

中华人民共和国国家标准

GB/T XXXXX—XXXX

电动汽车用电池管理系统功能安全要求及 试验方法

Functional safety requirements and testing methods for battery management
system of electric vehicles

(征求意见稿)

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 要求	3
5 相关项定义	3
6 危害分析和风险评估	4
7 功能安全要求	5
8 功能安全验证和确认	9
附录 A（资料性附录）以电池管理系统（BMS）为相关项的危害分析和风险评估（HARA）示例....	20
附录 B（资料性附录）以动力蓄电池系统为相关项的危害分析和风险评估（HARA）示例.....	27
附录 C（资料性附录）故障容错时间间隔（FTTI）确定方法示例.....	32

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国汽车标准化技术委员会（SAC/TC114）归口。

本标准起草单位：

本标准主要起草人：

电动汽车用电池管理系统功能安全要求及试验方法

1 范围

本标准规定了电动汽车用蓄电池管理系统（以下简称电池管理系统）的功能安全要求及试验方法。

本标准适用于电动乘用车用锂离子高压动力蓄电池管理系统，其它类型车辆的蓄电池管理系统可参照执行。

2 规范性引用文件

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

GB XXXXX-XXXX 电动汽车安全要求

GB XXXXX-XXXX 电动汽车用锂离子动力蓄电池安全要求

GB/T 34590.1-2017，道路车辆 功能安全 第1部分：术语 (ISO 26262-1:2011, MOD)

GB/T 34590.2-2017，道路车辆 功能安全 第2部分：功能安全管理 (ISO 26262-2:2011, MOD)

GB/T 34590.3-2017，道路车辆 功能安全 第3部分：概念阶段 (ISO 26262-3:2011, MOD)

GB/T 34590.4-2017，道路车辆 功能安全 第4部分：产品开发：系统层面 (ISO 26262-4:2011, MOD)

GB/T 34590.5-2017，道路车辆 功能安全 第5部分：产品开发：硬件层面 (ISO 26262-5:2011, MOD)

GB/T 34590.6-2017，道路车辆 功能安全 第6部分：产品开发：软件层面 (ISO 26262-6:2011, MOD)

GB/T 34590.7-2017，道路车辆 功能安全 第7部分：生产和运行 (ISO 26262-7:2011, MOD)

GB/T 34590.8-2017，道路车辆 功能安全 第8部分：支持过程 (ISO 26262-8:2011, MOD)

GB/T 34590.9-2017，道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析 (ISO 26262-9:2011, MOD)

GB/T 34590.10-2017，道路车辆 功能安全 第10部分：指南 (ISO 26262-10:2012, MOD)

GB/T XXXXX-XXXX 电动汽车用电池管理系统技术条件

3 术语和定义

GB/T 34590.1-2017界定的以及下列术语和定义适用于本文件。

3.1 蓄电池管理系统 battery management system; BMS

监视蓄电池的状态(温度、电压、荷电状态等)，可以为蓄电池提供通讯、安全、电芯均衡及管理控制，并提供与应用设备通讯接口的系统。

3.2 电池单体 secondary cell

将化学能与电能进行相互转换的基本单元装置，通常包括电极、隔膜、电解质、外壳和端子，并被设计成可充电。

3.3 高压系统 high voltage power system

电动汽车内部B级电压以上与动力电池直流母线相连或由动力电池电源驱动的高压驱动零部件系统，主要包括但不限于：动力电池系统和/或高压配电系统（高压继电器、熔断器、电阻器、主开关等），电机及其控制系统、DC/DC变换器和车载充电机等。

3.4 动力蓄电池系统 power battery system

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

3.5 故障容错时间间隔 fault tolerant time interval; FTTI

在安全机制未被激活情况下，从相关项内部故障发生到可能发生危害事件的最短时间间隔。

注1：安全相关的时间间隔参见图1。

注2：应评估所有危害事件的最短时间间隔，其取决于危害的特征。

注3：FTTI与相关项的功能异常表现而引起的危害有关。FTTI是安全目标的属性。

注4：在容错时间间隔内，如果相关项保持在安全状态或过渡到安全状态或过渡到紧急运行，则表明安全机制及时对故障进行了处理。

注5：危害事件的发生取决于存在的故障并且车辆处于故障可影响车辆行为的场景中。

示例：制动系统失效可能不会导致危害事件，直到实施制动。

注6：虽然仅在相关项层面定义FTTI，但在要素层面可规定最长故障处理时间间隔和故障处理后达到的状态，以支持功能安全概念。

注7：故障探测时间间隔可包括多个诊断测试时间间隔，以允许在诊断测试时间间隔足够小于故障探测时间间隔的情况下消除错误。

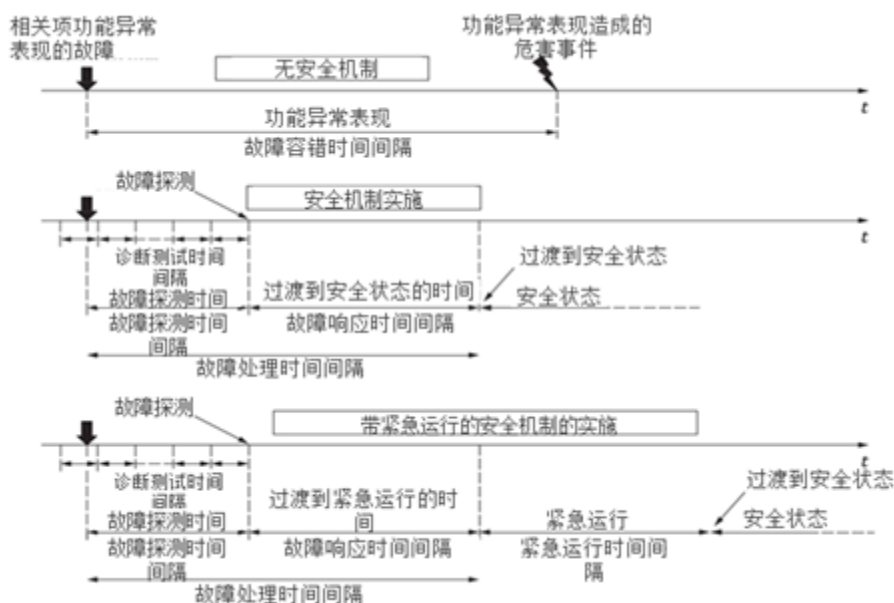


图 1 安全相关时间间隔

3.6 热扩散 thermal propagation

电池包或系统内由一个电池单体热失控引发的其余电池单体接连发生热失控的现象。

3.7 热失控 thermal runaway

电池单体放热连锁反应引起电池温度不可控上升的现象。

3.8 爆炸 explosion

突然释放足量的能量产生压力波或者喷射物，可能会对周边区域造成结构或物理上的破坏。

3.9 漏液 leakage

蓄电池内部电解液泄漏到电池壳体外部。

3.10 泄气 venting

单体电池或电池组中内部压力增加时，气体通过预先设计好的方式释放出来。

3.11 过充电 overcharge

当电芯或电池完全充电后继续进行充电。

3.12 过放电 over discharge

当电芯或电池完全放电后继续进行放电。

3.13 起火 fire

电池单体、模块、电池包或系统任何部位发生持续燃烧（火焰持续时间大于1 s）。火花及拉弧不属于燃烧。

注：火焰持续时间大于1 s是指单次火焰持续时间，而非多次火焰的累计时间。

4 一般要求

除非特别说明，电池管理系统（BMS）功能安全技术开发、流程开发等要求参照GB/T34590-2017《道路车辆 功能安全》。

5 相关项定义

5.1 总则

应按照GB/T34590-2017《道路车辆 功能安全》的要求进行相关项定义，相关项指的是实现车辆层面功能或部分功能的系统或系统组。

注：相关项及其范围可根据具体情况定义。附录A和附录B分别给出了以电池管理系统（BMS）和动力蓄电池系统为相关项的功能概念和相关项边界和接口示例。

5.2 功能概念

为满足车辆安全运行，确保车辆内部、外部人员以及车辆环境的安全，电池管理系统对充电状态及放电状态下的动力蓄电池状态进行监控和保护。

注1：附录A给出了电池管理系统（BMS）充电管理和放电管理的功能概念描述。附录B给出了动力蓄电池系统提供充电和提供放电的功能概念描述。

注2：充电状态包括外部充电、内部充电（例如整车制动能量回收）等。放电状态包括行车放电、静置放电等。

5.3 运行条件和环境约束

为满足车辆安全运行，需要明确相关项的运行条件及环境约束，可包含（如适用）：

- 1) 外部环境，例如，温度、湿度、路况、天气等；
- 2) 运行模式，例如，动力蓄电池系统处于充电状态、放电状态、静置状态等，或者电池管理系统处于激活状态或者休眠状态；
- 3) 相关项与整车其他相关项的依赖关系、接口关系等。

5.4 标准和法规要求

电池管理系统（BMS）开发可参考如下标准和法规要求：

- 1) GB XXXXX-XXXX《电动汽车安全要求》；
- 2) GB XXXXX-XXXX《电动汽车用锂离子动力蓄电池安全要求》；
- 3) GB/T 34590-2017《道路车辆 功能安全》；
- 4) GB/T XXXX《电动汽车用电池管理系统技术条件》。

6 危害分析和风险评估

6.1 总则

根据第5章相关项的功能概念，按照GB/T34590-2017《道路车辆 功能安全 第3部分：概念阶段》，基于车辆使用场景，分析识别相关项中因故障而引起的危害并对危害进行归类，定义相应的汽车安全完整性等级(ASIL)，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。

注：附录A和附录B分别给出了以电池管理系统（BMS）和动力蓄电池系统为相关项进行危害分析和风险评估的示例。

6.2 安全目标

通过危害分析和风险评估确定的电池管理系统（BMS）安全目标，如表1所示，包括安全目标、ASIL等级、安全状态和FTTI。

表1 安全目标

序号	安全目标	ASIL	安全状态	FTTI
1	防止电池单体过充导致热失控。	C	断开高压回路。	参见7.1.3
2	防止电池单体过放后再充电导致热失控。	C	断开充电回路。	参见7.2.3
3	防止电池单体过温导致热失控。	C	断开高压回路。	参见7.3.3

4	防止动力蓄电池系统过流导致热失控。	C	断开高压回路。	参见7.4.3
---	-------------------	---	---------	---------

注：充电回路指动力蓄电池从外部吸收能量的回路，包括外部充电及内部充电（例如整车制动能量回收）。

7 功能安全要求

7.1 防止电池单体过充导致热失控

7.1.1 一般要求

电池管理系统应监测电池单体电压，当电池单体电压值超过安全阈值时，使动力蓄电池系统在FTTI时间内进入安全状态，在电池单体过充故障退出、消除条件未满足时，不应退出安全状态。

注1：故障探测、响应、处理应在FTTI时间内完成。

注2：安全阈值应根据电池系统制造商过充测试结果给出。

7.1.2 运行模式

电池管理系统应处于激活状态。

7.1.3 故障容错时间间隔（FTTI）

电池单体过充故障容错时间间隔应根据电池系统制造商过充测试结果给出。

注：电池单体过充故障容错时间间隔（FTTI）的确定方法参考附录C，示意图参见图2。

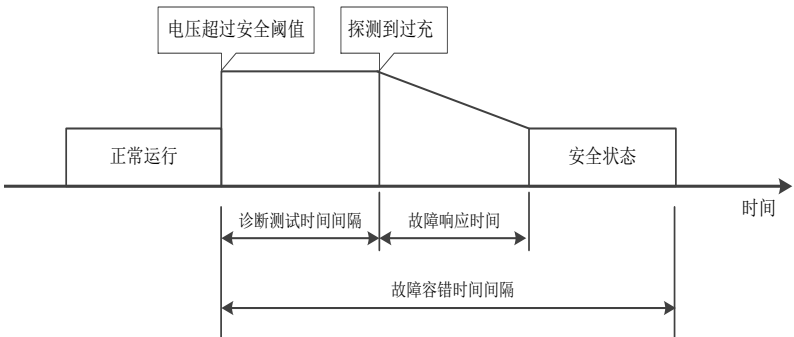


图2 电池单体过充故障容错时间间隔（FTTI）

7.1.4 安全状态的进入和退出

当确认电池单体电压值超过安全阈值时，电池管理系统应断开高压回路进入安全状态，在电池单体过充故障退出、消除条件未满足时，不应退出安全状态。

注：故障退出、消除条件由相关方协商确定。

7.1.5 报警和降级概念

在电池管理系统检测到电池单体过充故障后，应通过警告信号或提示信息等方式警告驾驶员。

如果动力蓄电池存在无法立即进入或保持安全状态的场景，应设计降级功能（例如限制充电功率）让整车进入紧急运行模式。

7.2 防止电池单体过放后再充电导致热失控

7.2.1 一般要求

电池管理系统应监测电池单体电压，当电池单体电压值低于安全阈值时，使动力蓄电池系统在FTTI时间内进入安全状态，在电池单体过放故障退出、消除条件未满足时，不应退出安全状态。

注1：故障探测、响应、处理应在FTTI时间内完成。

注2：安全阈值应根据电池系统制造商过放测试结果给出。

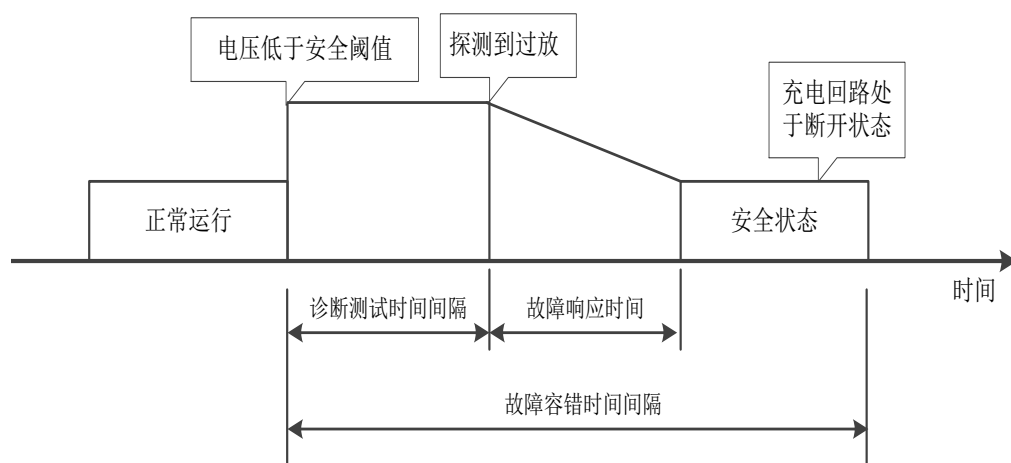
7.2.2 运行模式

电池管理系统应处于激活状态。

7.2.3 故障容错时间间隔（FTTI）

电池单体过放后再充电故障容错时间间隔应根据电池系统制造商过放后再充电的测试结果给出。

注：电池单体过放后再充电故障容错时间间隔（FTTI）的确定方法参考附录C，示意图参见图3。



7.2.4 安全状态的进入和退出

当确认电池单体电压值低于安全阈值时，电池管理系统应断开充电回路进入安全状态，在电池单体过放故障退出、消除条件未满足时，不应退出安全状态。

注：故障退出、消除条件由相关方协商确定。

7.2.5 报警和降级概念

在电池管理系统检测到电池单体过充故障后，应通过警告信号或提示信息等方式警告驾驶员。

如果动力蓄电池存在无法立即进入或保持安全状态的场景，应设计降级功能（例如限制充电功率、禁止制动能量回收功能的使用）让整车进入紧急运行模式。

7.3 防止电池单体过温导致热失控

7.3.1 一般要求

电池管理系统应监测电池单体温度，当电池单体温度值高于安全阈值时，使动力蓄电池系统在FTTI时间内进入安全状态，在电池单体过温故障退出、消除条件未满足时，不应退出安全状态。

注1：故障探测、响应、处理应在FTTI时间内完成。

注2：安全阈值应根据电池系统制造商过温测试结果给出。

注3：电池系统内温度测量点的分布应能保证代表电池系统中单体电池的最高温度。

7.3.2 运行模式

电池管理系统应处于激活状态。

7.3.3 故障容错时间间隔（FTTI）

电池单体过温故障容错时间间隔应根据电池系统制造商过温的测试结果给出。

注：电池单体过温故障容错时间间隔（FTTI）的确定方法参考附录C，示意图参见图4。

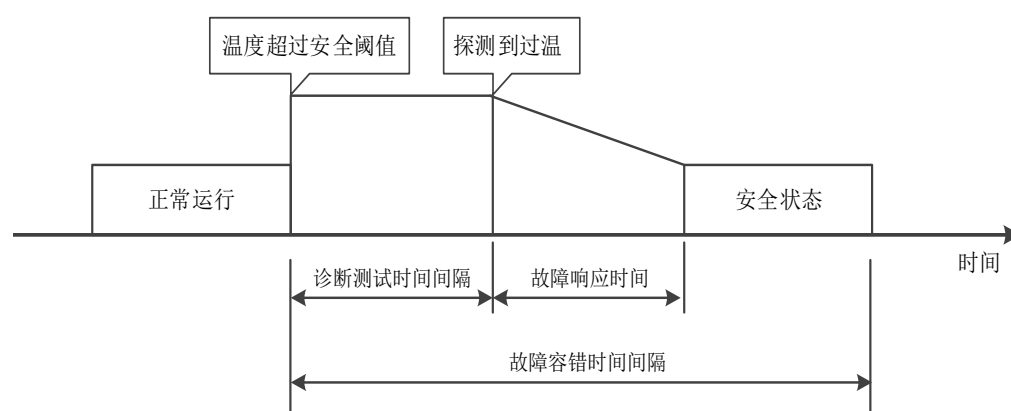


图4 电池单体过温故障容错时间间隔（FTTI）

7.3.4 安全状态的进入和退出

当确认电池单体温度值高于安全阈值时，电池管理系统应断开高压回路进入安全状态，在电池单体过温故障退出、消除条件未满足时，不应退出安全状态。

注：故障退出、消除条件由相关方协商确定。

7.3.5 报警和降级概念

在电池管理系统检测到电池单体过充故障后，应通过警告信号或提示信息等方式警告驾驶员。

如果动力蓄电池存在无法立即进入或保持安全状态的场景,应设计降级功能(例如限制充放电功率,禁止某些非安全运行相关功能的运行)让整车进入紧急运行模式。

7.4 防止动力蓄电池系统过流导致热失控

7.4.1 一般要求

电池管理系统应监测动力蓄电池系统电流,当动力蓄电池系统电流值高于安全阈值时,使动力蓄电池系统在FTTI时间内进入安全状态。在蓄电池系统过流故障退出、消除条件未满足时,不应退出安全状态。

注1:故障探测、响应、处理应在FTTI时间内完成。

注2:安全阈值应根据电池系统制造商过流测试结果给出,并考虑到电池单体温度的影响。

7.4.2 运行模式

电池管理系统应处于激活状态。

7.4.3 故障容错间隔 (FTTI)

动力蓄电池系统过流故障容错时间间隔应根据电池系统制造商过流测试结果给出。

注:动力蓄电池系统过流故障容错时间间隔 (FTTI) 的确定方法参考附录C,示意图参见图5。

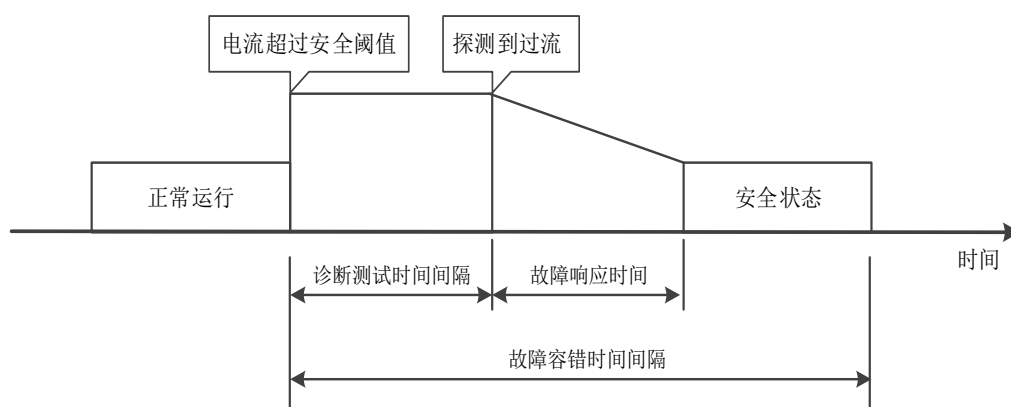


图5 动力蓄电池系统过流故障容错时间间隔 (FTTI)

7.4.4 安全状态的进入和退出

当确认蓄电池系统电流值高于安全阈值时,电池管理系统应断开高压回路进入安全状态,在蓄电池系统过流故障退出、消除条件未满足时,不应退出安全状态。

注:故障退出、消除条件由相关方协商确定。

7.4.5 报警和降级概念

在电池管理系统检测到电池单体过充故障后,应通过警告信号或提示信息等方式警告驾驶员。

如果动力蓄电池存在无法立即进入或保持安全状态的场景,应设计降级功能(例如限制充放电功率、禁止某些非安全相关功能的运行)让整车进入紧急运行模式。

8 功能安全验证和确认

8.1 总则

功能安全验证是确定功能安全要求的完整性和正确性,功能安全确认是确认安全目标得到充分实现且在系统及整车层面能够减轻或避免危害事件的发生。

8.2 功能安全验证

功能安全验证应在电池管理系统层面对功能安全要求与设计进行验证,验证方法包括评审、走查、检查、模型检查、模拟、工程分析、证明和测试,验证的目的是证明功能安全要求:

- a) 与验证活动的结果的一致性与符合性;
- b) 实现的正确性。

本标准中主要给出基于测试的功能安全验证方法,测试可在仿真环境或真实环境下进行。

8.2.1 防止电池单体过充导致热失控

8.2.1.1 测试目的

电池管理系统应监测电池单体电压,当电池单体电压值超过安全阈值时,使动力蓄电池系统在FTTI时间内进入安全状态,在电池单体过充故障退出、消除条件未满足时,不应退出安全状态。

8.2.1.2 测试对象

测试对象为电池管理系统。

8.2.1.3 测试要求

8.2.1.3.1 仿真环境测试应满足如下要求:

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.1.2章节规定的运行模式。
- c) 模拟电池单体电压信号进行测试。
- d) 调节模拟的电池单体电压信号,应至少包含低于安全阈值、达到安全阈值及高于安全阈值三个电压取值。
- e) 测试应对电池管理系统进入安全状态的过程(例如,安全阈值、时间、状态切换)进行监控。
- f) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.1.3.2 真实环境测试应满足如下要求:

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.1.2章节规定的运行模式。

- c) 测试对象所在的电池系统应由电池系统制造商许可的充电倍率进行充电，直到高于安全阈值。
- d) 测试应对电池管理系统进入安全状态的过程（例如，安全阈值、时间、状态切换）进行监控。
- e) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.1.4 测试结束条件

8.2.1.4.1 当符合以下任一条件时，结束仿真环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态。
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。

8.2.1.4.2 当符合以下任一条件时，结束真实环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态。
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。
- d) 测试对象所在电池系统发生漏液、泄气或起火爆炸。

8.2.1.5 测试通过准则

测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态。

8.2.2 防止电池单体过放后再充电导致热失控

8.2.2.1 测试目的

电池管理系统应监测电池单体电压，当电池单体电压值低于安全阈值时，使动力蓄电池系统在FTTI时间内进入安全状态，在电池单体过放故障退出、消除条件未满足时，不应退出安全状态。

8.2.2.2 测试对象

测试对象为电池管理系统。

8.2.2.3 测试要求

8.2.2.3.1 仿真环境测试应满足如下要求：

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.2.2章节规定的运行模式。
- c) 模拟电池单体电压信号，进行测试。
- d) 调节模拟的电池单体电压信号，应至少包含低于安全阈值、达到安全阈值及高于安全阈值三个电压取值。
- e) 测试应对电池管理系统进入安全状态的过程（例如，安全阈值、时间、状态切换）进行监控。

f) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.2.3.2 真实环境测试应满足如下要求：

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.2.2章节规定的运行模式。
- c) 测试对象所在的电池系统应由电池系统制造商许可的放电倍率进行放电，直到低于安全阈值。
- d) 测试应对电池管理系统进入安全状态的过程（例如，安全阈值、时间、状态切换）进行监控。
- e) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.2.4 测试结束条件

8.2.2.4.1 当符合以下任一条件时，结束仿真环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态；
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。

8.2.2.4.2 当符合以下任一条件时，结束真实环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态；
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。
- d) 测试对象所在电池系统发生漏液、泄气或起火爆炸。

8.2.2.5 测试通过准则

测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态。

8.2.3 防止电池单体过温导致热失控

8.2.3.1 测试目的

电池管理系统应监测电池单体温度，当电池单体温度值高于安全阈值时，使动力蓄电池系统在FTTI时间内进入安全状态，在电池单体过温故障退出、消除条件未满足时，不应退出安全状态。

8.2.3.2 测试对象

测试对象为电池管理系统。

8.2.3.3 测试要求

8.2.3.3.1 仿真环境测试应满足如下要求：

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.3.2章节规定的运行模式。

- c) 模拟电池单体温度信号，进行测试。
- d) 模拟的电池单体温度信号，应至少包含低于安全阈值、达到安全阈值及高于安全阈值三个温度取值。
- e) 测试应对电池管理系统进入安全状态的过程（例如，安全阈值、时间、状态切换）进行监控。
- f) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.3.3.2 真实环境测试应满足如下要求：

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.3.2章节规定的运行模式。
- c) 测试对象所在的电池系统应由电池系统制造商许可的充放电倍率进行充放电或者其它电池系统制造商推荐的电池单体加热方法，直到电池单体温度高于安全阈值。
- d) 测试应对电池管理系统进入安全状态的过程（例如，安全阈值、时间、状态切换）进行监控。
- e) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.3.4 测试结束条件

8.2.3.4.1 当符合以下任一条件时，结束仿真环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态；
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。

8.2.3.4.2 当符合以下任一条件时，结束真实环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态；
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。
- d) 测试对象所在电池系统发生漏液、泄气或起火爆炸。

8.2.3.5 测试通过准则：

测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态。

8.2.4 防止动力蓄电池系统过流导致热失控

8.2.4.1 测试目的

电池管理系统应监测蓄电池系统电流，当动力蓄电池系统电流值高于安全阈值时，使动力蓄电池系统在FTTI时间内进入安全状态。在蓄电池系统过流故障退出、消除条件未满足时，不应退出安全状态。

8.2.4.2 测试对象

测试对象为电池管理系统。

8.2.4.3 测试要求

8.2.4.3.1 仿真环境测试应满足如下要求：

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.4.2章节规定的运行模式。
- c) 模拟动力蓄电池系统电流信号，进行测试。
- d) 测试需要考虑影响电流安全阈值的参数，例如温度等。
- e) 调节模拟的动力蓄电池系统电流信号，应至少包含低于安全阈值、达到安全阈值及高于安全阈值三个电流取值。
- f) 测试应对电池管理系统进入安全状态的过程（例如，安全阈值、时间、状态切换）进行监控。
- g) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.4.3.2 真实环境测试应满足如下要求：

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态。
- b) 测试应针对7.4.2章节规定的运行模式。
- c) 测试对象所在的电池系统应由电池系统制造商许可的充放电倍率变化速率逐步提高充放电电流进行充放电，直到电流超过安全阈值。
- d) 测试需要考虑影响电流安全阈值的参数，例如温度等。
- e) 测试应对电池管理系统进入安全状态的过程（例如，安全阈值、时间、状态切换）进行监控。
- f) 测试应对电池管理系统退出安全状态的条件进行监控。

8.2.4.4 测试结束条件

8.2.4.4.1 当符合以下任一条件时，结束仿真环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态；
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。

8.2.4.4.2 当符合以下任一条件时，结束真实环境测试：

- a) 测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态；
- b) 测试对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 测试对象在故障容错时间间隔内未进入安全状态。
- d) 测试对象所在电池系统发生漏液、泄气或起火爆炸。

8.2.4.5 测试通过准则

测试对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态。

8.3 功能安全确认

功能安全确认需要在蓄电池或整车层面对功能安全目标的实现进行确认，确认方法包含检查和测试，目的包括：

- a) 证明安全目标在整车层面的实现是正确的、完整的并得到完全实现；
- b) 安全目标能够预防或减轻危害分析和风险评估中识别的危害事件及风险。

本标准中主要给出基于测试的功能安全确认方法。

8.3.1 防止电池单体过充导致热失控

8.3.1.1 目的

确认安全目标“防止电池单体过充导致热失控”得到正确实现，并能够有效预防由于电池单体过充导致热失控的发生。

8.3.1.2 确认对象

确认对象为动力蓄电池系统。

8.3.1.3 确认要求

- a) 影响确认对象功能并与确认结果相关的所有设备都应处于正常运行状态；
- b) 确认应在整车层面进行，至少包含真实的电池系统，基于车辆的实际工况或者模拟的车辆实际工况；

注：车辆的实际工况至少包含危害分析和风险评估中最严苛工况。

- c) 确认应包含违背安全目标的典型失效模式。

注：典型失效模式应至少包含危害分析和风险评估中导出该安全目标的功能异常，如非预期的充电。

- d) 确认应对动力蓄电池系统进入安全状态的过程（例如，安全阈值、时间和状态切换）进行监控。
- e) 确认应对动力蓄电池系统的状态进行监控。
- f) 确认应对动力蓄电池系统退出安全状态的条件进行监控。
- g) 确认结束后，应在确认环境温度下观察1小时。

8.3.1.4 确认结束条件

当符合以下任一条件时，结束试验：

- a) 确认对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态，并且电池未发生漏液、泄气或起火爆炸。
- b) 确认对象在故障容错时间间隔内进入安全状态，意外退出安全状态。

- c) 确认对象在故障容错时间间隔内未进入安全状态。
- d) 确认对象发生漏液、泄气或起火爆炸。

8.3.1.5 确认通过准则

确认对象在故障容错时间间隔内进入安全状态，无意外退出安全状态，并且在观察时间内未发生漏液、泄气或起火爆炸。

8.3.2 防止电池单体过放后再充电导致热失控

8.3.2.1 目的

确认安全目标“防止电池单体过放后再充电导致热失控”得到正确实现，并能够有效预防由于电池单体过放后再充电导致热失控的发生。

8.3.2.2 确认对象

确认对象为动力蓄电池系统。

8.3.2.3 确认要求

- a) 影响确认对象功能并与确认结果相关的所有设备都应处于正常运行状态；
- b) 确认应在整车层面进行，至少包含真实的电池系统，车辆的实际工况或者模拟车辆使用的工况；

注：车辆的实际工况至少包含危害分析和风险评估中最严苛工况。
- c) 确认应包含违背安全目标的典型失效模式。

注：典型失效模式应至少包含危害分析和风险评估中导出该安全目标的功能异常，如非预期的放电。
- d) 确认应对动力蓄电池系统进入安全状态的过程（例如，安全阈值、时间和状态切换）进行监控。
- e) 确认应对动力蓄电池系统的状态进行监控。
- f) 确认应对动力蓄电池系统退出安全状态的条件进行监控。
- g) 确认结束后，应在确认环境温度下观察1小时。

8.3.2.4 确认结束条件

当符合以下任一条件时，结束确认：

- a) 确认对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态，并且电池未发生漏液、泄气或起火爆炸。
- b) 确认对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 确认对象在故障容错时间间隔内未进入安全状态。
- d) 确认对象发生漏液、泄气或起火爆炸。

8.3.2.5 确认通过准则

确认对象在故障容错时间间隔内进入安全状态，无意外退出安全状态，并且在观察时间内未发生漏液、泄气或起火爆炸。

8.3.3 防止电池单体过温导致热失控

8.3.3.1 目的

确认安全目标“防止电池单体过温导致热失控”得到正确实现，并能够有效预防由于电池单体过温导致热失控的发生。

8.3.3.2 确认对象

确认对象为动力蓄电池系统。

8.3.3.3 确认要求

- a) 影响测试对象功能并与确认结果相关的所有设备都应处于正常运行状态
- b) 确认应在整车层面进行，至少包含真实的电池系统，车辆的实际工况或者模拟车辆使用的工况；
注：车辆的实际工况至少包含危害分析和风险评估中最严苛工况。
- c) 确认应包含违背安全目标的典型失效模式。
注：典型失效模式应至少包含危害分析和风险评估中导出该安全目标的功能异常，如高温下充电。
- d) 确认应对动力蓄电池系统进入安全状态的过程（例如，安全阈值、时间和状态切换）进行监控。
- e) 确认应对动力蓄电池系统的状态进行监控。
- f) 确认应对动力蓄电池系统退出安全状态的条件进行监控。
- g) 确认结束后，应在确认环境温度下观察1小时。

8.3.3.4 确认结束条件

当符合以下任一条件时，结束确认：

- a) 确认对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态，并且电池未发生漏液、泄气或起火爆炸。
- b) 确认对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 确认对象在故障容错时间间隔内未进入安全状态。
- d) 确认对象发生漏液、泄气或起火爆炸。

8.3.3.5 确认通过准则

确认对象在故障容错时间间隔内进入安全状态，无意外退出安全状态，并且在观察时间内未发生漏液、泄气或起火爆炸。

8.3.4 防止动力蓄电池系统过流导致热失控

8.3.4.1 目的

确认安全目标“防止蓄电池系统过流导致热失控”得到正确实现，并能够有效预防由于蓄电池系统过流导致热失控的发生。

8.3.4.2 确认对象

确认对象为动力蓄电池系统。

8.3.4.3 确认要求

- a) 影响测试对象功能并与测试结果相关的所有设备都应处于正常运行状态
- b) 确认应在整车层面进行，至少包含真实的电池系统，车辆的实际工况或者模拟车辆使用的工况；

注：车辆的实际工况至少包含危害分析和风险评估中最严苛工况。
- c) 确认应包含违背安全目标的典型失效模式。

注：典型失效模式应至少包含危害分析和风险评估中导出该安全目标的功能异常，如超过预期电流充电。
- d) 确认需要考虑影响电流安全阈值的参数，例如温度等。
- e) 确认应对动力蓄电池系统进入安全状态的过程（例如，安全阈值、时间和状态切换）进行监控。
- f) 确认应对动力蓄电池系统的状态进行监控。
- g) 确认应对动力蓄电池系统退出安全状态的条件进行监控。
- h) 确认结束后，应在确认环境温度下观察1小时。

8.3.4.4 确认结束条件

当符合以下任一条件时，结束确认：

- a) 确认对象在故障容错时间间隔内进入安全状态，并无意外退出安全状态，并且电池未发生漏液、泄气或起火爆炸。
- b) 确认对象在故障容错时间间隔内进入安全状态，意外退出安全状态。
- c) 确认对象在故障容错时间间隔内未进入安全状态。
- d) 确认对象发生漏液、泄气或起火爆炸。

8.3.4.5 确认通过准则

确认对象在故障容错时间间隔内进入安全状态，无意外退出安全状态，并且在观察时间内未发生漏液、泄气或起火爆炸。

附录 A
(资料性附录)

以电池管理系统（BMS）为相关项的危害分析和风险评估（HARA）示例

A.1 相关项定义

A.1.1 功能概念

A.1.1.1 充电管理

该功能旨在通过电池管理系统（BMS）的控制管理，使得动力蓄电池在充电过程中处于安全状态。电池管理系统（BMS）在动力蓄电池充电过程中对充电电压、充电电流、可检测到的电池温度等参数进行控制优化，确保动力蓄电池在充电过程中的安全。充电管理包括正常充电管理和能量回收管理。

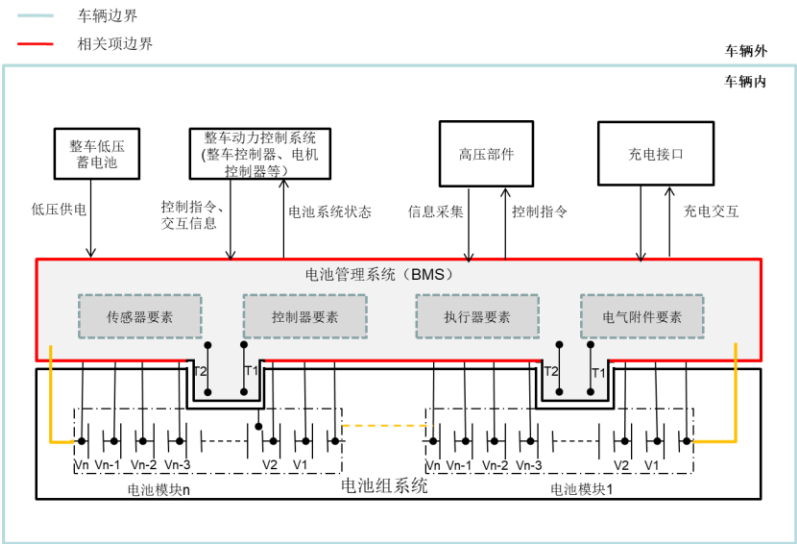
A.1.1.2 放电管理

该功能旨在通过电池管理系统（BMS）的控制管理，使得动力蓄电池在放电过程中处于安全状态。电池管理系统（BMS）在动力蓄电池放电过程中对放电电压、放电电流、可检测到的电池温度等参数进行控制优化，确保动力蓄电池在放电过程中的安全。

A.1.2 蓄电池管理系统（BMS）的边界和接口

按照GB/T 34590.3的5.4.2的要求，定义电池管理系统（BMS）相关项与其它相关项的边界和接口。

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



图A.1 BMS相关项的边界和接口参考示例

A.2 相关项在整车层面上的危害识别

A. 2.1 识别电池管理系统（BMS）的功能异常表现

按照GB/T 34590.3第6章的要求，应用危害与可操作性分析（HAZOP）方法识别电池管理系统（BMS）的功能异常表现，参见表A.1。

表A.1 HAZOP分析示例

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

A. 2.2 分析电池管理系统（BMS）的功能异常表现导致的整车层面危害

按照GB/T 34590.3第6章的要求，根据A.2.1中电池管理系统（BMS）的功能异常表现，分析可能导致的整车层面危害（最严重的情况），参见表A.2。

表A.2 整车层面危害（最严重的情况）

电池管理系统（BMS）功能异常表现的影响	整车层面危害（最严重的情况）
充电时充电电压超出预期，造成电池过充时无保护或保护不及时，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
充电时电流超出预期，造成电池过流时无保护或保护不及时，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
充电时电池温度超出预期，造成电池过温时无保护或保护不及时，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
放电时放电电压超出预期，造成电池过放时无保护或保护不及时	动力电池损坏报废，车辆动力丧失
放电时放电电流超出预期，造成电池过流时无保护或保护不及时，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
放电时电池温度超出预期，造成电池过温时无保护或者保护不及时，引发热失控	车辆冒烟、起火、爆炸、释放有害物质

A.3 场景分析

根据第5章运行条件和环境约束要求，分析典型的车辆运行场景，参见表A.3。

表 A.3 典型的车辆运行场景示例

	场 景 编 号	典型场景
车 辆 状 态	1	正常行驶（高速行驶，城市路况，转弯等）
	2	车辆静止无人看管充电
	3	车辆静止无人看管放电
	4	车辆长期静置
	5	碰撞（发生碰撞，碰撞之后）
	6	维修

A.4 ASIL 等级的导出

以电池管理系统（BMS）为相关项开展典型危害的危害分析和风险评估（HARA），并确定危害事件的ASIL等级。分析过程参见表A.4：

表 A.4 危害分析和风险评估示例

危害编号	功能	功能异常表现	整车层面的危害	假设	危害的详细描述	危害事件 (潜在的事故场景 - 考虑最差情况)	ASIL							备注
							S	理由	E	理由	C	理由	ASIL	
HZD-01	充电管理—充电电压管理	充电电压超出预期，导致电池过充，引发热失控	冒烟、起火、爆炸、释放有害物质	N/A	电池过充，析锂，引起电池内短路，导致热失控，车辆起火、爆炸	车辆静止无人看管充电，电池过充导致热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间 >10 %	2	有泄气、冒烟等预兆，人可逃离	C	
HZD-02	充电管理—充电电压管理	充电电压超出预期，导致电池过充，引发热失控	冒烟、起火、爆炸、释放有害物质	N/A	电池过充，析锂，引起电池内短路，导致热失控，车辆起火、爆炸	车辆正常行驶（高速行驶，城市路况，转弯），电池过充导致热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及乘员及行人	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间 >10 %	2	有泄气、冒烟等预兆，人可逃离	C	
HZD-03	充电管理—充电电流管理	充电电流超出预期，导致电池过流，引发热失控	冒烟、起火、爆炸、释放有害物质	N/A	充电电流超出电池允许的最大充电电流，导致电池热失控，车辆起火、爆炸	车辆静止无人看管充电，充电电流过大，导致电池过流，引发热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间 >10 %	2	有泄气、冒烟等预兆，人可逃离	C	
HZD-04	充电管理—电池温度管理	充电时电池温度超出预期，导致电池过温，引发热失控	冒烟、起火、爆炸、释放有害物质	N/A	充电时能检测到的电池包温度超出预期，造成电池过温，引发热失控，车辆起火、爆炸	车辆静止无人看管充电，高温环境下，电池过温导致热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间 >10 %	2	有泄气、冒烟等预兆，人可逃离	C	
HZD-05	放电管理—放电电压管理	放电时放电电压超出预期，导致电池过放	冒烟、起火、爆炸、释放有害物质	N/A	电池过放后再充电、析锂，引起电池内短路，导致热失控，车辆起火、爆炸	车辆静止无人看管放电，电池过放后再充电，导致热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间 >10 %	2	有泄气、冒烟等预兆，人可逃离	C	

H Z - 0 6	放 电 管 理 一 放 电 电 流 管 理	放电电流 超出预期，导致 电池过流，引发 热失控	冒烟、起火、 爆炸、释放 有害物质	N/A	放电电流超出 电池允许的最大 放电电流，导致 电池热失控， 车辆起火、爆炸	车辆正常行驶（高 速行驶，城市路况， 转弯），放电电流 过大，导致电池过 流，引发电池热失 控，车辆冒烟、起 火、爆炸、释放有 害物质，伤及乘客 和行人。	3	热失控起 火，爆炸 或产生有 害物质造 成人员伤 亡	4	平 均 运 行 时 间 >10 %	2	有 泄 气、冒 烟等预 兆，人 可逃离	C	
H Z - 0 7	放 电 管 理 一 电 池 温 度 管 理	放电时电 池温度超 出预期， 导致电池 过温，引 发热失控	冒烟、起火、 爆炸、释放 有害物质	N/A	电池包温度超 出预期，造成电 池过温，引发热 失控，车辆起 火、爆炸	车辆正常行驶（高 速行驶，城市路况， 转弯），高温环境 下，电池过温导致 热失控，车辆冒烟、 起火、爆炸、释放 有害物质，伤及乘 客和行人。	3	热失控起 火，爆炸 或产生有 害物质造 成人员伤 亡	4	平 均 运 行 时 间 >10 %	2	有 泄 气、冒 烟等预 兆，人 可逃离	C	

A.5 安全目标和安全状态

对于表A.4中具有ASIL等级的危害事件确定安全目标和安全状态，参见表A.5。

表 A.5 安全目标和安全状态

序号	安全目标	安全状态	FTTI
1	防止电池单体过充导致热失控。	断开高压回路。	电池单体过充故障容错时间间隔应根据电池系统制造商过充测试结果给出。 注：故障容错时间间隔（FTTI）的确定方法参考附录C。
2	防止电池单体过放后再充电导致热失控。	断开充电回路。	电池单体过放后再充电故障容错时间间隔应根据电池系统制造商过放后再充电的测试结果给出。 注：故障容错时间间隔（FTTI）的确定方法参考附录C。
3	防止电池单体过温导致热失控。	断开高压回路。	电池单体过温故障容错时间间隔应根据电池系统制造商过温的测试结果给出。 注：故障容错时间间隔（FTTI）的确定方法参考附录C。

4	防止动力蓄电池系统过流导致热失控。	断开高压回路。	动力蓄电池系统过流故障容错时间间隔应根据电池系统制造商过流测试结果给出。 注：故障容错时间间隔（FTTI）的确定方法参考附录 C。
---	-------------------	---------	--

附录 B

（资料性附录）

以动力蓄电池系统为相关项的危害分析和风险评估（HARA）示例

B.1 相关项定义

B.1.1 功能概念

B.1.1.1 提供放电

动力蓄电池系统向整车设备及外部设施提供能量。

B.1.1.2 提供充电

动力蓄电池系统从整车或整车外部吸收能量，包括从充电机吸收能量及整车制动能量回收等。

B.1.2 动力蓄电池系统的边界和接口

按照GB/T 34590.3的5.4.2的要求，定义动力蓄电池系统相关项与其他相关项的功能边界及相互接口。

示例：图B.1为动力蓄电池系统相关项的边界和接口示例，动力蓄电池系统为高压系统（>60V），包括电池、继电器及电池管理系统等元素，并与外部充电装置与驱动装置进行交互。动力蓄电池系统接口包括了两个高压接口与唤醒信号、整车通信、充电通信以及电源等低压接口。

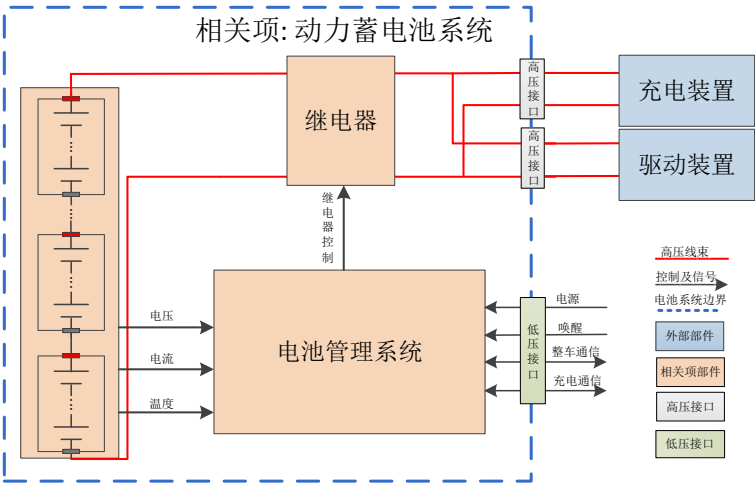


图 B.1 动力蓄电池系统相关项的边界和接口参考示例

B.2 相关项在整车层面上的危害识别

B.2.1 识别动力蓄电池系统的功能异常表现

按照GB/T 34590.3第6章的要求，应用危害与可操作性分析（HAZOP）方法识别动力蓄电池系统的功能异常表现，参见表B.1。

表 B.1 HAZOP 分析示例

引导词 功能	功 能 丧失	在有需求时，提供错误的功能			非 预 期 的 功 能 (在 无 需求时， 提 供 功 能)	输出卡滞在固定 值上（功能不能 按照需求更新）
		错误的功能（多于预期）	错误的功能（少于预期）	错 误 的 功能（方 向相反）		
提供放电 （温度、电 压、电流）	放 电 功 能 丧失	放电量大于预期； 电池放电时温度大于 预期； 放电电流大于预期。	放电量小于预期； 电池放电时温度小于 预期； 放电电流小于预期。	NA	非 预 期 放电	放电电流卡滞在 较高值； 放电电流卡滞在 较低值。
提供充电 （温度、电 压、电流）	充 电 功 能 丧失	充电量大于预期； 电池充电时温度大于 预期； 充电电流大于预期。	充电量小于预期； 电池充电时温度小于 预期； 充电电流小于预期； 电池电压小于预期时 充电。	NA	非 预 期 充电	充电电流卡滞在 较高值； 充电电流卡滞在 较低值。

B. 2. 2 分析动力蓄电池系统的功能异常表现导致的整车层面危害

按照GB/T 34590. 3第6章的要求，根据B. 2. 1中动力蓄电池系统的功能异常表现，分析可能导致的整车层面危害（最严重的情况），参见表B. 2。

表B. 2 整车层面危害（最严重的情况）

动力蓄电池系统功能异常表现的影响	整车层面的危害（最严重的情况）
放电量大于预期，造成动力蓄电池系统过放并损坏。	动力电池损坏报废，车辆丧失动力
电池放电时温度大于预期，造成动力蓄电池系统过温，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
放电电流大于预期，造成动力蓄电池系统过流，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
充电量大于预期，造成动力蓄电池系统过充，引发热失控	车辆冒烟、起火、爆炸、释放有害物质

电池充电时温度大于预期，造成动力蓄电池系统过温，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
充电电流大于预期，造成动力蓄电池系统过流，引发热失控	车辆冒烟、起火、爆炸、释放有害物质
电池电压小于预期时充电，引发热失控	车辆冒烟、起火、爆炸、释放有害物质

B.3 场景分析

根据第5章运行条件和环境约束要求，分析典型的车辆运行场景，参见表B.3。

表B.3 典型的车辆运行场景示例

	场景编号	典型场景
车辆状态	1	正常行驶（高速行驶，城市路况，转弯等）
	2	车辆静止无人看管充电
	3	车辆静止无人看管放电
	4	车辆长期静置
	5	碰撞（发生碰撞，碰撞之后）
	6	维修

B.4 ASIL 等级的导出

以动力蓄电池系统为相关项开展典型危害的危害分析和风险评估（HARA），并确定危害事件的ASIL等级。分析过程参见表B.4：

表B.4 危害分析和风险评估示例

危害	功能	功能异常表现	整车层面的危害	假设	危害的详细描述	危害事件	ASIL	备注
----	----	--------	---------	----	---------	------	------	----

							S	理由	E	理由	C	理由	A S I L	
HZD_01	提供放电功能	放电量大于预期	动力电池损坏报废，车辆动力丧失	无	电池过放，造成动力电池损坏报废，车辆动力丧失	车辆正常行驶（高速行驶，城市路况，转弯），放电量大于预期，导致电池损坏报废，车辆动力丧失，与后车发生追尾碰撞。	1	车辆动力丧失导致的追尾，引起驾驶员轻度或者中度的伤害	4	平均运行时间>10%	1	无危害，人员较大可能逃离	QM	
HZD_02	提供放电功能	电池系统放电时温度大于预期	车辆冒烟、起火、爆炸、释放有害物质	无	电池放电过温—热失控—冒烟、起火、爆炸、释放有害物质—人员伤亡	车辆正常行驶（高速行驶，城市路况，转弯），放电时温度大于预期，导致电池过温，引发热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及乘客和行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间>10%	2	有泄气，冒烟等预兆，人可逃离	C	
HZD_03	提供放电功能	放电电流大于预期	车辆冒烟、起火、爆炸、释放有害物质	无	电池充电过流—热失控—冒烟、起火、爆炸、释放有害物质—人员伤亡	车辆正常行驶（高速行驶，城市路况，转弯），放电时温度大于预期，导致电池过温，引发热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及乘客和行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间>10%	2	有泄气，冒烟等预兆，人可逃离	C	
HZD_04	提供充电功能	充电量大于预期	车辆冒烟、起火、爆炸、释放有害物质	无	电池过充—热失控—冒烟、起火、爆炸、释放有害物质—人员伤亡	车辆静止无人看管充电，充电时充电量大于预期，导致电池过充，引发热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间>10%	2	一般无严重后果，人员可逃生	C	

HZD_05	提供充电功能	电池充电时温度大于预期	车辆冒烟、起火、爆炸、释放有害物质	无	电池充电过温—热失控—冒烟、起火、爆炸、释放有害物质—人员伤亡	车辆静止无人看管充电，充电时电池温度大于预期，导致电池过温，引发热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间>10%	2	有泄气，冒烟等预兆，人可逃离	C	
HZD_06	提供充电功能	充电电流大于预期	车辆冒烟、起火、爆炸、释放有害物质	无	电池充电过流—热失控—冒烟、起火、爆炸、释放有害物质—人员伤亡	车辆静止无人看管充电，充电时电池电流大于预期，导致电池过流，引发热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间>10%	2	有泄气，冒烟等预兆，人可逃离	C	
HZD_07	提供充电功能	电池电压小于预期时充电	车辆冒烟、起火、爆炸、释放有害物质	无	电池过放后充电—热失控—冒烟、起火、爆炸、释放有害物质—人员伤亡	车辆静止无人看管充电，充电时电池电压小于预期时充电，引发热失控，车辆冒烟、起火、爆炸、释放有害物质，伤及行人。	3	热失控起火，爆炸或产生有害物质造成人员伤亡	4	平均运行时间>10%	2	有泄气，冒烟等预兆，人可逃离	C	

B.5 安全目标及安全状态

对于表B.4中具有ASIL等级的危害事件确定安全目标和安全状态，参见表B.5。

表B.5 安全目标及安全状态

序号	安全目标	安全状态	FTTI
1	防止电池单体过充导致热失控。	断开高压回路。	电池单体过充故障容错时间间隔应根据电池系统制造商过充测试结果给出。 注：故障容错时间间隔（FTTI）的确定方法参考附录C。
2	防止电池单体过放后再充电导致热失控。	断开充电回路。	电池单体过放后再充电故障容错时间间隔应根据电池系统制造商过放后再充电的测试结果给出。 注：故障容错时间间隔（FTTI）的确定方法参考附录C。
3	防止电池单体过温导致热失控。	断开高压回路。	电池单体过温故障容错时间间隔应根据电池系统制造商过温的测试结果给出。

			注：故障容错时间间隔（FTTI）的确定方法参考附录C。
4	防止动力蓄电池系统过流导致热失控。	断开高压回路。	动力蓄电池系统过流故障容错时间间隔应根据电池系统制造商过流测试结果给出。 注：故障容错时间间隔（FTTI）的确定方法参考附录C。

附录 C

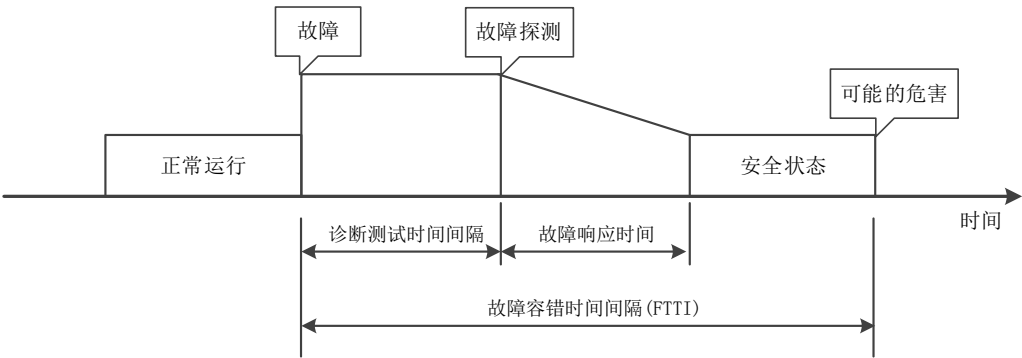
(资料性附录)

故障容错时间间隔（FTTI）确定方法示例

C.1 故障容错时间间隔的定义说明

故障容错时间间隔（以下简称FTTI）指在安全机制未被激活情况下，从相关项内部故障发生到可能发生危害事件的最短时间间隔, 如图C. 1所示。

以动力蓄电池系统为例,FTTI为从故障发生到蓄电池系统产生不可接受的危害的最短时间间隔。例如，电池单体从过充故障发生到电池单体发生热失控的最短时间间隔。



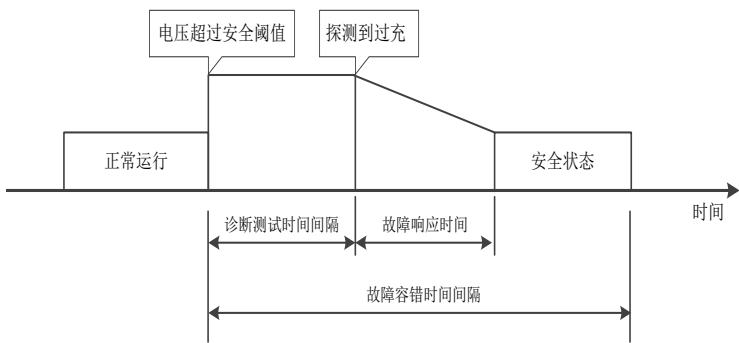
图C. 1 故障容错时间间隔

如图C. 1所示，在定义蓄电池系统的FTTI时，需要明确以下几点：

- 1) FTTI需要在动力蓄电池系统层面来定义；
- 2) FTTI与故障判定阈值紧密相关，应综合考虑FTTI与故障判定阈值之间的关系；
- 3) 故障指违背安全阈值，例如，过充故障发生意味着过充安全阈值被违背；
- 4) 可能的危害是不能接受的动力蓄电池系统危害，危害必须是明确的且可识别的，可由整车厂和制造商协商确定，如泄气、漏液等；
- 5) 从故障发生到产生危害的时间之内，蓄电池系统应以最严苛情况或整车厂和制造商确认的工况运行；

C.2 过充故障FTTI定义示例

本附录给出电池单体过充故障FTTI的确定方法及过程示例，示意图如图C. 2所示。



图C.2 电池单体过充故障容错时间间隔（FTTI）

C.2.1 确定过充安全阈值

安全阈值的确定需要考虑电池电芯的安全属性，违背该阈值意味着此时电芯在内部已经发生了不可逆反应，同时需要大于等于相关标准中规定的过充要求（例如120%SOC）。

示例：如根据电芯的测试数据，在过充到4.5V时电芯内产生不可逆反应，可以将4.5定为过充安全阈值。

C.2.2 确定可能的危害

整车厂和制造商应确定危害事件和危害事件的判定条件。

示例：可参考表C.1中对电池危害的等级划分。本示例以发生泄气作为危害事件的示例进行说明。

表C.1 危害等级示例

危害等级	描述	判定标准及影响
0	无影响	无影响，无功能丢失
1	被动保护开启	无影响；无漏夜；无泄气，无起火或火苗；无断裂；无爆炸；无放热反应或热失控。 电芯发生可逆的损坏，需要修复保护装置。
2	损坏	无漏夜；无泄气，无起火或火苗；无断裂；无爆炸；无放热反应或热失控。 电芯发生不可逆的损坏，需要维护。
3	漏夜 Δ Mass<50%	无泄气，无起火或火苗；无断裂；无爆炸。 电解液质量丢失<50%
4	泄气	无起火或火苗；无断裂；无爆炸。 电解液质量丢失>50%

5	起火或火苗	无断裂；无爆炸（例如，无飞出的部分）
6	断裂	无爆炸，但是部分部件分出
7	爆炸	爆炸（例如，电芯解体）

C.2.3 确定最严苛工况

整车厂与制造商确定最严苛的充电工况，在该工况下，电芯会在最短的时间内发生上述的危害事件。

假设最严苛工况确定如下：

- 1) 蓄电池系统温度为最高可使用温度，如65℃；
- 2) 充电电流为最高可允许充电电流，如200A；
- 3) 电池处于整车厂与制造商共同确定的健康状态，如80% EOL阶段；
- 4) 蓄电池充电状态为：标准充电至4.5V；
- 5) 其它条件与HARA中分析保持一致。

C.2.4 FTTI测试

按照C2.3中最严苛工况对蓄电池系统进行充电，要求如下：

- 1) 充电对象为动力蓄电池系统；
- 2) 在试验中，影响测试对象功能并与试验结果相关的所有保护设备（包括其他措施及外部措施）都应处于关闭状态；
- 3) 蓄电池系统应处于与HARA中假设的环境条件中；
- 4) 蓄电池系统应处于整车厂与制造商共同确定的健康状态；
- 5) 按照设定的最高充电电流200A对电池系统进行充电；
- 6) 测试应对单体电压进行监控；
- 7) 记录从充电开始到发生泄气的时间T；
- 8) 在试验结束后，应放置观察1h，确认无更严重的危害发生。

C.2.5 FTTI确定

理论上可以将测得从安全阈值违背到发生泄气时间T作为FTTI，但实际上考虑到电芯热失控反应是一个渐进的过程以及测试可能存在的误差，应在测得时间T的基础上留出一定余度，如 $FTTI=KT$ ， $0<K<1$ 。

在确定了FTTI后，重复C.2.4的试验过程，验证在该FTTI时间内，动力蓄电池系统无泄气发生。