阵

Fig.2 Hazardous event severity matrix

的安全完整性等级SIL应是SIL1。

根据IEC 61508规定，安全系统的运行模式分为低要求模式、高要求模式和连续模式三种。储能系统中的BMS执行安全功能的次数每年超过一次，属于高要求模式，因此其安全功能的需求失效概率应采用每小时危险失效平均频率PFH指标，可根据表3（摘自IEC 61508-1）确认BMS各安全功能的安全完整性等级及要求指标[13]。

表 3 安全完整性等级——在高要求或连续运行模式下安全功能目标失效量

Table 3 Safety integrity levels-target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

安全完整性等级(SIL)	安全功能的每小时危险失效平均频率(PFH)
4	$\geqslant 10^{-9}$ 且 $<10^{-8}$
3	$\geqslant 10^{-8}$ 且 $<10^{-7}$
2	$\geqslant 10^{-7}$ 且 $<10^{-6}$
1	$\geqslant 10^{-6}$ 且 $<10^{-5}$

对BMS中的各个针对危险事件的安全功能进行逐个评估后，综合得出BMS的安全完整性等级目标。

通过本阶段，项目团队可形成整体功能安全要求说明书，以及系统、软件、硬件安全功能分配说明书。

5 安全完整性实现及验证

5.1 软件安全完整性实现与验证

IEC 61508-3针对软件安全完整性有详细的规定要求，包括软件安全要求规范、系统安全软件方面的确认计划、软件设计和开发、可编程电子集成、软件操作和修改规程、软件相关的系统安全确认、软件修改、软件验证以及软件安全功能评估等内容[19]。考虑到IEC 61508是针对电气/电子/可编程设备的通用安全标准，实际BMS研发过程中软件功能安全等相关内容多是参考标准IEC 60730-1附录H进行。

5.1.1 软件架构要求

IEC 60730-1附录H提供了电子控制的软件架构要求[20]。根据分类要求，储能电站BMS应属于B类软件，此类软件控制功能具有以下架构之一：

（1） 带功能测试的单通道；

（2） 带周期性自测的单通道；

（3） 不带比较的双通道。

软件设计过程中，对于有功能安全要求的软件模块需注意选择合适的架构。

5.1.2 故障/错误应对措施

IEC 60730-1附录H表H.1针对不同的软件故障提供了相应的可接受应对措施，需要软件设计人员注意区别应用[16]。例如，针对变量存储故障，B类软件可采取的措施有周期性静态存储测试、带单比特位冗余的字保护、CPUs冗余比较、带比较的冗余存储或周期性自检以及带多比特位冗余的字保护等。

5.1.3 避免错误的措施方法

请参考IEC 60730-1附录H推荐的V型模型进

行软件开发流程管理[20]。

5.2　硬件安全完整性实现与验证

5.2.1　架构约束验证

硬件安全完整性架构约束可以通过以下两条路线进行验证：

路线1：基于硬件故障裕度和安全失效分数的概念；

路线2：基于由最终用户反馈的元器件可靠性数据、对指定的安全完整性等级增强的置信度和硬件故障裕度。

由于最终用户反馈的元器件可靠性数据比较难以收集，目前普遍常用路线1进行验证。完成危险识别和风险分析，得出FMEDA报告后，需要对各组件的硬件安全失效分数SFF进行计算，如果失效率λ为常数，则计算的公式为

$$SFF=(\Sigma\lambda_S+\Sigma\lambda_{Dd})/(\Sigma\lambda_S+\Sigma\lambda_{Dd}+\Sigma\lambda_{Du})$$

式中，λ_S为安全失效率，λ_{Dd}为可侦测的危险失效率，λ_{Du}为不可侦测的危险失效率。关于硬件组件的诊断覆盖率和安全失效分数SFF的计算，可参考IEC 61508-2附录C，诊断覆盖率约束参考附录A表A.2-A.14[21]。

5.2.2　硬件故障裕度和安全失效分数计算

IEC 61508标准按硬件复杂性将硬件分为以下两类：①A类，为复杂度低的类型，所有元器件组件的失效率数据都具有较为可信的数据；②B类，为复杂度高的类型，只要一个器件不具备可信的失效率数据都归属B类[12]。具有复杂逻辑运算单元的组件，例如DSP、MCU等一般归为B类。储能电站BMS一般都有一个或多个MCU，因此应按B类进行评估分析。需要说明的是，若采用的MCU符合IEC 61508认证的SIL2、SIL3等级，而剩余部件是低复杂度的电路，即符合IEC 61508-2的7.4.4.1.2，则可以按A类对剩余部件子系统完成评估后再与MCU子系统的SIL等级进行合并。

表4（摘自IEC 61508-2）所示为IEC 61508-2所提供的B类硬件安全完整性结构约束的计算数据[21]。根据FMEDA表格计算出组件的安全失效分数SFF，并通过风险分析得出SIL等级后，便可以通过表4确定需要的硬件故障裕度。

同样，若对已确定硬件故障裕度的组件，也可以通过表4核查是否符合需要的SIL等级。当各个子系统的SIL等级均确定后，按子系统的组合结构进行计算整体系统的SIL等级。IEC 61508-2附录C提供了相关示例，本文不再赘述。

表4　B类安全相关组件或子系统执行安全功能时的最大允许安全完整性等级

Table 4　Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

组件安全失效分数	硬件裕度		
	0	1	2
<60%	不允许	SIL1	SIL2
60%~<90%	SIL1	SIL2	SIL3
90%~<99%	SIL2	SIL3	SIL4
>99%	SIL3	SIL4	SIL4

IEC 61508-6附录B提供了硬件失效率评估技术示例[22]。每个安全功能需要单独计算E/E/PE安全相关系统的可靠性。分析方法要分为以下两类：

静态（布尔）和动态（状态/转移）模型，常见模型有可靠性框图、故障树、马尔科夫模型等；分析和蒙特卡洛仿真计算。

可靠性框图是较为简单可行的常见方法，下文将简述基于可靠性框图的量化硬件随机失效影响计算步骤，以供参考。

（1）作出如图3所示的安全系统的可靠性框图。

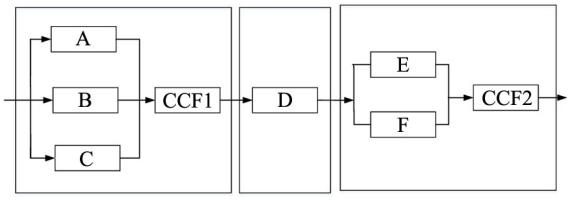

图3　完整安全回路的可靠性框图

Fig.3　Reliability block diagram of a whole safety loop

（2）根据图3所示的可靠性框图确定安全回路中的各子系统的结构类型（如1oo1、1oo2、2oo2等），确定共因失效模块CCFx及其共因因子β值。

（3）通过FEMDA表格分析各子系统中元件的失效率、失效模式、失效模式占比以及失效影响，得出个元件的失效类型（S、D）和诊断覆盖率DC，计算各子系统A～F的失效率λ_{DU}、λ_{DD}、λ_{SD}；

（4）按照IEC 61508-6附录B.3.3.2所提供的公式计算各个部分的PFH值[22]：①1oo1结构：$PFH_G=\lambda_{DU}$②1oo2结构：$PFH_G=2[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]$

（1−β）$\lambda_{DU}t_{CE}+\beta\lambda_{DU}$③2oo2 结构：$PFH_G=2\lambda_{DU}$

对于组件结构较为简单的应用，可以运用手工计算，而对于复杂结构的应用，需要采用专门的可靠性计算软件进行分析计算。计算结果若出现不符合 SIL 等级要求的组件，应采取相应的技术或管理措施进行风险降低。此过程需要根据现场反馈、用户需求多次反复各个步骤，进行循环改进。

6 结 语

BMS 是锂电池储能系统的核心部件之一，其可靠性和安全性是储能系统推广应用过程中关键性技术难题。基于国内外相关技术标准梳理以及实际工程经验，本文详细总结了 BMS 功能安全分析设计的具体过程和实用方法，具体包括系统分析、危险识别和风险分析、整体安全要求确定及安全功能分配、安全完整性实现及验证等环节。本文研究成果填补了国内关于储能系统锂电池 BMS 功能安全设计研究方面的空白，为电池系统的安全设计、安全验证、安全评估工程师提供参考，对我国储能电池系统的功能安全标准规范的研究和制定也有参考借鉴意义。本文所提供仅是其中一种可行方案，从业工程师需要根据储能系统的实际应用场景和各公司的能力进行合理选择。

参 考 文 献

[1] 中国能源研究会储能专委会, 中关村储能产业技术联盟. 储能产业研究白皮书2019[R]. 北京, 2019: 20.

[2] 北极星储能网. 电池不背锅!针对储能电站事故原因 韩国提出四大改善措施(附报告) [EB/OL]. [2019-6-13]. http: //chuneng. bjx. com. cn/news/20190613/985892. shtml.

[3] 彭忆强, 芦文峰, 邓鹏毅, 等. 新能源汽车"三电"系统功能安全技术现状分析[J]. 西华大学学报(自然科学版), 2018, 37(1): 54-61.
PENG Yiqiang, LU Wenfeng, DENG Pengyi, et al. Analysis of state of the art for new energy vehicle functional safety technologies[J]. Journal of Xihua University (Natural Science Edition), 2018, 37(1): 54-61

[4] 汪斌, 刘宁, 王家雁, 等. 纯电动车锂电池管理系统的应用浅析[J]. 汽车实用技术, 2014(1): 52-55.
WANG Bin, LIU Ning, WANG Jiayan, et al. Application analysis of lithium battery management system of pure EV[J]. Automobile Applied Technology, 2014(1): 52-55.

[5] 苏志高. 插电式混合动力汽车电池管理系统的设计与实现[D]. 成都: 电子科技大学, 2015.
SU Zhigao. Design and implementation of plug-in hybrid electric vehicle battery management system[D]. Chengdu: University of Electronic Science and Technology of China, 2015.

[6] SAGAR S T. Compliance of ISO 26262 safety standard for lithium ion battery and its battery management system in hybrid electric vehicle[C]// 2017 IEEE Transportation Electrification Conference (ITEC-India), Pune, 2017: 1-5.

[7] JIHAS K. ISO 26262 system level functional safety validation for battery management systems in automobiles[C]//2017 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, 2017: 1-5.

[8] WANG Yang, LI Yanwen, LI Chunshu, et al. Analysis and application of functional safety based on modified FMEA method[C]//2017 2nd Asia-Pacific Conference on Intelligent Robot Systems (ACIRS), Wuhan, 2017: 98-103.

[9] International Electrotechnical Commission. Secondary cells and batteries containing alkaline or other non-acid electrolytes − Safety requirements for secondary lithium cells and batteries, for use in industrial applications: IEC 62619[S]. 2017.

[10] American National Standards Institute, Standards Council of Canada. Batteries for use in stationary, vehicle auxiliary power and light electric rail (LER) applications: ANSI/CAN/UL-1973[S]. 2018.

[11] BUREAU VERITAS COLOMBIA. Functional and safety guide for battery management system (BMS) assessment and certification[EB/OL]. [2019-08-25]. http: //www. bureauveritas. com. co/vvxSBsos/GuideBMS_V0+2014. pdf.

[12] International Electrotechnical Commission. Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 4: Definitions and abbreviations: IEC 61508-4[S]. 2010.

[13] International Electrotechnical Commission. Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 1: General requirements: IEC 61508-1[S]. 2010.

[14] International Electrotechnical Commission. Failure modes and effects analysis (FMEA and FMECA): IEC 60812[S]. 2018.

[15] Department of Defense, United States of America. Military handbook - reliability prediction of electronic equipment: MIL-HDBK-217F[R]. 1991.

[16] Telcordia Technologies Special Report. Reliability prediction procedure for electronic equipment: Telcordia SR 332 issue 3[R]. 2011.

[17] International Electrotechnical Commission. Electric components − Reliability−Reference conditions for failure rates and stress models for conversion: IEC 61709[S]. 2017.

[18] International Electrotechnical Commission. Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 5: Examples of methods for the determination of safety integrity levels: IEC 61508-5[S]. 2010.

[19] International Electrotechnical Commission. Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 3: Software requirements: IEC 61508-3[S]. 2010.

[20] International Electrotechnical Commission. Automatic electrical controls —Part 1: General requirements: IEC 60730-1[S]. 2013.

[21] International Electrotechnical Commission. Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems: IEC 61508-2[S]. 2010.

[22] International Electrotechnical Commission. Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3: IEC 61508-6[S]. 2010.