ICS 43.080
T 47

团　　体　　标　　准

T/GDCKCJH 018—2020

电动汽车用动力电池管理系统功能安全评价技术

Functional safety evaluation technology of power battery management system for electric vehicles

2020 - 08 - 14 发布　　2020 – 09 - 01 实施

广东省测控技术与装备应用促进会　发布

目　　次

前　言

本标准的全部技术内容为推荐性。

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由广东省测控技术与装备应用促进会提出。

本标准由广东省测控技术与装备应用促进会归口。

本标准起草单位：广州广电计量检测股份有限公司、华南理工大学、广东省标准化研究院、深圳比克动力电池有限公司、广州汽车集团股份有限公司。

本标准主要起草人：陈明生、明志茂、刘桂雄、李远茂、黄继雄、安伟峰、符兴锋。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

引　言

本引言旨在介绍本标准的要求所依据的原则，理解这些原则对电动汽车用动力电池管理系统的功能设计和应用很有必要。需要注意的是，本标准仅考虑电动汽车用动力电池管理系统的功能安全评价方法，以提供对产品设计与评价的依据，不涉及电池管理系统的硬件和软件设计。

随着评价技术和功能的进一步发展必然会要求进一步修订本标准。

在标准范围内，确定电动汽车用电池管理系统的功能安全等级时采用何种评价方法，需遵守以下的优先次序：

——首先，如有可能，功能设计过程中应采用高于预期一个等级的安全完整性等级方案；

——其次，如果无法实行以上原则，那么需考虑设计多于一个的安全相关保护装置，以减少或消除危险发生的可能性；

——最后，无论采取何种体系划分方法、安全完整性等级划分方法，需对方法筛选进行阐述。

上述原则不能代替本标准的详细要求，只是让评价者了解这些要求所依据的原则。

电动汽车用电池管理系统的安全完整性等级与其硬件、软件设计及应用条件有关。其中应用条件包含了正常使用条件、可预见的误用条件和可预见的故障条件，还包括影响其安全的环境条件诸如温湿度、海拔等因素。

电动汽车用动力电池管理系统功能安全评价技术

1 范围

本标准规定了电动汽车用动力电池管理系统功能安全评价相关的术语及定义、功能安全评价要求。

本标准适用于装载在电动汽车上的锂离子电池管理系统和镍氢动力电池管理系统等功能安全评价。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19596-2017 电动汽车术语

GB/T 20438.5-2017 电气电子可编程电子安全相关系统的功能安全 第5部分：确定安全完整性等级的方法示例

GB/T 34590.9-2017 道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析

GB/T 38661-2020 电动汽车用电池管理系统技术条件

QC/T 897-2011 电动汽车用电池管理系统技术条件

IEC 61508-5 2010 电气、电子、程序可控的电子安全相关系统的功能性安全 第5部分：安全完整性水平的测定用方法实例（Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels）

ISO 26262-9-2018 道路车辆 功能安全 第 9 部分：以汽车安全完整性等级为导向和以安全为导向的分析（Road vehicles - Functional safety - Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses）

3 术语及定义

GB/T 19596界定的以及下列术语与定义适用于本文件。

3.1

动力电池管理系统 power battery management system

监视动力电池的状态（温度、电压、荷电状态等），可以为电池提供通信、安全、电芯均衡及管理控制，并提供与应用设备通信接口的系统。

3.2

电子电气系统 electrical and/ or electronic system

用于电动汽车的由电子/电气要素构成的系统，包括可编程电子要素。

3.3

受控设备 equipment under control; EUC

用于与电动汽车相关的设备、机器、装置或成套设备。

3.4

功能安全 functional safety

本标准指电动汽车用动力电池管理系统安全中与EUC和EUC控制系统相关的部分安全，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。

3.5

功能安全要求 functional safety requirement

定义了电动汽车用动力电池管理系统独立于具体实现方式的安全行为，或独立于具体实现方式的安全措施，包括安全相关的属性。

注1：功能安全要求可以是由安全相关的电动汽车用动力电池管理系统或基于其他技术的安全相关系统所执行的安全要求，目的是通过考虑确定的危害事件，使相关项达到或保持在安全状态。

注2：功能安全要求的定义可独立于电动汽车用动力电池管理系统开发概念阶段中使用的技术。

注3：安全相关的属性包括SIL等级信息。

3.6

保护层分析法 layer of protection analysis; LOPA

从电动汽车用动力电池管理系统危险识别中获得的数据作为出发点，对每个辨识出的危险通过记录初始原因和阻止或减轻危险的防护层来进行分析的方法。以此来确定风险降低的总量以及分析是否需要更多的风险降低。

3.7

动力电池系统 power battery system

一个或一个以上电动汽车用动力电池包及相应附件（电池管理系统、高压电路、低压电路、热管理设备以及机械总成）构成的、为电动汽车整车的行驶提供电能的能量存储装置。

3.8

安全 safety

没有不可接受的风险。

[ISO/IEC Guide 51-1999，定义3.1]

3.9

安全完整性 safety integrity

在规定的时间段内和规定的条件下，安全相关系统成功执行规定的安全功能的概率。

3.10

安全完整性等级 safety integrity level; SIL

一种离散的等级（四个可能等级之一），对应安全完整性量值的范围。安全完整性等级由高到低，安全完整性等级4是最高的，安全完整性等级1是最低的。

3.11

荷电状态 state of charge；SOC

当前电池中按照规定放电条件可以释放的容量占可用容量的百分比。

4 功能安全评价要求

4.1 评价原则

功能安全评价是寻求实现电动汽车用动力电池管理系统功能安全所需要的最低或必要成本，作为功能的目标成本。在动力电池管理系统功能安全评价工作中应遵循科学性、公正性、合法性和针对性原则。

4.2 一般流程

电动汽车用动力电池管理系统功能评价的一般流程如图1所示。

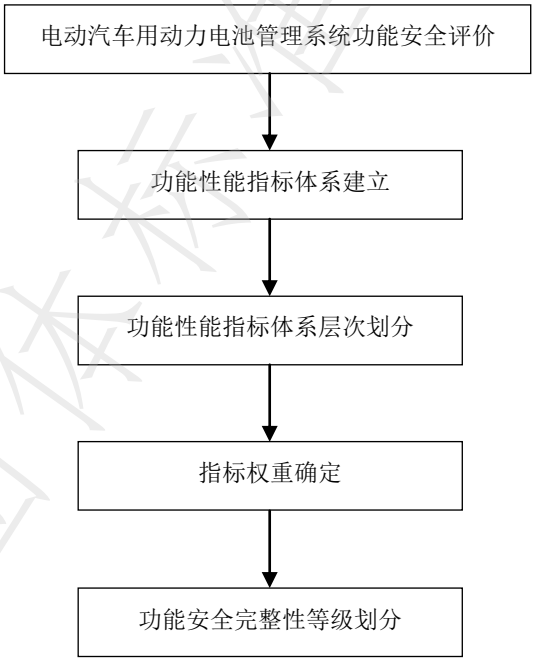


图1 功能安全评价流程示意

5 电动汽车用动力电池管理系统功能安全指标体系

电动汽车用动力电池管理系统功能安全指标体系及层次如表1所示。

表 1 电动汽车用动力电池管理系统功能安全指标体系及层次

序号	第一层次	第二层次	序号	第一层次	第二层次

1	测算与诊断性能	总电压测量精度	18	环境适应性	随机振动
2		总电流测量精度	19		机械冲击
3		单体（电芯组）电压测量精度	20		跌落
4		温度测量精度	21		低温性能
5		绝缘电阻测量精度	22		高温性能
6		SOC 估算精度	23		温度梯度
7		电池故障诊断	24		温度循环
8	绝缘性能	绝缘电阻	25		耐盐雾
9		耐电压性能	26		湿热循环
10	电气适应性能	直流供电电压	27	电磁兼容性	传导骚扰
11		过电压	28		辐射骚扰
12		叠加交流电压	29		电源线瞬态传导抗扰度
13		供电电压缓升和缓降	30		信号线/控制线瞬态传导抗扰度
14		供电电压瞬态变化	31		电快速瞬态脉冲群抗扰度
15		反向电压	32		辐射抗扰度
16		短路保护	33		静电放电
17	环境适应性	正弦振动	/	/	/

6 功能安全指标权重分配

6.1 指标权重分配方法

本标准优先采用主观赋权法中的层次分析法进行电池管理系统功能安全指标权重分配。主观赋权法在根据属性本身含义确定权重方面具有优势，但客观性较差。客观赋权法在不考虑属性实际含义的情况下，确定权重具有优势，但不能体现决策者对不同属性的重视程度，有时会出现确定的权重与属性的实际重要程度相悖的情况。综合赋权法为主观和客观赋权法的组合赋权方法，其算法与要求相对较高。应结合实际评价的系统复杂程度、预期工作量等要素选择适当的权重分配方法。

6.2 基于层次分析法的权重分配方法

6.2.1 方法流程

层次分析法的主要步骤如图 2 所示。具体示例见附录 B。

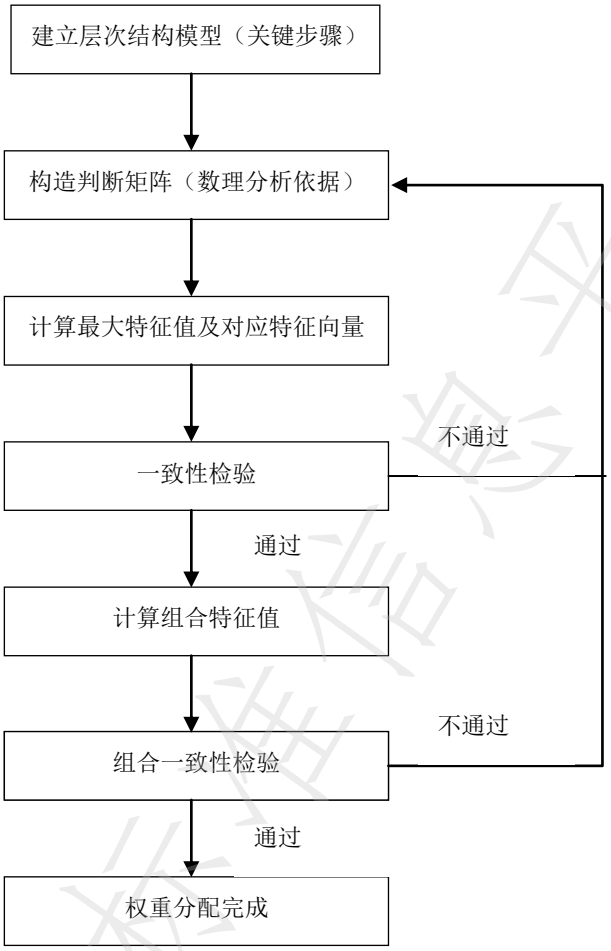


图2 层次分析步骤

6.2.2 层次结构

对于功能指标体系，单一层次的指标体系通常无法表达功能之间的关联特性，因此需要进行层次构建以便后续分析。常用的层次结构模型如图3所示。

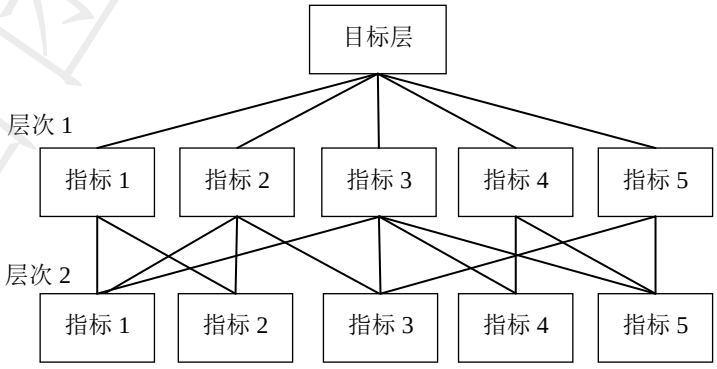


图3 层次结构模型示意

在构建层次体系模型后，就可以进行判断矩阵的构造以进行量化分析。针对两两指标的判断矩阵比例尺度如表 2 所示。

表 2 比例尺度

尺度	含义
1	两者的影响相同
3	前者比后者稍强
5	前者比后者强
7	前者比后者明显强
9	前者比后者绝对强
2、4、6、8	两者之比在上述两个相邻等级之间
1、1/2……1/9	两者之比为上述互为反数

6.2.3 一致性评判

计算一致性指标：

$$C.I.=\frac{\lambda_{\max}(\mathrm{A})-n}{n-1} \quad \cdots\cdots(1)$$

式中：

C.I.——一致性指标值；

$\lambda_{\max}$(A)——判断矩阵特征值；

n——判断矩阵阶数。

计算一致性比例：

$$C.R.=\frac{C.I.}{R.I.} \quad \cdots\cdots(2)$$

式中：

C.R.——一致性比例值；

R.I.——平均随机一致性指标。

其中，平均随机一致性指标 *R.I.*如表 3 所示。

表 3 随机一致性指标对照关系

n	1	2	3	4	5	6	7	8	9
R.I.	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45

当*C.R.*<0.1时，通常认为判断矩阵的一致性是可以接受的，否则应对判断矩阵做适当修正。

6.3 权重排序与分析

在统计理论和实践中,权重表明各个评价指标的重要程度。重要度排序通常有以下两种方法。数字法排序。用数字表明顺序，如 1 代表最重要，每个指标对应的数字就代表它的重要度顺序。变量名排序。在统计分析软件中根据重要性设置变量名，例如 a_1 表示最重要，a_2 表示次重要。本标准采用的是数字排序。

7 功能安全完整性等级划分

7.1 划分方法

7.1.1 基于风险图的定性划分方法

风险图方法，这是一种根据与电动汽车用动力电池的 EUC 和 EUC 控制系统相关的风险因素方面的

知识，确定安全相关系统的安全完整性等级的方法。这种方法可用于定性或定量。当采用这种方法时，为了简化，用一组参数，一起描述危险情况的性质。该组参数是当没有安全相关系统或其失效时的参数。从四个参数的每个参数组中选择一个参数，然后组合起选定的参数，用以确定分配到安全功能的安全完整性等级。

7.1.2 基于保护层分析的半定量划分方法

用保护层分析法（LOPA）分析危险并确定所需的安全功能，以及所需安全功能的完整性等级。应对 LOPA 方法进行调整以满足风险可接受准则。如果额外的风险降低是必需的而且如果是以 E/E/PE 安全相关系统的形式被提供，LOPA 方法能用来确定适当的 SIL。针对每一个危险，确定一个适当的 SIL 来将降低风险到可容忍的等级。

7.1.3 基于危险失效平均频率的定量划分方法

安全相关防护系统的危险失效平均频率可表达为：

$$P_{FH}=F_t/F_{np} \quad \cdots\cdots(3)$$

式中：

P_{FH}——危险失效平均频率；

F_t ——可容忍危险频率，数值上为使用寿命（小时数）的倒数；

F_{np} ——在没有额外的防护措施时的安全防护系统要求率。安全防护系统要求率是否已经实现了可容忍风险等级，需要通过事故风险分类进行确定。风险级别分为 4 个等级，风险等级 1 为无法容忍的风险；风险等级 2 为需要进一步研究后确定可容忍程度；风险等级 3 和风险等级 4 为可容忍风险。

7.2 安全完整性等级判定准则

下面列举了基于危险失效平均频率（定量划分法）的安全完整性等级判定准则。连续运行模式下的失效平均频率与安全完整性等级对应关系如表4所示。

表 4 失效平均频率与安全完整性等级对应关系

安全功能的每小时危险失效平均频率	安全完整性等级
[10^{-9}，10^{-8}）	4
[10^{-8}，10^{-7}）	3
[10^{-7}，10^{-6}）	2
[10^{-6}，10^{-5}）	1

附　录　A（资料性附录）电动汽车用动力电池管理系统典型结构与功能框架电动汽车用动力电池管理系统的组成

电池管理系统(Battery Management System, BMS)是电动汽车动力电池系统的重要组成。它一方面检测收集并初步计算电池实时状态参数，并根据检测值与允许值的比较关系控制供电回路的通断；另一方面，将采集的关键数据上报给整车控制器，并接收控制器的指令，与车辆的其他系统协调工作。电池管理系统的主要组成包括：电池终端模块（主要进行数据采集，如：电压参数、电流参数、温度、通信信号等）；中间控制模块（主要与整车系统进行通讯，控制充电机等）；显示模块（主要进行数据呈现，实现人机交互）。

A.2　电动汽车用动力电池管理系统的主要功能

为满足相关的标准或规范，BMS具备如下主要功能：

（1）电池参数检测。包括总电压、总电流、单体电压检测（防过充、过放和反极）、温度检测（单体和关键电缆接头温度）、烟雾探测（监测电解液泄漏）、绝缘检测（监测漏电）、碰撞检测等；

（2）电池状态估计。包括荷电状态、健康状态、功能状态、能量状态、故障及安全状态等；

（3）在线故障诊断。包括故障检测、故障类型判断、故障定位、故障信息输出等。故障检测是指通过采集到的传感器信号，采用诊断算法诊断故障类型，并进行早期预警。

（4）电池安全控制与报警。包括热系统控制、高压电安全控制。BMS诊断到故障后，通过网络通知整车控制器，并要求整车控制器进行有效处理（超过阈值时BMS可切断主回路电源）。

（5）充电控制。BMS中具有一个充电管理模块，它能够根据电池的特性、温度高低以及充电机的功率等级，控制充电机给电池进行安全充电。

（6）电池均衡。不一致性的存在使得电池组的容量小于组中最小单体的容量。电池均衡是根据单体电池信息,采用主动或被动、耗散或非耗散等均衡方式,尽可能使电池组容量接近于最小单体的容量。

（7）热管理。根据动力电池温度分布信息及充放电需求，决定主动加热/散热的强度，使得电池尽可能工作在最适合的温度，充分发挥电池的性能。

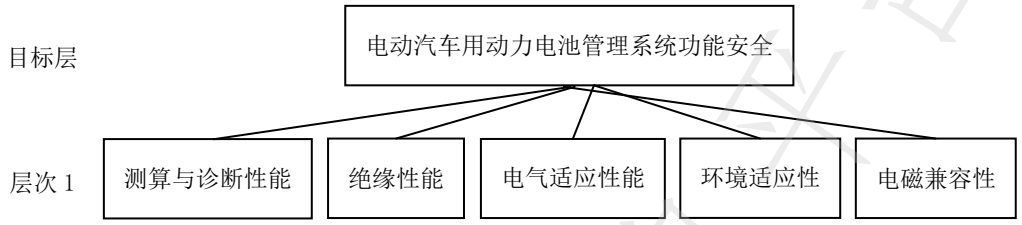
（8）网络通讯。BMS需要与整车控制器等网络节点通信；同时，BMS在车辆上拆卸不方便，需要在不拆壳的情况下进行在线标定、监控、升级维护等。

（9）信息存储。用于存储关键数据，如荷电状态和累积充放电容量值、故障码和一致性等。

（10）电磁兼容。要求BMS具有好的抗电磁干扰能力，同时要求BMS对外辐射小。

附　录　B 电动汽车用动力电池管理系统功能安全指标权重计算示例层次结构建模

以电动汽车用电池管理系统功能安全评价为目标层进行建模。如附图B.1所示。



图B.1 层次结构建模示意

B.2　构造判断矩阵

以设计准则层为例，包括5个准则，分别记为：测算与诊断性能B_1，绝缘性能B_2，电气适应性B_3，环境适应性B_4，电磁兼容性B_5。如表B.1所示。

表 B.1 判断矩阵

准则	B_1	B_2	B_3	B_4	B_5
B_1	1	3	1/7	1	1/3
B_2	1/3	1	1/5	1/2	1/2
B_3	7	5	1	5	3
B_4	1	2	1/5	1	1/2
B_5	3	2	1/3	2	1

B.3　权重计算、排序与一致性检验

通过计算得到的结果如表B.2所示。

表 B.2 准则层权重计算结果

参数	B_1	B_2	B_3	B_4	B_5	λ	*C.R.*	备注
权重	0.10653	0.06870	0.52106	0.10541	0.19830	/	/	/
权重重要度排序	3	5	1	4	2	/	/	/
特征值	/	/	/	/	/	5.2436	/	/
一致性检验	/	/	/	/	/	/	0.054381	应≤0.1

按照一致性检验要求可知，上述计算结果满足要求。其中，权重值最大的准则为电气适应性，最小值对应准则为绝缘性能。