# 《电动汽车安全指南》

（2019 版）

指导编制：

工业和信息化部

国家能源局

组织编制：

中国汽车工业协会

中国汽车动力电池产业创新联盟

中国电动汽车充电基础设施促进联盟

2019 年 10 月

# 《序言》

## 全国政协副主席、中国科协主席 万钢

世界汽车产业面临百年未遇之大变局，正在进入重大转型期。从市场角度看，汽车市场正在由少数发达国家为主，向以中国为首的发展中国家普及，市场规模将快速增长；从外部条件看，世界范围内的气候变化、环境污染和能源短缺正在成为制约汽车产业发展的重大因素；从内生动力看，新一轮科技革命，特别是电驱动相关技术、人工智能技术和互联网技术的迅猛发展正在为汽车产业的转型升级提供强大的技术支撑。在这场世界汽车产业的重大变革中，电动化、智能化、共享化成为最重要的发展方向。

习近平主席在 2014 年 5 月视察上汽集团时指出，新能源汽车技术研发能不能占领制高点，已经成为当今世界汽车产业的竞争焦点。汽车行业是市场很大，技术含量和管理精细化程度很高的行业，发展新能源汽车是我国从汽车大国迈向汽车强国的必由之路。要加大研发力度，认真研究市场，用活用好政策，开发适应各种需求的产品，使之成为一个强劲的增长点。习主席的重要指示，为我国新能源汽车发展绘制了蓝图，指明了方向。

在政府的积极作为、科技的支撑引领、巨大的市场规模、创新的商业模式共同作用下，我国新能源汽车产业取得显著的技术进步和快速的市场发展。目前正处于由导入期向成长期过渡的关键阶段，在全球产业体系中占据举足轻重的地位，引领和加速了全球汽车电动化、智能化、共享化的进程。

在当前市场成长的关键阶段，必须把安全作为新能源汽车最关键的指标，把提高新能源汽车安全性放在最重要的位置。新能源汽车的安全性，不仅是科学研究和产品设计问题，还与制造工艺、质量管控、零部件生产供应、产品使用、充电和维修保养等全产业链和全生命周期密切相关。因此，如何调动各方面的积极性，集聚全行业专家的智慧和经验，指导全行业全面提高新能源汽车的安全性，已成为当前最迫切的问题。

面对这个行业关键点，中国汽车工业协会、中国汽车动力电池产业创新联盟和中国电动汽车充电基础设施促进联盟组织全行业专家，编制了这本《电动汽车安全指南》，非常及时，非常重要。我相信，这本指南将对提高我国新能源汽车安全性，促进我国新能源汽车健康发展起到重要作用。希望产业界用好这本指南，并不断从实践中积累经验，充实完善各章节内容，群策群力，共同提高我国新能源汽车的质量和水平。希望中国汽车工业协会等组织编制单位，继续做好本项工作，不断汇总行业技术进步经验，逐年更新和修订这本指南，集众智、汇群力，为全行业提高质量发展贡献力量。

# 《前言》

## 中国汽车工业协会常务副会长兼秘书长 付炳锋

在当前汽车动力电动化的转型过程中，安全性是最重要的指标。本指南 2018 版沿电动汽车产业链和生命周期，将电动汽车安全性分成电动乘用车安全、电动客车安全、电池单体和模组、电池管理系统、电机与电控、充电安全、数据监控管理、维修保养、动力蓄电池回收再利用、安全事故处理、操作安全、运营车辆安全管理等 12 个方面，汇聚了全行业在一线工作的上百名专家意见。鉴于氢燃料电池汽车已进入小批量市场运营阶段，本指南 2019 版补充了氢燃料电池汽车安全方面的内容。

在政府规划指导、多项政策促进和全行业的共同努力下，中国的电动汽车发展正走在世界前列，发挥着引领作用。电动汽车各项技术日渐成熟，市场高速增长，产业化初期的安全性已成为当前中国电动汽车发展最突出的问题。电动汽车的安全性，涉及产品开发与制造、使用与充电、维修与保养等全产业链和全生命周期。因此，中国汽车工业协会、中国汽车动力电池产业创新联盟和中国电动汽车充电基础设施促进联盟组织全行业主要企业、机构、院校等专家编制了本指南。

本指南采取了尽量细化、具体化的原则，突出可操作性，指南 2019 版还增加了 4 项相关规范条件，作为附录一并纳入，以使本指南有较强的实际指导作用。当然，本指南是迄今为止的经验总结，随着产业化的不断深入，市场应用的进一步普及业界同仁的新经验、新认识、新发展将会在本指南后续版本中得以体现。

安全性是各国发展电动汽车面临的共同问题。中国电动汽车的推广应用先走了一步，遇到了很多在世界其他国家还没遇到问题，积累了一些独到的经验。因此，本指南对于世界其他国家的电动汽车发展，也应有很好的借鉴作用。所以，我们决定，公开发布本资料，放弃所有版权，同时发布中文版本和英文版本，供各国同行参考。

最后，向所有参加本资料编制的专家，致以最崇高的敬意！感谢你们在紧张工作之余，无私地奉献自己的经验智慧和宝贵的时间！

# 编制说明

## 一、编制背景

按照党中央国务院关于发展新能源汽车的总体部署，在国务院《节能与新能源汽车产业发展规划（2012－2020 年）》（国发〔2012〕22 号）和《关于加快新能源汽车推广应用的指导意见》（国办发〔2014〕35 号）、《关于加快电动汽车充电基础设施建设的指导意见（国办发〔2015〕73 号）》等文件的指导下，在鼓励新能源汽车推广应用的各项政策措施的推动下，中国电动汽车的推广应用取得了积极的进展，轻量化、动力驱动系统、动力电池等关键零部件产业初步形成规模，与世界先进水平的差距明显缩小。

但是，我们也看到我国电动汽车总体发展质量和水平还有待提高，特别是车辆安全性水平亟待提高，目前，产业总体上对安全性认识不足，产品设计的安全性要求积累不够，全链条中安全交互的机制没有形成，导致多起电动汽车起火事故发生，对产业发展造成负面影响。

电动汽车安全性事故的原因比较复杂，与材料选择、电芯和模块结构、系统集成、连接结构、整车匹配设计、生产管控、产品试验验证、售后服务、充电设备和工程电子、充电运维管理、回收再利用过程安全管理、火灾管控方法等多种因素有关。因此，2018 年汽车工业协会会同中国汽车动力电池产业创新联盟、中国电动汽车充电基础设施促进联盟启动了《电动汽车安全指南》（《指南》）编制工作，系统地梳理设计、制造、使用、再利用各个环节的安全风险及其防范措施，旨在促进全产业链加强安全意识，提高电动汽车全生命周期安全性水平。

本次发布的《指南（2019 版）》在 2018 版基础上进行了修订完善。

## 二、《指南》的定位

本《指南》从电动汽车全产业链条和全生命周期入手，梳理电动汽车的各种安全风险，参考现有国际国内相关标准，汇集一线专家的经验编制而成，目的是给从事电动汽车开发和生产企业从业人员，以及服务保障人员和广大消费者进行指导和提供参考。

希望通过本《指南》的研究制定及发布，提高全行业对电动汽车安全性的认知，提高安全性设计、制造水平，提高电动汽车合理使用和维护、以及安全性管控水平，探索安全的、系统性的解决方案和意外发生时的应急处理手段。与此同时，也希望本《指南》还能为电动汽车行业相关标准的制定和修订提供依据，为开展安全性研究项目提供方向。

## 三、《指南》主要内容

考虑到新能源载货类、专用车类产品种类繁杂，且用途多样，《指南》2018 版主要是覆盖在中国生产和销售的纯电动乘用车和纯电动客车的安全性，建议电动商用车可参考本指南执行。《指南》2019 版增加了氢燃料电池汽车安全性内容。

《指南》2019 版分两个部分，第一部分是纯电动汽车篇，较 2018 版的主要变化是把电机电控作为独立章节以细化其内容，其他章节也在 2018 版的基础上进行了修订完善；第二部分是氢燃料电池汽车篇，该篇系统梳理了燃料电池及其整车设计、制造、使用、氢能及基础设施等方面安全性。

**四、《指南》的编制与发布**

本《指南》由工业和信息化部、国家能源局指导编制。

本《指南》由国内主要整车、动力蓄电池、充电设施、运营、回收再利用等企业，以及氢能供应、氢燃料电池企业，行业组织、科研院校、机构 100 余家单位共同研究编制，在编制过程中广泛征求了国内外业界专家和企业、机构的意见。

本《指南》中英文两个版本同时公开发布。

本《指南》的解释权在《指南》编委会编写组（见附录）。

# 目　录

# 纯电动汽车篇

# 1.电动乘用车安全

## 1.1 防触电安全

### 1.1.1 电压等级

依据 GB/T18384.3-2015,根据整车的最大工作电压,将电气元件或电路分为以下等级，见表 1-1。

表 1-1 电压等级

| 电压等级 | 最大工作电压 U（V） | |
|---|---|---|
| | 直流 | 交流（rms） |
| A | 0<U≤60 | 0<U≤30 |
| B | 60<U≤1500 | 30<U≤1000 |

依据 GB/T18384.3-2015 第 1 号修改单,对于相互传导连接的 A 级电压电路和 B 级电压电路，当电路中直流带电部件的一极与电平台相连，且其它任一带电部分与这一极的最大电压值不大于 30Va.c.（rms）且不大于 60Vd.c.，则该传导连接电路不完全属于 B 级电压电路，只有以 B 级电压运行的部分才被认定为 B 级电压电路。

对于 48V 系统,只要可以保证直流系统不超过 60Vd.c,其交流电机之外的部分就可以不被认定为 B 级电压电路,不需要满足相关的触电防护要求。

### 1.1.2 使用中触电防护要求

使用中的人员触电防护要求应包括高压标记要求、直接接触防护要求、间接接触防护要求及防水要求四个部分。

#### 1.1.2.1 高压标记要求

##### 1.1.2.1.1 高压警告标记要求

应满足 GB/T 18384.3-2015 关于 5.1 章节的修改内容。

##### 1.1.2.1.2 B 级电压电线标记要求

应满足 GB/T 18384.3-2015 关于 5.2 章节的要求。

#### 1.1.2.2 直接接触防护要求

直接接触防护要求的提出是为了避免人员与带电部件直接接触而发生触电事故。直接

接触防护可以通过B级电压部件的遮拦和外壳实现人员与B级电压带电部分的物理隔离。除了 B 级电压部件的遮拦和外壳，高压连接器、高压维修开关、充电插座在插接/耦合及非耦合/断开状态下，都应该满足相应的要求。

**1.1.2.2.1 遮拦外壳要求**

B级电压部件的遮拦和外壳应依据GB/T18384.3-2015，满足IPXXB防护等级要求。如果遮拦或外壳可以徒手打开，则其可以打开的部分应具备高压互锁装置，满足1.1.2.2.5章节的高压互锁要求。

**1.1.2.2.2 连接器要求**

高压连接器在装配完好时，应满足IPXXD防护等级要求。如果高压连接器可以徒手打开，需要至少满足以下三个条件之一：

（1）在处于非耦合状态下满足IPXXB的防护等级要求；

（2）高压连接器的分开需要至少两个非连续的步骤，且需要先打开某个机械锁止机构后才能进行高压连接器的打开操作；

（3）高压连接器被分开后，应进行下电及下电后的放电，考虑到人在打开高压连接器后能触碰到带电部分的时间，车辆应在1s内将B级电压回路电压下降到30Va.c.（rms）且60Vd.c以下，或电路存储总能量小于0.2J；

（4）选用的配对耦合高压连接器物理结构上的连接引导部分应不同，以满足防错插功能。

**1.1.2.2.3 高压维修断开装置要求**

如果车辆具有高压维修开关且高压维修开关可以被徒手打开或者拔出，那么高压维修开关应至少满足以下两个条件之一:

（1）在高压维修开关被打开或拔出的状态下，高压维修开关的车辆端应满足 IPXXB的防护等级要求；

（2）在高压维修开关被打开或拔出后，应进行下电及下电后的放电，考虑到人在打开高压维修开关后能触碰到带电部分的时间，车辆应在 1s 内将 B 级电压回路电压下降到30Va.c.（rms）且60Vd.c以下，或电路存储总能量小于0.2J。

对于未配备高压维修开关的车辆，应根据不同高压设计方案，如通过断开12V电源或电子维修开关后同样可保证1s 内将B 级电压回路电压下降到30Va.c.(rms)或60Vd.c 以下。

#### 1.1.2.2.4 充电插座要求

车辆端充电插座在未耦合状态下，应至少满足以下要求之一：

（1）交流充电插座在未耦合状态下应满足 IPXXB，且应在充电插头被拔下 1min 内将 B 级电压回路电压下降到 30Va.c.（rms）且 60Vd.c 以下，或电路存储总能量小于 0.2J；

（2）由于直流充电座无法在未耦合状态下满足 IPXXB 要求，要满足更高的防护要求，应在充电插头被拔下后 1s 内将 B 级电压回路电压下降到 30Va.c.（rms）且 60Vd.c 以下，或电路存储总能量小于 0.2J。

#### 1.1.2.2.5 高压互锁要求

车辆上易于拆卸或可以徒手拆卸的遮挡/外壳及高压连接器应具备高压互锁装置。高压互锁的设计一般包括硬件设计及控制策略设计，应保证被保护部件被拆卸时，在人接触到 B 级电压带电部分前将 B 级电压带电部分变为不带电部分，具体应满足 1.1.2.3.6 故障后下电要求及 1.1.2.3.7 下电后放电要求。

### 1.1.2.3 间接接触防护要求

#### 1.1.2.3.1 绝缘电阻要求（不包含燃料电池）

依据 GB/T18384.3-2015，在最大工作电压下，直流电路绝缘电阻应至少大于 100Ω /V，交流电路应大于 500Ω /V。如果直流和交流的 B 级电压电路可导电的连接在一起，则应满足绝缘电阻大于 500Ω /V 的要求。

充电插座的绝缘电阻应满足 1.1.2.3.5 章节要求。

整车的绝缘电阻是各互相隔离的子系统中的最小绝缘电阻，各子系统是由构成子系统的各高压部件并联而成。

#### 1.1.2.3.2 绝缘监测要求

车辆应具备绝缘监测功能。绝缘监测功能应在车辆上高压前与上高压后持续对 B 级电压电路的绝缘电阻进行监测，从而区分电池包内绝缘故障与高压负载绝缘故障，并在绝缘阻值低于某个阈值时，予以报警。报警的阈值要大于等于 1.1.2.3.1 章节要求的绝缘电阻，具体数值可以由主机厂自行设定。报警方式可以是提示音或者通过仪表的文字或者符号显示。

#### 1.1.2.3.3 电位均衡要求

电位均衡是为了保证 B 级电压电路中的高压部件的可导电外壳不会因为绝缘电阻失效而带有高压电，从而形成电势差，产生触电风险。

电位均衡具体要求应满足 GB/T18384.3-2015 中 6.9 章节要求，在进行设计时，可以

要求单个部件的可导电外壳与电平台的电阻小于 40mΩ 。如果采用焊接的形式实现电位均衡，视为满足要求。

#### 1.1.2.3.4 电容耦合要求

电容耦合是针对 Y 电容的安全防护要求，如果高压系统中 Y 电容总能量超过对人体安全能量限值 0.2J，在高压系统内发生单点失效的情况下，就会发生触电事故，因此要对这种情况予以设计防护。

综上，电容耦合应满足以下两种要求之一：

（1）高压系统的 Y 电容的总能量不大于 0.2J；

（2）如 Y 电容总能量大于 0.2J，高压系统中各 B 级电压电路均应被双层绝缘层、遮栏或外壳防护，或者其单层遮栏或外壳，能至少承受 10kpa 压强且没有明显的塑形变形。

#### 1.1.2.3.5 车辆充电插座接地及绝缘电阻要求

交流充电插座应满足 GB/T18384.3-2015 中 6.10.2.1 章节要求。

直流充电插座应满足 GB/T18384.3-2015 中 6.10.2.1 章节要求。

#### 1.1.2.3.6 故障后下电要求

按照 GB/T31498-2015 的要求，在车辆发生碰撞后，应当立即进行高压下电，避免碰撞后造成人员与高压带电部分直接接触或间接接触引发的触电事故。

在发生绝缘失效、高压互锁等故障时，建议依据车辆状态比如行驶速度等具体情况来考量是否进行下电处理。

#### 1.1.2.3.7 下电后放电要求

车辆在每次正常下电后或者故障下电后，都应该将 B 级电压回路中能量大于 0.2J 的电容的能量释放掉，避免能量始终存储于 B 级电压回路中，在车辆故障或者车辆被拆卸时造成触电事故。

放电形式应具有主动放电及被动放电两种形式，主动放电应通过控制策略结合硬件设计在下电后 5s 内将 B 级电压回路电压下降到 30 Va.c.（rms）且 60 Vd.c 以下或将 B 级电压回路中电容存储的总能量降至 0.2J 以下。被动放电应始终有效，不依靠控制策略。在 B 级电压回路与电源断开后，应在 2min 内将 B 级电压回路电压下降到 30 Va.c.（rms）且 60 Vd.c 以下或将 B 级电压回路中电容存储的总能量降至 0.2J 以下。

### 1.1.2.4 防水要求

#### 1.1.2.4.1 整车防水要求

为了保障车辆涉水、清洗、暴雨等暴露于水后的电气安全，需要对车辆进行模拟涉水、

模拟清洗试验，并在试验后进行绝缘电阻测试以考核车辆是否存在触电风险。

模拟涉水及模拟清洗的试验要求应满足 GB/T18384.3-2015 中 8.2.1 及 8.2.3 中要求。在完成每项试验后，应先马上进行第一次绝缘电阻测试，24 小时后再进行第二次绝缘电阻测试。两次绝缘电阻测试结果均应满足 1.1.2.3.1 章节绝缘电阻要求。

#### 1.1.2.4.2 高压部件防水要求

所有高压部件在装配完好的情况下，后备厢及乘员舱外的高压部件防水等级应至少达到 IPX7，后备厢及乘员舱内的高压部件应至少达到 IPX4 等级要求。

#### 1.1.2.5 维修断开装置要求

车辆应具有可以断开高压回路的维修断开装置，可以采用高压维修开关或低压维修开关两种形式之一。

(1)高压维修开关

如车辆具有高压维修开关，应能通过对高压维修开关的操作，实现高压回路的通断。高压维修开关应具备高压互锁装置，以保证操作时不会造成电弧。

(2)低压维修开关

如车辆具有低压维修开关，应能通过断开低压维修开关，间接实现高压回路的断开。建议设计至少两种方式同时保证实现高压回路的间接断开，提高操作结果的可靠性。

### 1.1.3 碰撞后触电安全

#### 1.1.3.1 总要求

电动汽车在进行碰撞试验时可分为两种测试状态，一种是高压下电状态下进行试验，一种是高压上电状态下进行试验。对于高压上电状态下进行的碰撞试验，整车 B 级电压系统中每一个互相隔离的子 B 级电压子系统应至少当满足下面四项要求中的一项，保障车辆不发生直接接触和间接接触造成的触电事故；对于高压下电情况下进行的碰撞试验，由于电力负载没有电压和能量来源,应满足 1.1.3.4 物理防护要求或 1.1.3.5 绝缘电阻要求，REESS 和充电子系统应满足下面四项要求（1.1.3.2-1.1.3.5）中的一项。

#### 1.1.3.2 电压要求

应满足 GB/T31498-2015 中 4.2.2 章节要求。

#### 1.1.3.3 电能要求

应满足 GB/T31498-2015 中 4.2.3 章节要求。

#### 1.1.3.4 物理防护要求

应满足 GB/T31498-2015 中 4.2.4 章节要求。

#### 1.1.3.5 绝缘电阻要求

应满足 GB/T31498-2015 中 4.2.5 章节要求。

## 1.2 功能安全

本部分的功能安全，是指除电池系统和充电系统（相关内容参见后继章节）以外的功能安全。

#### 1.2.1 整车功能安全开发流程

功能安全开发流程应符合《GB/T34590-2017 道路车辆功能安全》相关规定要求。

#### 1.2.2 概念开发阶段

应基于 GB/T34590.3-2017 相关规定完成概念开发，并得出相关项定义、安全目标和功能安全要求，作为系统开发的必要输入。

#### 1.2.2.1 相关项定义

为了充分理解相关项，并为后续阶段的安全活动提供支持，应从相关项的功能、要素、接口、环境条件、相关法规要求和危害等方面考虑，详细定义相关项的功能性和非功能性要求。

#### 1.2.2.2 危害分析与风险评估

危害分析与风险评估的目的是识别相关项中因故障而引起的危害并对危害进行归类，制定相应的安全目标，以避免不合理的风险。

其中，应基于相关项的功能行为，来分析其潜在的危害事件。再从危害-事件的严重程度、暴露概率、可控性三个方面对相关项进行系统性的评估，从而确定安全目标及相应的 ASIL 等级。

#### 1.2.2.3 功能安全概念

功能安全概念主要是为了从安全目标中得出功能安全要求，并将其分配给相关项的架构要素或外部措施。

定义功能安全要求时，应从相关项的运行模式、故障容错时间间隔、安全状态、紧急运行时间间隔及功能冗余等方面进行考虑，同时可以使用安全分析（例如 FMEA、FTA、HAZOP）的方法 ，使制定的功能安全要求更加完善。

功能安全概念还应按照 GB/T34590.9-2017 中的要求进行验证，以表明与安全目标的一致性和符合性，及减轻或避免危害事件的能力。

### 1.2.3 系统功能安全开发

进行正式系统开发前，应基于 GB/T34590.4-2017 相关规定，指定系统层面产品开发的安全活动计划，包括确定设计和集成过程中适当的方法和措施、测试及验证计划、功能安全评估计划等。

#### 1.2.3.1 系统安全要求设计

技术安全要求是实现功能安全概念必要的技术要求，目的是将相关项层面的功能安全要求细化到系统层面的技术安全要求。

应基于 GB/T34590.4-2017 相关规定，根据功能安全概念、相关项的初步架构设想、外部接口、限制条件等系统特性来制定技术安全要求。

技术安全要求应从故障探测/指示/控制措施、安全状态、故障容错时间间隔等方面考虑，定义必要的安全机制。

#### 1.2.3.2 系统设计

系统设计应基于功能概念、相关项的初步架构设想和技术安全要求。在实现技术安全要求相关的内容时，应从验证系统设计的能力、软硬件设计的技术能力、执行系统测试的能力等方面考虑系统设计。

为避免系统性失效，应对系统设计进行安全分析以识别系统性失效的原因和系统性故障的影响。

为降低系统运行过程中随机硬件失效造成的影响，应在系统设计中定义探测、控制或减轻随机硬件失效的措施。

系统设计中定义软硬件接口规范，并在后续硬件开发和软件开发过程中进行细化。

#### 1.2.3.3 系统集成与测试

基于 GB/T34590.4-2017 相关规定，分别进行软硬件、系统、整车层级的集成和测试，验证每一条功能和技术安全要求是否满足规范，以及系统设计在整个相关项上是否得到正确实施。

为发现系统集成过程中的系统性故障，在确定测试方法时，应从以下几个方面考虑：

（1）功能和技术要求在系统层面是否被正确执行；

（2）安全机制在系统层面是否被正确的执行；

（3）外部接口和内部接口在系统层面执行的一致性和正确性；

（4）安全机制在系统层面的失效覆盖率的有效性；

（5）系统层面的鲁棒性水平。

#### 1.2.3.4 安全目标确认

应基于 GB/T34590.4-2017 中的规定，通过检查和测试等方式，确认安全目标是否在整车层面是正确、完整并得到完全实现。

确认安全目标前可以从确认流程、测试用例、环境条件等方面考虑，并制定详细的确认计划。

应根据安全目标、功能安全要求和预期用途，按计划执行整车层面的安全目标确认。具体确认方法可考虑详细定义的可重复性测试、安全分析、长期测试、用户抽测、评审等形式。

### 1.2.4 电控单元硬件开发

电控单元硬件开发流程应满足 GB/T 34590.5-2017 的要求，执行规定的安全活动，输出规定的交付内容。

#### 1.2.4.1 电控单元硬件安全要求

基于 GB/T 34590.5-2017 相关规定，将技术安全概念，技术安全要求和系统设计说明落实到硬件层级，设计完整且详细的硬件安全要求。

为保证硬件安全要求的完整性，在设计时应考虑包含以下内容：

（1）安全机制及其属性；

（2）验证的标准；

（3）硬件度量的目标值；

（4）FTTI；

（5）其它与安全相关的要求。

为保证硬件安全要求的质量，应按照 GB/T 34590.8-2017 中第 6 章的要求进行硬件安全要求的设计、验证和管理。

为使硬件被软件正确地控制和使用，应对软硬件接口（HSI）进行充分的细化，并描述出硬件和软件之间的每一项安全相关的关联性。

#### 1.2.4.2 电控单元硬件设计

基于 GB/T 34590.5-2017 相关规定，进行硬件架构设计和硬件详细设计，并进行硬件安全分析，以满足系统设计说明和硬件安全需求的要求。

为避免硬件的系统性风险，一般应进行硬件架构设计，然后进行硬件详细设计。

在硬件架构设计时，应确保每个硬件组件继承了正确的 ASIL 等级，并可追溯到与之相关的硬件安全要求。

在硬件设计时，应运用相关的经验总结，并考虑安全相关硬件组件失效的非功能性原因，如果适用，可包含以下因素：温度，振动，水，灰尘，EMI，来自硬件架构的其他组件或其所在环境的串扰。

为提高设计的可靠性，应遵循 GB/T 34590.5-2017 中的“模块化的硬件设计原则”和“鲁棒性设计原则”，如降额设计、最坏情况分析等。

为识别硬件失效的原因和故障的影响，应按 GB/T 34590.5-2017 中的要求，根据不同的 ASIL 等级，使用“演绎分析”（如 FTA）或“归纳分析”（如 FMEA）的方法进行安全分析。

如果安全分析表明生产、运行、服务和报废与安全相关，则应定义其与安全相关的特殊特性并输出说明性文件。

为验证硬件设计与硬件安全要求的一致性和完整性，应按 GB/T 34590.5-2017 中的要求，对硬件设计进行验证。

#### 1.2.4.3 电控单元硬件组件的鉴定

基于 GB/T 34590.8-2017 相关规定，对其中复杂的硬件组件及元器件应进行硬件组件的鉴定，确保硬件组件合规使用并为 FMEDA 分析提供基础数据。

#### 1.2.4.4 电控单元硬件架构度量的评估

基于 GB/T 34590.5-2017 相关规定，进行硬件架构度量的评估，并将评估结果和优化建议反馈到系统设计、硬件设计、软件设计环节，以优化产品设计，使最终的“单点故障度量”和“潜伏故障度量”满足对应 ASIL 的要求。

#### 1.2.4.5 随机电控单元硬件失效导致违背安全目标的评估

基于 GB/T 34590.5-2017 相关规定，进行 PMHF 评估或割集分析评估，闭环优化使相关安全目标没有由于随机硬件失效带来的不可接受的风险。

#### 1.2.4.6 电控单元硬件集成和测试

基于 GB/T 34590.5-2017 相关规定，进行硬件集成和测试，通过测试确保所开发的硬件符合硬件安全要求。

硬件集成测试用例的生成应考虑 GB/T 34590.5-2017 的表 10 中所列的方法。

为了验证安全机制的完整性和正确性，硬件集成测试应考虑以下方法：功能测试、故障注入测试和电气测试。

为了验证硬件在外部应力下的鲁棒性，硬件集成测试应考虑 GB/T 34590.5-2017 的表 12 中所列方法。

### 1.2.5 电控单元软件设计

#### 1.2.5.1 软件安全需求分析

软件安全需求分析目的是依据安全技术规范以及系统设计说明书指定软件安全需求，同时验证软件安全需求与安全技术规范及系统设计说明书是否一致。软件安全需求分析阶段需满足完整性、可测试性、可追溯性要求。

软件安全需求分析时，应从如下方面考虑：充分识别失效会违反安全技术要求的软件功能；需来源于安全技术要求和系统设计方案；应识别软件与硬件之间所有安全相关的属性；包含足够的硬件运行资源，有效的安全相关等信息的确认；软硬件接口说明书应是确认有效的；测试验证方法应是安全有效的。

#### 1.2.5.2 软件安全架构设计

软件安全监控架构设计目的在于开发一个可以满足并实现软件安全需求的软件架构。软件安全监控架构设计需结合功能安全相关软件需求和非功能安全相关软件需求，全局考虑软件的架构设计，并进行软件安全分析。

软件安全监控架构设计时，应从如下方面考虑：应该是可配置、可实施、易于测试和可维护的；需遵循模块化、高类聚、低耦合、低复杂度的要求；应细化到足够支持详细设计；应具备静态和动态特性；应满足独立性的要求；应覆盖软件安全需求等。

#### 1.2.5.3 软件失效分析与详细设计

软件失效分析与软件详细设计目的是基于软件架构设计及软件安全需求对软件功能模块进行详细设计，同时根据建模及编码指导书进行模型或源代码设计。

软件详细设计时，应从如下方面考虑：应包含足够的必要信息以便于允许后续活动开展；应详细描述其功能特征；应满足可测性、可维护、低复杂度、可读性和健壮性等要求；详细设计应满足与软件安全需求、软件架构、编码准则、详细设计说明书等一致性的要求。

#### 1.2.5.4 软件安全算法测试

软件算法测试用于证明软件单元模块符合软件详细设计说明书要求，该要求包括：软件功能要求的符合性，接口要求的一致性，算法的健壮与高效等。

软件算法测试案例设计时，需按照软件详细设计说明书，软件失效分析报告要求，采用需求分析、等价类划分、边界值分析、错误猜想等方法。

软件算法测试活动，要做好详细设计、失效分析报告、测试案例、测试数据、测试缺陷的双向可追溯性与过程的完整性。

软件算法测试同时还需要度量验证软件算法质量，包括单元覆盖度（如：语句覆盖度，

分支覆盖度，修正判定条件覆盖度等），代码编码规则，以及其他静态度量指标（如：圈复杂度等），具体请参见 GB/T34590.6-2017 相关要求。

#### 1.2.5.5 软件集成与架构符合性测试

软件集成与架构符合性测试主要用于验证软件组件集成功能，以及软件组建之间的接口是否符合软件架构设计文档要求。

软件集成通常可分为增殖式集成与一次性集成。不同的集成方式，对应的集成测试策略也不同。常用到的测试方法包括：基于需求的测试，接口测试，故障注入测试，资源占用测试以及模型与代码的背靠背测试。

软件集成测试也包含质量度量过程，主要度量指标包括功能覆盖度和函数调用覆盖度。

#### 1.2.5.6 软件安全需求验证

软件安全需求验证的目的在于确保软件在目标硬件环境上能够正确实现软件安全需求。通常需采用验证方法包括硬件在环测试、电子电气试验台架测试以及实车测试等。

软件安全需求验证不但要从功能角度验证软件安全需求的符合情况，还要从性能角度验证是否满足性能要求（如：程序安装测试、负载测试等）。

## 1.3 使用操控安全

### 1.3.1 操控安全基本要求

整车企业需提供用户使用说明书，明确安全操作要求，同时整车必须满足数据监控以及故障报警的基本功能。

### 1.3.2 正常场景安全

#### 1.3.2.1 车辆上下电安全

车辆上下电安全包括上下电流程设计以及安全操作步骤设计。

**上下电流程设计**：车辆在上电之前应当具备诊断高压部件故障的功能，包括硬件电路短路开路、绝缘阻值过低、高压互锁故障等。在闭合主接触器之前，检查到车辆等级高的故障，车辆应禁止上电；车辆高压上电后，检测到碰撞或高压故障时，应记录相关故障码，通过声光等信号通知驾驶员。

**安全操作步骤设计**：根据 GB/T18384.2-2105，车辆安全操作需满足如下要求：

（1）车辆从驱动系统断电到可行驶状态应至少经过两次有意识的不同动作；

（2）从可行驶状态到驱动系统断电只需要一个动作；

（3）动力电源对驱动电路的主开关功能是驱动系统电源接通/断开程序的必要部分，若驱动系统的电源接通/断开程序是通过车钥匙激活，要符合相关安全设计的要求；

（4）应当连续或者间歇向驾驶员提示，车辆处于可行驶模式；

（5）车辆停止时，驱动系统自动或手动关掉后，只可以通过上述程序重新进入“可行驶模式”。

#### 1.3.2.2 车辆行驶操作安全

按照 GB7258-2017，车辆以纯电动模式低速驱动时，应通过低速行驶提示音系统发出的声音提醒周边行人。驾驶员主动停止低速行驶提示系统停止工作时，应通过醒目的提示信号进行提示。

按照 GB/T 18384.2-2015，如果是通过改变电机旋转方向来实现前进和倒车的方向转换，应当满足以下要求，以防止意外切换到反向行驶。

（1）前进和倒车两个方向的行驶转换，要通过两个不同操作动作来完成；或者

（2）如果仅通过一个动作来完成，应使用一个安全措施使模式转换只有在车辆静止或低速时（建议小于 7km/h）才能完成；

（3）如果前进和倒车两个行驶方向的转换不是通过电机的旋转方向来实现的，则反向行驶要求不适用。

当驾驶员离开车辆时，如果驱动系统仍处于可行驶模式，需通过一个明显的信号装置提示驾驶员。切断电源后车辆不能产生由自身电驱动系统造成的不期望行驶。

#### 1.3.2.3 整车充电操作安全

按照 GB/T 18384.2-2015，车辆物理连接到外部电源进行充电时，应当具备装置防护充电枪脱落的情况，并且不能通过其自身的驱动系统移动。

车辆进行充电时，应当能够检测高压安全相关故障，并有能力在检测到相关故障时断开高压。

车辆进行充电时，应当能够通过 VCU 禁止一切可能使车辆发生移动的操作。

#### 1.3.2.4 整车-低电量报警提醒

按照 GB/T 18384.2-2015，如果可充电储能装置的低电量影响到了车辆的行驶，应通过一个明显的信号装置向驾驶员提示。当车辆在制造厂规定的低电量状态时，应当至少满足下列要求：

（1）通过其自身的驱动系统能够使车辆驶出交通区域；

（2）当没有独立的能量存储装置为辅助电力系统供电时，最小剩余电量应当能够为

照明系统提供满足有关规定的电量。

### 1.3.3 特殊场景安全

#### 1.3.3.1 车辆故障操作安全

如果电驱动系统采取了自动减少和限制车辆驱动功率的措施，并且影响了车辆的行驶，该状态要向驾驶员指示。

如果车辆因故障导致无法输出动力时，应通过一个明显的信号（例如：声或光信号）装置向驾驶员提示。

#### 1.3.3.2 车辆碰撞操作安全

车辆应具备碰撞检测功能。如果检测到碰撞事件发生，系统应能够禁止动力输出，切断主接触器，同时通过一个或者多个放电设备进行主动放电。

在车辆未维修完成前，不允许再次上电。

## 1.4 安全防护措施

### 1.4.1 整车通过性要求

为保证车辆在正常行驶中的动力电池底部安全性，整车企业应按照车型定义合理的最小离地间隙及最小纵向通过角，离地间隙和纵向通过角定义和测量按照 GB/T 3730.3 中要求执行。

整车企业可参考 ADR 43（Vehicle configuration and dimensions）中对于汽车通过性的最小目标（满载载荷下）：

（1）前后轴中点的离地间隙不小于 0.0333*轴距(单位为 m)；

（2）轴间的最小纵向角为 7.6°。

### 1.4.2 正面碰撞安全

#### 1.4.2.1 基本要求

按照国标 GB/T 31498-2015 评估电动汽车正面碰撞高压电安全性能，试验设置依据 GB11551-2014 或 GB/T20913-2007 进行，需满足 GB/T31498-2015 条目 4 技术要求的规定。

#### 1.4.2.2 附加要求

按照 C-NCAP 评估电动汽车正面碰撞高压电安全性能，试验设置依据 C-NCAP 管理规定进行（现行为 2018 版规程，前碰工况为 50FFB 和 64ODB），参照 C-NCAP 要求进行电安全评估，需满足测试规程 1.2.1.1.3 纯电动汽车/混合动力汽车（EV/HEV）电气安全条款规定的技术要求，不做星级要求。

### 1.4.3 侧面碰撞安全

#### 1.4.3.1 基本要求

按照国标 GB/T 31498-2015 评估电动汽车正面碰撞高压电安全性能，试验设置依据 GB20071-2006 进行，需满足 GB/T31498-2015 条目 4 技术要求的规定。

#### 1.4.3.2 附加要求

按照 C-NCAP 评估电动汽车侧面碰撞高压电安全性能，试验设置依据 C-NCAP 管理规定进行（现行为 18 版规程，侧面碰撞工况为 50AEMDB），参照 C-NCAP 要求进行电安全评估，需满足测试规程 1.2.1.1.3 纯电动汽车/混合动力汽车（EV/HEV）电气安全条款规定的技术要求，不做星级要求。

### 1.4.4 追尾碰撞安全

按照国标 GB/T 31498-2015 评估电动汽车正面碰撞高压电安全性能，试验设置依据 GB20072-2006 进行，需满足 GB/T31498-2015 条目 4 技术要求的规定。

（注：GB/T 31498-2015 暂未引用 GB20072-2006，目前为标准讨论稿阶段，后续将实施）

### 1.4.5 侧面柱碰防护

基于 EuroNCAP 评估电动汽车侧面柱碰撞高压电安全性能，试验设置依据 EuroNCAP 测试规程进行，需满足 EuroNCAP Technical Bulletin Testing of Electric Vehicles 的技术要求。

(注：高于现行国标及 C-NCAP 等测试体系)

### 1.4.6 整车底部安全防护

对于将动力电池布置于乘员舱外底盘下的电动汽车，建议整车企业基于典型滥用工况评估车辆的底部碰撞高压电安全性能，如针对常见的底部石击,底部刮擦工况等的设计防护，定义相应的动力电池底部滥用工况作为标准工况，提出动力电池包的底部防护性能要求。同时，对于布置在底盘下的高压连接器与线束增加防护装置。

### 1.4.7 碰撞后高压断电及报警提醒

车辆碰撞后，应满足 1.1.3 规定，同时应具备报警提醒功能。

### 1.4.8 控制器故障诊断

高压用电器件应具备故障诊断功能，并能通过整车诊断口读取故障码。

## 1.5 整车 EMC 安全

车辆的 EMC 辐射强度及抗干扰强度应符合下述规定，以保证车辆在 EMC 干扰下的安全行驶和对驾乘人员的保护。

### 1.5.1 整车车外电磁辐射骚扰及抗扰度要求

#### 1.5.1.1 车辆对外电磁辐射骚扰要求

车辆及其零部件系统应装置有无线电骚扰抑制器件及布置措置，以保护车辆使用环境中的外界无线电通讯设备正常工作。车外电磁场发射量应按 GB 14023-2011、GB34660-2017、GB/T 18387-2017 试验验证，并符合标准限值要求。

（1）车辆静态工况：车辆静止，12V 系统用电器全开；

（2）车辆动态工况：车辆 16km/h、40km/h、70km/h 恒速行驶；

（3）车辆充电工况：车辆处于充电模式，动力电池荷电状态（SOC）应处在最大荷电状态的 20%～80%之间。

#### 1.5.1.2 车辆抗电磁干扰要求

车辆应采用合理布置及屏蔽保护设计，在处于以下使用工况状态时，应耐受标准场强等级车外电磁场辐射干扰，而不发生功能状态偏离及安全降级。并按照 GB34660-2017 对 20MHz-2GHz 频段试验验证。

（1）车辆动态工况：车辆用电器全开，以 50km/h 恒速行驶；

（2）车辆充电工况：车辆处于充电模式，动力电池荷电状态（SOC）应处在最大荷电状态的 20%～80%之间。

### 1.5.2 整车车载电器电磁辐射骚扰及抗扰度要求

#### 1.5.2.1 车载电器电磁辐射骚扰要求

车载用电器设备（如：空调压缩机，驱动电机等）应装置有无线电骚扰抑制器件，以控制沿传导路径及空间辐射路径骚扰发射，保护车载无线电收发设备（如收音机，GPS，T-BOX 等）在安全范围工作。应按照 GB/T 18655-2018（建议不低于等级 3 限值）试验验证并符合标准限值要求。

（1）车辆静态工况：车辆用电器单独打开，车辆动力系统高压上电完成（PT Ready）；

（2）车辆动态工况：车辆 40km/h 恒速行驶；

（3）车辆充电工况：车辆处于充电模式，动力电池荷电状态（SOC）应处在最大荷电状态的 20%～80%之间。

### 1.5.2.2 车载电器电磁抗扰要求

车载用电器设备应采用合理布置及屏蔽保护设计，在处于以下使用工况状态时，应耐受车载发射机标准发射功率场强等级电磁辐射干扰，而不发生功能状态偏离及安全降级。应按照 GB/T 33012.3-2016 对不同发射机工作频段进行试验验证。

（1）车辆动态工况：车辆用电器全开，以 50km/h 恒速行驶；

（2）车辆充电工况：车辆处于充电模式，动力电池荷电状态（SOC）应处在最大荷电状态的 20%～80%之间。

### 1.5.3 整车充电过程中沿电源线骚扰和抗扰度要求

车辆处于电源线传导充电工况模式，应按照 ECE R10.5 试验验证；沿充电电源线的谐波发射，电压变化、波动和闪烁发射，射频传导发射的特性符合标准限值要求。应能耐受来自充电电源线的浪涌干扰，电瞬态快速脉冲群干扰，而不发生充电功能状态偏离及安全降级。

车辆处于无线充电工况模式，应包含接入电网的无线充电耦合设备装置，按 ECE R10.5 试验验证并通过。

### 1.5.4 整车乘员暴露于车辆电磁环境安全要求

本部分指人体所处车辆环境的低频磁场发射。

车辆在处于以下工况时，应按照“车辆电磁场相对于人体曝露的测量方法”（送审稿）试验验证；10Hz-400KHz 的磁场发射量符合 ICNIRP 2010 限值要求。

静态工况：车辆静止状态用电器全开，车辆动力系统高压上电完成（PT Ready）；

动态工况：车辆 40km/h 恒速行驶；车辆以 2.5 m/s2 的加速度和减速度行驶；

充电模式：动力电池荷电状态（SOC）应处在最大荷电状态的 20%～80%之间。

### 1.5.5 高压线束 EMC 要求

高压线束应具备 EMC 屏蔽措施，其走向布置不应形成 EMC 辐射增强。

高压线束屏蔽层应与高压部件可导电外壳有效连接。

## 1.6 整车热安全

整车设计应考虑防止动力电池、电机系统和其他高电压零部件过温而引发安全事故。

### 1.6.1 电机热保护要求

电机应设置温度传感器，并通过电机控制器实现温度检测功能。如果检测到电机温度过高，电机控制系统应限制电机功率或者禁止电机工作， 并通过一个明显的信号（例如：

声或光信号）装置向驾驶员提示。

### 1.6.2 电机控制器热保护要求

电机控制器具备温度检测功能，如果检测到温度过高，系统应限制电机功率或者禁止电机工作， 并通过一个明显的信号（例如：声或光信号）装置向驾驶员提示。

### 1.6.3 充电系统热保护要求

在充电过程中，整车的充电系统需要对充电口的温度进行监控，当采用国家标准规定的模式二充电，建议对充电插头进行温度监控。当超出温度保护阈值时，应能采取有效措施进行保护（如：降功率或者停止充电），以免导致器件损坏或者起火。

在充电过程中，整车的充电系统应具有车载充电器温度检测功能，当超出温度保护阈值时，应能采取有效措施进行保护（如：降功率或者停止充电），以免导致器件损坏或者起火。

### 1.6.4 动力电池热保护要求

整车应能有效的对电池系统进行散热和降温，以确保电池系统温度始终在正常使用范围内，以免温度过高影响电池系统寿命。整车设计时应考虑如果电池发生温度超出正常使用范围，应该限制功率输出，并加以提醒。

如果有热失控发生风险，整车应具备提前提醒和报警功能，确保驾乘人员提前安全撤离。

### 1.6.5 整车空调 PTC 热保护要求

空调 PTC 应具备过热保护和故障报警功能。

## 1.7 整车制造、存储、运输、报废等安全

车辆在制造环节中，动力电池系统高压维修开关必须在装配过程中始终处于断开状态，在车辆总装最后环节进行闭合，以确保制造过程高压电安全。车辆出厂前应具备安全检测流程。

车辆应避免长时间在高温环境（≥42±2℃）下停放，且停放期间动力电池 SOC 不宜过高（建议：SOC 处于 40-70%）。

车辆在运输过程中，必须移除动力电池系统的维修开关，确保整车处于下电状态。

车辆报废应有专业资质单位进行，车辆报废前应确认负载端电压低于 B 级电压或能量小于 0.2J，并对动力电池系统进行回收再利用，具体要求参见电池回收再利用章节。

## 1.8 整车换电设计安全

整车换电是指通过更换动力电池系统为电动汽车提供电能的方式，被更换的动力电池系统在换电站集中充电维护。

由于要满足动力电池系统快换及可靠耐久性要求，电池系统及具备换电功能的车辆需在电池系统、固定/锁止机构、连接器、电气及软件等方面满足安全设计要求。

### 1.8.1 换电用动力电池系统结构安全要求

动力电池系统机械强度应满足 GB/T 31467.3-2015 安全性测试要求。

#### 1.8.1.1 整体结构安全要求

动力电池系统壳体宜采用框架式结构，应具备足够的机械强度，承受电动汽车振动和冲击要求。

换电动力电池系统与整车应采用安全可靠的固定方式，动力电池系统在车辆行驶造成的随机振动下，不会出现产生危害的相对位移或产生明显的机械噪声，动力电池系统锁止机构不应出现变形或结构损坏。

#### 1.8.1.2 固定/锁止机构安全要求

换电动力电池系统与车辆底盘的固定应采用锁止操作机构，并具有防锁止失效功能。

锁止机构应能有效的将电池系统紧固在底盘上，应满足车辆的耐久，环境和冲击的性能要求；在车辆行驶过程中，不应存在锁止机构失效的风险，并且噪声应符合车辆 NVH 性能要求。

在换电过程中，车辆底盘上应具备动力电池系统安装导向定位机构，在插入锁止机构时能自动修正动力电池系统的位置偏移；

动力电池系统锁止机构应具备在车辆行驶造成的频繁振动、蠕动下，能自动跟随位移变化，以保证可靠连接。

#### 1.8.1.3 换电连接器安全要求

换电连接器应具备导向和三维浮动功能，确保换电动力电池系统与整车的安全可靠连接；连接器在正确耦合状态下满足 IP67 防护要求。

低压线束插接快换接头，要满足全生命周期插接的耐磨、密封要求；具备导向机构，满足换电过程中低压线束插接的导向定位要求。

高压线束插接快换接头，满足全生命周期插接的耐磨、密封要求；具备导向机构，满足换电过程中高压线束插接的导向定位要求。

液冷连接器插接快换接头，满足全生命周期插接的耐磨、密封要求；具备导向机构，满足换电过程中液冷连接器插接的导向定位要求；液冷连接器在换电或使用过程中，不能出现漏液情况。

### 1.8.2 换电电气安全要求

高压线束插接快换接头应满足触电安全部分连接器接触防护要求。

换电连接器应具备高压互锁功能。

### 1.8.3 换电控制要求

整车监控到车辆进入换电状态，应主动执行高压下电流程。

动力电池管理系统 BMS 建议具备换电工作模式，当 BMS 进入换电模式时，应能主动引导上下电、充电控制、电池故障处理。

VCU 或 BMS 应监控换电锁状态，当监控到换电锁没有到位，应采取不允许上高压或车辆跛行，建议 BMS 或其他控制器应记录车辆与对应电池包换电次数，便于后期维护。

# 2.电动客车安全

## 2.1 防触电安全

电动客车常见的高压（即 B 级电压，指最大工作电压大于 60Vd.c.或 30 V.a.c.，小于等于 1500Vd.c.或 1000 V.a.c.）部件（带电、用电、传输 B 级电压部件）如表 2-1 所示：

表 2-1　常见高压部件

| 序号 | 高压部件名称 |
|---|---|
| 1 | 动力蓄电池 |
| 2 | 超级电容 |
| 3 | 燃料电池 |
| 4 | 驱动电机 |
| 5 | 高压发电机 |
| 6 | 电动转向油泵 |
| 7 | 电动空压机 |
| 8 | DC/DC 变换器（包括隔离 DC/DC） |
| 9 | 控制器（驱动电机控制器、发电机控制器、电动转向油泵控制器、电动空压机控制器） |
| 10 | 高压维修开关 |
| 11 | 高压配电 |
| 12 | 电加热 |
| 13 | 电空调 |
| 14 | 充电插座 |
| 15 | 车载充电机 |
| 16 | 高压线束及连接器 |

### 2.1.1 安全标识要求

#### 2.1.1.1 高压警告标记要求

B 级电压部件，如 REESS 和燃料电池堆，应标记图 2-1 所示符号。符号的底色为黄色，边框和箭头为黑色。按照 GB2893、GB2894 和 GB/T5465.2 的规定。

当移开遮拦或外壳可以露出 B 级电压带电部分时，遮拦和外壳上也应有同样的符号清

晰可见。当评估是否需要此符号时，应当考虑遮拦/外壳可进入和可移开的情况；标记附近建议有明显可见的安全操作注意项目的提醒，如“电机控制器开盖要等 10 分钟后，测量母线电压值为安全电压后方可操作”。

图 2-1　高压警告标记

#### 2.1.1.2 B 级电压电线标记要求

B 级电压电路中电缆和线束的外皮应用橙色加以区别，外壳里面或遮拦后面的建议也用橙色加以区别。

B 级电压连接器可通过与之连接的线束来区分。

### 2.1.2 直接接触防护要求

直接接触防护是通过绝缘材料、外壳或遮栏实现人体与 B 级电压带电部件的物理隔离，外壳或遮栏可以是导体也可以是绝缘体。对于具体部件的直接接触防护要求应满足 2.1.2.1～2.1.2.4。

对于 $M_2$，$M_3$ 类车型，如果在车顶布置有顶部充电装置，如图 2-2 所示，若从车辆入口最底部台阶处到顶部充电装置的外露 B 级电压带电部分的最短路径长度至少为 3m，则顶部充电装置的外露 B 级电压带电部分可不满足直接接触防护要求。

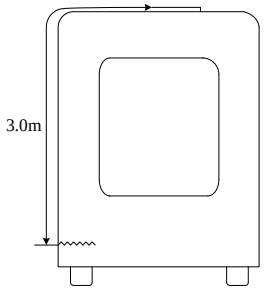



图 2-2　最短路径测量示意图

#### 2.1.2.1 遮拦外壳要求

如果通过遮栏或外壳提供触电防护，则 B 级带电部分应当布置在外壳里或遮栏后，防止从任何方向上接近带电部分。

遮栏和外壳需要满足如下两点要求：

（1）乘客舱内、货舱内的遮栏和外壳应满足 IPXXD 防护等级要求，乘客舱外、货舱外的遮栏和外壳应满足 IPXXB 防护等级要求；

（2）通常，遮栏和外壳只能通过工具才能打开或者去掉；若遮栏和外壳在不使用工具的情况下可以打开或者去掉，则要有某种方法使其中的 B 级电压带电部分在遮栏和外壳打开后 1s 内至少满足如下两种要求之一：

——交流电路电压应降到不超过 30Va.c.(rms)，直流电路电压应降到不超过 60Vd.c.；

——B 级电路存储总能量小于 0.2J。

#### 2.1.2.2 连接器要求

高压连接器在不使用工具的情况下，应无法打开，但以下三种情况除外：

（1）高压连接器分开后，应满足 IPXXB 的防护等级要求；

（2）高压连接器至少需要两个不同的动作才能将其从相互的对接端分离，且高压连接器与其它某个机构有机械锁止关系，在高压连接器打开前，该锁止机构必须要使用工具才能打开；

（3）在高压连接器分开之后，连接器中带电部分的电压能在 1s 内降低到不大于 30Va.c.(rms)且不大于 60Vd.c.。

#### 2.1.2.3 高压维修断开装置要求

对于装有高压维修断开装置的车辆，高压维修断开装置在不使用工具的情况下，应无法打开或拔出，但以下两种情况除外：

（1）高压维修断开装置打开或者拔出后，其中的 B 级电压带电部分满足 GB/T 4208 中规定的 IPXXB 的防护等级要求；

（2）高压维修断开装置在分离后 1s 内其 B 级电压带电部分电压降低到不大于 30Va.c.(rms)且不大于 60Vd.c.。

#### 2.1.2.4 充电插座要求

整车充电接口，不执行充电工作的充电接口应不带电。

车辆充电插座与车辆充电插头在断开时，车辆充电插座应至少满足以下一种要求：

(1)在断开后 1s 内，充电插座 B 级电压带电部分电压降低到不大于 30Va.c.(rms) 且不大于 60Vd.c.或电路存储的总能量小于 0.2J；

（2）满足 GB/T 4208 中规定的 IPXXB 的要求并在 1min 的时间内，充电插座 B 级电压

带电部分电压降低到不大于 30Va.c.(rms) 且不大于 60Vd.c.或电路存储的总能量小于 0.2J。

### 2.1.2.5 高压互锁要求

（1）B 级电压带电回路中的关键电路连接器建议结合整车控制系统实现软件或硬件互锁、联锁功能；

（2）在高压安全系统检测到某处连接断开或某处连接异常时，建议整车系统可以切断相关动力电源的输出并发出报警，直到该故障完全排除。

### 2.1.3 间接接触防护要求

### 2.1.3.1 绝缘电阻要求

（1）通则

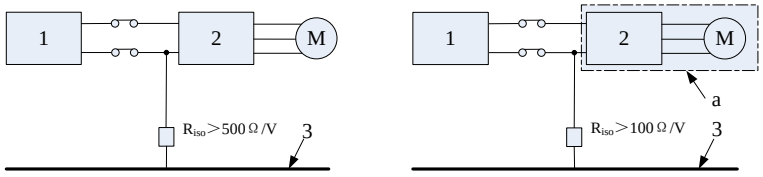
在最大工作电压下，直流电路绝缘电阻的最小值应至少大于 100Ω /V，交流电路应至少大于 500Ω /V。

整个电路为满足以上要求，依据电路的结构和组件的数量，每个组件应有更高的绝缘电阻。

如果直流和交流的 B 级电压电路可导电的连接在了一起（如图 2-3），则应满足以下两种选择中的一种：

——选择 1：组合电路至少满足 500Ω /V 的要求；

——选择 2：如果交流电路至少应用了一种 b（交流电路的附加防护方法）规定的附加防护方法，则组合电路应至少满足 100Ω /V 的要求。




选择 1　　选择 2

图 2-3 直流、交流电路传导连接的 B 级电压系统绝缘电阻的要求

说明：

1——动力电池或高压电源；

2——逆变器；

3——电平台；

a——交流电路。

（2）交流电路的附加防护方法

应用以下方法的一种或多种方法附加或替代 2.1.2 所述的直接接触防护来起到间接接触失效后的防护作用：

——用双重绝缘或加强绝缘替代基本绝缘；

——附加一层或多层绝缘体、遮拦和/或外壳；

——在车辆的整个寿命期间，采用有足够的机械强度和耐久度的刚性遮拦/外壳来应对故障。

（3）充电插座的绝缘电阻要求

——车辆交流充电插座

车辆交流充电插座应有端子将电平台与电网的接地部分连接。

车辆交流充电插座的绝缘电阻，包括充电时传导连接到电网的电路，当充电接口断开时应不小于 1MΩ 。

——车辆直流充电插座

车辆直流充电插座应有端子将车辆电平台和外接电源的保护接地相连接。

车辆直流充电插座的绝缘电阻，包括充电时传导连接到车辆直流充电插座的电路，当充电接口断开时应不小于 100Ω /V。

**2.1.3.2 绝缘电阻监测要求**

车辆应有绝缘电阻监测功能，并能通过 GB《电动汽车安全要求》6.2.3 的绝缘监测功能验证试验。在车辆 B 级电压电路接通且未与外部电源传导连接时，该装置能够持续或者间歇地检测车辆的绝缘电阻值，当该绝缘电阻值小于制造商规定的阈值时，应通过一个明显的信号（例如：声或光信号）装置提醒驾驶员，并且制造商规定的阈值不应低于 GB《电动汽车安全要求》5.1.4.1 的要求。

**2.1.3.3 电位均衡要求**

用于防护与 B 级电压电路直接接触的外露可导电部分，例如可导电外壳和遮栏，应传导连接到电平台，且满足以下要求：

（1）外露可导电部分与电平台间的连接阻抗应不大于 0.1Ω；

（2）电位均衡通路中，任意两个可以被人同时触碰到的外露可导电部分，即距离不大于 2.5m 的两个可导电部分间电阻应不大于 0.2Ω 。

若采用焊接的连接方式，则视作满足上述要求。

#### 2.1.3.4 电容耦合要求

电容耦合应至少满足以下要求之一：

（1）B 级电压电路中，任何 B 级电压带电部件和电平台之间的总电容在其最大工作电压时存储的能量应不大于 0.2 J，0.2 J 为对 B 级电压电路正极侧 Y 电容或负极侧 Y 电容最大存储电能的要求；此外，若有 B 级电压电路相互隔离，则 0.2J 为单独对各相互隔离的电路的要求；

（2）B 级电压电路至少有绝缘层、遮栏或外壳，或布置在外壳里或遮栏后，且这些外壳或遮拦应能承受不低于 10kPa 的压强，不发生明显的塑性变形。

#### 2.1.3.5 故障后下电要求

出现问题的 B 级电压电路可用监测电路内的故障或发现事故作为判断条件，由车辆的控制者选择采用断电的方式作为保护措施。

车辆在行驶过程中，出现整车断 B 级高压电的车辆异常情况时，在车速大于 5km/h 时应保持转向系统维持助力状态或至少保持转向助力状态 30s。切断供电的电路应在车辆制造商根据预测的故障和工作状态所设定的时间内满足下列条件之一：

——交流电路电压应降低到 30Va.c.(rms)，直流电路电压应降低到 60Vd.c.或以下；

——电路存储的总能量小于 0.2J。

#### 2.1.3.6 下电后放电要求

电机系统应有主动放电或被动放电功能，当 B 级电压系统断电后，主动放电在 3s 内或被动放电在 5min 内，直流母线电压应降至安全水平（直流电压 60 V 以下）。

且在故障(比如绝缘、短路等影响安全的故障)未解除的情况下，车辆应禁止再次上 B 级电压操作。

#### 2.1.3.7 爬电距离要求

车载储能装置的绝缘电阻、爬电距离应符合 GB/T 18384.1 第 5.2 条款的要求。

### 2.2 防水安全

#### 2.2.1 零部件防水要求

（1）B 级电压部件间连接器的防护等级应达到 GB/T 4208 规定的 IP67（充电口和受电装置除外）；

（2）B 级电压部件上使用的 A 级电压连接器及由此所组成的系统，防护等级应达到 IP67；

（3）B 级电压部件的防水等级建议不低于 IPX8，零部件及系统的防护等级按 GB4208 的试验条件进行，浸水时间建议不小于 24 小时。

——安装在客舱地板以下且距地面 500 mm 以下的 B 级电压电气设备和与 B 级电压部件相连的连接器（充电口除外）；

——安装在车顶且无防护装置的 B 级电压电气设备（受电装置除外）。

### 2.2.2 整车涉水要求

车辆应在 300mm 水深的水池中，以 5～10 km/h 的速度行驶 500m，完成涉水试验，时间 3～5 min；若水池长度小于 500 m，需要进行几次，总时间（包括在水池外的时间）应少于 10 min。车辆涉水试验完成后 10 min 内，按照 GB/T 18384.3 中 7.2 的绝缘电阻测量方法完成测量，总绝缘电阻值应大于 1 MΩ 。

### 2.2.3 整车浸水要求

安装在客舱地板以下且距地面 500mm 以下的 B 级电压电气设备和与 B 级电压部件相连的连接器（充电口除外）,需进行浸水试验。

车辆在退电状态，在水深 500mm 水池浸泡 24h，之后打开总火开关，并将点火开关开至 ON 档， 2 h 内车辆应不冒烟、不起火、不爆炸。

## 2.3 防火安全

### 2.3.1 火情预警

（1）可充电储能系统应具备火灾检测自动报警功能，（建议考虑起火前的烟雾、温度、气体等自动检测和预警）应在驾驶区给驾驶员提供声或光报警信号；

（2）车长大于等于 6m 的纯电动客车、插电式混合动力客车，应能检测动力电池工作状态并在发现异常情形时报警，且报警后 5min 内电池箱外部不能起火爆炸。

### 2.3.2 防火隔离

在可充电储能系统（或安装舱体）与客舱之间应使用阻燃隔热材料隔离，阻燃隔热材料的燃烧性能应符合 GB 8624 中规定的 A 级要求，并且按 GB/T10294 进行试验，在 300 ℃时导热系数应小于等于 0.04 W/（m·K）。

### 2.3.3 阻燃设计

可充电储能系统内零部件材料阻燃要求：除蓄电池单体外，可充电储能系统内其他非金属零部件，按照 5.3.2 规定的试验方法进行可充电储能系统内零部件材料阻燃试验，应满足以下阻燃要求：

a）满足以下任一条件的零部件，其材质需满足水平燃烧 HB 级和垂直燃烧 V-0 级的要求：

——单个零部件重量≥50 g；

——单个可充电储能系统内相同型号的零件总重量＞200 g。

b）其它非金属零部件材质需满足水平燃烧 HB75 级和垂直燃烧 V-2 级的要求。

## 2.4 控制安全

基于 GB/T 34590-4 相关规定，基于系统功能概念和技术安全要求，进行系统级别的安全要求定义，进行系统架构设计，明确软硬件接口定义规范，进行系统级别失效分析，为后续硬件和软件设计提供输入。

### 2.4.1 硬件设计要求

从硬件安全要求定义、硬件设计及实现、硬件失效模式分析、硬件系统测试等四个方面进行硬件设计工作，参考 GB/T 34590-5。

#### 2.4.1.1 硬件安全要求

所设计硬件产品应符合电气性能、环境适应性等车辆系统级要求。

（1）电气性能：所设计的硬件产品应符合 QC/T413 汽车电气设备基本技术条件所规定的电气性能要求；应根据 ISO16750-2 及 GB/T 28046.2 等满足工作电压、电源过电压性能、电源叠加交流电性能、电源电压跌落性能、电源启动特性、电源极性反接、抛负载性能、供电电压缓升和缓降性能、供电电压瞬时下降性能等要求；

（2）环境适应性：应满足车辆运行环境的需求，针对布置在底盘等湿区位置的产品防护等级不应低于 IP67；应根据 GB/T 28046.3 的要求满足低温性能、高温性能、温度冲击性能、温湿性能、盐雾性能、防护性能、自由跌落性能等产品性能要求。

#### 2.4.1.2 硬件设计及实现

需进行硬件架构度量的评估，并将评估结果和优化建议反馈到系统设计、硬件设计、软件设计环节，以优化产品设计。详细设计和实现阶段，应充分考虑功能冗余及功能要求，优先采用汽车级成熟电路单元，元器件选用汽车级芯片，以满足性能、功能及成本的要求。

#### 2.4.1.3 硬件失效模式分析

通过对硬件失效模式分析，识别硬件设计中因潜在风险导致的产品失效，建立 FMEA 表，以保证分析的完整性。对于侵害安全的失效模式，应制定相应的安全机制来保证安全性；对于非侵害安全的失效模式，需评估设定安全机制的必要性。

#### 2.4.1.4 硬件系统测试

为了验证安全机制的完整性和正确性，硬件系统测试应考虑按以下方法进行，通过测试确保所开发的硬件符合硬件安全要求。

（1）功能性测试，即采用黑盒测试技术针对被测硬件的接口规格说明进行测试；

（2）非功能性测试，即对硬件的性能或可靠性进行测试。

### 2.4.2 软件设计要求

基于 GB/T 34590-6 相关规定，进行软件安全要求的定义、软件架构设计、软件单元设计及实现、软件单元测试、软件集成及测试、软件安全要求与验证，并满足系统设计和软件安全需求的要求。

#### 2.4.2.1 软件安全要求的定义

基于 GB/T 34590-6 相关规定，软件安全要求来源于技术安全要求和系统设计规范，软件安全要求的定义考虑硬件的约束及对软件的影响。软件安全要求应针对每个基于软件模块的功能，这些功能的失效可能导致违背分配到软件的技术安全要求。软件安全需求分析阶段需满足完整性、可测试性、可追溯性要求。

#### 2.4.2.2 软件架构设计

基于 GB/T 34590-6 相关规定，软件架构设计描述全部软件组件及其在层次结构中的交互；静态方面，如所有软件组件间的接口和数据路径；动态方面，如进程顺序和时序行为都得到描述。

在软件架构设计应考虑软件架构设计的可验证性、可配置软件的适用性、软件单元设计及实现的可行性、软件集成测试中软件架构的可测性及软件架构的课维护性。软件架构设计需遵循高类聚、低耦合的要求具有模块化、封装性和简单性属性。

软件架构设计中，应使用 FFI(Free From Interface，例如：Time Protection, Memory Protection, Data protection)来避免软件要素间的相互干扰。

#### 2.4.2.3 软件单元设计及实现

基于 GB/T 34590-6 相关规定，基于软件架构设计开发软件单元的详细设计。软件单元的详细设计分别按照建模或编码指南，以模型或直接以源代码的形式实现。在进入软件单元测试前对详细设计和实现进行静态验证。软件单元的实现包含源代码的生成和转换为目标代码。

#### 2.4.2.4 软件单元测试

软件单元测试目的是要证明软件单元满足软件单元设计规范且不包含非预期的功能。

软件单元测试是根据软件单元设计规范，建立软件单元测试流程，并按照该流程执行测试。

在单元测试过程中，为了评估测试用例的完整性并证明没有非预期的功能，应确定软件单元层面的要求覆盖度，同时对覆盖度进行测量，如果认为已实现的结构覆盖率不充分，应增加额外的测试用例或给出接受的理由。

#### 2.4.2.5 软件集成及测试

基于 GB/T 34590-6 相关规定，按照软件架构设计，对软件要素之间特有的集成层次和接口进行测试，软件要素的集成和测试的步骤直接对应着软件的分层架构。

软件集成应完成各个软件单元分层集成到软件组件，直到整个嵌入式软件被集成，并考虑与软件集成相关的功能依存关系和软件集成和软硬件集成之间的依存关系。

在软件集成测试过程中，为了评估测试用例的完整性并证明没有非预期的功能，应确定软件集成层面的要求覆盖度，同时对覆盖度进行测量，如果认为已实现的结构覆盖率不充分，应增加额外的测试用例或给出接受的理由。

#### 2.4.2.6 软件安全要求验证

基于 GB/T 34590-6 相关规定，软件安全要求验证的目的是证明嵌入式软件在目标环境下满足软件安全要求。

软件安全要求验证中的测试环境可为硬件在环，测试台架，或者整车环境。可考虑使用工具(例如：traceability matrix)确保和评估软件安全要求的覆盖率，可以复用已有的测试用例。如果覆盖率不充分，应增加测试用例或给出可以接受的理由。

### 2.4.3 功能和操作设计

#### 2.4.3.1 上下电操作设计

整车控制系统应能控制 B 级电压电路的通断顺序，通电时，应先接通低压、后接通高压，断电时，应先断开使能信号使高压部件停止工作，后断开低压控制信号切断高压。

整车上高压时应检测制动踏板和档位信号，断电时只需断开电源开关即可。

#### 2.4.3.2 档位操作设计

换挡操作应在踩下制动踏板制动有效的情况下换挡有效。

#### 2.4.3.3 充电操作设计

当充电枪和整车连接时，整车不能发出扭矩驱动车辆行驶。

#### 2.4.3.4 转向操作设计

车辆在行驶过程中，出现需要整车主动断 B 级高压电的车辆异常情况时，应能通过声光报警通知驾驶员，且在车速大于 5km/h 时应保持转向系统维持助力状态或至少保持转向

助力状态 30 s 后再断 B 级电。

#### 2.4.3.5 制动优先设计

车辆行驶过程中，当制动踏板和加速踏板同时有效时，车辆应只响应制动踏板信号。

#### 2.4.3.6 车辆故障等级显示及处理机制

针对不同故障等级，各主机厂依据自身情况制定不同的故障处理机制，可参考下表：

| 故障级别 | 三级故障 | 二级故障 | 一级故障 |
|---|---|---|---|
| 说明 | 严重故障 | 较严重故障 | 警告故障 |
| 处理机制 | 通知驾驶员尽快切断驱动力 | 限制扭矩输出 | 仪表提示 |

针对不同故障等级，各主机厂依据自身情况制定不同的故障显示机制，可参考下表：

| 故障级别 | 三级故障 | 二级故障 | 一级故障 |
|---|---|---|---|
| 说明 | 严重故障 | 较严重故障 | 警告故障 |
| 仪表显示机制 | 声音警告，仪表显示整车三级故障 | 声音警告，仪表显示整车二级故障 | 仪表显示整车一级故障 |

## 2.5 碰撞安全

### 2.5.1 侧面碰撞防护设计

侧面防护结构按照《电动客车安全技术条件》附录 C 进行碰撞试验，车辆在碰撞试验后应符合 GB/T31498 中 4.2～4.4 的要求。

### 2.5.2 侧翻防护设计

车身防护结构若按 GB17578 进行上部结构强度验证试验，应在其可充电储能系统荷电量（SOC）30%～50%且处于上电状态下进行试验，试验后应符合 GB/T31498 中 4.2～4.4 的要求。

### 2.5.3 追尾碰撞防护设计

后高压舱 B 级电压部件的布置位置和防护结构应考虑被追尾后，符合 GB/T31498 中 4.2～4.4 的要求。

### 2.5.4 底部碰撞防护设计

底部碰撞防护设计要考虑两方面，一是离地间隙，二是防护结构。若动力电池布置在地板下，轴间最小离地距离建议设计为轴距的 4%或 3.3%（对于安装空气悬架的车辆），但不得小于 190mm，同时考虑防护结构设计，防护设计应能满足发生底部碰撞后符合 GB/T31498 中 4.2～4.4 的要求。

## 2.6 逃生安全

### 2.6.1 逃生窗的设计

（1）应急窗和撤离舱口的面积应大于或等于（$4\times10^5$）$mm^2$，且能内接一个 500mm×700mm（对车长小于或等于 7m 的客车为 450mm×700mm）的矩形；如应急窗位于客车后端面，则能内接一个 350mm×1550mm、四角曲率半径小于或等于 250mm 的矩形时也视为满足要求。

（2）应急窗应采用易于迅速从车内、外开启的装置；或采用自动破窗装置；或在车窗玻璃上方中部或右角标记有直径不小于 50mm 的圆心击破点标志，并在每个应急窗的邻近处提供一个应急锤以方便地击碎车窗玻璃，且应急锤取下时应能通过声响信号实现报警；客车后围应急窗的玻璃破碎装置应位于应急窗的上方或下方的中间位置，或者左右两侧均放置玻璃破碎装置。

（3）设有乘客站立区的客车车身两侧的车窗，若洞口可内接一个面积≥800mm×900mm 的矩形时，应设置为推拉式或外推式应急窗；若洞口可内接一个面积≥500mm×700mm 的矩形时，应设置为击碎玻璃式的应急窗，并在附近配置应急锤或具有自动破窗功能（侧窗洞口尺寸在车辆制造完成后从侧窗立柱内侧测量）。

（4）公路客车、旅游客车和未设置乘客站立区的公共汽车，车长大于 9m 时车身左右两侧应至少各配置 2 个外推式应急窗并应在车身左侧设置 1 个应急门，车长大于 7m 且小于等于 9m 时车身左右两侧应至少各配置 1 个外推式应急窗；外推式应急窗玻璃的上方中部或右角应标记有击破点标记，邻近处应配置应急锤；其他车长大于 9m 的未设置乘客站立区的客车，车身左右两侧至少各有 2 个击碎玻璃式的应急窗（车身两侧击碎玻璃式的应急窗总数小于等于 4 个时为所有击碎玻璃式的应急窗）具有自动破窗功能的，应视为满足要求。

（5）水平铰接于上端的应急窗，应有一个适当的机构保持其充分开启。铰接式应急窗的开启应保证车内外进出的畅通。

（6）客车侧窗的下边缘(推拉窗指金属下边框的上边缘)距其下方脚踏处地板平面（不含任何局部改变，如车轮、传动装置或卫生间等引起的局部变形）的高度应小于或等于 1200mm，且大于或等 500mm。对于推拉式和外推式侧窗，若可开启部分的下边缘低于 650mm，应在距地板 650mm～700mm 高度处设防护装置防乘客坠落车外；若该侧窗作为应急窗，其防护装置上方的洞口面积应大于或等于应急窗的最小尺寸；若侧窗洞口下边缘距其下方地

板平面大于或等于 650mm，也可不设防护装置。

（7）对驾驶员不能在座位上清楚看见的铰接式应急窗，应安装声响报警装置，该警示装置应由窗锁或把手(并非窗子本身）的运动来启动，当应急窗未完全关闭时提醒驾驶员。

### 2.6.2 逃生门的设计

（1）应急门的净高应大于等于 1250mm，净宽应大于等于 550mm；但车长小于等于 7m 的客车，应急门的净高应大于等于 1100mm，若自门洞最低处向上 400mm 以内有轮罩凸出，则在轮罩凸出处应急门净宽可减至 300mm。

（2）车辆侧面的铰接式应急门铰链应位于前端，向外开启角度应大于等于 100°，并能在此角度下保持开启。如在应急门打开时能提供大于等于 550mm 的自由通道，则开度大于等于 100° 的要求可不满足。

（3）通向应急门的引道宽度应大于等于 300mm，不足 300mm 时允许采用迅速翻转座椅的方法加宽引道。专用校车沿引道侧面设有折叠座椅时，在折叠座椅打开的情况下（对在不使用时能自动折叠的座椅，在座椅处于折叠位置时），引道宽度仍应大于等于 300mm。

（4）应急门应有锁止机构且锁止可靠。应急门关闭时应能锁止，且在车辆正常行驶情况下不会因车辆振动、颠簸、冲撞而自行开启。

（5）当客车停止时，应急门不用工具应能从车内外方便打开，即使从车外将门锁住，也应能用正常的开启装置从车内打开。车外应急门开启装置应由易于被移开或打破的装置来保护。客车不应安装有其他固定、锁止应急门的装置。

（6）客车(包括双层客车的下层)应急门的车外开启装置应距地面 1000mm- 1800mm，且距该门小于或等于 500mm；I 级、II 级和 III 级客车应急门的车内开启装置应距其下方地板(或踏步)的上表面 1000mm-1500mm，且距该门小于或等于 500mm。本规定不适用于位于驾驶区内的操纵件。

（7）所有应急门都应提供声响装置，在应急门未完全关闭时提醒驾驶员。该提醒装置应由门的锁止装置（例如，门闩或把手）的运动，而不是门本身的运动来启动。

### 2.6.3 逃生时间要求

操作乘客门应急控制器 8s 内应使乘客门自动打开或用手轻易打开到相应的乘客门引道量规能通过的宽度。

## 2.7 EMC 安全

### 2.7.1 整车车外辐射骚扰及抗扰度要求

整车对外部的电磁骚扰应满足 GB/T 14023、GB/T 18387 相关要求，以保护车辆外部的无线电通讯设备正常工作；

整车耐受外部的电磁辐射干扰应满足 GB/T 34660 相关要求，以保障车辆的功能状态和安全等级。

### 2.7.2 车载电器设备辐射骚扰及抗扰度要求

车载电器设备辐射骚扰及抗扰度应满足表 2-2 要求：

表 2-2

| 测试项目 | | 国标要求 |
|---|---|---|
| 发射 | 辐射发射 | GB/T 18655-2018 |
| | 传导发射 | GB/T 18655-2018 |
| | 瞬态传导发射 | GB/T 21437.2-2008 |
| 抗扰度 | 电波暗室法 | GB/T 33014.2-2016 |
| | 大电流注入 | GB/T 33014.4-2016 |
| | 瞬态传导抗扰度(电源线) | GB/T 21437.2-2008 |
| | 瞬态传导抗扰度(信号线) | GB/T 21437.3-2012 |
| | 静电放电 | GB/T 19951-2005 |

### 2.7.3 整车充电过程中沿电源线骚扰和抗扰度要求

车辆处于电源线传导充电工况模式，沿电源线骚扰和抗扰度建议参照 ECE R10.5 试验验证，满足相关要求。

### 2.7.4 整车乘员暴露于车辆电磁环境安全要求

整车乘员暴露于车辆电磁环境应满足 GB/T 37130 中的相关要求。

### 2.7.5 高低压线束设计布置要求

高压线束应具备 EMC 屏蔽措施，其走向布置不应形成 EMC 辐射增强。高压线束屏蔽层应与高压部件可导电外壳有效连接 。

## 2.8 存储、运输安全

### 2.8.1 存储安全

#### 2.8.1.1 场地要求

（1）存放场地应为专用停车场，应通风、排水良好，极端情况下积水深度不能超过300mm；

（2）存放场地位置应远离加油站、加气站、热源、潮湿、可燃设施/可燃物质堆放区域、有腐蚀性气体以及灰尘较大的地方，同时还应避免其他车辆或移动的物体对车辆造成撞击或挤压，为防止意外事件的二次影响，还应远离居民区或人群聚集区；

（3）存放区域周围 10 米内严禁进行金属切削、焊接或打磨工作；

（4）专用停车场应有视频监控装置及人员定期巡视机制，周期不得低于 3 次/天，巡视要有记录存档（存档周期一个月）。

#### 2.8.1.2 存放要求

（1）车辆存放时，建议两车之间的间距不小于 2m（车辆四周均需满足）；

（2）车辆长期储存（超过 3 个月）时，断 24V 总开关。环境温度在-30 ℃～50 ℃以内，SOC（荷电状态）40%～70%储存，储存环境湿度 5%～95%；超过 6 个月需要将电池充满电后再放电至 40%～70%并重新计算存储周期。否则可能会引起动力电池过度放电，降低电池性能；

（3）在环境温度为 0℃以下时，短期停放（一周内）车辆 SOC 需保证在 70%～80%；

（4）对于存储 3 个月以上车辆，重新投入运营前，还应进行如下保养项目：打开各电池舱，观察电池包与底盘车架固定是否牢靠。此过程同步观察高低压线束及连接器紧固情况，确认是否有松动及损坏；观察电池包情况，确认是否有变形、外盖损坏、异味、鼓胀。

——观察电池包固定点漆标是否错位，并用力矩扳手重新打力矩以确认力矩是否衰减并重新紧固电池包。

（1）使用压缩空气清除所有维修舱内的灰尘与杂物；

（2）将清洁完毕的车辆移至车库或停车场后，拉起驻车制动手柄，将档位退到 N 档，将钥匙打到 OFF，断开电源总开关；

（3）关闭车辆所有车窗玻璃，关闭车辆所有维修舱门并用机械钥匙锁紧。舱门应该保持关闭状态锁止，不能随意开启；

（4）关闭所有乘客门，断开电源总开关，妥善保管智能钥匙；

（5）长期停放的车辆，应由具有专项培训合格记录的人员对整车及关键零部件和车载储能装置、系统等，进行定期检查、维护，检查结果应有详细的记录存档。

#### 2.8.1.3 灭火设施配置要求

停车场停放时，车辆 5 m 内两边各摆放一个 $CO_2$ 灭火器或干粉灭火器，灭火器摆放位置便于取用；停车场需要配备足够的消防用水，电池起火的情况下，相关人员要与事故车辆保持至少十米距离，采用消防栓水带射水灭火，同时持续给电池系统降温。

### 2.8.2 运输安全

#### 2.8.2.1 拖运要求

采用非行驶方式运输时，应使用专用工具或升降台装运，防止车身和零部件变形损坏；装运时，客车之间应保留足够的间隔，用楔形块塞好车轮，并用绳索将客车拉牢，防止车辆滑移；装运后，应实施驻车制动，关窗锁门，按需加以覆盖，建议 SOC 在 40%-70%之间。

运输车辆，应尽可能远离火源、热源、高压线、易燃、易爆等危险物品，并设置高压警示标志。

#### 2.8.2.2 自运要求

采用自行行驶时，应遵守说明书中新车行驶的各项规定。

（1）评估当前电量是否满足目的地里程要求，避免电量不足导致车辆抛锚；

（2）车辆自运前必须做一个安全检查；

（3）车辆内灭火器配备必须齐全；

（4）车辆必须空载；

（5）禁止急加速急制动。

#### 2.8.2.3 事故后救援运输

发生事故后，在不能将事故车辆装运时，需要考虑事故车辆拖车的方便性，按照车辆使用说明书约定的拖车方式进行拖车，避免拖车过程中电机出现高温或反电动势过高，引发安全事故。

## 2.9 安全检查

### 2.9.1 日常检查

每日由驾驶员在出车前、行车中、收车后执行。新能源系统的日常检查项目如下：

表 2-3　新能源系统的日常检查项目

| 序号 | 维护项目 | 作业内容 | 技术要求 |
|---|---|---|---|
| 1 | 清洁 | 清洁新能源各部件 | 清洁高压发电机、驱动电机、电动转向油泵、电动空压机、高压控制柜等 |
| 2 | 检查 | 检查新能源高压舱 | 1）舱门锁止有效，舱内无灰尘、不漏水<br>2）高压线端子不露铜、不松脱、不磨蹭<br>3）动力电池箱及各接线头固定可靠<br>4）高压舱换气风扇工作正常，舱内温度显示正常 |
| | | 检查电机水冷系统 | 1）检查水箱水位，不足时添加<br>2）检查管路无弯曲、折叠、漏水现象 |
| | | 动力电池 | 1)箱体固定可靠，箱体表面无明显灰尘、锈蚀、变形<br>2)电池舱内干燥、清洁<br>3)各箱体高低压线连接正常，固定可靠，无松动现象 |
| | | 检查驱动电机、高压发电机、电动转向油泵、电动空压机 | 1）电机固定牢固<br>2）电机无异响、无故障<br>3）检查电动转向油泵、电动空压机无漏油、漏气等现象 |
| | | 检查仪表、档位操纵面板 | 显示正常、无故障 |

### 2.9.2 例行检查

依据使用说明书对车辆进行例行检查，新能源系统检查作业项目如下：

表 2-4　新能源系统检查作业项目

| 序号 | 检查项目 | 作业内容 | 作业要求 |
|---|---|---|---|
| 1 | 电动转向油泵 | （1）检视、清洁<br>（2）检查高压、低压插接口<br>（3）转向电机接地检测 | （1）除尘，保持干燥、干净，转向油泵壳体、接头无渗漏<br>（2）高压、低压插接口插接牢固、无端子松动<br>（3）接地线牢固、不松动，转向电机与车体之间的接地电阻应小于 0.1Ω 。 |
| 2 | 高压控制盒 | 检视、紧固控制盒箱体 | （1）控制盒固定牢固、不松动 |

| 序号 | 检查项目 | 作业内容 | 作业要求 |
| --- | --- | --- | --- |
| | | | （2）除尘，保持干燥、干净<br>（3）维修开关可正常断开、熔断器无高温变色，断路器工作正常 |
| 3 | 驱动电机控制器、高压发电机控制器 | （1）检查接线情况<br>（2）检视、清洁<br>(3)电机控制器壳体接地检测<br>（4）检查低压插接口<br>（5）电机冷却水管 | （1）接线牢固、不松动<br>（2）除尘，保持干燥、干净，冷却水管无老化、变形、渗漏<br>（3）电机控制器壳体与车体之间的电阻，应小于0.1Ω<br>（4）低压插接口插接牢固、无端子松动<br>（5）水管及接头可靠、无破损 |
| 4 | DC/DC、DC/AC、多合一控制器 | （1）视检各接线桩<br>（2）检视、清洁 | （1）固定可靠，表面干燥、干净<br>（2）各接线桩头不松动、不允许裸 |
| 5 | 动力电池组 | （1）检查电池箱<br>（2）视检固定及各接线桩<br>（3）电池电压及温度<br>（4）绝缘检测<br>（5）检查单体电池压差 | （1）检验动力电池组电芯电压、温度、压差、绝缘阻值等是否正常<br>（2）各接线桩头不允许裸露，<br>（3）检测单体电池电压压差不超标，温度不超过说明书要求。<br>（4）电池总正、负极对地绝缘电阻应大于标准值<br>（5）单体电池电压压差不超标 |
| 6 | 驱动电机<br>高压发电机 | （1）检查U、V、W端子接线、与屏蔽层接地情况<br>(2)检视电机输入线及接线盒<br>（3）检查清洁驱动电机表面灰尘情况<br>（4）检查低压插接口<br>（5）检查电机工作 | （1）U、V、W 端子接线牢固、无松动；检查电机外壳接地电阻小于0.1Ω<br>（2）输入电线的绝缘层无破损，接线盒完好<br>（3）驱动电机表面去尘，保持干燥、干净，散热筋的沟槽内无异物，冷却水管无老化、变形、渗漏<br>（4）低压插接口无破损，旋变线接线、高温传感器线固定可靠，有效<br>（5）试车，电机工作时无异响 |
| 7 | 电动空压机总成 | （1）检视空压机电源线和搭铁线 | （1）空压机总成电源线、搭铁线牢固，无松动<br>（2）油位正常 |

| 序号 | 检查项目 | 作业内容 | 作业要求 |
| --- | --- | --- | --- |
| | | （2）检查空压机油位<br>（3）检查、清洁空压机空气滤清器电机绝缘检测 | （3）清洁空压机空气滤芯<br>（4）电机三相线对地绝缘电阻应大于 2MΩ |
| 8 | 电动空调 | （1）检查空调机组<br>（2）空调绝缘检测 | （1）空调各部件表面清洁，不漏水，固定可靠，高低压接线不松动，不磨蹭<br>（2）空调压缩机、变频器高压线与地之间绝缘电阻高于 2MΩ |
| 9 | 电机水冷系统 | （1）管路<br>（2）水泵<br>（3）冷却水箱 | （1）管路无老化、变形、渗漏<br>（2）水泵工作正常<br>（3）水箱表面清洁、无损伤、无渗漏，风扇工作正常 |
| 10 | 充电接口 | 检查、清洁 | （1）充电接口固定可靠，无破损，烧焦等再现象<br>（2）插座内部干燥、清洁 |
| 11 | 绝缘检查 | （1）高压控制柜<br>（2）驱动电机、高压发电机、助力泵高压输入线 | （1）高压控制柜高压线与地之间电阻高于 2MΩ<br>（2）如遇下雨季节，还需单独对驱动电机、高压发电机、助力泵电机进行绝缘检查 |

### 2.9.3 年检机制建立

参照传统车辆、部件的年检方案，制定新能源部件的年检要求，降低新能源部件故障，减少新能源车安全风险。

| 建议补充年检项目 | |
| --- | --- |
| 动力电池系统 | 高压部件安全标示 |
| 电机控制器 | 整车绝缘 |
| 充电插座 | 电动空压机 |
| 灭火系统有效期 | 驱动电机 |
| 超级电容 | 低压/高压电气控制系统 |

## 2.10 电驱动总成安全

### 2.10.1 电安全

**2.10.1.1 耐压：**按照电压等级区分，冷态、热态要求不同施加频率为 50Hz~60Hz 的交流电压 1min，电压为（2*最大工作电压+1000）V（rms），实验过程中不发生介质击穿或电弧现象。

**2.10.1.2 绝缘：**按照电压等级区分，冷态、热态要求不同满足 H 级，动力端子与外壳、信号端子与外壳、动力端子与信号端子之间冷态及热态绝缘均应不小于 2MΩ 。

**2.10.1.3 接地：包括对屏蔽、接地要求**

电机、电机控制器外壳需要使用符合要求的铜线或铜编织线可靠接地，三相线和直流母线屏蔽层需可靠接地。驱动电机及驱动电机控制器中能触及的可导电部分与外壳接地点处的电阻不应大于 0.1Ω，并且具有明显的接地标志。

**2.10.1.4 故障下的安全性处理：降额、关机、三相短路、断路**

如表 2-5，根据不同的故障等级，驱动电机系统应能够实现降额、通知驾驶员关机、三相短路和断路等功能，确保系统安全。表中具体参数需要根据实际电压平台和系统设计与整车单位协商确定。

表 2-5　故障情况及处理措施

| 参数名称（高压） | 参数值 | 处理措施 |
|---|---|---|
| 过压报警电压 | TBD | 超过该电压，电机报警告，降额运行 |
| 过压故障电压 | TBD | 超过该电压，电机报过压故障，关脉冲停机 |
| 欠压报警电压 | TBD | 母线电压低于该电压时，电机报欠压警告，降额运行 |
| 欠压故障电压 | TBD | 母线电压低于该电压时，电机报欠压故障，关脉冲停机保护 |
| 转速一级（轻微）故障 | TBD | 超过该转速，电机报故障，降额运行 |
| 转速二级（一般）故障 | TBD | 超过该转速，电机报故障，零转矩输出 |
| 转速三级（严重）故障 | TBD | 超过该转速，电机报故障，关脉冲停机保护 |
| 电机过温报警（降额） | TBD | 控制器过温报警（降额） |
| 电机过温（关脉冲） | TBD | 控制器过温（关脉冲） |

### 2.10.2 机械安全

#### 2.10.2.1 转子强度

在设计阶段进行强度分析，通过实验以及其他类似产品的具体使用情况进行验证；驱动电机在热态下应能承受 1.2 倍最高工作转速试验，持续时间为 2min，其机械应不发生有害变形。

#### 2.10.2.2 壳体强度：碰撞安全

按照车辆的强度标准，对电机壳体进行有限元分析，并进行相关的震动实验进行验证，并符合国标要求：三个方向施加 10kPa 压强后，控制器不发生明显塑性变形。

#### 2.10.2.3 机械防触碰与警告

在旋转或有相对运动的部位贴警告标识。

### 2.10.3 热安全

#### 2.10.3.1 热预警、降额、保护

电机定子安装温度传感器，电机及控制器具有过温限功率及过温保护功能。

#### 2.10.3.2 转子退磁：高温下的退磁安全、转子温度估算

使用冷却水道对电机壳体进行散热，保证电机内部温度在正常温度以下。

#### 2.10.3.3 密封材料耐温、绝缘材料耐温。

密封材料耐温：电机全工况下，确保油封、O 型圈等密封材料可靠实用。

绝缘材料的耐温：绝缘材料耐温≥H 级，且在电机过温时能启动过温保护机制，避免温度进一步上升，确保温度传感器正常工作。

#### 2.10.3.4 阻燃材料使用：线束、注塑件

线束、注塑件均达到水平燃烧 HB 等级、垂直燃烧 V-0 等级。

### 2.10.4 防护安全

#### 2.10.4.1 防水/防尘设计：端盖、轴密封性设计

端盖、轴承采取合理的密封措施，防护等级不低于 IP67，且应满足 2.2.1 的要求。

#### 2.10.4.2 绝缘检测：与 VCU、BMS 配合检测

绝缘检测仪实时检测高压零部件对车身的绝缘电阻，当检测到绝缘电阻值低于设定值时，采取报警、下高压电等保护措施。

# 3 电池单体和模组

## 3.1 电池单体安全要求

### 3.1.1 电池单体制造环境要求

锂离子电池单体生产过程温度、湿度环境条件必须确定并得到保证。对于超出温度、湿度极限值的情况，应当制定适当的应对方案。锂离子电池对水分非常敏感，电极车间相对湿度应控制在 20%以下，装配车间注液工序应控制在 1%以下。

生产过程粉尘度必须控制。需要防止外来的颗粒物渗透到任何生产区域。生产系统需要防止金属磨损，如果不能防止金属磨损，应采取适当措施保证这些磨损产生的颗粒不进入生产过程。

应对检测到的粒子进行常规分析，以确定粒子的数量、大小和组成，特别是在导电性(如金属粒子)方面。颗粒数量、大小、成分超出规格要求应立即采取纠正措施，粉尘度应控制在 10 万级以下，部分关键工序应在 1 万级以下。

### 3.1.2 电池单体设计

#### 3.1.2.1 电池单体分类

目前用于动力的锂离子电池根据外型分为圆型电池、方型电池和软包电池。根据电池单体使用的正极活性物质不同，分为磷酸铁锂电池、锰酸锂电池、钴酸锂电池、三元电池等。

#### 3.1.2.2 电池单体容量

动力电池单体容量决定了后期电池模组和系统的组合方式和电池模组的热管理设计。较小容量电池单体有利于热的扩散，对整体电池系统热管理设计有益。较大容量电池单体有利于组合系统设计和制造过程简单化、成组率的提高和比能量的提升。

不断提升电池单体的比能量是长期、系统的工作，建议要在确保安全性、可靠性和关键电性能指标的前提下，提升电池单体的比能量。

#### 3.1.2.3 电池单体关键原材料

##### 3.1.2.3.1 正极材料

目前商品化的正极材料有钴酸锂、锰酸锂、三元材料（NCM 和 NCA）和磷酸铁锂。正极材料种类对电池的安全影响至关重要，一般采用差热分析方法比较正极材料的热稳定性。

为进一步改善正极本体热稳定性和正极材料电解液界面稳定性，通常采用掺杂和包覆

工艺，显著提升电池单体的安全性和循环性能。

正极材料水分含量、粒度分布、颗粒形貌、结晶形状、金属杂质和磁性物质(Fe-Ni-Zn-Cr)含量直接影响电池单体的安全特性，在整个原材料评价、供应商审核、生产现场应制定并优化控制标准。材料中的磁性物质含量控制在 50ppb 以下。

商用车推荐使用安全性高的磷酸铁锂和锰酸锂正极材料体系，乘用车考虑安全性和性能的平衡，推荐使用磷酸铁锂、锰酸锂和三元材料正极材料体系。

#### 3.1.2.3.2 负极材料

目前商业化锂离子电池负极材料主要是人造石墨、天然石墨、钛酸锂负极和硅碳复合石墨材料。为改善负极材料电解液界面稳定性，应对材料表面做包覆处理，减少副反应，提升电池单体循环性能和安全性能。

负极材料的反应活性随着比表面积的增加呈指数增加。比表面积过大，在电池发生内部短路或局部过热时，负极与电解液的副反应增加，产热量大，更容易引发电池热失控。负极材料的比表面积应该控制在合适的范围内。

负极材料伴随着锂离子的脱出嵌入会有明显的体积变化，体积变化过大会引起极片变形和极组内部压力增大，进而引发极片不平整部位的内短路。因此负极材料的选择要考虑膨胀率对安全的影响，根据电池单体不同结构设计对材料膨胀率提出上限要求。

负极材料杂质含量、比表面、粒度分布、颗粒形貌等直接影响电池单体的安全特性，在整个原材料评价、供应商审核、生产现场应制定并优化控制标准。

#### 3.1.2.3.3 隔膜

隔膜的作用是将正负极物理上隔离，阻止电池单体正负极短路，同时提供离子转移通道。隔膜材料要具有足够的化学、电化学、热特性和一定的机械稳定性。隔膜在长度和宽度上的尺寸可能由于温度、自身老化等原因而收缩变化，在正常工况环境条件下，都需要保证隔膜对正极和负极的完全覆盖。

对于聚烯烃类隔膜，要有较好的热稳定性、自动关断保护性能和力学稳定性；具有高绝缘性，至少耐受 250V 的高压绝缘测试；管控热收缩率，防止电池单体受热后出现大面积内短路引发热失控。穿刺强度对电池的安全性有较大影响，要优先选用穿刺强度高的隔膜。隔膜厚度和电池单体安全性强相关，动力电池隔膜厚度的选择建议充分考虑由于降低隔膜厚度带来的安全风险。

涂覆隔膜具有优良的热稳定性和抗氧化能力，对单体电池安全有益。

#### 3.1.2.3.4 电解液

电解液由电解质和溶剂两部分组成，主要是起到在正负极间传输锂离子的作用。电解液应在正负极表面形成稳定界面，具有较宽电化学工作窗口、强的抗氧化还原能力。电解液要有良好的极片浸润特性，使得电极反应均匀、快速，防止局部电解液干涸，形成死区析锂。

理想的电解液添加剂可以有效改善电池单体的电性能和安全性能。针对负极的电解液添加剂可以在负极表面形成稳定的 SEI 膜，提升电池单体循环性能和安全特性。针对正极的电解液添加剂可以防止电液氧化、正极材料溶出，提高电池单体循环性能和安全性能。正极过充添加剂可以在过充高电位滥用条件下，能够产生足够气体触发安全保护装置，终止电池单体充电，起到安全保护的功能。

电解液组分应具有良好的稳定性，保证使用过程不分解不变色，并做严格管理，电解液水分含量应小于 20ppm，HF 含量应小于 50ppm。

采用六氟磷酸锂为电解质，碳酸酯为溶剂的锂离子电解液在电池安全中有助燃作用，开发热稳定性高新型锂盐、阻燃溶剂、固态电解质，可以大幅度提高电池单体安全特性。

#### 3.1.2.3.5 壳盖设计

电池壳盖需要一定的强度和良好的密封性。

圆型电池和方型电池一般使用镀镍钢和铝材，可考虑设置有效的安全保护装置，具备如断电、熔断、泄压等功能。熔断电流、触发压力等参数要经过严格的实验设计和优化验证，既要保障电池在滥用条件下及时开启又要保证振动冲击条件下的可靠性和安全性。由于密封圈具有在较高热变形较大和遇高温熔化的特性，以及电解液的强腐蚀性，为了在电池单体全生命周期内保证密封的可靠性，需要考虑密封圈的耐高温、耐电解液腐蚀、耐老化。

软包电池使用铝塑多层膜做包装材料，通过热封的方式形成电池单体的壳体，在电池单体全生命周期内保证密封性的同时，电池单体内部压力增大时可从封装处泄压。铝塑多层膜材质、厚度、封装条件对电池单体密封性和安全性影响较大。

#### 3.1.2.3.6 箔材

锂离子电池一般负极使用铜箔、正极使用铝箔，起到正负极集流的作用。箔材要求高延展率、高强度，保证全生命周期电池的安全性。箔材表面的金属粉尘、油含量、达因值等关键指标要有效控制。

对铜铝箔的表面处理可以有效改善活性物质层和箔材结合力，减少工艺过程中电极物

质脱落问题和循环过程中电极剥离问题。

#### 3.1.2.4 电极设计

N/P 比是指单位面积负电极容量和正电极容量之比。在考虑涂覆量、材料克容量和极组结构等因素的公差条件下，在电池全生命周期内最小 N/P 比不低于 1.0（钛酸锂电池除外）。

电极的配方要经过实验优化，要保证粘合剂充足，防止电极活性物质脱落。锂离子电池电极具有三维多孔结构，要有良好的电子导电性和离子导电性。电极涂覆量、厚度、孔隙率要经过理论模拟和实验优化，保证在极限使用条件下负极不会有金属锂的析出。

电极纵向毛刺超出电极表面的部分不应大于隔膜总厚度的一半。

#### 3.1.2.5 极组设计

极组中负极的设计长度应能保证极组完全覆盖正极。在长度和宽度方向要保证隔膜对负极、负极对正极的覆盖。应做正负极电极之间短路分析，对短路薄弱区域进行绝缘保护。

极耳材质、长度、宽度和厚度设计具备与电池应用条件相匹配的电流承载能力，要保证焊接部位稳定可靠。极耳外露极组长度和极耳弯折点设计要保证不与电池壳发生短路。极耳应有保护胶带进行有效保护。极耳切断毛刺要严格管控。

极组中所有保护胶带应不溶于电解液，具有一定热稳定性、机械强度和粘结力。

极组的外型尺寸应设计与壳盖空间匹配，要对各个方向尺寸开展公差分析。极组外有保护胶带或保护套，防止装配时极组损伤。

#### 3.1.2.6 散热设计

电池单体在大倍率充放电时，电池内部会产生大量的热，温度升高，易引起安全问题。电池单体结构设计要模拟分析电池内部发热量分布、热扩散路径和传递速度，验证优化散热设计。

### 3.1.3 电池单体制造

#### 3.1.3.1 电极制造

##### 3.1.3.1.1 电极制造要求

电池单体电极制造包括制浆、涂覆、碾压、剪切四个部分，整个电极制造部分实施正负电极车间严格隔离策略，防止正负极粉尘交叉污染。

##### 3.1.3.1.2 制浆

制浆是将活性物质、导电剂、粘接剂等按照一定比例均匀的分散在溶剂中，形成稳定浆料的过程。原材料要检验合格并且可追溯。制浆过程中要确保各物料比例、分散参数等

符合规范，应采用适当的测量方法对浆料的分散效果和一致性进行检验。

识别线体上与材料和浆料接触易产生金属异物的部位，并进行管理，避免异常磨损导致的金属异物引入。采取除磁措施，并对磁性异物制定标准，进行管控。

制浆全过程密闭管理，防止材料泄漏或异物引入。

制浆过程的过滤装置规格和更换频次被定义，并对浆料颗粒度进行有效的监控管理。

#### 3.1.3.1.3 涂覆

涂覆工序是将制备好的浆料均匀的涂覆到基体箔的表面，然后通过烘烤让浆料中的溶剂完全蒸发的过程。

涂覆设备应能够实时连续监控面密度，超过工艺范围应能够报警并在后面的工序处理。极片的尺寸应能够实时监控，超过工艺范围能够报警并在后面的工序处理。

浆料在涂覆前需要经过过滤和除磁处理。

涂敷过程中的极片外观、粘接力、溶剂残留量需要监控。进入烘箱内部的风应有除尘、除湿控制措施。

使用含有有机溶剂的浆料涂敷时，涂布机的烘道需要配备 NMP 浓度自动监控装置，自动监测并具备报警、超限停机功能，建议控制 NMP 蒸气浓度不大于爆炸下限的 50%。如果是采用电加热方式，设备直接接触 NMP 蒸气的电热部分需要使用防爆电器，设置阻止异物点燃设施，停机排风的延时功能。

#### 3.1.3.1.4 碾压

碾压的作用是使涂敷后极片致密，提高电极的电子导电性。碾压过程应对碾压压力，速度和收放卷张力等工艺参数进行监控。对电极的延展和孔形态有监控措施。可利用非接触式在线测厚装置监控极片碾压过程工程能力。

碾压机应具备毛刷、磁棒等清洁装置，定期对碾压辊磨损及有效宽度进行检查，以保证碾压质量。

#### 3.1.3.1.5 电极成形

剪切电极成型是将碾压完成后的大卷极片按照一定的宽度分切成多个小条，极片宽度应符合设计要求。极片边缘毛刺做到持续检测。剪切切刀应按照规定频次进行修磨和维护。在剪切过程中应采取适当的防护措施，防止粉尘在极片表面上沉积。剪切机应具备毛刷和磁棒等清洁装置，及极片外观缺陷和分切宽度等监测装置，并有措施保证有缺陷的极片在后续过程中避免使用。

激光切电极成型是采用激光切和剪切工艺，在集流体上加工出所需形状，加工成型的

电极宽度、极耳尺寸等应符合设计要求。严格控制激光切毛刺，激光切边缘熔珠不超出极片厚度。设备激光切机构、剪切机关键备件规格和更换维保频次需要被定义，并进行有效的寿命监控管理。激光切电极所产生的飞溅粉尘和线体上与极片接触产生粉尘都应得到有效收集处理，避免异物引入极片。设备除尘机构需要被设计，点检、清洁、更换频次需要被定义，并进行有效的监控管理和定期进行异物分析，确保除尘机构作用的有效性。激光切后极片的尺寸应能够连续监控，超过工艺范围能够报警并进行不良品标识，在后工序处理。

#### 3.1.3.2 极组制成

极片的转移和运输要使用专用密闭运输设施，对极片卷实施有效防护和隔离，防止极片发生交叉污染，异物污染，碰撞等损害。

卷绕机除尘功能应具备有效的防交叉污染能力，正负极以及隔膜间应有防尘。隔膜需安装去除静电装置。具备安装有毛刷和吸尘装置，可以有效收集掉粉和落粒。超声焊接位置有吸尘措施，防止焊接振落的金属粉末、粉尘等落入极组。保持挂料轴、过轮、卷针、切刀、传感器清洁无异物，防止污染以损伤极片和隔膜表面。所有设备零件严禁使用铜、锌材料。

极片切断处毛刺和极耳切断处的毛刺要有控制要求，切刀要进行有效的管理。极耳和焊接位置绝缘胶带要有效覆盖。

卷绕过程中张力要根据隔膜特性合理设置，避免张力过大导致隔膜断裂或者隔膜孔变形。隔膜收尾长度要有效控制，隔膜切断处不应有裂口，抽丝现象。极组烫孔时不应损伤极组，控制烫孔温度不会造成隔膜烫伤以及收缩。

极组采用自动方式下料，避免人手触碰，要防止极组机械夹爪夹伤、损伤极组。极组100%经过绝缘电阻检测。

#### 3.1.3.3 装配

极组热压整形应控制压力、温度和时间，不能发生过压。极组外型尺寸和负极包裹正极情况要 100%检查。极组与电池壳有垫片、包膜等措施进行绝缘隔离，极组上端通过绝缘部件与电池壳绝缘隔离。

极组入壳时避免极组挫伤。焊接过程应防止焊渣飞溅，设置保护罩，防止异物掉入电池中；焊接时的压力、温度区域、熔深等要有效管理。

方型和圆型电池极耳弯折的形状要进行优化，弯折处极耳不能向极组内部折叠，且弯折后极耳不能接触电池壳壁，不能损伤极组。

电池周边焊接保证过程稳定。

圆型电池壳滚槽形变后，避免镀层整片掉落，安装有效除尘和除金属屑的装置。控制滚槽部位壁厚残留量，无壳体破裂。

装配后电池必须对正负极对齐度 100%X-Ray 检查，经过 100%绝缘耐压检测。

软包电池封装参数（压力、温度、封装厚度、有效封装宽度）要经过优化，过程进行有效管理，经过 100%绝缘耐压检测。

#### 3.1.3.4 注液

注液工序是将电解液均匀注入电池内部。注液前确认电液水分含量、HF 含量以及色度合格，极组中的正负极片水分控制在规格要求内。

注液后静置温度和时间要经过优化和控制，避免出现预充电时电解液浸润不充分的情况。要有称重系统 100%检测注液量。注液后的电池必须及时进行封口。

对注液后电池进行小电流预充电处理，减少化成早期的气体产生，同时对极组和壳盖进行电化学防护。预充电倍率、充电电压和温度等工艺条件需要优化和管理。

#### 3.1.3.5 化成和老化

化成设备需按设备维护要求进行定期校验，保证电压及电流控制精度，避免电池过充、过放、容量检测错误以及过程外部短路。选择合适的充放电流程，防止因流程错误导致的过充过放、析锂、厚度过高等问题。

电池单体建议经过老化工序后出厂。选择合适的老化工艺，防止因老化时间过短导致自放电筛选不完全。自放电的筛选标准要进行有效验证。

老化后的电池单体 100%测量电压、内阻、厚度，数据要求全追溯。电池存放和转运过程，应有措施防止电池外短、跌落和挤压等损伤。

### 3.1.4 电池单体安全评价

#### 3.1.4.1 电池单体热失控

热失控是指电池单体内部发生放热连锁反应引起温度急剧变化，从而可能导致电池过热、起火、爆炸等。目前分析引发电池热失控的原因主要有电池受到机械滥用、热辐射，电池内部短路，恶劣环境滥用等。

热失控可以通过实验手段模拟评价；评价方法包括通过加热、针刺等方式激发电池内短路，引发电池热失控。

当电压下降至初始电压的 25%，或温度达到电池厂商规定的最高工作温度，温升速率 $dT/dt \geq 1℃/s$，且持续 3s 以上时，可以认为电池发生了热失控。

热失控发生起火爆炸时，电池单体上的安全保护装置应启动。泄压和喷火的方向应进行设计，喷泻出来的物质量应控制，喷出的气体温度、体积、成分要研究分析，防止次生短路灾害的发生。

#### 3.1.4.2 电池单体安全要求

电池单体应该满足电、机、热的安全测试评价。要按照对应标准规定的测试方法GB/T31485进行锂离子动力电池单体安全评价。

### 3.1.5 单体电池使用安全

锂离子电池具有最佳的使用温度范围，超过使用范围易发生安全问题，较高温度下使用，副反应加剧，易引发热失控安全问题，低温充电负极易发生析锂问题。超过45℃和0℃以下应控制充放电策略，如降低倍率，保证电池在安全窗口内工作。控制充电方式，充电方式一般包括充电温度、充电倍率和充电电压。不同体系和设计的单体电池充电方式不同。针对某一单体电池产品，电池单体制造商应该提供温度-倍率-充电电压关系图，根据电池单体规格书设计系统充电策略。

锂离子电池在高温下长期存储，性能衰减严重，应避免。长期存放的电池，再次使用不建议直接采用快速充电的方式。

锂离子电池充电速度和使用寿命强相关，对于不具备快充特性的动力电池组，在条件允许的情况下，减少快充的使用，尽可能选择小倍率充电。

## 3.2 电池模组安全要求

### 3.2.1 电池模组环境要求

电池模组生产车间环境温度、湿度和粉尘级别应有规范要求，并实时监控。模组汇流排焊接工序粉尘级别应控制在30 万级以下。制造过程中应防止由于设备或工艺原因引入金属颗粒异物。

### 3.2.2 电池模组设计

#### 3.2.2.1 材料安全

电池模组部件应避免尖角设计，边缘和表面应控制毛刺和金属浮粉，应做表面防腐处理。

材料需要符合 ROHS，对于客户有特殊要求的应识别如硫含量等。材料应考虑防火、阻燃要求。

电气连接部件需要考虑防腐蚀处理，防止长时间使用接触电阻增大而导致发热。与单

体电池接触部件选用耐电解液腐蚀的材料，应考虑电解液泄漏后引发的绝缘失效等问题。

所有部件材料应考虑整车或系统的可靠耐久性要求，或易于更换，达到整车或系统的寿命一致。

绝缘部件的材料选择，应考虑高温环境对绝缘性的影响，确保在整车或系统工作最高温度时的绝缘性。

对于栓接结构设计应满足整车环境要求。

#### 3.2.2.2 机械安全

机械安全防护，设计时应考虑挤压、跌落、振动、冲击、翻转、碰撞等工况下防护结构对产品的防护，使产品能满足功能要求、各类安全法规要求等。

机械可靠性设计要满足整车设计寿命。应充分考虑运输、搬运和安装的耐久和可靠性。

电池单体在使用过程中厚度会发生膨胀，模组设计应根据电池单体性能，合理预留膨胀的空间，合理设计汇流排结构。评估在长时间充放电循环或高温存储后，电池单体膨胀对模组框架的作用力。模组框架强度、紧固力、变形量满足电池单体的膨胀需求同时满足系统的需求。

模组应考虑安全电压防护设计，以便在制造、运输或维修操作时起到保护，防止人员触电及外部短路。

要考虑防呆设计。防止在生产、安装、测试等过程中，出现因人员误操作而导致的电池模组短路起火，人员电击的事故。通常从机械防呆、颜色防呆、标识防呆等方面考虑。

#### 3.2.2.3 电气安全

选用绝缘介质强度较高的绝缘片保证模组的绝缘满足设计目标。耐压至少满足 GBT 18384—2015 要求，考虑异常情况下电气间隙、爬电距离在安全范围。电池模组的绝缘电阻在不同温湿度存储后应具有良好的可靠性。

设计应充分考虑组装、维修时带来的短路风险。

选择合适的材料、尺寸及表面处理技术，以便保证过流能力及焊接的可靠性。连接器推荐满足 USCAR-2 和 USCAR-37 要求。

电压采样线在近电池端应设计过流防护。

模组金属结构框架设计成等电位体，避免形成电势差对人体形成伤害。

模组输出端在装配完成后，应满足 IPXXB 的要求。

采样线束的装配应有防呆设计，避免错误安装导致短路等事故发生。

采样线采用耐高温的结构设计，避免造成电池组内部的二次短路事故。

汇流排应设计缓冲结构，降低振动等对焊点的拉扯。

#### 3.2.2.4 热安全

模组结构设计应保证电芯单体具有足够的散热面积，保证模组与热管理系统间热量传递满足相应散热、加热需求。电池单体散热界面高度差配合导热材料厚度维持在一个合理的公差范围内，保证和热管理系统可靠的接触。在寿命周期内，能满足导热和散热的设计要求,保证电池工作在理想温度范围。

导热材料的导热系数、厚度等参数能够满足模组散热需求；保证电池单体与热管理系统具有良好的热传递路径；导热材料电气绝缘性、防火等级满足电池系统的安全要求。

温度传感器设置位置及数量应能反应不同工况下最高温度和最低温度要求，同时应考虑温度传感器的精度、适用范围及响应时间。

热扩散防护设计。模组设计应考虑隔热防火措施，延缓电池模块中一只电池单体发生热失控时，引燃周围电池单体的时间。

电池系统内分区域对电池模组进行隔离，以减少热失控传递的速度，为乘员争取更长的逃生时间。

#### 3.2.2.5 功能安全

电压采样准确性。电压采集至少包含每串电池电压，电压采集线束压降及采样芯片精度满足电压采样的精度要求；电压采样及转换传输的时间要远小于系统最小容错时间；能够检测电压采样线束短路、断线、范围超限等故障。

温度采样准确性。为了能够及时了解电池模组的温度状态，温度采集每个模组至少应包含 2 个温度采集点，温度采集回路采集精度满足系统温度采集精度要求；温度采样及转换传输的时间要远小于系统容错时间；能够准确识别温度采样的超范围、短路、断路等异常故障。

均衡控制准确性。均衡电流设计满足电池系统均衡需求，均衡控制指令能够及时准确执行，并能够准确识别均衡控制回路的硬件及软件故障，如均衡控制失效等异常故障等。

通信传输准确性。模组的电压及温度能够及时准确传递给上级主控板，通信回路设计具备回路短路、断线、异常恢复等通信冗余机制。

电磁兼容。模组采集线束应尽量与高压动力线束垂直，避免高压动力传导/辐射串扰；模组从控板应能够确保负载电磁环境下的抗扰特性，在施加抗扰过程中确保电压采集、温度采集、均衡、通信等功能的正常运行；同时，应确保从控板在其工作过程中对外部其他部件的传导及辐射干扰。

对于金属外壳的模组通常应设计良好的接地点，避免尖锐带电体的尖端放电等。

### 3.2.3 电池模组制造

#### 3.2.3.1 电池单体绝缘

针对壳带电的电池单体使用绝缘材料通过包覆或喷涂等工艺实现有效的绝缘防护。绝缘前电池单体进行有效清洁，避免导电粉尘颗粒引入导致装配电池单体间短路风险产生。绝缘过程必须确保按设计需求部位绝缘层的有效包覆，同时确保绝缘层不被划伤，划破。

#### 3.2.3.2 模组组装

模组组装是将电池单体按照不同的串并联方式，与框架或固定支架等配合安装。

如胶水需要高温加速固化时，应优化控制加热温度，避免组件在高温下受损。

LMU（本地监视单元 Local Monitoring Unit，作为从板同单体电池直接连接）、BMS（电池管理系统 Battery management system）或 FPC（软性印刷线路板 Flexible Printed Circuit）安装过程中，从人员防护、工作环境、工具使用方式，均需考虑静电防护。

在模组装配挤压过程中，不能超过电芯所能承受的压力，挤压设备需要具备压力监控功能或设备设计选型保证压力不超过电芯承受能力，避免电芯过度挤压，造成的变形、漏液等安全问题出现。

对于软包电池单体，模组组装过程保证电芯极耳平面度要求，满足焊接条件，保证铝排连接的可靠性。

#### 3.2.3.3 框架焊接

框架焊接要保证焊接后模组的框架结构强度。

焊接时熔区及热影响区不出现超出允收规格的焊接缺陷。管控焊渣飞溅，防止规格外异物进入模组内，导致模组整体绝缘失效。

激光焊接要保证框架焊接强度和熔深要求。

#### 3.2.3.4 汇流排连接

汇流排通过栓接、电阻焊、激光焊等方式将电芯进行串并联。

采用激光焊接工艺，要注意对电芯极柱表面及汇流排去除氧化层和表面脏污。焊接时选用匹配的焊接参数，防止出现虚焊、焊漏等焊接不良。优化设计焊接工装，管控焊渣飞溅，防止规格外异物进入未焊接完成的模组内，导致模组整体绝缘失效。

采用电阻焊接工艺，应对焊头的修磨频次、寿命进行管控，保证焊接工艺稳定性和焊接强度。

采用栓接工艺，应保证扭矩满足结构强度要求及耐久性防止长期使用过程中栓接松

动，接触不良，出现安全问题。

同时模组中 CSC、BMS 或 FPC 等零部件做好隔离防护，避免焊接对电子零部件的损伤。

#### 3.2.3.5 采样线连接

通过栓接、超声焊、激光焊等工艺将电压和温度采样线与汇流排进行有效连接。

栓接过程须对扭矩进行控制。

超声焊和激光焊接要确认在匹配的焊接参数下进行焊接，防止出现虚焊、焊漏等焊接不良。激光焊接要对焊接所产生的颗粒粉尘进行收集处理。

模组采样线线序需要进行检测，避免安装错误，导致采样线短路、采集板或保险损坏、烧毁。

### 3.2.4 电池模组安全评价

#### 3.2.4.1 电池模组安全要求

##### 3.2.4.1.1 电安全评价

模组的电安全测试主要包括过充、过放、外部短路测试。电安全测试主要模拟在电池管理系统或充电桩失效的情况下，电池发生过充、过放、外部短路等异常，高压控制器件无法有效切断充放电回路时，电池应不出现起火、爆炸等安全事故。

过充测试，要求模组在满电状态下继续 1C 充电至电压达到规定终止电压的 1.5 倍或充电时间达到 1 小时停止充电，观察 1h。电池模组应不爆炸、不起火。

过放测试，要求模组在满电状态下以 1C 放电 90min，观察 1h。电池模组应不爆炸、不起火、不漏液。

外部短路测试，要求电池模组在满电状态下，以小于 5mΩ 的电阻短路电池模组正负极 10min，观察 1h。这种情况下应不爆炸、不起火。

##### 3.2.4.1.2 机械安全评价

电池模组的机械安全测试主要包含挤压、针刺、跌落等。机械安全测试主要模拟电池在滥用或发生交通事故时，电池遭受外部的异常撞击，如两车碰撞、车辆底部受硬物撞击等，电池发生一定的变形、刺穿、高处跌落等，电池应不出现爆炸、起火等安全事故。

挤压测试，电池模组满电状态下，以半径 75mm，长度不超 1m 的半圆柱体挤压电池在整车布局中最容易受挤压方向，挤压速度（5±1）m/s,模组挤压形变量达到 30%或挤压力达到 200kN，保持 10min，观察 1h。电池应不爆炸、不起火。

针刺测试，电池模组满电状态下，用φ 6-φ 10mm 的耐高温钢针，以（25±5）mm/s 的速度垂直电池极组方向，依次贯穿至少 3 个单体，钢针停留在电池中，观察 1h，记录安

全等级。

跌落测试，电池模组满电状态下，电池正负极端子朝下，从 1.2m 高度自由跌落到水泥地面上，观察 1h。电池应不爆炸、不起火、不漏液。

底部撞击工况测试，模拟整车底部受到飞石、金属块等异物撞击，模组、电芯底部受到挤压形变的场景。测试模组充电至 100%SOC，按图一要求固定安装测试对象，使用前端为半径 10mm 半圆球的圆柱体，撞击方向为半球体的球心与测试对象撞击面中心重合，撞击参数见表一。记录测试过程中电压、温度、挤压力、挤压速度、挤压最大形变量，观察 1h。这种情况下应不爆炸、不起火。

表 3-1：底部撞击工况测试参数

| 序号 | 撞击能量/J | 撞击头重量/kg |
|---|---|---|
| 1 | 50 | 5 |
| 2 | 100 | |
| 3 | 150 | |
| 4 | 200 | |
| 5 | 300 | |

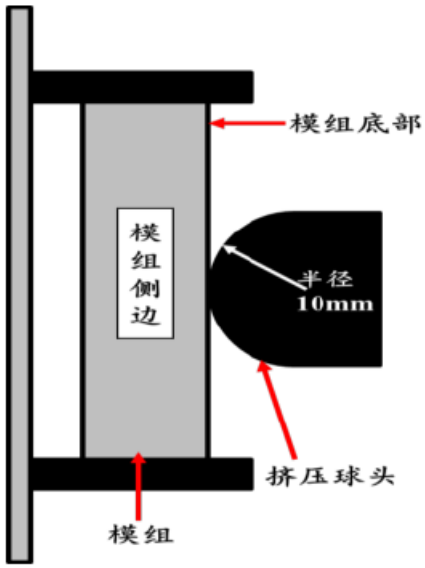



图 1 模组固定安装方式

备注：1.撞击能量根据动能定理 $E=1/2mv^2$ 计算。2.撞击头重量指前端为半径 10mm 半

圆球的圆柱体的重量。

#### 3.2.4.1.3 环境安全评价

电池模组的环境安全测试主要包括加热、温度循环、低气压、海水浸泡测试。环境安全测试主要模拟电池在恶劣环境中的应用，如异常高温情况、高低温反复变化情况、高海拔地区应用、雨季或异常情况车辆泡水等，不能出现安全问题。

加热测试，电池模组放入温箱中，以 5℃/min 的速率由室温升至 130±2℃并保持 30min 后停止加热，观察 1h。电池应不爆炸、不起火。

温度循环测试，电池模组满电状态下，将模组放入温箱中，从-40℃~85℃进行温度循环，每个循环 8h，进行 5 次循环。电池应不爆炸、不起火、不漏液。

低气压测试，电池模组满电状态下，放入气压箱，设置气压 11.6kpa（相当于海拔 15420m），静置 6h，观察 1h。电池应不爆炸、不起火、不漏液。

### 3.2.4.2 电池模组可靠性要求

#### 3.2.4.2.1 热扩散评价

热扩散测试是评估电池模组热扩散防护设计能力。通过加热、针刺、过充等方式模拟一只电池发生热失控后，模组设计能有效延缓热扩散，保证电池系统在 5min 内不发生起火、爆炸，给车上乘员足够的逃生时间。

#### 3.2.4.2.2 机械振动测试

振动测试模拟车辆长时间在复杂路况行驶（如搓板路、颠簸路、起伏路等）。电池长时间振动颠簸后电芯内部不能出现短路，模组结构不能散开脱落发生短路等安全问题。实验要对电池模组进行 X、Y、Z 三个方向的振动测试，每个方向 21h。要求测试后，电池连接可靠、结构完好，最小监控单元电压无锐变，电压差的绝对值不大于 0.15V，无泄漏、外壳破裂、爆炸或着火等现象，绝缘电阻不小于 100Ω /V。

电池模块中的零部件（包括支撑柱、紧固件等）无明显位移、扭转和弯曲；零部件的谐振频率与初始值的偏差应小于 10%，各个紧固螺丝的剩余紧固力不低于初始值的 60%；各个电连接点的电阻与初始值的偏差应小于 5%。

#### 3.2.4.2.3 机械冲击测试

机械冲击模拟车辆在急加速、急刹车情况下，电池能承受加速度的冲击而不出现安全问题。试验对电池模组施加 25g、15ms 的半正弦波形 Z 方向冲击 3 次，试验后观察 2h。要求电池无泄漏、外壳无破裂、无爆炸、无着火等现象,绝缘电阻不小于 100Ω /V。

#### 3.2.4.2.4 高温存储测试

高温存储测试主要评估的是电池的日历寿命。模拟电池在高温环境下（如 45℃或55℃）长时间存储，评估其恢复容量与初始容量的比例。

## 3.3 电池单体和模组包装运输安全要求

### 3.3.1 包装安全要求

电池单体和模组的包装应满足防水、防潮，必要时应该在包装袋中加干燥剂除湿。包装要考虑运输环境条件（公路运输、铁路运输、水路运输等情况）下对产品的保护，防止搬移过程中的挤压和损伤。

电池单体和模组应以最小单元隔离固定，预留安全距离，避免发生电气安全问题。

### 3.3.2 运输安全要求

电池单体和模组必须牢靠固定在货物运输装置的内部。

运输过程中的电池单体和模组所处环境温度需要监控，较高温度可能引起电池安全问题。

避免对电池单体和模组日晒、雨淋、受潮。

避免电池单体和模组受压，严格按照产品规格书要求摆放。

较低的电池单体和模组荷电状态对运输安全有利，建议控制 30-70%SOC。

锂离子电池单体和模组属于危险品，运输过程中应避开易燃、易爆、易腐蚀危险品，考虑配备消防设施。

# 4.电池系统

## 4.1 电池系统要求

### 4.1.1 BMS 设计开发与故障处理

#### 4.1.1.1 BMS 设计开发

BMS 基本功能的设计与开发建议关注以下内容：

（1）能有效对电池系统的单体电压、电流、温度、绝缘阻值等参数进行测量，测量精度及频率应在常规工况及恶劣极端工况下均满足国家标准要求，同时采样电路具有保护机制，避免高压短路故障。

（2）能准确计算电池系统 SOC、SOE、SOH，并结合当前电池电压、温度等状态计算安全的可用充放电功率区间，确保不会对电池造成单次或累积的安全影响。

（3）建议整车能较准确估算车辆剩余里程，防止电池系统在使用过程中因剩余里程错误导致动力系统异常中断。

（4）充电过程中，BMS 应同时监测电池系统及充电机状态，当电池系统或充电机发生故障时，应及时停止充电过程并进行报警。

（5）能够根据测量信息及电池使用条件，通过热管理系统对电池系统内部温度进行有效的调控，使电池充放电过程执行在合适的温度区间，避免因单次或累积的高低温操作引发的电池安全隐患。

（6）BMS 功能应通过必要的测试验证，包括：绝缘性能测试、电气适应性能测试、环境适应性能测试、电磁兼容性能测试，确保其在不同工况、环境下均能有效工作。

BMS 系统基本功能的设计与验证可参考 GB/T《电动汽车用电池管理系统技术条件》。

#### 4.1.1.2 故障处理基本要求

（1）能有效及时判断电池单体或系统的故障，包括但不限于电池过压、欠压、过温、过流、绝缘降低等，并能以可靠的通讯方式通知整车，并采取相应的措施。

- 根据电池类型标定不同的故障阈值
- 根据电池的使用环境、不同的生命周期调整合适的故障阈值和检测时间，确保系统安全。

（2）BMS 对电池故障的检测周期或消抖时间应满足安全需求，即在整个故障的检测、通讯、处理周期完成前电池系统不会发生对整车或乘员的危害。

（3）当发生故障的条件下，如非绝对必要，电池系统应先通知驾驶员采取必要措施

后，如通知驾驶员减速靠边等，再进行断电保护处理。

（4）发生故障后，应在确认故障消失或足够的安全余量后，才能允许对电池系统继续操作。对于电池系统的永久性故障，如电池单体严重过放至 1V 以下等，建议对故障进行锁存记录并防止对电池系统继续操作，避免后续的安全问题。

（5）BMS 建议具备故障存储功能，能够记录电池系统发生过的一段时间内的所有故障代码，并可在维护时通过外部操作清除；能够根据厂家需要记录第一次或最后一次发生故障时的详细数据，包括电池的单体电压、温度、电流等信息。

#### 4.1.1.3 典型故障信号处理策略

（1）阈值的设定通常由电芯企业及整车企业根据电芯特性及整车控制要求确定，不同电池系统的阈值不同。典型故障可参考《电动汽车用电池管理系统技术条件》，以下为参考处理策略：

• 电池温度大于设定阈值：建议采用降低充放电功率等保护措施；若保护措施无效，建议执行下电保护流程或中止充电。

• 电池温度小于设定阈值：建议启动加热功能，限制输入、输出功率。若需要进行充电流程，建议当电池温度加热至最低允许充电温度后再进行充电。

• 单体电压或总电压大于设定阈值：建议停止充电或禁止回馈；若电压持续升高或大于绝对安全阈值，建议执行下电保护流程。

• 单体电压或总电压低于设定阈值：根据放电深度程度不同可采取不同措施，如提示用户充电、禁止放电或执行下电保护流程等。

• 电芯一致性偏差大于设定条件：根据整车厂及电芯厂制定的判定条件可采取不同措施，如启动均衡、提示用户进店维护或执行下电保护流程等。

• 充电电流（功率）大于最大允许阈值：如在行驶过程中，建议降低或停止回馈；充电过程中建议进行降电流操作。若以上措施无效，建议执行下电保护流程。

• 放电电流（功率）大于最大允许阈值：建议降低运行功率；若无效，建议执行下电保护流程。

• 绝缘电阻小于设定阈值：建议根据绝缘故障程度采取通知整车或执行下电流程等。

• 电池系统内部温差大于设定阈值：建议采用降低充放电功率等保护措施；若保护措施无效，建议执行下电保护流程或中止充电。

• 高压回路异常：建议执行下电保护流程。

• BMS 采样、处理器及执行器相关故障（例如：电压采样故障、温度采样故障、电流

采样故障、MCU 故障、供电故障、存储故障、执行器故障、碰撞事件，等）检测、判定及处理方式，建议结合功能安全需求进行综合设计，以满足相关安全需求。

（2）应根据故障特点，细化故障处理策略，对故障进行分级管理，不同级别的故障采用不同的对应策略，例如：告警、限功率、下高压、提醒用户远离车辆,等，尽量避免行驶过程中的直接高压下电。

（3）故障阈值设置、判断时间、恢复时间应充分考虑电池系统的能力及车辆运行需求，避免漏报和误报。

### 4.1.2 充电、运行工况下许用电流、功率控制

#### 4.1.2.1 许用电流/功率限制

（1）充电、运行工况下，许用电流/功率控制限制表应充分结合电池系统的能力（结合电芯厂提供的许用电流/功率限制表）及车辆使用需求综合设定，考虑充电及运行工况（制动回馈、放电）对电流持续时间的需求，通常设定峰值电流/功率表（例如：2s，5s，10s，30s）、持续电流/功率表（例如：60s，3min，持续等）。

（2）因温度、SOC 变化而导致的峰值电流/功率及持续电流/功率切换时，BMS 应确保许用电流/功率平滑过渡。

（3）BMS 应充分考虑电池系统的许用能力，结合电池系统寿命终止时的可用电量、许用功率衰减，综合确定全寿命周期内的许用电流/功率限制值。

（4）功率限制值应考虑系统元器件最大承受能力，应根据系统各元器件可承受最大载流量值的最小值确定。

（5）BMS 实时监控电流及电压，如果实时充放电电流/功率超过许用电流/功率，BMS 记录 DTC，通知整车。

（6）当充放电电流/功率超过许用电流/功率，BMS 应执行多级控制策略，分阶段主动降低功率，避免电池系统起火、爆炸。

#### 4.1.2.2 充电功率控制策略

（1）直流充电

直流充电应遵循《GB/T 27930 电动汽车非车载传导式充电机与电池管理系统之间的通信协议》、《GB/T 18487.1-2011 电动汽车传导充电系统 第 1 部分：通用要求》、《GB/T20234.1-2015 电动汽车传导充电用连接装置 通用要求》等标准要求。

充电过程中，BMS 监控各种参数的变化，包括异常参数（如：过压、过温、过流等），当达到充满电的要求、或者故障发生时，向充电机发送充电中止指令，主动停止充电过程。

（2）交流充电

通常，BMS 向 OBC 发送电流需求及电压需求，通过 OBC 控制充电过程。充电过程中，BMS 监控各种参数的变化，包括异常参数（如：过压、过温、过流等），当达到充满电的要求、或者故障发生时，向 OBC 发送充电中止指令，主动停止充电过程。

#### 4.1.2.3 大功率充电策略

（1）电池供应商应充分执行大功率充电测试，提供规定时间内（例如：10min、15min、20min、30min）允许的最大电流值，该数值需要考虑温度、SOC 及 SOH 的影响。

（2）温度测量应尽量覆盖充电回路中可能的高温点，包括：电池模组的最高/最低温度点、车辆与充电桩的连接器、充电线缆、分流器形式电流传感器；同时应关注模组间连接铜排、电池包充电连接器的温度。

（3）BMS 应监控充电功率、温控点温度，当充电功率、测量点温度超出限制阈值，应及时向充电机通报故障。

（4）当发生故障需要停止大功率充电时，BMS 首先申请充电桩降低输出功率，由充电桩控制结束充电过程。如充电桩故障致使无法停止充电，BMS 应紧急断开充电继电器，停止大功率充电。

（5）针对大功率充电可能持续产生的大量热量，应优化热管理策略，适当降低启动制冷功能的温度阈值。充电结束后，如果电池包温度仍然偏高，需要继续维持制冷功能，使电池系统温度回到合理范围。

（6）应监控大功率充电的使用频率，避免频繁执行大功率充电可能导致的电池性能下降或安全隐患。

### 4.1.3 BMS 功能安全

BMS 功能安全的主要目的是避免 BMS 系统电子/电气功能异常引发的危害而导致严重人身伤害事件（起火、爆炸、排气、电击）的风险。

BMS 功能安全活动重点关注以下方面：确定功能安全目标与安全需求、功能安全产品开发、功能安全目标验证与确认。

#### 4.1.3.1 确定功能安全目标与安全需求

应在整车级别执行电池系统的危害分析与风险评估，明确功能安全目标、ASIL 等级、安全状态及 FTTI，定义功能安全需求及控制策略。

建议 BMS 包含以下功能安全目标，以避免电池系统的热失控风险：

- 防止电池单体过充导致热失控

• 防止电池单体过放后再充电导致热失控

• 防止电池单体过温导致热失控

• 防止动力蓄电池系统过流导致热失控

建议 BMS 包括以下功能安全目标，以避免电池系统的电击风险：

• 确保车辆碰撞发生时切断高压回路

• 绝缘失效禁止吸合高压接触器

• 高压互锁失效禁止吸合高压接触器

建议 BMS 包含以下功能安全目标，以避免系统动力异常中断：

• 避免非预期切断高压接触器

电池系统危害分析与风险评估及功能安全需求定义建议参考《GB/T 电动汽车用电池管理系统功能安全要求及试验方法》（预计 2019 年发布）

#### 4.1.3.2 功能安全产品开发

BMS 功能安全设计与开发应遵循严格的流程规范，应关注以下活动：

（1）使用 DIA 规范整车厂和供应商间的职责划分。

（2）执行汽车安全生命周期中的各级设计活动。针对不同设计阶段，实施相应的验证活动（评审/测试），使用适当的测试方法（例如：缺陷注入方法）验证安全机制的有效性，确保测试用例的完备性和测试覆盖度。

（3）在系统设计、软件设计、硬件设计阶段执行功能安全分析（FMEA、FTA、DFA、FMEDA），满足 ASIL 等级相关要求。

• 执行系统安全分析，识别违反功能安全目标的失效模式，通过系统设计确保故障发生时，整车能在 FTTI 时间内进入安全状态

• 执行软件安全分析，针对软件失效模式，确定软件安全机制

• 执行硬件安全分析，基于硬件器件的失效率、失效模式、失效分布，对硬件架构进行评估（SPFM、LFM、PMHF），完善硬件安全机制，确保满足安全等级要求

• 安全分析应持续、迭代执行，针对安全分析中发现的问题，需不断优化更新安全机制。

（4）软件设计建议采用标准化软件架构（例如：AUTOSAR），软件开发应遵循符合功能安全要求的建模规范和代码规范，使用多种模型/代码测试方法（例如：MIL、SIL、PIL、HIL）进行软件集成和测试，确保满足软件覆盖度要求。

（5）关注需求、设计、验证之间的双向追溯和一致性，确保需求变更、缺陷修正的

可跟踪性。

（6）执行软件/硬件组件鉴定和再用证明相关活动，确保软件/硬件组件使用的合适性。实施工具链置信度评估，确保工具置信度水平（TCL）满足要求。

（7）执行与安全目前等级相适应的认可措施，包括：认可评审、安全审核和安全评估。

功能安全产品开发活动建议参考《GB/T34590-2017 道路车辆功能安全》。

#### 4.1.3.3 功能安全目标验证与确认

应在系统级、整车级对 BMS 功能安全需求及功能安全目标执行验证与确认，确保达成整车功能安全目标。

如果除 BMS 功能安全保护机制外，整车还设计了其它安全机制（如：机械、化学等），功能安全目标的验证与确认也应覆盖这些安全机制。

电池系统的功能安全目标验证与确认活动建议参考《GB/T 电动汽车用电池管理系统功能安全要求及试验方法》（预计 2019 年发布）。

### 4.1.4 热失控、预警识别策略

#### 4.1.4.1 电池包热失控基本防护

电池包应具有热失控防护措施，保证热失控发生后，可以在一定时间内确保电池包不发生导致人生伤害的事件发生（起火、爆炸等）。

#### 4.1.4.2 热失控提前探测预防

BMS 可考虑监控导致热失控的事件（如电压、电流、温度超过安全使用范围、内短路等），在热失控发生前采取紧急应对措施（如报警、限制功率、切断高压回路等），同时提醒乘员采取避险措施。

#### 4.1.4.3 热失控探测及告警

（1）电池发生热失控及热扩散时，电池系统内部温度、气体成份、压力等参数会发生变化，应对热失控及热扩散进行试验研究，通过理论分析和实验验证，确定适合的热失控和热扩散探测手段（例如：温度、气体、压力等），并确保探测器的检测精度满足需求。

（2）当 BMS 确认发生电池热失控时，应把热失控信号传递给整车，整车应通过指示装置（仪表或其他装置）提供一个明显的热失控报警信号以及警示声，提醒驾驶员和乘客疏散；同时，BMS 请求下高压，整车根据当时工况进入紧急下电流程。

（3）建议 BMS 应准确监测电池系统及其部件的异常温度升高，对电池系统的热失控要尽可能早地发出预警信号。

（4）热失控探测及报警功能应在运行模式下执行，其有效性应通过整车级测试，避免漏报、误报。

（5）热失控探测及预警功能应满足整车功能安全要求。

## 4.2 电池系统安全

基于市场上出现的电动汽车泡水、碰撞、底盘划伤后的起火事件，电池系统安全从系统设计（机械安全、热安全、电气安全）、安全测试、生产三阶段展开，保证电池系统的安全。

### 4.2.1 机械安全

电池系统应具备足够的机械强度，保证在整车正常使用的生命周期内不会因振动、机械冲击等工况引发安全风险。

#### 4.2.1.1 基于正碰、侧碰、侧柱碰、底碰、石击的电池及整车安全设计

针对于整车碰撞衍生出电池系统碰撞、挤压工况，需要结合整车设计及电池系统安装位置有针对性的进行结构设计保证电池系统的机械安全。

电池系统的结构强度应至少满足《GB/T 31467.3-2015 电动汽车用锂离子动力蓄电池包和系统第 3 部分：安全性要求与测试方法》中电池系统模拟碰撞的标准要求或整车企业的标准要求。

##### 4.2.1.1.1 电池系统碰撞安全设计

（1）应分析碰撞过程中电池箱体及其内部结构（电池模组、高低压线束）产生的最大变形情况，并结合电池模组允许的最大变形量来判断碰撞过程中的安全风险；

（2）应具有吸能效果的结构设计，设计时应考虑相应材料的塑性要求；

（3）应具有合理的内部加强筋设计，提高整体结构强度；

（4）考虑电连接件的可靠性，避免碰撞过程中发生短路风险；

（5）提高热管理系统结构强度，增加防护设计，避免碰撞过程中冷却液泄露风险。

##### 4.2.1.1.2 电池系统挤压安全设计

（1）电池系统设计满足相应的刚度、强度要求：如外围采用防撞梁结构；

（2）合理的电池系统内部安全距离设计；

（3）合理的热管理系统布置：建议液冷系统水管布置避开易碰撞侧；

（4）合理的电气系统布置：电池系统内的高低压线束的走线路径应尽量与电池系统的非变形区域结构相连接，同时应加强绝缘防护及线束固定。

#### 4.2.1.1.3 电池系统防石击安全设计

（1）合理的底部装甲或防护板设计；

（2）箱体接插件端防护较薄弱，且易受沙石冲击，建议增加防护板遮挡。

### 4.2.1.2 振动可靠性安全设计

振动是对结构件耐久性的考验，区别于传统车，电池系统激励源产生主要是由于汽车在行驶过程中，路面的不平整造成的，路面的激励频率大部分都是集中在低频端，电池系统在设计过程中主要宗旨是提高电池系统的整体固有频率。

电池系统的结构强度应至少满足《GB/T 31467.3-2015 电动汽车用锂离子动力蓄电池包和系统 第 3 部分：安全性要求与测试方法》中电池系统振动可靠性的标准要求或整车企业的标准要求。

（1）提高电池系统整体固有频率：

• 提高电池系统刚度：如增加车体安装点，优化固定梁结构设计；

• 减少电池系统的重量：轻量化的结构设计及材料选择；

（2）疲劳强度高的材料选择；

（3）提高电池系统强度：避免质量过度集中，在质量集中位置增强结构设计；固定梁焊接要求、结构紧固件的选型及固定扭矩设计均应符合设计规范要求。

### 4.2.1.3 全生命周期高防护等级安全设计

安装在车身外部的电池系统应具备 IP67 或以上的防护等级，并应定期维护检测以避免整个生命周期内防护等级在使用过程造成降低。

#### 4.2.1.3.1 电池系统接触防护

（1）集成式 BDU，并具备外壳防护设计；

（2）模组级别正负极位置防护设计；

（3）高压连接器防护:

•连接器插座与插头中接触件都需与保护外壳做相互绝缘处理，保证外壳绝缘不带电，保证操作人员的安全。

• 在电池系统高压连接器防护设计时，最常选择使用的是 IPXXB/IPXXD 的防护等级。

#### 4.2.1.3.2 电池系统防水防尘

（1）电池系统箱体防护要求：

• 电池箱体防护在全生命周期等级达到 IP67 等级；

• 电池箱体密封垫设计时，考虑其吸水率、压缩率、及阻燃特性；

（2）防水透气阀:与箱体配合处防护在全生命周期等级达到 IP67 等级；

（3）电气接口防护要求:

连接器插座与插头连接端处于箱体外部，此端须保证插座与插头接触良好、过流、过压持续、稳定、拆卸方便，同时有插座端口保护盖设计。有以下内容需保证：

• 连接器插座与箱体配合处的防护等级须达到 IP67 等级；

• 连接器插座与插头连接后的防护等级须达到 IP67 等级；

• 连接器插座端口在未插合存放仓库时，保护盖须防尘防潮且能满足经过长途运输震动后保护盖不会掉落。

#### 4.2.1.3.3 电池系统防爆防护

电池系统应具备有效的泄压装置，可以快速平衡内外部气压变化，防止因内部气压过高造成壳体变形引起的防护等级降低或失效。

泄压装置安装的位置和方向应避免对乘员舱或车辆周边人员造成人身伤害，且应避免引燃整车。

#### 4.2.1.3.4 电池系统防腐防护

在全生命周期内防腐的要求，要根据电池系统使用寿命要求和使用区域环境要求来确定电池系统的防腐等级。

### 4.2.2 热安全

通过热管理系统对电池系统进行加热、散热、均衡、保温；电池系统内部要有防止热扩散的结构设计；关键部件的阻燃设计；来确保电池系统的热安全。

#### 4.2.2.1 可靠热管理系统设计

根据锂离子电池结构及工作原理可知，无论在高温或是低温，都有引发电池热失控的风险，而电池热管理系统的设计目标就是结合 BMS 控制策略和调整功能，控制电芯工作在舒适温度范围内、并降低电芯之间的温差实现性能均衡，从而保证系统热安全并延长系统寿命。要实现以上目标，需从冷却、加热、保温三个方面进行设计，同时还需保证整个系统的气密安全，不允许发生冷却液泄露。需关注低温冷却管路可能引发的冷凝水，避免因此而导致的绝缘、短路安全隐患。

（1）冷却

a.根据指定的严苛工况下的系统发热量确定电池包散热形式及控制边界，保证电池最高温度不超过允许使用温度，且大多数时间能在舒适温度范围工作。

b.建议正常工况下电池系统内部采集的温度点之间~~的~~最大温差不超过 5℃，极限工况

下最大温差不超过 10℃，且能满足极限工况的连续运行（例如持续高速工况加快充）。

c.为适应不同工况，散热系统可按有无 chiller 以及风扇挡位分为多种回路：

•风冷散热系统中，能够对风扇状态进行检测并判定是否工作正常；当风扇或冷却系统其它部件出现故障时能及时报警并采取保护措施（如限制充放电功率等）；

•液冷系统中，能够对压缩机、水泵等部件进行检测并判定是否工作正常；当冷却系统出现故障时能及时报警并采取保护措施（如限制充放电功率等）。

（2）加热

a.在指定环境温度下，实现在规定时间内将电池系统加热到规定温度，使系统能够快速达到允许充放电的工作温度。

b.电池系统最低温度低于最小允许充电温度时，建议对电池加热之后再进行充电。

c.加热过程中尽量降低电池系统内部采集的温度点之间最大温差。

d.以电池包内置加热部件（如 PTC 等）进行加热的设计中，应具备相应的安全设计（如引入二次热熔保护机制），当加热部件温度过高时，能够切断加热部件电源，防止加热元件出现干烧进而引燃电池。

（3）保温

a.将电池系统由常温环境分别转入高温和低温环境静置，在规定时间内系统中的电池最高/最低温度不超过目标值。

b.高温环境保温时，建议减小电池系统内部采集的温度点之间温差。

（4）气密安全

a.对于液冷系统，应采用相应的措施防止管路、接头等部位发生泄漏，并在生产过程中采取相应的检测工艺以确保产品安全。

b.当液冷系统发生泄漏至可能产生安全隐患的阈值的时，建议具有检测手段能及时检测并报警。

#### 4.2.2.2 电池系统热扩散防护设计

引起热失控风险的因素有很多，如极端的环境温度、过充过放、内短外短、电池制造缺陷等等。既然无法完全避免热失控风险，那就需要采取相关的防护设计来降低热失控发生时的危害。热量传递是热失控扩散蔓延的重要原因，因此传热特性会直接影响热失控扩散速率。此外，电池间的电连接也会影响热失控扩散。现行的热扩散测试标准和法规可参见《电动汽车用锂离子动力蓄电池安全要求》，测试对象为模组和电池包，要求单个电池发生热失控时，引起热扩散、进而导致乘员舱发生危险之前 5 分钟，应提供一个热事件

报警信号，同时建议系统应具备避免热失控事件传播到相邻电池的能力。可见，热扩散防护必须从电芯、模组、系统三个方面进行考虑。

（1）电芯级

a.相邻电芯间建议具备一定的隔热设计（如增加绝热毡、气凝胶等隔热阻燃材料），延缓热蔓延。

b.电芯防爆设计（如防爆阀等）指向建议避免直接朝向相邻电芯，防止产生链式反应。电芯的开阀保护时间，需要在单电芯、模组中保持一致性，开阀的条件应在一定的偏差范围内。

（2）模组级

a.模组间建议考虑合适的间距，具备一定的防止热蔓延的能力；建议采用隔热设计（如隔热罩等），抑制热量在相邻模组间的蔓延。

b.设计合理的电连接孔、泄气孔及火焰导向孔，防止蔓延。

c.对于不具备单体熔断功能的电芯，模组建议采用可熔断连接设计，防止电芯内短路时其他并联电池产生电流倒灌，引发热失控。

（3）系统级

a.电池壳体（包括上盖、底板以及密封条等附件）应采用阻燃材料，以避免明火引燃整车；

b.电池包内部高压线束（包括主回路高压线束、电池电压采集线束等）建议具有熔断保护，防止在热失控期间因线束受损短路引起的二次伤害。

#### 4.2.2.3 电池关键部件阻燃设计

为延缓热失控扩散，延长乘员逃生时间，电池系统的零部件应尽量选用阻燃等级较高或者不燃烧的材料，这样即使在热失控的极端环境下，这些零部件至少不会进一步加剧反应。

（1）电池系统内部有机材料（如结构胶、导热胶等）应采用阻燃等级较高的材料。

（2）应重点评估电池包内薄片非金属材料的阻燃等级。

（3）其他与电芯直接接触材料，以及电气件、热管理部件等应选用阻燃等级较高或者不燃烧的材料。

（4） 在电芯热失控以后，建议评估喷发物对模组周围带来的绝缘下降引起的短路造成的二次加热。

### 4.2.3 电气安全

#### 4.2.3.1 绝缘要求

##### 4.2.3.1.1 电气绝缘

（1）电池系统的绝缘设计应满足 GB/T18384 或企业要求；

（2）通过绝缘材料来提供触电防护的，则电气系统的带电部分应当全部用绝缘体覆盖；

（3）绝缘材料应能承受电动汽车及其系统的温度等级和最大工作电压；

（4）绝缘体应有足够的耐电压能力，进行耐电压试验不应发生绝缘击穿或电弧现象。

##### 4.2.3.1.2 电气间隙、爬电距离

（1）电池系统高压系统的电气间隙和爬电距离参考 GB/T 16935.1-2008；

（2）根据耐压等级、环境污染等级确定电气间隙；

（3）根据环境污染等级、材料 CTI 值、工作电压、工作海拔高度等确定爬电距离；

（4）当主电路与控制电路或辅助电路的额定绝缘电压不一致时，其电气间隙和爬电距离可分别按照其额定值选取。主电路或控制电路导电部分之间具有不同额定值时，电气间隙与爬电距离应按照最高额定绝缘电压选取。

##### 4.2.3.1.3 电位均衡

（1）所有组成电位均衡电流通路的组件（导体、连接部分）应能承受单点失效下的最大电流；

（2）电位均衡通路中任意两个可以被人同时触碰到的外露可导电部分之间的电阻应不超过 0.1Ω，满足标准 GB/T 18384.3-2015 要求。

#### 4.2.3.2 电连接可靠性安全设计

电池系统内的电连接设计包括模组内电连接设计和模组外电连接设计。模组内电连接设计包括：电芯间电连接、温度及电压采样；

（1）电芯间电连接

电芯间电连接需要满足过流要求，材质一般是铜、铝或者镍，应注意避免铜铝间电化学腐蚀。

（2）温度采样

a.作为检测电池状态的一个重要手段，在设计时主要关注两个方面：排布位置和连接可靠。

b.排布位置建议可采集到模组内最高及最低温度。

c.采样线可考虑防短路措施。

（3）电压采样

由于电压采样直接与电芯正负极相连，若连接位置阻抗过大，会影响电压的采样精度，因此，电压采样需选择阻抗较小且比较安全可靠的连接方式，采样线需要考虑防短路措施。

（4）模组外电连接设计

包括模组间电连接设计、模组与电气件间的电连接设计、电气件间电连接。

模组外电连接一般使用锁螺栓或螺母作为对外电连接端口，在设计时应注意避免电电连接部位受载，同时应保证螺栓连接可靠性。

（5）为了电池系统维护的方便性和安全性，建议系统要设计有专门的维修接口，如用于熔断器的更换，以及电池系统内单体电池状态调整接口。

#### 4.2.3.2.1 系统过电流能力

（1）电池系统内部主回路各连接部分应具有在整个生命周期内承受系统最大持续电流的能力。

（2）电连接面积选择考虑温升和老化要求。

#### 4.2.3.2.2 电气连接可靠性

（1）电池系统内部主回路各电连接部分应具有有效的设计，建议采用螺纹胶锁死，以保证在整个生命周期内保持连接阻抗的可靠性。

（2）电池系统内部主回路各电连接部分的连接阻抗应具备明确的指标及检测方法，以便在生产及维护时进行检测；

（3）电池系统内线束高低压连接端子与电线连接应牢固，应满足 QC/T 29106 汽车电线束技术条件中的规定；

（4）连接器需要具有一个锁紧装置以避免分离或接触不良。高压连接器应具有高压互锁功能。

#### 4.2.3.2.3 接地要求

高压零部件接地一方面是为了改善 EMC，另一方面是为了满足安全需要。高压零部件接地需满足如下要求：

（1）所有与高压部件靠近的金属导体必须接地，如：冷却板、接插件固定板、靠近高压线的冷却管道所连接的水口、BMU（HVM）外壳、EDM 金属底板、金属托盘等；

（2）所有接地点表面应保证导电性，不应有导电性差的漆及氧化物，防止接地不良；

（3）所有接地点应保证一定的安装扭矩；

（4）电池系统内部接地建议采用专用的接地螺栓螺母或使用编织导线，电池系统与

车底盘接地线推荐使用编织导线，同时接地端子需镀锡；

（5）接地线应尽可能短；

（6）电池系统内接地点应与车身电底盘连接。

### 4.2.4 电池系统安全性测试方法

电池系统级验证主要是验证电池系统完整的性能和功能，可考虑以下几个方面：

（1）按照《电动汽车用动力蓄电池安全要求》国标要求，通过振动、机械冲击、模拟碰撞、挤压、湿热循环、浸水、热稳定性、温度冲击、盐雾、高海拔、过温保护、过流保护、外部短路保护、过充电保护、过放电保护测试。

（2）建议进行带载振动试验，充分发掘连接异常及温升异常，评估安全可靠性（振动时充放电）。

（3）建议进行动态 IP 模拟测试（振动、冲击整车涉水等）。

（4）建议采用同一测试样品在环境温度、环境湿度、振动状态下同步进行多因素应力综合评估，评估完成后对该测试样品再进行 IP 防护等级评估，应能够满足 IP 防护等级的要求。

### 4.2.5 电池系统生产安全要求

#### 4.2.5.1 生产过程中安全防护要求

（1）严格按照工艺流程装配，装配过程中避免出现压线等现象，防止操作中短路。

（2）生产及转运过程中应对单体、模组、系统及关键部件（熔断器、接触器等）进行必要的防护，避免因磕碰、跌落等造成安全隐患。

（3）生产及转运过程中裸露的 BMS 或采集板应进行有效的静电防护。

（4）电池系统宜具备手动维修开关或 Fuse。生产及转运过程中，电池系统上的维修开关应当拔掉插头并盖上防护盖，确保切断电池系统对外的高压输出，电池系统上的高压连接器应装有防护盖，确保操作人员安全。

（5）对模组、壳体的连接硬点进行必要的防护，避免因部件变形造成紧固点失效。

（6）对柔性或易变形部件（如密封垫、发泡硅胶）等进行工装防护，避免因部件变形造成失效。

（7）电池系统内部应对带电部件及连接点进行有效的防护，满足 GB 4208 中规定的 IPXXB 防护等级要求，防止在生产或维护过程中因人员误触导致的安全隐患。

（8）装配过程中使用的工装及工具与产品接触部分宜采用绝缘材质或做好绝缘防护，避免装配过程产生短路风险。

（9）生产及装运过程各零部件应固定牢固，避免运动过程中摩擦损坏导致短路。

（10）接通高压电前，必须进行高压电部件壳体接地检查，确认高压电部件的装配和连接可靠。

（11）对高压电部件进行拆装前，必须进行断电操作，确认已断开紧急开关和 12V 电源。

（12）在高压部件的拆卸、安装或其他操作时，操作人员需要取得低压电工证资质，佩戴高压绝缘手套，穿绝缘靴，同时必须做好自身的绝缘保护措施，身上不得带有任何金属物品。

#### 4.2.5.2 合理的下线检测

| 序列 | 测试类别 | 测试项目 | 测试目的 |
|---|---|---|---|
| 1 | 线束测试 | 线束测试 | 检测电池系统低压接口所有针脚是否正确 |
| 2 | 静态测试 | CAN 通讯 | 检测产品通讯是否正常 |
| 3 | | 绝缘电阻 | 检查产品的绝缘电阻性能 |
| 4 | | 绝缘耐压 | 检查产品的绝缘耐压性能 |
| 5 | | 绝缘检测功能 | 检查 BMS 的绝缘检测功能 |
| 6 | | 高压互锁功能 | 检查 BMS 的高压互锁功能 |
| 7 | | 软件版本 | 检查软件版本是否正确 |
| 8 | | 硬件版本 | 检查硬件版本是否正确 |
| 9 | | 压差 | 检查未充放电前压差是否满足要求 |
| 10 | 充放电测试 | 总压 | 检查电池系统总压是否满足要求 |
| 11 | | 充电功能 | 检查充电是否正常 |
| 12 | | 放电功能 | 检查放电是否正常 |
| 13 | | 总电压精度 | 检查 BMS 电压精度值是否满足要求 |
| 14 | | 电流精度 | 检查 BMS 电流精度值是否满足要求 |
| 15 | 直流内阻测试 | DCR 测试 | 检查电池系统直流内阻值是否满足要求 |

## 4.3 动力电池运输要求

明确电池系统在运输过程中的包装、存储等条件的安全要求，防止运输过程中存在的安全隐患，或因自身的安全问题造成对环境或周围人员、财产的损坏。

### 4.3.1 运输检测标准

电池系统运输检测可参照联合国《关于危险货物运输的建议书——试验和标准手册》第 3 部分 38.3 款(简称 UN38.3)内容要求。

### 4.3.2 包装及运输要求

#### 4.3.2.1 包装要求

（1）电池系统的包装应符合防潮防震的要求，应采取措施防止电池系统与同一包装内导电物质相互接触。

（2）电池系统内部所有零部件应按照正常生产要求进行固定。

（3）电池系统所有接口需进行独立保护，防止碰撞和短路。所有电气接口设置绝缘阻燃防护罩，确保接口处无金属部分裸露在外。

（4）电池系统设有维修开关(MSD)的，包装前确保维修开关已经取下，且维修开关接口处有绝缘材料进行包裹保护。

（5）包装箱应考虑运输环境条件（公路运输、铁路运输、水路运输等情况），包装箱需经过堆码试验、跌落试验等试验合格。

（6）包装箱应易于制造、装配，便于储运、机械装卸。

（7）包装箱内应在指定位置装入随同电池系统提供的文件和物料。

（8）包装箱应设置产品标签，包含下列内容：名称、物料编码、客户名称、制造厂名或商标等、生产日期、SN、每箱的数量、净重和毛重、堆码重量极限。

#### 4.3.2.2 运输要求

（1）电池系统建议在 40%SOC 以下状态运输，以 30%SOC 为宜；

（2）根据联合国《关于危险货物运输的建议书-规章范本》（简称 TDG）的内容要求，电池系统在运输过程中应避开易燃、易爆、易腐蚀危险品；

（3）电池系统与包装箱必须完全定位锁死，包装箱与运输工具也需通过转运架等完全锁死；在运输过程中，应防止剧烈震动、冲击、日晒、雨淋；

（4）包装和运输过程中，要避免人员对动力电池系统的踩踏和不良接触；

（5）运输器具满足运输试验要求；

（6）运输器具要求绝缘，防止意外短路；

（7）消防设备能满足运输车辆发生紧急事故的需求。

## 4.4 动力电池售后保养要求

明确电池系统在使用过程中的维护保养的措施、项目、频次等基本要求，及推荐建议等，对其安全状态进行跟踪，及时排除安全隐患。

### 4.4.1 动力电池保养、检测规范

#### 4.4.1.1 日常维护

（1）充放电

建议在适当的环境温度、SOC 状态下对电池系统进行充放电。

（2）存放

长期存放时，电池系统电量要处在适当状态，并定期进行深度充放电；存放区域远离热源、化学腐蚀等场地。

（3）行驶

建议用户养成良好的驾驶习惯，避免猛踩油门，形成瞬间大电流放电。

#### 4.4.1.2 定期保养

为保证电池系统安全运行，建议电动汽车定期前往售后服务中心检查（建议每 5000 公里/每半年）。

对电池系统的定期保养与检测，必须由专业人员操作，且保养与检测场所应备有与电池系统接口配套的绝缘保护盖，在操作前需对电气接口安装绝缘保护盖，确保操作人员安全。

定期保养与检测可选择如下项目：

（1）均衡充电——可利用维护接口使用诊断工具读取电池系统内部电芯电压一致性状态，根据电芯电压差异情况使用专门的维护仪、或者车载充电机进行均衡充电保养。

（2）气密性检测——检测电池系统壳体防护状态，使用专用检测工装对电池系统外部接口进行封堵，向壳体内部注入气体，通过保压法进行测试。

（3）绝缘性能检测——检测电池系统绝缘性能，可通过 2 种方式进行。

• 车辆“启动”状态下，使用诊断工具读取 BMS 软件上报的绝缘值；（推荐）

• 车辆“下电”状态下，使用绝缘测试仪检测电池系统高压输出端对接地点的绝缘值。

（4）外观检查——检查电池系统外壳及表面部件（接插件、压力阀、紧固螺栓）是否存在变形、破损、裂纹、松动等情况。如发现异常，视情况进行开箱检查。

（5）故障码检查——使用诊断工具读取电池系统内部故障码，对当前故障和历史故

障进行评估，对功能、安全相关的故障码做进一步的诊断。

（6）冷却系统检查及维护，如风冷系统近出风口的过滤系统清理,保证散热通道的畅通。水冷系统的冷媒进行定期检测更换,避免由于冷媒的变性造成冷却系统的冷却性能及功能下降。

### 4.4.2 动力电池年检项目及方法

为保证电动汽车电池系统安全运行，建议对电池系统进行定期年检。

电池系统年检项目可包含“电池系统保养、检测规范”等相关检测，同时可视需要增加电耗测试（整车）和容量测试等项目。如针对续驶里程衰减较明显的车辆，可使用专业测试设备检测电池系统容量、内阻、温升等参数。

若在年检中发现特定故障，可开箱检查电池系统内部状态，重点关注箱内环境（是否有进水、泄漏）、零部件表面状态（生锈、霉变）、接插件状态、模组外形（是否有鼓包变形）、高压连接点紧固状态等等。如应重点关注碰撞事故历史车辆以及长年限、长里程车辆。

# 5 电机系统与电驱动总成安全

## 5.1 总体要求

随着国家能源战略导向、四阶段油耗以及碳排放积分法规出台，电动汽车将在未来占据更大市场。电动汽车以混合动力和纯电动汽车为主。在混合动力汽车中，除了传统发动机以外还有驱动电机系统，用以联合驱动和制动能量回收。在纯电动汽车中，电机则是唯一的动力驱动装置。

从电驱动总成发展趋势和构型特点上看，乘用车驱动电机向高速化、高压化和集成化方向发展，现有主流产品最高转速不超过 16000rpm，未来转速将达到 18000rpm 或更高。直流母线电压 150～350～800VDC 左右，电机输出功率在 30kW～250kW 之间，输出扭矩在 100Nm～500Nm 之间，配套合适速比的减速器或者变速器后电驱动总成输出扭矩（轮端）2000Nm～5000Nm；电机输出与车轮驱动轴同轴或者平行布置。

对于商用车来说，当前最主流的驱动形式是电机直接驱动，含电机匹配固定速比减速器的动力总成（轻型商用车应用广泛），重型商用车通常采用电机匹配两档或者多档变速器的动力总成。 商用车驱动电机通常输出功率在 50kW～300kW 之间，专用工程车辆驱动功率需求可达 400kW 以上。不同载荷的商用车所需要的驱动电机转矩从 400Nm～5000Nm 不同，商用车电机系统的直流母线电压通常在 350VDC～800VDC 之间或者更高。商用车最主要的驱动系统布置型式仍然是类似传统商用车的动力总成通过传动轴与主减速器连接的形式，轮边驱动、集成式电驱动桥在商用车也有广泛应用。

在动力总成中，电机不仅是一个动力源、传动部件，同时还是安全件和法规件。电机作为动力源，同发动机相比，电机可以四象限运行，以转矩控制模式为主。在软件功能或者硬件失效情况下，电驱动总成可能出现非预期的转矩输出，比如转矩输出过大或反向等故障，造成意外的人员伤害。作为传动件，电机是传动链上的一环，电机转矩波动或由于 PI 参数调整不当，可能导致传动系扭振造成整车舒适性方面的问题。在高压安全方面，除 48V 电机外，车用电机工作电压都超过了安全电压 60V，有的可达到 500V 甚至更高，存在高压安全风险。整车上公告要求电机按照 GB/T 18488 试验，在企业准入和补贴申领等环节都需要采集电机的编码和壳体拓印等信息，因此电机是法规件。电驱动总成通常位于整车的底部，运行环境恶劣；电机大部分工况处于高速旋转状态，特别是乘用车驱动电机的工作转速远高于传统燃油车的发动机工作转速，由此带来的机械安全问题尤其需要重视。电机稳态工作温度通常在 120℃左右，部分工况下甚至达到或超过 160℃，电机控制

器的最高工作温度也会达到100℃以上，电驱动总成温度监测、防止永磁同步电机高温退磁、防止高温接触烫伤等方面的要求亟待规范。电驱动总成在复杂的环境里工作，需要整个寿命期内适应各种气候环境。特别是在夏季内涝严重地区和冬季极寒地区，电驱动总成的防护安全要求更加苛刻。相比于传统燃油车，复杂电磁环境是电驱动总成需要面对的另一个挑战，这对电驱动总成的电磁兼容性提出了更高的要求。电驱动总成高压、大电流、高温等工作特点导致了电驱动总成的维护保养与传统燃油车动力总成相比有很大不同，维护保养过程中的人身安全需要特别关注。

综上，电驱动总成安全应从高压安全、机械安全、热安全、防护安全（含电磁辐射与抗扰等）、安全保护策略、功能安全、维护保养安全等七个方面进行全面考虑。

## 5.2 高压安全

相对于传统内燃机汽车而言， 电动汽车一般有高达上百伏的电气系统，超过了直流安全电压范围（直流 60V），如不进行合理的设计与防护，将可能带来人员电击等高压安全问题。在高压安全方面应主要考虑如下技术要求和措施，如绝缘电阻、耐电压、高压安全标识、高压接触防护、等电位连接、高压放电、高压接口安全、漏电保护和碰撞后安全等。

### 5.2.1 绝缘电阻要求

#### 5.2.1.1 电机定子绕组对机壳绝缘电阻要求

应符合 GB/T 18488.1-2015 中 5.2.7.1 条的规定。

#### 5.2.1.2 电机定子绕组对温度传感器绝缘电阻要求

应符合 GB/T 18488.1-2015 中 5.2.7.2 条的规定。

#### 5.2.1.3 电机控制器绝缘电阻要求

B 级电压的电机控制器，应符合 GB/T 18488.1-2015 中 5.2.7.3 条的规定并满足如下要求：

1）动力端子对外壳，冷态及热态绝缘电阻均不小于 5MΩ；

2）动力端子对低压端子（非地），冷态及热态绝缘电阻均不小于 5MΩ；

以上测量应按照最高工作电压选择兆欧表，测试方法按照 GB/T 18488.2 进行。

#### 5.2.1.4 绝缘检测要求

通常电池包内部集成的绝缘检测功能可以针对整车高压系统的直流侧绝缘情况进行监测和报警。建议电机控制器具有交流侧绝缘检测功能。

### 5.2.2 耐电压要求

按照电驱动总成的最高工作电压设定测试电压并考虑冷态、热态，制定不同要求，具体如下：

#### 5.2.2.1 驱动电机绕组的匝间冲击耐电压要求

应符合 GB/T 18488.1-2015 中 5.2.8.1 条的规定，最高工作电压是指三相交流线电压有效值。

#### 5.2.2.2 驱动电机绕组对机壳的工频耐电压要求

应符合 GB/T 18488.1-2015 中 5.2.8.2.1 条的规定。最高工作电压是指三相交流线电压有效值。漏电流控制值按照技术文件要求执行。

#### 5.2.2.3 驱动电机绕组对温度传感器的工频耐电压要求

应符合 GB/T 18488.1-2015 中 5.2.8.2.2 条的规定。温度传感器对驱动电机壳体的工频耐电压测试要求和限值同 5.2.8.2.2 条的规定。

#### 5.2.2.4 驱动电机工频耐电压测试电压及测试次数的要求

按照 GB 755 要求，驱动电机的工频耐电压应仅对成品电机进行测试， 验收时避免对绕组重复进行全值耐电压测试。如果应客户需求进行第二次或多次耐压测试时，试验电压值应为前一次测试电压值的 80%，直到测试电压降至 1500VAC 最低试验电压，测试时间为 1 分钟。

对于完全重绕的绕组，等同新电机对待，采用全值耐电压测试。

对于部分重绕的绕组或经过大修后的电机进行耐电压试验，则推荐采用下述细则：

1）对部分重绕绕组的试验电压值为新电机试验电压值的 75%。试验前，对旧的绕组应仔细地清洗并烘干。

2）对经过大修的电机，在清洗和烘干后，应承受 1.5 倍额定电压的试验电压，如额定电压为 100VAC 及以上时，试验电压至少为 1000VAC，如果额定电压为 100VAC 以下时，试验电压至少为 500VAC。

#### 5.2.2.5 电机控制器工频耐电压要求

在产品认证时，电机控制器需按照 GB/T 18488.1-2015 中 5.2.8.2.3 条的规定进行工频耐压测试。对于有 Y 电容的电机控制器，允许出厂检验进行直流耐压测试，测试值为规定的工频耐压值的 1.414 倍。

控制器整机装配完成后必须先进行绝缘和耐电压检测，测试通过以后才允许上高压运行。

耐电压测试要求如下：

1）电压等级要求参照 GB/T 18488.1-2015 中表 2 的规定。

2）试验过程和实验方法参照 GB/T 18488.2-2015 中 5.8.4 条的规定。

3）漏电流限值按照技术文件要求执行。

因耐压测试对某些器件产生一定的损伤，会影响到器件的使用寿命，所以应尽量减少耐压测试的次数。如果应客户需求进行第二次或多次耐压测试时，试验电压值应为前一次测试电压值的 80%，直到测试电压降至 1500VAC 最低试验电压，测试时间为 1 分钟。

### 5.2.3 屏蔽与接地

#### 5.2.3.1 电机与电机控制器间高压线束屏蔽与接地要求

高压多相连接系统应带有屏蔽层，屏蔽层两端与高压部件外壳有效接地，实现电缆两端 360 度全方位屏蔽，每端接地电阻不大于 40mΩ 。高压屏蔽电缆屏蔽层应符合 GB/T 25087-2010 中 6.3 条要求，并且满足整车电磁兼容要求。

#### 5.2.3.2 控制器直流母线屏蔽与接地要求

高压连接系统应带有屏蔽层，屏蔽层电机控制器端与控制器外壳有效接地，实现电缆 360 度全方位屏蔽，接地电阻不大于 40mΩ 。

#### 5.2.3.3 位置传感器线束屏蔽与接地要求

位置传感器线束应采用双绞线，并外套屏蔽层，建议屏蔽层两端良好接地。

#### 5.2.3.4 CAN 总线屏蔽要求

建议电机控制器 CAN 通讯线束使用屏蔽双绞线，屏蔽层在电机控制器端应良好接地；或者按照技术文件要求执行。

#### 5.2.3.5 电机、电机控制器及其他功率控制器接地要求

驱动电机、电机控制器及其他功率控制器产品金属外壳的接地电阻应不大于 100mΩ 。

电机机座、控制器壳体等与底盘或者车身地之间应有永久、可靠和良好的电气连接。

接地线端子的连接应可靠锁紧并具备防松功能。

#### 5.2.3.6 等电位连接

下图是电机系统的典型高压拓扑。当高压部件正负极均出现绝缘问题（如正负极同时与外壳短路或局部漏电）的情况下，为满足人员防触电要求，电机系统可导电外壳（遮拦）与整车电平台应实现可靠的等电位连接。

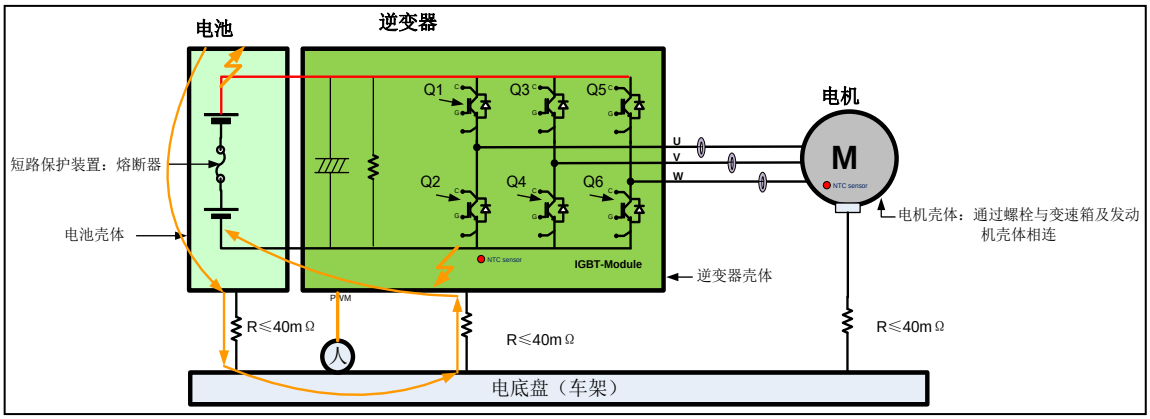



图 1　电机系统典型高压拓扑

等电位连接形式可采用如下三种方式连接，如图所示：

1）通过导体：如可导电的支架

2）电线束：如等电位连接线，颜色为棕色

3）直接连接：电机控制器直接通过螺栓与电平台相连或者焊接在车身上

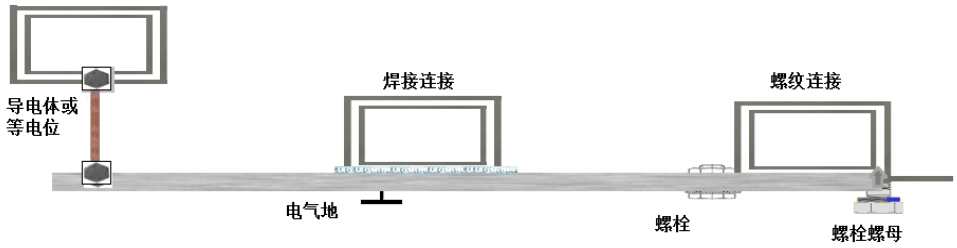



图 2　等电位连接形式

等电位连接要求：

1）阻值要求：电机系统的可导电外壳（遮拦）与整车电平台之间的电阻应小于 100mΩ。

2）短路电流：等电位连接应承载短路电流直至过流保护做出动作。

3）寿命：等电位的电阻需保持直至高压元件的指定寿命时间末。

4）连接要求：对于与车身地紧固的等电位连接形式，等电位连接线及螺栓应耐腐蚀超过其指定寿命时间，并且不允许自动松开。

5）接地端子不应兼作他用。

6）接地端子的螺栓和整车地应有足够截面，接地螺栓最小直径按 GB14711-2006 表 3（同下表 1）的规定，接地导线截面积按 GB 755-2008 表 19（同下表 2）的规定。

表 1　保护接地螺栓最小直径

| 电机额定电流 A | 保护接地螺栓最小直径 mm |
|---|---|
| ≤20 | 4 |
| ＞20~200 | 6 |
| ＞200~630 | 8 |
| ＞630~1000 | 10 |
| ＞1000 | 12 |

表 2　接地导线截面积

| 相线截面积/mm² | 接地导线或防护导线截面积/mm² | 相线截面积/mm² | 接地导线或防护导线截面积/mm² |
|---|---|---|---|
| 4 | 4 | 95 | 50 |
| 6 | 6 | 120 | 70 |
| 10 | 10 | 150 | 70 |
| 16 | 16 | 185 | 95 |
| 25 | 25 | 240 | 120 |
| 35 | 25 | 300 | 150 |
| 50 | 25 | 400 | 185 |
| 70 | 35 | | |

**5.2.3.7 接地标志要求**

接地点应有明显的接地标志。若无特定的接地点，应在有代表性的位置设置接地标志。

接地标志依据 GB/T 4026-2010 标以保护接地图形符号“⏚”，必要时再应用字母符号“PE”标志。这些标志不应放在螺栓、可拆卸的垫圈或用作连接导线的可能拆卸的零部件上。

**5.2.4 高压接插件和连接器**

1）B 级电压部件的遮拦和外壳应依据 GB/T 18384.3-2015，满足 IPXXB 防护等级要求。

2）选用的配对耦合高压接插件物理结构上的连接引导部分应不同，以满足防错插功能。

### 5.2.5 高压放电

在电机系统从高压回路断开后，由于电机控制器内部存在储能器件，如直流母线支撑电容等，电机系统内部高压并不会立即消失，而是慢慢下降，在常规维护或者售后维修时可能导致高压电击，造成人员伤亡。因此，为避免如上事故，电机系统需同时具备主动放电和被动放电功能，即使主动放电失效，被动放电依然有效，且在规定时间内必须降到安全电压以下，具体要求如下：

#### 5.2.5.1 主动放电要求

在电动汽车和混合动力汽车中使用的电机控制器输入端电压通常高于安全电压，为保护人身安全，要求在电机控制器的直流侧电容须配有放电电路，以快速降低直流侧电容的电压。电驱动总成必须具备主动放电功能。主动放电可以通过电机绕组或者外接专用放电电阻实施。

按照 GB/T 18488.1-2015 中 5.5.3 条的要求，当 B 级电压系统断电后，应在 3s 内将直流母线电压降至安全水平（直流电压 60 V 以下）。

#### 5.2.5.2 被动放电要求

电驱动总成还应具备被动放电的功能，在直流侧接入被动放电元器件实施。即使主动放电功能无法完成，被动放电装置仍可对直流侧电容进行放电。此功能必须始终有效，而非被触发后才有效。

当 B 级电压系统断电后，应在 2min 内将直流母线电压降至安全水平（直流电压 60 V 以下）。

### 5.2.6 高压防触电防护与警告

电驱动总成上应具有高压警示标志，高压警示标志应满足 GB/T 18384.3 -2015 中 5.1 条的内容。

图 3　高压警示标志

电驱动总成的 B 级电压部件的遮拦、外壳、接插件都应通过以下两种方式或其中一种满足直接接触防护的要求。

1）带电部分的基本绝缘；

2）遮拦或外壳，防止接近带电部分。

3）B 电压部件的遮拦、外壳、接插件至少要满足 GB/T 4208 中规定的 IPXXB 防护等级的要求。

如果遮拦或外壳可以徒手打开， 则其可以打开的部分应具备高压互锁装置，满足本文 5.2.7 章节的高压互锁要求。

### 5.2.7 高压互锁

高压互锁（High Voltage Inter-lock，简称 HVIL），是用低压信号监视高压回路完整性的一种安全设计方法。该互锁回路首尾连接在自动断开装置上，当高压电气回路上任何一个高压防护罩或插接件从回路上断开，就会触发一个低压电信号，高压立即被断开，且高压系统不能再次上电。对于满足防护等级 IPXXB 的高压接插件采用高压互锁措施；可拆卸的外壳采用高压互锁措施；如没有互锁措施，应能保证先触发高压系统的切断并保证外壳拆掉前有足够的时间使高压系统电压低于 60Vdc。高压互锁形式多样，可以用公母端接插件对配、微动开关或机械互锁等。推荐乘用车产品具备高压互锁功能，建议商用车产品选用高压互锁功能。如果高压接线系统具备高压互锁功能，系统的功率端子和信号端子应满足：

1）高压连接系统连接时，功率端子先接通，信号端子后接通；

2）高压连接系统断开时，信号端子先断开，功率端子后断开。

### 5.2.8 高压接触防护

可拆卸的电机控制器外壳，必须符合复杂拆卸，必须使用工具（非特指专用工具），并采用下列两种方式之一进行外壳拆除：

拆除三个以上螺栓或两种不同型号螺栓才能除去外壳。

只能使用配套的专用工具才能除去外壳，电机控制器安装在前机舱内，完全装配好的电机控制器防护等级应满足 ISO20653 规定的 IPXXB 或 IPXXD。

其他的可选措施包括高压互锁或者延迟接触：

延迟接触：应保证执行两个独立的操作后才能接近带电部件，第一步操作必须触发高压系统的切断并保证，第二步操作时高压部件电压已经低于 60Vdc 或低于 30Vac，人员触电防护同时应满足 GB/T 18384.3 的规定。

### 5.2.9 碰撞后安全

如果整车使用过程中发出碰撞，电驱动总成需根据整车控制器指令执行以下一个或多

个保护措施：

1）电机控制器切断负载电流，无功率输出；

2）电驱动总成激活无负载状态；

3）激活电驱动总成安全状态；

4）对高压电路主动放电。

具体指标要求如下：

1）当高压系统切断时，必须立即根据整车控制器要求开始高压电路的主动放电；

2）在碰撞信号发出的 3s 内，高压电路的电压必须降到 60Vdc 以下。

### 5.2.10 电驱动总成爬电距离和电气间隙要求

电气间隙为两导电部件之间在空气中的最短距离，与产品冲击耐受电压、污染等级、海拔高度有关。

#### 5.2.10.1 电机爬电距离和电气间隙要求

根据电机的耐压等级和海拔高度，参考 GB14711-2013 中 11 章节的规定确定电动机的爬电距离和电气间隙，具体要求见 GB14711-2013 表 4（工作电压 31V~750V）及表 14（1000V 以上，这个电压平台在当前电动汽车领域应用较少）。当工作电压在 750V～1000V 之间，建议按照 GB14711-2013 表 14 工作电压 1000V 下的爬电距离和电气间隙设计。

#### 5.2.10.2 控制器爬电距离和电气间隙要求

1）电机控制器高压系统的电气间隙和爬电距离参考 GB/T 16935.1-2008；

2）根据耐压等级、环境污染等级、工作海拔高度等确定电气间隙；参考 GB/T 16935.1-2008 附录 F.2，海拔修正系数参考 GB/T 16935.1-2008，表 A.2

3）根据环境污染等级、材料 CTI 值、工作电压等确定爬电距离；参考 GB/T 16935.1-2008 附录 F.4

4）当主电路与控制电路或辅助电路的额定绝缘电压不一致时，其电气间隙和爬电距离可分别按照其额定值选取。主电路或控制电路导电部分之间具有不同额定值时，电气间隙与爬电距离应按照最高额定绝缘电压选取。

### 5.2.11 高压接口安全要求

#### 5.2.11.1 防松脱设计要求

##### 5.2.11.1.1 可插拔高压接插件要求

可插拔高压接插件至少有两级锁止装置，至少需要两个不同的动作才能将其从相互的对接端分离；接插件之间具备防错插功能。可插拔高压接插件应满足 GB/T 37133-2018 附

录 A 的要求。

#### 5.2.11.1.2 其它方式连接的要求

高压连接系统的电缆压接、螺纹连接、焊接等连接装置，应无松脱、断裂等连接缺陷。

#### 5.2.11.2 高压连接系统防护要求

正常连接时高压连接系统的防护等级应不低于 IP67。若高压连接系统可不通过工具手动断开，则非连接状态的高压连接系统各部分的防护等级应满足 IPXXB。

#### 5.2.11.3 高压连接系统耐振动要求

高压连接系统的耐振动要求应满足 GB/T 37133-2018 第 7.4 条的要求。

#### 5.2.12 低压线束连接安全要求

#### 5.2.12.1 低压线束连接可靠性

低压连接系统的耐振动要求应满足 QC/T 29106-2014 第 4.10 条的要求。

#### 5.2.12.2 低压插件碰撞保护要求

设计时低压接插件应布置于不易受碰撞的地方或者应有一定的防碰撞保护，避免系统在运输、安装、运行过程中受损。

#### 5.2.12.3 低压线束密封性检查要求

正常连接时低压连接系统的防护等级应不低于 IP67。

## 5.3 机械安全

相对于传统内燃机汽车而言，电动汽车上驱动电机转速通常远超发动机，同时动力总成又有轻量化的设计要求，这就要求电驱动总成在开发及验证环节必须特别重视产品机械强度、刚度与轻量化的工程矛盾处理。轴承是电驱动总成中较容易发生故障的关键零件，影响整车安全；相对于传统变速箱系统，电驱动总成特有的高频、高压、大功率用电所导致的轴电流容易使轴承发生早期电腐蚀失效。传动系统的齿轮、轴系等都具有高转速、高可靠运行的特殊要求。以上这些方面都使得电驱动总成的机械安全尤为重要。

### 5.3.1 转子强度

电机转子是电机能量转换的重要组成部件之一，是电机中主要的旋转零部件，用于输出电机的动力。转子机械安全设计的主要方向是高转速转子铁芯形变量控制，转子冲片结构强度和许用不平衡量等。

驱动电机转子应能在所有规定工况下正常运行，而不出现影响使用的变形、松动、振动噪音增大、以及零部件的断裂、破碎和脱落等异常情况。

通过 CAE 辅助设计，考虑 1.2 倍电机最高工作转速工况下，转子铁芯的形变量应小于电机气隙的 10%，同时转子铁芯的最大应力应满足安全系数要求。

#### 5.3.1.1 超速试验要求

驱动电机在热态下应能承受 1.2 倍最高工作转速试验，持续时间为 2min，其机械结构应不发生有害变形。

#### 5.3.1.2 转子系统动平衡要求

转子动平衡量应满足 GB/T 9239.1 标准规定的 G2.5 级及以上的标准，特殊要求除外。

### 5.3.2 轴承可靠性

#### 5.3.2.1 轴承油脂、润滑、密封维护要求

轴承需要具有良好的工作环境，装配、运输及运行中不能有水或其他杂质进入轴承。允许轴承按照保养要求定期更换油脂甚至更换轴承，保证轴承润滑和正常运行。电机内部拆装维修时需要每次更换新轴承。维护轴承需要由专业厂家进行。

#### 5.3.2.2 轴承声音主观检测要求

对电驱动总成进行噪音出厂检测，通过声学设备判断电驱动总成的噪音特征是否存在异常。必要时或条件暂时不具备时，可结合一定的主观判断。

#### 5.3.2.3 轴电压和轴电流的防护

较大的轴电流会导致电机轴承出现早期电腐蚀，降低轴承寿命，产生异常振动噪音，建议高频电机采取轴电流抑制措施。推荐采取以下主要措施抑制轴电流：

1）设计合理的滤波器，减小变频电源共模电压，可以较好地消除 PWM 电机控制器产生的高频谐波。

2）电机一端轴承采取绝缘措施，来抑制轴电流。具体方法可以是采用绝缘轴承，或者在轴承座或端盖轴承室上设置绝缘结构实现。

3）双端轴承绝缘的同时将轴与外壳直接短接，抑制静电引起的共模轴电压，同时可以进一步减小油膜电压，保护轴承不受电腐蚀而损坏。

### 5.3.3 壳体强度

壳体的强度应满足不同工况下车辆的使用需求，通常参考 GB/T 28046.3-2011 或客户标准，保证在发生碰撞的情况下，在保证车内人员安全的前提下，尽可能的减少对电机的损害。

#### 5.3.3.1 壳体离地间隙要求

在整车的布置过程中，应保证驱动电机壳体要高于车架（或副车架）并留出一定的安

全距离，确保车辆在满载、过坑洼路面等极限工况下，防止电机拖底问题发生，保证行车安全。

#### 5.3.3.2 维护、检查、防脱落要求

电驱动总成在整车布局中的位置，应考虑在检查、维护过程中的便利性。车辆在运行一定周期后，需要对电驱动总成等相关部件进行检查、维护，通常采用力矩检查法或划线标记法（特殊情况）判别连接是否发生松动，一旦发现松动，应立即进行连接位置的锁紧、防松。避免车辆在使用过程中发生驱动电机松动、脱落，从而导致交通事故发生。

### 5.3.4 机械防触碰与警告

车辆传动装置为旋转部件，应在设计过程中考虑旋转部件对人身造成的伤害，通过物理结构将旋转部件与人体隔离。对于无法进行防护的旋转部件，在周边应粘贴或安装醒目的警告标识，以避免对人身的伤害。

水接头的设计应首先保证冷却管路的密封性、承压性和安装便利性。保证冷却水道的压力检测值不小于 250kPa 或依据客户要求，通常采用湿式检测法或干式检测法判别水道的密封性和承压性。

高、低压接插件应满足产品的 IP67 防护等级，同时对线束在一定长度范围内进行安装固定，防止在长期振动环境下运行对接插件密封和保护造成伤害。接插件周边和线束应设置有效的物理防护（例如金属或非金属保护罩、网），防止在运输、装配、车辆运行过程中，破坏接插件。

### 5.3.5 输出法兰防松脱检查要求

驱动电机系统输出法兰须与传动轴连接可靠，避免松脱。车辆在运行一定周期后，需要对电机输出法兰、传动轴及其相互间的紧固件等相关部件进行检查、维护。通常采用力矩检查法或划线标记法判别电机连接是否发生松动，一旦发现松动，应立即进行连接位置的锁紧、防松。避免车辆在使用过程中发生驱动电机松动、脱落，而导致交通事故发生。

### 5.3.6 花键润滑检查要求

动力总成通常由减（变）速器和驱动电机组成，而传动轴通常为内/外花键连接，长期暴露在空气中使用，极易发生锈蚀、磨损，造成花键连接失效。在设计之初应考虑花键的润滑密封等问题。通常在花键两端设置有密封圈，在密封的花键腔体内，填充一定量的润滑脂（油脂添加需适量，过量油脂会产生压力损坏轴承），以保证花键润滑有效。同时还应结合实际耐久试验情况，给出花键润滑脂的检查间隔时间和油脂填充量，通常每 5 年或 10 万公里或根据整车厂要求，进行一次检查。同时给出花键磨损的判别标准，必要时

需更换花键。

### 5.3.7 转轴的机械强度

电机转轴应能满足整车各种工况下的最大扭矩输出要求。电机轴的机械强度依赖于优化的结构设计、准确的受力分析和校核、材料选择、热处理和加工装配等。如有必要，需进行静扭试验和扭转疲劳试验。

参照标准 QC/T 534-1999，静扭强度后备系数应大于 1.8 倍的峰值扭矩

### 5.3.8 变/减速器静扭强度

变/减速器静扭强度后备系数不小于 2.5，试验方法按照 QC/T 1022-2015 中的 6.2.4.9。

### 5.3.9 变速器换挡安全

变速器换档可靠，无乱档，脱档，换不上档或摘不开档的现象。

### 5.3.10 驻车安全

车速高于 5km/h 时，误碰驻车功能按钮时应不能驻车；当处于非驻车状态时，无论发生任何异常情况，驻车机构都不能自动驻车；驻车后，驻车机构不能自动脱档；当汽车需要行驶时，驻车机构能使汽车顺利脱离驻车档；应设有手动解锁功能。

## 5.4 热安全

热失效是电驱动总成常见的失效形式，由于故障或长时间超负载运行，导致电机绕组烧毁或电机控制器功率模块损坏，会直接造成电动汽车失去动力，极大影响行车安全。因此在电驱系统设计中，必须考虑热安全因素，采取相应的对策保证系统安全运行。电驱系统性能输出能力往往受限于温升和工作温度限值。合理的温度设计能够最大化发挥电驱系统性能。温度场仿真、试验验证和实时监控保护三位一体，共同保证电动汽车运行安全。电机定子绝缘系统寿命与其工作温度强相关。经验表明，绝缘材料在超过其工作温度下使用，每增加 10℃，寿命减少约一半。长时间高温下工作容易造成绝缘纸、绝缘漆等提前老化、失效，造成绕组短路烧毁等严重后果。电机热性能设计的工作重点就在于控制电机工作温度，保证寿命。电机转子散热条件一般较差，转子铁损和磁钢涡流损耗产生的热量容易累积，造成转子温度升高。随着电机向高速化发展，转子将面临更大的散热压力。在设计方面，可通过温度场仿真可以对永磁体温度做初步评估，但是面对复杂多变的实际使用工况不能完全覆盖。在温度监控方面，转子作为旋转部件，一般难以直接布置温度传感器实时监测转子铁芯和磁钢的工作温度，可通过建立转子温度模型实时估算转子磁钢温

度，并建立相应的温度保护控制算法，保证磁钢始终工作在其许用工作温度范围内。

### 5.4.1 热预警、降额、保护

#### 5.4.1.1 温度传感器的冗余设计建议

建议电机和电机控制器均采用两路温度传感器进行温度监测，并在仪表中实时显示温度较高的一路温度传感器的温度。

#### 5.4.1.2 温度传感器测点与软件设计关系

在电机系统研制过程中，建议进行多温度传感器样机摸底测试。根据多温度传感器样机测试结果，确定批量供货产品的温度最高点以及与其它可能埋置温度传感器的温度差值，推荐温度传感器一个布置在三相中性点以监测三相温度，另一个尽可能布置在温度最高点。保护软件编写时，需要根据前述测试及温度传感器埋放位置，进行数据采集上报列表。一旦一个温度传感器失效，软件在采样切换到另一个有效温度传感器同时，也应根据切入传感器采样调整软件报警温度设置。另外软件也要根据前述试验认证留出足够的安全裕量。

#### 5.4.1.3 过热三级故障保护机制要求

系统需要使用三级故障处理机制；处理策略应符合产品技术文件规定。推荐的保护策略见本章 5.6 节。

### 5.4.2 转子退磁：高温下的退磁安全、转子温度估算

永磁体会产生由温度效应、过电流或不当电流控制角引起的退磁问题。电机设计阶段要充分校核峰值工况和三相短路工况下的退磁临界点，避免电机运行工况在临界点以上。同时估算电机持续运行时的转子温度，保证在大电流负载和控制角下，永磁体的温度不超过所选牌号磁钢的退磁温度限值。在电机系统研制阶段，建议进行必要的退磁测试认证。建议建立比较准确的转子温度估算模型，并将估算模型纳入控制软件保护程序中。下面是一种温度估算方案：通过大量测试建立定子绕组温度与转子磁钢温度之间关系曲线，在软件中通过监控定子温度，间接监控转子磁钢温度。

### 5.4.3 轴承耐温、密封材料耐温、绝缘材料耐温要求

轴承耐温应限制在极限工况温度范围内，温度范围由整车厂与电机供应商技术文件规定。推荐轴承工作温度范围-40℃～150℃。

电驱动总成的密封材料，如密封圈、密封胶垫和油封等，其耐温应大于 150℃。

电机的绝缘材料耐温等级应使用 H（允许工作温度 180℃）级及以上耐温材料（参考 GB/T 20113-2006）。绝缘系统温度等级取决于电机各种绝缘材料（绝缘纸、电磁线、绝缘

漆和端部绑扎线等）的最低耐温等级。供应商应在产品铭牌上明确标记绝缘系统等级。

### 5.4.4 阻燃材料使用

用于高压连接的线束、注塑件的阻燃性能应符合 GB/T2408-2008 规定的水平燃烧 HB 级，垂直燃烧 V-0 级。B 级电压电缆防护用波纹管及热收缩双壁管的温度等级应不低于 125℃，热收缩双壁管的性能应符合 QC/T 29106-2014 中附录 B 的要求，波纹管的性能应符合 QC/T 29106-2014 中附录 D 的要求。

### 5.4.5 人体防护与警告

#### 5.4.5.1 停机高温警示

任何可能被操作、维保人员触及的高温部件，例如壳体等，应有高温警示标志。具体停机高温警示要求由整车厂确定。举例如下：对于采用 H 级绝缘的电机，当绕组温度超过 160℃ 时，整车面板上应提示电机温度过高。电机绕组温度达到 170 ℃ 后应停机保护，停机后水冷电机金属壳体温度可能高达 120℃，30min 内请勿直接用手触摸，以免烫伤！

建议电驱动总成上粘贴当心高温表面警示标志，当心高温表面警示标志应满足 GB2894 中 4.2.3 章节的内容。

图 4　高温表面警示标志

#### 5.4.5.2 故障报警要求

当电驱动总成发生故障时，必须在仪表板进行提示，并进行声、光、电综合报警。

### 5.4.6 电驱动冷却系统（水泵、管路、连接件等）定期检查要求

建议电驱动总成的冷却系统每半年或整车行驶 4 万公里，需要进行一次定期检查或者按照整车厂提供的维护保养手册执行。检查冷却管道外部、进出水口附近、电机、电机控制器上是否有冷却液渗出；如有异常，判断泄露部件，进行相应更换或维修。

### 5.4.7 变/减速器油温要求

变/减速器油池温度最高不应超过 130 度。

## 5.5 防护安全

IP 防护是机械安全设计必须考虑的因素，电驱系统的密封设计或选型应能满足 IP6K7 和 IPX9K 要求。电驱动总成在复杂电磁环境中工作，这对电驱动总成的电磁兼容性提出了更高的要求，电驱动总成既要具备严格的电磁辐射和传导指标，同时也要具备优秀的抗干扰能力。

### 5.5.1 防水/防尘设计：端盖、轴密封性设计

#### 5.5.1.1 液冷（水、油等）介质防尘要求

驱动电机及控制器应具有防尘、防水能力，其防护等级应满足标准或客户规定的要求，最低要求是不低于 IP67。

电机在整车安装后，应满足车辆在断电状态下，在水深 50 cm 水池浸泡 24h 后，整车开机，电驱动开关置于“ON”位置，电机及电机控制器不应由于本身原因引起安全事故（例如：起火等）。

#### 5.5.1.2 油冷电机生产过程的防尘要求

油冷电机在装配和使用过程中，应特别注意电机的防尘。防止因灰尘、异物等进入电机内部，对绝缘、轴承等造成影响。

需要针对不同的零、部件分别制定清洁度控制指标。清洁度的控制需要同时控制杂质总重量和最大杂质颗粒度两项指标。清洁度指标按照企业内部标准执行。

#### 5.5.1.3 旋转密封设计要求

水冷式电机和油冷式电机的旋转密封设计有明显的不同，前者一般没有润滑介质，而后者有润滑介质。

针对水冷式电机，如采用橡胶油封的传统旋转密封技术，会因为缺少润滑，导致橡胶油封过早失效。

1）规范油封的安装，油封安装完后，检测密封性。

2）电机增加透气阀，平衡电机内外部的气压，避免因为呼吸效应导致油封密封部位出现气流的进出。

旋转密封件需要按照保养手册定期检查维护，必要时更换。

#### 5.5.1.4 控制器的防尘控制要求（针对现场维修）

驱动电机控制器维修需要在干燥、无尘、有静电防护的区域进行。 维修前，需要彻底清洁驱动电机控制器，维修后，应进行全面测试。

#### 5.5.1.5 高压线束密封设计要求

正常连接时高压连接系统的防护等级应不低于 IP67。若高压连接系统可不通过工具手动断开，则非连接状态的高压连接系统各部分的防护等级应满足 IPXXB

#### 5.5.1.6 低压线束密封设计要求

正常连接时低压连接系统的防护等级应不低于 IP67。

### 5.5.2 气密

#### 5.5.2.1 驱动总成冷却管路密封性检查要求

冷却水道气密需考虑充气压力、充气时间和保压时间。检测时间和压降需根据具体产品规格确定；也可以采用负压法测试。

#### 5.5.2.2 电机旋转密封检查要求

电机旋转密封检查通常采用两种方法：

1）按照 GB/T 4942.1-2006 标准进行相关要求的试验；

2）采用气密测试需考虑充气压力、充气时间和保压时间。检测时间和压降需根据具体产品规格确定；也可以采用负压法测试。

#### 5.5.2.3 控制器密封检查要求

控制器冷却水道密封检查要求：需考虑充气压力、充气时间和保压时间。检测时间和压降需根据具体产品规格确定；也可以采用负压法测试。

控制器壳体密封检查要求：在高压接插件、低压接插件耦合状态下，需考虑充气压力、充气时间和保压时间。检测时间和压降需根据具体产品规格确定；也可以采用负压法测试。

#### 5.5.2.4 电驱动总成高、低压连接密封要求

高压连接系统和低压连接系统正常连接状态下，需考虑充气压力、充气时间和保压时间。检测时间和压降需根据具体产品规格确定；也可以采用负压法测试。

#### 5.5.2.5 防冷凝要求

电机系统及电驱动总成产品在其生命周期内防尘防水等级应达到 IP67，在此基础上需要进一步考虑产品因温度变化而引起内部压强变化和呼吸效应，从而造成凝露现象，使产品腔体内积水，进而造成电气故障及零部件锈蚀。电机系统及电驱动总成产品应选配合理透气量的防水透气阀。透气阀的选型：与箱体配合处防护在全生命周期等级达到 IP67 等级。透气阀通常安装在产品的上部或侧面。

#### 5.5.2.6 电驱动总成涉水及涉水后的检查要求

按照 GB/T 18384.3-2015 中 8.3.1 和 8.3.2 的要求：

1）电机、电机控制器按照 GB/T 18488.1-2015 中 5.2.82 要求进行耐电压测试.；冷态绝缘电阻应符合产品出厂测试标准。

2）按照产品出厂测试标准检查控制器、驱动电机气密性。

### 5.5.3 EMC 及防护：电磁噪声对车载设备

新能源汽车对 EMC 要求越来越严苛，很多整车厂零部件公司硬性指标要求电机控制器满足 3 级标准，电机控制器设计过程中应考虑电磁兼容性，电磁骚扰主要通过辐射与传导两种途径对电子设备产生影响。

#### 5.5.3.1 电磁辐射骚扰

电驱动总成应满足 GB/T 18655-2018（建议等级 3 限值）的要求及 GB/T 36282-2018 标准限值要求。电驱动总成装到整车后，整车应满足 GB/T 18387 的要求。

按照 GB/T 36282-2018 的要求，在做发射类试验时，电驱动总成应处于工作状态，转速为额定转速的 50%，扭矩为额定扭矩的 50%，机械输出负载达到持续功率的 25%。

当转速或扭矩达不到其试验状态时，可调整扭矩或转速以达到持续功率的 25%，并在试验报告中特别注明。

#### 5.5.3.2 电磁辐射抗扰性

电驱动总成应通过合理布置及屏蔽保护设计使其抗干扰性满足表 3 中要求。

表 3　电磁辐射抗扰测试标准

| 测试项目 | 国标要求 |
| --- | --- |
| 电波暗室法 | GB/T 33014.2-2016 |
| 大电流注入法 | GB/T 33014.4-2016 |
| 瞬态传导抗扰度(电源线) | GB/T 21437.2-2008 |
| 瞬态传导抗扰度(信号线) | GB/T 21437.3-2008 |
| 低压瞬态传导发射 | GB/T 21437.2-2008 |
| 静电放电 | GB/T 19951-2005 |

#### 5.5.3.3 电磁辐射人体健康的安全性评估

车辆在处于以下工况时，应按照 GB/T 37130-2018 进行试验验证；10Hz-400KHz 的磁场发射量符合 GB/T 37130-2018 附录 A 中表 A.1、表 A.2 和表 A.3 限值要求。

1）静态工况：车辆静止状态用电器全开，车辆动力系统高压上电完成（PTReady）；

2）动态工况：车辆 40km/h 恒速行驶；

## 5.6 电驱动总成故障保护机制

乘用车电驱动总成的保护机制至少需要包括下列内容，具体处理策略实施可由整车厂与电驱动总成供应商协商达成一致。商用车电驱动总成的保护机制可参考乘用车要求，可按照与整车厂协商结果执行。

乘用车涉及功能安全相关的故障保护是要考虑安全状态的，这一点在 5.7 功能安全部分有描述。故障触发机制和恢复机制需要根据整车厂需求来完成设计和验证。此外故障容错时间和优先级的问题在 5.7 的功能安全开发中有介绍。

### 5.6.1 故障触发机制

根据一个或多个条件的判断，在一定的时间内判定当前故障状态是否已被触发的机制，叫做故障触发机制。

基本的故障触发机制包括以下类型：

当故障状态被触发后，根据当前的实际运行状态，在尽量减小对驾驶人产生干扰的前提下将系统进入安全状态的机制，叫做故障保护机制。

基本的故障保护机制包括以下类型：

1）电路板上单一物理量单次超出既定限值，触发故障状态。可以是模拟信号触发硬件故障保护，也可以是硬件驱动故障触发故障保护。

2）软件内部单一量单次超出限值【可标定】，触发故障状态。

3）软件内部单一量多次超出限值【可标定】，触发故障状态。

4）软件内部单一量在一段时间 T【可标定】内 N【可标定】次超出限值【可标定】，触发故障状态。

5）软件内部单一量与实时监控计算值【不可标定，变量】的偏差超出限值【可标定】，触发故障状态。

6）软件内部多个量超出限值【可标定】，并根据一定的逻辑判断后，触发故障状态。

7）主控芯片利用本身的检测机制保证程序执行正确性，否则触发故障状态,(例如：主控芯片检测时钟等信息，故障的触发是检测锁相环 PLL 的丢失（不可标定），)同时也要保证计算结果的正确，通过例如 lockstep 等机制检测故障，程序流也可以依据芯片内置 watchdog 保证执行周期，同时检测故障。

8）外设其他功能安全芯片保证主控芯片正常工作，否则触发故障状态。具体时序参考芯片手册。外设功能安全相关芯片检测程序运行状态。问答式检测在线机制或超时时间（可标定）进入 Safety Sate 状态。

9）在一段时间 T【可标定】内未完成预设功能，触发故障状态。这里预设功能不是指芯片本身的故障，而是电机控制器设计的基本功能，常见如：自学习，主动放电等。

### 5.6.2. 故障保护机制（进入安全状态或切换安全状态）

当故障状态被触发后，根据当前的实际运行状态，在尽量减小对驾驶人产生干扰的前提下将系统进入安全状态的机制，叫做故障保护机制。当故障条件发生变化时，安全状态也可以随之切换。

基本的故障保护机制包括以下类型：

1）软件检测模拟值包含电压、转速、温度等是否超出设置值【可标定】，系统进入 ASC 主动短路状态或三相开路状态，上报故障信息，存储故障信息，冻结相关数据帧。

2）根据 IGBT 当前的状态（正常、上桥故障、下桥故障），系统进入 ASC 上桥短路状态或 ASC 下桥短路状态。硬件检测模拟值是否超出限制值或存在硬件驱动故障，系统进入 ASC 主动短路状态。

3）根据系统状态，系统进入 ASC 主动短路状态或三相开路状态，上报故障信息，存储故障信息，冻结相关数据帧。根据 IGBT 当前的状态（正常、上桥故障、下桥故障），系统进入 ASC 上桥短路状态或 ASC 下桥短路状态。

4）进入零转矩模式。上报故障信息，存储故障信息，冻结相关数据帧。

5）进入跛行回家(Limp-home)模式，采取降额措施，具体降额的量以及比例与故障源物理量相关，其相关性可标定。上报故障信息，存储故障信息，冻结相关数据帧。

6）进入冗余模式，不做故障上报，存储故障信息。

7）故障条件消失时，清除故障 ，根据当前转速、电压等模拟信号，经过一定时间（可以标定）从主动短路 ASC 的安全状态可以切换到三相开路的安全状态，进入低压上电完成后的初始状态模式。

### 5.6.3 故障恢复机制

当故障状态被触发并进入安全状态后，根据当前的实际运行状态，使系统退出故障状态并具备重新实现原有功能的能力的机制，叫做故障恢复机制。

基本的故障恢复机制包括以下类型：

1）钥匙拔出，等待数秒后，重新执行 KL15 重新上低压电唤醒，清除故障。

2）KL15 重新上低压电唤醒，清除故障。

3）故障条件不满足时，KL50 重新上高压电，清除故障。

4）故障条件不满足时，CAN 通信发出特定指令后，清除故障。

5）故障条件不满足时，经过一段时间 T【可标定】后，或者满足一定计数条件【可标定】，清除故障。

6）故障条件不满足时，自动清除故障。一些降额故障或者 0 扭矩模式可以自动恢复，但是建议恢复阈值的设计考虑滞环。

### 5.6.4 电驱动系统故障保护示例

下面是保护策略实施案例：

#### 5.6.4.1 转矩反馈异常

故障描述：实际转矩与命令转矩偏差超过一定范围时，进行故障计数，同时，偏差在正常范围内，故障计数值需要减少。根据故障计数值达到不同阈值进行分级处理，故障分级阈值可以进行标定。转矩异常的原因可能是初始旋变位置错误或者电机参数不正常。

故障处理策略：

1）1 级故障进行降额处理，降额系数可标定，如果计数值小于故障阈值表示此故障可以进行恢复。取消降额保护。

2）3 级故障根据当前转速信息进行关管封脉冲或者主动短路处理，当转速降低到一定转速时，主动短路状态建议进入低压上电完成后的初始状态。

#### 5.6.4.2 CAN 通讯故障

故障描述：

1)超时监控。通过检测同 ID 报文的 Livecounter 计数值来进行监控，当 Livercounter 的不连续的情况出现一次，则记一次故障计数，当故障计数在一定时间内出现一定次数，则报出通讯失效故障，否则清 0 故障计数值。

2）探测总线通信失效，发送信息回读。MCU 从总线上回读已发送信息并与原始信息做比较。MCU 发送一帧特殊信息帧给整车控制器，整车控制器经过一个周期回复此信息，MCU 接收到之后进行比较。如信息不一致，报出通讯故障。

3）用于探测帧丢失，帧计数器。MCU 接收整车报文时，整车发送给 MCU 的报文，对同一帧 ID，进行计数每个单独的安全相关帧包含一个作为信息一部分的计数器。在生成每个连续帧时计数器值增加(翻转)。MCU 随后能通过验证计数器的值是否增加了 1 来探测任何的帧丢失或者帧未更新。如果帧未更新的话，报出帧丢失故障。

故障保护策略：通讯故障报出后可以进行降额处理，此故障在 CAN 通讯监测恢复后可以设置一定的扭矩恢复斜率，但是当 can 故障在一定时间内多次出现故障后建议取消恢复机制。

#### 5.6.4.3 微控制器故障（举三个例子，依赖芯片本身的安全机制）

故障描述：

1）时钟频率监测，MCU 提供内部时钟监控功能，可以监测芯片各模块的时钟信号。芯片内可以生成 100MHz 的时钟信号，独立于 PLL 系统工作。系统以这个时钟为参考，生成一个参考计数器来校验其他模块的时钟。如果计数器有溢出，则说明发生错误。可以检测到计数器要么低于下限值（时钟过慢）要么高于上限值（时钟过快）。

2）静态随机存取存储器的错误探测纠错码，静态随机存取存储器可以执行 4 个代码间距的错误代码修正，修正单字节错误和检测双字节错误。

3）程序存储器错误探测纠错码，为了预防数据损坏，程序存储器中数据包含错误探测纠错码。在程序存储器中数据可以进行两个位误差校正，三个位错误检测。

故障保护策略：根据芯片手册查询相关安全机制同时和硬件外围电路的设计相关。

#### 5.6.4.4 高压电容快速放电故障

故障描述：当主动放电时间超过 3 秒钟，且母线电压未降低到放电要求电压时，报放电超时。

故障保护策略：退出放电模式，或者切入其他放电模式，建议采用电机放电和电阻放电的其中一种方案。

#### 5.6.4.5 控制器直流侧短路

故障描述：当检测到直流侧发生短路时，报出故障。

故障保护策略：控制器一般报出 Desat 故障，驱动芯片会关掉 IGBT，如果进入三相短路状态，需要知道当前是哪个管报的 Desat 故障，转速较低时，可以采用封脉冲处理。

#### 5.6.4.6 控制器交流侧短路

故障描述：分为相间短路、对壳体短路，对母线正或者对母线负短路，当交流传感器检测到过流或者其他驱动芯片报 Desat 故障。

故障保护策略：过流故障根据当前转速信息进入关管封脉冲或者主动短路的处理策略，当转速降低到一定值时，主动短路可以退出并进入关管状态。Desat 故障同上。其中对壳体短路，一般会检测出三相电流之和较大不合理。

#### 5.6.4.7 自检异常

故障描述：MCU 检测异常。

故障保护策略：报自检故障，禁止执行预充操作。自检时间整车厂一般会明确要求。

此外根据整车厂单独要求会添加自学习功能，那么就要考虑自学习时间和自学习失败的报警。

#### 5.6.4.8 过压(高压)

故障描述：母线检测电压高于过压阈值。

故障保护策略：

1）一级过压：随着电压升高，电机响应扭矩线性降低。

2）二级过压：电机响应扭矩保持为 0。

3）三级过压：三相短路。当转速降低到一定值时，主动短路可以退出并进入关管状态。避免车辆静止状态还处于三相短路中，导致 IGBT 烧毁。

#### 5.6.4.9 欠压(高压)

故障描述：母线检测电压低于过压阈值。

故障保护策略：

1）一级欠压：随着电压降低，电机响应扭矩线性降低。

2）二级欠压：电机响应扭矩保持为 0。

#### 5.6.4.10 断路/开路(高压)

故障描述：当检测到断路/开路时，报出故障，交流侧断路可以检测三相不平衡。

故障保护策略：根据当前转速信息进入关管封脉冲或者主动短路的处理策略，当转速降低到一定值时，主动短路可以退出并进入关管状态。

#### 5.6.4.11 过流(高压)

故障描述：当检测到过流时，报出故障。

故障保护策略：根据当前转速信息进入关管封脉冲或者主动短路的处理策略，当转速降低到一定值时，主动短路可以退出并进入关管状态。

#### 5.6.4.12 驱动电机过温保护

故障描述：电机温度检测高于过温阈值，这里需要注意在热安全中有提及，电机转子温度需要有必要的监控手段。

故障保护策略：

1）一级过温：随着电机温度上升，电机响应扭矩线性降低。

2）二级过温：电机响应扭矩为 0。

3）三级过温：根据当前转速信息进入关管封脉冲或者主动短路的处理策略，当转速降低到一定值时，主动短路可以退出并进入关管状态。

#### 5.6.4.13 驱动电机控制器过温保护

故障描述：控制器温度检测高于过温阈值。

故障保护策略：

1）一级过温：随着电机控制器温度上升，电机响应扭矩线性降低。

2）二级过温：电机响应扭矩为 0.

3）三级过温：根据当前转速信息进入关管封脉冲或者主动短路的处理策略，当转速降低到一定值时，主动短路可以退出并进入关管状态。

#### 5.6.4.14 驱动电机控制器低压欠压

故障描述：当检测到电机控制器低压欠压时，报出故障。

故障保护策略：根据当前转速信息进入关管封脉冲或者主动短路的处理策略，当转速降低到一定值时，主动短路可以退出并进入关管状态。

#### 5.6.4.15 旋变故障

故障描述：

1）SIN/COS 超出范围（幅值超限）(DOS)；

2）EX 短路、开路，EX 的相位和 SIN/COS 相位超范围（LOT)；

3）SIN/COS 短路、开路（LOS)；

4）SIN/COS 正弦度不好（DOS)；

5）SIN/COS 大小波（包络幅值周期性变化）(DOS)。

故障处理策略：进行故障计数，同时，偏差在正常范围内，故障计数值需要减少。根据故障计数值达到不同阈值进行分级处理，故障分级阈值可以进行标定。

1）1 级故障进行降额处理，降额系数可标定，如果计数值小于故障阈值表示此故障可以进行恢复，取消降额保护。

2）3 级故障根据当前转速信息进行关管封脉冲或者主动短路处理，当转速降低到一定转速时，主动短路应当退出进入关管状态。

#### 5.6.4.16 位置信息检测异常

故障描述：电机在转矩控制过程中，不管是根据外部解码芯片得到的位置信息，还是 MCU 本身自带的软件解码功能得到的位置信息，都建议与估算转子位置进行二次校验。保证转子位置信息的正确性。

故障处理策略：当检测到转子位置偏差较大时，根据当前转速选择策略，需要切换无位置传感器控制算法并降低扭矩输出还是进入三相短路保护状态。

#### 5.6.4.17 驱动电机超速

故障描述：当检测到电机转速超过超速阈值时，报出故障。

故障保护策略：

1）一级超速：随着电机转速上升，电机响应扭矩线性降低。

2）二级超速：电机响应扭矩为 0。

3）三级超速：三相短路当转速降低到一定转速时，主动短路应当退出进入关管状态。

#### 5.6.4.18 12V/24V 供电丢失或者异常

故障描述：

1）无供电、毛刺、震荡、偏移；

2）过压；

3）欠压。

故障处理策略：芯片检测到供电异常切入备用 12V/24V 电源，如果没有备用电源则考虑延迟下电来进行降额停机处理。

#### 5.6.4.19 PWM 输出异常

故障描述：

1）常开；

2）缺相（无输出）；

3）频率漂移；

4）占空比漂移；

5）上升下降沿漂移。

故障处理策略：根据当前转速信息进行关管封脉冲或者主动短路处理，当转速降低到一定转速时，主动短路应当退出进入关管状态。

#### 5.6.4.20 IGBT 功率输出模块异常

故障描述：

1）短路；

2）过压（母线电压主接触器断开、集成电感过大）；

3）过流（负载过大导致过流）；

4）开路。

故障处理策略：根据当前转速信息进行关管封脉冲或者主动短路处理，当转速降低到一定转速时，主动短路应当退出进入关管状态。

#### 5.6.4.21 IGBT 节温过高

故障描述：IGBT 借助控制器损耗等信息进行节温估算，当超过一定阈值时，进行故障处理。

故障处理策略：

1）一级过温：随着电机控制器温度上升，电机响应扭矩线性降低。

2）二级过温：电机响应扭矩为 0。

3）三级过温：根据当前转速信息进入关管封脉冲或者主动短路的处理策略，当转速降低到一定值时，主动短路可以退出并进入关管状态。

## 5.7 电驱动总成功能安全

功能安全主要作用：当危害影响发生时，让电子电气系统进入一个安全状态并保持一个安全状态。包含两方面：系统失效（比如：错误系统设计）和随机硬件故障（比如电子电气元件老化）。其目的是使技术无法避免但又必须处理的危害最小化。

本指南修改遵循 ISO 26262，适用于道路车辆上由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。

1）提供了一个汽车安全生命周期(管理、开发、生产、运行、 服务、报废)，并支持在这些生命周期阶段内对必要活动的剪裁；

2）提供了一种汽车特定的基于风险的分析方法以确定汽车安全完整性等级（ASIL）；

3）应用汽车安全完整性等级（ASIL）定义-本指南适用的要求，以避免不合理的残余风险；

4）提供了对于确认和认可措施的要求，以确保达到一个充分、可接受的安全等级；

5）提供了与供应商相关的要求。

功能安全受开发过程(例如，包括需求规范、设计、实现、集成、验证、认可和配置)、生产过程、 服务过程和管理过程的影响。安全问题与常规的以功能为导向和以质量为导向的开发活动及工作成果相互关联。本指南涉及与安全相关的开发活动和工作成果。

本指南适用于安装在量产乘用车上的包含一个或多个电子电气系统的与安全相关的系统。

功能安全通常由整车厂提出安全目标，电驱动总成配套企业设计并实施功能安全方

案。不同的整车厂、电驱动总成企业在功能安全的要求和实施方案上存在差异。下面所述仅是一个指导性示例，无需严格遵照执行。

### 5.7.1 功能安全管理

#### 5.7.1.1 安全文化的定义

概要：组织创设安全文化，支持功能安全的实现。以此，建立并维护组织的规则和管理流程。

要求：

1）支持功能安全活动的企业文化的培养。

2）遵循功能安全标准的原则。

3）功能安全相关的问题的分析，评估，可追溯性。

4）执行功能安全相关的活动和文件管理规定。

5）遵循流程的建立、执行和维护方针。

6）确保赋予功能安全相关的管理人员适当的权限。

#### 5.7.1.2 安全活动相关的人才管理

概要：确保实施安全活动人员的能力，对于项目进行人才的分配及培养的支持。

要求：人员技能、权限的规定。

1）安全相关的设计和验证的能力。

2）相关审核评估的能力。

3）SO26262 及其他安全标准的知识。

4）公司内部规定。

5）领域知识。

6）管理能力。

#### 5.7.1.3 安全生命周期中的质量管理

概要：建立和管理 ISO/TS 16949 及 ISO 9001 的质量管理标准或与之等同的质量管理体系。

要求：公司内部的质量管理规定。

明确描述质量管理和功能安全的关联。

#### 5.7.1.4 功能安全管理的分工和责任

概要：任命具有权限、责任的安全管理者。

#### 5.7.1.5 功能安全活动的计划和调整

概要：制定安全计划，进行批准和认可评审，并进行维护、管理。

#### 5.7.1.6 功能安全生命周期的进程

参考：ISO 26262-1 Figure 1 — Overview of ISO 26262。

#### 5.7.1.7 安全档案的管理

制定认可措施计划，按照独立性和权限实施，认可措施安全所要求的独立性实施，执行认可措施的人员能够接触组织机构、必要的产品项目信息及工具。

#### 5.7.1.8 量产后的功能安全管理

安全完整性：安全功能是否能连续正常工作 15 年，是否能及时检测出系统错误（例如：危害产生影响之前）。

完整性：是否考虑了各个方面，是否所有的详细信息都被理解性地收集和保存。

文档：是否所有的细节都得到了证明，即使在以后（产品生命周期 15 年）。

#### 5.7.1.9 SOP 后的量产管理

组织应指定相关人员的责任和为生产发布后保持该项目的功能安全相关法律提供依据。

生产后释放的规范应保证项目功能安全的活动。

### 5.7.2 功能安全概念设计阶段

#### 5.7.2.1 相关项定义

目的：第一个目的是定义相关项即电机控制系统，与其环境和其它相关项的依赖性和相互影响。第二个目的是为充分理解相关项即电机控制系统提供支持，以便执行后续阶段的活动。

要求：相关项的功能要求、非功能要求及环境依赖性的确认。

定义相关项的边界、接口以及提出与其他相关项和要素的交互关系。

相关项的定义：功能列表、使用环境要求、法律法规要求、已知安全要求、功能框图、功能框图的边界。

#### 5.7.2.2 结构

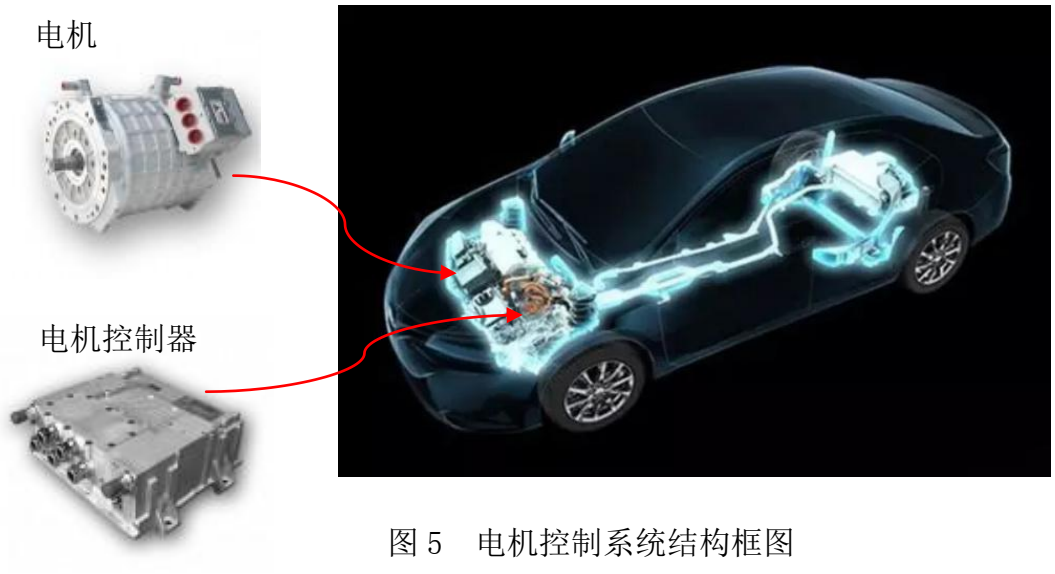



图 5　电机控制系统结构框图

电机控制系统包括如下组件：

电机控制单元；

电机控制执行机构。

#### 5.7.2.3 功能

电机控制系统应基于当前车辆状态和路况提供以下功能：

(功能安全边界定义的时候这里不考虑电机)

表 4　电机控制器功能

| 控制单元 | 功能 |
| --- | --- |
| 电机控制器 | 转矩控制<br>转速控制<br>其他控制（如母线电压控制、换挡控制等）<br>与整车通信<br>其他功能 |

表 5　电机控制器详细功能

| 功能描述 | 子功能 |
| --- | --- |
| 基本功能 | 转矩控制 |
| | 转速控制 |
| | 转矩安全故障保护 |

| | |
|---|---|
| | 高压安全故障保护（主动放电/被动放电/高压互锁等） |
| | 电流类故障保护（过流，硬件/软件分级） |
| | 电压类故障保护（过压/欠压/电压不合理（分高压和低压和芯片供电，分电动和发电），硬件，软件分级） |
| | 速度类故障保护（过速） |
| | 温度类故障保护（过温，硬件/软件分级） |
| | 传感器类故障保护（所有传感器的故障，包括且不限于对供电短路/对地短路/信号超限/信号不合理等） |
| | 通信类故障保护（CAN 通信，SPI 通信，LIN 通信等） |
| | 芯片类故障保护（芯片看门狗，时钟，时序，内存等） |
| | 电机本体类故障保护（缺相，匝间短路等） |
| | 连接可靠性类故障保护（三相接反等） |
| | 其他功能故障保护（自学习功能，防溜坡，主动阻尼等） |
| | 其他故障保护 |
| 其他功能 | 软件加密 |
| | OTA（*Over—the—Air* Technology） |

#### 5.7.2.4 非功能要求

1）直流母线电压范围；

2）工作环境温度范围（℃）；

3）进出水口间压差；

4）冷却方式；

5）冷却水入口温度；

6）水冷流量；

7）辅助电源或其他方式可保证系统处于安全状态；

8）需要进行有效的防水防尘措施；

9）电机控制器绝缘电阻应满足安规标准；

10）MCU 应满足 IP67 或更高等级的防护要求；

11）驱动电机系统在运行中所产生的电磁辐射干扰应符合相关国家标准和产品技术文件规定；

12）驱动电机系统电磁辐射抗干扰性应符合相关国家标准和产品技术文件规定。

#### 5.7.2.5 安全生命周期的启动

有了相关项定义之后，就要确定项目的安全生命周期，对项目的安全生命周期进行初始化，也就是开始对项目的安全生命周期进行细化。而要进行细化，就要区分项目是新产品研发还是既有产品的改造。如果是全新的设备研发，则相关工作就得从安全生命周期的开始做起。如果是既有产品的改造，那么从项目定义开始的这些流程都可以使用一些既有的文件对整个过程进行定制。现有产品升级改造，就要注意以下一些问题：

1）要做产品和使用环境的分析，以制定出预期更改，并评估这些更改产生的影响。

a）对项目的更改包括设计更改和执行更改。设计更改应该是由需求规范、功 能和性能的增加或者成本的优化所致，执行更改不能影响项目的规格和性能，但可以影响执行特征。执行更改可以由软故障更改，使用新的研发成果或生产工具所致。

b）如果配置数据和校准数据的更改会影响到产品的行为，则更改须考虑这些 数据。

c）对产品环境的更改应该是由产品要使用的新的目标环境或由于其他相关产 品或元素升级而引发。

2）要表述清楚产品使用的前后条件的差别，包括：

a）操作条件和操作模式；

b）环境接口；

c）安装特征，如：在车辆内部的位置，车辆的配置和变化等；

d）环境条件的范围，如：温度，海拔，湿度，震动，EMC 和汽油标号等。

1）要明确给出产品变更的描述以及影响的范围。如果不能明确产品的变更和对环境数据影响的改变，则相关影响的分析数据都要进行记录。

2）影响到的服役产品，需要进行升级的，要进行逐一列出。

3）定制的相关安全活动应符合各个应用生命周期阶段的要求，包括：

a）定制应基于影响分析的结果。

b）定制的结果应包括在符合 ISO26262-2 的安全计划中。

c）影响到的产品须返工，包括确认计划和验证计划。

确定了以上这些基本信息之后，对所要进行的产品研发或者设备更改工作就有了一个清晰明确的定义，对产品的预期使用功能、环境，以及与相关设备的接口也有了一个明确的定义，接下来就可以进行危险分析和风险评估了。

#### 5.7.2.6 危害分析和风险评估

危险分析和风险评估的目的和之前的 ISO13849,IEC62061 等的标准一样，都是为了

将设备存在的危险识别出来，并根据危险的程度按照一定的原则对其进行分类，从而针对不同的风险设定具体的安全目标，并最终减小或消除风险，避免未知风险的发生。

状况分析：故障行为记述了成为危害事件的运行状况及运行模式。

危害识别：在整车层面可以观测的状态或行为来定义危害。

通过 FTA（故障树分析）进行危害事件的提出危害分析与风险评估的目的是识别相关项中因故障而引起的危害并对危害进行归类，制定相应的安全目标，以避免不合理的风险。其中，应基于相关项的功能行为，来分析其潜在的危害事件。再从危害时间的严重程度、暴露概率、可控性三个方面对相关项进行系统性的评估，从而确定安全目标及相应的 ASIL 等级。概要：在整车层面通过运行场景和运行模式的组合来描述危害事件，通过组合各危害事件，来识别事件结果。

### 5.7.2.7 ASIL 等级定义

概要：对于每个危害事件，通过严重度/暴露概率/可控性的评估矩阵来定义 ASIL 等级

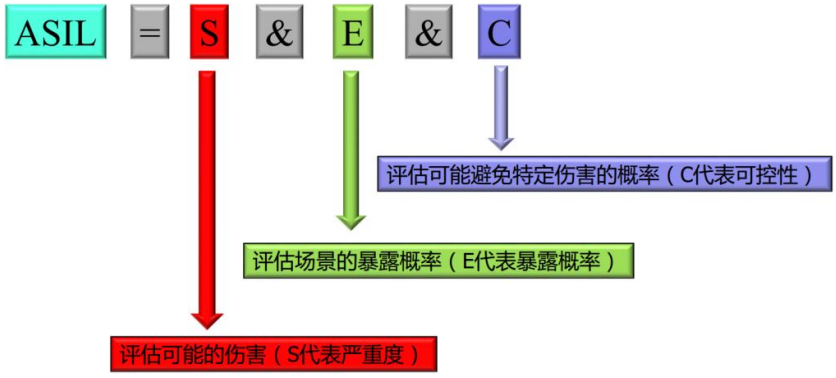



图 6　ASIL 等级定义

表 6　严重度/暴露概率/可控性的评估矩阵

| | | C1 | C2 | C3 |
|---|---|---|---|---|
| S1 | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | A |
| | E4 | QM | A | B |
| S2 | E1 | QM | QM | QM |
| | E2 | QM | QM | A |
| | E3 | QM | A | B |
| | E4 | A | B | C |
| S3 | E1 | QM | QM | A |
| | E2 | QM | A | B |
| | E3 | A | B | C |
| | E4 | B | C | D |

### 5.7.2.8 安全目标

概要：对于有 ASIL 等级的危害事件，定义它相应的安全目标。

要求：对每个危害实施危害分析和风险评估，定义其 ASIL 等级，设立安全目标。

功能安全目标还可以包含高压电击和电池起火等，取决于主机厂要求，但这里不展开。

表 7　功能安全目标

| 序号 | ID | 安全目标 | FTTI | ASIL | 安全状态 |
|---|---|---|---|---|---|
| 1 | SG-01 | 避免非预期的扭矩增加 | -ms（FTTI 故障容错时间间隔的设置要考虑系统和软件的具体情况） | C(视具体分析情况打分) | 报警提示，并关闭 PWM 或者进入三相短路状态由状态机进行逻辑判断 |
| 2 | SG-02 | 避免非预期的扭矩反向 | -ms | | 报警提示，并关闭 PWM 或者进入三相短路状态由状态机进行逻辑判断 |
| 3 | SG-03 | 避免非预期的扭矩快速震荡 | -ms | | 报警提示，并关闭 PWM 或者进入三相短路状态由状态机进行逻辑判断 |
| 4 | SG-04 | 避免非预期的扭矩丢失 | -ms | | 报警提示，并关闭 PWM 或者进入三相短路状态由状态机进行逻辑判断报警提示，并关闭 PWM |

### 5.7.2.9 功能安全概念

功能安全概念阶段的主要目的是通过前面的危险分析和风险评估之后得出的安全目标来确定具体的功能安全要求，并将它们分配到初步的设计架构，或者外部减少危险的措施当中去，以确保满足相关的功能安全要求。

安全概念主要是为了从安全目标中得出功能安全要求，并将其分配给相关项的架构要素或外部措施。制定功能安全要求时，应从相关项的运行模式、故障容错时间间隔、安全状态、紧急运行时间间隔及功能冗余等方面进行考虑，同时可以使用安全分析（例如 FMEA、FTA、HAZOP）的方法 ，使制定的功能安全要求更加完善。安全概念还应按照 GB/T34590.9 中的要求进行验证，表明与安全目标的一致性和符合性，即减轻或避免危害事件的能力。

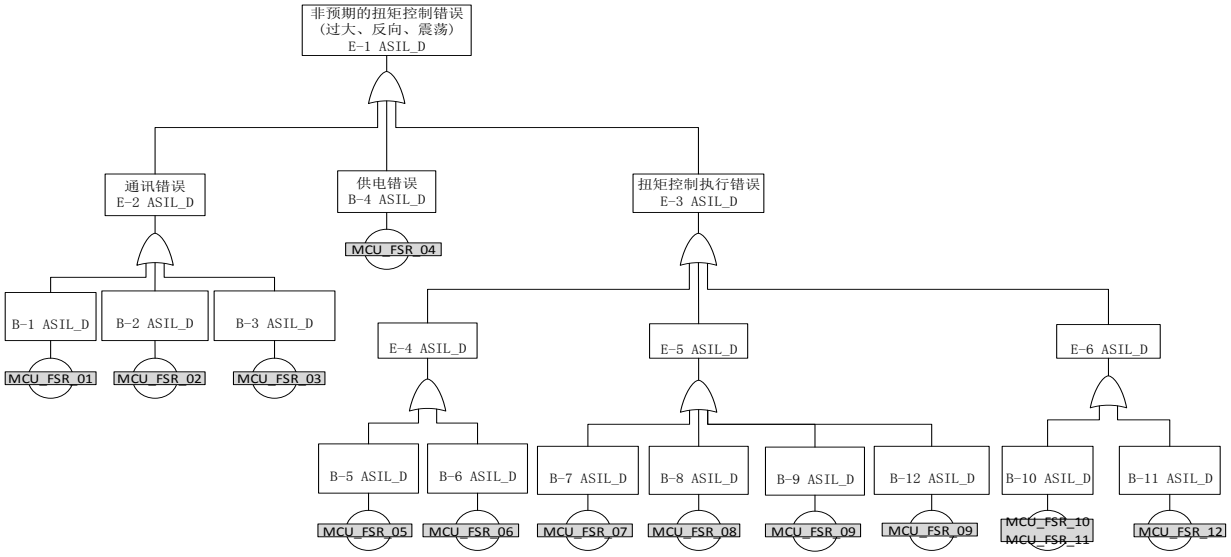



图 7　FSR 对应的 FTA 分析

#### 5.7.2.10 功能安全需求分配

功能安全需求分配到要素需要考虑以下几点：

1）基于相关项初期架构的要素

2）继承：ASIL 和功能安全需求信息

以下情况接受最高 ASIL 等级

若下一功能安全需求被分配到了相同的架构要素中。

若相关项包含多个系统，那么导出独立系统和他们的接口的功能安全需求

如果独立冗余：可以进行 ASIL 分配

另外，如果 ASIL 等级需要被拆解，则要符合 ISO26262-9 第五条款的要求。

### 5.7.3 功能安全的系统阶段

#### 5.7.3.1 启动系统层面产品开发

进行正式系统开发前，应基于 GB/T34590.4 相关规定，指定系统层面产品开发的安全活动计划，包括确定设计和集成过程中适当的方法和措施、测试及验证计划、功能安全评估计划等。

系统级产品开发启动的目标是确定和规划在系统开发各个子阶段的功能安全活动。这部分内容在 ISO26262-8 中也有描述。系统级安全活动包含在安全计划中。

#### 5.7.3.2 技术安全需求设计

技术安全要求是实现功能安全概念必要的技术要求，目的是将相关项层面的功能安全要求细化到系统层面的技术安全要求。应基于 GB/T34590.4 相关规定， 根据功能安全概

念、相关项的初步架构设想、外部接口、限制条件等系统特性来制定技术安全要求。技术安全要求应从故障探测/指示/控制措施、安全状态、故障容错时间间隔等方面考虑，定义必要的安全机制。

根据用于开发 FSR 和初步体系结构的“输入-过程处理-输出”（I-P-O）模型，确定输入、处理、输出的 TSR。

下面举几个例来说明：

表 8　输入中的技术安全需求

| Req. ID | TSR | ASIL | 导出源 | 对应的安全机制 | FTTI |
|---|---|---|---|---|---|
| | MCU通过AD检测12V输入电压。是否在合理范围内，如果超出范围则不响应开管指令。 | C | 对应的FSR功能安全需求 | 对应软硬件去分解 | 1ms |

表 9　处理过程的技术安全需求

| Req. ID | TSR | ASIL | 导出源 | 对应的安全机制 | FTTI |
|---|---|---|---|---|---|
| | MCU监控电机实际三相电流值：当三相电流之和大于20A（tbd）的时候，认为电流传感器采样有问题，进入故障状态；当三相电流和处于0~20A的时候，认为是正常的采样误差，不做处理。 | C | 对应的FSR功能安全需求 | 对应软硬件去分解 | 20ms |

表 10　输出的技术安全需求

| Req. ID | TSR | ASIL | 导出源 | 对应的安全机制 | FTTI |
|---|---|---|---|---|---|
| | PWM输出模块电路硬件冗余（例如双核锁步、非对称冗余、编码处理），利用芯片的双核锁步机制来保证PWM输出。处理单元以锁步（或以固定的延迟运行）方式运行两次并将结果进行比较。任何不匹配会导致错误状态，并通常导致复位。这里只是举例不限制任何芯片类型。 | C | 对应的FSR功能安全需求 | 对应软硬件去分解 | 20ms |

#### 5.7.3.3 制定安全机制

基于技术安全要求，制定安全机制：提出需要展开的技术安全需求。例：进一步展开技术安全需求，并分配容错事件间隔要求。

安全机制的讨论：基于技术安全要求及系统设计架构，讨论为了实现其功能运行的机

制。例：角度检测功能，基于要素及极限值进行讨论，需要在何处进行检测。

为使项目达到或维持一个安全状态的安全机制应规定：

1）安全状态的切换；

2）容错的时间间隔；

3）如果安全状态不能立即达到，应确定应急操作的时间间隔；

4）维持安全状态的措施。

ASIL 分解按照 ISO26262-9:2011，第 5 条款。

#### 5.7.3.4 系统设计

系统设计应基于功能概念、相关项的初步架构设想和技术安全要求。在实现技术安全要求相关的内容时， 应从验证系统设计的能力、软硬件设计的技术能力、执行系统测试的能力等方面考虑系统设计。为避免系统性失效， 应对系统设计进行安全分析以识别系统性失效的原因和系统性故障的影响。为降低系统运行过程中随机硬件失效造成的影响，应在系统设计中定义探测、控制或减轻随机硬件失效的措施。系统设计中定义软硬件接口规范， 并在后续硬件开发和软件开发过程中进行细化。

参考：ISO 26262-4 table2 properties of modular system design

为了避免失效造成的高复杂性，架构设计需要通过以下原则进行：

1）模块化；

2）适当的粒度级别；

3）简单性。

#### 5.7.3.5 导出技术安全概念

目的：基于系统设计的结果，将技术安全要求分配硬件、软件。

概要：由功能安全需求导出技术安全需求，进行系统设计，导出技术安全概念。

1）系统设计的可验证性；

2）软件硬件的技术实现性；

3）系统集成中的执行测试能力。

#### 5.7.3.6 实施安全分析

基于系统设计架构及技术安全概念的结果，采用 FTA 及 FMEA 方法进行安全分析。

#### 5.7.3.7 系统设计验证

参考：ISO 26262-4 Table 3 — System design verification。

#### 5.7.3.8 系统集成与测试

基于 GB/T 34590.4 相关规定，分别进行软硬件、系统、整车层级的集成和测试，验证每一条功能和技术安全要求是否满足规范，以及系统设计在整个相关项上是否得到正确实施。

集成和测试阶段包括三个阶段和两个主要目标如下所述：第一阶段为每个项目包含的元件的硬件和软件的集成。第二阶段是一个项目的元件的集成以形成一个完整的系统。第三阶段是项目与车辆的周围系统的集成。

集成过程的第一个目标是根据 ASIL 等级和安全需求规范测试符合各项安全要求。第二个目的是验证“系统设计”覆盖的安全要求正确地由整个项实施。项目元件的集成是从软件硬件集成，系统集成到整车集成系统。 集成测试会在每个阶段的执行来证明系统元件正确交互。根据 ISO26262-5 和 ISO26262-6 完成硬件和软件的开发，然后按照第 8 条款（项目集成和测试）开始进行系统集成。

#### 5.7.3.9 集成与测试的计划和定义

测试项目的导出方法

参考参考：ISO 26262-4 Table 4 —Methods for deriving test cases for integration testing

### 5.7.4 功能安全硬件设计阶段

基于 GB/T 34590-5 相关规定，将技术安全概念，技术安全要求和系统设计说明落实到硬件层级，设计完整且详细的硬件安全要求。

为保证硬件安全要求的完整性，在设计时应考虑包含以下内容：

1）安全机制及其属性；

2）验证的标准；

3）硬件度量的目标值；

4）FTTI；

5）其它与安全相关的要求。

为保证硬件安全要求的质量，应按照 GB/T34590-8 中第 6 章的要求进行硬件安全要求的设计、验证和管理。

为使硬件被软件正确地控制和使用，应对软硬件接口（HSI）进行充分的细化，并描述出硬件和软件之间的每一项安全相关的关联性。

#### 5.7.4.1 启动硬件层面产品开发

概要：基于安全计划和项目计划，定义并更新系统层面的安全活动计划。

计划产品开发中硬件元件的活动（包括支持过程）。

在设计过程中应使用适当的方法和措施。

硬件开发过程中应兼顾系统和软件的生命周期。

#### 5.7.4.2 硬件安全需求规范

硬件安全需求规范：硬件安全要求应来源于技术安全概念和系统设计规范：

1）详细的硬件-软件接口（HSI）要求。

2）所有与安全相关的硬件要求必须以硬件安全要求的形式出现。

3）故障对来自外部干扰的容忍（例如：开放式输入）。

4）安全机制用来检测和修复内部（例如：组件失效）和外部（控制失效）失效。

5）安全机制用来修复暂时性和永久性失效。

6）硬件指标的目标值。

#### 5.7.4.3 硬件架构设计

设计原则：

1）分层设计

2）避免不必要的接口复杂化

3）避免不必要的硬件组件复杂化（简单设计）

4）可维护性

5）可测试性

基于 GB/T 34590-5 相关规定，进行硬件架构设计和硬件详细设计，并进行硬件安全分析，以满足系统设计说明和硬件安全需求的要求。

为避免硬件的系统性风险，一般应进行硬件架构设计，然后进行硬件详细设计。在硬件架构设计时，应确保每个硬件组件继承了正确的 ASIL 等级，并可追溯到与之相关的硬件安全要求。

#### 5.7.4.4 硬件详细设计

在硬件设计时，应运用相关的经验总结，并考虑安全相关硬件组件失效的非功能性原因，如果适用，可包含以下因素：温度，振动，水，灰尘，EMI，来自硬件架构的其他组件或其所在环境的串扰。

为提高设计的可靠性，应遵循 GB/T 34590-5 中的“模块化的硬件设计原则”和 “鲁棒性设计原则”，如降额设计、最坏情况分析等。

为识别硬件失效的原因和故障的影响，应按 GB/T 34590-5 中的要求，根据不同的

ASIL 等级，使用“演绎分析”（如 FTA）或“归纳分析”（如 FMEA）的方法进行安全分析。

如果安全分析表明生产、运行、服务和报废与安全相关，则应定义其与安全相关的特殊特性并输出说明性文件。为验证硬件设计与硬件安全要求的一致性和完整性，应按 GB/T 34590-5 中的要求，对硬件设计进行验证。

#### 5.7.4.5 硬件设计-安全分析

识别失效的原因和故障的影响；

针对所考虑的安全目标，进行安全分析识别；

避免单点故障的有效性的证据；

避免潜伏故障的有效性的证据；

确定硬件设计的独立性；

如引入新危害，重新进行危害分析和风险评估。

#### 5.7.4.6 硬件设计-组件的鉴定

基于 GB/T 34590-8 相关规定，对其中复杂的硬件组件及元器件应进行硬件组件的鉴定，确保硬件组件合规使用并为 FMEDA 分析提供基础数据。

#### 5.7.4.7 硬件架构度量的评估

基于 GB/T 34590-5 相关规定，进行硬件架构度量的评估，并将评估结果和优化建议反馈到系统设计、硬件设计、软件设计环节，以优化产品设计，使最终的“单点故障度量”和“潜伏故障度量”满足对应 ASIL 的要求。

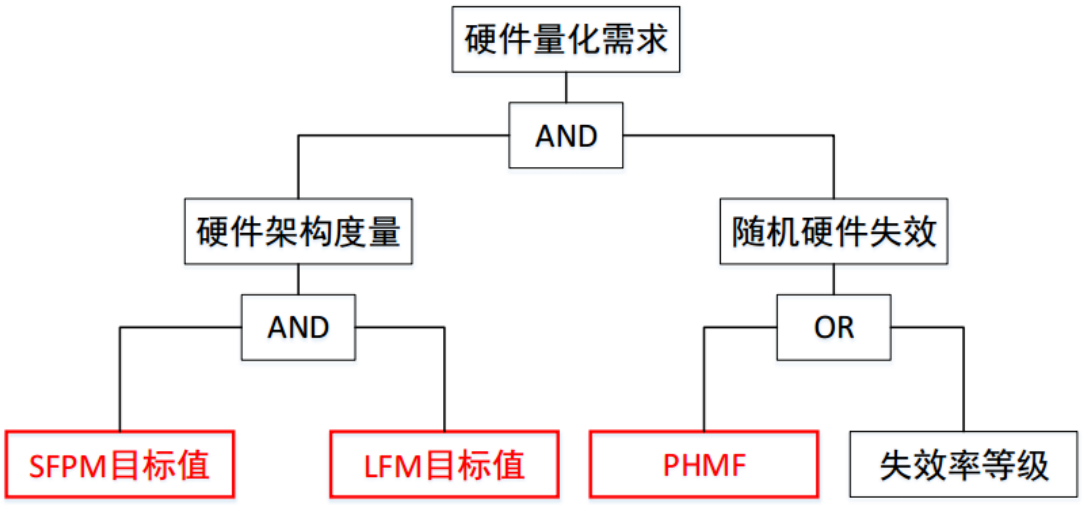



图 8　硬件量化需求

表 11　故障指标的评估

| | ASIL B | ASIL C | ASIL D |
|---|---|---|---|
| 单点故障指标 | ≥90% | ≥97% | ≥99% |
| 潜在故障指标 | ≥60% | ≥80% | ≥90% |

#### 5.7.4.7.1 硬件诊断覆盖率

参考 ISO26262-5。

#### 5.7.4.7.2 失效模式分类

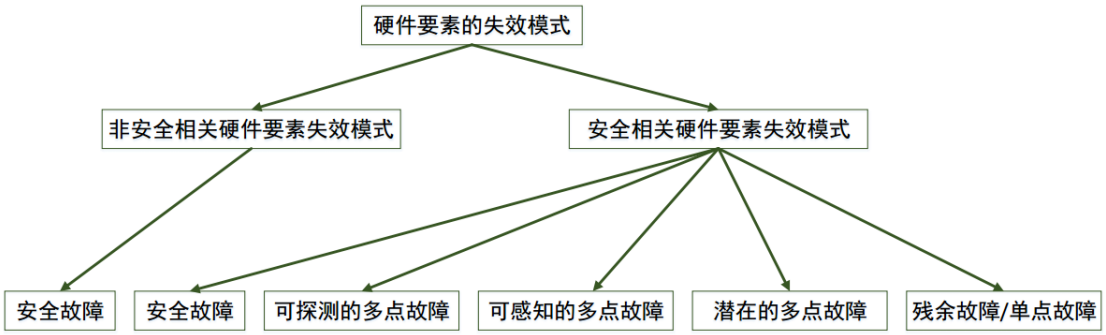



图 9　硬件失效模式分析

#### 5.7.4.7.3 随机硬件失效导致违背安全目标的评估

由于随机硬件失效而违背安全目标的目标值基于 GB/T 34590-5 相关规定，进行 PMHF 评估或割集分析评估，优化使相关安全目标没有由于随机硬件失效带来的不可接受的风险。

### 5.7.4.8 硬件集成和测试

基于 GB/T 34590-5 相关规定，进行硬件集成和测试，通过测试确保所开发的硬件符合硬件安全要求。硬件集成测试用例的生成应考虑 GB/T 34590-5 的表 10 中所列的方法。

为了验证安全机制的完整性和正确性，硬件集成测试应考虑以下方法：功能测试、故障注入测试和电气测试。为了验证硬件在外部应力下的鲁棒性，硬件集成测试应考虑 GB/T 34590-的表 12 中所列方法。

## 5.7.5 功能安全软件设计阶段

### 5.7.5.1 启动软件层面的产品开发

编写启动计划内容

1）启动软件开发活动的适当方法；

2）软件开发的剪裁；

3）配置软件开发；

4）软件生命周期的一致性；

5）方法、相应工具的选择；

6）选择适当的建模和编程语言；

7）设计和编码指南。

#### 5.7.5.2 软件安全需求规范

软件安全需求分析目的是依据安全技术规范以及系统设计说明书制定软件安全需求，同时验证软件安全需求与安全技术规范及系统设计说明书是否一致。

软件安全需求分析阶段需满足完整性、可测试性、可追溯性要求。

软件安全需求分析时，应从如下方面考虑：充分识别失效会违反安全技术要求的软件功能；需来源于安全技术要求和系统设计方案；应识别软件与硬件之间所有安全相关的属性；包含足够的硬件运行资源，有效的安全相关等信息的确认；软硬件接口说明书应是确认有效的；测试验证方法应是安全有效的。

#### 5.7.5.3 软件架构设计

软件安全监控架构设计目的在于开发一个可以满足并实现软件安全需求的软件架构。软件安全监控架构设计需结合功能安全相关软件需求和非功能安全相关软件需求，全局考虑软件的架构设计，并进行软件安全分析。

软件安全监控架构设计时，应从如下方面考虑：应该是可配置、可实施、易于测试和可维护的；需遵循模块化、高类聚、低耦合、低复杂度的要求；应细化到足够支持详细设计；应具备静态和动态特性；应满足独立性的要求；应覆盖软件安全需求等。

##### 5.7.5.3.1 软件架构设计原则

参考 ISO26262 Table 3 — Principles for software architectural design

1）软件架构设计应开发到软件单元层级，即不可再分级别。

2）软件架构应描述软件单元的静态设计。

3）静态设计：

a）软件结构包含它的等级；

b）数据处理的逻辑顺序；

c）数据类型和他们的特性；

d）软件元件之间的接口；

e）外部与软件之间的接口；

f）架构和外部不见部件的约束。

4）若基于模型开发，模型结构是固有的。

5）软件组件的动态设计：

a）功能和行为；

b）软件组件之间的数据流；

c）外部接口的数据流；

d）时间约束条件；

e）控制流和进程的并发性。

#### 5.7.5.3.2 软件架构设计安全分析

目的：

1）明确顺序和故障响应

2）推荐测试用例

3）识别软件故障规避策略

4）安全机制的效果展示。例如：诊断，控制硬件故障的恢复，为了解决系统失效机制。

5）评估资源使用和分配

验证方法：

参考 ISO26262-5 Table 6 — Methods for the verification of the software architectural design

### 5.7.5.4 软件单元设计和实现

软件详细设计时，应从如下方面考虑：应包含足够的必要信息以便于后续活动开展；应详细描述其功能特征；应满足可测性、可维护、低复杂度、可读性和健壮性等要求；详细设计应满足与软件安全需求、软件架构、编码准则、详细设计说明书等一致性的要求。

软件单元设计原则参考 ISO26262-Table 8 — Design principles for software unit design and implementation

### 5.7.5.5 软件安全算法测试

软件算法测试用于证明软件单元模块符合软件详细设计说明书要求，该要求包括：软件功能要求的符合性，接口要求的一致性，算法的健壮与高效等。软件算法测试案例设计

时，需按照软件详细设计说明书、软件失效分析报告要求，采用需求分析、等价类划分、边界值分析、错误猜想、故障注入等方法。

软件算法测试活动，要做好详细设计、失效分析报告、测试案例、测试数据、测试缺陷的双向可追溯性与过程的完整性。软件算法测试同时还需要度量验证软件算法质量，包括单元覆盖度（如：语句覆盖度，分支覆盖度，修正判定条件覆盖度等），代码编码规则，以及其他静态度量指标（如：圈复杂度等），具体请参见 GB/T34590-6 相关要求。

#### 5.7.5.6 软件集成与架构符合性测试

软件集成与架构符合性测试主要用于验证软件组件集成功能以及软件组建之间的接口是否符合软件架构设计文档要求。

软件集成通常可分为增殖式集成与一次性集成。不同的集成方式，对应的集成测试策略也不同。常用到的测试方法包括：基于需求的测试，接口测试，故障注入测试，资源占用测试以及模型与代码的背靠背测试。

软件集成测试也包含质量度量过程， 主要度量指标包括功能覆盖度和函数调用覆盖度。

参考 ISO26262-5Table 10 — Methods for software unit testing

#### 5.7.5.7 软件安全需求验证

软件安全需求验证的目的在于确保软件在目标硬件环境上能够正确实现软件安全需求。通常需采用验证方法包括硬件在环测试、电子电气试验台架测试以及实车测试等。软件安全需求验证不但要从功能角度验证软件安全需求的符合情况，还要从性能角度验证是否满足性能要求（如：程序安装测试、负载测试、软件安全需求覆盖度等）。

## 5.8 售后维护保养安全

电驱动系统维护保养人员要求：

在对电驱动系统进行维护保养之前，应对维护保养人员进行专业培训，需取得电工上岗证、维修电工资格证书的人员进行维护保养作业。作业时必须断开电机控制器高压电源，做好安全防护，确保维护保养人员知晓安全注意事项，熟悉所使用的测量设备、工具，熟悉操作要求。

### 5.8.1 电机控制器保养要求

#### 5.8.1.1 维护场所、环境要求

电机控制器维护保养时，应避免在有沙尘、雨雪等气象条件下进行露天操作，如条件

限制不得不在上述气象条件下进行维护时，应作适当防护，避免沙尘、水或其它杂质进入电机控制器系统内部。环境达不到要求时，不允许进行拆解维保。

#### 5.8.1.2 工具要求

使用专业检测检修设备和绝缘工具。比如；绝缘工具、绝缘钩、绝缘表、绝缘手套、护目镜、防静电服等。

#### 5.8.1.3 安全要求

由于存在高压触电危险（不同车型，电压值不同），作业时需按要求佩戴绝缘手套，绝缘鞋。所有作业要求必须进行断电、放电及高压 DC+、DC-对地电压检查，确保不带电操作。

#### 5.8.1.4 电机控制器维修要求

检修前，对电机控制器行进断电、放电、安全检查:

1）检修前，拔掉高压检修开关，关闭低压电源总开关，用放电导线夹对 DC+、DC-端放电。

2）用万用表直流电压档测量高压 DC+、DC-对地电压≤36V，即可进行检修操作。

#### 5.8.1.5 环境安全管理要求

1）危险源说明：高压触电。

2）个人劳动防护用品佩戴要求：穿工作服、绝缘防砸鞋，戴绝缘手套。使用前必须检查绝缘手套是否有破损、破洞或裂纹等，应完好无损。不能带水进行操作，保证内外表面洁净、干燥，确保安全。在潮湿环境作业时，须先用电吹风将绝缘手套吹干 5 分钟。

3）安全操作要求：检修前，需拔掉高压检修开关，进行断电、放电及高压 DC+、DC-对地电压检查；所有作业不得带电作业，不得私自试车。检修时应设置醒目的维修警示标识，防止其他人员误操作（如启动车辆、上电等）造成人员伤害。

4）环境保护要求：作业过程中所产生的废弃物，按客户要求进行分类收集，并放置到指定场所。检修进水的电机驱动总成时要非常小心!对于怀疑进水的电驱动总成，检修前必须先进行绝缘电阻检测并严格执行整车下电操作。

### 5.8.2 驱动电机维修保养要求

#### 5.8.2.1 维护场所、环境要求

电机维护保养时，应避免在有沙尘、雨雪的气象条件下进行露天操作，如条件限制不得不在上述气象条件下进行维护时，应作适当防护，避免沙尘、水或其它杂质进入电机内部。环境达不到要求时，不允许进行拆解维保。

#### 5.8.2.2 工具要求

使用专业检测设备和绝缘工具。

#### 5.8.2.3 安全要求

由于存在高压触电危险（不同车型，电压值不同），作业时需按要求佩戴绝缘手套，绝缘鞋。以下所有操作，均应确保按作业要求进行断电、放电及高压 DC+、DC-对地电压检查，确保不带电操作。

#### 5.8.2.4 检修前安全检测

1）拔掉高压检修开关，关闭控制器低压电源总开关，并用放电导线夹对三相线（U、V、W)端进行放电。

2）用万用表检查三相线对地电压应≤36V，即可进行维护操作。

3）检查电机外观无损伤。

4）旋转电机输出轴，确认是否可以正常转动、无异响。

5）检查电机水冷系统循环是否正常，有无漏液现象。

#### 5.8.2.5 旋变线圈及温度传感器检测（以永磁同步电机，位置传感器是旋转变压器为例）

用万用表欧姆档,检查电机旋变线圈阻值及温度传感器阻值求：

1）余弦线圈阻值；

2）正弦线圈阻值；

3）励磁线圈阻值；

4）温度传感器电阻值。

需要注意的是：以上阻值会随环境温度变化、测量工具、检测人员等因素的影响，测量数值会有发生偏差。

#### 5.8.2.6 三相绕组检测

1）将电机接线盒打开，拆掉三相线，用万用表欧姆档测试电机三相线（U、V、W)之间的相间电阻阻值（应平衡且相等）。

2）用绝缘检测仪 500V 电压档测三相线（U、V、W)对外壳的绝缘电阻值，应符合各产品的技术要求（不同产品绝缘阻值差异较大，实测数据是否合格按照相应产品的技术要求）。

#### 5.8.2.7 环境安全管理要求

1）危险源说明：高压触电。

2）个人劳动防护用品佩戴要求：穿工作服，绝缘防砸鞋，戴绝缘手套。使用前必须

检查绝缘手套是否有破损、破洞或裂纹等，应完好无损。不能带水进行操作，保证内外表面洁净、干燥，确保安全。在潮湿环境作业时，须先用电吹风将绝缘手套吹干 5 分钟。

1）安全操作要求：检修前，需拔掉高压检修开关，进行断电、放电及高压 DC+、DC-对地电压检查；所有作业不得带电作业，不得私自试车。检修时应设置醒目的维修警示标识，防止其他人员误操作（如启动车辆、上电等）造成人员伤害。拖车时的注意事项：整体拖车或电机联动的轮抬起。

4）环境保护要求：作业过程中所产生的废弃物，按客户要求进行分类收集，并放置到指定场所。检修进水的电机驱动总成时要非常小心！对于怀疑进水的电驱动总成，检修前必须先进行绝缘电阻检测并严格执行整车下电操作。

### 5.8.3 变/减速器维修保养要求

1）拔掉高压检修开关，关闭控制器低压电源总开关，并用放电导线夹对三相线（U、V、W)端进行放电。

2）用万用表检查三相线对地电压应≤36V，即可进行维护操作。

3）检查变/减速器外观无损伤。

4）旋转变/减速器输出轴，确认是否可以正常转动、无异响。

5）检查变/减速器有无漏油现象。

### 5.8.4 发生危险后的应急处理

#### 5.8.4.1 触电救助方法

在电驱动总成拆装过程中，若操作人员不慎发生触电事故，应紧急按照以下方法救助。

1）救助的过程中首先确保施救者自身安全。

2）切勿直接接触触电人员。

3）使用不导电工具（绝缘钩、干燥木棒、扫帚等）使触电者迅速地脱离电源。

4）立即拨打 120 急救电话。

5）检查触电者的生命机能，如没有呼吸和脉搏，在医生到来前进行人工呼吸和心肺按压。

#### 5.8.4.2 电气火灾救助

1）自我保护！切勿吸入烟气。

2）向消防部门报警。

3）当消防人员到场后须告知火灾涉及的是新能源电驱总成。

4）需要的情况下，扑灭附近的火源，或者使用覆盖法确保安全。

应迅速疏散人群，远离故障件，确保人身安全。

# 6. 充电安全

电动汽车充电基础设施由供电系统、充电设备、监控系统以及计量系统等构成。供电系统由提供电源的电力设备及配电线路组成；充电设施由充电设备、充电线缆及相关装置组成；监控系统由计算机设备以及信息网络设备组成，对充电设备及供电设备及设施运行状况、环境、安全状况及数据资源进行监测和管理；充电设施是电动汽车不可或缺的电能补充设施，充电安全需从充电设施的全生命周期关注其安全性，包括：设计、制造、建设、信息传输与数据存储、以及运行服务保障，建立良好可靠的充电安全机制，抵御安全风险和事故发生。

## 6.1 充电安全机制

### 6.1.1 安全防范目标

组成充电应用系统的各部分硬件、软件、设计、建设及运行维护，其安全目标设定应以预防为主，保证人员不受伤害为前提，实现电动汽车充电应用的安全性，并且：

（1）使用人员安全：在各种环境工况下，充电设备、电动汽车及辅助设施，均应确保使用人员的人身安全；

（2）充电设备与系统：充电设备应具备相应标准规定的电气安全防护能力设计，同时应保证对电动汽车充电过程在各种失效模式下具备相应保护措施；

（3）供电安全：充电桩的负荷约束，过载保护，谐波参数、短路保护应不影响供电电源的正常工作；

（4）控制与保护：电动汽车在充电过程中应建立故障风险监测及相应保护控制措施，在故障模式下应具备安全事故不扩散的控制能力；

（5）运营安全：充电环境、场站操作、运行管理，应满足充电服务安全运行为基本要求的目的。

（6）安全防控：应建立全过程的安全防控机制，设计阶段应充分重视充电设备对安全相关标准技术要求的执行，充分运用功能保护设计有效减低系统功能失效安全风险，制造阶段应重视产品生产制造质量水平提升和产品检验、认证检测和入网管理，建设阶段应严格执行充电设施建设竣工质量要求，运营阶段应提高运行维护保障能力和安全管理水平。

### 6.1.2 健全充电保护机制

充电过程是车辆与充电系统协同配合并实现电能传递的过程，充电失控易引发动力电池的安全事故，应注重充电过程的安全风险管理。

（1）主动安全措施

充电设备的充电控制应充分考虑主动安全保护的功能设计，充电过程中需校验 BMS 数据，对电池的关键参数，如电池总压、单体电压、温度，以及 SOC、SOH 等信息进行实时监测，对充电控制模式与充电状态进行可行度校验，对异常状况具有实时监测、诊断、差错辨识及故障预测和预警控制能力，当发现可能导致超出安全风险严重等级时，应主动停止充电并启动维护措施。

（2）充电特性与保护

现行充电管理是由车辆 BMS 作为充电主控侧，充电设备为被控侧执行 BMS 充电指令，结合电动汽车及动力电池管理系统充电特性输出，易进一步优化充电模式及充电特性控制要求，通过数据交互及可信度判别，形成与充电特性安全边界相适配的保护机制。提倡对电池系统、充电系统应具备健康状况监测、诊断及设置故障预警功能，且当电池系统出现安全风险状况时具有相应的保护措施。同时，电动汽车监控平台应具备对电池系统安全风险评估功能，并与充电系统建立实时通信能力，形成充电安全冗余保护机制，通过充电过程数据以及历史充电信息分析给出当前条件下最优的充电电压和电流,并进行在线充电风险度辨识，防止出现过充、大电流冲击导致动力电池性能损伤，实现充电设备的多重安全保护设计，保证电池充电安全。

（3）功能失效风险

组成充电系统的软硬件系统、功能组件，其耐久性、可靠性及环境因素影响致使性能衰退，电磁干扰产生通信差错，易导致充电过程中出现管理功能失效，电能传递偏离预期要求，由此可能引发过压过流及过充事故发生。

无论是车辆端或充电设备端的控制单元，功能设计上应遵循功能安全设计思想，如具备防死机、呆滞和 CPU 处理的自恢复能力，确保 BMS 与充电控制单元通信的可靠，通信连接上应具有心跳侦测、数据纠错、以及必要的容错能力，避免充电过程中如通信处理器或控制处理器故障形成假报文传递、关键参数畸变等状况，并能有效控制因此产生的充电功能失效而造成充电失控风险。

### 6.1.3 数据资源利用

合理利用充电数据资源信息及各类公共数据服务平台信息，包括行业联盟、安全运行

监测平台，应充分运用新技术发挥其充电安全保障的支撑作用，运用大数据分析和隐私信息数据清洗，在确保不泄露用户隐私和信息安全的前提下，面向充电安全提升需求 ，探索建立电池特性溯源及健康状况信息检索的数据支撑作用，开展预防性电池健康状况评估及标识，特别是充电方法合理性评估，提升充电服务行业安全保障能力。

### 6.1.4 注重安全防护措施

充电场站应为电动汽车提供安全的充电场所，确保充电操作及电能传输的安全，相应功能系统的建立，应具有电气及电能及消防安全措施，并在发生意外事故时，相应防护措施应能遏制事故危害的扩大，减少给周边人员和环境带来重大危险。

### 6.1.5 新技术应用及标准引领

应充分运用有利于提高充电安全及可靠性相关技术，发挥科技创新成果示范及标准引领作用，促进动力电池安全性能提升及充电设施监测和有效预警等共性技术研究成果的转化。深入开展新能源汽车与充电设施标准技术协同研究，不断提升充电安全标准精准化质量水平，发挥标准引领作用。

## 6.2 充电系统设计

充电系统安全性能应从设计阶段考虑，安全措施设计的运用可有效防止产品关键功能失效带来的安全风险。

### 6.2.1 通用设计要求

（1）充电设备应具有明显的安全标识以及应急故障时的处理方法提醒；

（2）充电系统电气元件，成套线缆的耐受电压等级、电磁兼容均需满足相

应标准规定的高压直流特性等相关指标要求；

（3）充电枪线的散热能力满足大电流长期工作需求，且需考虑枪线的太阳辐射，车辆碾压，跌落，高低温环境的适应性；

（4）充电设备使用应考虑环境温度、湿度、海拔、气压、耐候等影响因素，设备布置环境应具有雷电保护措施，工作环境应考虑湿度、粉尘、烟雾等安全要求；

（5）充电及供电设备带电导体护套应采用阻燃材料。

### 6.2.2 结构设计

充电设备产品应从设备接地、输出过载保护及紧急断电/急停（带载、分断能力）安全性要求，线缆抗碾压、充电口布置、锁止结构、互锁装置功能、连接器拔插要求、防松脱、偷盗安全要求，结构性防错、接触顺序、机构强度等安全要求，供电设备维修开关等

方面，依据相关标准技术要求开展设计。

充电机结构设计安全还应考虑以下三个方面：

（1）防止人体接近壳内危险部件；

（2）防止固体异物进入壳内设备；

（3）防止由于水进入壳内对设备造成有害影响。

#### 6.2.2.1 防尘、防水设计标准

根据国标 GB/T 4208《外壳防护等级（IP 代码)》要求，非车载充电机防护等级至少需要达到 IP54，交流充电设备防护等级至少需要达到 IP55，方可保证设备和人员安全。

防尘网安装在充电桩的进风孔处，主要功能是防止空气中的灰尘（灰尘中含有带电颗粒）进入设备，影响设备的可靠性。另外还有助于防止有害的昆虫从进风孔进入设备，对设备造成损坏。

#### 6.2.2.2 防盗设计

防盗设计主要考虑以下五个方面：

（1）设备安装应坚固可靠，在不破坏设备或安装件的条件下，不能移动设备或接触、获取设备中的部件（移动式充电机不包括在内)；

（2）必须使用钥匙或专用工具开启设备；

（3）充电机设计有门禁系统，通过后台监控防止设备被盗；

（4）充电机的零部件，不得通过使用常用工具（十字、一字螺丝刀、尖嘴钳、平口钳、榔头等）直接从设备外拆装。在设备外装配的紧固件，必须采用防盗紧固件，或装配后进行防盗处理；

（5）户外机柜锁具防盗等级按照公安部颁布的 GA/T 73-94《机械防盗锁》标准中明确规定，至少要满足 A 级标准。

#### 6.2.2.3 防火设计

由于温度过高、设备过载、元件失效和绝缘击穿、连接松动等原因可能会引起燃火的危险。充电机中材料、元器件等都有足够的能力防止火焰延伸到火源以外的地方。为减小这类危险，充电机设备需采用以下措施：

（1）提供过流保护；

（2）使用可燃性能恰当的材料；

（3）避免热源集中；

（4）采用散热件、温控系统以防止可能引火的高温；

（5）使用防火屏、罩将可能的火源与其外部隔离等等。

#### 6.2.2.4 防鼠设计

（1）充电机柜外壳有考虑防鼠设计，开孔和缝隙应能防止小型啮齿类动物的进入；

（2）机柜线缆进出孔处设堵头或必须用防火泥封堵进线孔，必须选用金属或厌鼠类材料；

（3）室外设备之间的互联电缆不因小型啮齿类动物的啃咬而失效。

#### 6.2.2.5 安装设计

固定式充电设备应安装牢固，具有防盗、防撞、防恶意破坏措施，在地下或半地下车库内设置充电设备时，合理确定防水标高，满足防积水要求。电缆管沟、基础底座内部电缆入口处应采取封闭措施，防止小动物进入底部箱体。充电设备采用壁挂式支撑时，应考虑充电设备的载荷和结构耐久性。

### 6.2.3 电气安全

充电设备依据应依据 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》、GB/T 27930《电动汽车非车载传导式充电机与电池管理系统之间的通信协议》、NB/ T 33001《电动汽车非车载传导式充电机技术条件》、NB/T 33002《电动汽车交流充电桩技术条件》等标准要求进行电气安全设计，应满足以下要求：

（1）接触电流安全性

人员触碰电流应满足 GB/T 18487.1 中 11.2 的安全要求；

电压要求应满足 GB/T 18487.1 中 4.4 的安全要求；

剩余电流应满足 GB/T 18487.1 中 10.3 的安全要求。

（2）接地安全

应满足 NB/T 33001 中 7.5.4 的要求。

（3）电气间隙和爬电距离安全

应满足 GB/T 18487.1 中 10.4 的要求。

（4）电磁辐射（电磁暴露）安全

对人和设备的伤害，传导干扰应满足 GB/T 18487.2-2017 中第 7 章的要求。

（5）电流冲击、电压波动

电流冲击应满足 GB/T 18487.1 中 9.7 的要求。

电压波动应满足 NB/T 33001 中 7.7.6 的要求。

（6）充电启停

应具有进行输出软启动自检、反灌电流测试、接触器关断测试、接触器粘连测试等相关安全保障措施。

（7）剩余电荷泄放

应符合 GB/T 18487.1 《电动汽车传导充电系统 第 1 部分：通用要求》。对于充电模式 3 和充电模式 4 应用，电动汽车供电设备断电后 1s 内，在其输出端子的电源线之间或电源线和保护接地导体之间测量的电压值，应小于或等于 60VDC，或等效存储电能小于或等于 0.2J；可采取两种设计方式，一是在输出直流继电器后端安装泄放电阻，泄放电阻的值根据模块电压、电容计算；二是部分采用内部自带泄放电阻的充电模块。充电设备进行 IMD 检测后，对充电输出电压进行泄放，也可在充电结束后，对充电输出电压进行泄放。同时，充电过程中，充电设备应具有输入输出过压、欠压保护，输出短路保护、输出反接保护、输出过载保护、输出接地监测等。

（8）过温保护

针对充电过程中的温度变化、设备内部电源模块电压与电流限制保护，充电接口功能及通信网络，传感器状态，具有异常温度状况监测与保护功能设计。

### 6.2.4 电气保护功能

非车载充电机应具有输入过欠压保护、输出过压保护、输出短路保护、输出过载保护、保护接地连续性、输入冲击电流、输出冲击电流、蓄电池反接保护、防逆流保护、接触器粘连检测、雷电防护等高压电气保护测试，应按照 NB/T 33008.1《电动汽车充电设备检验试验规范 第 1 部分:非车载充电机》中 5.4 进行相关保护功能测试,结果符合 NB/T 33001《电动汽车非车载传导式充电机技术条件》中 6.10 的规定。其中：

（1）失效保护:包括故障类、过载、短路、过温保护安全要求；

（2）软件保护:包括系统与设备各软件模块功能保护；

（3）硬件保护:包括高电压部件绝缘监测及电气隔离保护。

### 6.2.5 充电连接测试

充电连接实行互操作性要求，应符合 GB/T34657.1《电动汽车传导充电互操作性测试规范 第 1 部分：供电设备》中 6.3.4.4 输出电压超过车辆允许值测试、6.3.4.5 绝缘故障测试、6.3.4.6 保护接地导体连续性丢失测试、6.3.4.7 其他充电故障测试、6.4.4.4 保护接地导体连续性丢失测试、6.4.4.5 输出过流测试。

### 6.2.6 数据通信与安全

目前 BMS 与充电设备通讯协议的公开性、信息交互明码方式，以及总线式网络允许多

节点接入，从信息安全角度容易被第三方挂线侦听、窃取交互过程的信息，引发信息泄露；易于仿冒通讯节点发送干扰信息、虚假信息，造成充电过程的数据错误，引发充电安全事件；发送风暴数据，导致网络阻塞；通过该总线对 ECU 或充电桩的内部程序进行破坏性干预，植入非法代码，引起车辆使用安全或充电桩工作错误等。应充分意识到其危害性，采取防窃听、防攻击、防篡改、放植入等措施，提高充电信息安全。

### 6.2.7 通信控制失效

由于软硬件功能组件衰退致使通信差错或数据质量产生劣化，导致系统控制或服务功能丧失，在电能交换过程中偏离预期要求，由此所产生事故发生安全风险。

系统设计应采用软件心跳侦测、数据纠错、以及必要的激活措施，防止充电过程中通信处理器、控制单元死机、假报文传输、关键参数畸变等，有效改善 BMS 与充电控制单元间的通信质量，减少充电控制功能失效或失控风险。

### 6.2.8 充电数据收集、清洗、存储、查询

充电系统应具备记录极值单体电压及单体编号、极值温度，并根据充电电流和电压响应曲线进行充电异常判断功能，如通过电压变化率判断电池是否异常；具备数据清洗和存储功能，根据电池异常状态应配有对应的保护机制。

充电过程中 BMS、充电设备产生的充电安全相关的数据在数据处理的整个链路及利用过程中需要进行安全相关的设计。

在数据收集阶段,由于传输的方式多样化，需要针对每种传输方式进行数据防丢失、防篡改等安全设计。

在数据清洗阶段,由于数据产生的频率高、数据访问并发大,需要针对高并发的特性进行设计,以免由于数据清洗不及时导致后续数据的实时应用（比如充电安全的监控和预警）延迟较高。

在数据存储和查询使用阶段,需要针对数据的安全保护进行分层设计,防止数据出现未被授权而使用,保证数据被安全使用。由于数据量大,需要针对海量数据的高效存储和查询做针对性的设计,保证数据不丢失并被高效检索使用等。

## 6.3 充电设施安全要求

充电设施应通过本体安全设计、系统安全措施、工程建设等安全标准实施、运行维护、监测管理等支撑手段建立，保证充电基础设施安全。

### 6.3.1 充电设备标准安全技术要求应确保实施

#### 6.3.1.1 设备与接口标准

充电设备应符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》、NB/T 33001《电动汽车非车载传导式充电机技术条件》、NB/T 33002《电动汽车交流充电桩技术条件》的要求。在结构上，具有泄放电路、接触器、断路器、防雷保护器、急停保护、防止意外带电切断的锁止装置等保证安全保护元件。在绝缘保护方面，通过相关绝缘安全测试，包括绝缘电阻测试、介电强度、冲击耐压测试。同时，充电设备应具有牢固接地，保护接地、接地连续性监测等防触电的安全保护措施。

### 6.3.2 电气安全与防护

#### 6.3.2.1 设备电气安全

非车载充电机高压电气部分应按照 NB/T33008.1《电动汽车充电设备检验试验规范第 1 部分 非车载充电机》中安全要求进行测试：

（1）绝缘检测

非车载充电机电气部分绝缘检测功能应按照 NBT33008.1《电动汽车充电设备检验试验规范第 1 部分 非车载充电机》中 5.3.3 进行，结果符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》 中 B.4.1 和 B.4.2 的规定。

在绝缘检测前，分别选择以下测试电阻 Rt，分别选择在被测设备的直流输出 DC+与 PE 之间或 DC-与 PE 之间进行非对称绝缘测试、直流输出 DC+与 PE 之间和 DC-与 PE 之间进行对称绝缘测试。测试电压为被测设备额定充电电压；测试电阻 Rt 精度应满足 DL/T 1392-2014 中表 3 的规定；100Ω /V< Rt≤500Ω /V，检查是否有绝缘报警提示，是否允许充电；Rt≤100Ω /V，检查是否有绝缘报警提示，是否允许充电。

在自检阶段，绝缘检测的输出电压应为车辆通信握手报文内的最高允许充电总电压和供电设备额定电压中的较小值。

绝缘检测完成后，应按照 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中 B.4.2 的规定对充电电压进行泄放。检查充电前非车载充电机检测到绝缘水平下降至要求值以下时是否有告警提示或不允许充电。

充电机绝缘检测功能应与车辆绝缘检测工程相配合。

其闭合时间及检测方式按照 GB/T18487.1-2015 B.4.1 的要求取 DC+,PE 之间绝缘电阻，DC-,PE 之间绝缘电阻，两者之间小者。不检测 DC+,DC-之间。同时，在绝缘检测前，应检测直流输出接触器 K1,K2 的外侧电压，当电压超过+10V，或者小于-10V，都应停止绝

缘检测流程，并发出告警。

对绝缘检测的流程时序需要注意：在启动到绝缘检测电压-10V 时，闭合 K1,K2，然后进行绝缘检测。

（2）电气隔离要求

充电设备的动力电源输入和直流输出之间应采取电气隔离防护措施；对于一机多充式充电机，各直流输出接口之间也应采取电气隔离防护措施。

（3）接地安全

应符合 GB 18487.1 《电动汽车传导充电系统 第 1 部分：通用要求》、GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》、NB/T 33001 《电动汽车非车载传导式充电设备技术条件》。对于所有模式，在交流电网（电源）接地端子、直流电网（电源）接地端子和车辆插头的接地端子之间应提供保护接地导体，交直流充电设备均必须具备保护接地导体，保护接地导体的尺寸符合 GB 16895.3《低压电气装置 第 5-54 部分：电气设备的选择和安装 接地配置和保护导体》要求，车辆插头也需提供保护接地导体；交流充电转保护接地导体的尺寸与相线相同，直流保护接地导体尺寸符合 GB/T 33594《电动汽车充电用电缆》；交/直流充电设备均有接地连续性检测功能，PE 同时连接交流电网侧和车辆侧。电动汽车充电连接装置的接地保护应进行短时耐大电流测试，接地电路中的部件不得熔化断开或破损。接地导线和中线（如果有）的横截面积至少应等于相线导线横截面积，或者满足 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》标准中表 2 的要求。充电设备金属壳体应设置接地端子(螺栓)，其直径不应小于 6mm，并应有接地标志。充电设备金属材质的门板、盖板、覆板和类似部件,应采用铜质保护导体将这些部件和充电设备的结构主体框架连接，且保护导体的截面积不应小于 2.5㎜²。所有作为隔离带电导体的金属外壳、隔板、电气装置的金属外壳以及金属手柄等，均应有效等电位连接，且接地连续性电阻不应大于 0.1Ω；充电设备内的工作接地与保护接地应单独连接到接地导体(铜排)上，不应在一个接地线中串接多个需要接地的电气装置；接地母线和柜体之间的所有连接应避开（或穿透绝缘层）喷漆层，以保证有效的电气连接。

充电设备内的工作接地与保护接地均单独连接到接地导体(铜排)上，接地线与桩体钣金直接通过锯齿垫圈破开喷漆层，保证接地的连续性。

（4）剩余电流保护

应符合 GB/T 18487.1 《电动汽车传导充电系统 第 1 部分：通用要求》和 NB/T 33002《电动汽车交流充电桩技术条件》要求。对于交流充电设备，在电源进线侧需安装 A 型或

B 型剩余电流动作保护器，动作电流值为 30mA。

（5）直流输出回路短路保护

非车载充电机电气部分直流输出回路短路保护功能应按照 NB/T 33008.1《电动汽车充电设备检验试验规范第 1 部分 非车载充电机》中 5.3.4 进行，充电设备应停止充电过程并发出告警提示。

（6）电击防护

应符合 GB 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》、GBT 18487.3《电动车辆传导充电系统：电动车辆交流/直流充电设备(站)》和 NB/T 33001 《电动汽车非车载传导式充电设备技术条件》。应实时检测接触器、继电器工作状态，在继电器输入端进行电压采样，在充电设备启动后直流继电器闭合前对采样电压进行读取，判断直流继电器主触点是否粘连，如果粘连立即停止工作并告警；建议采用剩余电流动作断路器，若因剩余电流过大导致动作，断路器需要手动操作复位，可以通过柜外进行复位操作。充电设备在柜门上必须装有行程开关，若门打开，行程开关信号传输给主控制板，主控制板控制切断交流接触器。充电设备应该采用基本绝缘作为基本防护措施，和采用附加绝缘作为故障防护措施，或采用能提供基本防护和故障防护功能的加强绝缘。充电设备外壳材质宜选用绝缘阻燃材料。

（7）车辆插头锁止检测

充电机车辆插头应具备锁止装置，其功能应符合 GB/T 18487.1－2015 中 9.6、GB/T 20234.1－2015 中 6.3、GB/T 20234.3－2015 中附录 A 的要求。

在出现故障不能继续充电或充电完成时，锁止装置应能解锁且解锁前车辆插头端口电压不应超过 60 V。

非车载充电机车辆插头锁止功能试验应按照 NB/T33008.1《电动汽车充电设备检验试验规范第 1 部分 非车载充电机》中 5.3.5 进行，充电设备车辆插头应能有效锁止或解锁。

车辆插头锁止装置可分为电磁式（脉冲电压保持式）和电机式两种。

车辆插头锁止装置反馈可分为机械开关和光隔离两种。

当需要应急解锁时，充电枪一般采用内置电子锁解锁盒，解锁通过电容反向放电完成。

（8）预充电功能

非车载充电机应具有预充电功能，防止启动充电过程产生过大的冲击电流，并且提升输出直流接触器的电气寿命。启动充电阶段，电动汽车闭合车辆侧直流接触器后，充电机应检测电池电压并判断此电压是否正常。当充电机检测到电池电压正常后，将输出电压调

整到当前电池端电压减去 1 V～10 V，再闭合充电机侧的直流输出接触器。

充电设备预充电功能测试应按照 NB/T33008.1《电动汽车充电设备检验试验规范第 1 部分 非车载充电机》中 5.3.6 进行，结果符合 NB/T 33001《电动汽车非车载传导式充电设备技术条件》中 6.6 的规定。

（9）急停功能

应符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》、NB/T 33001 《电动汽车非车载传导式充电设备技术条件》。非车载充电机应具有急停装置，当启动急停装置时，一体式充电机应同时切断动力电源输入和直流输出；分体式充电机应切断相应充电终端的直流输出，也可同时切断充电机的动力电源输入。

其中，切断动力电源输入有切断充电机动力电源输入（远方）、切断充电机进线开关（分励脱扣器）、切断充电模块供电电源的三种方式。

启动急停装置，充电机应在 100 ms 内断开 K1 和 K2，且电子锁解锁时车辆接口电压不应超过 60VDC。因此，急停应串联在 K1,K2 供电回路中，且充电控制器需要采集到此状态，进行关机，泄放，解锁操作。

急停功能试验测试应按照 NB/T 33008.1《电动汽车充电设备检验试验规范第 1 部分 非车载充电机》中 5.3.10 进行，结果符合 NB/T 33001《电动汽车非车载传导式充电设备技术条件》中 6.9 的规定。

（10）绝缘状态监测与保护要求

充电设备应具备直流侧绝缘检测以及接地故障保护装置，防止直流侧绝缘不佳的时候，造成设备损坏，火灾，以及人身触电等人身财产损失。充电绝缘检测按照 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》附录 B 的要求，在充电机端和车辆端均设置绝缘检测电路，供电接口连接后到充电设备充电之前，由充电机负责充电机内部（含充电电缆）的绝缘检查；充电过程期间，由电动汽车负责整个系统的绝缘检查。绝缘检测为测量充电直流回路 DC+、PE 之间的绝缘电阻，与 DC-、PE 之间的绝缘电阻（两者取小值 R），当 R ＞ 500 Ω/V 视为安全；100Ω/V ＜ R ≤ 500 Ω/V 时，宜进行绝缘异常报警，但仍可正常充电；R ≤ 100 Ω/V 视为绝缘故障，应停止充电。

（11）温度监测与保护

充电设备应对充电连接器、充电设备内部进行温度监测，当设备温度超过限值时，充电设备应过温保护。充电设备内部动力电源输入电流所流经的回路，如接线端子、输入断路器、输入接触器等；功率变换单元及其内部元器件、输入输出端子；直流输出电流所流

经的回路，如接线端子、直流熔断器、直流接触器、功率电阻、电流采样分流器、车辆插头等。这些发热元器件及部件的最高温度小于等于元器件及部件最大耐受温度的 90%，且不应影响周围元器件的正常工作和无元器件损坏。在正常条件下，充电机在最大输出电流下长期运行，内部各发热元器件及各部位连接端子处的温升不应大于 NB/T 33001《电动汽车非车载传导式充电设备技术条件》表 2 的规定。充电设备组件、部分、绝缘体和塑料材料的温度应低于在设施寿命周期内正常使用时可能降低电气、机械性能的温度。

#### 6.3.2.2 过温保护

采取在充电设备外壳以及充电线缆表皮内安装温度传感器，实时检测温度，温度达到设定阈值后，立即向平台报警，给出温度预警提示，温度达到设定极值后，立即降低输出电流或者立即中断充电进程，并将相关信息回传至平台。

增加充电枪内部温度检测，充电枪厂家提供各类工况下的报警阈值。充电设备利用阈值，实现更精准的过温防护。

#### 6.3.2.3 耐环境要求

充电设备应通过防水测试、防尘测试，符合 IP 防护等级要求，应按照 NB/T33008.1《电动汽车充电设备检验试验规范第 1 部分 非车载充电机》中 5.5 进行防止固体异物进入试验、防止水进入试验、防盐雾试验，结果符合 NB/T33001《电动汽车非车载传导式充电设备技术条件》中 7.3 的规定。

（1）防凝露

符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》。对于室内的设备，最高温度为+40℃时空气的相对湿度建议不超过 50%，在较低温度下允许有更高的相对湿度，如+20℃为 90%。由于温度的变化，应考虑偶尔出现的湿度冷凝；对于室外的设备，相对湿度为 5%-95%。对于充电设备有液冷系统，应将其管路包裹保温层，且需要特殊结构设计的冷却管路，确保凝露形成时，可以通过管路顺利流出机壳内，不会触碰到电器元件；充电设备内宜安置湿度传感器，实时监控桩内环境湿度，当超过危险值时候采取相应措施。

（2）防碰撞

在充电设备内部宜安装碰撞行程开关，遇到碰撞触发开关，发出报警信号并停止充电。充电车位设置限位装置编入产品使用说明书中，充电设备外形设计应避免不规则、不易发现的低矮的突出物，放置车辆检测不到而发生误幢。充电设备在设计时，需考虑 1m 以下部分的结构强度，必须具备一定的防碰撞功能。

（3）防水溢

在充电设备内置浮子开关，在用电最低处同时安装两个浮子开关，采用冗余设计，确保设备水溢的时候触发开关，发送信号给控制器，紧急停止设备。

防风保护

户外型充电机应能承受 GB/T 4797.5 规定的不同地区最大风速的侵袭。

防锈（防氧化）保护

充电设备铁质外壳和暴露的铁质支架、零件应采用双层防锈措施，非铁质的金属外壳也应具有防氧化保护膜或进行防氧化处理。

三防（防潮湿、防霉变、防盐雾）保护

充电设备内印刷线路板、接插件等部件应进行防潮湿、防霉变、防盐雾处理。其中防霉变腐蚀试验参考 GB/T 2423.16－2008 中的试验方法 1，长霉程度等级不低于标准中要求的 2a；其中防盐雾腐蚀试验参考 GB/T 2423.17－2008 中 6 规定的试验方法，试验时间 48 h，试验后在 15 ℃～40 ℃流水中用柔软的刷子清洗 7 分钟，干燥 1 h，产品应无赤/青锈、没有出现涂装掉落现象、涂装无鼓起。

（7）故障紧急保护

定义关键传感器，当发生故障时，可以立即关断充电设备，全部关键传感器接入一个额外的安全电路，使得任意一个传感器检测出故障信号，桩端电源立即被自动物理切断

（8）高温沿海地区

我国长江以南的高温沿海地区使用的符合 NB/T 33001—2018 规定的电动汽车非车载充电机的基础上，考虑高温沿海地区最显著的环境因素（湿热、盐雾、太阳辐射）对充电机提出特殊要求。其中，高温沿海地区指我国长江以南的距离海岸线 50km 以内区域，或面积不大于 4 万平方公里的整个岛屿。

防盐雾性能按 T/CEC 214—2019《电动汽车非车载充电机高温沿海地区特殊要求》表 101 确定，无通风孔且柜内不产生凝露的，防护等级达到 IP54，未达到 IP65 的充电机，其属于Ⅱ型表面的零部件试验周期可比 T/CEC 214—2019《电动汽车非车载充电机高温沿海地区特殊要求》表 102 规定的低一个等级，防腐等级应为 A 类的充电机Ⅱ型表面的零部件不应降级。

#### 6.3.2.4 电磁兼容

充电设备电磁兼容 EMC 包括辐射骚扰限制测试、传导骚扰限制测试、静电放电抗扰度测试、浪涌抗扰度测试、电压暂降、短时中断抗扰度测试，符合 GB/T 18487.2《电动汽

车传导充电系统 第 2 部分：非车载传导供电设备电磁兼容要求》中 7.1、8.2 和 8.3 规定的要求。

#### 6.3.2.5 可靠性要求

充电设备产品设计寿命应至少满足 8 年设计,结构强度应确保能正常工作,外表面不能锈蚀,导线护套不得开裂,防水部位不得产生渗漏,设备寿命期内产品功能保持工作正常，性能衰减不超出容限值;充电设备整机平均故障间隔时间不应小于 26280h。

## 6.4 充电控制策略

充电控制策略包括：充电最高电压、最大允许电流、温度限值、单体极值等电池安全极值的安全与保护要求。充电过程中，与 BMS 交互充电过程报文，监控充电电压、电流、温度的变化，当超过所限定的允许充电限值时，应及时做停机保护。

针对不同类型的电池的单体极值监测，当单体电压超过允许充电极值时，充电设备应能够上报告警，并及时停止充电。

充电机应能根据充电过程参数，感知动力电池及车载电气设备的工作状态，判断 BMS 数据的有效性和一致性，防止动力电池发生过充危险。

充电控制策略应利用充电系统的大数据分析能力，对动力电池的安全风险进行预警，防止触发动力电池的安全事故。

### 6.4.1 充电控制

#### 6.4.1.1 充电时序要求

充电时序应符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》，GB/T 27930《电动汽车非车载传导式充电机与电池管理系统之间的通信协议》的充电时序要求。

#### 6.4.1.2 充电过程数据要求

充电过程中状态数据应能准确上报，特别是充电总电压，总电流、极限值、单体值等均按照要求上报，只要车载 BMS 发送，双协议模块，充电机均需要正确处理后转发，充电监控需要正确显示。同时，充电监控对于充电总电压，总电流、极限值、单体值均需要定期下发查询。充电中各个时间、充电电量、充电时长的数正确。其中，充电相关 BMV（单体电池温度）、BMT（单体电池电压）报文 GB/T 27930《电动汽车非车载传导式充电机与电池管理系统之间的通信协议》定义为可选报文，但为了充电设备能够及时发现充电安全风险，需定义为必选报文，并提高发送的频率。

GB/T 27930 中的 BMS 和车辆辨识报文(BRM)中车辆识别码 VIN 定义为可选报文，但为

了充电设备更好的基于车辆本身的属性以及车辆本身的充电历史数据发现充电安全风险，需定义为必选报文。

#### 6.4.1.3 基于充电过程数据的控制策略

充电设备可以利用积累的充电过程大数据建立充电安全防护模型，在充电过程中实时的基于安全防护模型、BMS 数据 搭建除了 BMS 异常报警之外的第二道防线，当检测到异常情况是，及时停机保护.

（1）充电设备的二重保护控制

充电设备应具备对电池的二重保护功能。

1）在恒流、恒压模式的充电过程中，当检测到输出电压大于车辆最高允许充电总电压或电流响应结束后检测到输出电流大于车辆当前需求电流的 110%（当前需求电流值大于等于 30A 时）或大于车辆当前需求电流+3A（当前需求电流值小于 30A 时），或，当 BMS 交互数据的单体电压达到电池最高单体电压，并持续一定时间后（15s），充电设备应在 1s 内断开 K1K2，并发出告警提示。

2）在充电过程中，当 BMS 数据的电池最高温度达到电池允许最高温度并持续一定时间后，充电设备应停止充电，并发出告警提示。

3）充电设备应具备电池过充保护，在检测到充进电池的电量和安时数大于电池的额定容量和能量时，应及时停止充电并报出告警。

4）充电设备应具备对 BMS 交互数据出现干扰、数据不更新、数据异常的判断功能，当出现异常数据会导致电池过充、过热、过压、过流时，应采取控制策略或停止充电，防止电池安全风险，并发出告警。

（2）充电系统利用大数据分析功能控制策略

充电系统应充分利用充电大数据分析的作用，建立电池特性溯源及健康状况信息检索的数据支撑作用，识别车辆充电过程中的风险。基于纵向充电历史数据的电池特性溯源和同类车型横向数据统计分析的充电安全模型，有助于对充电过程进行安全策略的调控，降低电池事故风险，延缓电池健康指标衰减，并对车辆未来的健康状况进行预测。

安全防护模型需要考虑实现的目标以及包含的维度包括：

1）结合车型的电池衰减特征、车辆的历史充电数据等估算出车辆电池容量的衰减程度,并结合车辆的充电行为特征、车辆的运营类型等对电池未来的容量衰减趋势做出预测。

2）车辆由于运行环境、运营类型、充电习惯、运行习惯的不同会导致车辆触发各个安全核心指标的周期、变化速率或者本身的实际阈值数据不同。为了实现尽可能提前对车

辆的异常指标发现并预警，需要对安全的核心指标的阈值建立对应的模型，需要包含的安全指标以及模型计算的分析维度参考如下：

电池充电过程中最高温度的阈值、温升速率的阈值、最大温差的阈值、最大压差的阈值、soc 速率的阈值、单体过压的阈值、电池过充的阈值需要结合车型、城市、时间以及车辆自身的历史充电数据的大数据特征进行动态确定

### 6.4.2 故障、异常状况监测及保护

（1）应具备充电系统发生各项故障时，通过合理处理策略保证充电安全；

（2）对安全监控参数超限发生后，充电监控系统向充电机发出紧急停机指令，充电机需要执行停机；

（3）充电桩控制系统对充电回路中每个继电器、接触器、熔断器做检测，检测器件是否正常，并作出故障告警；

（4）每个充电回路带有防反二极管，防止充电设备内部故障时，引起故障扩大；

（5）充电中实施枪头温度检测，当枪头温度过高时可中断充电；

（6）将有关信息存储到网络数据库，须确保网络数据库有效，如存储失败需给出错误信息。

### 6.4.3 故障分类及处理

严重故障，直接影响人身安全级别故障。如绝缘故障、漏电故障等。当发生严重故障时，设备或者充电模块须立即停机，等待专业维护人员维修；

电池热失控：可能引起电池总电压过充、电池单体电压过充、电池容量过充、电池温过高等导致电池热失控风险的故障，应立即停止充电，并主动告警，并在充电系统中后台中记录。

一般故障，不涉及人身安全但需及时维护的故障。主要为设备安全级别故障，如连接器故障（导引电路检测到故障），充电机检测到充电电流不匹配等。当发生一般故障时，充电设备停止本次充电，并做好故障记录（需重新插拔充电电缆后，才能进行下一次充电）。

告警提示，需要引起操作人员注意的相关问题。如充电握手阶段、配置阶段的超时、充电过程超时等。当充电设备处于告警提示状态时，充电设备中止充电，待故障现象排除后自动恢复充电（检测到故障状态解除后，重新通信握手开始充电）。

表 1　故障分类

| 故障分类 | 故障描述 | 故障名称 |
| --- | --- | --- |
| 严重故障 | 故障直接影响人身安全级别故障 | 绝缘故障 |
| | | 漏电故障 |
| | | 泄放回路故障 |
| | | 防雷故障 |
| 电池系统 | 可能引发电池热失控风险的故障 | 达到单体最高电压未停止充电 |
| | | 达到电池总电压未停止充电 |
| | | 达到电池最高允许温度未停止充电 |
| 一般故障 | 不涉及人身安全但需及时维护的故障 | 连接器故障（导引电路检测到故障） |
| | | 电子锁故障 |
| | | 急停故障 |
| | | 输入过/欠压 |
| | | 输入缺相 |
| | | 交流接触器故障 |
| | | 直流接触器故障 |
| | | 充电模块故障 |
| | | 充电电流不匹配 |
| | | 输出短路 |
| | | 输出过压/过流 |
| | | 电池反接 |
| | | 充电系统过温 |
| | | 充电枪过温 |
| 告警提示 | 设备处于告警提示状态 | 通信超时 |

根据充电结束的要求，可以分为正常停止充电、故障停止充电以及紧急停止充电。

正常停止充电：用户、车辆或供电设备中止充电过程，并非由故障导致停机。包括用户、车辆或供电设备正常主动中止充电。

故障停止充电：充电设备或车辆检测到故障而中止充电过程，当发生输出过压保护、通信线异常故障时，供电设备分别在 1s 和 10s 内打开接触器 K1、K2、K3、K4。

紧急停止充电：供电设备或车辆检测到故障而紧急中止充电过程，如出现安全危险。当发生控制导引信号异常、保护接地连续性丢失、不能继续充电故障时，供电设备应在100ms 打开接触器 K1 和 K2。

企业标准设计时，应遵循上述原则。

## 6.5 充电系统及设备功能设计

### 6.5.1 控制器软件功能安全设计

（1）输出过压保护功能

充电系统软件应具备输出过压检测及保护功能，当输出电压大于需求电压或者大于电池最高允许电压时，在 1s 内应切断输出功率回路，停止充电，充电系统报出输出过压故障。

（2）输出过流保护功能

充电系统软件应具备输出过流检测及保护功能，当输出电流大于需求电流或者大于电池最高允许充电电流时，再 1s 内应切断输出功率回路，停止充电，充电系统报出输出过流故障。

（3）输出接触器异常检测

充电系统具备功率回路异常检测功能，具备输出接触器粘连检测，输出接触器驱动失效检测，熔断器故障检测，在检测到以上故障后可以及时停止充电并报出故障。

直流接触器粘连检测方式，可采取以下三种方式：

1）参照车辆接触器黏连检测方式，利用绝缘电压，对比 K1,K2 内外侧电压；

此种方式控制逻辑复杂，但是借用充电系统现有的电压采样电路及绝缘电压，进行绝缘检测，成本较低。

2）外围电路检测接触器电阻；

需注入信号检测接触器状态，有影响车辆绝缘检测的风险；接触器在长期工作，主触头会有氧化，在无电流时内阻较大影响检测精度。

3）接触器本身自带节点；

接触器本身自带位置节点，实时反馈主触头位置；目前有三种反馈方式行程开关，干簧管，内置控制板。

（4）泄放回路故障检测

充电系统具备泄放回路粘连以及失效检测功能，在泄放回路粘连或者失效时应禁止充

电，防止安全事故。

（5）辅助电源回路保护

直流充电设备应能为电动汽车提供低压辅助电源。低压辅助电源应具备输出过电压、过电流、短路保护功能。避免电流倒灌损坏充电设备。

（6）绝缘检测

充电系统应具备绝缘检测功能，当 DC+对 PE、DC-对 PE，任何一边的阻抗小于 100 欧/V 的标准时，充电系统应准确报出绝缘故障并停止充电；当任何一边的阻抗小于 500 欧/V 时，充电系统应发出绝缘检测告警提示，可以继续充电。

（7）防雷防护

雷电防护的浪涌保护装置的安装和选型应满足 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中 11.7 规定的要求。

（8）系统故障检测

充电系统软件应具备门磁故障检测，防雷故障检测，湿度过大故障检测，风机故障检测等功能，在检测到系统故障时应准确报出故障并在 1s 内停止充电。

（9）输入欠压保护

充电系统具备输入欠压检测及保护功能，在系统发生欠压时应及时报出欠压故障，并停止充电，当充电系统输入前级有交流接触器时，应及时切断交流接触器防止欠压导致接触器线圈反复吸合，烧坏输入交流接触器，引起重大事故。

（10）输入过压保护

充电系统应具备输入过压检测及保护功能，在系统发生过压时，应及时报出过压故障，并停止充电，并切断输入级配电回路，防止后级器件因为过压损坏造成重大的事故。

（11）输入缺相保护

充电系统应具备输入缺相检测及保护功能，在系统发生缺相时，应及时报出缺相故障，并停止充电。

（12）系统过温保护

充电系统应具有过温检测及保护功能，当系统环境温度过高时具备温度限功率策略，防止系统温度变得更高；当系统温度超过环境温度保护值时，应停止充电，充电系统报出过温故障。

（13）充电枪过温保护

充电系统应具备充电枪过温检测及保护功能，充电过程中实时检测充电枪的温度，当

温度过高时可以限制充电枪输出功能，抑制温度再升高，当温度超过保护值时，应及时停止充电并报出充电枪过温故障。

（14）电池单体过压防护

充电系统应具备单体过压防护功能，在检测到电池当前单体电压大于电池允许的最高单体电压时应及时停止充电并报出告警。

（15）电池过温防护

充电系统应具备电池过温防护功能，在检测到电池当前最高温度大于电池允许的最高温度时应及时停止充电并报出告警。

（16）电池热失控防护

充电系统应具备电池热失控检测及防护功能，根据电池类型，在一段时间内当电池温升超过阈值时，应及时停止充电并报出告警。

（17）电池数据不刷新防护

充电系统应具备电池数据不刷新检测及防护功能，当电池数据在一段时间内持续不刷新，应及时停止充电并报出告警。

（18）电池反接保护

充电系统软件应具备电池反接检测及保护功能，从插枪开始，实时检测电池两端电压，如果发生反接，及时报出故障，切断功率回路，关闭充电模块，停止充电。

（19）电池过充防护

充电系统应具备电池过充检测及防护功能，在检测到充进电池的电量和安时数大于电池的额定容量和能量时，应及时停止充电并报出告警。

（20）充电枪老化预警防护

充电系统应具备充电枪老化预警防护，当检测到充电枪长时间适用，接触器电阻变大已经发生老化，应禁止该终端充电，并发出告警，提醒更换充电枪，防止更大的事故。

### 6.5.2 互操作性要求

充电设备应根据 GB/T 34657.1《电动汽车传导充电互操作性测试规范 第 1 部分：供电设备》要求，进行充电接口互操作性测试、直流充电互操作性测试、交流充电互操作性测试。电动车辆应根据 GB/T 34657.2《电动汽车传导充电互操作性测试规范 第 2 部分：车辆》要求，进行直流充电互操作性测试、交流充电互操作性测试。对于直流充电，电动车辆和非车载充电机需要按照 GB/T 35658《电动汽车非车载传导式充电机与电池管理系统之间的通信协议一致性测试》要求，进行肯定测试和否定测试。

充电互操作性是相同或不同型号、版本的供电设备与电动汽车通过信息交换和过程控制，实现充电互联互通的能力。协议一致性测试是一种功能性测试，它是在一定的网络环境下，利用一组测试序列，对被测协议实现进行测试，通过比较实际输出与预期输出的异同，判定被测实现在多大程度上与描述标准一致。协议一致性测试是互操作性测试的基础，只有通过协议一致性测试的产品，表明其符合相关协议标准要求，才有意义进行互操作性测试。

#### 6.5.2.1 充电接口互操作性

充电接口是保证电动汽车充电安全性、互换性的基础。车辆插头、车辆插座、供电插头、供电插座的结构尺寸应符合 GB/T 20234.2《电动汽车传导充电用连接装置 第 2 部分：交流充电接口》附录 A、GB/T 20234.3《电动汽车传导充电用连接装置 第 3 部分：直流充电接口》附录 A 规定的允许公差范围内。同时直流充电车辆插头、交流充电车辆插头、交流充电供电插头的最大外轮廓应符合 GB/T 20234.3-2015《电动汽车传导充电用连接装置 第 3 部分：直流充电接口》附录 C、GB/T 20234.2《电动汽车传导充电用连接装置 第 2 部分：交流充电接口》附录 C 的规定。这样不同制造商生产的插头和插座应能满足互换的要求。

#### 6.5.2.2 通信协议一致性要求

电动汽车直流充电通信协议作为实现电动汽车传导充电的基本要素，协议的标准化、规范化是保证电动汽车与充电基础设施互联互通的基础，是电动汽车充电安全性和兼容性的有效保障。因此十分需要且必要进行协议一致性测试，以降低因协议不兼容而造成电动汽车与充电设施的互联互通障碍。协议一致性测试被列为充电设备型式检验的必做项目。

电动汽车直流充电通信协议一致性测试案例分为物理层测试、数据链路层测试、应用层测试、充电流程测试、数据正确性测试。但因物理层和链路层特性主要由 CAN 控制器决定，因此一致性测试的主要内容为应用层测试、充电流程测试、数据正确性测试，具体又分为肯定测试和否定测试两类。具体测试要求和测试案例在 GB/T 34658《电动汽车非车载传导式充电机与电池管理系统之间的通信协议一致性测试》中规定。

#### 6.5.2.3 直流充电互操作性

##### 6.5.2.3.1 连接确认阶段要求

连接确认是实现正常充电的基础环节。在车辆插头与车辆插座进行插合过程中，充电设备和电动汽车通过监测连接确认信号（CC1 信号和 CC2 信号）的电压，确认充电接口是否完全连接。

车辆接口应具有锁止功能，该功能应符合 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》的相关要求，车辆插头端应安装机械锁止装置，供电设备应能判断机械锁是否可靠锁止。车辆插头应安装电子锁止装置，电子锁处于锁止位置时，机械锁应无法操作，供电设备应能判断电子锁是否可靠锁止。当机械锁或电子锁未可靠锁止时，供电设备应停止充电或不启动充电。

供电设备连接确认检测。充电机通过测量检测点 1 的电压值判断车辆插头与车辆插座是否已完全连接，当检测点 1 电压值为 4V 时，则判断车辆接口完全连接。

车辆连接确认检测。车辆控制装置通过测量检测点 2 的电压值判断车辆接口是否已完全连接，当检测点 2 的电压值为 6V，则车辆控制装置开始周期发送通信握手报文。

#### 6.5.2.3.2 自检阶段互操作性要求

在车辆接口完全连接后，首先确认车辆接触器 K5 和 K6 是否粘连。然后将闭合 K1 和 K2，进行绝缘检测，绝缘检测时的输出电压应为车辆通信握手报文内的最高允许充电总电压和供电设备额定电压中的较小值；绝缘检测完成后，将 IMD（绝缘检测）以物理的方式从强电回路中分离，并投入泄放回路对充电输出电压进行泄放，当泄放电压降至 60V DC 以下后断开 K1 和 K2。同时开始周期发送通信握手报文。车辆通过检测点 2 电压值判断车辆接口是否连接。如检测点 2 的电压值为 6V，则车辆控制装置开始周期发送通信握手报文。

车辆接触器粘连检测。在绝缘检测前，充电机闭合接触器 K1 和 K2 且不输出绝缘电压，当检测出外侧电压是否大于 10V，确认车辆接触器 K5 和 K6 发生粘连，充电机应不允许充电。

充电参数匹配性检测。当车辆通信握手报文内的最高允许充电总电压低于充电机输出电压范围下限值时，充电机应不允许充电。

绝缘电阻符合性检测。在充电机端和车辆端均设置 IMD 电路，供电接口连接后到 K5、K6 合闸充电之前，由充电机负责充电机内部（含充电电缆）的绝缘检查；充电机端的 IMD 回路通过开关从充电直流回路断开，且 K5、K6 合闸之后的充电过程期间，由电动汽车负责整个系统的绝缘检查。充电直流回路 DC+、PE 之间的绝缘电阻，与 DC-、PE 之间的绝缘电阻（两者取小值 R），当 $R > 500\ \Omega/V$ 视为安全；$100\Omega/V < R \leqslant 500\ \Omega/V$ 时，宜进行绝缘异常报警，但仍可正常充电；$R \leqslant 100\ \Omega/V$ 视为绝缘故障，应停止充电。

泄放投切要求。充电机进行 IMD 检测后，应及时对充电输出电压进行泄放，避免在充电阶段对电池负载产生电压冲击。绝缘检测结束时，充电机应及时对绝缘输出电压进行泄

放，当接口电压降到 60V DC 以下时，再断开接触器 K1 和 K2。

#### 6.5.2.3.3 充电准备就绪阶段要求

车辆与充电机进入充电参数配置阶段，充电机向 BMS 发送充电机最大输出能力的报文，BMS 根据充电机最大输出能力判断是否能够进行充电。当充电参数匹配成功后，车辆首先闭合接触器 K5 和 K6，使充电回路导通；充电机进行预充电检测，当检测到车辆端电池电压正常且在充电机正常输出范围内闭合 K1 和 K2，使直流供电回路导通。

电池电压匹配性检测。在配置阶段，当充电机检测到接触器外端电压与通信报文电池电压误差范围>±5%和/或不在充电机正常输出电压范围内，充电机应不允许充电。

预充电压输出要求。充电机输出电压比接触器外端电压低（1V—10V）时闭合接触器 K1 和 K2，以避免因接触器内外侧电压差太大闭合接触器造成冲击电流。

#### 6.5.2.3.4 充电阶段要求

充电阶段，车辆 BMS 实时向充电机控制装置实时发送电池充电需求参数，充电机根据电池充电需求来调整充电电压和充电电流以保证充电过程正常进行。同时充电机和 BMS 相互发送各自的充电状态。除此之外，BMS 根据要求向充电机发送动力蓄电池具体状态信息及电压、温度等信息。BMV，BMT，BSP 为可选报告，充电机不对其进行报文超时判定。BMS 根据充电过程是否正常、电池状态是否达到 BMS 自身设定的充电结束条件以及是否收到充电机中止充电报文（包括具体中止原因、报文参数值全为 0 和不可信状态）来判断是否结束充电；充电机根据是否收到停止充电指令、充电过程是否正常、是否达到人为设定的充电参数值，或者是否收到 BMS 中止充电报文（包括具体中止原因、报文参数值全为 0 和不可信状态）来判断是否结束充电。

通信超时检测。在充电过程中，如发生通讯超时，充电机应停止充电，并在 10s 内断开 K1、K2，车辆应断开 K5、K6；通讯恢复后，充电机重新进入握手辨识阶段时，车辆宜重新建立握手连接。当发生 3 次通讯超时即确认通讯中断，充电机应停止充电，并在 10s 内断开 K1、K2、K3、K4，车辆应断开 K5、K6，通讯恢复后，车辆应不能充电。

充电需求超 BMS 参数限值检测。在充电过程中，当充电需求电压值大于 BMS 最高允许充电总电压时，充电机应发送中止充电报文，并停止充电，或按照 BMS 最高允许充电总电压输出。在充电过程中，当充电需求电流值大于 BMS 最高允许充电电流时，充电机应发送中止充电报文，并停止充电，或按照 BMS 最高允许充电电流输出。

充电需求超供电设备参数限值检测。在充电过程中，当 BMS 充电需求电压值大于供电设备额定电压时，充电机应发送中止充电报文，并停止充电。在充电过程中，当 BMS 充电

需求电流大于供电设备最大输出电流时，充电机应按照供电设备最大输出能力输出。

充电需求为0值需求检测。在充电过程中，当BMS充电需求电流为0时，充电机应按最小输出能力输出。

实时采集数据超限值的输出响应检测。在充电过程中，当BMS采集的电压超过BMS最高允许充电总电压时，充电机应发送中止充电报文，并停止充电。

预估总电量超出蓄电池总电量的输出响应测试。在充电过程中，当动力蓄电池已充满，但允许继续充电时，充电机应停止充电。

输出过压检测。在充电过程中，当充电机输出电压若大于车辆最高允许充电总电压，充电机应在1s内停止充电，并断开K1、K2、K3、K4。

#### 6.5.2.3.5 正常充电结束阶段要求

充电正常结束过程，车辆控制装置根据电池系统是否达到满充状态或是否收到“充电机中止充电报文”来判断是否结束充电。在满足以上充电结束条件时，车辆控制装置开始周期发送“车辆控制装置(或电池管理系统)中止充电报文”，在确认充电电流变为小于5A后断开K5和K6。当达到操作人员设定的充电结束条件或收到“车辆控制装置(或电池管理系统)中止充电报文”后，非车载充电机控制装置周期发送“充电机中止充电报文”，并控制充电机停止充电以不小于100A/s的速率减小充电电流，当充电电流小于等于5A时，断开K1和K2。当操作人员实施了停止充电指令时，非车载充电机控制装置开始周期发送“充电机中止充电报文”，并控制充电机停止充电，在确认充电电流变为小于 5A 后断开K1、K2，并再次投入泄放回路，泄放回路的参数选择应保证在充电连接器断开后1秒内将供电接口电压降到60V DC以下。然后再断开K3、K4。达到解锁条件，车辆插头电子锁应能正确解锁。

当充电机和 BMS 停止充电后，双方进入充电结束阶段。在此阶段 BMS 向充电机发送整个充电过程中的充电统计数据，包括：中止荷电状态、动力蓄电池单体最高电压、动力蓄电池单体最低电压、动力蓄电池最高温度、动力蓄电池最低温度；充电机收到 BMS 的充电统计数据后，向 BMS 发送整个充电过程中的输出电量、累计充电时间等信息，最后停止低压辅助电源的输出。

#### 6.5.2.3.6 充电时序要求

充电连接控制时序和充电状态流程包括检测点1的电压值、K1和K2状态、K3和K4状态、K5和K6状态、充电状态、通信状态、车辆接口锁止状态、充电状态转换的间隔时间，应符合GB/T 18487.1《电动汽车传导充电系统 第1部分：通用要求》中B.5的规定，

通信状态应符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中 B.6 和 GB/T 27930《电动汽车非车载传导式充电机与电池管理系统之间的通信协议》中对应阶段的规定。

#### 6.5.2.3.7 非正常充电结束要求

通信线路异常状态检测。对于采用充电模式 4 的供电设备，在充电前和充电过程中，当通信线路发生短路、断路或接地故障时，充电机应停止充电并发出告警。

保护接地连续性检测。在充电过程中，充电机应能对从本体内部到车辆插头处 PE 线的保护接地性检测，当发生保护接地性丢失时，充电机应能在 100ms 内切断电源。在充电过程中，当发生 PE 断针时，对使用上拉电压 U2 大于 15.2 V、小于 31 V、且精度不大于 1%，或 U2 大于 22 V、小于 30 V、且精度不大于 5%的车辆应能发送 BMS 中止充电报文。

控制导引信号检测。在充电过程中，充电机通过对检测点 1 的电压进行检测，当发生开关 S 由闭合变为断开或车辆接口由完全连接变为断开时，充电机应在 50ms 内将输出电流降至 5A 或以下，100ms 内断开 K1、K2，统计报文交互完毕后断开 K3 和 K4。

其他不能继续充电故障检测。在充电过程中，当充电机出现不能继续充电的故障，则向车辆周期发送“充电机中止充电报文”，并控制充电机停止充电，应在 100ms 内断开 K1、K2，统计报文交互完毕后断开 K3 和 K4。在充电过程中，如果车辆出现不能继续充电的故障，则向充电机发送“车辆中止充电报文”，并在 300ms（由车辆根据故障严重程度决定）内断开 K5 和 K6。

### 6.5.2.4 交流充电互操作性

#### 6.5.2.4.1 连接确认阶段要求

连接确认是实现正常充电的基础环节。在供电插头与供电插座（连接方式 B）、车辆插头与车辆插座（连接方式 A、C）进行插合过程中，充电设备和电动汽车通过监测控制导引信号（CP 信号）、连接确认信号（CC 信号）的电压，确认供电接口、车辆接口是否完全连接。

当车辆插头与车辆插座插合后（方式 A 下为供电插头与供电插座），车辆的总体设计方案可以自动启动某种触发条件（如打开充电门、车辆插头与车辆插座连接或者对车辆的充电按钮、开关等进行功能触发设置），通过互锁或者其他控制措施使车辆处于不可行驶状态。

车辆控制装置通过测量检测点 3 与 PE 之间的电阻值来判断车辆插头与车辆插座是否完全连接（对于连接方式 B 和 C）。完全连接后，交流充电电流大于 16A 的车辆插座内配

备有电子锁，电子锁应在开始供电（K1 与 K2 闭合）前锁定车辆插头并在整个充电流程中（状态 3）保持。如不能锁定，由电动车辆决定下一步操作，例如：继续充电流程，通知操作人员并等待进一步指令或终止充电流程。供电控制装置通过测量检测点 1 或检测点 4 的电压来判断供电插头和供电插座是否完全连接（对于连接方式 A 和 B)。完全连接后，交流充电电流大于 16A 的供电插座内配备有电子锁，供电插座内电子锁应在开始供电（K1 与 K2 闭合）前锁定供电插头并在整个充电流程中（状态 3）保持。如不能锁定，终止充电流程并提示操作人员。锁止功能应符合 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》的相关要求。供电插座和车辆插座应安装电子锁止装置，防止充电过程中的意外断开。

供电设备连接确认检测。如供电设备无故障，并且供电接口已完全连接(对于充电模式 3 的连接方式 A 和 B)，则开关 S1 从连接 12V+状态切换至 PWM 连接状态，供电控制装置发出 PWM 信号。供电控制装置通过测量检测点 1 的电压值或检测点 4 来判断充电连接装置是否完全连接。

车辆连接确认检测。车辆控制装置通过测量检测点 3 与 PE 之间的电阻值来判断车辆插头与车辆插座是否完全连接。未连接时，S3 处于闭合状态，CC 未连接，监测点 3 与 PE 之间的电阻值为无限大；半连接时，S3 处于断开状态，CC 已连接，监测点 3 与 PE 之间的电阻值为 Rc + R4；完全连接时，S3 处于闭合状态，CC 已连接，监测点 3 与 PE 之间的电阻值为 Rc。 车辆控制装置通过测量检测点 2 的 PWM 信号，判断充电连接装置是否已完全连接。

#### 6.5.2.4.2 充电准备就绪要求

在车载充电机自检完成，且没有故障的情况下，并且电池组处于可充电状态时，车辆控制装置闭合开关 S2。供电控制装置通过测量检测点 1 的电压值判断车辆是否准备就绪。当检测点 1 的峰值电压为状态 3 对应的电压值时，则供电控制装置通过闭合接触器 K1 和 K2 使交流供电回路导通。

PWM 信号参数要求。供电设备在各阶段输出的检测点 1 电压、PWM 信号参数（正向幅值、负向幅值、占空比、频率、上升时间、下降时间）应符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中表 A.5 的规定。

#### 6.5.2.4.3 启动和充电阶段互操作性要求

当电动汽车和供电设备建立电气连接后，车辆控制装置通过判断检测点 2 的 PWM 信号占空比确认供电设备的最大可供电能力，并且通过判断检测点 3 与 PE 之间的电阻值来确

认电缆的额定容量。车辆控制装置对供电设备当前提供的最大供电电流值、车载充电机的额定输入电流值及电缆的额定容量进行比较，将其最小值设定为车载充电机当前最大允许输入电流。当车辆控制装置判断充电连接装置已完全连接，并完成车载充电机最大允许输入电流设置后，车载充电机开始对电动汽车进行充电。

充电过程中，车辆控制装置应周期性对检测点 3 与 PE 之间的电阻值（对于连接方式 B 和 C）及检测点 2 的 PWM 信号占空比进行监测，供电控制装置应周期性对检测点 4 及检测点 1（对于充电模式 3 的连接方式 A 和 B）的电压值进行监测。确认供电接口和车辆接口的连接状态，监测周期不大于 50ms。车辆控制装置对检测点 2 的 PWM 信号进行不间断检测，当占空比有变化时，车辆控制装置根据 PWM 占空比实时调整车载充电机的输出功率，检测周期不应大于 5s。

供电设备输出能力要求。对于具备可调节占空比功能的供电设备，分别设置输出占空比在 5%、10%、其最大供电电流对应的占空比，其充电充电状态应符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》表 A.1 的要求；对于不可调节占空比功能的供电设备，设置输出占空比在其最大供电电流对应的占空比，供电设备应能输出其对应最大供电电流。

PWM 占空比变化要求。当 PWM 占空比为 10％时，开关 S2（若车辆配置 S2）保持闭合，车辆应能正常充电，充电电流不大于 6 A；当 PWM 占空比为 90％时，开关 S2（若车辆配置 S2）保持闭合，车辆应能正常充电，充电电流不大于 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中 A.3.7.1 的要求；当 PWM 占空比正常范围内变化时，开关 S2（若车辆配置 S2）保持闭合，车辆应能正常充电，车辆应在检测到 PWM 占空比变化后的 5 s 内调整充电电流，充电电流低于 PWM 占空比所对应的最大电流。

PWM 占空比超限要求。当 PWM 占空比为 6.5%、98.5%，车辆应能在 8 s 内将充电电流减小至最低（＜1 A）。

PWM 频率边界值要求。当 PWM 频率在 1030Hz 和 970Hz 时，开关 S2（若车辆配置 S2）保持闭合，车辆应能正常充电。

输出过流保护要求。供电设备检测车载充电机实际工作电流，当（1）供电设备 PWM 信号对应的最大供电电流≤20A，且车载充电机实际工作电流超过最大供电电流+2A 并保持 5s 时或（2）供电设备 PWM 信号对应的最大供电电流＞20A，且车载充电机实际工作电流超过最大供电电流的 1.1 倍并保持 5s 时，供电设备应在 5s 内断开输出电源并控制开关 S1 切换到+12V 连接状态。

#### 6.5.2.4.4 正常充电结束要求

在充电过程中，当达到车辆设置的结束条件或者驾驶员对车辆实施了停止充电的指令时，车辆控制装置断开开关 S2，并使车载充电机处于停止充电状态。

在充电过程中，当达到操作人员设置的结束条件、操作人员对供电装置实施了停止充电的指令时，供电控制装置应能将控制开关 S1 切换到+12V 连接状态，当检测到 S2 开关断开时在 100 ms 内通过断开接触器 K1 和 K2 切断交流供电回路，超过 3s 未检测到 S2 断开则可以强制带载断开接触器 K1 和 K2 切断交流供电回路。连接方式 A 或 B 时，供电接口电子锁在交流供电回路切断 100ms 后解锁。

#### 6.5.2.4.5 充电时序要求

充电连接控制时序和充电状态流程包括检测点 1 的电压值、检测点 3 的电压值、PWM 信号、充电状态、供电接口锁止状态和车辆接口锁止状态（对于充电电流大于 16A 且采用连接方式 A 或连接方式 B）、充电状态转换的间隔时间，应符合 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中 A.4 和 A.5 的规定。

#### 6.5.2.4.6 非正常充电结束要求

车辆 CC 回路异常状态检测。车辆控制装置通过检测 PE 与检测点 3 之间的电阻值（对于连接方式 B 和 C）来判断车辆插头和车辆插座的连接状态，在充电过程中，当判断开关 S3 由闭合变为断开（状态 B）时，车辆控制装置控制车载充电机在 100 ms 内停止充电，然后断开 S2（若车辆配置 S2）；当判断车辆接口由完全连接变为断开（状态 A）时，车辆控制装置控制车载充电机停止充电，然后断开 S2（若车辆配置 S2）。

车辆 CP 回路异常状态检测。车辆控制装置通过对检测点 2 的 PWM 信号进行检测，在充电过程中，当信号中断时，车辆控制装置控制车载充电机应能在 3s 内停止充电，然后断开 S2（若车辆配置 S2）。

供电 CC 回路异常状态检测。供电控制装置通过对检测点 4 进行检测（对于充电模式 3 的连接方式 A 和 B），在充电前，当检测到供电接口由完全连接变为断开（状态 A），供电控制装置控制开关 S1 切换到+12V 连接状态且且不闭合交流供电回路。在充电过程中，当检测到供电接口由完全连接变为断开（状态 A），供电控制装置控制开关 S1 切换到+12V 连接状态并在 100 ms 内断开交流供电回路。

供电 CP 回路异常状态检测。在充电前，当检测出检测点 1 的电压值为 12V（状态 1）、9V(状态 2) 或者其他非 6V（状态 3）的状态，供电控制装置应在 100ms 控制开关 S1 切换到+12V 连接状态且且不闭合交流供电回路。在充电过程中，当检测出检测点 1 的电压值

为 12V（状态 1）、9V(状态 2) 或者其他非 6V（状态 3）的状态，供电控制装置应在 100ms 断开交流供电回路。

#### 6.5.2.5 非正常充电结束要求

无论是车辆端以及充电设备端，一当充电连接启动，严禁发送互操作要求的对方报文，避免导致造成充电控制的紊乱。

## 6.6 充电接口安全

### 6.6.1 充电接口安全要求

#### 6.6.1.1 充电接口安全设计要求

充电接口设计安全，应从载流安全、温度监测、防止带电插拔、IP 防护等级、接触电阻和压接电阻、接口强度、电缆连接强度、电气安全、电缆组件长度和电缆结构等方面进行安全设计，具体应满足下述要求：

（1）充电接口载流安全、温度监测设计

额定充电电流大于 16A 的应用场合，供电插座、车辆插座均应设置温度监控装置，供电设备和电动汽车应具备温度监测和过温保护功能。如采用温度开关或温度传感器。对于选择温度开关的充电桩，当端子温度达到保护阈值时应停止充电。

（2）防止带电插拔

充电接口需满足 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》中 6.3、GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中 9.3 和 9.6 要求，充电接口应具备锁止装置。当电流大于 16A 时，供电插座和车辆插座端需设计电子锁，并且对于直流充电产品需设计电子锁结构，并设计互锁结构，当由于故障在直流负载下断开时，不应出现危险情况。充电时，车辆接口电子锁锁止，防止带电拔插。车辆插头端应安装机械锁止装置，供电设备能判断机械锁是否可靠锁止。车辆插头安装电子锁止装置，电子锁处于锁止位置时，机械锁应无法操作，供电设备应能判断电子锁是否可靠锁止。当机械锁或电子锁未可靠锁止时，供电设备应停止充电或不启动充电。

（3）IP 防护等级

充电接口应符合 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》中 6.9 防护等级要求，在与配属的保护装置连接后，充电接口防护等级满足 IP54；充电接口配合使用后防护等级满足 IP55。

（4）接触电阻和压接电阻设计

温升需满足 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》中 6.13 要求，端子温升不能超过 50K。

（5）接口强度设计

充电产品强度应满足 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》中 6.21 中车辆碾压要求及 GB/T 11918.1《工业用插头插座和耦合器 第 1 部分：通用要求》中第 24 章中机械强度要求。

（6）电缆连接强度

充电接口应设计电缆固定结构，在受力情况下满足 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》中 7.14 电缆及其连接中要求。

（7）充电接口电气安全

充电接口爬电距离及电气间隙应满足 GB/T 11918.1《工业用插头插座和耦合器 第 1 部分：通用要求》中第 26 章中要求。

（8）充电电缆组件长度设计

电缆长度不应设计过长，导致充电电缆在使用过程中容易扭曲，鼓包。

（9）充电电缆结构设计

充电电缆结构应满足 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》中 9.2 电缆加长组件中的要求，除了电缆组件，不应使用电缆加长组件连接电动汽车和电动汽车供电设备。

#### 6.6.1.2 交直流连接器检测要求

交直流连接器检测应到国家认可具有 CMA、CNAS 检测资质的检测机构进行强制性检测，检测标准依据：

（1）非车载充电机，应符合 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》、GB/T 20234.3《电动汽车传导充电用连接装置 第 3 部分：直流充电接口》标准要求。

（2）交流充电桩，应符合 GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》、GB/T 20234.2《电动汽车传导充电用连接装置 第 2 部分：交流充电接口》标准要求。

#### 6.6.1.3 充电接口制造安全

（1）电产品生产过程中应严格控制插孔中弹片的工艺，确保充电产品接触件接触电阻一致性。

（2）充电电缆组件装配过程中需严格控制电缆组件的压接工艺，确保压接后压接电阻的一致性。

（3）温度传感器装配过程中也需严格控制温度传感器的装配工艺，确保装配后温度传感器检测的稳定性。

#### 6.6.1.4 充电接口使用安全

（1）充电设备应安装在具有遮雨设施的地方。

（2）充电设备安装位置不应有积水。

（3）充电设施不应安装在粉尘严重的地方。

（4）充电应选用具备温度传感器的充电枪，充电机应有高温报警控制及断电功能。

（5）定期对充电连接器进行维护保养，使用前必须总是先检查充电电缆及其接触位置是否有损坏和污染，禁止使用已损坏的充电电缆或车辆插口等。

（6）充电过程中充电枪应交替使用，选择温度较低的充电枪进行充电，选择较为清洁的充电枪进行充电。

（7）充电枪与充电插座充电时，不能斜插。

（8）充电枪充电座插合时，应垂直用力，不应摇晃充电枪。

（9）充电时充电枪电缆必须捋顺，不得扭曲使充电枪座在使用过程中受力。

（10）在充电过程中，必须保证充电操作员对充电过程进行监控，如遇台风、暴雨、冰雹等极端恶劣天气（包含但不限于以上三种），应当立即终止充电过程。

（11）充电过程中，如充电接口持续散发出浓烈的刺激性气味，应立即终止充电过程，第一时间上报设备安全员。

（12）使用结束后，应将充电连接器归位，并将充电枪线捋顺，避免充电枪线盘绕，在充电过程中强行拖拽，造成充电线束扭曲，鼓包。

#### 6.6.1.5 充电接口维护安全

（1）供电插头、车辆插头定期保养及异常检测，包括插头外观异常排查、车辆插头相线之间以及相线与地线之间电压测试、插头相线对地线绝缘电阻及耐压测试、插头端子表面氧化异常排查、插头各相线导体及电缆电阻测试，当出现机械锁钩断裂、端子防触帽热熔、端子孔充满异物、尾部出线松脱、端子位移内缩、端子防触帽脱落时建议更换插头。

（2）供电插座、车辆插座定期保养及异常检测，包括插座外观异常排查、插座相线对地线绝缘电阻及耐压测试（测试前需确认相线之间无电压）、插座应做定期保养（如：异物清理、簧片表面特殊处理、更黄簧片等）、插座插拔力测试、插座电子锁测试、插座

固定螺栓及接地线束螺栓扭矩测试、插座各相线导体及电缆电阻测试，当出现正常镀银端子、端子护套热熔、端子过温泛黄、端子严重过温暗黄、簧片表面布满异物时建议更换插座。

（3）正常使用情况下每周使用高压气枪、毛刷进行清洁，如无条件可以使用无尘布或棉签对充电座插枪进行清洁。如果因意外情况（如充电枪丢弃、掉落在地上），应及时采用上述方法进行清洁。

（4）严禁使用螺丝刀、镊子等尖锐物体触碰充电枪插针和充电座插孔，避免损伤插针及插孔。

### 6.6.2 电气连接防松安全设计

供电设备结构包括外壳、隔板、门的闭锁装置和铰链，连接和拼接等应具有足够的机械强度以承受正常使用和故障条件下所遇到的应力。所有连接和拼接在机械上应牢固，在电气上应连续，避免机械损伤。所有用于外部连接、零部件之间以及零部件内部连接的导线、相互接触的导体或者裸露的带电零部件应具有符合最高工作电压的绝缘保护或绝缘距离。螺钉、螺母、垫圈、弹簧或类似零件应充分固定并能够承受正常使用所产生的机械应力，防止松动引起的跨越附加绝缘或加强绝缘的电气间隙或爬电距离的安全隐患。充电设备内部所有用作电气连接的电缆应满足与线径相匹配的载流能力要求。所有电气连接的电缆端子或接头应符合连接强度要求。与输出连接的充电电缆在超出拉力要求的外力作用下断开时，应保证电缆中保护接地线是线束中最后一个被断开的。充电过程中，当充电线缆被外力拉断时，供电设备应立即停止充电输出，不能存在电击或能量危险。

## 6.7 充电设备试验与安全评价

检测指的是用指定的方法检测测试某种物体（气体、液体、固体）指定的技术性能指标。电动汽车充电设备检测是一个很大的工程体系，具有涉及因素多、涉及面较广以及动态性强的特点。通过开展试验检测，可以探索和确定单一或多个环境因素对充电的影响，考核充电设备的环境适应性；验证充电设备是否符合规定的环境要求，充电产品是否合格，为运营商和用户对充电设备接收或拒收的决策依据；另外还可以检测出不合格的或有潜在缺陷的充电产品，促进制造商提高设计工艺、改进技术，从而促进充电设备的可靠性、安全性。

目前国内对于试验检测环节的标准主要有国家标准 GB/T 34657.1《电动汽车传导充电互操作性测试规范 第 1 部分：供电设备》、GB/T 34658《电动汽车非车载传导式充电机与

电池管理系统之间的通信协议一致测试》，在编制《电动汽车供电设备安全要求及试验规范》（报批阶段），NB/T 33008.1《电动汽车充电设备检验试验规范 第 1 部分：非车载充电机》、NB/T 33008.2《电动汽车充电设备检验试验规范 第 2 部分：交流充电桩》，另外国家电网公司也发布了相关的充换电设施检测系列企业标准。这些标准主要在现行的国家标准 GB/T 18487.1《电动汽车传导充电系统 第 1 部分：通用要求》、GB/T 20234.1《电动汽车传导充电用连接装置 第 1 部分：通用要求》、GB/T 20234.2《电动汽车传导充电用连接装置 第 2 部分：交流充电接口》、GB/T 20234.3《电动汽车传导充电用连接装置 第 3 部分：直流充电接口》、行业标准 NB/T 33001《电动汽车非车载传导式充电机技术条件》、NB/T 33002《电动汽车交流充电桩技术条件》的要求为基础建立并扩展充电安全试验方法与评价方法。

### 6.7.1 直流充电设备检测要求

目前，国内非车载充电机检测标准基本都是符合性检测型标准，即标准规定低温、高温、湿热、温升、电击防护、绝缘电阻、工频耐压、稳流精度、电磁兼容、机械强度、噪声等电气、机械和安全性能方面的试验项目，用以确保非车载充电机在使用时的安全性。结合我国电动汽车产业发展及安全标准现状，依据我国各个地区的环境差异，及时对非车载充电机运行条件及部分检测指标进行相对调整和补充完善。

（1）一般检查

一般检查主要包括检查非车载充电机及其零部件的外观、标志、基本构成、机械开关设备、防盗措施、充电模式和连接方式、电缆管理及贮存、电气隔离等。主要通过目测或简单的试验来确认非车载充电机及其零部件是否满足结构要求。

（2）功能试验

功能试验主要包括充电控制功能试验、通信功能试验、绝缘检测功能试验、直流输出回路短路检测功能试验、车辆插头锁止功能试验、预充电功能试验、显示功能试验、输入功能试验、计量功率试验、急停功能试验。

（3）安全要求试验

安全要求试验主要包括输入过压保护试验、输入欠压保护试验、输出过压保护试验、输出短路保护试验、过温保护试验、开门保护试验、启动急停装置试验、输入电流过冲试验、蓄电池反接试验、防逆流功能试验、接触器粘连试验。

（4）电击防护试验

电击防护试验主要包括直接接触防护试验、动力电源输入失电试验。电击是电流通过

人体时引起的病理生理效应。电流通过人体时主要对人体的肌肉、血液循环和呼吸的功能产生影响，有时还引起严重的灼伤，对人体伤害的程度与电流的大小、电流通过人体的部位以及电流持续时间的长短有关。

（5）电气间隙和爬电距离试验

爬电距离是沿绝缘表面测量的两个导电部件之间，在不同使用条件下，导体周围的绝缘材料带电，导致绝缘材料的带电区域出现带电现象。电气间隙是测量两个导电部件之间或导电部件与设备保护接口之间的最短距离。也就是说，在保证电气性能的稳定性和安全性的前提下，空气可以达到最短的绝缘距离。根据非车载充电机的额定绝缘电压等级对应不同的电气间隙和爬电距离，小母线、汇流排或不同级的裸露的带电导体之间，以及裸露的带电导体与未经绝缘的不带电导体之间的电气间隙不小于 12 mm，爬电距离不小于 20 mm。

（6）电气绝缘性能试验

电气绝缘性能试验，主要包括绝缘电阻试验、工频耐压试验、冲击耐压试验。

为衡量绝缘材料对电流的“限制”能力，引入绝缘电阻的概念，绝缘电阻是指用于表征绝缘体阻止电流流通的能力。绝缘电阻太低，泄露电流会很大，不但造成电能的浪费，还会引起发热而损坏绝缘体。因此绝缘电阻是表征绝缘体特性的基本参数之一。

工频交流耐压试验是鉴定电力设备绝缘强度最有效和最直接的方法，是预防性试验的一项重要内容。此外，由于交流耐压试验电压一般比运行电压高，因此通过试验后，设备有较大的安全裕度，因此交流耐压试验是保证电力设备安全运行的一种重要手段。

冲击耐压试验即可用于研究充电机遭受大气过电压（雷击）时的绝缘性能，又可用于研究电力设备遭受操作过电压时的绝缘性能。

（7）接地试验

检查充电机金属壳体的接地螺栓直径不应小于 6 mm，且有接地标志；充电机的门、盖板、覆板和类似部件，应采用保护导体将这些部件和充电机主体框架连接，用量规或游标卡尺测量保护导体的截面积不应小于 2.5 $mm^2$；通过电桥、接地电阻试验仪或数字式低电阻试验仪测量，充电机内任意应该接地的点至总接地之间的电阻不应大于 0.1 Ω，测量点不应少于 3 个，如果测量点涂敷防腐漆，需将防腐漆刮去，露出非绝缘材料后再进行试验，接地端子应有明显的标志；充电机内部工作地与保护地应相互独立，应分别直接连接到接接地导体（铜排）上，不应在一个接地线中串接多个需要接地的电气装置。

（8）充电输出试验

针对目前充电机不同的输出特性，给出具备恒功率和不具备恒功功能的充电机试验点，充电机输出试验主要包括最大恒功率输出试验、功率控制试验、低压辅助电源试验、稳流精度试验、稳压精度试验、电压纹波因数试验、电流纹波试验、输出电流设定误差试验、输出电压设定误差试验、限流特性试验、限压特性试验、输出电流响应时间试验、输出电流停止速率试验、启动输出过冲试验、输出电流测量误差试验、输出电压测量误差试验、测量值更新时间试验、效率试验、功率因数试验。

（9）待机功耗试验

在充电机不连接试验系统且无人员操作，仅保留其后台通讯、状态指示灯等基本功能的状态，测量充电机的待机功耗不应大于 N×50 W。

（10）协议一致性试验

按照 GB/T 34658《电动汽车非车载传导式充电机与电池管理系统之间的通信协议一致性测试》规定的方法，检查非车载充电机的每个车辆接口的通信协议应符合标准要求。

（11）控制导引试验

按照 GB/T 34657.1《电动汽车传导充电互操作性测试 第 1 部分：供电设备》规定的方法，检查非车载充电机的每个车辆接口的控制导引功能应符合标准要求且相互独立。主要包括充电控制状态试验、充电连接控制时序试验、控制导引电压限值试验、通信中断试验、保护接地导体连续性试验、连接检测信号断开试验、输出冲击电流试验、蓄电池电压与通信报文不符试验、蓄电池电压超过充电机范围试验、蓄电池二重保护功能试验、车辆最高允许充电总电压不匹配试验、充电需求大于蓄电池参数试验。

（12）噪声试验

噪声是各种频率和不同强度的杂乱声音的组合。考核非车载充电机在强噪声场中的工作性能和耐强噪声的能力，测定设备对强噪声的响应。

（13）内部温升试验

电机在机电能量转换过程中所产生的损耗最终转化为电机各部件的温升，电动汽车用驱动电机的单机容量较大，电机体积较小、电机散热环境恶劣，其运行时会产生较高的单位体积损耗，带来严重的温升问题，从而影响电机的寿命和运行可靠性。对充电机内部包括动力电源输入电流所流经的回路，如接线端子、输入断路器、输入接触器等；功率变换单元及其内部元器件、输入输出端子；直流输出电流所流经的回路，如接线端子、直流熔断器、直流接触器、功率电阻、电流采样分流器、车辆插头等安装测温元件。温度可用融化颗粒、变化指示器或热电偶进行测量。

（14）允许温度试验

在充电过程中，检查充电接口在额定负载下，充电机手握可接触部分、可触及但非手握部分的金属材料和非金属材料的温度应符合标准要求。

（15）机械强度试验

采用不同的锤对电气设备进行撞击试验都可能产生机械应力。在严酷度条件下对充电机实施撞击，可以评定充电机的坚固度。

（16）防护试验

防护试验主要包括防尘试验、防水试验、防盐雾试验、防锈（防氧化）试验。防尘试验用于防止固体异物进入壳内设备，防水试验用于防止由于水进入壳内对设备造成有害影响，防盐雾试验用于提高充电机内印刷线路板、接插件等关键部件的防盐雾能力，防锈（防氧化）试验用于要求充电机铁质外壳、暴露的铁质支架、零件以及非铁质的金属外壳等代表性试样进行防锈处理。

（17）环境试验

环境试验主要包括低温试验、高温试验、交变湿热试验。环境试验的目的仅限于用来确定非车载充电机在低温、高温湿热环境下使用的能力。测试非车载充电机能否在低温、高温条件下放置足够长时间以达到温度稳定，以及在高湿度与温度循环变化组合以及表面产生凝露的条件下使用、运输和贮存的适应性。防止由于温度改变而对非车载充电机产生有害作用。

（18）电磁兼容性试验

电磁兼容性试验主要包括，静电放电抗扰度试验、射频电磁场辐射抗扰度试验、电快速瞬变脉冲群抗扰度试验、浪涌（冲击）抗扰度试验、辐射骚扰试验、传导骚扰试验、谐波电流试验。

静电放电抗扰度试验，用以评估电动汽车非车载充电机遭受静电放电时的性能，以及人体靠近充电机可能发生的静电放电现象。

射频电磁场辐射抗扰度试验，用以评估电磁辐射以某种方式对大多数电子设备的影响。

电快速瞬变脉冲群抗扰度试验是为了评估非车载充电机的供电电源端口、信号、控制和接地端口在受到电快速瞬变（脉冲群）干扰时的性能。

浪涌（冲击）抗扰度试验，用以找出充电机在规定的工作状态下时，对由开关或雷电作用所产生的有一定危害电平的浪涌(冲击)电压的反应。

辐射骚扰试验和传导骚扰试验避免非车载充电机影响无线电广播和电信业务，又可以允许其他设备在合理的距离处按预定的要求工作。

谐波电流试验，电动汽车充电机的整流装置是电动汽车充电站接入电力系统产生谐波的主要原因。所谓谐波，就是对周期性非正弦电量进行傅里叶级数分解，除了得到频率与工频相同的分量（该分量称为基波），还得到一系列大于工频的分量，这部分分量称为谐波。和许多其他形式的污染一样，谐波的产生影响整体（电气）环境，而且影响范围可能波及到距其源点较远之处。

### 6.7.2 交流充电设备检测要求

目前，国内交流充电桩检测标准基本都是符合性检测标准，包括了电气、机械和安全性能方面的试验项目，用以确保交流充电桩在使用时的安全性。目前交流充电桩的技术仍处于不断地进步和更新之中，特别是在交流充电桩与电网互动环节提出了有序充电的需求，新的功能和技术要求处于起步阶段，要不断跟踪电动汽车新技术的发展，确保标准的技术内容先进、可操作性。

（1）一般检查

一般检查主要包括检查交流充电桩及其零部件的外观、标志、基本构成、机械开关设备、防盗措施、充电模式和连接方式、电缆管理及贮存等。主要通过目测或简单的试验来查看电动汽车交流充电桩及其零部件是否满足结构要求。

（2）功能试验

功能试验主要包括通信功能试验、充电连接装置检查、锁止装置检查、显示功能试验、输入功能试验、计量功能试验。

（3）安全要求试验

安全要求试验主要包括输出短路保护试验、过温保护试验、急停保护试验、接触器粘连监测试验、接触电流试验、漏电保护试验。

（4）内部温升试验

对交流充电桩内部包括动力电源输入电流所流经的回路，如熔断器外壳、母线连接处、铜——铜、铜搪锡——铜搪锡、铜镀银——铜镀银等安装测温元件。温度可用融化颗粒、变化指示器或热电偶进行测量。

（5）允许温度试验

在充电过程中，检查充电接口在额定负载下，充电机手握可接触部分、可触及但非手握部分的金属材料和非金属材料的温度应符合标准要求。

（6）电击防护试验

电击防护试验，主要包括直接接触防护试验、开门保护试验、动力电源输入失电试验。

（7）电气间隙和爬电距离试验

爬电距离是沿绝缘表面测量的两个导电部件之间，在不同使用条件下，导体周围的绝缘材料带电，导致绝缘材料的带电区域出现带电现象。电气间隙是测量两个导电部件之间或导电部件与设备保护接口之间的最短距离。也就是说，在保证电气性能的稳定性和安全性的前提下，空气可以达到最短的绝缘距离。根据非车载充电机的额定绝缘电压等级对应不同的电气间隙和爬电距离，小母线、汇流排或不同级的裸露的带电导体之间，以及裸露的带电导体与未经绝缘的不带电导体之间的电气间隙不小于 12 mm，爬电距离不小于 20 mm。

（8）绝缘性能试验

电气绝缘性能试验，主要包括绝缘电阻试验、工频耐压试验、冲击耐压试验。

通常讲的绝缘并非完全的电气隔离，为衡量绝缘材料对电流的“限制”能力，引入绝缘电阻的概念，绝缘电阻是指用于表征绝缘体阻止电流流通的能力。绝缘电阻太低，泄露电流会很大，不但造成电能的浪费，还会引起发热而损坏绝缘体。因此绝缘电阻是表征绝缘体特性的基本参数之一。

工频交流耐压试验是鉴定电力设备绝缘强度最有效和最直接的方法，是预防性试验的一项重要内容。此外，由于交流耐压试验电压一般比运行电压高，因此通过试验后，设备有较大的安全裕度，因此交流耐压试验是保证电力设备安全运行的一种重要手段。

冲击耐压试验即可用于研究充电机遭受大气过电压（雷击）时的绝缘性能，又可用于研究电力设备遭受操作过电压时的绝缘性能。

（9）接地试验

检查交流充电桩金属壳体的接地螺栓直径不应小于 6 mm，且有接地标志；充电桩的门、盖板、覆板和类似部件，应采用保护导体将这些部件和充电桩主体框架连接，用量规或游标卡尺测量保护导体的截面积不应小于 2.5 $mm^2$；通过电桥、接地电阻试验仪或数字式低电阻试验仪测量，充电桩内任意应该接地的点至总接地之间的电阻不应大于 0.1 Ω，测量点不应少于 3 个，如果测量点涂敷防腐漆，需将防腐漆刮去，露出非绝缘材料后再进行试验，接地端子应有明显的标志；充电桩内部工作地与保护地应相互独立，应分别直接连接到接接地导体（铜排）上，不应在一个接地线中串接多个需要接地的电气装置。

（10）待机功耗试验

对于一机双充以下的交流充电桩，仅保留其后台通讯、状态指示灯等基本功能的状态，测量充电桩的待机功耗不应大于 15 W。

（11）控制导引试验

按照 GB/T 34657.1《电动汽车传导充电互操作性测试 第 1 部分：供电设备》规定的方法，检查交流充电桩的每个供电接口（连接方式 B）或车辆接口（连接方式 C）的控制导引功能应符合标准要求且相互独立。主要包括充电控制状态试验、充电连接控制时序试验、控制导引电压限值试验、保护接地导体连续性试验、控制导引信号异常试验、断开开关 S2 再闭合试验、过流试验。

（12）噪声试验

噪声是各种频率和不同强度的杂乱声音的组合。考核交流充电桩在强噪声场中的工作性能和耐强噪声的能力，测定设备对强噪声的响应。

（13）机械强度试验

采用弹簧锤对电气设备进行撞击试验都可能产生机械应力。在严酷度条件下对交流充电桩实施撞击，可以评定交流充电桩的坚固度。

（14）防护试验

防护试验主要包括防尘试验、防水试验、防盐雾试验、防锈（防氧化）试验。防尘试验用来检测交流充电桩防止固体异物进入壳内的能力，防水试验用于检测设备防止由于水进入壳内对设备造成有害影响的能力。防盐雾试验用于提高充电桩内印刷线路板、接插件等关键部件的防盐雾能力，防锈（防氧化）试验用于要求充电桩铁质外壳、暴露的铁质支架、零件以及非铁质的金属外壳等代表性试样进行防锈处理。

（15）环境试验

环境试验主要包括低温试验、高温试验、交变湿热试验。环境试验的目的仅限于用来确定非车载充电机在低温、高温湿热环境下使用的能力。测试交流充电桩能否在低温、高温条件下放置足够长时间以达到温度稳定，以及在高湿度与温度循环变化组合以及表面产生凝露的条件下使用、运输和贮存的适应性。防止由于温度改变而对交流充电桩产生有害作用。

（16）电磁兼容性试验

电磁兼容性试验主要包括，浪涌（冲击）抗扰度试验、电快速瞬变脉冲群抗扰度试验、射频电磁场辐射抗扰度试验、静电放电抗扰度试验、辐射试验。

浪涌（冲击）抗扰度试验，用以找出充电机在规定的工作状态下时，对由开关或雷电

作用所产生的有一定危害电平的浪涌(冲击)电压的反应。

电快速瞬变脉冲群抗扰度试验是为了评估交流充电桩的供电电源端口、信号、控制和接地端口在受到电快速瞬变（脉冲群）干扰时的性能。

射频电磁场辐射抗扰度试验，用以评估电磁辐射以某种方式对大多数电子设备的影响。

静电放电抗扰度试验，用以评估电动汽车交流充电桩遭受静电放电时的性能，以及人体靠近充电机可能发生的静电放电现象。

辐射试验避免交流充电桩影响无线电广播和电信业务，又可以允许其他设备在合理的距离处按预定的要求工作。

### 6.7.3 充电设备性能安全评价

#### 6.7.3.1 全生命周期检测

全生命周期检测强调对充电设备全寿命发展过程实施持续不断、协调统一的检测，保证各个阶段的活动前后衔接，各个阶段决策的一致性，在满足功能性能指标需求的前提下，达到充电设备在全寿命周期内检测投入人力物力最优。适用于生命周期方法的研究对象必须符合两个条件，即具有生命的特征和存在的有限性。电动汽车充电设施就符合这两个条件，由此以电动汽车充电设施为研究对象，创新性地将全生命周期方法应用到电动汽车充电设施的检测中。

充电设备的全生命周期检测是指从设备的规划、论证、研发、量产、出厂、收货、投运、使用直到充电设备折旧后的淘汰或报废前的整个过程中对充电设备进行的全面合理的检测，建立统一的检测明细表，采用工作流的技术，将充电设备生命周期内各环节产生的数据流串起来，形成充电设备从研发到运维整个过程的闭环检测，动态调整每个充电设备的检测项目与需求，最终到达确保充电设备的质量与技术指标达标的目的。充电设备的全生命周期检测大体分为三个阶段：充电设备的前期检测、充电设备的中期检测、充电设备的后期检测。

（1）设备的前期检测。充电设备前期检测的内容主要包括设备研发阶段的检测与设备量产前的型式试验阶段检测，前期检测以技术上先进、经济上合理、生产上适用、产品满足检测标准为原则，充电设备前期检测的意义重大：①提高设备的投资效率，因为它在整个生命周期检测中投资比重最大；②决定了设备的质量和水平，确保设备的使用效率。在研发中，对充电设备而言，在研发的检测中遵循电气性能、机械性能、安全性能等检测顺序，确保在型式检测前满足标准的要求；在型式检测中，要完成检测标准中的所有规定

项目，而且指标满足标准要求。

（2）充电设备的中期检测。充电设备中期检测的内容包括出厂阶段检测与到货阶段检测。中期检测确保了充电设备在量产及运输过程中的质量技术达标，为将来设备的运行打下良好的基础。充电设备的量产过程中，势必会存在所生产设备的优劣之分，也会出现技术不达标的充电设备，出厂阶段检测的目标就在于剔除不满足技术指标的设备，保证出厂设备的合格率；设备在运输、拆卸过程中面临着各种挑战，导致到货时设备存在不合格情况，因此有必要对设备进行到货试验。

（3）充电设备的后期检测。充电设备后期检测即为设备安装使用阶段的检测，包括投运阶段的检测与运维阶段的检测。这期间的检测比较繁杂且时间跨度大，占充电设备全生命周期的大部分时间，是充电设备全生命周期检测的重要环节。后期检测确保了充电设备的正常运行，同时排除设备在运行期间具有安全方面隐患，因此在充电设备投运和运维阶段进行检测具有重大意义。正确的使用和维护、保养设备可使设备保持良好的状态，达到检测的各项技术指标，减少或防止突发性故障和非正常停运，使充电设备发挥最大效能，提高仪器设备的使用效率。

充电设备一旦报废，对充电设备进行检测即不具有意义，因此从生命周期该阶段开始不进行充电设备的检测。

充电设备生命全周期检测坚持检测思路的连贯性和一致性，不仅要注重充电设备的功能性检测，更要注重检测项目的规划与分配，通过对充电设备资源的合理规划，针对设备不同生命期间对检测项目进行有效合理的配置，这样不仅使充电设备满足了各阶段的性能要求，还避免了充电设备检测项目的重复性，减小了充电设备检测的成本，满足其经济性。

#### 6.7.3.2 性能评价体系

建立充电设备性能评价体系是判别充电设备性能状态的有效方法，充电设备性能评价体系内的每一个评价指标都能够衡量被评价的充电设备的某一方面性能的优劣，因此所建立的性能评价体系的优劣会直接影响充电设备性能状态的判别结果的正确率。为了建立科学的充电设备性能评价体系，全方位反映被评价的充电设备的性能状态，性能评价体系的建立必须遵守完整性原则、科学性原则、客观性原则、可操作性原则、独立性原则、定性分析与定量分析相结合原则。

(1) 完整性原则。评价体系必须能够全面地对被评价对象进行综合评价。评价对象不同，所选择的评价指标就不同，必须根据评价对象的自身特点选择评价指标。但选择的评价指标不能过于单一，必须涵盖各个方面，要能够从不同的方面反映被评价对象的主要情

况，从而建立一个有层次的指标系统，使评价体系成为一个有机整体。

(2) 科学性原则。为建立科学的评价指标体系，评价指标必须科学而客观地反映评价对象的各个方面的状况。任何评价都是围绕着评价目标而进行的，评价的科学性就要求评价者在一定的约束条件下，科学合理地衡量被评价对象，实现评价目标。评价指标的科学性表现为评价指标符合客观实际，符合已被实践证明的科学理论。

(3) 客观性原则。评价指标的选择要以客观事实为基础，不能主观臆断。在经过大量科学分析，相关资料文献查阅的基础上，建立层次分明的评价体系。充电设备的各个评价指标是在查阅现有的国内外相关标准及大量科学分析的基础上，并征询有关技术人员的意见后确定的。

(4) 可操作原则。评价指标应是可测量、可比较的，即可以对评价指标进行定性或定量测量，且同类指标可进行相互比较。选择的评价指标必须含义明确，相关数据资料容易获得，计算简单可行。

(5) 独立性原则。各个评价指标之间应尽可能相互独立，尽量避免出现重复考虑评价对象某一方面的情况，使评价体系简洁，降低评价指标的冗余程度，使评价结果更加准确而不失真。

(6) 定性分析与定量分析相结合原则。为全面反映被评价对象的情况，评价指标中应有定性指标与定量指标，并将定性指标量化，为采用定量评价的方法奠定基础。

## 6.8 充电设备制造

充电设备的产品质量是保证充电安全的基础条件，充电设备制造生产厂商应按照ISO9001，IATF16949 的相关要求，采用过程方法建立质量管理体系，形成制造生产质量管理文件和流程制度，加以实施和保持，并持续改进，以满足产品质量、环境和职业健康安全管理的法律法规要求。

充电设备制造的质量管理体系应从设计开发质量，供应商及物料质量，生产制造过程质量，检验测试质量，流程体系质量等方面进行全流程管理，具体包括以下质量流程体系：

1）设计开发项目管理

有效开展产品开发工作，确保产品满足顾客和国家标准要求，提升产品质量；提供新产品开发的标准化作业流程，以作为产品开发之依据。

2）产品制造管理程序

确保产品制造过程受控，确保质量体系及产品持续有效，适用于公司批量生产的产品。

3）生产计划和交付管理程序

通过对销售订单/销售预测订单的汇总、评审，规划销售计划、生产计划、物料需求计划、采购交货计划，并促进所有计划的有效进行，确保 100%按时交付订单。适用于销售订单/销售预测订单的汇总、评审，规划销售计划、生产计划、物料需求计划、采购交货计划的编制与管理实施。

4）项目工程管理程序

全面贯彻落实国家、地方、行业相关的法律法规，促进公司工程技术管理工作正常有序进行，为企业的施工生产经营活动提供技术保障，促进企业的工程管理工作标准化、规范化，加强建设工程质量管理，保证工程项目施工的正常运行和项目管理技术、质量目标的实现。

5）运维服务管理程序

以建立优质的工程服务体系为目标，完善工程服务制度，提高公司运维服务质量。

6）文件与记录控制程序

规范公司内各类受控文件/记录的申请、编写、发行、使用、修订、废止、管理维护等作业活动。为维持各项文件/记录的识别与收集、归档保管与维护、查找、回收与销毁处理等程序，以证明达成系统有效运作。

7）人力资源管理程序

为使公司人力资源维持稳定发展，建立公平、公开、公正且有效率的人力资源制度，增进员工专业知识与工作技能，促使本公司选获和培育优秀人才。

8）设备工装管理程序

为规范设备从申请到报废全过程、全寿命管理，保障设备正常运行及合理使用。

9）采购管理程序

使用合理成本在最需要的时间与地点，以最高的效率获得最适当数量，负荷规格与质量的材料，顺利交给需要部门使用；同时建立书面程序，以确保采购产品负荷规格要求。

10）供应商管理程序

为保证新供应商满足开发要求，保证产品质量，为公司建立和发展稳定良好的供应商开发体系，及供应商日常管理。

11）物流管理程序

从供应商材料、物流、厂内物流、交付物流各个环节对物流管理过程进行控制，确保物流管理过程符合质量管理体系要求。

12）仓储管理程序

为规范仓库现场管理，加强公司仓库安全管理工作，确保仓库物料准确性以及确保仓库人员与物品安全

13）实验室管理程序

为规范公司内外实验室的管理及测试方法。

14）测量设备管理程序

对检验、测量和试验设备的选型、校准。维修保养以及管理进行有效的控制，以保证所用设备的测量精度和准确性满足使用要求。

15）IT 管理程序

为了确保公司的信息系统正常运维，确保各部门在使用信息系统过程中的问题能够得到及时解决，统一规范信息中心和各部门间的工作流程。

16）不合格品管理程序

对可疑和不合格产品或材料进行标识、记录、评审、隔离和处置，是来料、制程等阶段所产生的不合格品得到有效控制，防止不合格品被误用，确保不合格品不流入下一个流程。

17）制程、成品检验

确保进料、制程、成品及出货品质得到有效管控，从而满足客户要求。

18）进料检验管理程序

定义公司物料进料检验程序及仓库材料复检检验程序，以确保进料品质特性符合公司要求，且对进料数量及纳期进行管制，使之不影响工厂生产进度，确保来料品质符合规格要求，最终使产品品质符合客户要求。

19）管理程序

对 SPC 统计过程受控，确保组织对所有新制造进行过程研究，验证过程能力，并为过程控制提供附加输入。

20）体系审核管理程序

确保系统审核有效实施，验证公司管理系统实施的有效性和符合性。

21）过程审核管理程序

通过对产品及过程的质量能力进行评定，识别缺陷并采取措施，改进过程、优化体系。

22）产品审核管理程序

审核已通过最终检验并准备交付的产品是否与客户提供的特性数据一致，从而判断产

品的质量并追溯质量缺陷原因。

23）管理评审管理程序

对公司质量管理体系的持续适宜性、充分性和有效性进行评审，确保体系及其运行效果不断改善。

24）持续改进管理程序

为确保本公司的质量、职业健康、安全和环境管理体系运行的有效性，切实做到持续改进。

## 6.9 充电设施建设

充电设施安全生产管理必须坚持安全第一、预防为主的方针，建立健全安全生产的责任制度和群防群治制度。工程设计、施工应当符合按照国家规定制定的建筑安全规程和技术规范，保证工程的安全性能。

### 6.9.1 充电场站建设规划充电站选址布局

（1）充电站选址应与城市中低压配电网的规划和建设密切结合，以满足供电可靠性、电能质量和自动化的要求。

（2）充电站的规划宜充分利用就近的供电、交通、消防、给排水及防排洪等公用设施，与党政机关办公楼、中小学校、幼儿园、医院门诊楼和住院楼、大型图书馆、文物古迹、博物馆、大型体育馆、影剧院等重要或人员密集的公共建筑应具有合理的安全距离。

#### 6.9.1.2 充电站环境要求

（1）充电站不应靠近有潜在火灾或爆炸危险的地方，当与有爆炸危险的建筑物毗邻时，应符合现行国家标准《爆炸危险环境电力装置设计规范》GB 50058 的有关规定。

（2）充电站不宜设在多尘或有腐蚀性气体的场所，当无法远离时，不应设在污染源盛行风的下风侧。

（3）充电站应满足环境保护和消防安全的要求，与其他建筑物、构筑物之间的防火间距应满足《火力发电厂与变电站设计防火规范》GB 50229、《建筑设计防火规范》GB 50016 的有关要求。

（4）充电站选址应避开室外地势低洼、易积水的场所、易发生次生灾害和有剧烈振动的地点。

（5）充电区域应具备一定的通风条件。

（6）充电站的环境温度应满足为电动汽车动力蓄电池正常充电的要求。

（7）可能发生严重潮湿天气的区域，应具有对空气湿度的监测和处理的设备和手段。

（8）充电设备安装在室内时，为防止温度过高，宜安装通风设施。

（9）充电设备宜安装在距地面一定高度的地方，满足防雨、防积水要求。

### 6.9.2 场站安全设计要求

（1）场站布局

场站包括站内建筑、站内外行车道、充电区、临时停车区及供配电设施等；站区总布置应满足总体规划要求，并应符合站内工艺布置合理、功能分区明确、交通便利和节约用地的原则；场站内建筑的布置应方便观察充电区域；场站的进出站道路应与站外市政道路顺畅衔接。

（2）设备布局

充电设备的布置不应妨碍其他车辆的充电和通行，同时应采取保护充电设备及操作人员安全的措施。电气设备的布置应遵循安全、可靠、适用的原则，并便于安装、操作、搬运、检修和调试。发生严重充电安全事故时，保证其他用户能够有足够的逃生时间；事故发生后快速实现多级联动救援，如消防、医疗等，保证生命及财产安全。

（3）环境保护和消防安全的要求

充电站的建设（构）筑物火灾危险性分类应符合现行国家标准《火力发电厂与电变站设计防火规范》GB 50229 和《建筑设计防火规范》GB 50016 的有关规定。充电站内的充电区和配电室的建（构）筑物与站内外建筑物之间的防火间距应符合现行国家标准《建筑设计防火规范》GB 50016 和《高层民用建筑设计防火规范》GB 50045 的有关规定，充电站建（构）筑物相应厂房类别划分应符合表 4.9-1 的规定。

（4）充电站不应靠近有潜在火灾或爆炸环境的地方

当与有爆炸危险源建筑物毗邻时，应符合现行国家标准《爆炸危险环境电力装置设计规范》GB 5058 的有关规定。

（5）充电站建设在加油加气站

建设时应符合现行国家标准《汽车加油加气站设计与施工规范》GB 50156，充电桩布局在辅助服务区中。箱式变电站、配电箱、充电桩划分为丙、丁、戊类，其与加油、加气储罐、设备的安全间距应符合表 4.9 2~4 的规定；

（6）对于采用低压 0.38kV 供电的充电场站，采用电力电缆供电时，供电距离不宜超过 200m；

（7）就近布置要求

设备外轮廓距离充电车位边缘的净距不宜小于 0.4m。充电设备的布置不应妨碍其他车辆的充电和通行，同时应采取保护充电设备及操作人员安全的措施。

（8）充电站内道路的设置应满足消防及服务车辆通行的要求

充电站的出入口不宜少于 2 个，当充电站的车位不超过 50 个时可设置一个出入口，入口和出口宜分开设置，并应明确指示标识。

（9）充电站内双列布置充电位时，中间行车道宜按行驶车型双车道设置。单列布置充电车位时，行车道宜按行驶车型双车道设置。

（10）充电场地建设应确保正在进行充电的车辆与其它车辆之间留有 3m 以上的安全距离。

### 6.9.3 建筑物安全

（1）抗震、防雨、防风、防雷设计要求

建筑设计应满足《建筑结构荷载规范》GB 50009、《混凝土结构设计规范》(2015 年版)GB 50010、《建筑地基基础设计规范》GB 50007、《建筑抗震设计规范》(2016 年版)GB 50011、《建筑物防雷设计规范》GB 50057 等国家和行业规范的要求，确保安全适用，经济合理；

（2）停车防撞设计要求

为确保充电基础设施安全，应设置有效的防止电动汽车撞击充电设施的措施。

### 6.9.4 变配电要求

1、变电站总体设计满足安全性要求

变电站不应靠近有潜在火灾或爆炸危险的地方，当与有爆炸危险的建筑物毗邻时，应符合现行国家标准《爆炸危险环境电力装置设计规范》GB 50058 的有关规定。箱式变电站安全距离应满足国家标准《建筑设计防火规范》GB50016。

2、高低压变压器容量配置合理，设计满足安全性要求

（1）变压器容量不宜大于 1250kVA，当用电设备容量较大、负荷集中且运行合理时，可选用较大容量的变压器。

（2）变压器应选用难燃型或不燃型，外壳防护等级不应低于 IP2X。

（3）变压器箱体、支架、基础型钢及外壳应分别单独与保护导体可靠连接，紧固件及防松零件齐全。

（4）中低压配电系统宜采用单母线或单母线分段接线；低压接地系统宜采用 TN-S 系统。

（5）低压进出线开关、分段开关宜采用断路器；来自不同电源的低压进线断路器和低压分段断路器之间应设机械闭锁和电气联锁装置，防止不同电源并联运行。

（6）低压进线断路器宜具有短路瞬时、短路短延时、长延时和接地保护功能。宜设置分励脱扣装置，不宜设置失（低）压脱扣装置。

（7）对非车载充电机、监控装置以及重要用电设备，宜采用放射式供电；

（8）开关柜宜选用小型化、无油化、免维修或少维护的产品。

（9）低压三相回路宜选用五芯电缆，单相回路宜选用三芯电缆，且电缆中性线截面应与相线截面相同。

（10）动力和照明宜共用变压器。

3、线缆选择合理，走线路径优化，敷线合理安全

变电站靠近充电设施，低压电缆尽量最短。电力电缆宜选用铜芯交联聚乙烯绝缘类型，宜选用阻燃电缆。电缆敷设存在可能受到机械外力损伤、振动、浸水及腐蚀性或污染物质等损害时，应采取防护措施。电缆敷设不得存在绞拧、铠装压扁、护层断裂和表面严重划伤等缺陷。

4、配电箱选择符合国家强制验收标准

（1）配电箱内应有可靠的防电击保护，装置内保护接地导体排应有裸露的连接外部保护接地导体的端子，并应可靠连接。当设计未做要求时，连接导体最小截面积应符合现行国家标准《低压配电设计规范》GB 50054 的规定。

（2）配电箱基础应可靠接地。

### 6.9.5 附属建筑

#### 6.9.5.1 必要的雨棚、电缆沟等附属建筑

为保证充电设施及充电过程安全，充电基础设施建设应配建必要的雨篷等附属设施，其设计及施工要求满足国家及行业相关规范标准要求。

#### 6.9.5.2 配备有效防雷接地系统

建筑及充电设施应采取有效的防雷接地措施，并满足《建筑物防雷设计规范》GB 50057 等国家和行业规范的要求。

### 6.9.6 清晰明确的安全标识

充电设施应设置明显的安全标志，确保运营过程流程顺畅、安全可靠。

### 6.9.7 弱电与监控系统

#### 6.9.7.1 弱电设备设计满足安全性要求

弱电设备应满足防雷、接地、防火、防停电、防静电等方面要求，保证弱电系统正常运行。

#### 6.9.7.2 充电监控

（1）充电监控系统应采集充电设备工作状态、温度、故障信号、功率、电压、电流、电能量等信息。

（2）充电监控系统应实现向充电设备下发控制命令，遥控起停、校时、紧急停机、远方设定充电参数等控制调节功能。

#### 6.9.7.3 供电监控

（1）供电监控系统应采集充电站供电系统的开关状态、保护信号、电压、电流、有功功率、无功功率、功率因数、电能计量信息等。

（2）供电监控系统应能控制供电系统负荷开关或断路器的分合。

（3）大中型充电站的供电监控系统应具备供电系统的越限报警、事件记录、故障统计等数据处理功能。

#### 6.9.7.4 安防监控

##### 6.9.7.4.1 安防监控系统

（1）大型充电站安防监控系统的设计应符合现行国家标准《安全防范工程技术规范》GB 50348 的有关规定，应设置视频安防监控系统，并具有入侵报警、出入口控制设计。中小型充电站可适当简化。

（2）视频安防监控系统的设计应符合现行国家标准《视频安防监控系统工程设计规范》GB 50395 的相关规定。根据安全管理要求在充电站的充电区、营业窗口等位置宜设置监控摄像机；宜具有与消防报警系统的联动接口。

（3）入侵报警系统的设计应符合《入侵报警系统工程设计规范》GB 50394 的相关规定。根据充电站的安全管理要求在充电站内供电区、监控室等位置设置入侵探测器。

（4）充电站出入口控制系统的设计应符合《出入口控制系统工程设计规范》GB 50396 的相关规定。根据充电站的安全管理要求在充电站出入口等位置设置出入口控制设备。

##### 6.9.7.4.2 监控系统要求

（1）摄像机宜安装在监视目标附近不易外界受损的地方，安装位置不应影响现场设备运行和人员正常活动。安装的高度，室内宜距地面 2.5~5m；室外应距地面 3.5~10 米，并不得低于 3m。

（2）摄像机镜头应避免强光直射，保证摄像机照射面不收强光损伤图像。镜头视场

内，不得有遮挡监视目标的物体。

（3）所有监控点需要支持 24 小时不间断录像、计划录像等多种模式，管理员可以根据不同的需求进行选择。

（4）视频监控系统采集的音视频信息资料留存时限不得少于 30 日，视音频信息的存储、播放应具有原始完整性。

（5）所有监控点晚上在无灯光的情况下也能看到现场图像。

（6）系统应具有联网功能，以满足远程用户通过网络进行视频观看。

### 6.9.8 消防安全

#### 6.9.8.1 建（构）筑物的防火要求

（1）充电站建（构）筑物构件的燃烧性能、耐火极限、站内的建（构）筑物与站外的民用建（构）筑物及各类厂房、库房、堆场、储罐之间的防火间距应符合《建筑设计防火规范》GB 50016 第 3 章的规定。

（2）变压器室、配电室、蓄电池室的门应向疏散方向开启；当门外为公共走道或其他房间时，应采用乙级防火门；中间隔墙上的门应采用由不燃材料制作的双向弹簧门。

（3）监控室、办公室、休息室的门应采用不燃材料，向外开启；门应通向无爆炸、无火灾危险的场所；非抗爆结构设计的窗应朝无爆炸、无火灾危险的方向设置。

（4）电缆从室外进入室内的入口处、电缆竖井的出入口处、电缆接头处、监控室与电缆夹层之间以及长度超过 100m 的电缆沟或电缆隧道，均应采取防止电缆火灾蔓延的阻燃或分隔措施，并应根据充电站的规模及重要性采取下列一种或数种措施。

（5）采用防火隔墙或隔板，并用防火材料封堵电缆通过的孔洞。

（6）电缆局部涂防火涂料或局部采用防火带、防火槽盒。

#### 6.9.8.2 电力设备的防火要求

（1）变压器室、配电室、户外电力设备的耐火等级、与其他建（构）筑物和设备之间的防火间距应符合《火力发电厂与变电站设计防火规范》GB 50229 第 11 章的规定。

（2）电力设备的消防安全要求应符合《电力设备典型消防规程》DL 5027 的有关规定。

（3）电力电缆不应和热力管道、输送易燃、易爆及可燃气体管道或液体管道敷设在同一管沟内。

（4）对于带电设备，应配置干粉灭火器、卤代烷灭火器或二氧化碳灭火器，但不得配置装有金属喇叭喷筒的二氧化碳灭火器。

（5）根据不同的储能装置，应配置专用灭火器；如没有专用灭火器，应根据起火物质特性配备用于隔离的措施（如干砂覆盖）。

### 6.9.8.3 消防设施及警报装置

消防设计应《建筑设计防火规范》(2018 年版)GB 50016，《建筑灭火器配置设计规范》GB 50140 等国家和行业规范的要求。消防配备合理，消防设施放置或装设地点的环境条件应符合其生产厂的规定和要求，消防疏散通道顺畅，消防标识清楚。

1、电动汽车充电场站火灾种类

电动汽车充电站主要火灾种类为 A 类和 E 类，其定义如下：

A 类火灾：固体物质火灾。

E 类火灾（带电火灾）：物体带电燃烧的火灾。

2、灭火器的选择

（1）灭火剂的选用应以提高灭火有效性、降低对设备和人体影响为原则。

（2）A 类火灾场所应选择水型灭火器、磷酸铵盐干粉灭火器、泡沫灭火器或卤代烷 1211 灭火器。

（3）E 类火灾场所应选择磷酸铵盐干粉灭火器、碳酸氢钠干粉灭火器、卤代烷 1211 灭火器或二氧化碳灭火器.但不得选用装有金属喇叭喷筒的二氧化碳灭火器。

（4）基于磷酸铵盐干粉灭火器可以覆盖 A 类、B 类、C 类、E 类火灾种类，所以充电场站内的所有灭火器均采用磷酸铵盐干粉灭火器。

3、配置级别和数量

（1）充电车位区，采用 3A 类灭火级别和采用 5kg 手提式磷酸铵盐干粉灭火器。

（2）手提式灭火器的配置与车位数量和充电设备的配置有关，要求 1 具灭火器宜覆盖 2 台直流充电桩，要求 1 具灭火器宜覆盖 4 台 7kW 流充电桩，且单个地点不少于两具灭火器。

（3）对于无车棚的充电站，应为灭火器搭建防直晒、雨淋等保护措施。

4、警报装置

（1）充电站应设置火灾自动报警系统，当发生火灾或受到火灾威胁时，应立即切断电源。

（2）室内可能出现可燃气体或有毒气体时，应设置相应的检测报警器。

### 6.9.8.4 消防给水

（1）消防给水管道和消火栓的设计应符合《建筑设计防火规范》GB 50016 的有关规

定。

（2）水喷雾灭火系统的设计应符合《水喷雾灭火系统技术规范》GB 50219 的有关规定。

#### 6.9.8.5 消防供电及照明

（1）消防水泵、火灾探测报警与灭火系统、火灾应急照明应按Ⅱ级负荷供电。

（2）消防用电设备应采用单独的供电回路，当发生火灾切断生产、生活用电时，仍应保证消防用电，其配电设备应设置明显标志。

（3）消防用电设备的配电线路应满足火灾时连续供电的需要。

（4）控制室、配电室、消防水泵房和疏散通道应设置火灾应急照明。

（5）人员疏散用的应急照明的水平照度不应低于 0.5 lx，继续工作应急照明不应低于正常照明照度值的 10%。

（6）火灾应急照明的备用电源连续供电时间不应少于 30min。

#### 6.9.8.6 防雷

（1）充电站的防雷要求应符合《建筑物防雷设计规范》GB 50057、《交流电气装置的过电压保护和绝缘配合》DL/T 620 的有关规定。

（2）充电站配置专用电力变压器时，电力线宜采用具有金属护套或绝缘护套电缆穿钢管埋地引入充电站，电力电缆金属护套或钢管两端应就近可靠接地。

（3）信号电缆应由地下进出充电站，电缆内芯线在进站处应加装相应的信号避雷器，避雷器和电缆内的空线对均应作保护接地，站区内严禁布放架空缆线。

（4）充电站供电设备的正常不带电的金属部分、避雷器的接地端均应做保护接地，严禁做接零保护。

（5）电气设备内部防雷地线应和机壳就近连接。

#### 6.9.8.7 其他

（1）充电站应设有便于监控室、办公室、休息室及充电区工作人员安全撤离的通道。

（2）应尽可能提高充电站设施以及充电操作过程中对充电车辆、动力蓄电池和操作人员的安全性。

（3）应采取有效的隔离措施并设置醒目的警示标志，防止无关人员进入充电站。

### 6.9.9 充电场站建设施工

建设单位、勘察单位、设计单位、施工单位、工程监理单位及其他与建设工程安全生产有关的单位，必须遵守《中华人民共和国建筑法》、《中华人民共和国安全生产法》、《建

设工程安全生产管理条例》等安全生产法律、法规的规定，保证建设工程安全生产，依法承担建设工程安全生产责任。

建筑施工企业应当在施工现场采取维护安全、防范危险、预防火灾等措施；有条件的，应当对施工现场实行封闭管理。

#### 6.9.9.1 安全施工准备

（1）建设单位应当向施工单位提供施工现场及毗邻区域内供水、排水、供电、供气、供热、通信、广播电视等地下管线资料，气象和水文观测资料，相邻建筑物和构筑物、地下工程的有关资料，并保证资料的真实、准确、完整。

（2）施工组织设计中的安全技术措施或者专项施工方案必须符合工程建设强制性标准。

（3）总承包单位依法将建设工程分包给其他单位的，分包合同中应当明确各自的安全生产方面的权利、义务。总承包单位和分包单位对分包工程的安全生产承担连带责任。

#### 6.9.9.2 施工过程安全管理

（1）施工单位主要负责人依法对本单位的安全生产工作全面负责。施工单位应当建立健全安全生产责任制度和安全生产教育培训制度，制定安全生产规章制度和操作规程，确保安全生产费用的有效使用，并根据工程的特点组织制定安全施工措施，消除安全事故隐患，及时、如实报告生产安全事故。

（2）作业人员进入新的岗位或者新的施工现场前，应当接受安全生产教育培训。未经教育培训或者教育培训考核不合格的人员，不得上岗作业。

#### 6.9.9.3 工程验收要求

验收应依据国家及行业相关验收规范进行验收。建筑工程竣工经验收合格后，方可交付使用；未经验收或者验收不合格的，不得交付使用。所有验收资料必须存入工程建设档案，工程建设档案存档应满足《建设工程文件归档规范》GB/T50328 的要求。

充电设备建设交付的现场验收可参照《电动汽车充电设备现场检验技术规范》（NB/T 送审稿）要求。

## 6.10. 充电设施运行操作与维护安全要求

### 6.10.1 安全风险识别与防范措施

#### 6.10.1.1 充电系统安全风险识别

应对设备电气接地、高压绝缘防触电、充电枪老化漏电、过热、过载、防水、防火控

制逻辑失效等安全隐患进行日常检查，消除安全隐患风险。

#### 6.10.1.2 安全防范措施

##### 6.10.1.2.1 充电设备安全防范措施

（1）防触电风险：充电设备配置专用钥匙，由专业人员维护；做好机柜接地保护功能，总输入开关配置漏电保护功能。

充电枪：高压直流侧通过充电前的桩端绝缘检测和充电中的车端绝缘检测避免漏电风险。

（2）充电机内部配置具备短路和过载保护功能的交流输入断路器确保前级安全；充电机与电动汽车之间增加具备短路和过载保护的快速熔断器来保证后端风险后安全；通过软件功能的冗余保护功能，多重防护功能充电策略确保充电安全。

（3）充电控制逻辑完全满足新国标，要求充电桩，电动汽车完全遵守执行。

（4）通过结构设计、软件仿真方式确保系统散热和防护功能满足要求，同时在系统设计中需对防护或散热失效后具备二次保护功能，确保系统充电过程对环境的适应性。

##### 6.10.1.2.2 信息安全风险防控

###### 6.10.1.2.2.1 漏洞扫描要求

（1）定期对平台内所有主机进行漏洞扫描，当出现重大安全隐患或风险预警时，需立即对涉及安全隐患的主机进行漏洞扫描。

（2）漏洞扫描工具应采用通过国家权威测评机构检测的专用扫描工具，漏洞扫描设备、漏洞扫描软件对操作系统进行漏洞扫描，还应搭配使用其它主流扫描工具进行交叉验证。漏洞扫描工具在使用前应进行漏洞库升级。

（3）漏洞扫描结束后，根据扫描发现的漏洞问题完成漏洞修复工作。“高危”漏洞三个工作日内完成修复，“中危漏洞”五个工作日内完成修复，“低危漏洞”当月完成修复。漏洞修复工作完成后，由安全责任部门进行复测。

###### 6.10.1.2.2.2 风险评估要求

（1）每年对平台进行一次风险评估。委托具备相关风险评估资质的第三方机构开展评估工作。

（2）根据险评估报告进行整改，对报告中提出的安全风险，开展风险处置。完成风险处置工作后，需组织第三方机构进行二次评估，验证风险处置工作的有效性。

（3）对风险评估报告及过程文件进行归档备案。

###### 6.10.1.2.2.3 渗透测试要求

（1）每季度对车联网平台进行渗透测试。渗透测试应采用人工渗透测试方式，渗透测试包括但不限于越权、注入、跨站、敏感信息泄露等漏洞的测试。

（2）渗透测试完毕后需出具渗透测试报告，报告中应记录测试时间、测试范围、测试用例及测试结果。

（3）渗透测试结束后，根据测试发现的漏洞问题完成漏洞修复。“高危”漏洞三个工作日内完成修复；“中危漏洞”五个工作日内完成修复；“低危漏洞”当月完成修复。漏洞修复工作完成后，由安全责任部门进行复测工作。

### 6.10.2 运行操作

1、运行管理规范化；日常安全运行管理及人责任员落实；制定充电设备安全操作规范，确保充电操作安全。

2、安全护具配备齐全。

3、建立健全安全检查机制，时消除运行安全隐患，确保充电操作安全。

4、运行维保人员专业队伍建设

（1）运维工作人员必须取得电工特种作业操作证，持证上岗。

（2）原则上电工作业时应两人作业，一人操作，一人监护。

（3）运维人员应掌握电气安全知识，熟练掌握触电急救和事故紧急处理措施。

### 6.10.3 告警级别与应急处置

（1）充电过程中应设置设备安全告警级别，充电设备根据告警级别进行相对应安全处置预案，包括：绝缘故障处置预案、漏电故障处置预案、泄放回路故障处置预案、防雷故障处置预案、人员触电处置预案、火灾事故处置预案等专项应急处置预案，且需通过相关专家的评审。并定期进行专项预案的应急演练。

（2）设备过电压、过电流、过温、过充电能量报警与处置。

### 6.10.4 充电设备维修保养

（1）充电设备运营商应定期组织专业人员对充电设备进行维修保养。

（2）检查充电机整体外壳是否平整，查看是否出现凹凸痕迹、划伤、变形等缺陷。检查充电机内部进线经过长时间的使用是否出现不紧固可靠，有锈蚀、毛刺、裂纹等缺陷和损伤；检查充电机内部是否干净整洁，电源模块吸风口防尘网和排风口是否堆满灰尘，若堆满灰尘应及时清理干净，必要时对防尘网进行更换和保养，防止电源模块出现故障。检查充电机内部内部各电器元件是否出现变色、变形等现场；需及时进行更换维护。检查充电机内部各电器元件连接是否松动；若发现内部各电器元件有松动现象，需及时解决，

防止故障出现。

（3）检查充电机主板和电源板连接端子是否松动；若电源板 220V 进线端子松动，充电机会出现屏幕不亮，绝缘检测仪不亮，主板上遥信灯同样不亮。需及时接好电源板接线端子。检查充电机内部各器件是否可以正常使用；显示屏触摸是否有反应；主板与显示屏是否通讯正常，手动充电是否可以正常启动。

（4）检测各类开关、继电器、接触器是否正常工作，触点是否完好，通过万用表测量各类开关、继电器、接触器的通断。检测充电机绝缘电阻，充电机输入回路对地、输出回路对地、输入对输出之间绝缘电阻应不小于 10MΩ 。

### 6.10.5 充电连接器接口维护方法及要求

充电设备运营商应定期组织专业人员对充电连接器进行维护。维护时，首先需检查充电枪头及充电插座是否清洁干净，枪头插针表面应无积尘，枪头内无泥沙残留。充电枪绝缘帽应无脱落、插针端正且无烧灼氧化变色等异常、插头塑料件无融化迹象、线缆无脱落或破损、充电无过温。

其次，对充电连接器进行清洁保养，用小毛刷清扫充电枪表面灰尘，用气枪清洁充电枪枪头内（充电枪头内控、插针端子表面）灰尘，接着用小毛刷清扫充电桩挂枪座表面及周边灰尘，用气枪清洁充电桩挂枪座内部灰尘。

充电枪闲置状态下或充电结束后，应将充电枪线缆整理好悬挂于充电桩上，并将充电枪插回充电桩挂枪座，防止灰尘进入枪头。

### 6.10.6 充电运营安全措施

（1）各类型场站应该有灭火器配置，电动汽车充电器灭火器的配置应该符合现行国家标准《建筑灭火器配置设计规范》GB50140 的有关规定。

（2）充电站的防雷接地、防静电接地、电气设备工作接地一机保护接地应共用接地装置，且接地电阻不得大于 4Ω 。

（3）充电场站建设应该安装有照明设施及监控装置。照明以户外照明为主，监控系统应可直观对现场进行总览，也可对局部进行细节观察，监控信息可被记录和回放。

### 6.10.7 充电设施运行安全管理

#### 6.10.7.1 运行维护要求

1、做好充电设备、充电连接器、配电设备日常检查与日常保养

2、充电设备维修管理

3、远程监测与设备维护

4、建立安全生产制度

充电运营商应建立完善的充电设施管理制度、规范文件、操作规程等的制定。

（1）充电设施运营机构应建立健全管理制度和安全规范。

（2）充电设施的运营应根据服务环节设置岗位，明确责任人、工作流程、职责，制定岗位操作规程。

（3）充电设施运营机构应设置安全管理组织，配备专职或兼职的安全员，各环节的安全应明确责任人，将运营服务安全管理贯穿于运营服务的全员和全方位。

（4）充电设施运营机构应采取日常检查、定期检查、不定期抽查、普查、专项检查等方式进行自我评价。每月应至少对充电设施运营整体情况进行一次自我评价。

（5）自我评价内容应包括：

检查、评估规章制度、操作规程的制定和执行情况。

检查作业人员的现场记录。

（6）评价前应制定评价计划，成立评价小组。评价后应编写评价报告。

### 6.10.7.2 安全操作培训

（1）管理人员和作业人员应接受安全生产教育和岗位技能培训，掌握电动汽车安全知识、用电安全规范、电动汽车发生紧急情况的处理方法和触电急救法，考核合格后上岗。

（2）管理人员应了解电动汽车的构造和充换电设备的工作原理，掌握充换电服务流程。

（3）安全员应了解电动汽车的构造、充电设施设备的工作原理，掌握充换电操作规程、安全知识和应急处理方法。

（4）操作人员应了解电动汽车原理及构造，掌握本岗位操作规程和紧急情况的处理方法。

（5）充换电作业人员应了解动力蓄电池应用的基础知识，掌握电动汽车充电安全知识、本岗位操作规程和紧急情况的处理方法。

（6）电池维护人员应了解充换电设备和电动汽车构造，掌握动力蓄电池的基本知识和本岗位操作规程，电池的检测、故障判断和处理。

（7）充电监控人员应了解动力蓄电池电化学性能和动力蓄电池应用的基本知识，掌握监控系统使用和充电控制方法。

（8）直流充电服务人员应由充电作业人员为用户提供；整车交流充电服务可采用客户自助服务模式为用户提供。

（9）设备或系统应设置各级别的操作权限，防止误操作。

### 6.10.7.3 安全隐患与排查

应建立对设备的例行检查制度，开展和环节安全隐患分析，及时对故障进行维修、问题排查、维护检修，做好相关记录:

（1）充电设施基础设施应齐全，符合相关标准的要求。设备的使用与管理应由专人负责，应定期对设备进行巡视、维护与检修。

（2）作业人员应对设备定期进行巡视、维护与检修，不应使用故障设备提供充电服务。

（3）电气设备的检修、测试及维修应由专业技术人员进行，非专业人员不应从事电气设备和电气装置的维修，设备维修前应切断电源。

（4）管理人员和作业人员应定期检查各种安全标志，发现有变形、破损或褪色，应进行整修或更换。

（5）巡查安全员应对充电设施进行巡查，纠正违规操作，发现安全隐患应及时处置。

（6）采取日常检查、定期检查、不定期抽查、普查、专项检查等方式进行自我评价。每月应至少对充电设施运营整体情况进行一次自查报告。

（7）辖区内管理的充电设施应有故障和事故记录。

### 6.10.7.4 突发事件应急处理预案

（1）充电设施运营机构应设置应急组织，建立突发事件应急预案，包括火灾、车辆故障、电池破损燃烧爆炸、供电系统故障、人员触电、电池故障、设备故障等。

（2）应急预案应满足统一指挥，分级负责；组织机构健全；人员和物资配备充足；通信畅通；行动迅速、准确等基本要求。应急预案的主要内容应包括：组织机构、人员、物资、事件等级、报告程序、事故处置方法、快速疏散方法、紧急救护措施、现场保护、清理和善后工作等。

（3）应急预案中涉及的应急设备应在指定场所存放，专人负责，并定期检查应急预案所需物资的有效性。

（4）每半年应至少进行一次应急预案的全员培训和演练，针对演练中的问题，修改和完善应急预案。

（5）突发事件的处置应按应急预案的要求进行。

## 6.11 信息安全

### 6.11.1 运营平台技术要求

#### 6.11.1.1 系统安全防护

**6.11.1.1.1** 系统配置应具备至少双节点的冗余配置，网络接入应具备至少双链路的接入方式，以避免硬件单节点故障或单网络链路的中断而导致业务系统瘫痪。

**6.11.1.1.2** 服务器主机应采用双机配置以冷备用或热备用的方式进行冗余防护，若采用租用云服务的方式则应考虑增加计算资源节点的冗余数量。

**6.11.1.1.3** 网络及安全设备在配置时应与接入的网络链路相匹配，在采用双链路接入配置的方式时，网络 及安全设备应配置为双节点的方式。

**6.11.1.1.4** 应配置安全设备或同等功能的组件。

**6.11.1.1.5** 存储资源在配置时应根据运营平台的业务数据规模核算具体容量。自建数据中心时，在保证服务器设备自身的存储空间充足时，还应配置独立的存储设备，并应双机配置或采用异地数据中心备份的方式。租用云服务时应提供冗余配置的存储资源或异地备份。

#### 6.11.1.2 网络安全防护

**6.11.1.2.1** 运营平台系统应根据不同的业务进行分区分域，将系统划分为不同的子网网段。

**6.11.1.2.2** 重要服务器主机及核心业务区应部署在内网区域，通过路由设备建立安全的访问路径，避免其直接与外网进行连接；核心业务区与其他日常业务网段划分不同子网，并采取可靠的技术隔离手段。

**6.11.1.2.3** 网络接入的出入口访问应通过安全防护设备进行控制与隔离，建立完善的过滤策略及入侵防范策略。

**6.11.1.2.4** 对网络的访问权限进行控制，平台应具备安全审计的防护标准；对运营业务中产生的数据和操作进行日志记录，并可进行备份。

**6.11.1.2.5** 各业务系统区域应具备独立且完整的硬件及网络规划，以避免各业务阶段使用的硬件或基础资源混乱而造成对正式运营系统的影响。

**6.11.1.2.6** 重要的运营平台生产系统宜具备双活热备的系统配置，可自主切换业务。

**6.11.1.2.7** 提供对充电设备的网络访问行为能力，对异常行为进行阻断。

#### 6.11.1.3 基础软件安全防护

**6.11.1.3.1** 操作系统及相关组件应定期更新升级补丁，确保系统软件的稳定可靠。

**6.11.1.3.2** 应定期对系统应用进行漏洞扫描，进行监测入侵防范及恶意代码防范。

**6.11.1.3.3** 应实时对系统进行安全监控，保证对系统应用的各操作合法并有操作审计记录。

**6.11.1.3.4** 各主机基础软件均应具有严格的身份认证配置，口令应具有一定的复杂度，并定期进行更换。

**6.11.1.3.5** 应实时监控各服务器硬盘存储资源，并具备实时提醒告警等功能。

#### 6.11.1.4 业务系统安全防护

**6.11.1.4.1** 业务软件应配置至少双冗余的结构，避免因业务软件的崩溃造成应用单节点故障，导致业务功能无法使用，影响业务运营系统。

**6.11.1.4.2** 业务软件在对外进行数据交互时，应有本运营公司的数据交互协议或加密方式，避免在交互过程中造成数据混乱无法识别或被非法解析导致数据信息泄露。

**6.11.1.4.3** 业务软件在交互过程中应具备自有的数据校验机制，对其数据传输的完整性、安全性进行保障。

**6.11.1.4.4** 业务信息中具有重点需要防护的数据敏感信息时，应有数据脱敏的机制。

**6.11.1.4.5** 业务系统功能的操作安全防护应配置审计系统，各业务操作应详细记录。

**6.11.1.4.6** 业务系统应按实际运营情况中发现的问题漏洞，实施业务系统的更新升级，并明确备案各阶段版本及更新说明。

**6.11.1.4.7** 业务数据应配置数据备份机制，根据运营需求确定历史数据的缓存时间及备份数量。

**6.11.1.4.8** 应对实时访问行为进行监测，及时告警异常行为。

### 6.11.2 充电设备技术要求

#### 6.11.2.1 设备安全

**6.11.2.1.1** 设备的进、出线孔应使用合适的装置或适当的措施密闭，防止外部仪器工具的进入。

**6.11.2.1.2** 设备内部的通信部件应有明显的难以去除的标记，以防被更换。

**6.11.2.1.3** 充电设备检测到异常应主动告警并禁止充电。

**6.11.2.1.4** 操作系统应保证代码可控或采用必要安全加固措施。

**6.11.2.1.5** 应建立能够识别充电设备本体代码、主动阻断未知代码执行的安全免疫机制，通过对充电设备本体代码的完整性校验，防止其被篡改并可以在异常状态下执行自动恢

复。

**6.11.2.1.6** 以最小化安装方式配置软件，对非必要功能的使用进行禁止或限制。

**6.11.2.1.7** 应对系统软件升级且充电设备业务应用的加载软件应具备认证机制，只有经过认证的软件才能在本体系统上运行。

**6.11.2.2 数据安全**

**6.11.2.2.1** 充电设备具备本机充电记录读取功能，不应显示用户完整的敏感信息。

**6.11.2.2.2** 未经使用者授权，充电设备不应主动获取或向第三方提供充电权限认证以外的信息。

**6.11.2.2.3** 充电设备应具备数据有效性校验功能，保证数据符合系统设定要求。

**6.11.2.2.4** 未经授权的任何实体不能从加密存储区域的数据中还原出用户隐私数据的真实内容。

**6.11.2.2.5** 不应未经授权擅自修改和展示用户信息。

**6.11.2.2.6** 充电设备应保证存储和传输过程中数据的完整性。

**6.11.2.2.7** 充电设备应保证存储和传输过程中敏感数据的保密性。

**6.11.2.3 控制安全**

**6.11.2.3.1** 充电设备维护、升级、调试等过程中，应使用身份认证管理技术。

**6.11.2.3.2** 具有账号管理功能的充电设备，其用户身份鉴别信息应具有复杂度要求。

**6.11.2.3.3** 具有账号管理功能的充电设备，应提供并启用登录失败处理功能；多次登录失败后应采取必要的保护措施，当超出限制值时，采取特定的动作。

**6.11.2.3.4** 具有账号管理功能的充电设备，在用户身份证认证信息丢失或失效时，可提供鉴别信息恢复机制。

**6.11.2.3.5** 具有账号管理功能的充电设备应对登录的用户分配账号和权限。

**6.11.2.3.6** 具有账号管理功能的充电设备应及时删除或停用多余的、过期的账号，避免共享账号的存在。

**6.11.2.3.7** 充电设备外部访问接口应采取安全保护措施。

**6.11.2.3.8** 充电设备应具备控制接入的开关。当建立数据连接时，充电设备能够发现该连接并给用户相应的状态提示，仅当用户确认建立本次连接时，连接才可建立。

**6.11.2.3.9** 充电设备应为不同访问主体类别提供不同的访问权限。访问权限划分应遵循最小特权原则。

**6.11.2.3.10** 关闭非系统运行和维护所必须的网络通信端口。

**6.11.2.3.11** 未授权用户不得读取审计信息。

**6.11.2.3.12** 应能按照频次将所有的审计记录备份至本地，或者将事件数据安全地发送到外部。

**6.11.2.3.13** 充电设备应保护已存储的审计记录，以避免未授权的删除、修改或覆盖，并检测对审计记录的修改。

**6.11.2.3.14** 充电设备应确保审计记录保持一定的记录数和维持时间，审计日志留存能力不少于 10000 条。

**6.11.2.3.15** 审计日志要覆盖对设备有较大影响的操作。

### 6.11.3 移动智能终端软件技术要求

#### 6.11.3.1 运行机制要求

**6.11.3.1.1** 在安装和卸载过程中，不得捆绑下载其他应用软件；不得安装功能说明文档中未说明的额外功能，不得安装用户未知和未允许的第三方应用。

**6.11.3.1.2** 卸载应彻底，卸载后不应残留相关临时文件、活动程序或模块。

**6.11.3.1.3** 包含可有效表征供应者或开发者身份的签名信息、软件属性信息。

**6.11.3.1.4** 应对安装包或升级包的完整性、合法性进行校验。

#### 6.11.3.2 应用安全要求

**6.11.3.2.1** 应具备身份鉴别功能，能够对登陆用户进行身份标识和鉴别。

**6.11.3.2.2** 不应内置匿名帐户，禁止匿名用户的登录。

**6.11.3.2.3** 具备口令强度和口令时效性检查机制。

**6.11.3.2.4** 授权用户访问的内容不能超出授权的范围。

**6.11.3.2.5** 未得到许可前不应访问终端数据和终端资源。

**6.11.3.2.6** 未得到允许前不应修改和删除终端数据。

**6.11.3.2.7** 未授权用户不得读取审计信息。

**6.11.3.2.8** 应能按照频次将所有的审计记录备份至本地，或将事件数据安全地发送到外部。

**6.11.3.2.9** 审计日记留存时间应不少于 6 个月。

**6.11.3.2.10** 未经授权的任何实体不能从加密存储区域的数据中还原出用户私密数据的真实内容。

**6.11.3.2.11** 不应存在数据存储和处理过程中的非法调用和窃取漏洞。

**6.11.3.2.12** 不应以明文形式存储或通过网络传输用户敏感数据，以防数据被未授权获

取。

**6.11.3.2.13** 备份机制应完整有效，且应对备份数据进行保护。

### 6.11.3.3 恶意行为防范要求

**6.11.3.3.1** 在用户不知情或未授权的情况下，应用程序不应订购非法业务。

**6.11.3.3.2** 在用户不知情或未授权的情况下，应用程序不应非法获取信息。

**6.11.3.3.3** 在用户不知情或未授权的情况下，应用程序不应接受远程控制端指令并进行相关操作。

**6.11.3.3.4** 应用程序不应导致电动汽车智能充电终端无法正常使用。

### 6.11.3.4 其他安全要求

**6.11.3.4.1** 应用软件代码应防止被反编译和反调试。

**6.11.3.4.2** 源代码中不存在已公布的高危风险漏洞。

**6.11.3.4.3** 应用软件应做日志放泄露措施。

## 6.11.4 接口安全技术要求

### 6.11.4.1 充电设备和运营平台之间的接口

**6.11.4.1.1** 充电设备与运营平台之间的通信应优先采用硬件加密认证设备进行认证加密，对来源于运营平台的控制命令和参数设置指令应采取安全鉴别和数据完整性验证措施。

**6.11.4.1.2** 充电设备与运营平台之间的业余数据应采用加密措施，实现数据的保密性，并且应该符合国家相关的管理规定，禁止使用已知为不安全的加密算法和安全措施。

**6.11.4.1.3** 充电设备应具备防网络干扰功能，在网络瘫痪等紧急情况下，可通过备用方案保证充电设备的正常使用。备用方案启动应有明确标识，在网络恢复后，充电设备应主动上传网络异常状态和备用方案充电记录。

**6.11.4.1.4** 需远程维护的，采用安全加密协议或虚拟专用网络等技术建立安全的访问路径、可通信通道确保远程接入安全。

### 6.11.4.2 充电设备和电动汽车之间的接口

**6.11.4.2.1** 充电设备和电动汽车之间的通信网络应通过安全网关与外部网络进行隔离，由网关进行可信消息的分发和处理。

**6.11.4.2.2** 协议应用数据不应使用明文传输，由应用协议负责安全加密机制的实现。

**6.11.4.2.3** 充电设备和电动汽车建立安全的传输通道后，通信双方应能验证消息的完整性。

#### 6.11.4.3 运营平台之间的接口

**6.11.4.3.1** 应采用多因子认证方式进行平台认证，保障信息交换接口安全、稳定、可靠地运行。

**6.11.4.3.2** 应采用 IP 访问控制、时间访问控制等手段或结合使用，以限制同一终端在一定时间内对平台数据接口的高频访问。

**6.11.4.3.3** 消息发送方应对消息字段中涉及交易及隐私等数据采用安全可靠且普遍使用的加密算法，消息接收方在校验参数合法性后方可进行后续业务处理。

**6.11.4.3.4** 消息报文应使用数字签名、重发机制等方式保障传输和接收数据的完整性。

#### 6.11.4.4 以移动智能终端做为认证接口

**6.11.4.4.1** 设备上附属的二维码应具备适当的加密机制，在二维码编码前进行加密，以保证只有通过解密识别的扫码设备才能正确识别出设备信息。

**6.11.4.4.2** 二维码中涉及的关键、敏感数据需要进行安全防护。

**6.11.4.4.3** 通过移动智能终端扫描二维码获得服务凭证，必须与后台进行信息交换，获得真实的服务认证结果。

**6.11.4.4.4** 移动智能终端与运营平台进行的认证服务过程，应采用安全传输方式。二维码涉及各系统之间信息传输，各系统之间应建立安全通信信道，应对交易数据采用安全方式进行传输，确保数据不被监听和篡改。

**6.11.4.4.5** 应对传输的数据进行保密性保护，不应引起信息泄露。

**6.11.4.4.6** 应具备对传输数据的鉴别机制，确保发出数据的完整性和接收数据完整性的校验。

#### 6.11.4.5 以智能卡作为认证接口

**6.11.4.5.1** 应用管理数据在卡片的初始化期间建立，应定义初始的安全域。

**6.11.4.5.2** 发卡机构应建立可靠、完善的密钥管理制度。

## 6.12 换电站安全

电池更换站应为纯电动汽车用户提供安全、快速、可靠的电池箱更换场所，电池箱更换和充电的过程应始终处于被监控的状态。

换电站安全规范、消防安全、监控、充电等相关要求及建设要求，旨在规范电池更换站建设、消防、监控等要求，实现对电动汽车电池快速更换的要求。

### 6.12.1 站址安全

电池更换站选址应满足 GB/T 51077《电动汽车电池更换站设计规范》中第 3 章要求。

电池更换站内的建（构）筑物与站外建筑之间的防火间距应符合现行国家标准《建筑设计防火规范》GB 50016 和现行国家标准《高层民用建筑设计防火规范》GB 50045 的有关规定。

### 6.12.2 消防安全

电池更换站安全和消防要求应满足 GB/T 29772《电动汽车电池更换站通用技术要求》中第 12 章要求。

电池更换站内应设置事故电池隔离措施；电池存储区域应设有事故电池紧急运送通道，电池更换站内宜配置应急转运车、移动沙箱等，对事故电池进行有效处理，保证事故电池快速、安全地运出充电架。

### 6.12.3 监控要求

监控系统应满足 GB/T 29772《电动汽车电池更换站通用技术要求》中第 9 章要求。

监控系统应具备实时存储电池充电数据、更换电池的信息（电池编码、电池的信息等）及车辆信息等数据。

监控系统应具有数据接口功能，向运营平台转发：电池更换站站况、电池组使用信息(包含车上的电池)、充电机工作状态、计量计费信息、车牌识别信息等并协助将所有数据通过 TCP/IP 协议上传至云端服务器。

监控系统应具备车牌识别（VIN 编码）、计量计费、费用结算等功能。

监控系统具有数据采集功能、数据处理与存储、事件记录、人机操作与图形编辑、报警处理、通信功能、报表管理与打印功能、系统维护与系统自检、可扩展性、充电信息管理功能等。

监控系统应能采集的数据包括：充电机工作状态、温度故障信号、充电机功率、充电电压、充电电流、充电电量、汽车行驶里程、电池更换次数等。电池箱的出厂编号、版本、单体电压、温度、SOC、故障信号等。

监控系统应满足 NB/T 33005《电动汽车充电站及电池更换站监控系统技术规范》的第 6 章要求。

监视：监控系统应能对站内主要设备运行参数和设备状态、通信状态和通信报文进行监视，并实时显示。

报警：监控系统应能对站内设备状态异常、故障，测量值越限、突变及监控系统软、硬件、通信接口及网络故障进行报警处理。

### 6.12.4 设备安全

快换电池箱应满足 NB/T 33025《电动汽车快速更换电池箱通用要求》的要求：

快换电池箱应满足车载使用工况要求，电池箱固定应采用机械式锁止机构，并具有防止锁止失效功能。电池箱锁止机构应能在三个相互垂直的轴上将电池箱固定在托架上，在车辆行驶造成的频繁振动下，不会出现产生危害的相对位移或产生明显的机械噪声。

电池箱锁止机构的解锁和锁止应通过受控方式操作，锁止机构的工作状态应能可靠检测。

电池箱锁止机构应能承受振动和冲击的影响。

在异常情况下应能通过手动方式解锁并拉出电池箱。

电池箱连接器应满足 GB/T 32879《电动汽车更换用电池箱连接器通用技术要求》的要求：

连接器的防触电保护应符合 GB/T 11918《工业用插头插座和耦合器 第 1 部分：通用要求》中第 9 章的要求。

连接器的接地保护应符合 GB/T 11918《工业用插头插座和耦合器 第 1 部分：通用要求》中第 10 章的要求。

连接器插头和插座耦合后，防护等级不应低于 GB 4208《外壳防护等级（IP 代码)》中 IP55 的要求。连接器插头和插座脱开后，防护等级应符合 GB 4208 外壳防护等级（IP 代码)》中 IP2X 的要求。

电池箱更换设备应满足 NB/T 33006《电动汽车电池箱更换设备通用技术要求》中第 5 章第 5 节 的要求。

### 6.12.5 车辆安全

快换电池箱与车辆的固定安全应满足 QC/T 743《电动汽车用锂离子蓄电池》的要求。

### 6.12.6 电池更换安全

换电站设备应能识别换电车辆，获知车载电池箱身份编码（应满足 20132391-T-524（国标，未发布)《电动汽车电池更换用电池箱编码技术规范》要求)，以及电池箱的出厂编号、版本、行驶里程、更换次数、当前状态等等信息，保证电池箱在站内换电及换电后的充电过程中的安全。

## 6.13 质量保证体系

按照 GB/T 19001、GB/T 24001 和 GB/T 28001 三个标准及相关法律法规的要求，结合

充电设施的设计、建设及运营维护，按照活动过程模式及 PDCA 循环原理，建立质量、环境和职业健康安全管理体系并形成文件。通过实施、保持和持续改进质量保证体系，确保其质量的可靠性与稳定性。

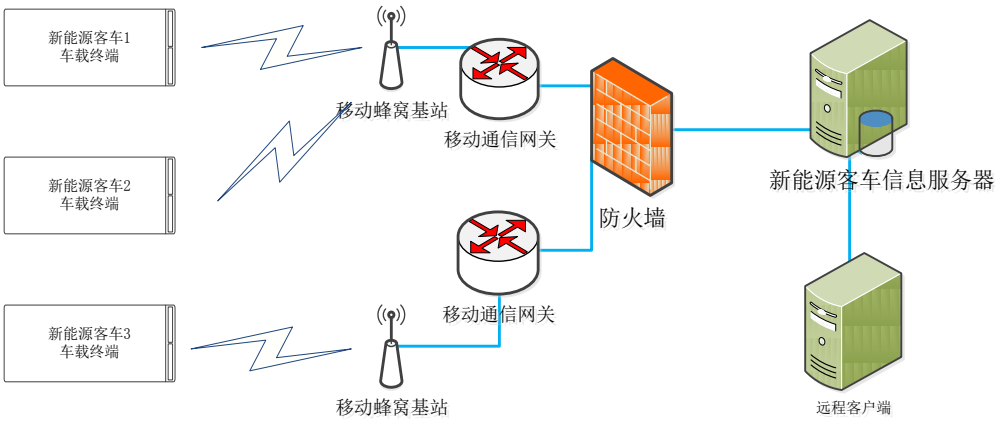
# 7. 数据监控管理

车辆状态监测主要使用新能源三电系统的运行状态数据、车辆驾驶数据，服务于三电系统的设计改进。因车辆交互数据均为敏感数据，特别是和车辆控制相关的数据，所以硬件环境和软件环境都需有防入侵，防监听和防篡改的要求。

## 7.1 车辆状态监测

应具备采集、存储、传输车辆运行状态、报警、充电、定位等数据的功能， 以 GB/T 32960《电动汽车远程服务与管理系统技术规范》为支撑，实现电动汽车数据向国家、地方平台逐级上报，形成三级安全监管体系。

采用卫星定位技术（GPS/BDS）、 无线通讯技术（GPRS/3G/4G/5G）、 地理信息（GIS）技术和云计算及数据挖掘技术， 建立电动汽车企业远程监控平台， 实现对车辆地理位置和运行状态各项参数的监控。包括车速、电池状态、电机状态、安全报警等整车数据、驱动电机数据、极值数据、报警数据、车辆位置数据、发动机数据、燃料电池、故障情况下的单体数据（单体电压/单体温度）等信息。




### 7.1.1 数据采集

数据采集参数范围包含但不限于 GB/T32960.3（具体见表 7-1）的要求。实时数据的采集频率不应低于 1 次/s。

表 7-1

| 数据表示内容 | 长度/字节 | 数据类型 | 描述及要求 |
|---|---|---|---|
| 整车数据 | | | |
| 车辆状态 | 1 | BYTE | 0x01：车辆启动状态；0x02：熄火；0x03：其他状态；0xFE：表示异常；0xFF：表示无效 |

| | | | |
|---|---|---|---|
| 充电状态 | 1 | BYTE | 0x01：停车充电；0x02：行驶充电；0x03：未充电状态；0x04：充电完成；0xFE：表示异常；0xFF：表示无效 |
| 运行模式 | 1 | BYTE | 0x01：纯电；0x02：混动；0x03：燃油；0xFE：表示异常；0xFF：表示无效 |
| 车速 | 2 | WORD | 有效值范围：0~2200（表示 0km/h~220km/h），最小计量单元：0.1km/h；0xFE：表示异常；0xFF：表示无效 |
| 累计里程 | 4 | DWORD | 有效值范围：0~9999999（表示 0km~999999.9km），最小计量单元：0.1km/h；0xFE：表示异常；0xFF：表示无效 |
| 总电压 | 2 | WORD | 有效值范围：0~10000（表示 0V~1000V），最小计量单元：0.1V；0xFE：表示异常；0xFF：表示无效 |
| 总电流 | 2 | WORD | 有效值范围：0~20000（偏移量 1000A，表示-1000A~1000A），最小计量单元：0.1A；0xFE：表示异常；0xFF：表示无效 |
| SOC | 1 | BYTE | 有效值范围：0~100（表示 0%~100%），最小计量单位：1%，0xFE：表示异常；0xFF：表示无效 |
| DCDC 状态 | 1 | BYTE | 0x01：工作；0x02：断开；0xFE：表示异常；0xFF：表示无效 |
| 挡位 | 1 | BYTE | bit7：预留，预留位用 0 表示<br>bit6：预留，预留位用 0 表示<br>bit5：1 代表有驱动力；0 代表无驱动力<br>bit4：1 代表有制动力；0 代表无制动力<br>bit3~bit0：0000 代表空挡；0001 代表 1 挡；<br>0010 代表 2 挡；0011 代表 3 挡；0100 代表 4 挡；0101 代表 5 挡；0110 代表 6 挡；1101 代表倒档；1110 代表自动 D 挡；1111 代表停车 P 挡 |
| 绝缘电阻 | 2 | WORD | 有效范围：0~60000（表示 0kΩ~60000 kΩ，最小计量单位：1kΩ |

| | | | |
|---|---|---|---|
| 加速踏板行程值 | 1 | BYTE | 有效值范围：0~100（表示 0%~100%），最小计量单位：1%，0xFE：表示异常；0xFF：表示无效 |
| 制动踏板状态 | 1 | BYTE | 有效值范围：0~100（表示 0%~100%），最小计量单位：1%，“0”表示制动开关的状态；在无具体行程值情况下，用“0x65”即“101”表示制动有效状态，0xFE：表示异常；0xFF：表示无效 |
| 驱动电机数据 | | | |
| 驱动电机序号 | 1 | BYTE | 驱动电机顺序号，有效值范围 1~253 |
| 驱动电机状态 | 1 | BYTE | 0x01：耗电；0x02：发电；0x03：关闭状态；0x04：准备状态；0xFE：表示异常；0xFF：表示无效 |
| 驱动电机控制器温度 | 1 | BYTE | 有效值范围：0~250（数值偏移量 40℃，表示-40℃~210℃），最小计量单位：1℃；0xFE：表示异常；0xFF：表示无效 |
| 驱动电机转速 | 2 | WORD | 有效值范围：0~65531（数值偏移量 20000，表示-20000r/min~45531r/min），最小计量单位：1r/min；0xFE：表示异常；0xFF：表示无效 |
| 驱动电机转矩 | 2 | WORD | 有效值范围：0~65531（数值偏移量 20000，表示-2000N.m~4553.1rN.m），最小计量单位：0.1N.m；0xFE：表示异常；0xFF：表示无效 |
| 驱动电机温度 | 1 | BYTE | 有效值范围：0~250（数值偏移量 40℃，表示-40℃~210℃），最小计量单位：1℃；0xFE：表示异常；0xFF：表示无效 |
| 电机控制器输入电压 | 2 | WORD | 有效值范围：0~60000（表示 0V~6000V），最小计量单元：0.1V，0xFE：表示异常；0xFF：表示无效 |
| 电机控制器直流母线电流 | 2 | WORD | 有效值范围：0~20000（数值偏移量 1000A，表示-1000A~+1000A），最小计量单元：0.1A，0xFE：表示异常；0xFF：表示无效 |
| 极值数据 | | | |
| 最高电压电池子系统号 | 1 | BYTE | 有效值范围：1~250，0xFE：表示异常，0xFF：表示无效 |

| | | | |
|---|---|---|---|
| 最高电压电池单体代号 | 1 | BYTE | 有效值范围：1~250，0xFE：表示异常，0xFF：表示无效 |
| 电池单体电压最高值 | 2 | WORD | 有效值范围：0~15000（表示 0V~15V），最小计量单元：0.001V，0xFE：表示异常；0xFF：表示无效 |
| 最低电压电池子系统号 | 1 | BYTE | 有效值范围：1~250，0xFE：表示异常，0xFF：表示无效 |
| 最低电压电池单体代号 | 1 | BYTE | 有效值范围：1~250，0xFE：表示异常，0xFF：表示无效 |
| 电池单体电压最低值 | 2 | WORD | 有效值范围：0~15000（表示 0V~15V），最小计量单元：0.001V，0xFE：表示异常；0xFF：表示无效 |
| 最高温度子系统号 | 1 | BYTE | 有效值范围：1~250，0xFE：表示异常，0xFF：表示无效 |
| 最高温度探针序号 | 1 | BYTE | 有效值范围：1~250，0xFE：表示异常，0xFF：表示无效 |
| 最高温度值 | 1 | BYTE | 有效值范围：0~15000（表示 0V~15V），最小计量单元：0.001V，0xFE：表示异常；0xFF：表示无效 |
| 车辆位置数据 | | | |
| 定位状态 | 1 | BYTE | bit0：0 代表有效定位；1 代表无效定位<br>bit1：0 代表北纬；1 代表南纬<br>bit2：0 代表东经；1 代表西经<br>bit3~7：保留 |
| 经度 | 4 | DWORD | 以度为单位的维度值乘以$10^6$，精确到百万分之一度 |
| 维度 | 4 | DWORD | 以度为单位的维度值乘以$10^6$，精确到百万分之一度 |
| 报警数据 | | | |
| 最高报警等级 | 1 | BYTE | 为当前发生的故障中的最高等级值，有效值范围：0~3，“0”表示无故障；“1”表示 1 级故障，指代不影响车辆正常行驶的故障；“2”表示 2 级故障，指代影响车辆性能，需驾驶员限制行驶的故障；“3”表示 3 级故障，为最高级别故障，指代驾驶员应立即停车处理或请求救援的故障；具体等级对应的故障内容由厂商自行定义；“0xFE”表示异常，“0xFF”表示无效 |
| 通用报警标志 | 4 | DWORD | bit0：1 代表温度差异报警；0 代表正常<br>bit1：1 代表电池高温报警；0 代表正常<br>bit2：1 代表车载储能装置类型过压报警；0 代表正常 |

| | | | |
|---|---|---|---|
| | | | bit3：1 代表车载储能装置类型欠压报警；<br>0 代表正常<br>Bit4：1 代表 SOC 低报警；0 代表正常<br>bit5：1 代表单体电池过压报警；0 代表正常<br>bit6：1 代表单体电池欠压报警；0 代表正常<br>bit7：1 代表 SOC 过高报警；0 代表正常<br>bit8：1 代表 SOC 跳变报警；0 代表正常<br>bit9：1 代表可充电储能系统不匹配报警；0 代表正常<br>bit10：1 代表电池单体一致性差异报警；0 代表正常<br>bit11：1 代表绝缘报警；0 代表正常<br>bit12：1 代表 DCDC 温度报警；0 代表正常<br>bit13：1 代表制动系统报警；0 代表正常<br>bit14：1 代表 DCDC 状态报警；0 代表正常<br>bit15：1 代表驱动电机控制器温度报警；0 代表正常<br>bit16：1 代表高压互锁状态报警；0 代表正常<br>bit17：1 代表驱动电机温度报警；0 代表正常<br>bit18：1 代表车载储能装置类型过充；0 代表正常<br>bit19~31：预留 |
| 可充电储能装置故障总数 N1 | 1 | BYTE | N1 个可充电储能装置故障，有效值范围：0~252，“0xFE”表示异常，“0xFF”表示无效 |
| 可充电储能装置故障代码列表 | 4xN | DWORD | 扩展性数据，由厂商自行定义，可充电储能装置故障个数等于可充电储能装置故障总数 N1 |
| 驱动电机故障总数 N2 | 1 | BYTE | N2 个驱动电机故障，有效值范围：0~252，“0xFE”表示异常，“0xFF”表示无效 |
| 驱动电机故障代码列表 | 4xN2 | DWORD | 厂商自行定义，驱动电机故障个数等于驱动电机故障总数 N2 |
| 其他故障总数 N4 | 1 | BYTE | N4 个其他故障，有效值范围：0~252，“0xFE”表示异常，“0xFF”表示无效 |
| 其他故障代码列表 | 4xN4 | DWORD | 厂商自行定义，故障个数等于故障总数 N4 |

### 7.1.2 数据传输

应具有将采集到的实时数据发送到企业远程监控平台的功能。传输数据种类：见上表。传输时间间隔：传输信息的时间周期应可调整，车辆正常行驶时，上报信息的时间周期最大不应超过 30s，当车辆出现 3 级报警时，应上报故障发生时间点前后 30s 的表 6-1 所包括的全部数据项，且信息采样周期应不大于 1s，其中故障发生前数据应以补发的形式进行传输。其中 3 级报警指驾驶员应立即停车处理或请求救援的故障。如：电池高温报警、整车绝缘报警等。。同时，企业远程监控平台应具备按照 GB/T32960.3 中规定的平台交换通信协议，将车载终端采集的数据及相关信息传输给公共平台的能力。

### 7.1.3 车辆电池状态监测

基于电池的容量、温度、电流、电压、SOC、充电模式等与电池相关的数据，设立包括但不限于车辆充电次数、充电类型、充电 SOC 分布、电池最高/最低温分布、单体电压分布等指标，并结合电池健康度影响因素、电池健康度预测等算法模型，从电池的使用、电池健康、电池故障报警等多维度分析监测新能源车的电池状态。

除通过大数据分析监测车辆的电池状态，建议不定时为维修站或用户推送电池健康、电池预警等数据，进一步对电池状态进行监测，从而及时预防电池问题，极大的提高电池的安全性能。

### 7.1.4 车辆电机状态监测

基于电机的转速、扭矩、温度、温差、电机故障报警等与电机相关的数据，从电机转速分布、电机扭矩分布、电机温度分布、电机温度报警等多维度分析监测新能源车的电机状态。

除通过大数据分析监测车辆的电机状态，也不定时为维修站或用户推送电机健康、电机预警等数据，进一步对电机状态进行监测，从而及时预防电机问题，极大的提高电机的安全性能。

### 7.1.5 车辆驾驶行为监测

基于车辆的出行天数、出行次数、行驶里程、车速等与用户驾驶行为相关的数据，结合里程焦虑模型、驾驶安全性模型等算法模型，从车辆月均出行天数、日均出行次数、出行时间分布、单行驶循环车速分布、里程焦虑评分等多维度分析监测车辆的驾驶行为。

通过大数据分析监测车辆的驾驶行为，定时为用户推送驾驶行为报告、驾驶行为评分、驾驶建议等，引导用户健康驾驶，提高用户的出行安全。

## 7.2 危险情况下的远程控制

生产企业应建立和完善企业远程监控平台的运维和服务体系。对有上报给企业远程监控平台 3 级故障的车辆，主动通过平台通知相应的售后服务人员进行及时的故障排除。

## 7.3 车辆信息安全

### 7.3.1 车辆硬件信息安全

汽车硬件的信息安全目标即为保障车辆硬件在实现数据运算及数据存储等功能时的安全性，可以对抗针对加解密操作的密码分析攻击、侧信道攻击及故障注入攻击等破坏数据保密性和完整性的安全威胁，防止车辆网络系统被入侵，保证车辆硬件功能可以正常使用。

车辆硬件设计时应考虑在量产产品中去除电路板上标注芯片、端口及管脚功能的可读丝印，并封闭可以非法对芯片内存访问或更改芯片功能的调试接口。

车载控制器内部的敏感数据通信线路应尽量隐蔽，以防止针对板级数据传输的窃听和伪造攻击。关键芯片应尽量减少暴露管脚，如采用 BGA/LGA 封装的芯片。控制器应考虑使用硬件模块实现关键敏感数据的存储和运算的物理隔离，保证模块中的数据不可被非授权访问。

车辆硬件设计时应使用必要的安全机制或者防护机制，防御和对抗相应攻击，如：

（1）针对安全芯片的电压或时钟的单次故障注入攻击；

（2）针对安全芯片的电磁或激光的单次故障注入攻击；

（3）针对加密芯片的侧信道简单功耗分析（SPA）攻击；

（4）针对加密芯片的侧信道一阶差分功耗分析（DPA）攻击；

（5）针对加密芯片的侧信道相关功耗分析（CPA）攻击。

### 7.3.2 车辆网络环境信息安全

车辆网络环境包括车辆内部的网络环境及外部的网络环境，内部的网络主要指车辆内部各个子系统之间的通信，外部网络包括了车辆通过蜂窝网络与服务器之间的通信、车车之间及车路协同通信、车内短距离（蓝牙、WIFI 等）通信。

车辆网络环境复杂，需要在整车网络设计时考虑不同业务场景下进行数据交互时，保障内部各子系统间的指令数据传输不会被伪造、窃听、重放等手段攻击；保障车内网络与外部威胁的安全隔离；保障车辆与蜂窝网络、移动终端通信时，可以对抗嗅探、中间人攻击、重放等安全威胁，保障车辆网络环境的安全。

应使用必要的防护技术手段，将车辆内部的子系统进行信息安全域的划分，定义不同域的安全等级，建立域之间的安全访问策略。

车辆在通过蜂窝网络连接时，应采用相应的安全策略，保障接入真实可靠的网络，并能够识别来自蜂窝网络的非法连接请求。在与核心业务平台进行通信时，应与公网进行逻辑隔离，并使用强验证手段，确保只有授权的主体可以实施相应的操作。

车车通信与车路协同通信时，车辆端需要对所连接的节点的身份进行认证，数据应加密进行传输。

车辆在与移动设备进行通信时，应具备用户手动打开或关闭短距离无线连接的能力，并对已建立的连接，使用必要的手段进行明确的连接状态显示。车辆只在某些特定状态下接受外来通信连接请求，并对连接的设备进行认证授权操作。

### 7.3.3 OTA 数据安全加密与防篡改

车辆的 OTA 主要分为两类，一种是 FOTA（Firmware-over-the-air，固件在线升级），指给车载系统或内部控制器进行固件升级；另一种是 SOTA（Software-over-the-air，软件在线升级），指对固件以外的软件（如地图）升级。无论哪种升级，都面临车辆端与服务器间的升级包传输风险及升级包篡改风险。

在进行 OTA 升级过程中，需从升级包发布、升级包传输、终端升级三个阶段进行防御。OTA 服务器端可增加部署安全服务器，提供安全基础设施、如密钥生成与管理、数字加密及数字签名等，以抵御针对升级包的逆向分析攻击、篡改攻击等。基于安全服务器实现升级包加固功能，最终由 OTA 服务器发布加固后的升级包。安全服务器的基础功能可使用软件方案实现，也可配合部署硬件加密机实现。

在 OTA 服务端与车辆端构建安全传输通道，实现双向身份认证，及传输加密等功能，保证升级包传输过程的安全。终端系统在升级流程前增加升级包校验机制，对升级包进行解密和合法性验证，验证通过方可进入系统升级流程。

## 7.4 信息数据保存和分析

数据监控平台应确保数据存储安全，在分析使用时应确保数据不泄露，禁止数据被非法使用。

### 7.4.1 信息数据本地存储

（1）车载终端应按照最大不超过 30s 的时间间隔将采集到的实时数据保存在内部存储介质中。当车辆出现 3 级报警时，车载终端应按照最大不超过 1s 的时间间隔将采集到

的实时数据保存在内部存储介质中。其中 3 级报警指驾驶员应立即停车处理或请求救援的故障。如：电池高温报警、整车绝缘报警等；

（2）车载终端内部存储介质容量应满足至少 7 天的实时数据存储。车载终端内部存储介质存储满时，应具备内部存储数据的自动循环覆盖功能；

（3）车载终端内部存储的数据应具有可读性；

（4）车载终端断电停止工作时，应完整保存断电前保存在内部介质中的数据不丢失。

### 7.4.2 信息数据平台服务器存储

车载终端的数据实时上传到企业远程监控平台，通过企业远程监控平台可实时监控车辆运行状况，同时将相关的运行数据保存到服务器，为保证车辆历史数据可追溯，数据存储时间应不少于 5 年（参照天津地标）。

### 7.4.3 信息数据分析

基于电动汽车实时运行状态的监测，搭建企业远程监控平台，为每台运营车辆建立标准、规范的数据档案库。采用大数据与数据挖掘技术，从安全、能耗和节能等角度，实现电动汽车全生命周期多方位的监控与分析。如：车辆故障分析、车辆百公里能耗分析、动力电池状态分析、司机驾驶行为分析等。

## 7.5 充电数据管理

充电机应按照《GB/T 27930 电动汽车非车载传导式充电机和电池管理系统之间的通信协议》向整车发送充电数据。

车辆应通过 BMS 对充电设备的在线状态，充电过程中的电压、电流、电量、电池等信息进行监测，并具备以下功能：

（1）充电状态监测；

（2）充电设备充电过程中电压、电流、电量等信息持续监测；

（3）充电车辆电池信息监测；

（4）对充电过程中潜在安全问题进行预警；

（5）记录车辆充电情况，包括但不限于开始时间、结束时间、充电电流、开始 SOC、结束 SOC。

# 8.维修保养

## 8.1 电动汽车的通用维修保养

虽然电动汽车和传统汽车驱动方式不同，但依然要进行日常的保养维护，电动汽车需要针对电池系统和电动机等高压部件进行日常的保养。

随着使用年限增加，由于功能性部件的性能磨损、老化、腐蚀等原因，可能致使行车安全性能逐渐降低，定期按照规定进行保养，才能保障电动汽车的行车安全。

由于电动汽车采用高压电的特点，对其高压线束以及高压部件进行维护保养操作时有触电风险，需要由专业人员配备专业设备在 4S 店或专业场所进行保养操作，严禁非专业人员进行随意非正规拆解。

电动汽车在下列特殊情况下，必须进行专业维修保养：

（1）电动汽车浸水或长时间涉水后；

（2）电动汽车底部动力电池受到碰撞后；

（3）电动汽车发生碰撞事故后；

（4）故障灯显示需要进店进行维修保养的；

按照用户使用手册规定的周期进行定期保养。

### 8.1.1 操作人员的要求

B 级电压部件的维护保养人员应受过专业培训，取得电工上岗证、维修电工资格证书且经过培训合格的专业人员执行，并严格遵守电工安全操作规程，维护人员必须使用专业作业工具（上位机、绝缘表、扭力扳手、绝缘鞋、绝缘手套等）。

### 8.1.2 操作前的要求

操作前，在系统进行维护和保养前必须切断动力电源。操作方法参考 11.4。

### 8.1.3 操作过程要求

操作过程要求参考 11.5。

### 8.1.4 其他操作要求

（1）在清洗车辆时，禁止高压水枪对 B 级电压系统进行直接冲洗；

（2）定期检查设备舱内的防水和降温设备，下雨天气时检查排气扇是否能够正常工作，排气扇通风口是否有雨水进入；

（3）必须使用符合国家标准的充电设备，充电作业人员需经过培训合格、持证上岗，充电时请使用“自动充电”功能，严禁使用“手动充电”功能；严禁对电池系统盲充，严

禁带电拔枪，严禁未拔枪行车；禁止雷电天气、雨天露天给电动车充电；雷雨天气，必须在有雨水及雷电防护的区域充电，充电时请检查充电插头有无水迹，充电过程随时查看有无绝缘报警。

## 8.2 动力电池的维修保养要求

### 8.2.1 动力电池日常使用保养要求

#### 8.2.1.1 正确的进行充放电

在使用过程中，根据实际情况准确把握充电时间，参考平时使用频率及行驶里程，把握充电频次，及时补电，尽量避免动力电池电量耗尽导致车辆停止才充电。

#### 8.2.1.2 车辆长期静置时须定期充电

车辆闲置时，因电池本身的自放电特性和车载电子设备的休眠耗电，电池也会非常缓慢的放电。为防止电池过放，所以车辆长期静置时，应对车辆定期进行充电。车辆在不同SOC时可以静置的最长时间，如下表，应在该时间段内对车辆进行充电，充至SOC≥50%。

| 序号 | SOC区间 | 车辆典型最长静置时间 |
|---|---|---|
| 1 | SOC＞40% | 三个月 |
| 2 | SOC≤40% | 两个月 |
| 3 | SOC≤20% | 一个月 |
| 4 | SOC≤10% | 20天 |
| 5 | SOC≤5% | 7天 |

### 8.2.2 动力电池的维修

动力电池由于其设计高电压特点，需要专业人员进行维修。

#### 8.2.2.1 维修人员要求

动力电池的维修作业必须由具有新能源从业经验或取得相关从业资质证书的专业人员实施。维修人员须佩带绝缘手套和绝缘鞋。

#### 8.2.2.2 维修场地要求

动力电池维修场所必须干净（无油脂、无污渍且无金属屑）、干燥（无泄漏的液体），并且没有飞溅的火星。因此应避免在车辆清洁区或进行车身维修区域附近，必要时应使用活动隔板进行分离。维修场所应通风良好(室内)或尽量开阔(室外),有严禁烟火、防水和高压危险的明显标识,非维修人员禁止进入维修场所。

#### 8.2.2.3 维修过程要求

维修人员进行动力电池维修作业时，应断开一处或者多处高压母排，将维修单元的电压降至 60V.d.c 以内。

当检测到电池单体出现质量问题时,原则上需整箱更换,当不得不更换单体电池时,必须由经过相应培训的专业人员严格按相关操作规程更换。

在高压部件或高压线处及其附近区域请勿使用有尖锐或锋利边缘 / 棱角的工具。在低压电线束上允许使用剪线钳打开导线扎带。失效的或损坏的高压线必须废弃掉，以免再次使用。不得将工具遗忘在动力电池内部。在封闭壳体盖前，检查工具箱中工具的完整性，检查箱体内是否遗留螺栓等小零件。为了在修理时不会将螺栓遗忘在动力电池内部，建议使用一般磁化工具。

维修过程如果工作中断，则应放上壳体盖并旋入几颗螺栓以防止意外打开。在维修结束时应检查动力电池系统和电池液冷系统的气密性。

维修场所应具备消防安全措施，以应对出现浓烟、明火等紧急情况，同时拨打报警电话,设立警示标志。

## 8.3 电机控制器的维修保养要求

### 8.3.1 电机控制器保养要求

电机控制器为高压电器件，维修时，需由专业人员配备专业设备进行操作，严禁非专业人员进行非法拆解,电机控制器从整车上拆下后，严禁进行拆解。

拆卸电机控制器前应确保：

（1）作业时必须断开整车低压电源、电机控制器高压电源，做好安全防护、知晓安全注意事项、熟悉作业设备及工具、熟悉操作要求；

（2）作业时，应避免沙尘、雨雪气象情况下露天操作，避免沙尘、水及其他杂质进入电机控制器内部；

（3）作业时，需使用专业检测检修设备和绝缘工具，人员佩戴绝缘手套、穿绝缘鞋；所有操作均应进行断电、放电、高压 DC+/DC-对地电压检测，确保不带电操作；

（4）具体的作业内容及要求依据主机厂的维保手册执行。

### 8.3.2 电机控制器维修要求

#### 8.3.2.1 电机控制器维修前提

电机控制器为高压电器件，维修时，需由专业人员配备专业设备进行操作，严禁非专业人员进行非法拆解,电机控制器从整车上拆下后，严禁进行拆解。

拆卸电机控制器前应确保：

（1）整车高压下电，移除动力电池维修开关；

（2）整车低压电下电；

#### 8.3.2.2 电机控制器检查及更换

（1）整机拆卸：将电机控制器的各个螺栓、进出水管及高低压接插件拆卸后取下电机控制器，拆卸过程中防止冷却液进入各接插件；

（2）由专业人员根据电机控制器故障诊断及处理方法进行维修；

（3）重新安装电机控制器回整车；

（4）检查高压端子：要求对高压端子进行绝缘屏蔽包裹；

（5）检查屏蔽端子：要求对屏蔽端子进行绝缘胶带包裹；

（6）测量高压线与屏蔽线绝缘；

（7）安装高压端子：将高压端子安装回电机控制器，并用螺栓锁紧，高压端子应严格按壳体标识安装，以免装错；动力端子的扁平面与母排的平面紧贴，不允许使用折弯面安装；

（8）固定屏蔽线束：固定屏蔽端子，要求屏蔽端子与动力母线端子严格分开，不允许有接触；

（9）高压端子安装完成后应进行绝缘检测；

（10）安装所有罩盖，按照扭矩要求拧紧螺栓，最好使用扭矩扳手；

（11）装回低压接插件及低压电源；

（12）安装冷却管路，并检查泄露，不允许电机控制器内部留存空气。

（13）控制器防水等级为 IP67，请勿用高压水枪或其他工具冲洗控制器，如需清洗请用柔软干燥的棉布或其他布类擦拭，请勿用酒精或有机溶剂擦拭；

（14）维修保养完成后整车上电，通过车载绝缘检测设备实施绝缘检测，如有绝缘故障及时处理。

## 8.4 驱动电机维修保养要求

对车辆进行清洗时，尽量避免使用高压水流对电机高、低压接插件部位进行冲洗，以免造成电气故障以及绝缘失效故障。

### 8.4.1 驱动电机保养要求

（1）作业时必须断开整车低压电源、电机控制器高压电源，做好安全防护、知晓安

全注意事项、熟悉作业设备及工具、熟悉操作要求；

（2）维护保养作业时，应避免沙尘、雨雪气象情况下露天操作。避免沙尘、水分及其他杂质进入电机内部；

（3）维护保养作业时，需使用专业检测检修设备和绝缘工具，人员佩戴绝缘手套、穿绝缘鞋。所有操作均应进行断电、放电、高压 DC+/DC-对地电压检测，确保不带电操作；

（4）具体的作业内容及要求依据主机厂的维保手册执行。

### 8.4.2 驱动电机维修要求

驱动电机为高压电器件，维修时，需由专业人员配备专业设备进行操作，严禁非专业人员进行非法拆解,驱动电机从整车上拆下后，严禁进行单体拆解。

（1）关闭低压电源，拔掉高压电路维修开关，用放电导线夹对三相线端进行放电；

（2）用万用表检测三相线对地电压应≤30V.a.c，才可进行维修作业；

（3）检查电机水冷循环系统无泄漏防冻液现象；

（4）检查电机壳体有无破损，若有破损更换驱动电机；

（5）检查钢丝螺套有无损坏、装配不到位或脱落，若有更换驱动电机；

（6）检查三相高压连接铜排有无破损，若有更换驱动电机；

（7）检查低压接插座内针脚有无歪针、退针、断针，若有歪针，使用专用工具扶正，若有退针断针，则更换驱动电机；

（8）检查密封圈，若有遗失、损坏，补充或更换密封圈；

（9）检查花键轴润滑脂，若有不均匀，及时补充润滑脂；

（10）检查花键轴，若有磨损、断裂，需更换驱动电机；

（11）检查电机空载状态下，手动转动是否自如顺畅，若有卡滞、顿挫感，需及时检查排除，若无法解决，需及时更换驱动电机。

## 8.5 高压电连接类维修保养要求

### 8.5.1 高压线缆维修保养要求

（1）高压线束无断裂、老化龟裂、变色、烧蚀、外皮破损、导体外露现象，绝缘性能良好；

（2）高压线束固定牢靠，固定点无松动、脱落，驱动电机、转向电机、电动空压机的高压线束预留出（30~50）mm 的振动余量，与棱边有防护，与周边无磨损；

（3）高压线束与 B 级电压部件电连接部位，端子无缺陷，固定螺栓无松动、无端子

氧化、烧蚀现象，高压线束维修拆装后保证端子导电面清洁，无灰尘及油污，避免接触电阻变大，异常发热；

（4）检测高压线与地之间绝缘电阻高于 20MΩ；检测屏蔽层接地情况，接地电阻小于 0.5Ω；

（5）维修保养完成后整车上电，通过车载绝缘检测设备实施绝缘检测，如有绝缘故障及时处理。

### 8.5.2 高压连接器维修保养要求

（1）高压连接器不应有损伤、变形等缺陷，插接处不应有锈蚀引起的拆卸困难，高压连接器安装牢靠，无松脱现象，密封圈不应从护套中脱出；

（2）连接器绝缘电阻要求：高压连接器端子与屏蔽层之间绝缘电阻值≥20MΩ；

（3）高压连接器外壳无腐蚀、破损，连接器内部清洁无异物和水，高压连接器导电部位无氧化、异常发热、烧蚀现象；

（4）高压连接器经维修插拔后，保证插接到位，锁止结构安装到位，无虚接；

（5）维修保养完成后整车上电，通过车载绝缘检测设备实施绝缘检测，如有绝缘故障及时处理。

（6）连接器故障需直接更换高压线束总成，更换方法参见车辆自带的《维修手册》。

### 8.5.3 交直流充电插座维修保养要求

#### 8.5.3.1 交直流充电插座保养要求

建议定期对交直流充电插座进行清洁。

##### 8.5.3.1.1 交直流充电插座检查

（1）充电插座防护端盖完好无破损，座内部清洁，无异物及积水，绝缘性能良好，充电插座内部防水圈（若可见）无破损、脱落；

（2）充电插座翻盖及其锁止卡扣无破损、断裂，充电插座导电部位无氧化、异常发热、烧蚀现象；

（3）充电插座固定牢靠，无松脱，端子无发黑、断裂、簧片脱落等；

（4）车辆充电 30 分钟后（快充电池充电不少于 10 分钟），无充电插座温度报警；

（5）维修保养完成后整车上电，通过车载绝缘检测设备实施绝缘检测，如有绝缘故障及时处理。

##### 8.5.3.1.2 异常问题处理过程及措施

（1）交直流充电插座出现问题，需更换高压线束总成；

（2）若有异物，应使用带绝缘手柄的镊子等工具取出异物或风枪吹出异物；

（3）若有水渍，应使用干净的无尘布擦干（充电口端子不允许使用纸巾），或风枪吹干；

（4）若有粉尘，应使用尼龙软毛圆刷（软毛圆刷直径：直流插口建议为 10mm，交流插口建议为 5~6mm）和无尘布进行清洁。

#### 8.5.3.2 交直流充电插座维修要求

##### 8.5.3.2.1 交直流充电插座常见故障诊断及处理方法

| 故障描述 | 处理方法 |
| --- | --- |
| 绝缘故障 | 更换高压线束总成 |
| 过温故障 | 清理充电插座、更换充电枪，故障复现则更换高压线束总成 |
| 充电插座翻盖损坏 | 更换高压线束总成 |
| 端子烧蚀 | 更换高压线束总成 |
| 密封圈破裂 | 更换高压线束总成 |

##### 8.5.3.2.2 交直流充电插座维修前提要求

维修交直流充电插座前应确保：

（1）整车高压下电，移除动力电池维修开关；

（2）整车低压电下电。

##### 8.5.3.2.3 交直流充电插座维修检查及更换

充电插座故障需直接更换高压线束总成，更换方法参见车辆自带的《维修手册》。

### 8.5.4 充电枪维修保养要求

#### 8.5.4.1 充电枪保养要求

建议定期对充电枪进行清洁。

##### 8.5.4.1.1 充电枪检查

充电枪保护盖无破损、开裂；

端子周边无水渍、粉尘等异物；

端子无发黑、断裂脱落等；

充电线电缆无破损、开裂。

#### 8.5.4.2 充电枪维修要求

##### 8.5.4.2.1 充电枪常见故障诊断及处理方法

| 故障描述 | 处理方法 |
| --- | --- |
| 枪头或线束损坏 | 需更换充电线 |
| 充电功能失效 | 需更换充电线 |

#### 8.5.4.2.2 充电枪维修前提要求

非工作状态。

#### 8.5.4.2.3 充电枪维修检查及更换

需更换充电线总成。

## 8.6 功率电子类高压部件维修保养要求

功率电子类部件包括车载充电器，DCDC 转换器，DC/AC 逆变电源等。

### 8.6.1 功率电子类高压部件保养要求

对车辆进行清洗时，尽量避免使用高压水流对功率电子类高压部件接插件部位进行冲洗，以免造成电气故障。

### 8.6.2 功率电子类高压部件维修要求

#### 8.6.2.1 功率电子类高压部件维修前提要求

功率电子类高压部件为高压电器件，维修时，需由专业人员配备专业设备进行操作，严禁非专业人员进行非法拆解。

维修功率电子类高压部件前应确保：

（1）整车高压下电，移除动力电池维修开关；

（2）整车低压电下电。

#### 8.6.2.2 功率电子类高压部件更换

若为液冷系统，先分离液冷管路：

（1）断开冷却液管道；

（2）取出冷却液管卡环；

（3）拔下冷却液管；

（4）用水嘴套套住冷却液管道口与功率电子类高压部件水嘴口。

接着分离高压连接：

（1）分离低压接插件，断开低压线束；

（2）分离高压接插件，断开高压线束；

（3）取出功率电子类高压部件。

# 9.动力蓄电池回收再利用

遵循《节能与新能源汽车产业发展规划》要求，加强动力蓄电池梯级回收利用，在管理方法、体系建立上要明确各方责任、权利、义务。政府不但要引导电池生产企业对电池回收再利用，同时也鼓励发展专业化电池循环利用企业。

为了实现动力蓄电池回收再利用产业的环境效益和经济效益双赢的目标，必须用安全的措施来防范可能发生的安全事故，认识到“安全”才是其发展的根本。因此对于动力蓄电池回收再利用的循环经济发展产业，必须在各相关环节上进行事先的评估，采取切实可行的安全评估及防范策略，在过程中进行安全控制，从而实现动力蓄电池回收再利用行业的健康发展。

## 9.1 动力蓄电池回收梯次利用及再生利用概述

### 9.1.1 本文使用名词术语解释

《电动汽车安全性指南》界定的以及下列术语和定义适用于本文件

动力蓄电池：为电动汽车动力系统提供能量的蓄电池，由蓄电池包（组）及蓄电池管理系统组成，包括锂离子动力蓄电池、金属氢化物/镍动力蓄电池等，不含铅酸蓄电池。

废旧动力蓄电池是指：

(1) 经使用后剩余容量或充放电性能无法保障电动汽车正常行驶，或因其他原因拆卸后不再使用的动力蓄电池。

(2) 报废电动汽车上的动力蓄电池。

(3) 电池生产企业生产过程中报废的动力蓄电池。

(4) 经梯次利用后报废的动力蓄电池。

(5) 其他需回收利用的动力蓄电池。

以上废旧动力蓄电池包括废旧的蓄电池包、蓄电池模块和单体蓄电池。

回收：废旧动力蓄电池收集、分类、贮存和运输的过程总称。

拆卸：将动力蓄电池从电动汽车上拆下的过程。

拆解：对废旧动力蓄电池进行逐级拆分的过程。

贮存：废旧动力蓄电池收集、运输、梯次利用、再生利用过程中的存放行为，包括暂时贮存和区域集中贮存。

利用：废旧动力蓄电池回收后的再利用，包括梯次利用和再生利用。

梯次利用：将废旧动力蓄电池（或其中的蓄电池包/蓄电池模块/单体蓄电池）应用到其他领域的过程，可以一级利用也可以多级利用。

再生利用：对废旧动力蓄电池进行拆解、破碎、分离、提纯、冶炼等处理，进行资源化利用的过程。

汽车生产企业：获得《道路机动车辆生产企业及产品公告》的国内电动汽车生产企业和电动汽车进口商。

电池生产企业：国内动力蓄电池生产企业和动力蓄电池进口商。

报废汽车回收拆解企业：取得资质认定，从事报废汽车回收拆解经营业务的企业。

综合利用企业：是指符合《电动汽车废旧动力蓄电池综合利用行业规范条件》要求的废旧动力蓄电池梯次利用企业或再生利用企业。

梯次利用企业：即梯次利用电池产品生产及应用企业，是指对废旧动力蓄电池（或其中的蓄电池包/蓄电池模块/单体蓄电池）进行必要的检测、分类、拆解和重组，使其可应用至其他领域的企业。

再生利用企业：是指对废旧动力蓄电池进行拆解、破碎、分离、提纯、冶炼等处理，实现资源再生利用、原材料回收利用等的企业。

### 9.1.2 动力蓄电池回收梯次利用及再生利用流程

根据电动汽车相关规范和要求，动力蓄电池梯次利用及再生利用流程、回收服务网点作业规程见图 9-1-1、图 9-1-2、图 9-2。


图 9-1-1

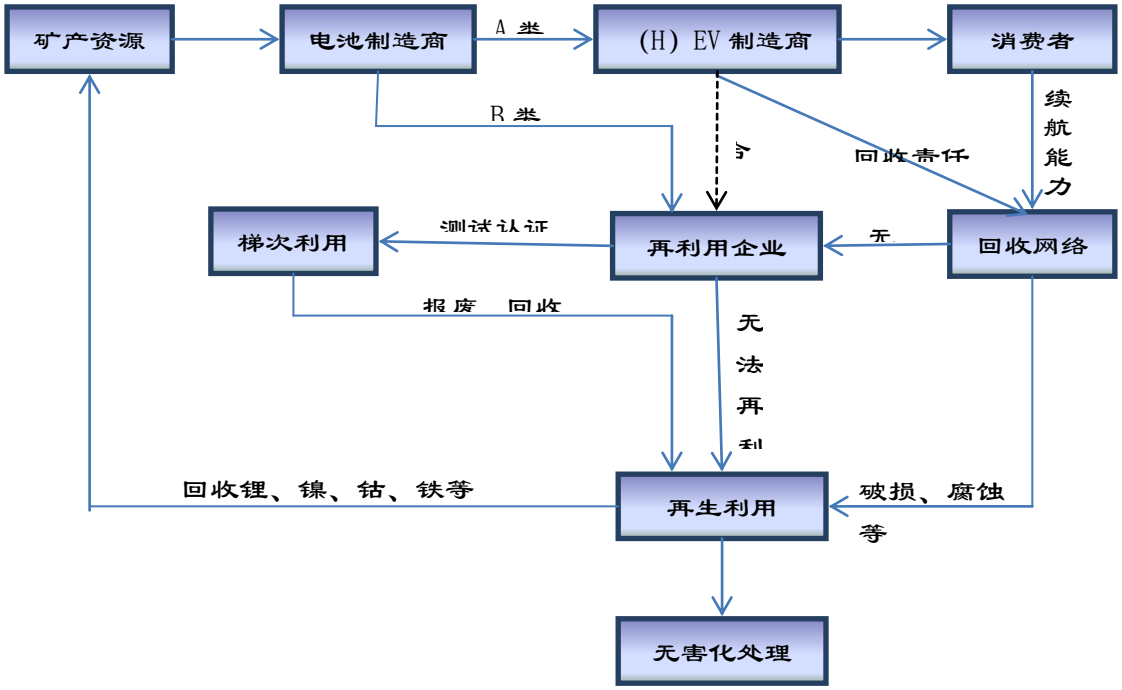

矿产资源
电池制造商
A 类
(H) EV 制造商
消费者
续航能力
R 类
梯次利用
再利用企业
回收网络
无
报废 回收
无法再利
回收锂、镍、钴、铁等
再生利用
破损、腐蚀等
无害化处理

图 9-1-2

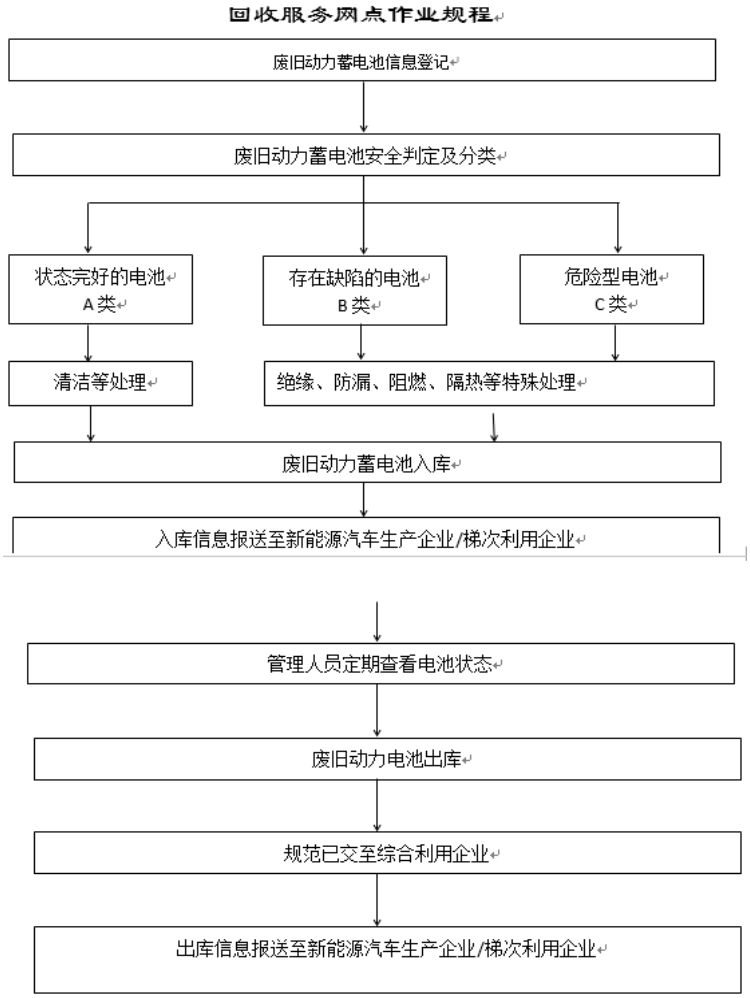

回收服务网点作业规程
废旧动力蓄电池信息登记
废旧动力蓄电池安全判定及分类
状态完好的电池
A类
存在缺陷的电池
B类
危险型电池
C类
清洁等处理
绝缘、防漏、阻燃、隔热等特殊处理
废旧动力蓄电池入库
入库信息报送至新能源汽车生产企业/梯次利用企业
管理人员定期查看电池状态
废旧动力电池出库
规范已交至综合利用企业
出库信息报送至新能源汽车生产企业/梯次利用企业

图 9-2

### 9.1.3 环境安全

#### 9.1.3.1 总体要求

从事动力蓄电池综合利用企业及梯次利用企业，总体要求应遵循下列要求：

1、各相关企业应建立健全各部门安全环保责任制

（1）综合利用企业及梯次利用企业应组织制定部门安全环保规章制度和操作规程。

（2）综合利用企业及梯次利用企业应定期开展安全环保检查，消除事故隐患。

（3）综合利用企业及梯次利用企业应定期进行各部门人员的安全环保培训，企业相关责任人应定期进行考核，并督促落实安全环保制度实施，消除安全环保隐患。

2、各相关企业全产业链环境安全要求;

（1）综合利用企业及梯次利用企业应对综合利用过程中产生的有毒有害、易燃易爆等残余物（包括废料、废气、废水、废渣等）进行妥善管理和无害化处理，无相应处置能力的，应按相关要求交由具备相关资质的企业进行集中处理。

（2）综合利用企业及梯次利用企业运输过程应符合国家相关法律法规标准要求，尽量保证蓄电池结构完整，采取防火、防水、防爆、绝缘、隔热、防震等安全保障措施，并制定应急预案。

（3）综合利用企业及梯次利用企业噪声排放应符合 GB 12348 要求，具体标准应根据当地人民政府划定的区域类别执行。

（4）综合利用企业及梯次利用企业作业环境应符合 GB Z1、GBZ2 要求；

（5）梯次利用企业应参照《生产经营单位生产安全事故应急预案编制导则》（GB/T 29639）的要求编制安全环保应急预案，具有安全环保应急处置能力。定期检查贮存废旧动力蓄电池的状态，如发现有安全、环保等隐患应及时采取措施处置并移交至综合利用企业。

## 9.2 动力蓄电池回收网络和储运安全

### 9.2.1 梯次电池企业的责任及义务

从事动力蓄电池综合利用企业及梯次利用企业，在责任及义务方面应遵循下列要求：

#### 9.2.1.1 汽车生产企业提供梯次电池企业共享梯次电池运营数据信息

（1）汽车生产企业提供梯次电池企业共享梯次电池电压、容量、锂离子类别、串并联等信息；

（2）汽车生产企业提供梯次电池企业共享梯次电池循环次数、电池生产时间等信息；

（3）汽车生产企业提供梯次电池企业共享电池系统结构设计信息。

### 9.2.2 回收动力蓄电池运输前电池系统处置要求

从事回收动力蓄电池的企业，在责任及义务方面应遵循下列要求：

（1）运输之前电池及电池容量最低及最高数值应符合安全运输的要求。

### 9.2.3 回收动力蓄电池运输前包装要求

#### 9.2.3.1 回收动力蓄电池运输前包装规范，堆叠要求

从事动力蓄电池综合利用企业及梯次利用企业在回收动力蓄电池时，在包装规范，堆叠方面应遵循下列要求：

（1）综合利用企业制订回收动力蓄电池运输前电池单体及电池系统包装要求，在防振动、防水、防晒、防碰撞等方面作预处理，应采用箱装，包括普通木箱、胶合板箱、金属箱、塑料箱、纸质等符合第九类危险品对应的二类包装的要求，依据包装容器的质量和特点，材质、型式、规格、方法和动力蓄电池重量进行选用，便于装卸、运输和储存；

（2）净重不超过 400kg 的 A 类及 B 类废旧动力蓄电池按照《危险货物运输包装通用技术条件》（GB 12463）的要求实施包装，净重超过 400kg 的按照《危险货物大包装检验安全规范》（GB 19432）的要求实施包装；

（3）B 类废旧动力蓄电池的包装应具有足够的强度，承受正常运输条件下的各种作业风险；

（4）C 类废旧动力蓄电池应根据其特性选择相应的包装材质，不得与其他货物混合包装，包装应能够有效阻断电池废液等渗漏；

（5）综合利用企业制订回收动力蓄电池运输前电池单体及电池系统在叠放层数上作规定，木箱或者纸箱包装分别对应各自的承重能力规定叠放层数限制， 以防运输中途发生碰撞及摩擦导致安全事故发生；

（6）电池的包装箱上应贴有“准备处理的锂电池组”或“准备回收的锂电 池组”等内容的标签，按照《危险货物包装标志》(GB 190)的要求进行标志；

（7）处理后的电池的包装箱上应贴有“损坏/残次品锂电池或锂电池组”等内容的标签；

（8）电池的包装箱上应贴有紧急联系人信息。

#### 9.2.3.2 回收动力蓄电池运输工具的要求

从事动力蓄电池综合利用企业及梯次利用企业在回收动力蓄电池时，在运输工具方面

应遵循下列要求：

（1）运输电池货物前，综合利用企业与汽车生产企业应共同制定运输路线和运输应急预案；

（2）运输电池货物时，应采取防止污染环境的措施，并遵守国家有关危险货物运输管理的规定；

（3）运输电池货物的车厢应保持清洁干燥，不得任意排弃车上的残留物，运输结束后被动力蓄电池污染过的车辆，应到具备相应条件的地点进行清洗处理；

（4）运输电池货物的车辆禁止搭乘无关人员；

（5）运输电池货物的车辆不得在居民聚居点、行人稠密地段、政府机关、名胜古迹、风景游览区停车。如需在上述地区进行装卸作业或临时停车，应采取安全措施。

#### 9.2.4 回收动力蓄电池信息追溯要求

从事动力蓄电池综合利用企业及梯次利用企业，应遵循《新能源汽车动力蓄电池回收利用溯源管理暂行规定》，在信息追溯方面具体应遵循下列要求：

1、专用回收电池系统本体标识要求

（1）回收前在各电池及电池系统上统一位置贴对应的追溯编码序列号标签。

（2）追溯编码序列号标签按 GB/T 34014-2017《汽车动力蓄电池编码规则》进行编制。

2、 回收动力蓄电池及电池系统数据信息追溯与实物对应的要求

梯次利用企业将各电池对应的序列号编码分类别进行管控及追溯。

## 9.3 动力蓄电池回收再利用检测分类及拆解安全

### 9.3.1 一般要求

#### 9.3.1.1 安全拆解工具及设施使用要求

从事动力蓄电池拆解的梯次利用企业，在安全设施及拆解工具方面应遵循下列要求：

（1）梯次利用企业应具备满足耐腐蚀、坚固、防火、绝缘特性要求的专用分类收集储存设施；

（2）梯次利用企业应具有高压绝缘手套、防高压电弧面罩、绝缘电弧防护服等安全防护工具，绝缘救援钩、自动体外除颤器、医用急救箱等救援医护设备；

（3）梯次利用企业应具备有毒有害气体、废水废渣处理等环境保护设施和应对相应

火灾危险性类别的安全消防设备；

（4）应具备危险废物临时贮存仓库用以收集破损时泄露出来的冷却液、电解液等有毒有害液体和含重金属的电池材料，场地地面应进行防腐、防渗处理，并建有防腐、防渗的紧急收集池；

（5）梯次利用企业应具备动力蓄电池编码信息追溯和管理设备；

（6）梯次利用企业应具备绝缘检测设备，如绝缘电阻测试仪等；

（7） 梯次利用企业应具备国家相关规定的消防设施，如消防栓、沙箱、灭火器等；

（8）梯次利用企业应配备专用起吊工具、专用拆解工作台、绝缘套装工具等，专用拆解工作台需要可靠接地。

#### 9.3.1.2 场地要求

从事动力蓄电池梯次利用的企业，在场地方面应遵循下列要求：

（1）梯次利用企业厂房建筑应符合 GBZ 1 要求，建筑耐火等级和照明设计应符合 GB 50016 和 GB 50034 的要求；

（2）梯次利用企业厂区应按照 GB 50140 要求配置灭火器，设计有给水排水工程的应符合 GB 50069 规定；

（3）梯次利用企业车间应具备通风设备、废液处理设施及废渣收集设施；

（4）梯次利用企业场地应建有围墙并按处理工艺划分功能区域，宜划分为贮存区、处理区、分析检测区、管理区等，各功能区域应有明显的界线和标志。

#### 9.3.1.3 人员要求

从事动力蓄电池梯次利用的企业，在人员方面应遵循下列要求：

（1）作业前，应按 GB/T 11651 的要求穿戴和使用劳动保护用品，未按要求执行的人员不得靠近作业区和操作设备；

（2）应掌握事故应急处理和紧急救护的方法；

（3）应定期体检，并符合 GBZ 188 规定，人员健康状况应符合工作性质要求；

（4）操作人员应接受岗前培训和定期培训，并通过考核；

（5）梯次利用企业应配备专业技能满足环保作业、安全操作（含危险废物收集、存储、运输）、急救知识等要求的相应专业人员，并持有相应的资格证书。

#### 9.3.1.4 梯次利用企业安全拆解规范

从事动力蓄电池梯次利用的企业，在安全拆解规范方面应遵循下列要求：

（1）电池系统拆解过程严禁单独操作；

（2）拆解前首先检查工具及设施，确认安全正常使用；

（3）拆解前制订安全拆解程序或作业指导书，按照指定的拆解作业程序或作业指导书进行拆解；

（4）拆解时无关人员禁止在场，并做好安全防护处理预案。

#### 9.3.1.5 梯次利用企业物料管控要求

从事动力蓄电池梯次利用的企业，在企业物料管控方面应遵循下列要求：

（1）拆解后的电池模组及电池单体应进行绝缘防护处理，并做绝缘标记；

（2）对拆解后的动力蓄电池应做带电标记，并及时转移至悬挂有警示标志的存储区域进行隔离；

（3）拆解后，零部件、材料、废弃物不得随意丢弃，应分类储存在专用容器中，并标识，避免混存、混放；

（4）废油液、废电路板等危险废物应设专人进行管理，贮存应按 HJ 2025 的要求执行，并定期进行规范转移；

（5）冷却液的贮存应按 GB 29743 的要求执行。

### 9.3.2 梯次利用企业电池系统拆解安全要求

从事动力蓄电池梯次利用的企业，在电池系统拆解安全方面应遵循下列要求：

（1）应采用专用起吊工具和起吊设备将回收动力蓄电池系统起吊至专用拆解工作台；

（2）应使用绝缘工具拆除高压线束、线路板、电池管理系统、高压安全盒等功能部件；

（3）拆解过程中应避免金属物件与高低压接头进行接触，以免造成短路起火。

### 9.3.3 梯次利用企业电池模组拆解安全要求

从事动力蓄电池梯次利用的企业，在电池模组拆解安全方面应遵循下列要求：

（1）应采用专用模组拆解设备对模组进行安全、环保拆解；

（2）应采用专用起吊工具及起吊设备将模组起吊至拆解工作台；

（3）应采用绝缘工具拆除模组上导线、连接片等连接部件；

（4）拆解过程中应做好绝缘防护措施，对高低压连接接头应用绝缘材料及时进行封堵，不应徒手拆解模组。

### 9.3.4 梯次利用企业拆解分选过程中的检测安全

#### 9.3.4.1 梯次利用企业分选检测的防护要求

梯次利用企业在对动力蓄电池分选检测时，应遵循下列防护要求：

（1）检测设备接地装置应符合 GB 50057-2010 规定；

（2）作业前，应按 GB/T 11651 的要求穿戴和使用劳动保护用品，未按要求执行的人员不得靠近作业区和操作设备。

#### 9.3.4.2 梯次利用企业分选检测的操作安全

梯次利用企业在对动力蓄电池分选检测时，应遵循下列操作安全要求：

（1）操作人员应接受岗前培训和定期培训，并通过考核；

（2）操作检测设备的人员在使用前必须熟悉使用说明，严格按照操作规程进行操作；

（3）检测设备应定期进行校验，定期进行点检及维护保养；

（4）测试场所应具备国家相关规定的消防设施，如消防栓、沙箱、灭火器等。

### 9.3.5 梯次利用企业电池分级分选要求

梯次利用企业电池分级分选时，需测试电池开路电压及内阻，通过化成分容进行分级分选，以提高电芯一致性。

## 9.4 动力蓄电池回收再利用电池组设计安全要求

### 9.4.1 梯次电池系统的设计安全

梯次电池系统包含有梯次电池，电池管理系统，结构件，线束等四大部分组成，系统的安全性设计须从梯次电池的分选，电子电气的设计，阻燃结构，热管理设计、多重防燃烧设计、以及电池管理系统的设计等几方面综合考虑进行设计，保证系统的安全性。

#### 9.4.1.1.梯次电池的分选

根据梯次电池或模组容量、电压、内阻、自放电对电芯或模组进行严格分选后配组使用，不同的应用场景有不同的要求。

#### 9.4.1.2 梯次电池组电子电气的设计要求

梯次电池组的电子电气设计从警示标识、接触防护、绝缘防护、外短路防护、过电流防护等方面考虑。

（1）警告标识底色为黄色，边框应使用黑色。当人员接近电池系统时，应能清晰地看到该警示标识，提醒人员注意高压安全。推荐使用 GB 2894-2008《安全标志及其使用导则》；

（2）直接接触防护在设计上采用绝缘、防护罩、遮拦等措施；间接接触防护在设计上采用等电位（保护接地）、保护切断、漏电保护等措施；

（3）梯次电池组的电绝缘设计主要通过电芯、模块和系统三个方面进行；

（4）为防止电池短路及过载现象的发生，需在电池系统回路中选用熔断器进行保护。熔断器被设计成回路中最薄弱的环节，在正常工作下，熔断器不会熔断。当回路中发生短路或严重过载时，熔断器中的熔丝或熔片会立即熔断，以保护电路及电气设备。

（5）过流保护设计指当电池系统在运行过程中监测到电流超出规定的范围和持续时间时，电池系统将此异常信息发送给 BMS，并要求降功率运行，回路电流在规定的时间内，电流还未下降至规定的范围内，电池系统将通过切断整个回路的电流，保证整个电源回路不会因为长时间过流导致起火、爆炸的事件发生。

#### 9.4.1.3 热管理设计要求

动力电池热管理设计两个重要内容：

（1）保持电池内和电池间的温度均衡；

（2）把电池绝对温度控制在合理范围内，梯次电池组的热管理设计须满足梯次电池组在不同行业的环境温度条件下使用；

（3）要具备阻燃结构设计。

#### 9.4.1.4 阻燃结构设计要求

防火与阻燃可以从两方面来考虑：1）被动防火与阻燃；2）主动防火与阻燃。

被动防火与阻燃指的是在电池系统设计时， 电池系统的零部件尽量使用阻燃等级比较高或者不能燃烧的材料。 电池系统内部的塑胶件， 达到一定的阻燃等级，高低压线束选用阻燃等级较高的产品。高低压线束，建议选择耐温 125℃以上。参考 GB/T 2408-2008《塑料 燃烧性能的测定 水平法和垂直法》

主动防火与阻燃设计可以从两方面来考虑：一是在电池系统设计中，加入防火结构来防止外部的火焰直接进入箱体内部；二是在动力电池系统设计时，在箱体内部增加消防系统。

#### 9.4.1.5 多重防燃烧机制设计

梯次电池的应用问题要有多次安全处理机制，要从机制上主动防燃烧和燃烧预警以及被动防燃烧处理。

（1）主动防燃烧

充电中，应考虑多级保护措施，避免电池在各种异常情况下不发生过压，引起电池充电事故。要考虑通讯的冗余设计，确保通讯的准确性和精确性。

（2）燃烧预警

在电芯将要失效的前，根据电池的各种运行参数，和报警信号要做到提前预警，避免

事故的发生。

（3）被动防燃烧

利用防燃烧机制阻断火源和空气氧气的接触，比如六氟七丙烷等。

#### 9.4.1.6 梯次电池组生产流程的安全要求

应考虑电池采样端子的防呆，按照管理系统规格书约定的顺序安装。避免不必要的操作失误引起对管理系统的损坏。

电池正负极的采用防呆设计，避免后续安装反接导致的隐患。

### 9.4.2 电池管理系统对安全的要求

#### 9.4.2.1 管理系统的可靠性设计

（1）绝缘检测、短路保护及其恢复、过流保护及其恢复，符合应用场景的行业规范或国家规范；

（2）电磁干扰设计要符合相关的应用领域的电磁干扰设计要求；

（3）电池管理系统应该具有较低的温升，增加其可靠性，减少对电池局部热辐射；

（4）要防止启动大电流或者运行当中电流突变，对梯次电池的瞬时大电流冲击；

（5）针对应用场景，可靠性设计指标（MTBF）应达到标准要求。

#### 9.4.2.2 管理系统对充放电安全管理要求

（1）梯次电池产品充电电流设计应该符合充电设计要求；

（2）梯次电池产品放电电流设计应该符合放电设计要求、温升要求；

（3）过充、欠压、过温保护等要符合行业规范或国际标准。

#### 9.4.2.3 电池对故障管理要求和在线监测和分析

电池管理系统对于电池出现各种故障进行告警，电池管理系统应能根据故障等级，给出可区分的告警指示。

通过对电池的运行参数的解析，得到电池的衰减状况，从而调整电池运行参数，规避风险。

## 9.5 动力蓄电池回收再利用电池生产安全要求

### 9.5.1 检测

动力蓄电池回收利用应进行安全判定检测，检测项目如下图表 9-3（见附表 1）所示。

#### 9.5.1.1 外观检测

（1）检测人员需进行相关的上岗培训，具备一定的安全防护知识，且配备相应的绝

缘措施，如：绝缘手套、绝缘鞋（靴）等；

（2）检测设备、工具需进行绝缘，避免使用过程中造成电池组短路；

（3）检测区域需进行明确划分，并作出标识，合理设立安全逃生通道。

#### 9.5.1.2 性能检测

1、分容、配组

（1）分容设备宜采用分体设备，即装电池部分和设备电控部分分开，设备应具备电池电压、电流、容量异常报警功能，具备安全诊断能力，试验全局保护和分局保护（全局保护即在化成的各个步骤都有电压过高、电压过低、电压变化率异常等诊断功能；分布保护即每个步骤检查其参数有无异常，如该工步充、放电容量值等），对动力蓄电池的充放电设备宜有两个电压参考基准实现安全冗余；

（2）配组工序在周边安全范围内，不可布置明火工序或高火灾风险的工序；

（3）分容工序应具备事故通风能力,以保证车间空气流通。

2、老化

（1） 应明确规划放置区域，试验电池与生产电池应有区分；

（2）若电池间摆放需进行隔离时，隔离物应为不燃材料；

（3）应采用远程或现场监控措施，并安装烟感、温感报警器；

（4）车间应就近配置足够的灭火器材、个人防护装备以及应急物品；

（5）老化房间应设立防火墙，与相邻的房间应无门、窗或洞口。

### 9.5.2 梯次电池组装

（1）相关操作人员需参加对应岗位培训，可按照对应作业指导书进行操作，具备相应的安全操作技能；

（2）车间设施和设备等具备防止电池组外短路、高压电弧的保护措施；

（3）高压区域的设备应具有安全自锁、故障自诊断等功能，避免接错线路的电池模组、电箱短路燃烧；高压区域应隔离，相关工作人员需具备一定的专业知识以及相关安全知识；

（4）电池组的装配及测试过程需做好绝缘措施，接触电池组的工具裸露部分宜缠绕绝缘材料，减少短路风险；相关工作台面及地面做好绝缘，避免电池模组带电导线接触接金属导体造成短路或电弧伤害；

（5）生产周转工序建议增加带防碰撞、防跌落等防护措施的周转箱或周转托盘；

（6）车间现场需有明确的区域划分，各岗位工序需满足操作要求，接触相关电子元

器件岗位需做好防静电处理，如：佩戴静电手环、地面做静电处理等；

（7）车间现场应配备火灾爆炸事故发生时的应急隔离措施，能够将电池组有效隔离；

（8）车间现场应配有消防栓、灭火器、消防水桶或消防沙袋等应急物品，并合理设立逃生通道，发生异常情况时，能够正确使用应急物品。

### 9.5.3 梯次电池功能及性能检测

（1）检测过程应配备具有电池组检测知识的专业人员全程进行监控；

（2）检测过程应采取必要的绝缘措施，如绝缘手套、绝缘鞋（靴）、绝缘工具等；

（3）检测仪器、仪表需满足安装要求，且针对特殊操作规范的仪器、仪表需有明显安全标识，如：高压危险、请勿靠近等；

（4）检测过程应在温度应为 25℃±5℃，相对湿度为 15%～90%，大气压力为 86kPa～106kPa 的环境中进行；

（5）检测区域应作出明确标识，需配备单独的隔离区域，可对现场异常进行隔离处理，且合理设立安全逃生通道，并配备相应的消防栓、灭火器、消防沙袋等应急物品。

### 9.5.4 仓储

（1）仓储场地的地面须做硬化、防渗漏及绝缘处理，按照《环境保护图形标志-固体废物贮存（处置）场》（GB 15562.2）的要求设置固体废物的警告标志，同时在显著位置设置危险、易燃易爆、有害物质等警示标识，并在地面设置黄色标志线。参照《废蓄电池回收管理规范》（WB/T 1061）、《电池废料贮运规范》（GB/T 26493）和《一般工业固体废物贮存、处置场污染控制标准》（GB 18599）的要求开展废旧动力蓄电池贮存工作；

（2）废旧动力蓄电池的贮存应根据动力蓄电池类型（磷酸铁锂、三元等）及分类结果采用不同的贮存方式，具体如下：

同一类型的 A 类（A、B、C 分类见图 8-2）废旧动力蓄电池应采用隔开贮存。

不同类型的 A 类废旧动力蓄电池及同一类型的 B 类废旧动力蓄电池应采用隔离贮存。

不同类型的 B 类废旧动力蓄电池及 C 类废旧动力蓄电池应采用分离贮存。

贮存方式应符合下表中各项规定：

| 贮存方式要求 | 隔开贮存 | 隔离贮存 | 分离贮存 |
|---|---|---|---|
| 贮存区间距/m | 0.5-1.0 | 0.3-0.5 | 0.5-1.0 |
| 通道宽度/m | 1-2 | 1-2 | 5 |
| 墙距宽度/m | 0.3-0.5 | 0.3-0.5 | 0.3-0.5 |

（3）成品电池组长期存放时，建议定期进行安全检查，现场安装监控、烟感和温感报警器；

（4）仓库搬运者应使用合适的搬运工具（如叉车、推车等），电池运输时应轻取轻放，避免电池组受到机械损伤；

（5）仓库应有相应区域划分，并设置隔离区域，有效预防电池组异常蔓延；

（6）仓库内应合理配备消防栓、灭火器、消防水桶或消防沙袋，并合理的设立逃生通道。

## 9.6 梯次电池使用安全要求

### 9.6.1 梯次电池使用场景及要求

（1）锂离子电池有最佳的使用温度范围，超过使用范围易发生安全问题。电池上限使用温度最好低于 45℃，较高温度下使用，易引发热失控安全问题。低温充电负极易发生析锂，要控制充电方式，0℃以下应恰当的减小充电电流或禁止充电；

（2）需要在超出温度范围下长期工作，应采用电池内置加热或降温元件或使用空调恒温等,将电池控制在适宜温度；

（3）存放时间超过半年的电池，再次使用时，应采用小电流充放电激活后再正常使用。充电速度与使用寿命以及安全风险相关性较强,在条件允许的情况下，选择小倍率充电；

（4）应该避免在高温下长期满电存储的电池，防止电池性能衰减，安全风险升高；

（5）对于备电使用的梯次电池，宜要考虑长期备电时电池带电量的适宜量，实现保证备电电量充足，又能达到电池带电存储的安全状态；

（6）对于储能使用的梯次电池，宜设定适当的浅充浅放充电放电策略。实现延长电池使用寿命的目的，降低安全风险。

### 9.6.2 充放电电流、电压、保护功能要求

（1）梯次电池使用时，充放电电流和电压应根据使用环境进行适当的调整。使用温度趋于电池使用温度极限时，充放电电流和电压应适当降低；

（2）充电设备需符合电池充电最高电压、最大允许电流、温度限值、单体极值等要求，应具备安全与保护机制。充电过程中，充电设备应监控充电电压、电流、温度的变化，当超过所限定的允许充电限值时，应及时做停机保护；

（3）用电设备需适配电池工作电压范围，电流允许范围。放电过程中，当检测到电

池电压或电流超标后，应具备主动实施功率限制，防止电池超功率运行发生损坏。

### 9.6.3 电池的安装及施工要求

（1）容量较小的梯次电池可设置可靠的锚点固定或其他结构固定。当堆叠时不宜过高过多，应考虑电池散热能力、箱体承重以及稳固性，防止温度累积、电池滑落或意外移动引起安全风险；

（2）容量较大的梯次电池宜采用电池柜安装。电池柜应通风、散热良好。电池柜应可靠、牢固，承重后日久使用不变形；

（3）大规模部署的梯次电池应安装在电池室内，电池室应有良好通风和照明、温度适宜，自动消防装置。电池室安装在楼面时，楼面承重应能满足需要。电池应采用适当的方式进行固定，防止滑落或意外移动引起安全风险；

（4）梯次电池组的连接线须采用国标导线连接，连接线规格应与电池容量、馈电距离相匹，满足载流量及电压降的要求。连接的导线、相互接触的导体或者裸露的带电零部件应具有符合绝缘保护或绝缘距离。螺钉、螺母、应充分固定并能够承受正常使用所产生的机械应力，所有电气连接的电缆端子或接头应符合连接强度要求。防止松动引起的绝缘或阻抗升高引发的安全隐患。

### 9.6.4 使用防护要求

（1）使用时，电路系统应有过流与短路的自动保护功能，过流或短路故障排除后应自动或人工恢复正常工作状态；

（2）梯次电池在接入设备系统时，应配置规格适宜断路器，断路器应具备电流超标自动断开功能以及手动断开和恢复功能。在回路电流发生电流异常时能够进行保护性断开动作；

（3）梯次电池在接入设备系统时，应配置规格适宜熔断器装置，在回路电流发生电流异常时能够进行保护性断开动作；

（4）当断路器与熔断器配合时，应考虑动作特性的不同，对级差做适当调整；

（5）安装后梯次电池应摆放整齐并保证足够的空间和间距，防水、防尘、防雷以及恒温。数量较多的梯次电池柜或电池舱室应配置自动消防装置。

### 9.6.5 运行监控要求

（1）梯次电池使用时，应对电池的总电压、单体电压、电流和温度的参数信息进行监控，当参数超出安全风险级别时，应主动停止充放电并启动告警。当单体电压和温度发生突变或超常时，应发出告警并限制使用；

（2）大规模部署的梯次电池，运行过程中需校验 BMS 数据，对电池的关键参数，如电池总压、单体电压、温度极值，以及 SOC、SOH 等信息进行实时监测，当发现可能导致安全风险时，应主动停止充放电并启动告警，通知人工处理。

#### 9.6.6 定期检查与维护要求

（1）部署梯次电池的用户应定期组织专业人员对电池进行检查和维护。需定期检查电池箱体、面板部件是否清洁干净，电池输出端子表面应无积尘，通讯端子、指示灯正常工作。铜耳绝缘帽应无脱落、螺栓紧固良好且无烧灼氧化变色等异常、插头塑料件无融化迹象、线缆无脱落或破损；

（2）对于备电使用场景，应定期进行以下维护和诊断

定期放电：由于梯次电池长期备电运行，不利于电池性能保持，应该定期放电维护。宜每一个月应进行一次放电，用小电流以恒流放出一定比例容量的电量，并及时用相应电流进行恒流限压充电，恢复带电量。

核对性放电：宜至少每隔 2 年进行一次核对性试验，运行了 4 年以后的梯次电池，应至少每年作一次核对性放电。进行核对性放电后应及时进行充电。经过核对性放充电，梯次电池组容量达不到预定使用效果的，建议更换。

（3）对于储能使用场景，应定期进行以下维护和诊断

核对性放电

宜至少每隔 1 年进行一次核对性试验，运行了 2 年以后的梯次电池，应至少每半年作一次核对性放电。进行核对性放电后应及时进行充电。经过核对性放充电，梯次电池组容量均达不到达不到预定使用效果的，建议更换。

## 9.7 动力蓄电池材料再生利用安全要求

### 9.7.1 一般要求

#### 9.7.1.1 人员要求

（1）应建立和健全安全生产管理机构，按规定配备专职安全生产管理人员；生产经营主要负责人、安全生产管理人员都应具有安全生产管理资格证；

（2）定期对员工进行安全法律法规、安全生产规范和劳动保护等安全教育培训，经过考试合格后方可上岗；

（3）特种作业和特种设备人员必须按照国家有关规定经专门的安全培训机构培训，取得特种作业操作资格证书和特种设备作业人员证书后方可上岗作业；

（4）上岗前，作业人员应按规定穿戴齐全劳动防护用品，确保规范，有效；

（5）外来参观、学习等访客人员，入厂前必须接受相应的安全教育，并在专人引导下进入；

（6）建议建立监护人制度：作业中应指派有经验、掌握作业危险处置的人员担任监护人，在吊装作业、动火作业、受限空间作业、高处作业时安全管理人员应在现场进行监督。应及时制止违章作业，在发生危险时采取紧急救援措施，在作业完成后，应会同有关人员清理现场。

#### 9.7.1.2 再生利用工具及设备要求

（1）吊装设备：必须状况良好，检验合格，具有起重机主管部门颁发的使用许可证；起重机械上的各种安全防护装置及监测，指示，自动报警信号装置等应齐全完好，安全防护装置不完整或已失效的起重机械不得使用；吊装工作区域应有明显标志，并设专人警戒，与吊装无关人员严禁人内；

（2）大型设备：粉碎机入口应有防错设施，确保人员不会误入或人员进入检修时设备不会启动；开关应有明显标识，具有防误操作的机构；

（3）应进行废水、废气、噪声排放的日常控制和管理，做好废气废水废渣处理设施的运行记录，应规定保存期限；

（4）企业对涉及煤气、氧气、氢气等易燃易爆危险化学品生产、输送、使用、储存的设施以及油库、电缆隧道(沟)等重点防火部位，应当按照有关规定采取有效、可靠的防火、防爆和防泄漏措施。企业对具有爆炸危险环境的场所，应当按照《爆炸性环境设备通用要求》（GB3836）及《爆炸危险环境电力装置设计规范》(GB50058)设置自动检测报警和防灭火装置；

（5）企业对反应槽、罐、池、釜和储液罐、酸洗槽应当采取防腐蚀措施，设置事故池，进行经常性安全检查、维护、保养，并定期检测，保证正常运转。企业实施浸出、萃取作业时，应当采取防火防爆、防冒槽喷溅和防中毒等安全措施。

#### 9.7.1.3 原材料要求

（1）带电原材料：在运输、生产过程中应保证带电原材料不会因短路、磕碰等原因导致起火爆炸；

（2）不带电原材料：确保粉料不散播到空气中，确保车间人员健康安全；

（3）原材料如残留电解液，需有收集容器将电解液收集，不能直接渗漏到地面上，亦不能将电解液烘干直接排放到大气中。

#### 9.7.1.4 方法要求

（1）应进行危险、有害因素辨识，并制定相应安全措施：包括但不限于工艺安全、能量隔离；

（2）应有各种应急预案，包括但不限于火灾爆炸、生产安全、特种设备、职业卫生、有毒有害作业等预案，定期组织人员疏散演习；

（3）针对吊装工位，应严格遵守国标或行业标准，如（HG30014）；

（4）按照法律法规、行业标准或企业规范要求，所有应保留适当形式的文件或记录的信息，作为证据应予以保留一定年限；

（5）企业应当建立有限空间、动火、高处作业、能源介质输送等较大危险作业和检修、维修作业审批制度，实施工作票(作业票)和操作票管理，严格履行内部审批手续，并安排专门人员进行现场安全管理，确保作业安全。

#### 9.7.1.5 环境和场地要求

（1）新建、改建及扩建项目的设计应按相关国家标准设计及验收；

（2）车间及厂区环境与卫生应符合 GBZ1《工业企业设计卫生标准》、GBZ2.1《工业场所有害因素职业接触限值第 1 部分：化学有害因素》、GBZ2.2《工业场所有害因素职业接触限值第 2 部分：物理有害因素》、GB3095《环境空气质量标准》、GB12348《工业企业厂界环境噪声排放标准》要求；

（3）厂区内，应按照 GB15630《消防安全标志设置要求》的规定设置必要的消防设施和消防通道，设置消防设施的地点应有明显的标志牌；

（4）禁火区域严禁吸烟和携带火种进入。

### 9.7.2 再生利用过程安全要求

#### 9.7.2.1 单体电芯拆解

（1）应进行无害化拆解，不推荐人力进行；

（2）拆解前应确保电芯电压处于安全范围；

（3）拆解过程中产品废水废气废渣根据相应环保标准进行处理。

#### 9.7.2.2 湿法冶炼

（1）应按照国家安全生产监督管理总局令第 91 号《冶金企业和有色金属企业安全生产规定》和国家安全生产监督管理总局令第 26 号《冶金企业安全生产监督管理规定》中相关要求执行；

（2）进罐作业前应有工作量和时间分析并制定工作路线，作业时应防止人员中毒或

窒息；

（3）对空气中可燃气体进行检测及报警；

（4）对作业区域进行有毒有害因素的检测并记录；企业在使用酸、碱的作业场所，应当采取防止人员灼伤的措施，并设置安全喷淋或者洗涤设施；

（5）实行多班作业时要认真执行交接班制度，做好记录和检查工作。

### 9.7.3 仓储要求

（1）参考 9.2.3.1 及 9.5.4；

（2）废渣严禁直接倾倒，应集中储存，交与有回收资质的厂家处理。

## 9.8 动力蓄电池回收再利用安全数据管控要求

### 9.8.1 动力蓄电池回收再利用溯源管理

数据信息溯源须在电池回收及储运、回收再利用检测分类及拆解、再利用电池组设计、再利用电池生产、梯次电池使用、动力电池材料再生利用、安全事故处理这七大环节中，实现数据、对象和应用场景之间的全流程立体可追溯。

#### 9.8.1.1 各个流程阶段的数据管理

1、对象编码

（1）在电池回收过程中，应按照《GB/T 34014-2017 汽车动力蓄电池编码规则》给回收电池包打上标签并匹配其专属序列号，对应其原始出厂编码，实现电池出厂数据与后续再利用数据之间的联通。

（2）在电池再利用过程（包括将回收电池包拆解成最小单元(模组或电芯)、电池包重组及其材料再生）中，应分别给最小单元和重组电池包打上标签、匹配其专属序列号并关联各流程数据。

（3）每个标签序列号对应不同流程中该标签对象所能采集的一系列数据，将其串联起来达到数据溯源和管理的目的。

2、数据采集与管理

（1）在电池回收再利用流程中，采集各环节安全事故的诱因数据和现象数据，并按照隐患溯源、成因分析、事后追责的顺序进行数据整理。

（2）数据采集工作需结合电池回收再利用过程中的实际场景，实现采集过程的低成本、高效率、简洁化、非重复。

（3）对于流程中存在却难以对应数据类型的其他安全隐患，可以考虑增加数据采集

模块、增加数据源，实现对安全隐患更全面的监管。

#### 9.8.1.2 过程数据的处理和存储

（1）根据数据的属性、完整程度、采集难易度等差异，对不同类型数据进行预处理，便于数据存储；

（2）根据数据之间的合理关联，设计与之匹配的存储方案。在保障数据安全的前提下，尽量优化数据的读写与更新速度；

（3）确定溯源过程中数据与安全隐患之间的逻辑关系；

（4）结合实际应用场景，挖掘安全隐患的量化评判标准，提出排查处理方式的合理化建议。

### 9.8.2 大数据分析和运营管理

#### 9.8.2.1 安全隐患预测告警

（1）流程监管：根据所采集的数据信息，结合生产、储运、使用等实际场景，按照产品与场景互相验证原则进行全流程安全监管；

（2）各环节中间产品质量监管：对各环节中间产品进行相应检测，分析其产出数据是否满足产品安全相关要求，必要时可引入第三方检测机构进行与流程相协调的质量监督；

（3）产品使用监控：对使用场景中电池数据进行全方位采集和阶段性分析，通过各项性能指标变化情况判断其是否存在安全隐患，达到预警目的。

#### 9.8.2.2 安全隐患反馈和处理

（1）应及时排查预警的安全隐患；

（2）实现隐患对象数据溯源，协助分析人员找到隐患发生的来源；

（3）对隐患处理结果进行后续跟踪，查看该类型隐患是否能够准确预测并得到及时处理，持续优化全流程风险管控能力；

（4）将安全隐患相关的反馈、处理和后续跟踪记录与相关流程数据相关联，实现全流程数据之间的互联互通。

### 9.8.3 安全事故中的数据运用

#### 9.8.3.1 安全事故前的数据溯源

安全事故发生后，可调取的事故相关信息主要包括：

（1）事故对象在回收再利用各环节中的全流程数据、隐患的历史告警、反馈处理和后续跟踪记录；

（2）结合安全事故发生后的现场情况，梳理事故对象全流程可获得数据，综合分析安全事故发生成因。

#### 9.8.3.2 安全优化建议

（1）为保障溯源过程的准确性，检测人员须定期对数据采集方法进行必要的校准或校验，做好相应的数据记录。相关检测机构应根据实际使用条件，做好产品质量验证、数据准确性评估等监督工作；

（2）通过数据溯源对事故成因进行分析，并根据数据记录界定相关责任方；

（3）对于不能判断成因的安全事故，通过溯源事故对象的历史数据信息，总结事故发生的潜在因素，对该类型事故进行合理规避；

（4）相关责任方应对已发事故进行细致分析，补充之前被忽略、却对实际安全保障至关重要的数据项，优化数据项与安全项之间的逻辑关联，实现更准确的预警、更高效地排查，不断迭代升级、优化溯源流程。

# 10. 安全事故处理

## 10.1 事故处理方法和流程

列举可能发生的事故类型，针对相应事故类型进行有针对性处理，以便能够达到快速处理事故，争取救援时间。

### 10.1.1 碰撞事故救援

#### 10.1.1.1 总则

车辆受损则按以下步骤处理：

（1）车辆钥匙或启动开关切换到关闭，并断开低压蓄电池；

（2）在条件允许的情况下，断开维修开关（若有）；

（3）如果车辆碰撞非常严重，请第一时间协助车上所有人员逃离车辆，拨打 4S 店救援电话及联系交警、保险公司，进行救援、定责及定损；

（4）事故造成自燃事故请参考火灾事故扑救方案。

#### 10.1.1.2 人员搜救

1、侦查检测，划定救授区域

救援车辆到场后，现场指挥员立即对事故现场进行侦查，了解被困人员位置、数量及伤势等。对两车、多车相撞的，以事故车辆为中心，分别划定区划定救授区域，此区域严禁非救援人员进入。若事故车辆动力电池电解液泄漏现象，则应通过检测再划定警戒区域。

2、安全防护，设定警戒范围

设定事故现场的范围，做好整个事故现场的安全防护工作，车辆碰撞事故常常导致交通堵塞，为避免因其它车辆驶入造成二次事故发生，现场指挥员要及时与交警部门配合对事故路段实施交通管制，进入救援区域人员要严格按照个人安全防护要求佩戴安全防护装具，设立安全员，随时做好破拆、切割过程中现场安全监测。

3、作业实施，营救被困人员

根据到场力量确定施救作业人员分组，一般以 5-6 人为一组，现场指挥员 1 人，负责组织协调所属人员开展营救工作，确定救人方法，同时兼任安全员；破拆救人组 2-3 人，负责被困人员解救，要求熟悉器材装备性能并能熟练操作各项破拆工具；设备协调员 1 人，负责提供、递送装备，人员不足时可随时协助破拆组开展工作；医疗护理员 1 人，负责了解被困人员受伤情况，开展紧急医疗救助，监测伤员生命体征，必要时稳定被困人员情绪，如专业医疗人员到场及时，可让医生担任该项工作。

实施破拆救人：

（1）车辆固定

根据事故车辆所发生的侧倒、倾覆情况，使用三点或四点支撑系统，使车辆完成固定；

（2）车门移除

乘员被方向盘、制动装置困住胸腹或下肢，第一选择一般为破拆临近车门开辟救生通道；

（3）车顶移除

为开辟更为充足的救人空间，最大限度地接近伤员，当事故车辆内部情况较为复杂，受困人员较多时，也可以选择移除车顶救人的方法；

（4）仪表盘顶升

如乘员胸腹部被方向盘卡住，首先尝试能否向后移动座椅，若不能移动，宜使用顶撑法进行仪表盘升起。

救援中应注意的几个事项

（1）在开展救援工作前应首先确定车辆断电（高压、低压电源），且尽量避免触及油路、电路，以免发生二次事故，危及救援和被困人员；

（2）破拆过程避免动力电池受损、受力，如事故中动力电池已变形、破损要实时监控电池温度，出现异常升温要用水进行持续冷却，进行防爆、防火处理；

（3）救援前要第一时间清理受伤人员身边的玻璃等锋利物体，清除安全带、安全气囊等保护装置，若气囊未展开，应采取措施防止气囊弹起。救援过程中要随时观察伤员情况，如有必要，协助到场医护人员先开展急救，积极与被困人员沟通，让其了解救援进展情况，鼓励其配合救援工作开展；

（4）减少救援现场障碍物，破拆、移除出的部件要及时清理至第一区域以外，避免救援人员在施救过程中发生绊倒、撞伤等情况；

（5）剪切车身柱、车顶轨时要清除装饰塑料、密封胶带等物品，避开安全气囊充气装置、安全带固定增强装置、安全带延伸器等物品，防止人员受伤及装备受损；

（6）移出伤者过程中要事先了解其受伤部位，如有需要进行肢体固定、包扎后使用木板、担架抬出，避免造成二次伤害。

#### 10.1.1.3 车辆处置

轻微碰撞

轻微碰撞，未伤及新能源高压系统、动力电池事故，由交警和保险公司定责、定损后联系服务店维修处理。

严重碰撞

伤及新能源高压系统、动力电池事故，由交警和保险公司定责、定损后联系拖车，拖至 4S 店维修处理。拖车过程中需要对动力电池温度全程监控，如异常升温需要进行物理降温，防止起火、爆炸。

动力电池漏液、变形处理如下：

（1）车辆动力电池漏液

a. 车辆电源退电至 off 档；

b. 断开低压蓄电池附件 3 分钟后进行下一步操作；

c. 断开动力维修开关（若有）；

d. 断开动力电池正负极连接；

e. 对动力电池正负极母线插接件及线束端插接件用绝缘胶带进行绝缘密封，防止短路及进入异物；

f. 电解液发生少量泄漏时，请远离火源，使用吸液垫吸附后置于密闭容器中，或采用焚烧方式处理。发生大量泄漏时，请统一收集，按照危险化学品处理，可加入葡萄糖酸钙溶液来处理有毒气体 HF。

g. 将车辆拖到店内进行动力电池拆卸，拆卸后动力电池安全存放；

注： c、d、e 三步操作人员需穿戴：绝缘胶鞋+绝缘手套。f、g 两步操作人员需穿戴：绝缘胶鞋+防酸碱手套+防护目镜；

在电池安全存放前需全程对动力电池温度监控，如异常升温需要进行物理降温，防止起火、爆炸。

（2）动力电池变形

a. 车辆电源退电至 off 档；

b. 断开低压蓄电池附件 3 分钟后进行下一步操作；

c. 断开动力维修开关（若有）；

d. 断开动力电池正负极母线；

e. 对动力电池正负极母线插接件及线束端插接件用绝缘胶带进行绝缘密封，防止短路及进入异物；

f. 将车辆拖到店内进行动力电池拆卸，拆卸后动力电池安全存放；

g. 变形严重需将动力电池各模组连接断开存放；

注：c、d、e、f、g 三步操作人员需穿戴：绝缘胶鞋+绝缘手套

在电池安全存放前需全程对动力电池温度监控，如异常升温需要进行物理降温，防止起火、爆炸。

（3）车辆密封性受损

a. 等待维修时需将车辆移至无进水、腐蚀风险场所安全存放；

b. 如车辆无法移至无进水、腐蚀风险场所安全存放，则需要用防水车衣覆盖等措施避免进水、腐蚀风险。

#### 10.1.1.4 现场清理

（1）应全面、细致地检查和清理现场，并向车主和有关部门移交现场。撤离现场时应当清点人员，整理器材装备。将车辆救援回附近 4S 店进行检查，协助查明事故原因；

（2）对现场进行垃圾清理，并检查是否有事故遗留物，便以后续查明事故原因。提醒车主和有关部门妥善处理受损电池，合理采取转运方式，防止事故车辆在转运及后期静置过程中起火。在转移车辆时，不能直接进行拖挂，应根据相关技术要求进行转移。在高压电池电量全部放出之前，应将车辆置于距离建筑物或其他车辆 15 m 之外的地方；

（3）如果动力电池发生泄漏（有明显液体流出），请按照以下方法对进行操作：

发生少量泄漏时，请远离火源，使用吸液垫吸附后置于密闭容器中，或采用焚烧方式处理。操作前请佩戴防腐蚀手套。发生大量泄漏时，请统一收集，按照危险化学品处理，可加入葡萄糖酸钙溶液来处理有毒气体 HF。当人体不慎接触泄露液体时，应立即用大量水冲洗 10～15 分钟，如果有疼痛感可用 2.5%的葡萄糖酸钙软膏涂敷，或用 2～2.5%的葡萄糖酸钙溶液浸泡止痛。若无改善或出现不适症状，请立即就医。

### 10.1.2 水域事故救援

#### 10.1.2.1 侦查

侦查车辆积水深度，根据不同积水深度采取相应救援措施。需要注意的是动力电池系统在水中也会着火和爆炸，救援过程中需要注意安全。

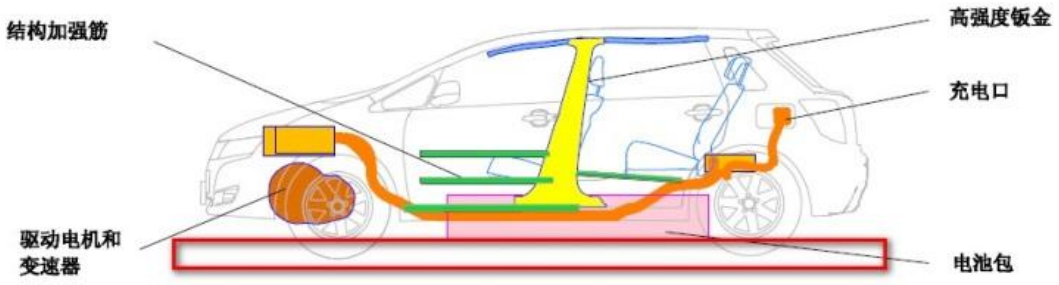
（1） 积水深度在门槛以下（如下图）

a. 将车辆缓慢开离积水路面，车辆停放在安全地区检查车辆内是否进水并将车辆内部积水进行处理，若车辆可以继续行驶将车辆行驶至维修点进行全面排查；

b. 如果车辆出现异常，请拨打 4S 店电话请求救援；

c. 如果车辆无法继续行驶，请保证人员安全的情况下立即切断电源，并拨打 4S 店及

保险公司电话请求救援。

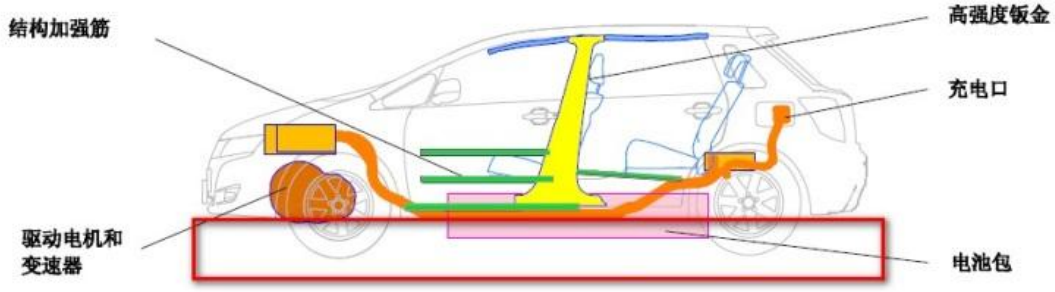



（2）积水深度在门槛处或接近门槛（如下图）

a. 将车辆缓慢开离积水路面，车辆停放在安全地区检查车辆内是否进水并将车辆内部积水进行处理，若车辆可以继续行驶将车辆行驶至 4S 店进行全面排查；

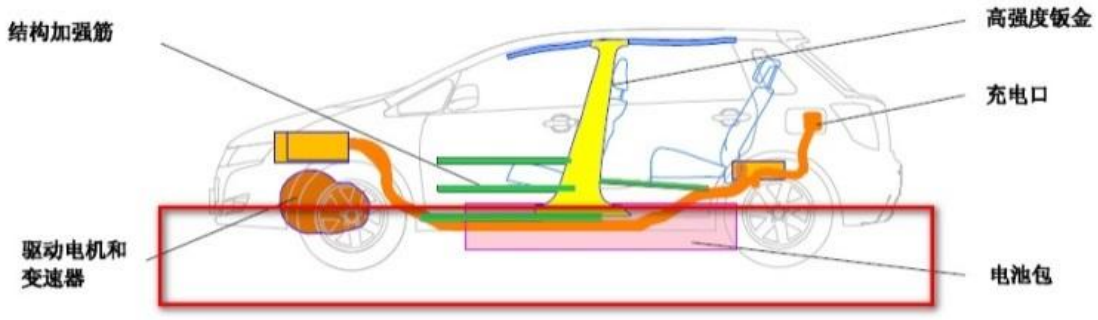
b. 如果车辆出现异常，请拨打电话请求救援；

c. 如果车辆无法继续行驶，请保证人员安全的情况下立即切断电源，并拔打 4S 店电话请求救援。




（3）积水深度在门槛以上（如下图）

所有人员离开车辆，保证人员安全。拨打 4S 店电话请求救援，请保证人员安全的情况下切断电源。



#### 10.1.2.2 人员搜救

搜救应包括以下内容：

（1）水域温度、深度、水面宽度、水流方向、岸边地形等情况，了解事故现场及周边的道路、交通、水源等情况；

（2）遇险人员的位置、数量和伤亡情况；

（3）通过外部观察，判断事故车辆动力电池和高压电系统的受损情况；

（4）评估现场救援处置所需的人力、器材装备及其他资源；

（5）做好救援人员的安全防护，进行人员搜救；

（6）分析现场情况，充分考虑救助过程中可能存在的危险因素，确定救援方案；

（7）若有人员在车内，应及时击破车窗或打开车门，并及时拨打 120 救助，救援车辆到场后，现场指挥员立即对事故现场进行侦查，了解被困人员位置、数量及伤势等，遇险人员救出后交由医疗急救人员进行救护；

（8）查明车辆牵引部位、牵引途径，明确车辆停放的安全区域；

（9）调大型吊车到场，确定起吊方案，将落水车辆吊上路面。

#### 10.1.2.3 车辆处理

（1） 车辆高压元件未浸水

a. 读取车辆是否报漏电故障；

b. 未报漏电故障进行常规检修；

c. 已报漏电故障参照“（3）车辆动力电池包母线以上部位浸水”方案处理。

（2）车辆高压元件已浸水

a. 车辆电源退电至 off 档；

b. 断开低压蓄电池附件 3 分钟后进行下一步操作；

c. 断开动力维修开关（若有）；

d. 断开动力电池正负极母线；

e. 将车辆运送至服务店内；

注：c、d、e 步骤作业人员需穿戴绝缘胶鞋+绝缘手套；

在电池安全存放前需全程对动力电池温度监控，如异常升温需要进行物理降温，防止起火、爆炸。

（3）车辆动力电池包母线以上部位浸水

a. 车辆电源退电至 off 档；

b. 断开低压蓄电池附件 3 分钟后进行下一步操作；

c. 断开动力维修开关（若有）；

d. 断开动力电池正负极母线；

e. 对动力电池正负极母线插接件及线束端插接件用绝缘胶带进行绝缘密封，防止短路及进入异物；

f. 将车辆拖到店内进行动力电池拆卸。

注：c、d、e 步骤作业人员需穿戴绝缘胶鞋+绝缘手套；

在电池安全存放前需全程对动力电池温度监控，如异常升温需要进行物理降温，防止起火、爆炸。

#### 10.1.2.4 现场清理

（1）将车辆电源退电至 off 档；

（2）断开低压蓄电池附件 3 分钟后进行下一步操作；

（3）断开动力维修开关（若有）；

（4）断开动力电池正负极母线；

（5）对动力电池正负极母线插接件及线束端插接件用绝缘胶带进行绝缘密封，防止短路及进入异物；

（6）对车辆积水进行清理，拖回 4S 店做进一步检查。

注：（3）、（4）、（5）步骤作业人员需穿戴绝缘胶鞋+绝缘手套；

在电池安全存放前需全程对动力电池温度监控，如异常升温需要进行物理降温，防止起火、爆炸。

### 10.1.3 火灾事故扑救

#### 10.1.3.1 灭火战术

（一）用户发现电动汽车着火

建议司机遵循以下步骤：

（1）停止车辆；

（2）如果可能的话靠边，断蓄电池负极及紧急维修开关，离车；

（3）离车辆 30 米左右，并注意交通安全；

（4）拨打 119 求助；

不要自己去灭火。

（二）服务店发现电动汽车着火处理方法

（1）整车退电至 OFF 档；

（2）条件允许断开低压电池负极、断开紧急维修开关（若有）；

（3）用消防沙、干粉、水扑灭明火（干粉、水需要持续使用，使用水或水基灭火器灭火后必须对动力电池进行拆解安全处理）；

（4）出现火势发展迅猛或者火势失控的情况下，需要通知消防人员使用持续、大量的消防水进行灭火；

（三）救援规范要求

（1）佩戴安全防护设备：绝缘手套（需准备高压电工以及防电池解液酸碱性两种）、绝缘胶鞋、绝缘胶垫、绝缘外套和防护眼镜等，其耐压级必须大于 1000V；

（2）起火的情况下，火势较小处于可控状态时应采用合适的灭火剂：干砂、化学干粉、二氧化碳，不要使用水基灭火器；

（3）当车辆着火或电池受到严重的挤压、弯曲等损害，出现火势发展迅猛或者火势失控的情况下，需要通知消防人员使用持续、大量的消防水进行灭火 30 分钟；

（4）当火势被扑灭后，需要随时关注，防止复燃；

（5）防止火灾扩大，应使周围的任何可燃物品远离起火车辆。

#### 10.1.3.2 现场清理

（1）检查现场是否有残留火源，避免再次点燃；

（2）将车辆救援回附近 4S 店进行检查，进一步查明起火原因；

（3）现场进行垃圾清理，并检查是否有易燃引燃物，便以后续查明起火原因。

### 10.1.4 触电事故处理

#### 10.1.4.1 总则

（1）识别触电原因，评估后确定救援方案；

（2）做好救援人员的安全防护；

（3）救援前切断触电电源；

（4）人员隔离电源后进行救治；

（5）车辆设备隔离电源后处置；

（6）现场清理。

#### 10.1.4.2 处理方法

处于运营及生产现场正在运行、维保、调试、充电的车辆发生人员触电、电气设备短路时应遵循以下方法分别处置。

人员触电：首先确认触电人员身体是否和车载电气设备有接触，如有接触，

处置人员应首先戴绝缘手套用绝缘棒进行人和设备的隔离，然后根据情况进行人工呼吸进行施救。

电气设备短路：电气设备短路会产生爆响和电弧放电现象，人员应远离电气

设备防止灼伤并在第一时间关闭车钥匙，并拔出手动快断器和切断充电机供电电源（如在充电），如电弧放电还在进行说明此操作不能断开短路电源，在此情况下应立即疏散人员远离车辆。

#### 10.1.4.3 注意事项

（1）车载电源及高压系统的应急处置应由认证高压电气维修人员，在规范的防护措施保护下进行；

（2）触电者未脱离电源前，救护人员不准直接用手触及伤员；

（3）未采取绝缘措施前，救护人不得直接触及触电者的皮肤和潮湿的衣服；

（4）严禁救护人直接用手推、拉和触摸触电者；救护人不得采用金属或其他绝缘性能差的物体（如潮湿木棒、布带等）作为救护工具；

（5）在拉拽触电者脱离电源的过程中，救护人宜用单手操作，并且救护人身体部位及所穿的鞋不能潮湿，这样对救护人比较安全。

### 10.1.5 充电事故处理

#### 10.1.5.1 总则

（1）识别充电事故原因，评估后确定救援方案，注意充电事故往往会发生着火、爆炸现象；

（2）做好救援人员的安全防护；

（3）切断充电站电源；

（4）车辆设备隔离电源后处置；

（5）现场清理，特别是需要注意泄露的电解液遇水会产生的有毒液体，对现场环境产生的影响。

#### 10.1.5.2 处理方法

（1）应首先确定充电站电源位置并切断；

（2）在确保人身安全的情况下，应首先采用拔出电动汽车的充电枪或剪断充电线等手段，断开充电设备与车辆的连接。

按照上述灭火和触电的要求进行应急救援。

## 10.2 安全事故原因排查方法和程序

为了能够明确是否发生的前因后果，同时保证事故原因排查过程准确无误，特针对各类型事故的原因排查方法进行说明。

为了准确无误的定位事故发生的原因，应遵循下述相关流程。

### 10.2.1 成立调查小组

发生安全事故后，相关交通事故处理部门应当牵头组织成立调查组，进行事故调查处理。

事故调查小组由县级以上人民政府或者授权的有关部门和对应车辆厂商组织的人员组成，对事故原因进行调查分析。

根据事故调查工作需要，还可邀请有关专家参加事故调查工作。

事故调查组应进行合理分工，在客观科学的前提下，尽快完成调查工作。

事故调查组成员在事故调查过程中，应当恪尽职守，客观公正，实事求是。遵守事故调查组的纪律，保守事故调查的秘密，在事故调查处理工作结束前，不得擅自对外发表意见。

### 10.2.2 调查取证

针对造成事故发生的可能原因进行调查取证，按照规定的调查取证流程应遵循如下要求和步骤。

#### 10.2.2.1 总则

为了更好的保证调查取证高效、有序的进行，指导相关单位合理履行职责，制定该调查取证的指导方法。

安全事故的调查取证应坚持客观、公正的原则，不得隐瞒或者捏造。任何单位和个人不得妨碍和非法干预安全事故调查取证，所有调查取证的过程和结果应做好实时记录和归档，保证调查取证的有效性和可追溯性。

#### 10.2.2.2 现场勘查

在事故发生后，事故调查小组成员应及时赶赴事故现场，进行勘查。事故现场应及时保护，不得被破坏或者特殊情况下也应能被及时复原。向当事人或者目击者了解事故发生的经过情况。提取事故现场存留的相关痕迹和物证（视频监控资料，残留物，致害物等），对事故相关物件进行封存和记录。

在勘查前应巡视现场周围情况，确定现场勘查的范围和顺序。勘查后结合现场勘查收

集的相关信息和事故发生地周边走访了解的结果，对事故进行初步的分析和判断。

#### 10.2.2.3 车辆审查

在事故调查中应提取出事故车辆的年检，保养和维修记录。对可能造成事故的车辆潜在问题进行记录。

建议从事故车辆生产厂家获取相关车辆信息，核查车辆相关法规符合性申明，技术规格文件和测试报告等。

#### 10.2.2.4 具体原因分析

事故按照场景划分为碰撞事故，水域事故和火灾事故。在发生时需结合不同的事故场景对可能的事故原因进行分析和判断。

##### 10.2.2.4.1 碰撞事故

###### 10.2.2.4.1.1 人为原因分析

从车辆驾驶员的角度分析事故的发生原因，由于人为因素导致车辆间的碰撞或车辆与其它障碍物之间的碰撞事故发生。分析判断发生碰撞事故时驾驶员是否有如下不良行为：

（1）超速、酒后驾驶、疲劳驾驶、无证驾驶、违反交通法规、开情绪车、斗气车的行为；

（2）服用感冒类药品后驾驶车辆，行驶过程中接听电话、抽烟、聊天、看风景等不良行为；

（3）在风、雪、雾等恶劣气候条件未进行减速慢行，车辆未按规定进行年检、日常保养及检修。

从他人的角度分析事故发生的原因，存在他人干扰的因素，导致驾驶员驾驶失控发生碰撞事故。

###### 10.2.2.4.1.2 路况原因分析

车辆在行驶过程中，由于道路交通异常或者其他环境问题导致碰撞事故的发生。

分析在行车道路上是否有不能被驾驶员不易感知到的前方车辆或障碍物，在行车过程中是否存在不可预见的路况变化导致车辆出现碰撞事故。

###### 10.2.2.4.1.3 产品原因分析

由于车辆突发故障导致的碰撞事故或者碰撞发生的严重程度超过车辆的防护设计，分析车辆在碰撞时可能存在如下问题：

（1）操作装置：由于车辆的制动，转向等操作装置异常，诸如刹车失效无法有效制动，方向盘失效无法有效控制方向，操纵杆失效无法进行换挡操作等车辆部分控制功能丧

失或者完全失控，驾驶员无法有效控制车辆进而导致碰撞事故发生；

（2）电池系统：电池系统在出现短路，过温，欠压，漏电等异常情况下车辆可能出现保护性掉电，动力丧失等险情导致碰撞事故发生。碰撞严重程度的不同也可能会导致电池系统出现变形、短路，进而可能发生其他例如起火等危险；

（3）配电系统：配电系统在出现短路，漏电等情况下车辆可能出现保护性掉电，动力丧失等险情导致碰撞事故发生；

（4）高压线束：高压线束在出现短路，过温，漏电等情况下车辆可能出现保护性掉电，或高压线束的连接异常可能直接导致的掉电，动力丧失等情况导致碰撞事故发生。在碰撞发生后，若高压线束布置的不合理则可能出现车内人员触电和拉弧等危险情况，更恶劣的情况可能导致起火；

（5）驱动系统：驱动系统在出现短路，过温，漏电等情况下车辆可能出现保护性掉电或由于自身故障出现抛锚时导致碰撞事故发生；

（6）低压系统：低压系统，可能出现的例如供电异常，导致车辆抛锚，或者由于系统异常出现错误的报警信息或错误的车辆状态提示等影响行车安全，导致碰撞事故发生。

#### 10.2.2.4.2 水域事故

##### 10.2.2.4.2.1 人为原因分析

从车辆驾驶员的角度分析事故的发生原因，由于人为因素导致车辆部分进水抛锚或车辆完全入水的事故发生。分析判断驾驶员导致车辆发生水域事故时是否有如下不良行为：

（1）超速、超速行驶、酒后驾驶、疲劳驾驶、无证驾驶、违反交通法规、开情绪车、斗气车的行为；

（2）服用感冒类药品后驾驶车辆，行驶过程中接听电话、抽烟、聊天、看风景等不良行为；

（3）在风、雪、雾等恶劣气候条件未进行减速慢行，车辆未按规定进行年检、日常保养及检修；

从他人的角度分析事故发生的原因，存在他人干扰的因素，导致驾驶员驾驶失控发生水域事故。

##### 10.2.2.4.2.2 路况原因分析

车辆在行驶过程中，由于道路交通异常或者其他环境问题导致水域事故的发生。

分析在行车道路上是否有驾驶员不易感知到的前方危险水域或在涉水行驶时潜在的危险路况，在行车过程中是否存在不可预见的路况变化或环境变化导致车辆出现水域事

故。

车辆在停放过程中，由于外部环境因素变更导致车辆出现水域事故。

#### 10.2.2.4.2.3 产品原因分析

由于车辆自身的设计缺陷或车辆存在的故障导致的水域事故的发生，分析车辆在遇到水域事故时可能存在如下问题：

（1）操作装置：由于车辆的制动，转向等操作装置异常，诸如刹车失效无法有效制动，方向盘失效无法有效控制方向，操纵杆失效无法进行换挡操作等车辆部分控制功能丧失或者完全失控。驾驶员无法有效控制车辆，车辆在失控情况下进入危险水域，导致水域事故发生。发生水域事故时车辆出现熄火，由于危险部件进水可能导致更恶劣的结果，例如漏电、短路、起火等；

（2）电池系统，配电系统，高压线束，驱动系统，低压系统等部件在出现器件故障导致抛锚在涉水路段，由于可能存在的防水问题，车辆可能出现漏电或者起火等更严重的水域事故。另外行驶时经过涉水路段或停放在危险水域时，防水问题也可能导致车辆出现漏电或者起火等更严重的水域事故。

### 10.2.2.4.3 火灾事故

#### 10.2.2.4.3.1 人为原因分析

从车辆驾驶员的角度分析事故的发生原因，由于人为因素导致车辆出现异常情况导致火灾事故发生。分析判断发生碰撞事故时驾驶员是否有如下不良行为：

（1）超速、超速行驶、酒后驾驶、疲劳驾驶、无证驾驶、违反交通法规、开情绪车、斗气车的行为；

（2）服用感冒类药品后驾驶车辆，行驶过程中接听电话、抽烟、聊天、看风景等不良行为；

（3）在风、雪、雾等恶劣气候条件未进行减速慢行，车辆未按规定进行年检、日常保养及检修。

从他人的角度分析事故发生的原因，存在他人干扰的因素，导致驾驶员驾驶失控发生火灾事故或他人的故意纵火等行为导致车辆出现火灾事故。

#### 10.2.2.4.3.2 路况原因分析

车辆在行驶过程中，由于道路交通异常或者其他环境问题导致火灾事故的发生。

分析在行车道路上存在某些事物例如潜在的火源或易燃物等可能诱发车辆出现火灾事故。

在恶劣的道路环境下行驶的车辆出现零部件损伤或者更严重的车辆发生倾覆等极端情况可能导致车辆出现自燃的事故。

车辆在其他场景，例如正常的停放或者充电状态下可能被其他火源引燃发生火灾事故。

#### 10.2.2.4.3.3 产品原因分析

由于车辆自身的设计缺陷或车辆存在的故障导致的火灾事故的发生，分析车辆在遇到火灾事故时可能存在如下问题：

（1）操作装置：由于车辆的制动，转向等操作装置异常，诸如刹车失效无法有效制动，方向盘失效无法有效控制方向，操纵杆失效无法进行换挡操作等车辆部分控制功能丧失或者完全失控，驾驶员无法有效控制车辆进而导致车辆失控发生碰撞造成起火或车辆进入危险的火场导致起火发生火灾事故；

（2）电池系统：电池系统在出现过充，过放，内部短路，过温，受到外部冲击导致的受损等问题时，可能起火引发火灾事故；

（3）配电系统：配电系统在出现内部故障短路，异物进入导致短路和外部冲击变形引发的短路时，可能起火导致火灾事故；

（4）高压线束：高压线束在出现短路，过温等情况时可能起火导致火灾事故；

（5）驱动系统：驱动系统在出现短路，过温等情况时可能起火导致火灾事故；

（6）低压系统：低压系统在出现短路，过温等情况时可能起火导致火灾事故。

单个系统或部件的故障，起火等也可能导致其他高压部件的故障，或者直接引燃其他部件导致更严重的火灾事故。

#### 10.2.2.4.4 其它事故

车辆除了碰撞事故，水域事故和火灾事故发生，在日常行驶，维修保养或者充电过程中可还能会发生触电事故和充电事故。

#### 10.2.2.4.4.1 人员触电

##### 10.2.2.4.4.1.1 人为原因分析

从接触车辆的驾驶人员，维修人员或者其他人员的角度分析事故的发生原因，由于人为因素导致触电事故发生。分析判断发生触电事故时相关人员是否有对应不良行为。

驾驶人员：存在不正确的操作，违规驾驶等导致的其他诸如碰撞，水域事故时车辆出现漏电，进而导致相关人员触电，或在无相关专业培训的情况下擅自进行拆车维修等导致触电事故发生；

维修人员：在车辆进行维修保养过程中，未按照相关指导手册进行违规操作，导致发生触电事故；

其他人员：在车辆行驶或者停放过程中，由于蓄意破坏或者通过工具接触到车辆的高压部分，或无意中接触到有潜在危险的事故车辆导致的触电事故。

#### 10.2.2.4.4.1.2 路况原因分析

车辆在行驶过程中，由于道路交通异常或者其他环境问题导致触电事故的发生，例如正常的停放或者充电状态下可能被其他危险电路搭接或者短路导致触电事故。

#### 10.2.2.4.4.1.3 产品原因分析

从车辆自身的设计缺陷或车辆存在的故障导致的触电事故的发生，分析车辆在遇到触电事故时可能存在如下问题：

（1）操作装置：由于操作装置异常导致的车辆失控发生碰撞，水域事故等可能间接导致的触电事故发生；

（2）电池系统：电池系统的高压回路与车身间的绝缘电阻减小或出现搭接的情况导致金属车身带电出现触电事故；

（3）配电系统：配电系统的高压回路与车身间出现漏电的情况导致金属车身带电出现触电事故，且配电系统接地异常导致的电位均衡出现异常也可能导致触电事故；

（4）高压线束：高压线束存在绝缘层磨损，接插件脱落，在其他事故中出现高压线束被割断等场景导致高压电路外露或与其他金属件短路，出现触电事故；

（5）驱动系统：驱动系统的高压回路与车身间的出现漏电的情况导致金属车身带电出现触电事故，且驱动系统接地异常导致的电位均衡出现异常也可能导致触电事故；

（6）低压系统：低压系统可能存在与高压供电系统间的隔离出现故障，导致低压系统带高压电，出现电击事故。

### 10.2.2.4.4.2 充电事故

在充电过程中涉及大能量的转换，对线缆连接和相关能量传输，储存系统的要求都较高，也相对比较容易发生事故。

#### 10.2.2.4.4.2.1 人为原因分析

从充电线路安装人员，充电操作人员或者其他人员的角度分析事故的发生原因，由于人为因素导致充电事故发生。分析判断导致充电事故时相关人员是否存在对应不良行为。

充电线路安装人员：充电线路在安装过程中未严格遵循车辆生产厂家提供的安装指导说明，在接线过程中可能存在规格不满足要求，将充电盒等安装在有潜在风险的区域等错

误行为均可能导致实际充电过程中出现起火，触电发生充电事故。

充电操作人员：操作人员在充电过程中，违规使用充电设备，私自改装充电设备，车辆状态未稳定即连接充电线，车辆充电过程中移动车辆或其他不按照操作说明的给充电设备带来潜在故障的行为均可能导致充电事故发生；

其他人员：在车辆充电过程中，蓄意破坏充电设备或使用其他工具干扰设备正常充电等行为均可能导致充电事故发生。

#### 10.2.2.4.4.2.2 产品原因分析

从车辆自身的设计缺陷或车辆存在的故障导致的充电事故的发生，分析车辆在遇到充电事故时可能存在如下问题：

（1）充电装置：由于充电装置异常导致的车辆在充电过程中发生电路短路、接插件虚接、充电保护失效，车载充电机过压、过流、过温，充电线缆过流、过温等异常情况均可能导致充电事故发生；

（2）电池系统：充电过程中电池系统可能存在的过充，过温，过流，过压等异常情况可能导致充电事故的发生；

（3）高压线束：内部高压线束在进行大电流传输时可能发生过温，过流的情况导致充电事故发生；

（4）保护策略：在充电过程中可能的保护策略失效，车辆出现不期望的动作或在充电电压电流异常，电池包过充等情况下未能正确执行保护策略导致充电事故发生。

#### 10.2.2.4.4.2.3 其它原因分析

车辆在充电过程中可能有由于外部环境变化，电网电压异常，充电线路老化，外部事故等其他原因也会间接导致车辆在充电过程中发生可能出现的充电异常甚至发生起火漏电等事故。

（1）外部环境：车辆在充电过程中，外部环境变化导致充电无法正常进行，出现影响充电安全的危险源可能导致充电事故；

（2）电网电压：车辆在充电过程中，可能存在电网电压异常导致充电电压发生异常的超出充电规格要求导致危险发生的充电事故；

（3）充电线路：充电线路在长期使用或者接线时采用老化的线缆，线缆内阻较大导致发热可能起火导致充电事故；

（4）外部事故：车辆在充电过程中，受外部可能发生的起火，碰撞等事故影响进而导致车辆充电异常发生充电事故。

### 10.2.3 事故分析总结

事故发生后可参考上述事故原因及排查方法进行分析，再根据实际事故严重程度及分析情况输出分析总结。事故调查组组长主持召集召开事故分析会。会议通报事故调查情况，分析事故原因，提出防范措施等。

（1）通过对事故的调查，科学分析事故原因，总结事故发生的教训和规律，提出有针对性的防范和整改措施，促进产品改进，防止类似事故再度发生；

（2）根据事故原因进行事故性质分析，对事故严重程度以及是属于责任事故或非责任事故作出认定；

（3）根据事故调查所确认的事实和事故原因事故性质，对事故责任加以分析判断，判断事故责任人（方）。

## 10.3 安全事故整改评估方法

通过安全事故的整改和评估及时发现并消除车辆问题并排查隐患，能对各类事故有效地控制和预防。

### 10.3.1 总则

为建立电动汽车安全事故整改和责任追究执行情况跟踪督办流程，推动电动汽车安全事故责任追究和整改措施的落实，检查评价安全事故整改措施落实效果，提出此评估方法。

**成立评估小组**：评估小组一般应由参加事故调查处理的有关厂商人员、交通事故管理部门人员等组成，必要时评估小组可以聘请第三方机构（具有与事故发生责任单位相关联的专业技能机构）或熟悉相关业务的专家。

评估小组在评估过程中应秉承“四不放过”和科学严谨、实事求是的原则，做到事实清楚，定性准确，程序合法，手续完备。发现任何与整改措施不符或不到位的现象，都应及时予以纠正或要求限期整改。且整改完成后需要经过评估小组再次确认方可进行下一步评估动作。

评估工作方案：

评估小组应依照下列方法对事故责任单位（部门）开展评估：

（1）列出评估清单，包括但不限于事故排除方法和流程评估、整改措施及技术文件评估、整改措施落实情况评估等；

（2）听取事故责任单位（部门）事故发生后管理整改工作情况的汇报；

（3）向相关人员询问了解事故发生后整改措施落实到位情况；

（4）收集相关文件及资料，包括但不限于详细的事故分析总结报告、变更前后的技术工艺文件、试验报告等。文件可采用机打、扫描电子版等经过签字确认并可在后期有效追溯的格式；

（5）对事故责任单位（部门）整改后的现场状态进行全面检查，可以采取随机抽查，利用录音、录像等多种方式，真实反映事故责任单位（部门）在事故发生后整改措施落实到位情况。

评估人员应做好全程记录，记录内容包括时间、地点、检查内容、整改后仍存在的问题等，并由相关责任人签字确认。

从以下两方面点检评估安全事故的整改效果：

#### 10.3.1.1 技术原因分析

（1）定位准确

对问题的描述需明确说明发生的时间、地点、时机、现象、环境条件，涉及批次、与故障相关数据，同时运用故障树及因果图等方法列出所有可能的故障原因。

（2）机理清楚

采用理论分析或实验分析问题产生的机理，同时需考虑清楚设计、工艺、制造、零部件、原材料等各种因素。

（3）问题复现

通过试验、模拟实验及原理性复现的方法进行故障复现，在确保安全的情况下，实验条件要和问题发生的现场一致。

（4）措施验证

解决的措施要与原因一一对应，要明确采取的措施是否会引起此生故障，说明如何解决。

（5）举一反三

针对在产产品及同类产品进行措施推广，确保同类问题不发生。

#### 10.3.1.2 管理要求落实

（1）过程清楚

对问题的描述要明确说明发生的时间、地点、时机、现象、环境条件，涉及批次、与故障相关数据，以及在研发、生产、使用等过程中是否发生过同类问题，初步还原问题发生和发展的全过程。

（2）措施落实

对问题措施落地制定计划，整改措施是否全面、可行、有效，且相关证据齐全完整。

（3）完善规章

针对存在的问题，管理制度或技术文件是否需要完善，完善的内容必须经过有效的评审和审核。

### 10.3.2 评估小组

车辆所属方、车辆生产企业、行业主管部门、专业机构等多方人员组成评估小组。根据事故情况和后果，可调整评估小组成员。

### 10.3.3 评估工作方案

（1）事故发生、施救处置后，需保持车辆状态不变，由车辆所属方和车辆生产企业共同检查车辆，初步分析事故原因。如是重大事故需通报行业主管部门参与；

（2）如果初步分析事故是车辆产品原因，由车辆所属方和车辆生产企业共同拆检与事故起因有关的零部件。如是重大事故需行业主管部门及专业机构参与；

（3）查明事故原因后，由评估小组出具事故原因分析报告。如果是车辆产品原因造成的安全事故，由车辆生产企业提供整改措施，经车辆所属方认可后，予以落实整改。如果不是车辆产品原因造成的安全事故，由车辆生产企业提供改进建议，交付车辆所属方参考改进。如是重大事故需行业主管部门及专业机构参与；

（4）改进实施后，由车辆所属方和生产企业定期进行车辆安全检查，验证整改效果，期限为半年至一年。

### 10.3.4 评估标准

安全事故整改方案的评估标准：

（1）有效性：要求整改方案能有效解决事故隐患，避免相同问题再次发生；

（2）可操作性：要求整改方案能操作落实；

（3）时效性：要求整改方案能及时实施（固化措施需要时间较长的，制定临时解决方案）；

## 10.4 事故报告要求

依据表 10-1 内容进行事故报告编制：

表 10-1

<table>
<tr><td>事故发生时间</td><td colspan="2">事故发生地点</td><td>伤亡情况</td><td>事故类型</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td>火灾/水域/碰撞/其它</td></tr>
<tr><td>事故车辆厂商</td><td>事故车辆品牌</td><td>事故车辆型号</td><td>事故车辆动力类型</td><td>事故车辆电池供应商</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>事故描述</td><td colspan="4">1 发生过程描述<br>2 救援过程描述<br>3 结果描述</td></tr>
<tr><td rowspan="2">事故原因</td><td colspan="2">主观原因</td><td colspan="2">客观原因</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>整改措施</td><td colspan="4"></td></tr>
<tr><td>事故调查组<br>成员名单</td><td colspan="4"></td></tr>
<tr><td>其它说明事项</td><td colspan="4"></td></tr>
</table>

# 11. 操作安全

## 11.1 操作指导培训及资质认证体系

### 11.1.1 操作资质分级、权限及要求

（1）新能源高压电气系统的安装、调试(含充电调试)、维修必须由持电工证的合格电工执行，并严格遵守电工安全操作规程进行。其他非高压系统的维修可由机修、电工、钣金等维修人员进行操作；

（2）应具有新能源车辆高、低压电路系统、控制系统故障诊断与维修作业的能力；能够熟练使用新能源车辆维修所需的检测仪器及设备，准确判断车辆故障并排除新能源系统故障；能够应用技术资料解决新能源系统技术问题；

（3） 新能源车辆维修站维修人员应接受生产厂家（或行业认可的培训机构）培训，经过理论与实操考试合格后方可对新能源高压系统进行维修。

电动客车整车维修站要具有二类以上汽车维修企业资质；三类维修资质维修站可根据经营允许的范围对车辆进行维修，如维修新能源车辆的电路及控制系统，需配备有专业的新能源电器维修人员。

### 11.1.2 新能源高压系统维修人员的资质考核

（1）人员根据岗位任职要求组织培训和考核，考核合格后颁发上岗证，期限为三年，内部每年定期进行考试，若不合格，则重新进行培训或者转岗；

（2）负责培训管理人员对特定岗位人员进行资格确认，必要时进行理论或实际操作的抽查；

（3）特定岗位人员资格鉴定的方式有：审核资格证书的有效性、实际操作考核、日常工作业绩评价等。

## 11.2 新能源车操作指导通用要求

### 11.2.1 携带医疗电子器械的维修人员注意事项

汽车的零部件使用了强磁，同时车辆在充电、远程通信系统工作时会产生辐射电磁波，使用诸如植入型心脏起搏器或者植入型心脏复率除颤器的人员不得操作此类车辆，以免电磁波影响到医疗设备的功能。

### 11.2.2 气囊维修检查注意事项

为避免造成安全气囊失效，其维修必须由厂家或厂家授权的操作人员进行。

在安全气囊传感器或者其他的安全气囊系统传感器附近进行操作时，要关闭电源，同时避免敲打传感器，大的振动会启动传感器，并打开安全气囊，可能会造成严重的伤害。

## 11.3 操作前准备工作

### 11.3.1 防护要求

维修人员必须佩戴必要的安全防护用品，如：绝缘手套、绝缘胶鞋、绝缘胶垫和防护眼镜等，其耐压等级必须大于 1000V。安全防护用品根据其产品使用寿命及时更换。

使用前必须检查绝缘手套、绝缘胶鞋等防护用品是否有破损、破洞或裂纹等，不能带水进行操作，保证内外表面洁净、干燥，确保安全。

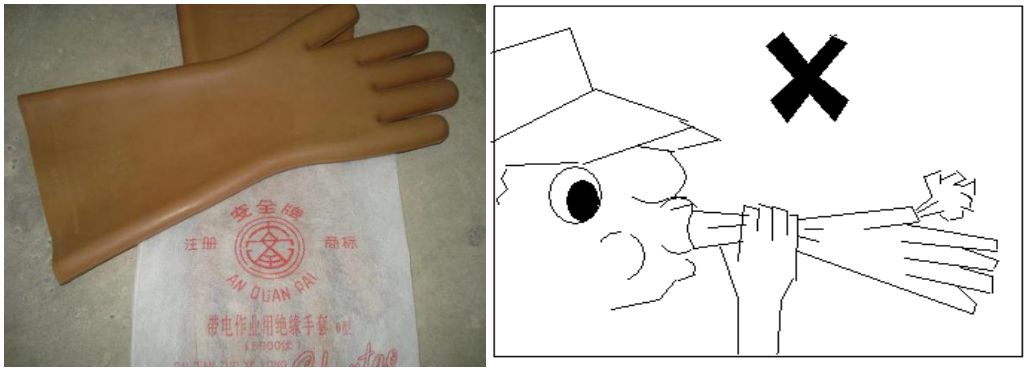



图 11-1 检查绝缘手套

### 11.3.2 专用工具要求

维护和保养新能源部分所需工具：兆欧表、万用表、钳流表（含直流及交流）、具有绝缘手柄的操作工具（含力矩扳手、快速扳手、螺丝刀等）、绝缘手套、绝缘鞋等。检测用仪器需要先检查功能及附件均工作正常后方可使用，操作工具应提前使用绝缘胶带包裹除去与标准件接触点以外的裸露金属部分，避免因仪器故障或操作工具裸露金属部分误触带电部件，导致高压事故。

### 11.3.3 专人监控

监督维修人员资质、工具使用、防护用品佩戴、备件安全保护、维修安全警示牌等是否符合要求；

对维修过程中的安全维修操作规程进行检查，应按安全维修操作规程指挥操作，维修人员在做完一个操作后告知监护人，监护人在作业流程单上作标记；

监护人及维修人员必须具备国家认可的《特种作业操作证（电工）》与《初级（含）

以上电工证》；

监护人及维修人员必须经过专业的混合动力及纯电动车型新车型培训，并通过考核。

### 11.3.4 禁止事项

严禁未经培训的人员进行高压部分检修，禁止一切带有侥幸心理的危险操作，避免发生安全事故。

严禁不按章操作。

## 11.4 高压回路的断开

在系统进行维护和保养前必须切断动力电源。

断开操作方法及恢复操作方法详见产品使用说明书。

## 11.5 操作注意事项

（1）电气电路的维护必须由持电工证的合格电工执行，并严格遵守电工安全操作规程进行。

（2）高压操作区域应张贴警示标志和隔离带，以防非预期人员进入或操作 。

（3）高压操作区域应配备绝缘垫、消防设施和救援设施。

（4）操作工具不得随意摆放，不可放在口袋，更不能放在高压零部件上，使用后需放置指定位置。

（5）操作前，检查安全设施或工具是否完好，确认完好后再操作。

（6）操作前，应检查车辆情况，尤其是高压部件的情况，确认完好后再进行操作，车辆熄火，断开高压维修断开装置或高压输出连接器。

（7）高压零部件识别：橙色线缆以及所连接部分和带高压标志的都是高压零部件。非专业人士不能对高压线路、高压元件进行切割或打开。

（8）拔掉后的高压维修断开装置、连接器或接口需做绝缘处理。

（9）禁止高压正负极同时操作。

（10）在进行维护作业时应严格防止高压线束的绝缘层破损漏电。

（11）高压操作时，保证至少两人在场；一人操作，一人保持一定距离观察，起到安全提醒作用。

（12）在清洗车辆时，请避开高、低压元件，严禁用水直接冲洗高、低压元件。

（13）制订高压作业指导书，操作人员需根据作业指导书进行操作。

（14）各螺栓连接处的力矩要严格按照螺栓扭矩要求来执行。

# 12. 运营车辆安全管理

为保障新能源营运车辆安全运行，保障人民群众的生命财产安全，促进新能源营运车辆的健康可持续发展，按照各部委相关要求，编制新能源营运车辆安全管理指南，新能源营运车辆的安全性包括车辆自身、驾乘人员、运营环境等方面，各地方营运车辆管理部门对运营车辆有不同的要求。本章从车辆角度规范新能源营运车辆安全性要求。

## 12.1 电动营运车辆的一般性要求

### 12.1.1 营运证办理

按照所在地对运营车辆的要求和营运证办理流程进行运营证件的办理。

#### 12.1.2 电动汽车生产企业监控平台

根据国家《新能源汽车生产企业及产品准入管理规定》，电动汽车生产企业应当建立电动汽车产品运行状态监控平台，对已销售的全部电动汽车产品的全生命周期运行和安全状态进行实时监控。企业监控平台应当与地方和国家的监管平台对接。电动汽车生产企业应当在产品全生命周期内，为每一辆电动汽车产品建立档案，跟踪记录汽车使用、维护、维修情况（包括动力电池回收和处置情况）。按照国标，企业电动汽车监控平台可实现电池信息实时监控、车辆运行状态监控、车辆故障实时预警、车辆历史工况数据查询、对接国家监管平台的功能，并配置 CAN 车载终端（硬件）、配置服务器（硬件）。还可根据实际情况具有电池性能对比分析、车辆能耗对比、驾驶行为量化分析、重要零部件健康分析、自动化报表生成导出、维修保养跟踪及提醒功能。

#### 12.1.3 营运车辆改装要求

营运企业不得对车辆进行私自改装。若出于营运需要，必须进行改装的，事先需获得车辆生产厂家的书面许可。

## 12.2 电动营运车辆配置类安全要求

#### 12.2.1 车端一键报警功能

新能源营运车辆配备如一键报警模式的报警功能，主要功能：

（1）在遇到车辆自身故障抛锚或者不能正常行驶的情况下，一键报警，及时联系就近服务站进行救援、维修或相关指导；

（2）在遇到危险时，可以一键报警至呼叫中心，由呼叫中心进行报警。

### 12.2.2 车端 GPS 或 BDS 定位系统

新能源营运车辆必须配备 GPS 或 BDS 定位系统。采集信息为车辆的实时信息，如位置、在线情况、电量情况等，可根据车辆所在位置和在线时长进行车辆调度，协助维修、救援等。

### 12.2.3 前碰撞预警功能

新能源营运车辆可配备前碰撞预警系统功能，主要功能为可识别行人或机动车辆，当与前方障碍物可能发生碰撞时，通过声音或仪表显示进行预警，避免碰撞的发生。

### 12.2.4 驾驶员疲劳及健康状况检测功能

新能源营运车辆可配备驾驶员疲劳检测功能，主要功能为实时监控驾驶员状态，当诊断出酒精度超标、体温、血压异常或者当其遮挡监测镜头、疲劳闭眼、打哈欠、接打电话、抽烟等异常行为时进行预警，避免安全事故的发生。

### 12.2.5 油门误踩防护功能

新能源营运车辆可配备油门误踩防护功能，主要功能为当检测到车辆前方障碍物的距离小于安全时距，而司机有急踩油门动作时，切断整车动力输出，降低追尾等碰撞事故发生的概率。

### 12.2.6 碰撞缓解控制功能

新能源营运车辆可配备碰撞缓解控制功能，主要功能为当车辆检测到前方障碍物的距离小于安全时距，而驾驶员未采取相应动作时，控制系统依次：报警-断油-制动，降低事故概率。

## 12.3 电动营运车辆维修保养的安全要求

新能源生产企业要建立健全新能源营运车辆售后安全运行档案，做好安全检查、保养等服务，特别加强对动力电池、线束和连接器在内的高压系统的检查维护。重点对 IP 防护失效、车辆泡水、车辆碰撞、线束连接松动、频繁充放电、长期搁置及工作行驶环境恶劣的车辆加强保养。

营运车辆的使用频率高、行驶里程长，在一般车辆保养的基础上，营运车辆的保养频率要有所提高，保养项目有所增加。保养频率上主要按照行驶里程间隔进行，如增加 10 万公里、10 至 20 万公里、20 至 30 万公里的保养。保养项目上根据行驶里程不同而设置有针对性的检查保养项目，主要项目为动力电池、驱动电机、电机控制器等。动力电池检查至少包括电池的外观检查、软件诊断、气密性检测、开箱检查及换件和容量测试等内容。

对检查过程中发现的问题车辆，立即组织人员进行处理，消除安全隐患。

针对 IP 防护失效、车辆泡水、车辆碰撞、线束连接松动、频繁充放电、长期搁置及工作行驶环境恶劣的车辆分别设定特定的检查项目。

## 12.4 电动营运车辆远程监控的安全要求

### 12.4.1 车载监控

新能源车辆按照国家规定《电动汽车远程服务与管理系统技术规范》进行监控，能够采集到车辆基本信息，如车牌号、位置、车速、动力电池、电机、充电等信息。

### 12.4.2 通信接口要求

主要服务于远程监控平台，首先应满足国家和地方（北京、上海等）数据采集数据技术规范，如企业有其他更多需求，根据实际情况通信端口有所不同。如国家平台严格按照 GB/T 32960-2016 的规范标准，设计通讯数据结构和数据项字段，实现数据接口标准化。

### 12.4.3 企业监控平台

企业监控平台应对出现故障/报警的实车以及信息交换情况进行检查，做好相关记录，并进一步完善突发事件应急处理机制和应急处理预案。安全监控系统功能应符合国家标准要求，能及时反馈车辆安全信息，并对发现的整车及动力电池等关键系统运行状态异常、存在安全隐患的车辆能够及时预警并采取有效措施解决出现的问题。

对长期不在线的车辆进行安全隐患排查确定车辆实际使用状态。

## 12.5 电动营运车辆的安全事故处理要求

新能源营运车辆首先需满足第 9 章安全事故处理要求。

电动汽车营运企业应与生产企业一起制定新能源营运车辆事故应急预案、抢险救援方案和事故调查方案。

新能源营运车辆发生起火等安全事故后要立即启动应急救援预案并组织抢险救援工作。

新能源乘用车发生起火、燃烧等安全事故，未造成人员伤亡的，相关企业应在规定时间内主动上报地方政府；如造成人员死亡或重大社会影响的，应在 6 小时内主动上报。

## 12.6 健全安全管理机制

驾驶员的管理：电动汽车和传统汽车相比由电机直接驱动，起步加速性能较好，另外，

驱动电机参与辅助制动，既可以节能，也减少传统制动系统的磨损。对于驾驶员来说，适应其特点，可以更好地操作电动汽车。驾驶员根据车企提供的驾驶操作规范进行有序操作可以规避或降低事故风险，因此需要建立健全电动汽车的驾驶操作理论和实训要求，并纳入到驾驶员的考核指标里。

车辆的管理：新能源车辆应针对运营和存放过程中可能出现安全风险、碰撞事故、着火事故等，出具应急预案，如果能够第一时间获取信息，并按照应急预案执行，可以避免事故广大，降低社会影响。因此需要建立健全安全管理机制，比如成立车辆监控中心，实时监控车辆状态，尤其是电池的健康状态，并制定车辆发生着火安全事故的应急处理预案。

## 12.7 健全安全培训机制

管理层：应制定全员安全考核机制，并对其负责，把安全培训及新能源部件维护、保养方法的定期培训作为绩效考评指标，同步把所有车辆的安全事故作为最重要的考核内容。

机务人员：定期组织培训电动汽车关键部件的维保要求及新能源事故应急处理方法，将车辆因未及时维保或保养不当导致的新能源安全事故作为月度评价指标，提高机务人员对按期维保的责任心。

## 12.8 加强停运和报废安全管理

运营单位应建立专门的新能源车停运和报废安全管理规定，对于停运车辆要定期对有安全隐患的部件进行维护，对于已达报废条件的车辆不允许继续运营。针对报废动力电池等高危险部件，运营单位应按照《新能源蓄电池回收管理暂行办法》程序，展开电池回收，禁止私自进行处理。

# 氢燃料电池汽车篇

# 1 整车通用安全

## 1.1 一般设计准则

相对于纯电动车辆而言，氢燃料电池电动汽车的安全问题增加了氢安全相关内容。鉴于氢易燃易爆的特性及整车的电耦合使用环境，氢安全将直接影响到整车的安全性，且比纯电动汽车的安全性更为复杂。燃料电池电动汽车整车氢安全设计的一般原则如下：

（1）失效安全原则。在进行氢系统设计时，必须保证即使在某一零部件失效时，也不会因之导致更加严重的后果。换言之，当系统单一零部件出现故障时，系统是安全的。

（2）最简化原则。在进行氢系统设计时，在满足安全需求和使用需求的前提下，系统应尽可能简化，避免冗余。

（3）区域布置原则。在进行氢系统安装时，应将系统零部件尽可能集中布置，并根据压力等级进行分区域布置。

（4）氢电隔离原则。在进行氢系统安装时，应将氢系统与电气系统进行有效隔离。隔离措施可以是系统的物理隔离，也可以是针对可能产生火花的零部件自身的隔离，例如采用防爆电器。

## 1.2 失效评估及失效安全设计

### 1.2.1 失效安全设计一般原则

整车通用安全的核心在于保护人员免受危险因素的影响。针对燃料电池电动汽车的潜在失效进行对应的安全设计，燃料电池电动汽车的潜在失效后果主要包括：

（1）车辆运行过程系统零件故障和/或由外部事件（如碰撞）导致车辆系统损坏；

（2）车辆运行、维修过程中出现由操作失误引发的危险（例如高电压、极端温度、高气压，以及易燃或有毒流体）；

（3）由子系统或部件故障引起的车辆系统损坏，无法正常使用。

### 1.2.2 危害的隔离和分离

燃料电池电动汽车重点考虑氢的有效隔离，常用的设计方案是将可能产生电弧或火花等火源形式的点与氢系统进行隔离，或将可能产生静电、电弧及火花的地方可靠接地。

设计层面，氢系统应优先选择利于通风释放的部位进行布置，若无法满足需增加必要的通风设计以避免氢气聚集引发危险；同时氢系统与电气系统尤其是高压电气系统需保持一定的安全距离（如对商用车，安全距离重点关注线束接插件距离氢气管接头的距离，一

般大于 100mm 以上；如果接头有防护，则距离可适当减小），避免电火花的能量引燃氢气；车辆故障或碰撞事故时，氢系统可基于温度、压力、流量等物理量实现快速断氢。

使用层面，车辆加氢过程禁止上高压，可仅唤醒必要的控制器（实现加氢功能以及加氢过程的监测功能），减少电气系统与氢系统之间的耦合风险。

### 1.2.3 失效安全设计

危害分析和风险评估的目的是识别相关项中因故障而引起的危害，并对危害进行归类，制定防止危害事件发生或减轻危害程度的安全目标，以避免不合理的风险。基于设计 FMEA 与过程 FMEA，失效安全从功能安全、系统安全、硬件安全和软件安全等四个方面开展设计工作。

1.2.3.1 功能安全设计

基于 GB/T34590.2-2017 相关规定，根据 ASIL 等级的安全目标进行功能安全审核和评估工作。燃料电池电动汽车的功能安全设计要求参考 GB/T24549-2009 的相关内容。针对车辆的不同故障等级，制定不同的故障处理机制，表 1-1 给出了某车型设计中的故障分级及处理机制示例。

表 1-1 燃料电池电动汽车故障分级及处理机制

| 故障级别 | 三级故障 | 二级故障 | 一级故障 |
|---|---|---|---|
| 说明 | 严重故障 | 较严重故障 | 警告故障 |
| 处理机制 | 车辆下高压 | 车辆限制扭矩输出 | 仪表提示 |

### 1.2.3.2 系统安全设计

基于 GB/T34590.4-2017 相关规定，根据功能安全概念和系统架构设想定义技术安全要求，明确软硬件的外部接口、限制条件和系统配置要求等；同时定义系统对于影响实现安全目标的激励的响应，包括失效和相关的激励组合，并与每个相关运行模式及规定的系统状态进行组合。系统架构设计过程中，为保证系统安全，应重点关注以下要素：

（1）应消除已识别出的引起系统性失效的内/外部原因，或减轻它们的影响；

（2）为减少系统性失效，宜应用值得信赖的汽车系统设计原则，包括技术安全概念的再利用、要素设计的再利用、探测和控制失效机制的再利用、标准化接口的再利用。

### 1.2.3.3 硬件安全设计

从硬件安全要求定义、硬件设计及实现、硬件架构评估及失效分析、硬件系统集成及测试等四个方面进行硬件安全设计工作，参考 GB/T34590.5-2017。

**硬件安全要求定义：**基于技术安全概念和系统设计规范，定义硬件安全要求，同时细化控制安全设计涉及的软硬件接口（HSI）规范。硬件安全要求设计应包含以下内容：

（1）具备覆盖相关的瞬态故障（例如所用技术而产生的瞬态故障）的内部安全机制；

（2）具备应对外部失效的容错功能；

（3）具备探测硬件零部件失效、故障诊断和发送失效信息等功能。

**硬件设计及实现：**基于硬件架构度量的评估，充分考虑功能冗余及功能要求，优先采用车规级成熟电路单元，元器件选用车规级元器件；同时考虑与安全相关的元器件失效的非功能性原因，包括温度、振动、湿度、灰尘、电磁干扰、噪声、环境串扰等因素。具体设计要求如下：

（1）符合 QC/T413-2002 汽车电气设备基本技术条件所规定的电气性能要求；根据 GB/T28046.2-2011 的要求满足工作电压、电源过电压性能、电源叠加交流电性能、电源电压跌落性能、电源启动特性、电源极性反接、抛负载性能、供电电压缓升和缓降性能、供电电压瞬时下降性能等要求；高压防护安全参考《电动汽车安全指南》中第一章及第二章相关设计要求。

（2）满足车辆运行环境的需求，针对布置在底盘等湿区位置的产品防护等级不应低于 IP67；根据 GB/T28046.3-2011 的要求满足低温性能、高温性能、温度冲击性能、温湿性能、盐雾性能、防护性能、自由跌落性能等产品性能要求；同时考虑防火隔离和阻燃设计，燃料电池系统与客舱之间使用阻燃隔热材料隔离，阻燃隔热材料的燃烧性能符合 GB 8624-2012 中规定的 A 级要求。燃料电池系统内零部件材料均需考虑阻燃要求，满足以下阻燃要求：金属材质零部件材质满足水平燃烧 HB 级和垂直燃烧 V-0 级的要求，其它非金属零部件材质满足水平燃烧 HB75 级和垂直燃烧 V-2 级的要求。

**硬件失效模式分析：**通过对硬件失效模式分析，识别硬件设计中因潜在风险导致的产品失效，建立 FMEA 表，以保证分析的完整性。对于侵害安全的失效模式，应制定相应的安全机制来保证安全性；对于非侵害安全的失效模式，需评估设定安全机制的必要性。硬件失效分析应识别以下内容，并给出相应的措施：

（1）对安全故障，制定相应的安全机制，主要包括与硬件自身故障相关的探测、指示和控制措施；影响到系统硬件的外部设备发生故障的探测、指示和控制措施；系统实现或维持在安全状态下措施；细化和执行报警和降级概念的措施；以及防止故障潜伏的措施。

（2）对单点故障或残余故障，评估设定安全机制的必要性，主要评估系统实现或维持在安全状态下措施的有效性，同时评估残余故障的诊断覆盖率。

（3）对多点故障（无论是可感知的、可探测的或潜伏的），评估设定安全机制的必要性，主要评估可接受的多点故障探测事件间隔内潜伏故障的失效探测及警示驾驶员措施的有效性，同时评估潜伏故障的诊断覆盖率。

**硬件系统测试：**为了验证硬件设计与硬件安全要求的正确性、一致性和完整性，硬件系统测试应考虑按以下方法进行。测试内容以硬件设计的具体要求为主：

（1）功能性测试。针对被测硬件电气性能、高压防护性能等进行测试。

（2）非功能性测试。针对硬件的环境适应性、防水阻燃性能、耐久可靠性等进行测试。

#### 1.2.3.4 软件安全设计

基于 GB/T34590.6-2017 相关规定，进行软件安全要求的定义、软件架构设计、软件单元设计及实现、软件单元测试、软件集成及测试、软件安全要求验证，并满足系统设计和软件安全需求的要求。

**软件安全要求的定义：**软件安全要求的定义来源于技术安全要求和系统设计规范，同步考虑硬件约束（硬件的接口规范、设计规范及运行模式等）对软件的影响。软件安全要求应针对每个基于软件的功能，这些功能的失效可能导致违背分配到软件的技术安全要求。软件安全定义需满足完整性、可测试性及可追溯性要求。

**软件架构设计：**软件架构设计描述全部软件组件及其在层次结构中的交互。静态方面，如所有软件组件间的接口和数据路径；动态方面，如进程顺序和时序行为。软件架构设计提供了实施软件安全要求和管理软件开发复杂性的方法。软件架构设计应考虑软件架构设计的可验证性、可配置软件的适用性、软件单元设计及实现的可行性、软件集成测试中软件架构的可测性及软件架构的可维护性。为避免因高度复杂性导致的失效，软件架构设计需具有模块化、封装性和简单性属性。具体方法包括优化软件组件的层次、限制软件组件的规模、限制接口规模、组件内高内聚、组件间低耦合、恰当调度的特性以及限制中断的使用等。

**软件单元设计及实现：**基于软件架构设计开发软件单元的详细设计。详细设计分别按照建模或编码指南，以模型或直接以源代码的形式实现。在进入软件单元测试阶段前对详细设计和实现进行静态验证。软件单元的实现包含源代码的生成和转换为目标代码。具体方法包括：（1）子程序和函数采用一个入口和一个出口；（2）无动态对象或动态变量，否则需要在其产生过程中对齐进行在线测试；（3）变量初始化；（4）不能重复使用变量名称；（5）避免全局变量，否则需证明对全局变量的使用是合理的；（5）限制使用指针；（6）

无隐式类型转换；（7）无隐藏数据流或控制流；（8）没有无条件跳转；（9）无递归。

**软件单元测试：**软件单元测试目的是要证明软件单元满足软件单元设计规范且不包含非期望的功能。根据软件单元设计规范，建立软件单元测试流程，并按照该流程执行测试。在软件单元测试过程中，证明软件单元达到：（1）符合软件单元的设计规范；（2）符合软硬件接口的定义；（3）已定义功能；（4）确信没有非预期的功能；（5）鲁棒性；（6）足够的资源来支持它们的功能。为了评估测试用例的完整性并证明没有非预期的功能，应确定软件单元层面的要求覆盖率，同时对结构覆盖率进行测定，如果认为已实现的结构覆盖率不充分，应定义额外的测试用例或提供接受理由。

**软件集成及测试：**按照软件架构设计，对软件要素之间特有的集成层次和接口进行测试，软件要素的集成和测试的步骤直接对应着软件的分层架构。软件集成应完成各个软件单元分层集成到软件组件，直到整个嵌入式软件全部被集成，并考虑与软件集成相关的功能依存关系和软件集成和软硬件集成之间的依存关系。软件集成测试方法与软件单元测试类似，目的是为证明软件组件和嵌入式软件均实现相应的功能要求。

**软件安全要求验证：**软件安全要求验证的目的是证明嵌入式软件在目标环境下满足软件安全要求。软件安全要求验证中的测试环境可为硬件在环，电控单元网络环境及整车环境。可考虑使用工具(例如 trace ability matrix)确保和评估软件安全要求的覆盖率，可以复用已有的测试用例。如果覆盖率不充分，应增加测试用例或给出可以接受的理由。

## 1.3 整车 EMC 及电气可靠性安全

燃料电池电动汽车上的所有可能影响车辆安全运行的电气组件，在功能上都应该能够承受车辆暴露于其中的电磁环境。车载储能系统、驱动系统和控制系统运行在高电压、大电流以及处在较大的 dU/dt 或 dI/dt 条件下，车辆应可正常运行，不应造成误停车。车辆在满足传统内燃机汽车 EMC 要求的同时，还应符合车辆不同运行状态下的 EMC 特殊要求。

### 1.3.1 整车车外辐射骚扰及抗扰度要求

整车对外部的电磁骚扰应满足 GB14023-2011、GB/T18387-2017 相关要求，以保护车辆外部的无线电通讯设备正常工作；

整车耐受外部的电磁辐射干扰应满足 GB/T34660-2017 相关要求，以保障车辆的功能状态和安全等级。

### 1.3.2 车载电器设备辐射骚扰及抗扰度要求

车载电器设备辐射骚扰及抗扰度应满足表 1-2 的要求。

表 1-2 辐射骚扰及抗扰度测试要求

| 测试项目 | | 国标要求 |
|---|---|---|
| 发射 | 辐射发射 | GB/T18655-2018 |
| | 传导发射 | GB/T18655-2018 |
| | 瞬态传导发射 | GB/T21437.2-2008 |
| 抗扰度 | 电波暗室法 | GB/T33014.2-2016 |
| | 大电流注入 | GB/T33014.4-2016 |
| | 瞬态传导抗扰度(电源线) | GB/T21437.2-2008 |
| | 瞬态传导抗扰度(信号线) | GB/T21437.3-2012 |
| | 静电放电 | GB/T19951-2005 |

### 1.3.3 整车充电过程中沿电源线骚扰和抗扰度要求

车辆处于电源线传导充电工况模式，沿电源线骚扰和抗扰度建议参照 UN R10《关于批准车辆电磁兼容性的统一规定》（第 5 版）的试验方法进行验证，需满足相关要求。

### 1.3.4 整车乘员暴露于车辆电磁环境安全要求

整车乘员暴露于车辆电磁环境应满足 GB/T 37130-2018 中的相关要求。

### 1.3.5 高低压线束设计布置要求

高压线束应具备 EMC 屏蔽措施，其走向布置不应使 EMC 辐射增强。高压线束屏蔽层应与高压部件可导电外壳有效连接。

### 1.3.6 整车电气可靠性要求

燃料电池电动汽车整车需完成电气可靠性测试并达到要求，具体测试项目及参考标准如表 1-3 所示。

表 1-3　电磁兼容性测试项目及参考标准

| 测试项目 | 标准要求 |
|---|---|
| 过电压 | GB/T 28046.2-2011 |
| 叠加交流电 | |
| 供电电压缓升和缓降 | |
| 供电电压瞬时下降 | |
| 电压骤降复位性能 | |

| | |
|---|---|
| 启动特性 | |
| 抛负载 | |
| 反向电压 | |

## 1.4 整车碰撞安全

碰撞传感器检测到整车发生碰撞时，应能够自动切断电源和氢气供应，以确保碰撞后车载供氢系统的完整性、电气系统完整性等。具体要求如下：

（1）车载供氢系统完整性

高压氢气瓶的固定装置不应出现断裂、脱落或导致高压储氢系统安全功能失效的移位或变形；高压管路系统不应破损、断裂，瓶口阀不应损坏失效； 在发生碰撞后的 60 min 之内，车载供氢系统的平均氢气泄漏率不得超过 118 NLPM；封闭空间内的氢气浓度不应超过 4%。

（2）电气系统完整性

根据 GB11551-2014 和 GB20071-2006 适用范围的规定，对带有 B 级电压电路的燃料电池电动汽车进行碰撞试验后，高压安全应符合 GB/T 31498-2015 的相关要求。

### 1.4.1 侧面碰撞防护设计

侧面防护结构可参考 GB 20071-2006 等标准进行碰撞试验，车辆在碰撞试验后应符合 GB/T 31498-2015 中 4.2～4.4 的要求。

### 1.4.2 侧翻防护设计

车身防护结构若按 GB 17578-2013 进行上部结构强度验证试验，应在其可充电储能系统荷电量（SOC）30%～50%且处于上电状态下进行试验，试验后应符合 GB/T 31498-2015 中 4.2～4.4 的要求。

### 1.4.3 后碰撞防护设计

后高压舱 B 级电压部件的布置位置和防护结构应考虑被追尾后，符合 GB/T 31498-2015 中 4.2～4.4 的要求，对燃料电池乘用车，后碰撞测试方法可参考 GB/T 20072-2006。

### 1.4.4 底部碰撞防护设计

底部碰撞防护设计要考虑两方面，一是离地间隙，二是防护结构。防护设计应能满足发生底部碰撞后符合 GB/T 31498-2015 中 4.2～4.4 的要求。

## 1.5 安全标记要求

### 1.5.1 高压警告标记要求

B 级电压部件，如 REESS（车载可充电储能系统）和燃料电池堆，按照 GB 2893-2008、GB 2894-2008 和 GB/T 5465.2-2008 的规定，应标记图 1-1 所示符号。符号的底色为黄色，边框和箭头为黑色。

当移开遮拦或外壳可以露出 B 级电压带电部分时，遮拦和外壳上也应有同样的符号清晰可见。当评估是否需要此符号时，应当考虑遮拦/外壳可进入和可移开的情况；标记附近建议有明显可见的安全操作注意项目的提醒，如“电机控制器开盖要等 xx 分钟后，测量母线电压值为安全电压后方可操作”。

图 1-1 高压警告标记

### 1.5.2 B 级电压电线标记要求

B 级电压电路中电缆和线束的外皮应用橙色加以区别，外壳里面或遮拦后面的建议也用橙色加以区别。

B 级电压连接器可通过与之连接的线束来区分。

### 1.5.3 危险物质标识

车辆易见位置张贴表示氢燃料类型的图形标识，压缩氢气的标识代号为 CHG、液态氢的标识代号为 $LH_2$，图形标识见下图，标识尺寸及字体按 GB/T 17676-1999 的规定。标志应清晰、醒目、防水、防腐，标志应贴在车辆醒目位置。

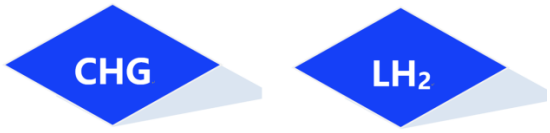



图 1-2 氢燃料标识

# 2 车载氢系统安全

## 2.1 安装及布置

### 2.1.1 车载氢系统安装及布置一般准则

（1）车用氢系统的安装需依据 GB/T 24549-2009 《燃料电池电动汽车 安全要求》、GB/T 26990-2011《燃料电池电动汽车 车载氢系统技术条件》与 GB/T 29126-2012《燃料电池电动汽车 车载氢系统试验方法》的规定，确保车载氢系统安装后，在正常使用条件下，应能安全、可靠地运行。此外，车载氢系统中的储氢瓶与固定装置间应有防护垫，防止固定装置磨损瓶体，并严禁损伤氢瓶的缠绕层。

（2）车载氢系统（从氢气加注口至燃料电池进口，主要包括储氢瓶、管路、连接件、阀件与支架等）需型式试验，分别在车辆坐标系 X、Y、Z 三个方向施加 8 倍于充满标称工作压力氢气的储氢瓶重力的力，测量检查储氢瓶与固定座的相对位移，其值应小于 13mm。此外，严禁储氢瓶瓶嘴及附带的阀门或易熔合金塞经受长期应力。在储氢瓶运输、安装、拆装过程中，尽量不采取直接吊装瓶嘴、阀门或易熔合金塞的方式进行。

（3）储氢瓶及附件的安装位置，应距车辆的边缘至少有 100mm 的距离，否则，应增加保护措施。

（4）氢系统管路、接头安装位置及走向要避开热源、电器、蓄电池等可能产生电弧或火花的地方，尤其管路接头不能位于密闭的空间内，应安装在能看得见或操作者易于操作的位置。高压管路及部件可能产生静电的地方要可靠接地，并采取其他控制氢泄漏量及浓度的措施，确保即使产生静电也不会发生安全问题。

（5）储氢瓶和管路一般不应装在乘客舱、行李舱或其他通风不良的地方，但如果不可避免要安装在行李舱或其他通风不良的地方时，应设计通风管路或其他措施，将可能泄漏的氢气及时排出。管路接头不得通过和安装在载人车厢内，不得安装在高热源、易磨损或易受冲击的位置。

（6）支撑和固定管路的金属零件不应直接与管路接触，需要加装非金属衬垫，但管路与支撑和固定件直接焊合或使用焊料连接的情况例外。

（7）加氢口不应位于乘客舱、行李舱或其他通风不良的地方；加氢口应具有能够防止尘土、液体和污染物等进入的防尘盖，防尘盖旁应注明加氢口的最大加注压力；加氢口应设置在客车侧面；加氢口应能够承受来自任意方向的 670N 的载荷，不应影响到氢系统气密性。

（8）在可能发生泄漏的部位及载人车厢内，都应合理地安装氢气泄漏探测器，探测器应安装在氢气最易发生积聚的位置，一般为局部最高点，通风不好的地方。

（9）当储氢瓶布置在车架下方时，储氢瓶下方应采取有效防护措施，应有效避免驱动轮造成的异物飞溅撞击储氢容器，且储氢瓶及其附件不允许布置在客车前轴之前。

（10）当储氢瓶安装在车辆的外露空间时，应采取有效的防护措施。

（11）储氢瓶周围应避免有尖锐、棱角等结构的零件。

（12）储氢瓶底置设计时，储氢瓶舱体的两侧舱门上应有格栅，保证正常通风。

（13）储氢瓶底置设计时，储氢瓶舱体与乘客舱应保证有效的隔离，防止泄漏的氢气进入乘客舱。

（14）储氢瓶底置设计时，与氢系统无关的电气线路和气体管路接头应尽量避开储氢瓶舱室。

（15）燃料电池汽车上的储氢装置在使用或存放时应安装牢固，具有缓冲保护措施，以防止其使用时发生移动或损坏。横向移动幅度不应引起危险。任何完整的高压氢气储存容器应包括一个连接固定装置，应采取必要措施，避免热源及电器、蓄电池等可能产生电弧的部件对氢气供应系统的影响。

### 2.1.2 乘用车载车储氢瓶安装及布置案例

乘用车车载储氢瓶配置应综合考量足够的乘客空间、行李置放空间与燃料储量，并考虑车辆安全性与重量平均分配，建议轿车车载储氢瓶置于轿车底盘下方中部、后座乘客椅座的下方，以及后备箱与后轮间的开放空间。受空间的限制和规避停驶期间安全排放的风险，可采用两个或三个 35MPa/70MPa 高压储氢瓶。乘用车储氢瓶的安装及布置方案策略案例参考图 2-1。

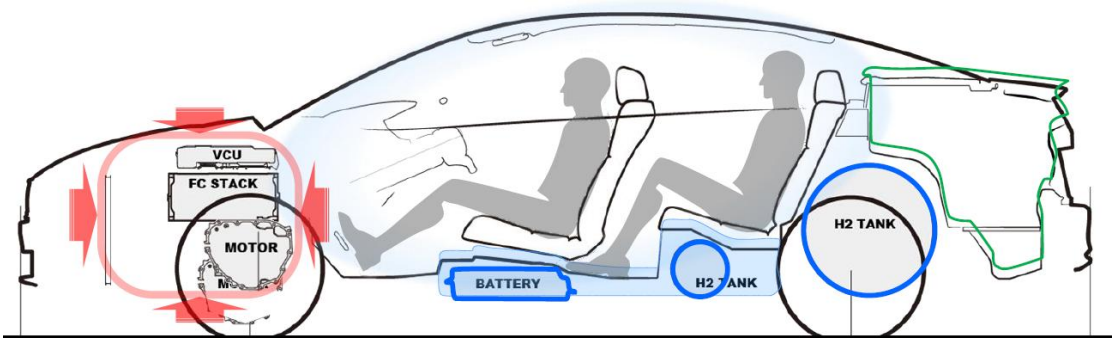



图 2-1　燃料电池乘用车储氢瓶放置策略案例

### 2.1.3 商用客车车载储氢瓶安装及布置案例

由于底盘放置了动力电池、DC/DC 转换器及驱动电机，加上目前商用客车多为低底盘客车以方便乘客搭乘，建议将燃料电池商用客车的多瓶组车载氢系统布置于车顶。除了考虑负载均衡以及不影响客车内部乘车空间外，车顶氢系统的罩壳可做成玻璃钢件，顶裙围采用成型的铝合金板，有效地保证车辆外观的平整性与连贯性。顶部的空间更有利于布置多个氢瓶，以增加储氢量和续驶里程。此外氢系统罩壳顶部可以打开，方便储氢瓶的维护与安全操作。图 2-2 为供氢系统布置于顶部前半部的燃料电池商用客车案例。

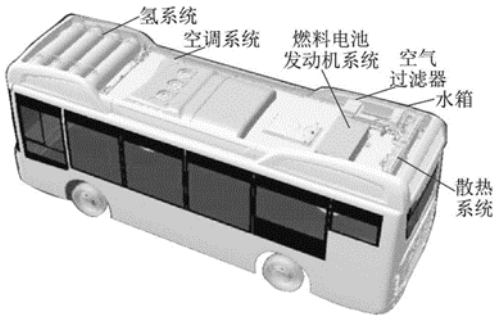



图 2-2　燃料电池商用客车储氢瓶放置案例

### 2.1.4 商用货车车载储氢瓶安装及布置案例

商用货车为了保证其续驶里程超过 350 公里，目前通常布置多瓶组 35MPa 的车载氢系统，中小型货车设置双瓶组或三瓶组，大型货车的储氢瓶可能会超过四组，必要时采用 70MPa 储氢系统以提高储氢量和续驶里程。建议将储氢瓶以横卧叠排式放置于靠近牵引头的车辆底盘上，可增加货车箱的空间利用率。商用货车氢系统的布置方案可参考图 2-3。

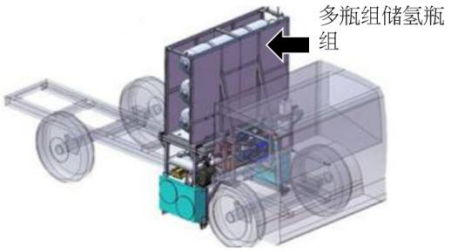



图 2-3　燃料电池商用车储氢瓶放置策略

## 2.2 安全设计及管理

### 2.2.1 氢系统安全设计一般原则

（1）氢气供应、连接装置及管路应能防止氢腐蚀及氢脆。

（2）氢气供应系统应有过流保护装置或其他措施，当检测到氢气储存容器或管路内

压力异常降低或流量异常增大时，能自动关断储氢瓶内的氢气供应；如采用过流保护阀，该阀应安装在主关断阀上或紧靠主关断阀处；还应设置压力释放装置，在释放管路的出口采用必要的保护措施，防止在使用过程中被异物堵塞，影响气体排放。

（3）氢气供应阀组应符合以下要求：向燃料电池系统供应氢气，既具有减压阀功能，又具有安全关闭阀功能，阀的关断时间不超过 1s；电气操作的氢气供应阀应符合 GB14536.19-2017 规定的要求。

（4）氢系统可能产生静电的地方要可靠接地，接地点应使用铜螺母，供氢系统外壳与接地端子间的电阻应小于 0.1Ω；或采取控制氢泄漏量及浓度的措施，以使得即便在产生静电的地方也不会发生安全问题。

（5）氢系统应安装氢气浓度检测装置，当检测到氢气浓度超过 50%LFL，能自动关断储氢瓶内的氢气供应。

（6）氢系统其他安全技术要求，应符合 GBT34872-2017 的要求。

### 2.2.2.高压储氢瓶

车载高压储氢瓶应依据 GB/T 35544-2017《车用压缩氢气铝内胆碳纤维全缠绕气瓶》、TSG R0006-2014《气瓶安全技术监察规程》等法规和标准进行设计、制造与检验；储氢瓶充装、运输、储存、使用与检验须符合 TSG R0006-2014《气瓶安全技术监察规程》及 TSG R0009-2009《车用气瓶安全技术监察规程》的规定。车用储氢瓶常用的公称工作压力有 35 MPa 和 70MPa 两种规格，工作环境温度为-40℃～85℃，设计使用寿命 15 年（35 MPa）和 10 年（70 MPa），根据工作压力和使用场景的不同，设计循环充放次数为 7500-11000 次，当气瓶实际使用年限未达到设计年限，但充装次数已达到设计循环充放次数时候，气瓶应当报废；此外，车辆已达使用年限或欲报废时，气瓶需随车报废。

#### 2.2.2.1 高压储氢瓶生产制造资格

高压储氢瓶制造厂家应具有与所生产储氢瓶相符合的压力容器特种设备制造许可。车用压缩氢气铝内胆碳纤维全缠绕气瓶所需要的制造许可资质为 B3（3）。

#### 2.2.2.2 型式试验与出厂试验

车用高压储氢瓶应依据 GB/T 35544-2017《车用压缩氢气铝内胆碳纤维全缠绕气瓶》中的规定，按规格进行型式试验，按批次进行破坏性试验，逐只进行出厂试验，并达到合格指标。为了确保高压储氢瓶的安全性，试验项目包括：缠绕层力学性能、拉伸试验、水压试验、气密性试验、水压爆破试验、常温压力循环试验、火烧试验、极限压力温度循环试验、加速应力破裂试验、裂纹容限试验、环境试验、跌落试验、氢气循环试验、枪击试

验、耐久性试验、使用性能试验等。

**2.2.2.3 定期检验**

（1）按《气瓶安全技术监察规程》的要求，储氢瓶应逐只或随车进行定期检验，储氢瓶定期检验周期为三年，并应到有资质的检验单位定期去检验。

（2）储氢瓶的拆卸检验会改变系统管路阀件的密封状态，重新装配的过程可能会导致管路连接件的失效和必要的更换，同时需要重新检测系统密封的可靠性。在储氢瓶本体质量可靠的前提下，应尽量避免或减少储氢瓶的拆卸检验。

（3）储氢瓶在使用过程中，发现有严重腐蚀、损伤或对其安全可靠性有怀疑时，应提前进行检验。

（4）报废储氢瓶应进行破坏处理确保其无法再次充装。

2.2.2.4 储氢瓶的安全使用

（1）采购和使用有制造许可证的企业的产品，并在检验合格有效期内。

（2）使用者必须到已办理充装注册的单位或经销注册的单位充装氢气。

（3）储氢瓶使用前应进行安全状况检查，并对充装气体进行确认。不符合安全技术要求的储氢瓶严禁使用。应严格按照使用说明书的要求使用储氢瓶。

（4）储氢瓶及其系统的放置地点，不应靠近热源、明火及易受电击的地方，应保证气瓶瓶体干燥。

（5）储氢瓶及其系统不应储存在阳光曝晒和高潮湿及含有腐蚀介质的环境中，如需长期储存，应采取可靠的防潮防护等措施。

（6）储氢瓶的复合材料层严禁划伤、磕碰以及酸碱腐蚀。

（7）严禁敲击、碰撞、挖补、打磨储氢瓶，严禁在储氢瓶上进行电焊引弧，严禁损伤缠绕层及擅自更改气瓶标签，严禁用温度超过 85℃的热源对储氢瓶加热。

（8）开启瓶阀时，操作者应站在瓶阀气体喷出方向的侧面，避免气流朝向人体。

（9）禁止在带压力的气瓶上用拧紧瓶阀或垫圈螺母的方法来消除泄漏。

**2.2.2.5 储氢瓶出现火灾时的消防措施**

（1）在确保人身安全的情况下，切断气源。

（2）疏散人员远离火灾区，并往上风处撤离；对着火区进行隔离，防止人员入内，可能的话，将处在火灾区附近、未受火直接影响的储氢瓶转移到安全地段。

（3）如氢气无法切断的话，可让气体燃烧，直到储氢瓶内的氢气烧完为止。注意：这种处理方法是在假设火势可以控制的前提下采用的，而且，燃烧过程中，应持续用水对

储氢瓶进行持续冷却，直到氢气完全烧尽为止，避免储氢瓶因过热而发生爆炸事故。

（4）若着火点是在室外通风条件良好的地方，如可能，站在安全位置上进行灭火。并用水对着火的储氢瓶、以及着火区附近的所有压力容器进行持续冷却，使它们在火场中保持冷却。不得设法搬动或靠近被火烘热的储氢瓶。

（5）如遭遇火警，应立即向消防队报告，告知对方着火的详细地点以及着火原因。火灾解除后，不得使用遭受火灾影响的储氢瓶。

### 2.2.3 高压系统阀门

车载氢系统除储氢瓶外，还可包含：加氢口（加注口）；安装于电堆与车载氢系统之间的减压阀、安全阀、手动排空阀；集成式瓶口阀，含电磁阀、单向阀、手动截止阀、温度传感器、温度驱动的压力释放装置(TPRD)、压力传感器等；或压力驱动(如爆破片等)的压力释放装置(PRD)，以上构成高压系统核心安全阀门。基本的典型加注与保护措施如图 2-4 所示。另外在储氢瓶与驾驶座附近配置氢气传感器或氢气泄漏检测装置，可在规定响应时间内（一般 1s）感知氢气泄漏、关闭氢气瓶电磁阀并发出警报，形成多重保护措施。

加氢口应符合 GB/T 26779-2011《燃料电池电动汽车加氢口》标准规定，并单独进行强制性检验。集成式瓶口阀和温度驱动的压力释放装置，除了单独进行型式试验之外，还应与高压氢瓶一起进行火烧试验以验证其安全性，并出具型式试验报告。

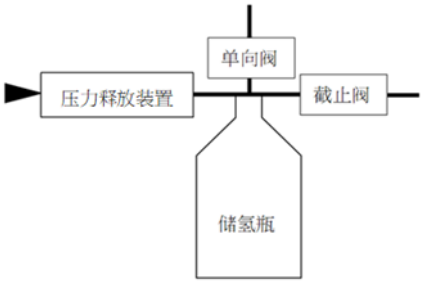



图 2-4　氢气基本加注流程与保护措施示意图

#### 2.2.3.1 储氢瓶内部压力、温度过高

（1）当储氢瓶内部压力超过额定值，有安装 PRD 的会自动将多余压力排空。

（2）当储氢瓶内外部温度过高，TPRD 熔断并释放储氢瓶内部因温度升高造成压力的升高，从而保护氢瓶的安全。

#### 2.2.3.2 氢气泄漏

（1）氢气传感器可在其响应时间内（一般为 1s）感知到氢气泄漏。在燃料电池系统

中易发生氢气泄漏或者氢气积聚的部位（危险区域，0 区和 1 区的稀释范围内），且驾驶员容易识别的部位安装氢气泄漏报警提醒装置，泄漏量与警告信号的级别由制造商根据车辆的使用环境和要求决定，建议配置与传感器相应的安全连锁装置。当空气中氢气体积含量不低于 2.0%±1.0%时，发出警告；空气中氢气体积含量不低于 3.0%±1.0%立即关断氢供应；但如果车辆装有多个氢系统，允许仅关断有氢泄漏部分的氢供应。

（2）出现氢泄漏时，在确保人身安全下，根据情况将车辆断电，自动关闭瓶口阀中的电磁阀，切断从瓶内氢气泄漏的源头。

（3）消除周围明火，停止周围一切可能产生明火或火花的作业。

（4）疏散人员，避开气流，往上风处迅速撤离，对漏气场所进行隔离，避免无关人员入内。

（5）车辆上的储氢瓶发生泄漏时，不得将氢气排放到有火花、通风条件差、密闭或存放氧化剂（如氧气）的地方。注意：排空储氢瓶时，应控制氢气流速，避免因氢气流速过快而导致氢气着火事故。排空氢气的过程中，现场应准备适当的灭火装置并有人在现场监控，以确保安全。排空后，关上瓶阀。

（6）进入漏气地段之前，应事先对该地段进行合理通风，加速扩散，确保安全。

（7）漏气储氢瓶要妥善处理，修复并检验合格后再用。

### 2.2.4 控制仪表类（压力表，各类传感器与控制器，液位计等）

车用各类仪表的标准须符合 QC/T 727《汽车、摩托车用仪表》、QC/T 824-2009 《汽车用转速传感器》中的规定，其中包含：

（1）压力表应能承受 30000 次的交变循环试验。试验时其各部分应无异常变化。

（2）转速传感器应能承受 1000h 的交变循环试验。试验时其各部分应无异常变化。

（3）汽车用电子车速里程表应 100000km 的耐久性试验。试验时其各部分应无异常变化。

（4）电流表应能承受 30000 次的电流交变循环测试。试验时其各部分应无异常变化。

（5）温度表应能承受 3000 次的指示交变循环测试。试验时其各部分应无异常变化。

（6）电压表应能承受 20000 次的电压交变循环测试。试验时其各部分应无异常变化。

（7）氢气泄漏传感器应有 8 年的寿命。

（8）定期检验各仪表功能是否正常。

（9） 燃料电池汽车建议有自检功能，可自动诊断车辆上所有的电子传感器使用疲劳次数，提供信息给驾驶员判断车辆安全的依据。

### 2.2.5 储氢瓶的固定结构

储氢瓶的固定结构失效会使得氢瓶及其管路阀门等失去保护，缩短其使用寿命甚至发生氢气泄漏等安全事故。

（1）储氢瓶安装到框架后，建议针对每个系列的车载供氢系统进行振动可靠性试验，检验结构件、支撑件强度和车载氢系统的管路与支架的可靠性。

（2）建议定期检查车载氢系统固定结构松紧程度，并观察氢瓶是否有位移和转动。

## 2.3 氢气加注

### 2.3.1 高压氢气加注工艺

高压氢气加注主要涉及的步骤，包括高压氢气长管拖车内的氢气转注至加氢站，再经由氢气压缩机增压输送至高压储氢瓶（瓶组或蓄能器），并经过热交换系统降温，最后再通过加氢机对车辆进行加注。

加注工艺及设施、氢气压缩工艺及设备、氢气储存系统与设备、加氢机与氢气管道和附件需达到 GB 50516-2010《加氢站技术规范》、GB/T 34584-2017《加氢站安全技术规范》中的要求；加氢机的设计制造应符合 GB/T 31138-2014 和 GB 50516-2010 的有关规定。

用于充装燃料电池汽车的氢气质量应符合 GB/T 37244-2018《质子交换膜燃料电池汽车用燃料氢气》或 SAE J2719-2015《Hydrogen Fuel Quality for Fuel Cell Vehicles》标准的规定，尤其应注意气体杂质成分的控制与检测，因为微量的 CO、CO2、硫化物、烷烃、卤化物等杂质就会导致 Pt 催化剂中毒、双极板腐蚀、MEA 劣化，使得燃料电池性能衰减和性能不可恢复，卤化物还会造成加氢站不锈钢设备的应力腐蚀。不能用直接采用工业氢气和高纯氢气质量标准。

在首次加注氢气至储氢瓶前，为了确保瓶内氢气无燃烧的可能性，建议使用氮气或惰性气体进行瓶内吹扫，然后通过符合 GB/T 37244-2018 的氢气进行置换。

若氢气出站的质量无法达到标准，应根据进站氢气纯度或杂质含量选择相应的氢气纯化装置，氢气纯化装置宜设在氢气压缩机前；加氢工艺系统中的纯化、压缩、计量、混合、输送、储存等工序，均应设有压力检测点，并应根据安全运行的要求设置超压或低压报警装置。

### 2.3.2 加注安全与智能化监控

（1）氢气加注应在空旷、通风敞开环境下操作，加氢机不宜安放在室内。如果要在室内进行加氢操作，应选择空旷通风区域，并有防止泄漏氢气聚集和预防火灾事故的安全

措施。

（2）加氢机应安放在高度超过 120 mm 的基座上，基座边缘离加氢机至少 200mm。加氢机周围应设置防撞柱（栏），预防车辆撞击造成加氢机损坏。

（3）加氢机或加氢岛应设置紧急切断按钮以及与加氢系统配套的自动控制装置，当紧急切断按钮被触发时应实现下列连锁控制：

●加氢站断电（监控、照明用电除外）；

●自动关闭加氢机进气管道的切断阀；

●自动关闭上游的压缩系统。

（4）加氢机内应设置氢气泄漏检测报警装置，当泄漏氢气在空气中含量达 0.4%时应向加氢站内控制系统发出报警信号，当泄漏氢气在空气中含量达 1.6%时应向加氢站内控制系统发出停机信号，并自动关闭阀门停止加气。

（5）为了防止消费者在加氢枪未脱离车辆时将车辆驶离加氢站，导致相关管路破裂引起氢气大量泄漏，在连接加氢枪的加气软管上应设置拉断阀。拉断阀、加气软管及软管接头等，应符合下列规定：

●拉断阀在外力作用下分离后，两端应能自行密闭，防止氢气泄漏；

●加气软管及接头应选用具有抗腐蚀性能的材料。

#### 2.3.2.1 高压加氢过程中的温度监控

高压氢气在储氢瓶快速加注过程中，会产生热量，导致储氢瓶内温度伴随着加氢过程快速升高，给储氢瓶的使用带来安全隐患，因此加氢机必须通过设计合理的加注程序和手段，控制加注过程的温升，确保高压氢气安全的快速加注。

（1）70MPa 加氢机必须具备氢气预冷功能。预冷温度和加注速率可参照 SAE J2601《Fueling Protocols for Light Duty Gaseous Hydrogen Surface Vehicles》标准。如果加氢机具备红外通讯功能，应满足 SAE J2799-2014《Hydrogen Surface Vehicle To Station Communications Hardware And Software》。

（2）35MPa 加氢机可通过预冷、控制加注速率、延长加注时间等措施，确保加注过程储氢瓶内温度不超过 85℃。

#### 2.3.2.2 防超压加注及防超量加注

氢气加氢机应具有充装、计量和控制功能，并应符合下列规定：

（1）加氢机额定工作压力为 35MPa 或 70MPa，分别针对不同的车载氢系统。

（2）设置自动加注程序进行保护，当加注到储氢瓶的设定压力时，自动停止加注。

（3）配置安全阀预防系统超压。

（4）加氢机充装气流量不应大于 3.6kg/min。

（5）加氢机计量宜采用质量流量计计量，最小分度值应为 10g。

### 2.3.2.3 加氢枪与加氢口的通讯协议

在 70MPa 高压氢气运用场景中，加氢枪与安置在车辆上的加氢口之间需有通讯协议，使得站上的管理系统中心可实时监控车辆上储氢瓶压力、温度等安全数据，此通讯协议应符合 SAE J2799-2014《Hydrogen Surface Vehicle To Station Communications Hardware And Software》中的有关规定，通讯界面如图 2-5 所示。

通讯协议应满足以下要求：

（1）车辆上储氢瓶的内部温度、加注压力、储氢瓶参数等信息可通过此通讯回馈至加氢机后回传至站上管理系统；

（2）站上管理系统可根据接受到的压力、温度等信息，调整加注程序；

（3）当车辆上储氢瓶的内部温度、加注压力等信息超出车辆本身的规范，可通过此协议回馈信息，使得加氢机停止加注；

（4）车辆上的储氢瓶加注次数（疲劳充放次数）累积接近设定值时，可通过此协议回馈信息，于车辆显示仪表及管理系统中心显示警告标语；累积至设定值时，可通过此协议回馈信息，管理中心判别不予加氢。

（5）当此通讯协议不能够被加氢机或管理系统辨别，又或者通讯协议讯号中断，则停止加注。

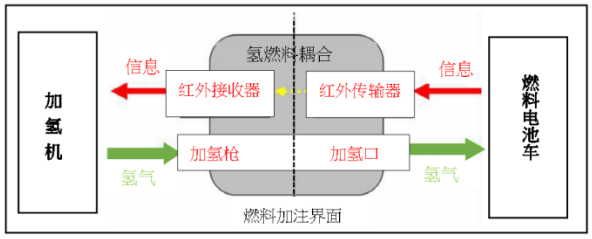



图 2-5　加氢枪与加氢口界面图

### 2.3.2.4 加氢安全机制与控制策略

加氢过程中的氢气计量控制应符合，GB/T 34584-2017《加氢站安全技术规范》与 GB 50516-2010《加氢站技术规范》中的规定。

（1）加氢之前，燃料电池系统、汽车高压电系统必须关闭；汽车必须在加氢站接地（除非汽车制造厂商申明不需采取接地措施）。

（2）所有氢气泄放点，都汇集统一排放。

（3）当有报警发生后，系统自行切断氢气进气。

（4）加氢机应设置安全泄压装置，并具备管路系统吹扫及高压气体泄放功能。

（5）管路端配有压力表及压力传感器，指示各管管路内部压力。高压管路出口配有安全泄压阀，起到泄压保护作用，保护管路压力不超过设定压力值。

## 2.4 氢气安全释放

### 2.4.1 高压氢气释放

加氢站与燃料电池车高压氢气释放应符合 GB 4962-2008《氢气使用安全技术规程》、GB/T 24549-2009《燃料电池电动汽车 安全要求》的规定。

#### 2.4.1.1. 加氢站方面

（1）氢气排放管应采用金属材料，不得使用塑料管或橡皮管。

（2）氢气排放管应设阻火器，阻火器应设在管口处。

（3）氢气排放口应垂直设置，当排放含饱和水蒸气的氢气（产生两相流）时，在排放管内应引入一定量的惰性气体或设置静电消除装置，保证排放安全。

（4）室内排放管的出口应高出屋顶 2m 以上，室外设备的排放管应高于附近有人员作业的最高设备 2m 以上。

（5）排放管应设静电接地，并在避雷保护范围之内。

（6）排放管应有防止空气回流的措施。

（7）若贮存场所设有氢气排空管，室外氢气排空管与避雷针的水平距离不小于 10m，高度上低于避雷装置 5m。

（8）氢气排放速度应不超过 150m/s。

（9）排放管应有防止雨雪侵入、水气凝集、冻结和外来异物堵塞的措施。

#### 2.4.1.2 燃料电池汽车方面

（1）氢气排放系统通向空气排放系统混合后向外界排放。因此排放系统应采用抗冷凝物腐蚀的材料制造，若采用非金属材料则应考虑其温度极限、强度和对冷凝物的耐腐蚀。

（2）燃料电池系统的排气部件应经久耐用。排气管路应具有适当的支撑并配备防雨盖或其他不限制或阻碍气体从排气管道排出。应提供相应措施，如排水装置，以防水、冰和其他杂物在排气管内积聚或阻塞排气管路。排气系统应良好密封，不得有泄漏。

（3）车外释放：在启动、行车、停车等常规操作中，应保证释放、吹扫和其他溢出

等情况下，跟氢气有关的危害不会发生。汽车排气时，不能导致汽车周围氢气浓度超过75%LFL，应在距离排气口 100mm 处气流中心线上进行氢气浓度测量。

（4）车内释放：乘客舱、其他舱中氢气浓度应低于 25%LFL。

（5）当发生故障或意外事故时，燃料系统需要通风放气。气体流动的方位、方向应远离人、电、静电累积源。氢气释放装置应安装在汽车的高处，且应防止排出的氢气对人员造成危害，避免流向汽车乘客舱、行李舱、车轮所在空间，避免流向汽车的电气端子、电气开关器件等部件。

#### 2.4.1.3 所有 PRD 排气一般原则

（1）不应直接排到乘客舱和行李舱。

（2）不应排向车轮所在的空间。

（3）不应排向其他氢气容器。

（4）与 PRD 相连的管道、通道和出口的制造材料使用熔点高于 538℃（1000℉）的金属材料。

# 3 燃料电池堆及系统安全

## 3.1 燃料电池堆安全

### 3.1.1 燃料电池堆设计

#### 3.1.1.1 燃料电池堆分类

目前车用的燃料电池主要是质子交换膜燃料电池堆（PEMFC），质子交换膜燃料电池堆根据极板使用的材料不同，分为金属极板燃料电池堆和石墨极板燃料电池堆等。

#### 3.1.1.2 燃料电池堆功率

燃料电池堆体积比功率决定了后期电堆和系统的组合方式以及电堆的热管理设计。较小体积比功率电池堆有利于热的扩散，对整体电堆和系统热管理设计有益。较大体积比功率电池堆有利于系统设计和制造过程简单化和电池堆体积的减小。

不断提升燃料电池堆体积比功率是长期、系统的工作，建议要在确保安全性、可靠性和关键电性能指标的前提下，提升燃料电池堆的比功率和功率。

#### 3.1.1.3 燃料电池堆关键材料

燃料电池堆使用的材料对工作环境应有耐受性，燃料电池堆的工作环境包括振动、冲击、多变的温湿度、电势以及腐蚀环境；在易发生腐蚀、摩擦的部位应采取必要的防护措施。

（1）质子交换膜

质子交换膜是质子交换膜燃料电池的核心部件，其主要作用是分隔阳极和阴极，阻止燃料和空气直接混合发生化学反应，并传导质子、阻止电子在膜内传导；质子交换膜的质子传导率越高，膜的内阻越小，燃料电池的效率越高。质子交换膜材料要具有足够的化学、电化学、热稳定性和一定的机械稳定性，保证燃料电池在工作过程中能够耐受气流冲击、电流冲击和自由基攻击而不发生降解，保证燃料电池内部不会发生气体窗口窜漏、短路等危险。

对于全氟磺酸膜类质子交换膜，要有较好的热稳定性、化学稳定性和良好的机械稳定性，避免其在高温时发生化学降解，防止燃料电池在高温和高电位时出现化学降解导致气体窜漏引发氢氧混合。气体串漏对燃料电池的安全性有较大影响，要优先选用机械强度高的质子交换膜。质子交换膜厚度和燃料电池安全性密切相关，燃料电池质子交换膜厚度的选择建议充分考虑由于降低隔膜厚度带来的安全风险。

（2）气体扩散层

气体扩散层由支撑层和微孔层两部分组成，其主要作用包括作为燃料气进入催化层之前的缓冲与扩散层；为电子和反应生成的水提供传输通道；作为膜电极的支撑骨架为质子交换膜和催化剂提供物理支撑。

气体扩散层的材料主要有碳纤维纸、碳纤维编织布、无纺布和碳黑纸，其中碳纤维纸由于制造工艺成熟、性能稳定、成本相对较低和适于再加工等优点，成为扩散层的首选。气体扩散层在生产制造时需要避免存在较长的毛刺，避免在与质子交换膜热压的时候刺破质子交换膜，导致气体串漏引发危险。

（3）膜电极

膜电极主要由质子交换膜、气体扩散层和催化层组成。目前存在三代膜电极制备技术：第一代为 GDE、第二代 CCM 及第三代有序化膜电极。膜电极是电化学反应主要发生场所，提高膜电极性能能够有效提高燃料电池单电池的性能。

在膜电极的制备过程中，过度压紧碳纸有可能会刺穿质子交换膜，造成阴极和阳极两侧窜气，产生危险。所以碳纸的热压程度应根据使用质子交换膜的厚度控制在合适的范围内。

伴随着电化学反应的进行，膜电极中质子交换膜逐渐失效，一方面会导致磺酸基团流失，降低质子交换膜的导电性能；另一方面会导致质子交换膜降解，同样会导致阳极侧与阴极侧之间发生窜气，产生危险。

（4）极板

燃料电池极板是燃料电池的核心零部件，其主要作用包括单电池之间的连接；在膜电极表面输送氢气和氧气；收集和传导膜电极产生的电流；排出反应产生的热量和水。目前商业化燃料电池极板材料主要是石墨碳板、复合极板和金属极板三大类。

极板要求高电导率、高导热率和高强度，保证全生命周期燃料电池的安全性。极板表面的金属粉尘、油含量、达因值等关键指标要有效控制。对金属极板的表面处理可以有效改善材料的耐腐蚀性和寿命，减少燃料电池在工作中的酸和水汽腐蚀问题。

（5）端板

燃料电池端板需要一定的强度和良好的绝缘性。

燃料电池端板一般使用金属、环氧树脂、玻璃纤维板和聚酯纤维板，端板上有集流板负责将电流导出电池，端板上有弹簧和弹簧盖板，通过弹簧和弹簧盖板，将燃料电池堆的紧固力控制在一定范围内。端板要经过严格的实验设计和优化验证，并进行强度测试，保证振动冲击条件下的可靠性和安全性。同时燃料电池堆在工作时温度较高，需要保证端板

在较高温度下的稳定性、控制形变。

#### 3.1.1.4 散热设计

燃料电池堆在大功率放电时，电池内部会产生大量的热，导致温度升高，易引起安全问题。燃料电池堆在结构设计时，要模拟分析电池内部发热量分布、热扩散路径和传递速度，验证优化冷却水流量和温度，保证电堆产生的热量能够及时高效的排出电堆，使电堆的温度控制在合理的范围内。

#### 3.1.1.5 密封设计

燃料电池堆的密封主要是极板与膜电极之间的活化区域密封，一般采用硅橡胶、氟硅橡胶、三元乙丙橡胶（EPDM）、聚异戊二丁烯（PIB）、氯丁橡胶和丁睛橡胶等高弹体材料。除此以外还有 MEA 各层间的密封、接头密封、封装外壳的防水防尘等。活化区域密封件主要功能是防止气体、冷却水从极板和膜电极的边缘泄漏出去，造成易燃气体泄漏，因此需要在极板和膜电极上设计密封结构，同时需要设计密封胶线。由于密封胶线在电堆组装应力及较高温度下变形较大，压缩永久形变会变差，在燃料电池运行环境下会缓慢降解，为了在燃料电池堆全生命周期内保证密封的可靠性，需要考虑密封圈的耐温、耐压、耐自由基和 F 攻击等特性。

#### 3.1.1.6 封装设计

燃料电池堆在组装完成后需要进行封装，因为极板和膜电极侧面在未进行封装时是裸露的，当燃料电池堆在向外输出电能时，一旦有导电物体接触极板，就会导致导电物体带电，甚至引起电堆的短路，从而引起人员、设备和电堆的危险。封装材料必须具有较强绝缘性和高可靠性，保证在燃料电池堆在生命周期内不会脱落或失效。

燃料电池堆应有外壳做必要防护，防止其部件与外部高温部件或环境接触。燃料电池堆外壳应避免容易对人体产生危害的结构。

封装外型尺寸应设计与电堆和端板空间匹配，要对各个方向尺寸开展公差分析，同时保证封装材料在装配时不被损坏，从而导致极板或膜电极的裸露。

### 3.1.2 燃料电池堆制造环境要求

燃料电池堆生产过程温度、湿度环境条件必须确定并得到保证。一般不允许出现超出温度、湿度极限值的情况，为此应制定适当的应对方案。燃料电池膜电极（MEA）对水分非常敏感，典型地，在 25℃时，膜电极车间的相对湿度应控制在 40%±5%。

必须控制燃料电池堆生产过程的粉尘度，需要防止外来的颗粒物渗透到任何生产区域。生产系统需要防止金属磨损，如果不能防止金属磨损，应采取适当措施保证这些磨损

产生的颗粒不进入生产过程。应对定期检测到的粒子进行常规分析，以确定粒子的数量、大小和组成，特别是在导电性（如金属粒子)方面。颗粒数量、大小、成分超出规格要求应立即采取纠正措施。粉尘度应控制在 10 万级以下，MEA 制备、金属板涂层部分关键工序的粉尘度应在 1 万级以下。

### 3.1.3 燃料电池堆测试

#### 3.1.3.1 燃料电池堆测试要求

燃料电池堆在出厂前需要进行相关的测试，在保证性能的同时保证安全，同时需要对电池堆的外观进行检测，保证电池堆外观没有明显缺损。

#### 3.1.3.2 燃料电池堆泄漏测试

为确保电池堆的气密性，需要对燃料电池堆进行泄漏测试。将电池堆的氢气、空气和冷却水端口与泄漏测试机的三个端口相连接。打开测漏机开始进行泄漏测试，测试电池堆的外部泄漏量（总外漏、空气腔外漏、氢气腔外漏、冷却腔外漏）和内部窜漏量（空到氢窜漏、氢到空窜漏、空到冷窜漏、氢到冷窜漏)。电池堆中每片单电池外部泄漏量和内部窜漏量分别不得超过相应的规定值，该规定值由测量使用气体的类型、压力以及 MEA 的面积来确定。

#### 3.1.3.3 燃料电池堆绝缘性和耐高压测试

使用高压绝缘测试仪对电池堆进行绝缘性测试。把电池堆放在高压绝缘测试台，短接阴阳极两个集流板的端子。打开万用表，测量端口端子与阴阳极端子之间的电阻，读数应很高（显示 ″OL″)。

对电池堆进行耐高压测试，确保金属杆压住所有的绑带，确保电池堆两端短接，高压绝缘测试仪的红色正极线夹到短接线端，黑色负极线接到金属杆，用安全罩盖住电池堆组件，打开电源开始测试。当计时器结束时，记录绝缘阻值。

#### 3.1.3.4 燃料电池堆性能测试

燃料电池堆在完成泄漏测试、电绝缘测试和耐高压测试后，确保没有泄露、绝缘和耐高压问题才可以进行燃料电池堆性能测试。

将燃料电池堆放置在燃料电池性能评价测试台上，连接好供气管路、冷却水管路、负载线路、巡检线路，待一切线路连接就绪，开始给电池堆进行加热，待电池堆温度到达指定温度后开始给燃料电池堆进行通气和加载，加载电流根据电池堆的设计有所区别，一般加载至额定工作电流，同时检测燃料电池堆电压情况，单节电压最低不能低于 0.3V，避免燃料电池堆中单池电压过低引起反极，将质子交换膜烧穿引起氢空混合，出现安全隐患。

当单节电压低于 0.3V 时，应及时减小电流输出，提升燃料电池单池最低电压，如果减小电流仍单池电压仍然低于 0.3V，应立即停止测试，寻找原因。

### 3.1.4 燃料电池堆安全评价

#### 3.1.4.1 机械冲击评价

燃料电池堆安装固定后，在 3 个轴向：X 向、Y 向、Z 向上以 5.0g 的冲击加速度进行冲击试验。机械冲击脉冲采用半正弦波形、持续时间 15ms，每个方向各进行一次。

燃料电池堆冲击测试之后，机械结构应不发生损坏，气密性满足前述 3.1.4.2 气密性检测要求，绝缘性应满足前述 3.1.4.3 绝缘性要求。

#### 3.1.4.2 振动评价

振动测试模拟车辆长时间在复杂路况行驶（如搓板路、颠簸路、起伏路等）。燃料电池堆长时间振动颠簸后电池堆内部不能出现错位从而发生短路和气体泄漏等安全问题。实验要对燃料电池堆进行 X、Y、Z 三个方向的振动测试，每个方向 21h。要求测试后，电池堆连接可靠、结构完好，最小监控单元电压无锐变，电压差的绝对值不大于 0.15V，无泄漏、外壳破裂、爆炸或着火等现象。燃料电池堆的绝缘性能和气密性性能无明显下降。

振动测试后，燃料电池堆中的零部件无明显位移、扭转和弯曲；零部件的谐振频率与初始值的偏差应小于 10%，各个紧固螺丝的剩余紧固力不低于初始值的 60%；各个电连接点的电阻与初始值的偏差应小于 5%。

#### 3.1.4.3 气密性评价

燃料电池堆处于冷态，关闭燃料电池堆的氢气排气端口、空气排气端口和冷却液出口，同时向氢气流道、空气流道和冷却液流道通入氮气，压力均设定在正常工作压力，压力稳定后关闭进气阀门，测量气体泄漏量，具体指标应满足 3.1.4.2 的要求。

#### 3.1.4.4 电安全

（1）绝缘性能

燃料电池堆在加注冷却液而且冷却液处于冷态循环状态下，正负极的对地绝缘性要求分别不应低于 100Ω /V。

（2）人员触电防护

燃料电池堆人员触电防护要求应符合 GB/T 18384.3-2015 的相关规定。

应防止人员与 B 级电压电路的带电部分直接接触，因此燃料电池带电外层需有遮栏或外壳，防止接近带电部分。

（3）接地保护

当燃料电池堆输出电压高于 60V，燃料电池堆需有接地点，接地点与所有裸露的金属间电阻小于 0.1Ω 。

具体测量方法为，测量前燃料电池堆与其相连的其他供电电源和负载断开，测量时测量仪表端子分别连接至接地端子和燃料电池堆外壳。

#### 3.1.4.5 警示标识

燃料电池堆的警示标识应满足以下规定：

（1）当燃料电池堆的最高电压大于 60V 时，燃料电池堆上应有高压电标识，标识符号采用 GB/T 18384.1-2015 中规定的标记符号；

（2）燃料电池堆要进行极性标识，正极使用红色，负极使用黑色；

（3）其他方面内容标识和说明，应符合 GB/T 20042.2-2008 中第八章的规定。

### 3.1.5 燃料电池堆储运安全

#### 3.1.5.1 包装安全要求（包括铭牌、警示标签和包装）

燃料电池堆的包装应防水、防潮，必要时应该在包装袋中加干燥剂除湿。包装要考虑运输环境条件（公路运输、铁路运输、水路运输等情况）下对燃料电池堆的保护，防止搬移过程中的挤压和损伤，导致安全失效。

燃料电池堆应以最小单元隔离固定，预留安全距离，避免发生电气安全问题。

#### 3.1.5.2 运输与贮存安全要求

燃料电池堆必须牢靠固定在货物运输装置的内部；避免对燃料电池堆日晒、雨淋、受潮；避免燃料电池堆受压，严格按照产品规格书要求摆放。

## 3.2 燃料电池系统安全要求

### 3.2.1 通用安全性

#### 3.2.1.1 外壳防护

燃料电池系统的外壳应具有保护操作人员不受带电、过热（最高表面温度超过 60℃）等存在危险性部件的伤害，在带电或过热的部位应具有警示标识，警示标识应符合 GB 2894-2008 的规定。

燃料电池系统外壳安全防护设计时应考虑外力挤压、跌落、振动、冲击等工况下外壳结构对燃料电池系统的防护，使系统仍能够满足功能要求。外壳防护材料应符合 ROHS 要求，还应满足客户特殊要求，如识别如硫含量等有害化学成分。

（1）燃料电池系统外壳不得具有可能造成人身伤害的尖利边角和粗糙表面，金属外

壳通常应设计良好的接地点，避免尖锐带电体的尖端放电；

（2）燃料电池系统外壳应具有足够的强度、刚度、耐用性、耐腐蚀性及其他物理特性，以在存储、运输、安装及最终使用地区的工作环境条件下，避免出现外壳的局部塌陷、间距缩小、结构松动、零部件移动或其他严重缺陷，防止增大着火和意外事故的危险；

（3）如果燃料电池系统安装于车辆易涉水部位，则燃料电池系统外壳的设计和试验应符合 IP67 防护等级；

（4）由于故障或其他原因，燃料电池系统内的零件可能松动或被甩出，因此外壳应足以容纳这些零件并能防止它们甩出；

（5）在系统全生命周期内，外壳通风口设计应考虑到正常工作情况下不会被尘埃、雪花或植物堵塞；

（6）在系统全生命周期内，根据燃料电池系统的使用寿命要求和使用区域环境要求来确定系统的防腐蚀等级；

（7）如果系统外壳内有保温材料，保温材料在正常情况下除导热率低以外还应具有吸水性低、阻燃性好、电绝缘性能好等特点。

#### 3.2.1.2 控制系统及保护部件

设计和制造燃料电池系统的控制系统时，应满足安全和可靠性分析的要求，确保系统部件的单点故障不会导致危险情况发生，设计的手动装置应明确标识，可防止意外调节、启动与关闭。

燃料电池控制系统一般应具备下述告警信息：负载过载、氢气泄漏、燃料电池故障、辅助储能模块故障、DC/DC 模块故障、供氢压力低、供氢压力高、系统输出电压高、系统输出电压低、短路、过温、环境温度高、环境温度低、空气压力低、空气压力高、冷却水路压力低、冷却水路压力高、通讯故障、系统绝缘低、空压机故障等。系统应能自动发出告警信号，并能通过通信接口将告警信号传送到近端、远程监控设备。

燃料电池系统在以下几种工况下应在控制系统中提供紧急关机和非正常关机功能：

（1）过载保护。当系统输出在额定功率 100%-110%之间，持续 10min 或输出超过额定功率 110%，持续 3s，电压变换单元应自动进入输出限流保护状态，故障消除后，应能自动恢复工作。在上述工况下，燃料电池系统应能发出报警信号；

（2）燃料电池系统入口氢气高、低压保护。当系统检测到供氢压力低于系统规定的最低压力，应发出报警，燃料电池系统故障停机，同时主动关断阀件停止供氢；当系统检测到供氢压力高于系统规定的最高压力时，应发出报警，燃料电池系统故障停机，关断储

氢系统电磁阀停止供氢，同时通过泄压装置，及时释放压力；

（3）输出过电压及欠电压保护。系统输出电压超过过压保护设定值或者低于欠压设定值时，应发出报警信号。当电压超过过压保护设定值时，燃料电池系统应能自动关机保护；

（4）短路或漏电保护。当系统中有电路短路或漏电时，控制系统应能通过显示屏或声光等方式发出报警信号，同时可自动切断燃料电池发电输出线或紧急关机；

（5）氢气泄漏保护。系统应具有氢气泄漏检测功能，并在发生泄漏时能发出报警信号；氢泄漏浓度超过 20000ppm，燃料电池系统自动切断发电输出线或紧急关机；

（6）系统过温保护。当系统冷却水出口温度超过温度限值，应发出报警，燃料电池系统故障停机；

（7）燃料电池故障保护。当燃料电池出现单体电压以及压差超过限定值，燃料电池系统应自动进入输出限流保护状态，故障消除后，应能自动恢复工作；如果故障无法消除，应发出报警，并请求燃料电池系统停机。

为保证燃料电池系统能够正常、安全运行，应安装恰当的保护部件，并满足以下要求：

（1）保护性装置安装位置应满足维护和检测要求；

（2）保护性装置应独立于其他装置可能具有的各种功能；

（3）应提供诸如安全泄放阀等限压装置；

（4）氢气浓度传感器应根据 IEC61779-6 规定进行选择、安装、校对、使用和维护。

### 3.2.1.3 软管及软管组合件

软管及软管组合件至少应符合 GB/T15329.1-2003 中Ⅰ型管的规定。

（1）用于输送水、氢气、空气的软管应耐腐蚀，减少离子析出，使用过程中没有不可接受的物理性质劣化和对介质的化学污染；

（2）内部压力超过 100kPa 的管路系统的设计、安装和测试应符合 GB/T 20801.2-2006 规定；

（3）氢气管路及连接装置应能防止应力腐蚀开裂。管路在燃料电池系统正常、紧急情况、故障运行和停车条件下，都应能在最大允许工作压力和最大允许工作温度下使用。

### 3.2.1.4 金属管路及其连接件要求

金属管路及其连接件应符合 GB/T20972.1-2007 的规定，与氢气相关的金属部件，其抗氢脆性应符合 HB5067-2005 中的规定，防止当进入燃料电池系统的氢气前端减压阀发生故障时，导致系统管路有高压氢气而发生的氢脆。

氢气管路及连接装置应能防止应力腐蚀开裂。高压下承载或输送流体的刚性与柔性管路和配件都应按照 ISO16528-2007 中的要求进行设计、安装和试验。

金属管路系统应能承受最高运行温度和最高运行压力的共同作用，并能与使用、维修和保养时所可能接触的其他材料、化学品相容。金属管路系统应保持完好，并应具有足够的机械强度，满足耐振动性要求。金属成型弯管在弯曲时不应产生影响使用的缺陷。金属管路安装前应彻底清理管路内表面颗粒物，仔细清除管路端口的障碍物和毛刺。

### 3.2.1.5 硫化橡胶和热塑橡胶部件要求

硫化橡胶和热塑橡胶零部件，应符合以下条件：

（1）在制造商规定的产品寿命内，所有材料应能满足运行的最高温度和最高压力的综合要求，并能与正常使用、维护和检修将接触到的其他材料和化学品相容；

（2）外壳体的聚合物零部件和橡胶零部件应防止被机械损伤。聚合物和橡胶管路可根据使用情况必要时加装防护套管或外罩；作为氢气、空气排放系统管路，应采用抗冷凝物腐蚀的材质制作，应鉴定其耐温、强度和抗冷凝物反应的性能；

（3）输送氢气的聚合物或橡胶管件应预防可能的过热，在温度达到比氢气输送管路材料的最低变形温度（HDT）还低 10℃之前，控制系统应能切断氢气的供应；设计时根据安全及可靠性考虑采用适当的泄压装置或方法来保护零部件，防止过压引起损坏；

（4）运输流体（如氢气）的非金属管材会在其内外表面积累静电荷，并且部分电荷可转移至管材两端连接的金属配件上，管材外表面或配件的放电有可能足以点燃环境中的易燃气体。因此用于危险区域内的聚合物或橡胶材料应具有防止静电电荷累积的有效措施，如具有导电性；或通过测试证明，测试电压达到 1000V，末端电阻小于 1MΩ/m，该非金属管材材料可减轻电荷积累现象，可选用该管材；或通过静电累积试验来检测正常和非正常工作条件下，管材材料上不会因为流体流过管材而产生引燃的静电荷。在不满足上述要求的情况下，设计时须将流体气速限定在特定值之内，使静电荷不会在这种非金属材料上产生累积；

（5）硫化橡胶和热塑性橡胶部件应按 GB/T3512-2014 的规定进行热空气加速老化试验和耐热试验（老化时间不低于 96h），试验后性能仍满足发电系统的要求。

### 3.2.1.6 材料和元器件以及结构设计要求

材料和元器件以及结构设计应符合 GB3836.1-2010 中Ⅱ类设备的防爆安全规定。发电系统内部的材料及元器件应满足以下要求：

（1）发电系统使用过程中，内部导线和元器件能够承受最大电流的使用要求，同时

承受发电系统正常运作状态下可能产生的任何温度；

（2）在规定的允许温度下，发电系统内部的导线和元器件的机械强度不会降低，不会因为热膨胀而超过材料允许承受的应力，不会损坏邻近的绝缘部件；

（3）内部导线的选用应符合 GB3836.4-2010 中 5.6 的规定；

（4）内部导线及元器件的连接装置应符合 GB3836.4-2010 中 7.2 的规定，与金属部件接触的内部导线，应有机械保护或加以适当固定以防损坏。

#### 3.2.1.7 接地要求

发电系统内部部件的导体外壳应同电平台连接，确保在氢气泄漏时，不会因静电引燃氢气。

CAN 总线支路距离控制符合规范，屏蔽单点接地，请保证在抗干扰能力最差的地方单点接地，屏蔽线接法避免采用拧股方式。

燃料电池系统内部高压零部件一般接地处理，这一方面是为了改善 EMC，一方面是为了满足安全需要。高压零部件接地需满足以下要求：

（1）所有与高压部件接触的可导电部分必须接地；

（2）系统接地点应有明显标识，接地点用铜螺母；所有接地点应保证导电性，不应有导电性差的漆及氧化物，防止接地不良；系统外壳、所有可触及的金属零部件与接地端子之间的电阻应不大于 0.1Ω；

（3）所有接地点锁紧螺母应保证一定的安装扭矩，接地线应尽可能地短；

（4）高低压线束保持安全间距，屏蔽线需要按要求连接，屏蔽线需要最短。

#### 3.2.1.8 燃料电池系统热安全

燃料电池系统散热元器件主要包含水冷散热器和风冷散热器，上述散热器应具有足够的散热面积，保证系统内部热源与热管理系统之间热传递满足设计需求。燃料电池系统设计时应考虑防止燃料电池电堆、空压机等高电压零部件过温而引发安全事故。

（1）燃料电池系统内部使用的电机应设置温度传感器，并通过电机控制器实现温度检测功能。如果检测到电机温度过高，通过 CAN 通讯向燃料电池系统控制器输出电机温度报警或者电机温度过高信号，控制系统应限制电机功率或停止工作。温度传感器的设置位置及数量应能反应不同工况下最高温度和最低温度要求，同时应考虑温度传感器的精度、适用范围及响应时间；

（2）燃料电池系统应能有效对燃料电池堆进行散热和降温，以确保燃料电池堆工作温度始终在正常使用范围内，以免温度过高影响燃料电池堆的使用寿命；

（3）为保证特定区域使用的燃料电池系统低温启动性能，设计有加热元器件。在燃料电池系统内置加热部件进行热设计时，应具备相应的安全设计（如引入二次热熔保护机制），当加热部件温度过高时，能够切断加热元器件电源；

（4）对于热管理系统中的液冷流路，当系统可能发生泄漏甚至产生安全隐患时，热管理系统设计应考虑具有相应的检测手段，并发出报警信号；

（5）针对燃料电池系统可能存在的着火风险，系统零部件应尽量选用阻燃等级较高或者不燃烧的材料，即使在热失控的极端条件下，系统内零部件至少不会加剧燃烧反应。

### 3.2.2 部件安装及防护

（1）在燃料电池系统设计制造时，应充分考虑其组件、配件的安装稳定性，以便在预定的运行条件下使用不会发生翻倒、坠落或意外移动的风险。

（2）所有燃料系统的部件和连接管线应安装牢固，并配有刚性支撑。如必要时，可使用防震支架，避免因汽车振动而导致损坏、泄漏等故障。

（3）所有燃料电池系统的部件都要采取适当的保护措施，且不应放置在汽车的最外缘，压力释放装置（PRD）、排气管道除外。可能排出或泄漏出氢气的出口应远离可能产生火花或高温的器件。

### 3.2.3 燃料电池系统安全测试

#### 3.2.3.1 气体泄漏测试

燃料电池系统在进行该项测试时泄漏量不得超过规定限值。在进行该试验前，应按照氢系统、空气系统、冷却系统分类，确定不同系统中，进行该项试验的部件应能承受与燃料电池系统正常运行过程中相同的内部压力。氢系统、空气系统、冷却系统应作为独立试验段，分别加压。

应在试验段的入口处连接一个能够为气体介质提供试验压力的、合适的加压系统或稳压系统以及一个能够精确测量泄漏量的流量测量装置，流量测量装置应位于加压系统和试验段之间，应通过合适的方法对试验段出口进行密封。使所有功能部件处于开启位置，在试验段的所有部件上均保持所要求的测试压力。

气体介质应逐渐进入试验段以便试验段在大约 1min 内逐渐达到不低于下表中规定的压力值。该压力应保持至少 1min，或者更长时间，应记录在此时间段内流量测量装置显示的任何泄漏量。

表 3-1　泄漏量试验要求

| 危险 | 试验类型 | 系统设计条件 | 试验参数 | 通过/失败依据 |
| --- | --- | --- | --- | --- |
| 易燃/空气/冷却剂 | 气压 | 所有压力 | 1.1 倍设计压力 | 使用行业认可的检漏液无气泡，不超过泄露率 L |

### 3.2.3.2 气压强度测试

当采用惰性气体或空气进行该项测试时，处于测试中的燃料电池系统部件应不出现破裂、断裂、变性或者其他可见的物理损坏。

在进行该试验前，应按照氢系统、空气系统、冷却系统分类，确定不同系统中，进行该项试验的部件能承受与燃料电池系统正常运转过程中相同的内部压力。氢系统、空气系统、冷却系统应作为独立试验段，分别加压。必要时可通过便捷方法将被测试验段其与燃料电池系统的其他部分隔开。

应在试验段的入口处连接一个能够为气体介质提供试验压力的、合适的加压系统或稳压系统。使所有功能部件处于开启位置，在试验段所有部件上均保持所要求的测试压力。气体介质应被逐渐加注到测试段，在大约 1min 内达到不低于表 3-2 中规定的统一表压。该压力至少保持 1min，或者更长时间，然后应将压力降低至设计压力。应依据下表确定是否通过。

表 3-2　气压强度试验要求

| 危险 | 试验类型 | 系统设计条件 | 试验参数 | 通过/失败依据 |
| --- | --- | --- | --- | --- |
| 易燃 | 气压 | ≥13kPa | 1.3 倍设计压力 | 无破裂、断裂、变性或者其他物理损坏 |
| | | 13kPa＞P＞3.5kPa（电堆为大于 5.5kPa 小于 13kPa | 17kPa | 无破裂、断裂、变性或者其他物理损坏 |
| | | ≤3.5kPa（电堆为 5.5kPa | 5 倍设计压力（电堆为 3 倍） | 无破裂、断裂、变性或者其他物理损坏 |
| 空气 | 气压 | ≥100kPa | 1.3 倍设计压力 | 无破裂、断裂、变性或者其他物理损坏 |
| | | ＜100kPa | 无要求 | 无要求 |
| 冷却液 | 气压 | ≥1.1MPa 或者≥120℃ | 1.3 倍设计压力 | 无破裂、断裂、变性或者其他物理损坏 |
| | | ＜1.1MPa 和＜120℃ | 无要求 | 无要求 |

### 3.2.3.3 燃料饥饿测试

燃料电池系统应以标称功率和正常运行参数运行至稳定状态。为了引发燃料饥饿，将燃料流量减少到代表最坏情况的水平，该最坏情况由燃料电池系统制造商提供的风险评估

确定。电压监测系统或其他安全系统应提供一个信号，用于在达到危险状态之前，将燃料电池系统转换到安全状态。

#### 3.2.3.4 氧气/氧化剂饥饿测试

燃料电池系统应以标称功率和正常运行参数运行至稳定状态。 为了引发氧气/氧化剂饥饿，将氧气/氧化剂流量减少到代表最坏情况的水平，该最坏情况由燃料电池系统制造商提供的风险评估确定。电压监测系统或其他安全系统应提供一个信号，用于在达到危险状态之前，将燃料电池系统转换到安全状态。

#### 3.2.3.5 冷却缺失/受损测试

在制造商规定的最大允许功率输出及制造商规定的稳定条件下运行时，将冷却液流（如果与氧化剂分开的话）立即停止，以模拟冷却系统出现缺失或受损等故障。

燃料电池系统应满足下列其中一种情况：

（1）在冷却液关闭后，燃料电池系统在制造商规定的允许时间内运行；

（2）在达到结构材料的使用温度极限之前，燃料电池系统因性能下降而关闭；

（3）燃料电池系统运行直到安全系统提供信号，使得燃料电池在达到危险状态之前，将燃料电池系统转换到安全状态。

#### 3.2.3.6 冷冻/解冻循环测试

该测试仅适用于存储温度或工作温度低于 0° C 的 PEMFC 燃料电池系统。

在以稳定方式正常运行后，应关闭燃料电池系统，然后将燃料电池系统冷冻在制造商指定的最低环境温度条件下。冷冻后，根据制造商的规格将其融化，直至达到最低 10° C。该冻结/解冻循环重复十次，之后，应重复进行泄漏测试。

#### 3.2.3.7 电气过载测试

燃料电池发电系统应能够承受电气过载。在制造商允许输出电流高于额定电流，且能工作一段时间的情况下，燃料电池系统应先在额定电流下达到热稳定，然后将输出电流增加到制造商允许的数值并在制造商规定的时间内保持不变。该系统不应有起火、震动、破裂、断裂、永久变型或者其他物理损坏的危险。

若制造商不准许较高的电流，则不应进行该测试。

### 3.2.4 燃料电池系统电气安全性

#### 3.2.4.1 电路的电压等级

根据发电系统及其内部电路的工作电压(U)，将电路分为不同等级，具体参考参考《电动汽车安全指南》第一章相关内容。

### 3.2.4.2 标识

（1）电气设备

如燃料电池系统电压接近 B 级电压，则其附近应标示 B 级电压设备的标志（如图 1-1 所示）。参照 GB2893-2008、GB2894-2008 和 GB/T5465.2-2008 的规定。

其他电气设备标识要求参考《电动汽车安全指南》第一章及第二章相关内容。

（2）B 级电压配线的识别

B 级电压电缆和线束外皮应由橙色加以区别，外壳里面或遮拦后面的也建议用橙色加以区别。B 级电压连接器可通过与之连接的线束来区分。

### 3.2.4.3 触电防护要求

通常情况下，燃料电池系统上易触及的导电部件不应存在带电风险。为防止意外接触带电部件，应对燃料电池系统采用合适的结构和防护外壳，防止人员触电，包括：直接接触防护和间接接触防护。具体要求参考《电动汽车安全指南》第一章及第二章相关内容。

### 3.2.4.4 绝缘要求

燃料电池系统的绝缘设计应满足 GB/T18384-2015 或者企业要求。燃料电池系统及其内部电路的绝缘防护措施应符合以下要求：

（1）对于 A 级电压的电路不要求提供绝缘防护；

（2）对于任何 B 级电压电路的带电部件应采取绝缘措施，提供危险接触的防护，绝缘措施包括但不限制于基本绝缘或遮挡/外壳或多种绝缘方式组合，无论采用何种方式都应达到 GB/T18384.3-2015 规定的要求。

（3）依据 GB/T18384.3-2015 规定，在最大工作电压下，直流电路绝缘电阻应至少大于 100Ω /V，交流电路应大于 500Ω /V。如果直流和交流的 B 级电压电路可导电的连接在一起，则应满足绝缘电阻应大于 500Ω /V 的要求。

### 3.2.4.5 电气间隙与爬电距离

燃料电池系统内部的绝缘体应有足够的耐电压能力，进行耐电压试验不应发生绝缘击穿或电弧现象。

（1）燃料电池系统高压电气间隙和爬电距离参考 GB/T16935.1-2008，燃料电池堆阳极和阴极不受这些间隙和爬电的要求；

（2）燃料电池系统设计中，可根据耐压等级、环境污染等级确定电气间隙；

（3）燃料电池系统设计中，可根据环境污染等级、材料 CTI 值，工作电压、工作海拔高度等确定爬电距离；

（4）当主电路与控制电路的额定绝缘电压不一致时，其电气间隙和爬电距离可分别按照其额定值选取。主电路或者控制电路导电部分之间具有不同额定值时，电气间隙与爬电距离应按照最高绝缘电压选取。

### 3.2.4.6 电气连接可靠性

（1）燃料电池系统内部各回路电连接部分应具有有效的设计，建议采用螺纹胶锁死，以保证系统整个生命周期内保持连接阻抗的可靠性；

（2）燃料电池系统内部各回路电连接部分的连接阻抗应具备明确的指标及检测方法，以便在生产、维护时进行检测；

（3）燃料电池系统内线束高低压连接端子与电线应连接牢固；

（4）连接器需要具有一个锁紧装置以避免分离或接触不良，高压连接器还应具有高压互锁功能。

### 3.2.5 燃料电池系统安全监控要求

燃料电池系统的设计和制造应充分考虑正常或非正常使用过程中可能遇到的各种故障和/或事故的安全风险，采取相应的处理措施加以避免。并参照 GB/T 7826-2012 进行相应的风险评估及可靠性分析。

对于无法避免的安全风险，应提供安全提示标识和处理说明，以及声、光等警示及自动和/或手动处理措施。

控制系统的设计应具有监控燃料电池系统各个功能子系统运作状况的功能，并能防止因系统部件的单一故障而升级为危险情况的保护功能。

人工控制装置应有明确标识，且设计样式可防止意外调节与启动。

### 3.2.6 冲击、振动与碰撞

振动是结构件耐久性的考验，区别于传统车，燃料电池系统激励源主要来自汽车行驶过程中路面的不平整造成的，路面的激励频率大部分集中在低频端，燃料电池系统设计中应据此考虑燃料电池系统的整体固有频率。

燃料电池系统应具有一定的抗冲击振动的能力，保证正常使用、运输或储存过程中产生的冲击振动不会对系统各个部件产生损害。

（1）系统设计时应分析碰撞过程中外壳防护箱体及其内部结构（燃料电池堆、高低压线束、辅助系统）产生的最大变形情况，并基于燃料电池堆优先保护的原则来判断冲击、振动与碰撞过程中的安全风险；

（2）外壳防护箱体可根据空间要求，设计加强筋或波形板等加强结构，提高整体结

构强度；

（3）可结合车辆整车布置考虑具有吸能效果的结构设计，设计时应考虑响应材料的塑性要求；

（4）考虑电气连接件的可靠性，避免造成电气部件电线脱落或碰线，避免因振动导致的短路等现象；

（5）提高供氢系统、热管理系统结构强度，增加防护设计，避免冲击、振动与碰撞过程中氢气管路系统损坏和氢气泄漏，避免冷却液泄漏。

### 3.2.7 电磁兼容

燃料电池系统设备应通过合理布置及屏蔽保护设计，在工作/非工作状态下时，耐受车载发射机标准发射功率场强度等级电磁辐射干扰时，不发生功能状态偏离及安全降级。应按照 GB/T33012.3-2016 对不同发射机工作频段进行试验验证。

燃料电池系统应能抗工作环境下电磁干扰，在预设的环境中确保电压、温度等信号采集，通信、电磁阀启闭等功能正常运行，并且在正常运行时，不会产生高于规定水平的电磁干扰。

燃料电池系统的高压线束应具备 EMC 屏蔽措施，其走向布置不应使得 EMC 辐射增强，信号采集控制线束应尽量与高压线束垂直，避免高压线束辐射串扰。高压线束屏蔽层应与高压部件可导电外壳有效连接。

# 4 燃料电池汽车操作、维护及基础设施

## 4.1 用户指南及手册

燃料电池汽车整车制造商应提供用户手册，指明汽车特定的操作、燃料和安全特性。至少包括安全操作程序，包含操作环境，汽车上储存、使用的燃料、冷却剂等物质的注意事项。

### 4.1.1 燃料电池车辆存放

（1）氢燃料电池车辆气罐中如已加注氢气的，必须停放于露天场地，确保场地、通道通风条件良好。燃料电池车辆在满足整车密闭空间测试要求后，可停放于室内场地，室内停车场在最高处布置氢气泄漏探测系统和联动排气系统。

（2）停车场地需确保通风条件良好，车辆之间的通道畅通，不得堆放其他杂物。停车场地应远离加油站、加气站、热源、潮湿、可燃设施/可燃物质堆放区域、有腐蚀性气体以及灰尘较大的地方。同时还应避免其他车辆或移动的物体对车辆造成撞击或挤压，防止意外事件的二次影响。

（3）专用停车场应排水、通风良好，场地极端积水高度不得高于车辆涉水高度。

（4）存放期间车辆加氢口必须盖上帽盖，防止雨水及灰尘的侵入，同时必须确保加氢口舱门处于锁闭状态。

（5）对于日常运营状态下的氢燃料电池车辆，不可避免的需要进入地下停车场或则其他相对环境封闭的通用性室内场所。建议车辆操作人员在进入这些场所之前关闭燃料电池系统，以纯电的模式驶入，待离开以上场所之后再重新打开燃料系统的混动模式。

### 4.1.2 燃料电池汽车运营中的日常安全检查

（1）目测高压氢瓶表面是否有损伤。在管路供氢状态下使用肥皂水或检漏液检查氢系统的气密性，主要包括加注接口、加注口压力表、主电磁阀、减压阀、安全阀、放空阀及各接头等，同时检查连接管路的完好性。

（2）目测氢系统框架是否有裂缝、变形等异常现象。

### 4.1.3 燃料电池车辆加氢安全注意事项

（1）燃料电池车用氢气必须符合国家标准 GB/T 37244-2018《质子交换膜燃料电池汽车用燃料 氢气》要求。

（2）车辆到达加氢车位后应关闭燃料电池系统、拉紧手刹，夜间应关闭车灯。

（3）司机下车打开加氢口舱门，然后至安全区域等待。

（4）由加氢站具备充装资质的专业加氢人员对车辆加氢。

（5）加氢结束后司机应确认加氢枪和静电接地线已拔下，加氢口压力表读数在正常范围内，加氢口防尘罩已归位，并将加氢口舱门锁好。

（6）司机上车后，先查看仪表盘气瓶压力和温度数据是否正常，有无故障报警，确认无故障后启动车辆，驶离加氢站。

#### 4.1.4 燃料电池车辆操作中的其他一般注意事项

（1）燃料电池车辆应严格按照整车产品使用说明书操作。

（2）车内严禁使用明火，车内不放置易燃、易爆物品。

（3）检修操作应在燃料电池系统完全停机并确认高压端无电压后再进行。

（4）加完氢气后，请盖好加氢口的防尘帽，避免进入杂物。

（5）车辆动力系统上电状态不能加氢。

（6）氢气管路安装和检修完成后，应对氢气管路进行吹扫，避免有异物进入燃料电池系统。

## 4.2 燃料电池车辆紧急情况处理

### 4.2.1 氢气意外泄漏处理

#### 4.2.1.1 燃料电池车辆可能发生氢气泄漏的若干预兆

（1）氢气管路松动；

（2）压力表的压力读数持续下降；

（3）氢气泄漏报警；

（4）氢系统低压报警；

（5）管路安全阀泄压；

（6）氢瓶 PRD 泄压；

（7）氢气管路变形；

（8）阀门变形；

（9）氢瓶表面出现损伤；

（10）氢瓶或阀门出现位移或错位。

#### 4.2.1.2 氢气泄漏应急处理措施

当发现氢气泄漏时，应第一时间疏散车内人员，关闭氢阀开关、车辆钥匙，关闭电源翘板开关，打开所有车窗进行通风，设立警戒标识，并通知整车厂售后人员及时到场。

氢气发生大量泄漏或积聚时，首先应当拨打报警电话，并同时采取以下措施：及时切断气源，并迅速撤离泄漏污染区人员至上风处；对污染泄漏区域进行通风，对已泄漏的氢气进行稀释，若不能及时切断气源时，应采用水雾进行稀释，防止氢气积聚形成爆炸性气体混合物；高浓度氢气会使人窒息，应及时将窒息人员移至良好通风处，进行人工呼吸，并迅速就医。

当氢气发生泄漏并着火时应采取以下措施：及时切断气源；若不能立即切断气源，需用大量水强制冷却着火设备；采取措施，防止火灾扩大，如采用大量消防水雾喷射其它引燃物质和相邻设备；氢火焰肉眼不易察觉，消防人员应佩戴自给式呼吸器，穿静电服装进入现场，注意防止外露皮肤烧伤。

#### 4.2.1.3 燃料电池车辆氢气泄露时的其他注意事项

氢系统的应急处置应由经过专门培训的维修人员实施，维修人员应着装防静电服、防静电鞋，并去除身上的静电。

氢气属于易燃易爆的气体，在应急处置现场，维修人员应时刻注意不允许出现火花、高温热源、明火等易引燃氢气的操作，不允许使用电动工具、电焊、非防爆工具等。

严禁私自拆卸、敲击氢气管道和氢瓶，严禁带压操作。

### 4.2.2 车辆意外燃烧处理

燃料电池汽车任何部位起火时，首先将钥匙开关打到 OFF 挡，疏散乘客，根据现场情况拨打报警电话。

消防人员到场后，向消防人员指明氢气瓶、燃料电池系统、动力电池等重大危险源的位置，并介绍气瓶数量及瓶内氢气剩余量等信息。

保证人身安全的情况下，有条件的进行如下操作：

（1）如果车辆线束冒烟起火，救援人员可佩戴简单的个人防护用品（如过滤式消防自救呼吸器、防火手套）对起火点用干粉灭火器、二氧化碳灭火器或水基灭火剂进行喷射，优先使用水基灭火剂进行灭火。

（2）如果动力电池箱起火，及时联系消防部门在距离起火箱＞5 米位置用高压水枪进行喷射；同时，需对氢气瓶进行喷射，避免高温导致瓶口和瓶尾的压力释放装置（PRD）开启，造成氢气大量排出。当发生大量电池起火或电池系统火灾时，应尽快建立至少三支消防水枪阵地，向起火电池箱持续喷射大量的、充足的水。火灾扑灭后，应向燃烧或被火烘烤过的电池系统继续喷水降温，防止复燃。其他与动力电池箱相关安全措施可参考《电动汽车安全指南》第三章。

（3）如果在充电过程中出现火灾，务必第一时间停止充电，再执行下一步灭火动作。

（4）如果人员不慎吸入浓烟，请尽快转移并就医。

（5）条件允许的情况下，由专业人员操作，断开手动维护开关。

## 4.3 燃料电池车辆的检修与维护

### 4.3.1 燃料电池车辆检修注意事项

（1）非氢系统检查维修：如果不涉及动火的，检查维修工作只需要确保周围空气流通性良好。如在室内维修的，确保厂房内部净空高度不低于 8 米。如果涉及动火的，必须将本车内氢气泄放完毕或将氢系统完整拆卸下来后方可动火。

（2）氢系统动火检修前，保证系统内部和动火区域的氢气体积分数在安全范围以内。检修或检验设施应完好可靠，个人防护用品穿戴符合要求。防止明火和其它激发能源进入禁火区域，禁止使用电炉、电钻、火炉、喷灯等一切产生明火、高温的工具与热物体。动火检修应选用铜质工具。

（3）所有动火检测，必须确保明火周围 3 米范围内没有其他无关的氢燃料系统。

### 4.3.2 燃料电池车辆维护安全事项

（1）对氢系统管阀件进行维护作业时，选择通风良好的地点，将管路内的氢气排空再进行零部件的维护。

（2）操作人员在放氢气作业前，应设置警示标示或隔离带，要触摸静电释放器，将身体静电导除。

（3）放气操作人员应经过培训、考试合格后上岗操作。

（4）放气现场安全区域内禁止携带手机、打火机、非防爆对讲机、火柴等火源火种和易产生静电的物品入内。

（5）放气现场安全区域 30 米内禁止使用明火作业。

（6）放气现场严禁穿易产生静电的服装及带铁钉的鞋进入。

（7）放气现场安全区域内使用的工具应为防爆工具。

（8）放气作业区域，仅用于放气作业，其他作业活动严禁在此区域内进行。

（9）放气过程中，应关闭车辆的电源及门窗，同时打开车厢内顶部所有天窗。

（10）放气过程中，除指定的放气操作人员外，其他人员一律不得入内。

（11）车辆放完氢气后，需对车辆四周、舱体和车厢内部进行检测，确保无余气后，方可驶离。

（12）雷雨天气禁止放气作业。

（13）氢燃料电池车辆如需进行动火等整改工作时，需将氢气放空后方可作业。

## 4.4 氢气加注设施的运行与管理

### 4.4.1 加氢设施运行操作与维护

加氢站竣工后，需针对操作人员与设备分别进行培训与定检，并建立安全管理制度、风险管理体系和事故应急预案，维持加氢站设施的稳定性；加氢站运营主体应规范其运行信息的记录，对运行维护、检验、紧急事故及人员资质等数据进行实时记录与定期保存；在加氢站储氢罐和氧气压缩机间的安全距离内，禁止停放车辆、堆放物品和携带火种。

操作人员培训与要求方面：

（1）需进行员工培训，含证照培训、三级教育培训、日常培训等。

（2）配备好护目镜、安全帽、工作服和安全鞋等安全防护装备。

（3）整个操作过程的安全工作由现场负责人监督管理，严格执行带气工作操作流程。

（4）操作人员及现场其他工作人员严禁带火种入场，穿防静电服装进入，不得使用可能会产生静电火花的钢制操作工具等。

（5）工作人员负责现场警戒（现场警戒标志等）巡回检查，严禁杂人入内，进入作业现场的所有人员必须关闭手机，现场严禁明火及产生静电火花。

（6）操作期间采访人员严禁使用闪光灯、新闻灯、与调试无关的人员谢绝入场。

（7）操作人员熟练使用消防器材和消防设施，懂得安全知识。

加氢站定检与维护方面：

（1）消防器材必须严格按照设计要求的数量和规格进行配备并放置到规定地点，定时检查灭火器是否符合使用要求。

（2）建立隐患排查流程（综合性、季节性、节假日、日常、专业性检查）。

（3）建立危险源辨识、风险评价和控制管理，建立应急管理（应急预案、应急演练、演练评估）。

（4）建立事故（事件）调查和报告管理流程。

（5）已投产加氢站现场不得进行火种作业，特殊情况必须动火时，经安全主管部门办理有关手续后，方可进行。

（6）所有操作机械设备部件，必须符合防爆要求。

（7）对所有密封点进行定期检查，投产区域不漏油、不漏水。

（8）应定期对各种阀门进行检查，确保其正常功能。

（9）避免在封闭区域连续排放氮气，以免造成窒息危险。在吹扫过程中采用间断排放。

（10）雷雨、大雨天气停止操作，小雨天气如需进行作业，应对连接接口处及用电设施做好防雨措施。

### 4.4.2 加氢站质量管理体系

建议加氢站需满足 ISO 9001:2015 以及 IATF16949:2016 质量管理体系中的规定。两种标准的搭配运用了过程方法，再加上计划-执行-检查-处理循环(PDCA)和基于风险的思维，如图 4-1 所示，使其质量管理体系与其他管理体系标准的要求保持一致或整合，有利于加氢站运营方吸引顾客、开发新产品和服务、减少浪费或提高生产效率的一系列情形。

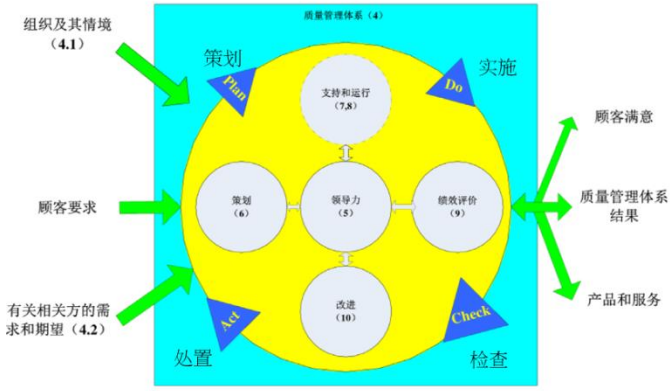



图 4-1　计划-执行-检查-处理循环(PDCA)管理方法运作模式

### 4.4.3 计量收费系统

为了提高个加氢站的运行效率，建议运营商建立中央管理平台，并通过物联网收集各加氢站的数据资料分析，且每个加氢站拥有各自的管理子平台，收集各加氢枪与车辆等信息，获得精确的加氢时间、加氢重量、金额等信息。

### 4.4.4 项目建设

#### 4.4.4.1 加氢站建设

（1）氢气运输方式：加氢站可采用高压氢气长管拖车、氢瓶集装格瓶组运输、管道输送，或自备制氢系统等方式供氢。

（2）加氢站类型：加氢站可与天然气加气站或加油站联合建站，相关规范须符合 GB 50516-2010《加氢站技术规范》、GB/T 34584-2017《加氢站安全技术规范》，上述标准同时也规范了氢能车辆加氢站的氢气输送、站内制氢、氢气存储、压缩、加注以及安全与消

防等方面的安全技术要求。

（3）若为天然气加气站或加油站联合建站，尚需分别达到 GB 50028-2016《城镇燃气设计规范》以及 GB 50156-2012《汽车加油加气站设计与施工规范》的有关规定。

（4）配有自备制氢系统、移动式加氢设施时，需符合 GB 50177-2005《氢气站设计规范》、GB/T 19774-2005《水电解制氢系统的技术要求》及 GB/T 19773-2005《变压吸附提纯氢系统技术要求》的有关规定。

（5）防静电措施：加氢站需特别注意防止静电起火的发生，因此涉及到氢气的系统、控制电路与元件，站内都需要设置静电消除器以及规定有关人员穿防静电服，且相关措施须符合 SY/T354-2017《本安型人体静电消除器安全规范》与 GB 3836.4-2010《爆炸性环境 第 4 部份：由本质安全型“i”保护的设备》的规范。

（6）加氢站等级划分，如下表。

表 4-1 加氢站等级划分

| 等级划分 | 储氢罐容量 | |
|---|---|---|
| | 总容量 kg | 单罐容量 kg |
| 一级 | 4000-8000 | ≤2000 |
| 二级 | 1000-4000 | ≤1000 |
| 三级 | ≤1000 | ≤500 |

#### 4.4.4.2 加氢基础设施设计与安全要求

加氢站基础设施设计与安全要求需注意下列事项：

（1）加氢站及各类加氢合建站的火灾危险类别应为甲类。

（2）加氢站及各类加氢合建站内有爆炸危险房间或区域的爆炸危险等级应为 1 区或 2 区。

（3）加氢站及各类合建站内的建筑物耐火等级不应低于二级。

（4）加氢站、加氢加气合建站、加氢加油合建站的等级划分应符合 GB 50516-2012 的有关规定。

（5）加氢站与充电站合建时，充电工艺设施的设计应遵循 GB 50966-2014 和 GB/T 29781-2013 的有关规定。

（6）采用强制通风时，通风设备的通风能力在工艺设备工作期间应大于 12 次/h，工艺设备非工作期间应大于 5 次/h。通风设备技术规格和设计应符合 GB50058-2014《爆炸

危险环境电力装置设计规范》有关规定。

（7）采用自然通风时，通风口总面积不应小于 300cm²/m²（地面），换气次数不得低于 5 次/h，且应靠近氢气聚集的部位设置。

（8）事故排风换气应使用额外的强制通风装置，并且次数不得少于 15 次/h。

（9）当发生故障或意外事故时，燃料系统需要通风排气，气体流动方向、方位应远离人、电与点火源。

（10）加氢站作业区内不得种植树木、油性植物和易造成氧气聚集、易燃烧的各种植物。

（11）加氢站内不得设置经营性的餐饮、住宿及娱乐设施。严禁设置洗车、修车等作业场所。加氢站的站房可与辅助服务区合建，但站房与辅助服务设施之间应设置无门窗洞口且防水极限不低于 3h 的实体墙。

（12）有爆炸危险区域的等级定义应符合现行国家标准 GB50058-2014《爆炸危险环境电力装置设计规范》的有关规定。

（13）加氢机爆炸危险区域的划分，应符合下列规定：加氢机内部空间为 1 区，以加氢机外轮廓线为界面，4.5m 为半径的地面区域底和以加氢机顶部上为 4.5m 为顶面的圆台形空间 2 区，如图 4-2。

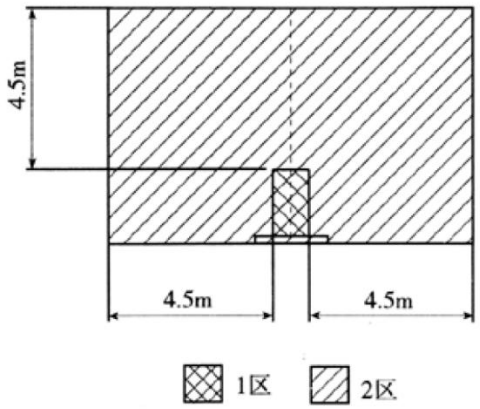



图 4-2　加氢机爆炸危险区域划分

（14）加氢站需要有遮篷，且遮篷为由内而外斜坡向上避免氢气累积；设备本身为 1 区，以设备外轮廓线为界面，4.5m 为半径的地面区域、顶部空间为 2 区。

（15）设备的放空管应集中置。从氢气放空管管口计算，半径为 4.5m 的空间和顶部以上 7.5m 的空间区域为 2 区，如图 4-3。

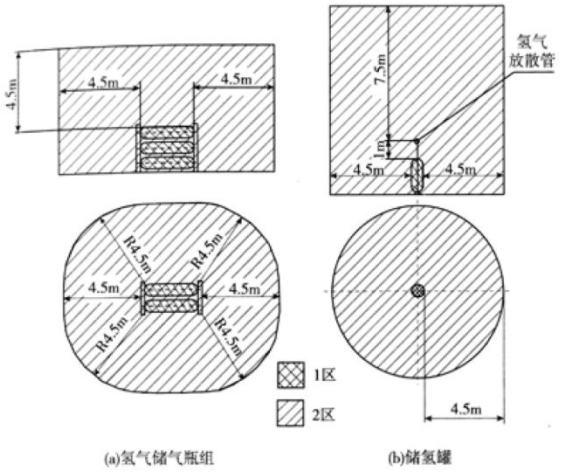



图 4-3 室外或罩棚内的储氢罐或氢气储气瓶组爆炸危险区域划分

加氢站的氢气工艺设施与站外建筑物、构筑物的防火距离，不应小于下表规定。

表 4-1　加氢站的氢气工艺设施与站外建筑物、构筑物的防火距离(m)

| 项目名称 | | 储氢罐 | | | 氢压缩机、加氢机 | 放空管口 |
|---|---|---|---|---|---|---|
| | | 一级 | 二级 | 三级 | | |
| 重要公共建筑 | | 50 | 50 | 50 | 50 | 50 |
| 明火或散发火花地点 | | 40 | 35 | 30 | 20 | 30 |
| 民用建筑物保护类别 | 一类保护物 | 35 | 30 | 25 | 20 | 25 |
| | 二类保护物 | 30 | 25 | 20 | 14 | 25 |
| | 三类保护物 | 30 | 25 | 20 | 12 | 25 |
| 生产厂房、库房耐火等级 | 一、二级 | 25 | 20 | 15 | 12 | 25 |
| | 三级 | 30 | 25 | 20 | 14 | |
| | 四级 | 35 | 30 | 25 | 16 | |
| 甲类物品仓库，甲、乙、丙类液体储罐，可燃材料堆场 | | 35 | 30 | 25 | 18 | 25 |
| 室外变配电站 | | 35 | 30 | 25 | 18 | 30 |
| 铁路 | | 25 | 25 | 25 | 22 | 40 |
| 城市道路 | 快速路、主干路 | 15 | 15 | 15 | 6 | 15 |
| | 次干路、支路 | 10 | 10 | 10 | 5 | 10 |
| 架空通信线 | 国家一、二级 | 不得跨越，且不得小于杆高 1 倍 | | | | |

| | | |
|---|---|---|
| | 一般 | |
| 架空电力线路 | ＞380V | 不得跨越，且不得小于杆高 1.5 倍 |

此外，若含自备制氢系统、移动式加氢设施时，应符合以下要求：

（1）制氢房环境和建筑安全： 建筑物间距应符合 GB 50177-2005《氢气站设计规范》的规定。制氢室结构设计和安装要求应符合 GB50016-2014《建筑设计防火规范》要求，制氢室内安装制氢主机、冷却用水泵和水箱、加电解液用水泵和水箱，非防爆电机水泵等不准安装在制氢室内。

（2）制氢系统供电安全：水电解制氢室的供电装置必须符合 GB50058-2014《爆炸危险环境电力装置设计规范》、GB 50254- 2014《电气装置安装工程施工及验收规范》和 GB 50169-2016《电气装置安装工程接地装置施工及验收规范》的规定，制氢间及氢气储罐区域内应被划分为爆炸性气体环境危险区域 1 区，制氢间门窗边沿以外、氢气罐外壁以外半径 4.5m 的地面、空间，以及氢气排放口周围半径 4.5m 的空间和顶部 7.5m 的区域为 2 区。

（3）制氢系统防雷设施安全：水电解制氢室及设备必须安装防雷装置，为防止水电解制氢设备在生产过程中产生静电必须安装接地地网，保证设备良好接地。接地装置和防雷设施必须符合 GB50169-2016《电气装置安装工程接地装置施工及验收规范》和 GB50057-2010《建筑物防雷设计规范》的规定。

（4）氢气检测及安全响应系统：制氢系统中有火灾和爆炸危险的区域内(制氢间及氢气储罐)需设置可燃气体(氢气)检测报警仪，符合 GB 50493-2009《石油化工可燃气体和有毒气体检测报警设计规范》中的相关要求。

（5）氢气长管拖车停车位与站内建筑物、构筑物的防火距离应按 GB 50516-2010《加氢站技术规范》中氢气储罐的防火距离确定。

#### 4.4.4.3 加氢站验收与安全评价

施工单位按合同规定范围内的工程全部完成后，应及时进行工程竣工验收。工程竣工验收，应由建设单位负责，组织施工、设计、监理等单位共同进行，合格后即应办理竣工验收手续。工程竣工验收时，由施工单位提交的竣工验收文件是工程竣工验收的依据和工程质量“终身制”的依据，必要时应进行抽查检测或试验。施工单位应提交下列文件：

（1）综合部份：竣工技术文件说明，开工报告，工程竣工证书，图纸会审记录、设计变更清单及其相应签证文件，材料和设备质量证明文件及其复验报告。

（2）建筑工程：工程定位测量记录，地基验槽记录，钢筋检验记录，混泥土工程施工记录，混凝土/砂浆试件试验报告，设备基础允许偏差项目检验记录，设备基础沉降记

录，钢结构安装记录，钢结构防火层施工记录，防水工程试水记录，填方土料及填土压实试验记录，合格焊工登记表，隐蔽工程记录，防腐工程施工检查记录。

（3）合格焊工登记表，隐蔽工程记录，设备开箱检查记录，静置设备安装记录，设备清理、检查、吹扫、置换、封存记录，设备安装记录，设备单机运行记录，阀门试压记录，安全阀调整试验记录，管道系统安装检查记录，管道系统试验记录，管道系统吹扫/置换记录，设备、管道系统防静电接地记录，电缆敷设和绝缘检查记录，报警系统安装检查记录，接地体、接地电阻、防雷接地安装测定记录，电气照明安装检查记录，防爆电气设备安装检查记录，仪表调试及其系统试验记录。

（4）竣工图。

（5）观感检查记录表。

### 4.4.5 氢气系统的监控

加氢站应建立中央监控和数据采集系统，且应可连接各加氢站的信息并向客户开放有关数据，结合大数据收集、建立优化管理体系以及客户端软件运用，提升加氢站的效率。数据采集与数据上传至数据分析资料库，针对加氢站的系统监控数据包括：

（1）压力监控，分别检测管道与储氢瓶灌是否超压，以及判断储氢瓶罐的储氢量。

（2）氢气流速监控。

（3）管道与储氢瓶罐的温度监控。

（4）加氢机的加注次数、加氢量与金额的监控与分析。

（5）车辆上储氢瓶的加注次数、加氢量等信息可回馈至加氢站管理中心。

（6）实时传递安全信息，及时反应，降低安全风险。

（7）加氢站及各类加氢合建站进出口、氢气储存区、储气区、氢气加注区、加油加气区、充电区、主控室及总电力配送室应设不间断视频监控，并把监控视频上传数据采集系统，做好数据备份。

（8）加氢站及各类加氢合建站周围宜设置周围报警装置，报警信号应纳入监控系统。

（9）加氢站及各类加氢合建站所有的报警信号及其处理结果都应记入系统数据库中。

（10）加氢站及各类加氢合建站监控与数据采集系统所有的核心单元应设有不间断备用电源，该备用电源可以在断电后 60min 内保持供电。

（11）通过结合客户端软件应用，应可实时提供客户加氢站加氢情况，减少加氢等待时间、自动计算距离加氢站路程及时间，并适时提醒客户。

# 附录一：《电动汽车安全指南》（2019 版）相关规范

1. 电动乘用车动力蓄电池热事件报警要求
2. 电动乘用车安全设计规范

# 附录二：《电动汽车安全指南》（2019 版）编写委员会

**1、指导单位：**

工业和信息化部装备工业司

国家能源局电力司

科技部高新技术司

国家发改委产业协调司

财政部经济建设司

**2、专家指导组：**

组长：董扬 中国汽车工业协会

成员：

王秉刚（科技部 863 计划电动汽车重大科技专项特聘专家）

李　骏（中国工程院院士 清华大学）

欧阳明高（中国科学院院士　清华大学）

孙逢春（中国工程院院士 北京理工大学）

吴　锋（中国工程院院士 北京理工大学）

郑贺悦（工业和信息化部装备中心副主任）

李开国（中国汽车工程研究院）

肖成伟（天津十八所）

王震坡（北京理工大学）

魏学哲（同济大学）

王子冬（中国动力电池产业创新联盟）

王　芳（中国汽车技术研究中心）

许艳华（中国汽车工业协会）

侯福深（中国汽车工程学会）

蔡　蔚（汽车电子驱动控制与系统集成教育部工程研究中心）

邵浙海（普天新能源有限责任公司）

刘永东（中国电力企业联合会）

高步文（中国铁塔公司）

姜延吉（中国铁塔公司）

**3、编制组**

组长：许艳华（中国汽车工业协会）

副组长：王子冬（中国动力电池产业创新联盟）

（1）各章节编写负责人：

康华平（上海汽车集团股份有限公司）

浦金欢（上海汽车集团股份有限公司）

王德平（中国第一汽车集团有限公司））

周安健（重庆长安汽车股份有限公司）

杨子发（北京新能源汽车股份有限公司）

李高鹏（郑州宇通客车股份有限公司）

刘继红（北汽福田欧辉客车）

丁照石（天津力神电池股份有限公司）

孟祥峰（宁德时代新能源科技股份有限公司）

郭晓冬（东软睿驰汽车技术有限公司）

张文宇（北京普莱德新能源电池科技有限公司）

劳　力（华霆动力技术有限公司）

洪木南（重庆长安新能源汽车有限公司）

邓小嘉（上海蔚来汽车有限公司）

邵浙海（普天新能源有限责任公司）

陈晓楠（国网电动汽车服务有限公司）

鞠　强（青岛特来电新能源有限公司）

李德胜（万帮充电设备有限公司）

高　健（中国铁塔公司）

郑　郧（张家港清研再制造产业研究院）

蔡　蔚（汽车电子驱动控制与系统集成教育部工程研究中心）

（2）主要参编单位：

**整车企业**

上海汽车集团股份有限公司

中国第一汽车集团有限公司

重庆长安汽车股份有限公司

东风汽车集团有限公司

北京新能源汽车股份有限公司

广州汽车集团股份有限公司

比亚迪汽车工业有限公司

浙江吉利控股集团有限公司

北汽福田汽车股份有限公司

江淮新能源汽车技术有限公司

安徽江淮汽车集团股份有限公司

上海蔚来汽车有限公司

中国重型汽车集团有限公司

郑州宇通客车股份有限公司

北汽福田汽车股份有限公司欧辉客车公司

厦门金龙联合汽车工业有限公司

金龙联合汽车工业（苏州）有限公司

中通客车控股股份有限公司

威马汽车技术有限公司

重庆长安新能源汽车有限公司

小鹏汽车

上汽大通汽车有限公司

**动力电池企业**

天津力神电池股份有限公司

宁德时代新能源科技股份有限公司

合肥国轩高科动力能源有限公司

国联汽车动力电池研究院有限责任公司

深圳市比亚迪锂电池有限公司

天津捷威动力工业有限公司

微宏动力（湖州）有限公司

中航锂电（洛阳）有限公司

江苏塔菲尔新能源科技股份有限公司

东软睿驰汽车技术有限公司

上海捷能汽车技术有限公司

北京普莱德新能源电池科技有限公司

华霆（合肥）动力技术有限公司

深圳市比克电池有限公司

中航锂电（洛阳）有限公司

**充电设施及运营企业**

普天新能源有限责任公司

国网电动汽车服务有限公司

青岛特来电新能源有限公司

万帮充电设备有限公司

北京新能源汽车股份有限公司

西安特锐德智能充电科技有限公司

中航光电科技股份有限公司

**动力电池回收再利用企业**

中国铁塔股份有限公司

张家港清研再制造产业研究院

张家港清研检测技术有限公司

浙江华友循环科技有限公司

江门朗达集团

东莞市沃泰通新能源有限公司

江苏博强新能源科技股份有限公司

深圳博磊达新能源科技有限公司

**燃料电池系统企业**

上海重塑能源科技有限公司

广东国鸿氢能科技有限公司

云浮（佛山）氢能标准化创新研发中心

**车载储氢及供氢企业**

张家港富瑞氢能装备有限公司

张家港氢云新能源研究院有限公司

**车辆运营企业**

氢车熟路汽车运营（上海）有限公司

**电机系统与电驱动总成企业**

精进电动科技股份有限公司

上海电驱动股份有限公司

科力远混合动力技术有限公司

合肥巨一动力系统有限公司

中车时代电动汽车股份有限公司

华为技术有限公司

浙江方正电机股份有限公司上海分公司

厦门法拉电子股份有限公司

**科研院校、机构**

中国北方车辆研究所

国网电力科学研究院

北京交通大学

同济大学

上海大学

哈尔滨理工大学

中国科学院电工研究所

浙江大学

中国汽车技术研究中心

中国汽车工程研究院

（3）主要参编人员：

张鹏、贾宏涛、吕志伟、林富、陈东、傅洪、宋芳、龙建琦、李遵杰、黄敏、刘爽、孙权、吴刚、张国兴、李博宇、熊金峰、刘宝坤、范志先、邝勇、王洪军、苏亮、刘朝辉、魏长河、魏文博、宋光吉、刘和平、杜卫彬、赵永刚、施红、张峥、崔义、江文峰、高秀玲、方伟峰、王振兴、孙龙、王帅峰、李文斌、金慧芬、姜斌、张硕、赵兴华、苏千叶、田秀君、张友群、杨勇、林志宏、梁建、伊炳希、刘德云、朱肃然、杨振鹏、鲁志佩、朱玉龙、王书洋、蒋光辉、邱志鹏、殷劲松、鲍伟、郑博文、涂蔷、刘喜信、李刚、韩竞科、吕超、王燕、田崔钧、田维、邓迟、茹永刚、周强、方明、吴尚洁、桑林、张萱、刘文珍、

白鸥、张彩萍、顾文武、陈保江、胡进永、周夏荣、商国平、刘木林、曾涛、汪承晔、汪清、王海斌、文彦东、郝斌、谷冬平、代中华、蔡春霞、裴正强、梁亚飞、王健、孙纯哲、孔庆波、张舟云、黄炳健、刘继红、蔡蔚、张清路、徐强、张亮亮、刘传康、凌新亮、周东升、伍理训、燕希强、王铎霖、卜庆元、赵吉诗、陈文凤、麦家铭、马天才、周伟、杨代军、刘冬安、张懿、王学圣、严岩、王美燕、朱龄、朱紫嫣。

（4）总体协调及统稿人

王耀、邹朋、卫友亮、马小利、高雷、刘岩、张帆、李康、秦雪亮

联系单位和联系人：

中国汽车工业协会 邹朋 18610920317

中国汽车动力电池产业创新联盟 马小利 13683507578

中国电动汽车充电基础设施促进联盟 张帆 13810280098