电动乘用车安全设计规范

目录

1.总体要求

1.1 范围

本规范规定了电动乘用车安全设计要求，仅针对电动乘用车特有安全相关部分。包括触电防护安全，操作安全，失效保护，功能安全，电池系统安全，EMC 安全以及热安全等方面设计要求，以保护车内外人员的安全。本规范不适用于指导装配、维修。

1.2 规范性引用文件

GB/T 18384.2-2015 电动汽车安全要求第 2 部分：操作安全和故障防护
GB/T 18384.3-2015 电动汽车安全要求第 3 部分：人员触电防护
GB/T 20234.1-2015 电动汽车传导充电用连接装置第 1 部分：通用要求
GB/T 18487.1-2015 电动汽车传导充电系统第 1 部分：通用要求
GB/T 31498-2015 电动汽车碰撞后安全要求
GB/T 19596-2017 电动汽车术语
GB/T 31467-2015 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
GB/T 34590 道路车辆功能安全

1.3 术语和定义

GB/T 19596-2017 界定的以及下列术语和定义适用于本文件。**A 级电压电路**

最大工作电压小于或等于30Va.c.（rms），或小于或等于60Vd.c.的电力组件或电路。

B 级电压电路

最大工作电压大于 30Va.c.（rms）且小于等于 1000Va.c.（rms），或大于 60Vd.c.且小于或等于 1500Vd.c.的电力组件或电路。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 30 Va.c.（rms）且不大于 60 Vd.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。

可行驶模式：

当踩下加速踏板（或激活某种控制设备）或松开制动系统，车辆的驱动系统就可以移动车辆的模式

ASIL 等级：

汽车安全完整性等级，四个等级中的每一个等级定义了 GB/T 34590 中相关项或要求的必要的要求和安全措施，以避免不合理的残余风险，D 代表最高严格等级，A 代表最低严格等级。

2.触电防护设计规范

2.1 B 级电压标记

2.1.1 B 级电压部件标识

B 级电压部件应具有高压警告标识，标识应满足 GB/T18384.3 第 1 号修改单中 5.1 章节的修改内容。标识应粘贴在装配后醒目或拆卸时清晰可见的位置，如 B 级电压部件体积较大，建议粘贴多个标识用于警示。

图 1 高压警告标记

2.1.2 B 级电压线缆标识

应满足 GB/T18384.3 中 5.2 章节的要求。

2.2 直接接触防护

2.2.1 遮栏或外壳接触防护设计

B 级电压部件的遮栏和外壳应满足 IPXXD 防护等级要求。如果遮栏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，并满足 2.7 章节的高压互锁要求。

2.2.2 高压连接器接触防护设计

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：

——在处于非耦合状态下满足 IPXXB 的防护等级要求。

——高压连接器的分开需要至少两个非连续步骤，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。

——高压连接器被分开后，车辆应在 1s 内将 B 级电压回路电压下降到 30 Va.c.（rms）且 60 Vd.c.或以下，或电路存储总能量小于 0.2J。

2.2.3 高压维修断开装置接触防护设计

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:

——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。

——在高压维修开关被打开或拔出后，车辆应在 1s 内将 B 级电压回路电压下降到 30 Va.c.（rms）且 60 Vd.c.或以下，或电路存储总能量小于 0.2J。

2.2.4 充电插座接触防护设计

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：

——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 30 Va.c.（rms）且 60 Vd.c.或以下，或电路存储总能量小于 0.2J。

——直流充电座应在充电插头被拔下后 1s 内将 B 级电压回路电压下降到 30 Va.c.（rms）且 60 Vd.c.或以下，或电路存储总能量小于 0.2J。

2.3 间接接触防护

2.3.1 绝缘电阻设计

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。在最大工作电压下，整车各直流电路绝缘电阻应至少大于 100 Ω /V，各交流电路应大于 500 Ω /V。如果直流和交流的 B 级电压电路可导电的连接在一起，则应满足混合电路绝缘电阻大于 500 Ω /V 的要求。

充电插座的绝缘电阻应满足 2.3.5 章节要求。

2.3.2 绝缘电阻监测功能设计

车辆应具备绝缘监测功能。绝缘监测功能应在车辆高压上电状态下持续对 B 级电压电路的绝缘电阻进行监测，并在绝缘值低于某个阈值时，予以报警。报警的阈值要大于等于 2.4.1 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。

2.3.3 电位均衡设计

电位均衡应满足 GB/T 18384.3-2015 中 6.9 章节要求，如果采用焊接的形式实现电位均衡，视为满足要求。

2.3.4 电容耦合设计

电容耦合应满足以下两种要求之一：

——B 级电压系统的 Y 电容的总能量应不大于 0.2J；

——如 Y 电容总能量大于 0.2J，B 级电压系统中各 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。

2.3.5 充电插座接地和绝缘电阻设计要求

交流充电插座应满足 GB/T 18384.3-2015 中 6.10.2.1 章节要求。

直流充电插座应满足 GB/T 18384.3-2015 中 6.10.2.1 章节要求。

2.4 密封性设计要求

2.4.1 电池包密封性设计要求

在装配完好的情况下，动力电池防护等级应至少达到 IP67。密封设计应考虑到日后维修可操作性及可恢复性。

2.4.2 车辆充电插座密封性设计要求

充电插座防护等级应满足 GB/T 20234.1-2015 中 6.9 章节要求。

2.4.3 其它高压零部件密封性设计要求

其它 B 级电压部件在装配完好的情况下，针对乘员舱和行李舱外部件防护等级应至少达到 IP67，乘员舱和行李舱内部件应至少达到 IPX4 等级要求。

2.4.4 整车防水设计要求

车辆应在模拟涉水、模拟清洗试验后，进行绝缘电阻测试。模拟涉水及模拟清洗的试验要求应满足 GB/T 18384.3-2015 中 8.2.1 及 8.2.3 中要求。在完成每项试验后，应立即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 2.3.1 章节绝缘电阻要求。

2.5 高压维修断开装置设计

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。

2.5.1 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。

2.5.2 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。

2.6 B 级电压系统电容放电设计

车辆在每次正常下电后或者故障下电后，都应将 B 级电压回路中能量大于 0.2J 的电容的能量释放掉，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高压回路切断后 3s 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 3min 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。

2.7 高压互锁（HVIL）功能设计

车辆上易于拆卸或可以徒手拆卸的遮栏/外壳、高压连接器和高压维修开关应具备高压互锁装置。高压互锁设计应能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其变为不带电部分，且应满足 2.6 章节 B 级电压系统电容放电设计要求。

3.操作安全设计规范

本章从安全防错设计出发，主要包括如下几个方面的操作安全设计：整车上下电、车辆行驶、驻车、充电互锁、电池过充，电子换挡系统等。本章不含远程车辆控制，如遥控泊车等功能的操作安全设计内容。

3.1 整车上下电操作安全

整车上下电操作设计应满足以下要求：

车辆从驱动系统电源切断状态到“可行驶模式”应至少经过两次有意识的不同动作。

从可行驶模式到驱动系统电源切断状态只需要一个动作。

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。如果驱动系统的电源接通/断开程序是通过车钥匙激活的，则应符合相关安全设计的要求。

应连续或间歇的向驾驶员指示，车辆已经处于“可行驶模式”。

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

3.2 车辆行驶操作安全

3.2.1 倒车操作安全

如果是通过改变电机旋转方向来实现前进和倒车两个行驶方向转换的，应满足以下要求，以防止当车辆行驶时意外切换到反向行驶：

——前进和倒车两个行驶方向的转换，应通过驾驶员两个不同的操作动作来完成，或者；

——如果仅通过驾驶员的一个操作动作来完成，应使用一个安全设备使模式转换只有在车辆静止或低速时才能够完成。

如果前进和倒车两个行驶方向的转换不是通过改变电机的旋转方向来实现的，则目前用于内燃机车辆的国家有关规定适用于电动汽车。

3.2.2 低速提示音

车辆低速行驶时，应具备低速提示音功能，且需满足以下要求：

（1）提示音系统的工作车速范围为大于 0km/h 且小于等于 20km/h。

（2）车辆的车外噪音需在其所包含的各个 1/3 倍频程上，其中至少两个 1/3 倍频程上不小于下表中所规定的声级，且同时满足其总声压的要求。

表 1 最低声级限值 dB(A)

频率（Hz）		匀速向前行驶 车速10 km/h	匀速向前行驶 车速20 km/h	倒档行驶
计权声级（总声级）		**52**	**58**	**49**
1/3 倍频程	160	47.0	52.0	
	200	46.0	51.0	
	250	45.0	50.0	
	315	46.0	51.0	
	400	47.0	52.0	
	500	47.0	52.0	
	630	48.0	53.0	
	800	48.0	53.0	
	1000	48.0	53.0	
	1250	48.0	53.0	
	1600	46.0	51.0	
	2000	44.0	49.0	
	2500	41.0	46.0	
	3150	38.0	43.0	
	4000	36.0	41.0	
	5000	33.0	38.0	

3.3 驻车

整车驻车设计应满足以下要求：

当驾驶员离开车辆时，如果驱动系统仍处于“可行驶模式 ”，则应通过一个明显的信号装置（例如：声或光信号）提示驾驶员。

切断电源后车辆即不能产生由自身电驱动系统造成的不期望的行驶。

3.4 整车充放电操作安全

3.4.1 充电操作安全

交流和直流充电时，相关充电接口按照 GB/T 20234.1-2015 和 GB/T 18487.1-2015 的要求。当车辆与外部电路（例如：电网、外部充电器）连接时，不能通过其自身的驱动系统使车辆移动。

3.4.2 放电操作安全

具备放电功能的车辆，应设计过流保护、漏电保护/绝缘检测功能；当发生过流或漏电时，应及时切断放电回路。

舱内放电功能应由用户选择是否开启/关闭。当用户未开启舱内放电功能时，舱内放电插座不能带电；当用户开启舱内放电功能时，应满足下述任一条件：

——舱外充放电插座不能带电；

——舱外充放电插座具备有效的遮档或防护措施；

舱外放电功能应由用户选择是否开启/关闭。当舱外放电线缆未与车辆连接时，舱外放电口不能带电；当舱外放电线缆与车辆连接后，应使车辆处于不可行驶状态；当舱外放电线缆与车辆连接且用户开启舱外放电功能时，舱内放电插座和外接充电插座均不能带电。

4.失效保护设计规范

4.1 碰撞安全设计

车辆应具备碰撞检测装置，持续对车辆的状态进行检测，检测到碰撞时，车辆立即执行碰撞断电流程。碰撞断电流程应包括切断高压电池输出以及高压系统剩余电能的主动放电。检测装置可设计多条硬线或者通讯线路控制断电流程，在一定程度上能避免在碰撞发生时出现单点失效。

碰撞属于严重故障，车辆应能防止再次上电，直到专业维修人员对车辆进行维修后并消除该故障。

4.1.1 防触电保护设计

4.1.1.1 总要求

车辆在进行碰撞试验时，分为两种测试状态：

高压下电状态下进行试验：应满足4.1.2.3 物理防护要求或4.1.2.4 绝缘电阻要求，电池系统和充电子系统应满足下面四项要求（4.1.2.1-4.1.2.4）中的一项；

高压上电状态下进行试验：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（4.1.2.1-4.1.2.4）中的一项。

4.1.1.2 电压要求

应满足GB/T31498-2015 中4.2.2 章节要求，测量方法应满足GB/T31498-2015 中附录A.1 章节要求。

4.1.1.3 电能要求

应满足GB/T31498-2015 中4.2.3 章节要求，测量方法应满足GB/T31498-2015 中附录A.1 或A.2 章节要求。

4.1.1.4 物理防护

应满足GB/T31498-2015 中4.2.3 章节要求，测量方法应满足GB/T31498-2015 中附录A.3 章节要求。

4.1.1.5 绝缘电阻

应满足GB/T31498-2015 中4.2.5 章节要求，测量方法应满足GB/T31498-2015 中附录A.4 章节要求。

4.2 紧急下电设计

整车相关控制器应对各系统故障进行分级处理，应根据发生故障组合对人员安全、行车安全的故障进行分级，结合工况进行相应处理。如发生如：碰撞、热失控、电池系统漏液等故障时建议采取紧急下电措施。

4.3 行驶中异常处置设计

4.3.1 功率降低提示

如果电驱动系统采取了自动限制和减少车辆驱动功率的措施，驱动功率的限制和降低影响到了车辆行驶，该状态应向驾驶员提示。

注：这一措施可以限制驱动系统故障的影响和驾驶员过分的功率要求。

4.3.2 电池系统低电量提示

如果电池系统的低电量影响到车辆的行驶，应通过一个明显的信号装置（例如：声或光信号）向驾驶员提示。当车辆处在制造厂规定的低电量状态时，应至少满足下列要求：

——通过其自身的驱动系统能够使车辆驶出交通区域；

——当没有独立的能量存储装置为辅助电力系统供电时，最小剩余电量应能为照明系统提供满足有关标准规定所需的电量。

4.3.3 电池系统热事件报警

动力电池 BMS 可监控导致热失控的事件，在热失控发生时，通过车载装置提供醒目的警示信息，并伴有声音报警，提醒乘员立即疏散，同时报警信息应通过车载终端上传至企业监控平台。

4.4 应急救援

4.4.1 拖车

车辆应具备一定的配合救援能力，车辆能被低速拖动且车辆的驱动系统不会因此被损坏。

4.4.2 应急救援

车辆必须随车配备救援信息卡，通过阅读，方便救援人员迅速了解车辆结构和潜在威胁，提高救援效率，避免次生事故的发生。

救援信息卡至少应包含以下信息：车身加强部位、电池布局、高压电路、高压维修断开装置、安全气囊及其重要控制单元位置，参考的救援切割位置等信息。

救援信息卡通常为A4纸大小，置于方便取阅的位置；救援信息卡在材料选用时应考虑长期使用的因素。

4.5 继电器粘连

4.5.1 粘连预防策略

避免触点在大电流条件下的带载吸合与断开，直流母线回路应设计预充回路，预充策略应对预充时间和预充压差进行控制，设定阈值应保证继电器吸合电流控制在要求的使用寿命范围内；BMS或相关控制器应设计预充短路保护策略，保护预充继电器及预充电阻。可在BMS硬件上设计监测车辆12V电源电路，若监测到12V电源异常，则应采取相应故障预警。

断开继电器需判断电流大小，当小于设定阈值时允许断开继电器；在大于阈值时，按照超时策略执行。

4.5.2 粘连诊断

动力电池系统应具备继电器粘连故障诊断功能，当诊断出故障时应有故障提示。

4.6 其他失效防护设计

车辆应根据故障的风险等级，对故障进行分类，当故障的风险等级较低且未影响到安全时，可优先选择保护车辆部件或继续维持车辆的主要的行驶、充电功能，仅通过提醒的方式告知驾驶员。

如空调系统常见故障包括：绝缘失效、功率模块烧蚀（短路）、堵转、干烧等，对空调系统故障处理建议根据整车状态进行相关处理，尽量降低对动力系统的影响，不影响车辆行驶功能。

5.电控系统功能安全设计规范

5.1 电动乘用车安全目标

下列 ASIL 目标等级定义指的是最低要求。

5.1.1 驱动系统安全目标

在设计之初，对以下安全目标应有明确的 ASIL 等级定义。

- **安全目标 1： 避免非预期加速**

序号	安全目标	ASIL	安全状态	FTTI
1	避免非预期加速	B	加速度不超过驾驶员预期	FTTI 应根据厂家实车测试或仿真结果给出

- **安全目标 2： 避免非预期减速**

序号	安全目标	ASIL	安全状态	FTTI
1	避免非预期减速	B	减速度不超过驾驶员预期	FTTI 应根据厂家实车测试或仿真结果给出

- **安全目标 3： 避免非预期移动**

序号	安全目标	ASIL	安全状态	FTTI
1	避免非预期移动	B	保持静止状态不输出扭矩	FTTI 应根据厂家实车测试或仿真结果给出

- **安全目标 4 避免非预期反向**

序号	安全目标	ASIL	安全状态	FTTI
1	避免非预期反向	B	保持驾驶员期望的驾驶方向	FTTI 应根据厂家实车测试或仿真结果给出

5.1.2 电池管理系统安全目标

- **安全目标 1：防止电池过充**

序号	安全目标	ASIL	安全状态	FTTI
1	防止电池过充	C	断开高压回路	FTTI 应根据厂家动力蓄电池过充测试结果给出

- **安全目标 2：防止电池过放后再充电**

序号	安全目标	ASIL	安全状态	FTTI
1	防止电池过放后再充电	C	断开高压回路	FTTI 应根据厂家动力蓄电池过放后再充电测试结果给出

- **安全目标 3：防止电池过温**

序号	安全目标	ASIL	安全状态	FTTI
1	防止电池过温	C	断开高压回路	FTTI 应根据厂家动力蓄电池过温测试结果给出

- **安全目标 4：防止电池过流**

序号	安全目标	ASIL	安全状态	FTTI
1	防止电池过流	C	断开高压回路	FTTI 应根据厂家动力蓄电池过流测试结果给出

5.1.3 充电系统安全目标

- **安全目标 1：防止充电口过温**

序号	安全目标	ASIL	安全状态	FTTI
1	防止充电口过温	B	停止充电	FTTI 应根据厂家充电口过温测试结果给出

- **安全目标 2：防止快充未关闭导致拉弧**

序号	安全目标	ASIL	安全状态	FTTI

1	防止快充未关闭导致拉弧	B	充电停止，电子锁解锁	无

5.1.4 高压系统安全目标

- **安全目标 1： 防止触电**

序号	安全目标	ASIL	安全状态	FTTI
1	防止触电	C	断开高压回路，释放高压回路能量	各企业自行定义。

5.2 驱动系统功能安全设计要求

5.2.1 避免非预期加速安全要求

5.2.1.1 非预期加速监控要求

驱动系统应设计探测机制，能探测到导致车辆非预期加速的失效。

5.2.1.2 非预期加速安全状态要求

驱动系统探测到导致车辆非预期加速的失效后，应在故障容错时间间隔（FTTI）内进入安全状态；不满足故障消除条件时，不应退出安全状态。

注 1：避免非预期加速的安全状态见 5.1.1

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据主机厂非预期加速测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.2.1.3 报警和降级概念

驱动系统探测到导致车辆非预期加速的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应采用报警和降级概念，通过紧急运行来达到安全状态。

5.2.1.4 紧急运行

驱动系统探测到导致车辆非预期加速的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）限制输出扭矩。

5.2.2 避免非预期减速安全要求

5.2.2.1 非预期减速监控要求

驱动系统应设计探测机制，能探测到导致车辆非预期减速的失效。

5.2.2.2 非预期减速安全状态要求

驱动系统探测到导致车辆非预期减速的失效后，应在故障容错时间间隔（FTTI）内进入安全状态；不满足故障消除条件时，不应退出安全状态。

注 1：避免非预期减速的安全状态见 5.1.1

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据主机厂非预期减速测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.2.2.3 报警和降级概念

驱动系统探测到导致车辆非预期减速的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应采用报警和降级概念，通过紧急运行来达到安全状态。

5.2.2.4 紧急运行

驱动系统探测到导致车辆非预期加速的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）限制输出扭矩。

5.2.3 避免非预期移动安全要求

5.2.3.1 非预期移动监控要求

驱动系统应设计探测机制，能探测到导致车辆非预期输出扭矩的失效。

5.2.3.2 非预期移动安全状态要求

驱动系统探测到导致车辆非预期输出扭矩的失效后，应在故障容错时间间隔（FTTI）内进入安全状态；不满足故障消除条件时，不应退出安全状态。

注 1：避免非预期移动的安全状态见 5.1.1

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据主机厂非预期移动测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.2.3.3 报警和降级概念

驱动系统探测到导致车辆非预期输出扭矩的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应采用报警和降级概念，通过紧急运行来达到安全状态。

5.2.3.4 紧急运行

驱动系统探测到导致车辆非预期输出扭矩的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户。

5.2.4 避免非预期反向安全要求

5.2.4.1 非预期反向监控要求

驱动系统应设计探测机制，能探测到导致车辆非预期输出反向扭矩的失效。

5.2.4.2 非预期反向安全状态要求

驱动系统探测到导致车辆非预期输出反向扭矩的失效后，应在故障容错时间间隔（FTTI）内进入安全状态；不满足故障消除条件时，不应退出安全状态。

注 1：避免非预期反向的安全状态见 5.1.1

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据主机厂非预期反向测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.2.4.3 报警和降级概念

驱动系统探测到导致车辆非预期输出反向扭矩的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应采用报警和降级概念，通过紧急运行来达到安全状态。

5.2.4.4 紧急运行

驱动系统探测到导致车辆非预期输出反向扭矩的失效，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）限制输出扭矩。

5.3 电池管理系统功能安全要求

5.3.1 防止过充安全要求

5.3.1.1 电芯电压过压监控要求

电池管理系统应实时监测动力蓄电池单体电压，并诊断动力蓄电池最高单体电压值是否超过安全阈值。

注 1：安全阈值应根据厂家动力蓄电池过充测试结果给出。

5.3.1.2 过充安全状态要求

电池管理系统确认动力蓄电池最高单体电压值超过安全阈值时，应在故障容错时间间隔（FTTI）内进入安全状态（见附录 A）；不满足电池单体过充故障消除条件时，不应退出安全状态。

注 1：防止电池过充的安全状态见 5.1.2.1

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据厂家动力蓄电池过充测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.3.1.3 报警和降级概念

电池管理系统确认动力蓄电池最高单体电压值超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态（见附录 A），应采用报警和降级概念，通过紧急运行来达到安全状态。

5.3.1.4 紧急运行

电池管理系统确认动力蓄电池最高单体电压值超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）基于动力蓄电池状态和高压回路设计状态，可选择限制充电功率到安全阈值、或禁止充电功能、或切断充电回路。

5.3.2 防止过放后再充电的安全要求

5.3.2.1 电芯电压欠压监控要求

电池管理系统应实时监测动力蓄电池单体电压，并诊断动力蓄电池最低单体电压值是否低于安全阈值。

注 1：安全阈值应根据厂家动力蓄电池过放测试结果给出。

5.3.2.2 过放后再充电安全状态要求

电池管理系统确认动力蓄电池最低单体电压值低于安全阈值时，应在故障容错时间间隔（FTTI）内进入安全状态（见附录 A）；不满足电池单体过放故障消除条件时，不应退出安全状态。

注 1：防止电池过放后再充电的安全状态见 5.1.2.2。

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据厂家动力蓄电池过放测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.3.2.3 报警和降级概念

电池管理系统确认动力蓄电池最低单体电压值低于安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态（见附录 A），应采用报警和降级概念，通过紧急运行来达到安全状态。

5.3.2.4 紧急运行

电池管理系统确认动力蓄电池最低单体电压值低于安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）基于动力蓄电池状态和高压回路设计状态，可选择限制充放电功率到安全阈值或切断充放电回路。

5.3.3 防止过温的安全要求

5.3.3.1 电芯温度监控要求

电池管理系统应实时监测动力蓄电池单体或模组温度，并诊断动力蓄电池单体或模组温度值是否超过安全阈值，温度传感器的布置应能探测单体或模组的最高温度。

注 1：安全阈值应根据厂家动力蓄电池过温测试结果给出。

5.3.3.2 过温安全状态要求

电池管理系统确认动力蓄电池单体或模块温度超过安全阈值时，应在故障容错时间间隔（FTTI）内进入安全状态（见附录 A）；不满足电池单体过温故障消除条件时，不应退出安全状态。

注 1：防止电池过充的安全状态见 5.1.2.3

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据厂家动力蓄电池过温测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.3.3.3 报警和降级概念

电池管理系统确认动力蓄电池单体或模块温度超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态（见附录 A），应采用报警和降级概念，通过紧急运行来达到安全状态。

5.3.3.4 紧急运行

电池管理系统确认动力蓄电池单体或模块温度超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态（见附录 A），应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）基于动力蓄电池状态和高压回路设计状态，可选择限制充放电功率到安全阈值、或切断充放电回路。

5.3.4 防止过流的安全要求

5.3.4.1 电流监控要求

电池管理系统应实时监测动力蓄电池电流，并诊断动力蓄电池电流值是否超过安全阈值。

注 1：安全阈值应根据厂家动力蓄电池过流测试结果给出。

5.3.4.2 过流安全状态要求

电池管理系统确认动力蓄电池电流超过安全阈值时，应在故障容错时间间隔（FTTI）内进入安全状态（见附录 A）；不满足电池单体过流故障消除条件时，不应退出安全状态。

注 1：防止电池过充的安全状态见 5.1.2.4

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据厂家动力蓄电池过流测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.3.4.3 报警和降级概念

电池管理系统确认动力蓄电池电流超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态（见附录 A），应采用报警和降级概念，通过紧急运行来达到安全状态。

5.3.4.4 紧急运行

电池管理系统确认动力蓄电池电流超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）基于动力蓄电池状态和高压回路设计状态，可选择限制充放电功率到安全阈值、或切断充放电回路。

5.4 充电系统功能安全要求

5.4.1 防止充电口过温安全要求

5.4.1.1 充电口温度监控要求

充电系统应实时对充电口温度进行监控，并诊断充电口温度值是否超过安全阈值。

注 1：安全阈值应根据厂家充电口过温测试结果给出。

5.4.1.2 充电过温安全状态要求

充电系统确认充电口温度超过安全阈值时，应在故障容错时间间隔（FTTI）内进入安全状态（见附录 A）；不满足充电口过温故障消除条件时，不应退出安全状态。

注 1：防止电池过充的安全状态见 5.1.3.1。

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障容错时间间隔（FTTI）应根据厂家充电口过温测试结果给出。

注 4：故障消除条件由厂家自行确定。

5.4.1.3 报警和降级概念

充电系统确认充电口温度超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态（见附录 A），应采用报警和降级概念，通过紧急运行来达到安全状态。

5.4.1.4 紧急运行

充电系统确认充电口温度超过安全阈值，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户；

（2）基于动力蓄电池状态和高压回路设计状态，可选择限制充电功率到安全阈值、或切断充电回路。

5.4.2 防止快充未关闭导致拉弧的安全要求

5.4.2.1 快充状态监控要求

充电系统应实时监控直流快速充电状态。

5.4.2.2 快充未关闭安全状态要求

充电系统应在快充口设计锁止机构，若监控到快充状态处于正在充电时，则不允许解锁，快充枪无法拔出；只有监控到快充状态不处于正在充电时，才允许解锁，快充枪才允许拔出。

5.5 高压系统功能安全要求

5.5.1 防止触电的安全要求。

5.5.1.1 防触电监控要求

若高压器件直接暴露在用户可直接接触的范围（如：高压防护取消，或高压接插件未正常连接），高压系统应能通过高压互锁装置实时检测到异常状态。

高压系统应设计绝缘监测机制，能对高压系统的绝缘状态进行实时监测。

5.5.1.2 防触电监控安全状态要求

高压系统通过高压互锁装置检测到高压器件直接暴露在用户可直接接触的范围时，应在故障容错时间间隔（FTTI）内进入安全状态（见附录 A）；不满足消除条件时，不应退出安全状态。

高压系统通过绝缘监测机制检测到绝缘阻值过低时，应在故障容错时间间隔（FTTI）内进入安全状态；不满足消除条件时，不应退出安全状态

注 1：防止触电的安全状态见 5.1.4.1。

注 2：故障检测、故障判断、故障处理应在 FTTI 时间内完成。

注 3：故障消除条件由厂家自行确定。

5.5.1.3 报警和降级概念

高压系统确认高压器件直接暴露在用户可直接接触的范围、或监测到绝缘阻值过低，且判断无法在故障容错时间间隔（FTTI）内进入安全状态（见附录 A），应采用报警和降级概念，通过紧急运行来达到安全状态。

5.5.1.4 紧急运行

高压系统确认高压器件直接暴露在用户可直接接触的范围、或监测到绝缘阻值过低，且判断无法在故障容错时间间隔（FTTI）内进入安全状态，应按下述定义执行紧急运行：

（1）发送报警信息警示用户。

5.6 部件安全设计要求

5.6.1 关键传感器信号监控要求

- 应采用安全机制/措施保证关键传感器信号失效模式诊断覆盖率符合相应 ASIL 等级要求；
- 当探测到信号失效后，应在规定时间内采取故障动作，避免出现违反安全目标的行为。

示例：安全机制/措施可包含但不限于：通过在线监控进行失效探测；测试模式；输入比对/表决；传感器有效范围；传感器相关性；传感器合理性检查。

5.6.2 微处理器监控要求

- 应采用安全机制/措施保证微处理器各要素的失效模式诊断覆盖率符合相应 ASIL 等级要求；
- 当探测到微处理器要素失效后，应在规定时间内采取故障动作，避免出现违反安全目标的行为。

示例：微处理器的要素包括：电源；时钟；非易失性存储器；易失型存储器；数字输入/输出；模拟输入/输出；处理单元（算数和逻辑单元、寄存器、地址运算、中断处理、控制逻辑、寄存器配置）；通信等。

5.6.3 执行器监控要求

- 应采用安全机制/措施保证执行器失效模式诊断覆盖率符合相应 ASIL 等级要求；

- 当探测到执行器失效后，应在规定时间内采取故障动作，避免出现违反安全目标的行为。

示例：安全机制/措施可包含但不限于：通过在线监控进行失效探测；测试模式；一致性控制。

6.电池系统安全设计规范

6.1 机械防护

电池包中所有结构件均应能满足国标要求的机械安全性能：振动、挤压、机械冲击、模拟碰撞、跌落、翻转等，要求托盘、关键连接结构，包含机械连接结构和电连接结构，必须有足够的机械强度，可以发生塑性变形，但不能破损。

6.1.1 电池结构部件安全设计要求

6.1.1.1 电池包上盖安全设计

电池上盖是电池结构中十分重要的一部分，起到密封、顶部防护，泄压、提高整包扭转刚度等作用。在进行 Pack 上盖安全设计时，需注意考虑以下几点：

- 电池上盖应具备足够的模态刚度，至少应大于路面激励频率。在模态无法达标的情况下，应增加抗振缓冲物，以缓解电池上盖的机械振动。
- 电池上盖在自然下垂条件下的变形不应过大，建议小于 0.5mm/g。
- 对于有泄压装置的电池包上盖，上盖的抗拉破坏强度应大于泄压装置的开启阀值。

6.1.1.2 电池包底部防护安全设计

- 电池包防撞击结构设计

对于安装在车辆底盘下方的电池包，其高压接口位置附近需要有防撞击横梁，能够防止障碍物直接撞击电池包高压接口，在物理结构上起到碰撞防护效果。

- 电池包底部护板结构设计

电池包底部应设计有护板防护，减少石击和汽车搁底时对电池包造成的损伤。

石击是指道路上飞溅的碎石击打壳体的表面，对壳体造成损伤。

汽车搁底是指汽车行驶中因路面不平或颠簸导致地面突起的部分与车底零部件剐蹭。

电池底部破坏工况可以分为两大类，一类是高速穿刺工况，一类是低速挤压刮蹭工况。在电池底部安全防护的设计过程中，应根据不同工况的特点，明确电池底部防护应达到的等级，再进行具体的防护策略选择。

防护工况	高速穿刺；低速挤压等
防护等级	正常使用；不起火爆炸等
防护策略	结合整车结构防护；电池底部单独防护等

6.1.2 电池系统结构设计特性规范

电池包结构强度设计要求

乘用车动力电池包一般安装于整车底部，振动是电池包面临的最常见机械工况，在设计开发中应重点考虑，同时结合乘用车使用场景，扭转，弯曲疲劳也应该纳入开发考虑。
电池包的模态应高于整车模态。

电池包按照 GB/T31467.3-2015 试验后，能够保持连接可靠，结构完好，电池系统无泄漏，外壳破坏，能够通过 IP67 测试，无起火爆炸等现象。

电池包滥用侵入安全设计

电池 Pack 应能配合整车通过主流的碰撞测试标准，如 C-NCAP、E-NCAP、IIHS 等标准，达到良好星级。在碰撞后，电池系统应满足相应的电安全要求。

6.2 电池危害与控制预防设计

本节将主要阐述电池失效后潜在的危害及相应的安全设计需求。以下内容陈述了多种失效模式，并对每个失效模式充分枚举了潜在的直接原因，同时针对各原因提出了控制预防措施的建议。不过电池包系统的安全设计并不是各种安全因素的简单堆砌，还需要设计者根据实际情况做出最合适的系统匹配，使安全性能满足设计要求。

6.2.1 起火/爆炸

可燃气体防护

针对电解液分解会产生可燃气体，电解液中应增加阻燃剂。

电池包应设计有泄压阀，保持电池包内部压力平衡，避免产生爆炸。

过充

按照电池安全测试标准进行过充测试，不起火，不爆炸。

6.2.1.1 外短路

按照外短路测试标准，不起火不爆炸。

6.2.1.2 电芯内短路

内短路是指电池隔膜失效时，内部正负极活性材料相互接触，因电化学电势差产生的放电并伴随产热的现象。

内短路主要可分为三类：

（1） 机械滥用，如针刺、挤压引发的隔膜破裂而造成的内部短路。

（2） 电滥用，如过充、过放、低温充电等导致的电池内部锂晶枝生长，并导致隔膜刺穿而导致的内短路。

（3） 热滥用，电池温度过高， 隔膜收缩崩溃导致内短路。

在电池包结构设计时应该充分考虑挤压、搁底对电池包的影响，同时建议充分利用车身对电池包进行保护。

电芯满足过充和过放测试的要求，BMS 需要包含过充保护、过放保护功能，电芯温度低时，建议先将电池温度加热至适合的充电温度，再进行充电。

动力电池系统应充分的考虑电池热管理系统的设计，根据整车工况和需求选择合适电池冷却的方案，并配合 BMS 控制策略，将电芯温度控制在合适的温度。

6.2.2 热蔓延

模组设计应考虑隔热防火措施，延缓电池模块中热蔓延的时间，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。

电池系统与乘员舱之间需要考虑隔热防火设计，延缓火焰蔓延到乘员舱的时间，为乘员逃生争取时间

单个电芯发生热失控时，BMS 应能提供报警信号，从报警信号发出至电池包可见明火，时间不小于 15min。

6.2.3 漏液

电池系统设计时应考虑漏液保护，如果出现漏液，整车需通过声音提醒或仪表（光闪烁）提醒用户，显示相关信息。

如果行驶时，通过限制功率至将车速降低至安全值后进行断电，降功率值和时间可根据整车性质进行调整确认。

如果上电时，不允许上高压（ready）；

如果充电时，禁止充电；

6.2.4 被动预防措施

电连接部分要保证连接的可靠性和耐腐蚀性，避免连接不可靠或被腐蚀后电阻增加而导致发热。

6.2.5 过温

确保电池系统热管理的设计可满足恶劣工况下的安全需求，包含最恶劣环境和使用工况下的虚拟仿真与试验验证。设计预防措施主要有：

1. 电池超温后实施主动限功率，避免系统超温后持续大负荷工作并生热。
2. 主动冷却系统，将电池温度控制在适宜的温度区间。

当电池周边布置有高温零件，需在电池与高温零件之间设计合适隔热件。

6.3 电子防护

BMS 应能按照国标要求采集并上传电池信息以及报警信息。

BMS 应至少具备下表功能：

功能	要求
1、动力电池电压监测，异常状态报警和保护功能	电压监测：通过采集器获得各电池的电压信息，再通过计算得到动力电池的总电压；当监测电压值处于异常状态时，发出动力电池电压异常警报，并采取相应保护措施。
2、动力电池充、放电电流监测功能，异常状态报警和保护功能	电流监测：可以监测动力电池的充放电电流；当监测电流值处于异常状态时，发出动力电池电流异常警报，并采取相应保护措施。
3、动力电池温度监测，异常状态报警和保护功能	温度监测：通过采集器获得各电池和电池包的温度信息；当监测温度值处于异常状态时，发出动力电池温异常警报，并采取相应保护措施；检测电池进出液口温度。
4、充放电管理功能	电池管理系统可以根据整车功能需求及动力电池实时状态对动力电池进行充放电管理。
5、上电管理功能	上电管理功能：可以通过整车状态和动力电池状态，进行上电管理。
6、继电器供电和控制功能	继电器供电和控制功能：根据各功能需求，给继电器供电，并控制分压继电器、正极继电器、负极继电器、预充继电器的通断。
7、热管理控制	热管理控制：根据采集器子网监控动力电池温度及监测水冷管进水口温度，控制电池热管理系统对电池进行加热或冷却。
8、碰撞断电处理	碰撞断电处理功能：根据接收到的硬线碰撞信号或 CAN 信号，判断是否需要立即断开正极继电器和负极继电器，并记录相应的故障码。
9、发送绝缘报警，记录绝缘故障码，并触发绝缘保护处理功能	实时监测绝缘状态发送绝缘状态信息，记录绝缘故障码： 绝缘保护处理功能：在监测到绝缘故障后，对充放电采取一定的限功率或其他保护措施。
10、充电口温度监测	监控充电口温度，并及时上传温度数据，车载充电系统接收到此报文后进行判断是否需要执行限功率或禁止充电等相关操作。
11、继电器粘连故障检测功能	粘连故障检测功能：通过整车下电过程中电机控制器的母线电压或辅助触点状态来判断各个继电器是否粘连，并发送粘连状态给仪表报警的功能。

12、下电管理功能	下电管理功能：在不同整车电源模式下，综合判断车速和整车发送的下电信号，确定是否需要断开主继电器，断开整车高压供电。

7.EMC 安全设计规范

7.1 整车电气、电子部件布局设计要求

各电气电子部件在整车上的布置位置、方向等，要遵循其走线顺畅、走线的距离最短、走线形成的环路面积最小的原则，以降低线缆作为等效天线向外辐射电磁波的效率，且降低耦合外界干扰信号而影响其本身正常工作。

整车上的强干扰源（如电源、电控、OBC 等高压零部件）与敏感设备（如车载天线、接收机、功放、VCU、中控屏、雷达等）在整车上布置时需保证其在空间上隔离开，推荐空间直线距离 10cm 以上，避免敏感设备被干扰而影响正常工作，部分敏感设备可以通过调整其布置方向来减小与强干扰设备之间的空间耦合，亦可以借助整车结构的优势（金属格挡、凹槽等）进行布置，同样可以减小被干扰几率。

7.2 整车布线设计要求

高压线束是否使用屏蔽线缆设计可根据整车和零部件实际情况决定。如若整车高压线束（高压直流母线、电机三相线、充电电源线等）使用屏蔽线，推荐使用屏蔽编织密度不低于85%的单层屏蔽线或者双层屏蔽线（编织网+编织网或者编织网+铝箔）。线缆屏蔽层在与接插件或者车身、零部件机壳搭接时建议 360° 全搭接。

低压控制线、信号线、通信线等可根据整车和零部件实际情况确认是否使用屏蔽线、双绞线、同轴线等。对于整车 CAN 通信线，电机旋变线，信号采样线等敏感信号线如若使用屏蔽线，建议使用双绞单层或者双层屏蔽线，以增加线束的抗干扰能力；对于音视频信号线，建议使用同轴线在保证信号质量的前提下提高其抗干扰能力；对于部分强干扰低压线束，也可使用屏蔽双绞线以降低线束本身的噪声发射水平。

高压线束与低压线束应分层设计走线，以降低高低压之间的耦合干扰，高压线束与低压线束尽可能不要平行走线，应垂直交叉走线，若不可避免平行走线时，要保证平行走线尽可能短，且间隔>20cm 或中间加金属隔离结构，以降低高低压之间的耦合干扰。另外，高压线束和低压线束的走线路径应尽可能短、环路面积最小，以减小线束对外的辐射发射及耦合到外部干扰；低压线束集中走线时，应把低压敏感信号线与强干扰源的低压线分开走线，避免相互之间的耦合干扰。

7.3 车载电气部件壳体接地设计要求

为了保证干扰噪声环路可控，电气设备的壳体都推荐进行专门的搭铁接地设计，从而保证零部件壳体和车身等电势，保证部件上的干扰信号具有低阻抗的泄放路径，降低对外的电磁辐射发射。推荐整车必要进行接地的部件有：电机驱动器，电机本体，高压电池包，车载电源，发动机，空调压缩机等其它包含电机的部件。

壳体接地设计需要考虑的几个方面：接地线，接地位置（电气部件本体和车身端），紧固螺钉，车身搭接面处理。接地线，在满足高压安全要求的前提下，可使用铜编织带或者线缆形式实现，线缆长度推荐不超过 20cm；接地线本身需要保证较低的直流阻抗与交流阻抗。接地位置要求分为电气部件本体和车身端，电气部件本体的接地位置需要尽可能靠近高压线束接插件端口，可以保证较低噪发射水平和较高的抗干扰能力，例如动力电池包壳体接地位置，靠近高压出线口位置（近端）接地优于远端接地，近端可以有效减小噪声环路面积；车身端接地位置要求尽量靠近部件本体位置，以缩短接地线长度。紧固螺钉要求，接地线紧固

螺钉本身需要导电设计，并且需要做防腐蚀处理，否则会影响接地效果；螺钉规格推荐使用M8（含以上），以增大接触面积。接地线车身搭接面需要导电处理，并且需要防腐蚀工艺处理；搭接面面积需要超过紧固螺栓头（或螺母）面积。

另外，高压电气部件至少1根搭铁线，强干扰源零部件建议2根以上搭铁线，搭铁线尽可能短、粗（建议：长度≤20cm，长宽比小于5，保证接地阻抗最小）。

7.4 整车系统屏蔽设计要求

7.4.1 零部件机壳屏蔽设计

高压电气部件的机壳应做屏蔽设计，以降低零部件对外的电磁辐射发射，同时也降低其受到外部电磁辐射干扰。具体设计要求如下：

（1）上下壳搭接处得密封胶不能影响搭接阻抗，用导电密封胶条最佳，建议上下机壳搭接阻抗≤5mΩ；

（2）机壳螺钉搭接处不能喷漆、涂胶等影响搭接效果；

（3）机壳上螺孔的间距建议≤7cm；

（4）若机壳有开孔需求，孔缝最长边的尺寸建议≤5cm；

7.4.2 高压线缆总成屏蔽设计

高压线缆总成是否屏蔽设计，应根据整车及零部件EMC设计策略确定。

若高压线缆总成为屏蔽设计，则屏蔽层在端口 360^0 搭接，不建议悬空和猪尾巴形式搭接，且屏蔽层需双端接地，建议屏蔽层的直流电阻≤25mΩ/m，连接器两端屏蔽层直流电阻≤5mΩ/m，屏蔽层（靠近连接器尾部）到产品壳体或适配件的搭接电阻≤10mΩ。

7.4.3 低压线缆屏蔽设计

针对通信信号线、旋变信号线，其对干扰信号比较敏感，且会影响整车的安全性能；因此必要时应做专门的屏蔽设计，以降低此类信号受到的耦合干扰。

敏感的通信线建议使用屏蔽双绞线，屏蔽层双端接地，接地线应通过低压端子的管脚接至板子内部的信号参考地平面。

7.5 车载电气和电子部件端口滤波及防护设计要求

7.5.1 滤波设计

车载电气、电子设备产生的电磁干扰信号会通过端口传导至线束后：一方面，线束的天线效应会产生对外的辐射发射，引起辐射发射超标及辐射干扰其它车载电器；另一方面，干扰信号经线束传导至其他车载电器，对其产生直接的传导干扰。因此，对车载电气、电子设备的端口建议根据实际情况做滤波设计，具体设计要求如下：

（1） 高压母线端口：可采用电容、磁环组合的方式进行差模、共模滤波；

（2） DCDC电源的低压（12V）输出端口：建议采用电感、电容组合进行滤波；

（3） 低压电源输入端口：建议可采用电感、电容组合进行差模滤波设计；

（4） 通信端口：建议采用电感、电容组合进行差模、共模滤波设计。

以上所有的滤波电路设计时均需根据各电气、电子部件的噪声频率特性进行，对特定噪声的频段进行选型设计，必要时可利用仿真软件进行辅助参考，但不能仅依靠仿真的结果，必须要进行实际测试验证。

7.5.2 防护设计

低压电源输入端口、通信端口等低压敏感信号端应进行防护设计，防护设计除了选用本身抗干扰性较强的芯片或器件外，也可增加像共模电感、电容、TVS（瞬态抑制二极管）、压

敏电阻等器件进行防护设计，具体使用可根据各部件或整车实际的干扰波形的特性来选型确定。

8.热可靠性设计规范

8.1 电池热可靠性

8.1.2 温控目标

温控目标包含三方面设计因素，电芯温度设计目标、冷却系统温度目标以及加热系统温度目标。

8.1.2.1 电芯温度设计目标

电芯温度设计目标应综合考虑电芯材料体系、电芯安全、功率要求、循环寿命以及车辆使用场景等因素共同确定，一般锂离子电池的最佳设计温度范围是 20～30℃。

8.1.2.2 冷却系统温度目标

冷却系统是为了电池系统高温时实现冷却的目的，如采用冷却工质，应对冷却工质的温度范围设定具体的值，设定时应综合考虑电芯温度设计目标要求、冷却速率、车辆能提供的冷却能力等因素。

8.1.2.3 加热系统温度目标

加热系统是为了电池系统低温时实现加热的目的，如采用加热工质，应对加热工质的温度范围设定具体的值，设定时应综合考虑电芯温度设计目标要求、电芯允许的加热温度、加热安全、加热速率、车辆能提供的加热能力等因素。

8.1.3 冷却系统的技术路线与选用策略

冷却系统技术路线的确定主要结合电芯温度设计目标、车辆使用场景、电芯发热功率以及温差要求、空间、能耗和成本等因素综合选择。冷却形式及性能参考值如下表：

形式	换热系数（$W/m^2 \cdot K$）	成本
自然冷却	5-25	低
主动风冷	25-100	低
主动液冷	500-15000	中
主动直冷	2500-25000	高

冷却策略的制定主要依据电芯冷却温度要求、车辆使用工况、温差要求、能耗要求、充电时间、整车提供的冷却能力等综合确定。后续设计方案中确定液冷系统流量、制冷介质入口温度、电子水泵 PQ 曲线。

8.1.4 加热系统的技术路线与选用策略

加热系统技术路线的确定主要结合电芯温度设计目标、加热使用场景、加热速率、加热安全、加热系统使用寿命以及温差、空间、能耗和成本等因素综合选择。常见的加热形式及性能特点如下表：

形式	特点	空间要求	温度范围	成本
加热膜	电阻	0.5～2mm	≥60℃	低
PTC	控温加热	2～8mm	60～80℃	中
液热	对流加热	8～13mm	40～60℃	高

加热策略的制定主要依据电芯加热温度要求、车辆使用工况、温差要求、充电时间、充电容量、加热安全、整车提供的加热能力等综合确定。

8.1.5 保温设计

保温是指利用电池系统的结构形式以及保温材料进行隔热和保温处理，主要目的是为了减少外部热源对电池系统的影响，以及保持系统温度的能力。保温性能的设计目标应平衡低温能量保持率要求以及高温条件下的冷却能力进行综合制定。

保温主要通过隔热等措施实现，需要同时考虑隔热路径上隔热材料是否对机械性能产生影响。

8.1.6 零部件热可靠性设计

零部件的设计需确保加热、冷却以及保温子系统发挥性能作用。在满足功能设计的前提下，保证电池产品使用寿命周期内的可靠性，并进行老化、耐久等可靠性测试进行验证。

8.2 驱动系统热安全设计

8.2.1 驱动系统冷却条件及冷却设计要求

冷却系统使动力系统关键零部件工作在合适的温度范围内，防止因温度失控导致性能受限甚至损坏

。当工况和环境条件变化时，仍能保证驱动系统可靠地工作和维持最佳的冷却水温度。

8.2.2 驱动电机及控制器的过热监控与过热保护

驱动电机控制器需监控功率模块的温度，驱动电机绕组的温度。对于没有自带温度传感器的驱动系统零部件，需至少在温度最高的区域附近加装温度传感器，根据温度传感器与温度最高区域的相对位置，估算监控温度的许用范围。

根据监控点的许用温度范围实施过热保护措施，应设置过温报警温度点，以提醒用户降功率运行。

8.3 充电系统热安全设计

充电系统的热可靠性主要针对车载充电机、DCDC、高压线束、充电桩及无线充电设备。

8.3.1 充电系统冷却条件及冷却设计要求

充电系统的冷却设计应使得其满足高低温正常运行的要求：在低温环境下长时间静止后能够正常起动，在高温环境下持续工作不出现超温现象。

充电系统的冷却设计除了需要保证零部件的热可靠性，对于风冷设计还需要保证其运行噪声满足设计要求，对于水冷设计还需要保证其系统流阻和气密性满足设计要求并尽量减小冷却液的用量。

8.3.2 过热监控与过热保护

充电系统需要按照 GB/T18487.1-2015《电动汽车传导充电系统第 1 部分通用要求》，额定工作电流大于 16A 时须有设计相应的温度监控并反馈给整车控制器或 BMS。

根据监控点的许用温度范围实施过热保护措施，应设置过温报警温度点，以提醒用户降功率运行。

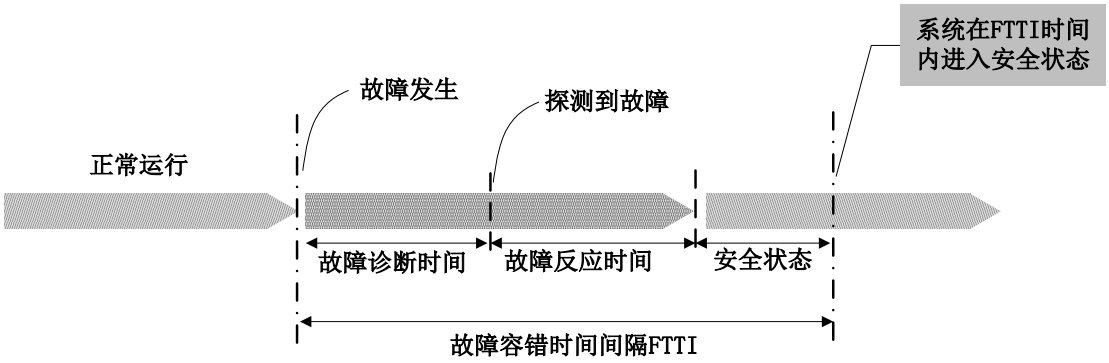
8.4 空调系统过热监控与保护

空调系统热源包含空调压缩机、加热器、冷凝器及相关管路、泵体等。设计时应避免极端工况或部分零件失效模式下导致的热源温度上升造成系统损坏。

同时对加热器表面设置温度传感器监控温度上升情况。加热装置为风暖式的表面温度不得高于 140℃，加热装置为水暖式的加热器表面温度不得高于 110℃，出水口应设置高温防护装置以防止附件部件受到高温加热产生变形或其他损坏。

附录 A：

1、系统应在故障容错时间间隔（FTTI）内进入安全状态，具体见下图：



2、若系统无法在故障容错时间间隔（FTTI）内进入安全状态，应执行紧急运行，具体见下图：