ICS 43.040
CCS T35

中华人民共和国国家标准

GB/T XXXXX—XXXX

电动汽车用驱动电机系统功能安全要求及试验方法

Functional safety requirements and testing methods for drive motor system of electric vehicles

（征求意见稿）

（本草案完成时间：2022 年 3 月 20 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

本文件起草单位：

本文件主要起草人：

电动汽车用驱动电机系统功能安全要求及试验方法

1 范围

本文件规定了电动汽车用驱动电机系统（以下简称“驱动电机系统”）的功能安全要求及试验方法。

本文件适用于电动汽车用驱动电机系统，其他类型的驱动电机系统可参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34590-XXXX（所有部分） 道路车辆 功能安全（ISO 26262:2018，MOD）

GB/T 18488-XXXX 电动汽车用驱动电机系统

GB 18384-2020 电动汽车安全要求

3 术语和定义

GB/T 34590.1-XXXX界定的以及下列术语和定义适用于本文件。

3.1

驱动电机系统 drive motor system

安装在电动汽车上，为车辆行驶提供驱动力、实现机械能与电能间相互转化的系统。

[来源：GB/T 18488—XXXX，X.X.X]

3.2

驱动电机 drive motor

将电能转换成机械能为车辆行驶提供驱动力的电气装置，该装置也可具备机械能转化成电能的功能。

[来源：GB/T 18488—XXXX，X.X.X]

3.3

驱动电机控制器 drive motor controller

控制动力电源与驱动电机之间能量传输的装置，由控制信号接口电路、驱动电机控制电路和驱动电路组成。

[来源：GB/T 18488—XXXX，X.X.X]

4 一般要求

除非特别说明，驱动电机系统功能安全技术开发、流程开发等要求应参照GB/T 34590-XXXX（所有部分）执行。

5 相关项定义

5.1 总则

应按照GB/T 34590.3-XXXX的要求进行相关项定义，相关项指实现整车层面功能或部分功能的系统或系统组合。

注：相关项及其范围可根据具体情况定义。附录A给出了以驱动电机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

驱动电机系统的功能性要求还应满足GB/T 18488-XXXX、GB 18384-2020。

注：附录A给出了驱动电机系统输出驱动转矩、输出制动转矩的功能概念描述。

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）：

a) 外部环境，例如：温度、湿度、路况、天气等；
b) 驱动电机系统处于驱动模式、制动模式、待机模式等，或者驱动电机系统处于工作状态或者非工作状态；
c) 相关项与整车其他相关项的依赖关系、接口关系等。

6 危害分析和风险评估

6.1 总则

根据第5章相关项定义，按照GB/T 34590.3-XXXX，基于车辆使用场景，分析识别驱动电机系统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：以驱动电机系统为相关项进行危害分析和风险评估的示例见附录A。

6.2 安全目标

通过危害分析和风险评估确定的驱动电机系统的安全目标及其属性，应至少包含表1所列的内容。

表 1 驱动电机系统的安全目标及其属性

序号	安全目标	ASIL	安全状态	FTTI
1	防止电机无法输出驱动转矩	A	发出警示	见7.1.3
2	防止电机非预期的输出驱动转矩过大	C	发出警示，终止转矩输出	见7.2.3
3	防止电机转矩输出方向反向	C	发出警示，终止转矩输出	见7.3.3
4	防止电机非预期的输出驱动转矩	C	发出警示，终止转矩输出	见7.4.3
5	防止电机无法输出制动转矩	A	发出警示	见7.5.3
6	防止电机非预期的输出制动转矩过大	C	发出警示，终止转矩输出	见7.6.3
7	防止电机非预期的输出制动转矩	C	发出警示，终止转矩输出	见7.7.3

如果出现与表1所列的要求不一致的情况，应具备相应的证据来证明驱动电机系统不会因功能异常表现而导致不合理的整车危害风险。应至少包括如下证据：

a) 全部整车危害风险已被考虑，并制定了合理的安全目标；
b) 所制定的安全目标针对目标市场是适用和充分的。

7 功能安全要求

7.1 防止电机无法输出驱动转矩

7.1.1 一般要求

整车控制器（VCU或其他控制器，取决于整车电子架构）应确保发送给驱动电机控制器（MCU）的工作模式请求、转矩指令等信号的正确性和完整性。

驱动电机系统应检测这些信号的正确性和完整性，当检测到异常时，驱动电机系统应执行合理的故障处理来避免违背安全目标。

驱动电机系统应避免无法输出驱动转矩，除非对应故障将导致更严重的整车危害。

当驱动电机系统输出驱动转矩低于安全阈值时，驱动电机系统应在故障容错时间间隔（FTTI）内进入安全状态，当相关故障退出或消除条件未满足时，不应退出安全状态。

注：无法输出驱动转矩的安全阈值可以由最大加速能力、可达到最高车速等整车参数指标推导得出，可由整车制造商与驱动电机系统供应商协商确认。

故障探测、响应、处理应在FTTI时间内完成。

7.1.2 运行模式

驱动电机系统应处于驱动工作状态。

7.1.3 故障容错时间间隔（FTTI）

无法输出驱动转矩的故障容错时间间隔，如图1所示，应根据分析、测试等方式给出。

注1：无法输出驱动转矩的故障容错时间间隔的确定方法见附录B。

注2：无法输出驱动转矩的故障容错时间间隔由整车制造商与驱动电机系统供应商协商确认。

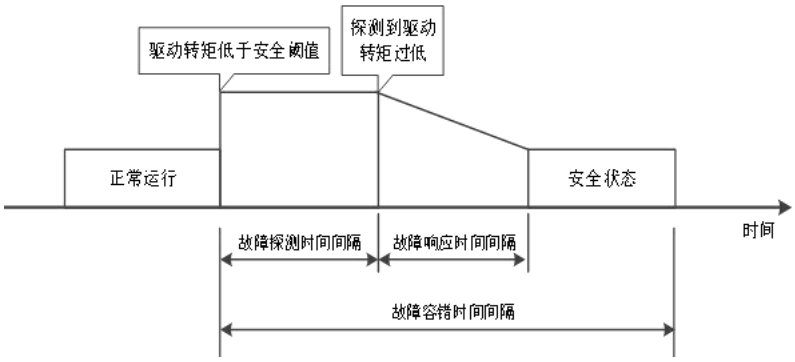

图 1 无法输出驱动转矩的故障容错时间间隔

7.1.4 安全状态的进入和退出

当确认无法输出驱动转矩的相关故障发生时，驱动电机系统通过警示驾驶员来进入安全状态，在无法输出驱动转矩相关故障退出或消除条件未满足时，不应退出安全状态。

注：故障退出或消除条件由整车制造商与驱动电机系统供应商协商确定。

7.1.5 报警和降级概念

当无法输出驱动转矩的相关故障发生时，驱动电机系统应反馈故障标志和原因等信息，用于整车实现驾驶员警告功能。

7.2 防止电机非预期的输出驱动转矩过大

7.2.1 一般要求

整车控制器（VCU或其他控制器，取决于整车电子架构）应确保发送给驱动电机控制器（MCU）的工作模式请求、转矩指令等信号的正确性和完整性。

驱动电机系统应检测这些信号的正确性和完整性，当检测到异常时，驱动电机系统应执行合理的故障处理来避免违背安全目标。

当驱动电机系统非预期输出的驱动转矩高于安全阈值时，驱动电机系统应在FTTI时间内进入安全状态，当相关故障退出或消除条件未满足时，不应退出安全状态。

注：非预期输出的驱动转矩过大的安全阈值可以由最大加速能力、可达到最高车速等整车参数指标推导得出，可由整车制造商与驱动电机系统供应商协商确认。

故障探测、响应、处理应在FTTI时间内完成。

7.2.2 运行模式

驱动电机系统应处于工作状态。

7.2.3 故障容错时间间隔（FTTI）

非预期的输出驱动转矩过大的故障容错时间间隔，如图2所示，应根据分析、测试等方式给出。

注：非预期的输出驱动转矩过大的故障容错时间间隔由整车制造商与驱动电机系统供应商协商确认。

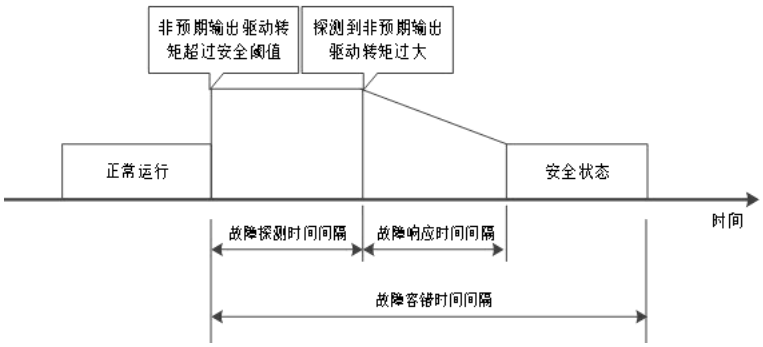

图 2 非预期的输出驱动转矩过大的故障容错时间间隔

7.2.4 安全状态的进入和退出

当确认非预期的输出驱动转矩过大的相关故障发生时，驱动电机系统应通过警示驾驶员并终止转矩输出来进入安全状态，在非预期的输出驱动转矩过大相关故障退出或消除条件未满足时，不应退出安全状态。

注：故障退出或消除条件由整车制造商与驱动电机系统供应商协商确定。

7.2.5 报警和降级概念

当非预期的输出驱动转矩过大相关故障发生时，在保证FTTI时间内进入安全状态的前提下，可进行转矩降额等处理；驱动电机系统应反馈故障标志和原因等信息，用于整车实现驾驶员警告功能。

7.3 防止电机转矩输出方向反向

7.3.1 一般要求

整车控制器（VCU或其他控制器，取决于整车电子架构）应确保发送给驱动电机控制器（MCU）的工作模式请求、转矩指令等信号的正确性和完整性。

驱动电机系统应检测这些信号的正确性和完整性，当检测到异常时，驱动电机系统应执行合理的故障处理来避免违背安全目标。

当驱动电机系统输出转矩方向与请求方向相反时，驱动电机系统应在FTTI时间内进入安全状态，当相关故障退出或消除条件未满足时，不应退出安全状态。

故障探测、响应、处理应在FTTI时间内完成。

7.3.2 运行模式

驱动电机系统应处于工作状态。

7.3.3 故障容错时间间隔（FTTI）

驱动电机输出转矩方向反向的故障容错时间间隔，如图3所示，应根据分析、测试等方式给出。

注：驱动电机输出转矩方向反向的故障容错时间间隔由整车制造商与驱动电机系统供应商协商确认。

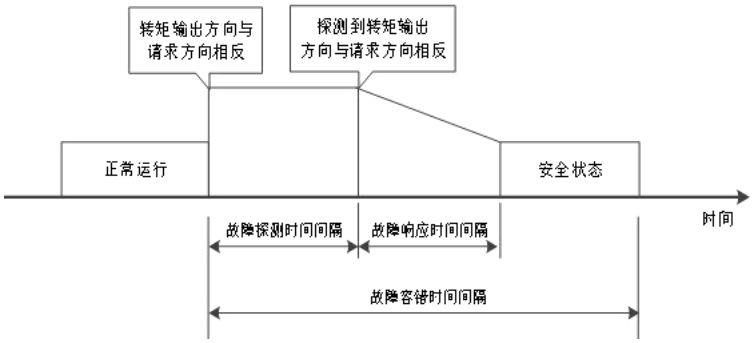

图 3 驱动电机输出转矩方向反向的故障容错时间间隔

7.3.4 安全状态的进入和退出

当确认驱动电机输出转矩方向反向的相关故障发生时，驱动电机系统通过警示驾驶员并终止转矩输出来进入安全状态，在驱动电机输出转矩方向反向相关故障退出或消除条件未满足时，不应退出安全状态。

注：故障退出或消除条件由整车制造商与驱动电机系统供应商协商确定。

7.3.5 报警和降级概念

当驱动电机输出转矩方向反向的相关故障发生时，驱动电机系统应反馈故障标志和原因等信息，用于整车实现驾驶员警告功能。

7.4 防止电机非预期的输出驱动转矩

7.4.1 一般要求

整车控制器（VCU或其他控制器，取决于整车电子架构）应确保发送给驱动电机控制器（MCU）的工作模式请求、转矩指令等信号的正确性和完整性。

驱动电机系统应检测这些信号的正确性和完整性，当检测到异常时，驱动电机系统应执行合理的故障处理来避免违背安全目标。

当驱动电机系统非预期输出的驱动转矩高于安全阈值时，驱动电机系统应在FTTI时间内进入安全状态，当相关故障退出或消除条件未满足时，不应退出安全状态。

注：非预期输出驱动转矩的安全阈值可以由最大加速能力、可达到最高车速等整车参数指标推导得出，可由整车制造商与驱动电机系统供应商协商确认。

故障探测、响应、处理应在FTTI时间内完成。

7.4.2 运行模式

驱动电机系统应处于非驱动工作状态且车辆处于静止状态。

7.4.3 故障容错时间间隔（FTTI）

非预期输出驱动转矩的故障容错时间间隔，如图4所示，应根据分析、测试等方式给出。

注：非预期输出驱动转矩的故障容错时间间隔由整车制造商与驱动电机系统供应商协商确认。

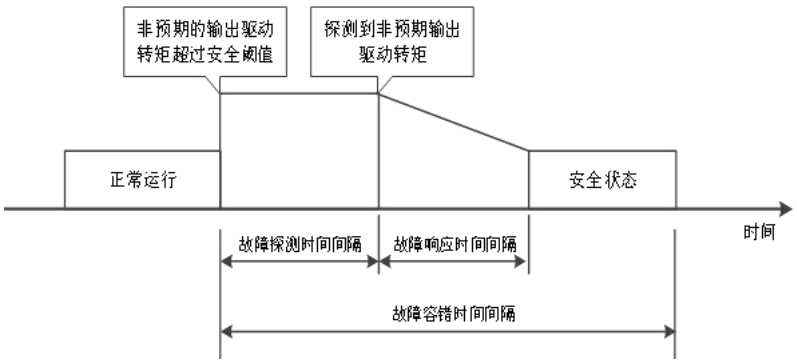

图 4 非预期输出驱动转矩的故障容错时间间隔

7.4.4 安全状态的进入和退出

当确认非预期输出驱动转矩的相关故障发生时，驱动电机系统通过警示驾驶员并终止转矩输出来进入安全状态，在非预期输出驱动转矩相关故障退出或消除条件未满足时，不应退出安全状态。

注：故障退出或消除条件由整车制造商与驱动电机系统供应商协商确定。

7.4.5 报警和降级概念

当非预期输出驱动转矩的相关故障发生时，驱动电机系统应反馈故障标志和原因等信息，用于整车实现驾驶员警告功能。

7.5 防止电机无法输出制动转矩

7.5.1 一般要求

整车控制器（VCU或其他控制器，取决于整车电子架构）应确保发送给驱动电机控制器（MCU）的工作模式请求、转矩指令等信号的正确性和完整性。

驱动电机系统应检测这些信号的正确性和完整性，当检测到异常时，驱动电机系统应执行合理的故障处理来避免违背安全目标。

驱动电机系统应避免无法输出制动转矩，除非对应故障将导致更严重的整车危害。

当驱动电机系统输出制动转矩低于安全阈值时，驱动电机系统应在FTTI时间内进入安全状态，当相关故障退出或消除条件未满足时，不应退出安全状态。

注：无法输出制动转矩的安全阈值可以由最大制动能力等整车参数指标推导得出，可由整车制造商与驱动电机系统供应商协商确认。

故障探测、响应、处理应在FTTI时间内完成。

7.5.2 运行模式

驱动电机系统应处于工作状态。

7.5.3 故障容错时间间隔（FTTI）

无法输出制动转矩的故障容错时间间隔，如图5所示，应根据分析、测试等方式给出。

注：无法输出制动转矩的故障容错时间间隔由整车制造商与驱动电机系统供应商协商确认。

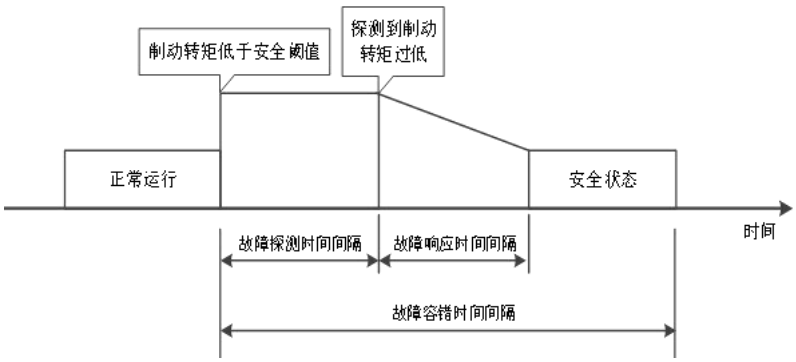

图 5 无法输出制动转矩的故障容错时间间隔

7.5.4 安全状态的进入和退出

当确认无法输出制动转矩的相关故障发生时，驱动电机系统通过警示驾驶员来进入安全状态，在无法输出制动转矩相关故障退出或消除条件未满足时，不应退出安全状态。

注：故障退出或消除条件由整车制造商与驱动电机系统供应商协商确定。

7.5.5 报警和降级概念

当无法输出制动转矩的相关故障发生时，驱动电机系统应反馈故障标志和原因等信息，用于整车实现驾驶员警告功能。

7.6 防止电机非预期的输出制动转矩过大

7.6.1 一般要求

整车控制器（VCU或其他控制器，取决于整车电子架构）应确保发送给驱动电机控制器（MCU）的工作模式请求、转矩指令等信号的正确性和完整性。

驱动电机系统应检测这些信号的正确性和完整性，当检测到异常时，驱动电机系统应执行合理的故障处理来避免违背安全目标。

当驱动电机系统非预期输出过大的制动转矩高于安全阈值时，驱动电机系统应在FTTI时间内进入安全状态，当相关故障退出或消除条件未满足时，不应退出安全状态。

注：非预期的输出制动转矩过大的安全阈值可以由整车质量、运行车速等整车参数指标推导得出，可由整车制造商

与驱动电机系统供应商协商确认。

故障探测、响应、处理应在FTTI时间内完成。

7.6.2 运行模式

驱动电机系统应处于工作状态。

7.6.3 故障容错时间间隔（FTTI）

非预期的输出制动转矩过大的故障容错时间间隔，如图6所示，应根据分析、测试等方式给出。

注：非预期的输出制动转矩过大的故障容错时间间隔由整车制造商与驱动电机系统供应商协商确认。

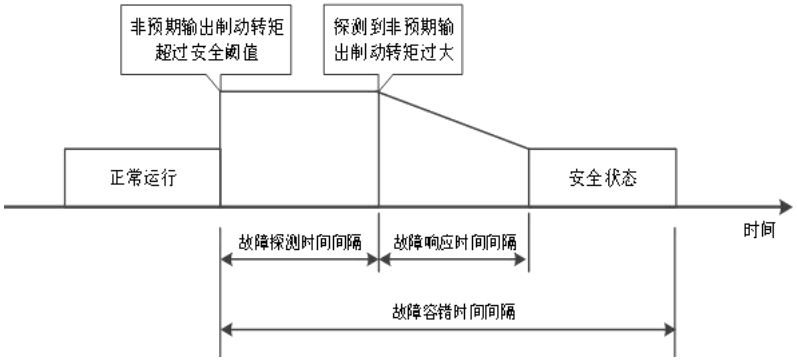

图 6 非预期的输出制动转矩过大的故障容错时间间隔

7.6.4 安全状态的进入和退出

当确认非预期的输出制动转矩过大的相关故障发生时，驱动电机系统应通过警示驾驶员并终止转矩输出来进入安全状态，在非预期的输出制动转矩过大相关故障退出或消除条件未满足时，不应退出安全状态。

注：故障退出或消除条件由整车制造商与驱动电机系统供应商协商确定。

7.6.5 报警和降级概念

当非预期的输出制动转矩过大相关故障发生时，在保证FTTI时间内进入安全状态的前提下，可进行制动转矩降额等处理；驱动电机系统应反馈故障标志和原因等信息，用于整车实现驾驶员警告功能。

7.7 防止电机非预期的输出制动转矩

7.7.1 一般要求

整车控制器（VCU或其他控制器，取决于整车电子架构）应确保发送给驱动电机控制器（MCU）的工作模式请求、转矩指令等信号的正确性和完整性。

驱动电机系统应检测这些信号的正确性和完整性，当检测到异常时，驱动电机系统应执行合理的故障处理来避免违背安全目标。

当驱动电机系统非预期输出的制动转矩高于安全阈值时，驱动电机系统应在FTTI时间内进入安全状态，当相关故障退出或消除条件未满足时，不应退出安全状态。

注：非预期的输出制动转矩的安全阈值可以由最大加速能力、可达到最高车速等整车参数指标推导得出，可由整车制造商与驱动电机系统供应商协商确认。

故障探测、响应、处理应在FTTI时间内完成。

7.7.2 运行模式

驱动电机系统应处于非制动工作状态且车辆处于静止状态。

7.7.3 故障容错时间间隔（FTTI）

非预期输出制动转矩的故障容错时间间隔，如图7所示，应根据分析、测试等方式给出。

注：非预期输出制动转矩的故障容错时间间隔由整车制造商与驱动电机系统供应商协商确认。

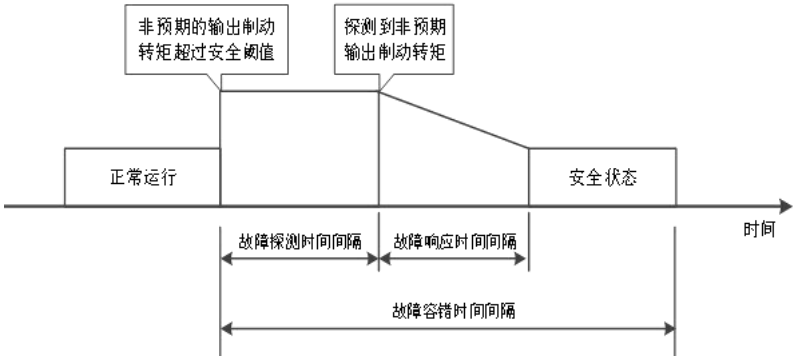

图 7 非预期输出制动转矩的故障容错时间间隔

7.7.4 安全状态的进入和退出

当确认非预期输出制动转矩的相关故障发生时，驱动电机系统通过警示驾驶员并终止转矩输出来进入安全状态，在非预期输出制动转矩相关故障退出或消除条件未满足时，不应退出安全状态。

注：故障退出或消除条件由整车制造商与驱动电机系统供应商协商确定。

7.7.5 报警和降级概念

当非预期输出制动转矩的相关故障发生时，驱动电机系统应反馈故障标志和原因等信息，用于整车实现驾驶员警告功能。

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，应在驱动电机系统层面进行验证，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。

本文件中主要给出基于测试的功能安全验证方法，测试可在模拟环境下进行。真实环境下的测试，本文件不作具体要求。

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功能减轻或避免危害事件的发生。应在驱动电机系统或整车层面对功能安全目标的实现进行确认，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。

8.2 功能安全验证

8.2.1 防止电机无法输出驱动转矩

8.2.1.1 测试目的

驱动电机系统应检测输出转矩状态，当输出驱动转矩低于安全阈值时，使驱动电机系统在FTTI时间内进入安全状态，在无法输出驱动转矩的故障退出或消除条件未满足时，不应退出安全状态。

8.2.1.2 测试对象

测试对象为驱动电机系统。

8.2.1.3 测试要求

模拟环境下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 规定的运行模式，所选择的测试工况点应至少包括电机在两个象限（驱动工况对应的两个象限）运行工况，且在每个象限内应选取典型的工作点，例如：低转矩和低转速、高转矩和高转速、低转矩和高转速等组合，以确保安全机制的有效性；
c) 应通过注入故障的方式进行测试，注入的故障会导致系统降级从而丢失驱动转矩；
d) 测试应使驱动电机系统进入安全状态，并发出报警信息；
e) 测试应对驱动电机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

当符合以下任一条件时，结束模拟环境下测试：

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未进入安全状态；
c) 测试对象未能发出正确的报警信息；
d) 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。

8.2.1.5 测试通过准则

测试通过准则应同时满足如下条件：

a) 测试对象在注入故障后进入安全状态，并无意外退出安全状态；且从注入故障到进入安全状态的时间间隔应小于或等于故障容错时间间隔要求；
b) 测试对象发出了正确的故障报警信息。

8.2.2 防止电机非预期的输出驱动转矩过大

8.2.2.1 测试目的

驱动电机系统应检测输出转矩状态，当电机非预期的输出过大的驱动转矩超过安全阈值时，使驱动电机系统在FTTI时间内进入安全状态，在非预期的输出过大的驱动转矩的故障退出或消除条件未满足时，不应退出安全状态。

8.2.2.2 测试对象

测试对象为驱动电机系统。

8.2.2.3 测试要求

模拟环境下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 规定的运行模式，所选择的测试工况点应包括电机在两个象限（驱动工况对应的两个象限）运行工况，且在每个象限内应选取典型的工作点，例如：低转矩和低转速、高转矩和高转速、低转矩和高转速等，以确保安全机制的有效性；
c) 应通过注入故障的方式进行测试，注入的故障所引起的非预期的输出驱动转矩值应至少包括低于安全阈值、达到安全阈值和高于安全阈值三个类型；
d) 测试应对驱动电机系统进入安全状态的过程（例如：安全阈值、时间、状态切换、报警信息）进行监控；
e) 测试应对驱动电机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

当符合以下任一条件时，结束模拟环境下测试：

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未进入安全状态；
c) 测试对象未能发出正确的报警信息；
d) 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。

8.2.2.5 测试通过准则

测试通过准则应同时满足如下条件：

a) 测试对象在注入故障后可以进入安全状态，并无意外退出安全状态；且从注入故障到进入安全状态的时间间隔应小于或等于故障容错时间间隔要求；
b) 测试对象进入安全状态时的转矩满足设计要求的安全阈值；
c) 测试对象发出了正确的故障报警信息。

8.2.3 防止电机转矩输出方向相反

8.2.3.1 测试目的

驱动电机系统应检测输出转矩状态，当电机转矩输出方向与请求方向相反时，使驱动电机系统在FTTI时间内进入安全状态，在电机转矩输出方向与请求方向相反的故障退出或消除条件未满足时，不应退出安全状态。

8.2.3.2 测试对象

测试对象为驱动电机系统。

8.2.3.3 测试要求

模拟环境下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 规定的运行模式，所选择的测试工况点应至少包括电机在四个象限运行工况，且在每个象限内应选取典型的工作点，例如：低转矩和低转速、高转矩和高转速、低转矩和高转速等组合，以确保安全机制的有效性；
c) 应通过注入故障的方式进行测试，注入的故障所引起的转矩反向安全阈值应至少包括低于安全阈值、达到安全阈值和高于安全阈值三个类型；

d) 测试应对驱动电机系统进入安全状态的过程（例如：安全阈值、时间、状态切换、报警信息）进行监控；
e) 测试应对驱动电机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

当符合以下任一条件时，结束模拟环境下测试：
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未进入安全状态；
c) 测试对象未能发出正确的报警信息；
d) 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。

8.2.3.5 测试通过准则

测试通过准则应同时满足如下条件：
a) 测试对象在注入故障后可以进入安全状态，并无意外退出安全状态；且从注入故障到进入安全状态的时间间隔应小于或等于故障容错时间间隔要求；
b) 测试对象进入安全状态时的转矩满足设计要求的安全阈值；
c) 测试对象发出了正确的故障报警信息。

8.2.4 防止电机非预期的输出驱动转矩

8.2.4.1 测试目的

驱动电机系统应检测输出转矩状态，当电机非预期的输出驱动转矩超过安全阈值时，使驱动电机系统在FTTI时间内进入安全状态，在非预期的输出驱动转矩的故障退出或消除条件未满足时，不应退出安全状态。

8.2.4.2 测试对象

测试对象为驱动电机系统。

8.2.4.3 测试要求

模拟环境下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 规定的运行模式，所选择的测试工况点应至少包括电机在四个象限运行工况，且在每个象限内应选取典型的工作点，例如：低转矩和低转速、高转矩和高转速、低转矩和高转速等组合，以确保安全机制的有效性；
c) 应通过注入故障的方式进行测试，注入的故障所引起的非预期输出驱动转矩的安全阈值应至少包括低于安全阈值、达到安全阈值和高于安全阈值三个类型；
d) 测试应对驱动电机系统进入安全状态的过程（例如：安全阈值、时间、状态切换、报警信息）进行监控；
e) 测试应对驱动电机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

当符合以下任一条件时，结束模拟环境下测试：
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未进入安全状态；
c） 测试对象未能发出正确的报警信息；
d） 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。

8.2.4.5 测试通过准则

测试通过准则应同时满足如下条件：
a） 测试对象在注入故障后可以进入安全状态，并无意外退出安全状态；且从注入故障到进入安全状态的时间间隔应小于或等于故障容错时间间隔要求；
b） 测试对象进入安全状态时的转矩满足设计要求的安全阈值；
c） 测试对象发出了正确的故障报警信息。

8.2.5 防止电机无法输出制动转矩

8.2.5.1 测试目的

驱动电机系统应检测输出转矩状态，当输出制动转矩低于安全阈值时，使驱动电机系统在FTTI时间内进入安全状态，在无法输出制动转矩的故障退出或消除条件未满足时，不应退出安全状态。

8.2.5.2 测试对象

测试对象为驱动电机系统。

8.2.5.3 测试要求

模拟环境下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 7.5.2 规定的运行模式，所选择的测试工况点应至少包括电机在两个象限（制动工况对应的两个象限）运行工况，且在每个象限内应选取典型的工作点，例如：低转矩和低转速、高转矩和高转速、低转矩和高转速等组合，以确保安全机制的有效性；
c） 应通过注入故障的方式进行测试，注入的故障会导致系统降级从而丢失制动转矩；
d） 测试应使驱动电机系统进入安全状态，并发出报警信息；
e） 测试应对驱动电机系统退出安全状态的条件进行监控。

8.2.5.4 测试结束条件

当符合以下任一条件时，结束模拟环境下测试：
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未进入安全状态；
c） 测试对象未能发出正确的报警信息；
d） 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。

8.2.5.5 测试通过准则

测试通过准则应同时满足如下条件：
a） 测试对象在注入故障后进入安全状态，并无意外退出安全状态；且从注入故障到进入安全状态的时间间隔应小于或等于故障容错时间间隔要求；
b） 测试对象发出了正确的故障报警信息。

8.2.6 防止电机非预期的输出制动转矩过大

8.2.6.1 测试目的

驱动电机系统应检测输出转矩状态，当输出制动转矩超过安全阈值时，使驱动电机系统在FTTI时间内进入安全状态，在非预期的输出制动转矩过大的故障退出或消除条件未满足时，不应退出安全状态。

8.2.6.2 测试对象

测试对象为驱动电机系统。

8.2.6.3 测试要求

模拟环境下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 7.6.2 规定的运行模式，所选择的测试工况点应包括电机在第二和第四象限运行工况，且在每个象限内应选取典型的工作点，例如：低转矩和低转速、高转矩和高转速、低转矩和高转速等，以确保安全机制的有效性；

注：制动定义为电机工作在第二和第四象限。

c) 应通过注入故障的方式进行测试，注入的故障所引起的非预期的输出制动转矩过大安全阈值应至少包括低于安全阈值、达到安全阈值和高于安全阈值三个类型；

d) 测试应对驱动电机系统进入安全状态的过程（例如：安全阈值、时间、状态切换、报警信息）进行监控；

e) 测试应对驱动电机系统退出安全状态的条件进行监控。

8.2.6.4 测试结束条件

当符合以下任一条件时，结束模拟环境下测试：

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未进入安全状态；

c) 测试对象未能发出正确的报警信息；

d) 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。

8.2.6.5 测试通过准则

测试通过准则应同时满足如下条件：

a) 测试对象在注入故障后可以进入安全状态，并无意外退出安全状态；且从注入故障到进入安全状态的时间间隔应小于或等于故障容错时间间隔要求；

b) 测试对象进入安全状态时的转矩满足设计要求的安全阈值；

c) 测试对象发出了正确的故障报警信息。

8.2.7 防止电机非预期的输出制动转矩

8.2.7.1 测试目的

驱动电机系统应检测输出转矩状态，当输出制动转矩超过安全阈值时，使驱动电机系统在FTTI时间内进入安全状态，在非预期的输出制动转矩的故障退出或消除条件未满足时，不应退出安全状态。

8.2.7.2 测试对象

测试对象为驱动电机系统。

8.2.7.3 测试要求

模拟环境下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 7.7.2 规定的运行模式，所选择的测试工况点应至少包括电机在四个象限运行工况，且在每个象限内应选取典型的工作点，例如：低转矩和低转速、高转矩和高转速、低转矩和高转速等组合，以确保安全机制的有效性；
c) 应通过注入故障的方式进行测试，注入的故障所引起的非预期输出制动转矩的安全阈值应至少包括低于安全阈值、达到安全阈值和高于安全阈值三个类型；
d) 测试应对驱动电机系统进入安全状态的过程（例如：安全阈值、时间、状态切换、报警信息）进行监控；
e) 测试应对驱动电机系统退出安全状态的条件进行监控。

8.2.7.4 测试结束条件

当符合以下任一条件时，结束模拟环境下测试：

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未进入安全状态；
c) 测试对象未能发出正确的报警信息；
d) 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。

8.2.7.5 测试通过准则

测试通过准则应同时满足如下条件：

a) 测试对象在注入故障后可以进入安全状态，并无意外退出安全状态；且从注入故障到进入安全状态的时间间隔应小于或等于故障容错时间间隔要求；
b) 测试对象进入安全状态时的转矩满足设计要求的安全阈值；
c) 测试对象发出了正确的故障报警信息。

8.3 功能安全确认

8.3.1 防止电机无法输出驱动转矩

8.3.1.1 目的

确认安全目标“防止电机无法输出驱动转矩”得到正确实现，并能够有效警示驾驶员关于电机无法输出驱动转矩导致车辆驱动力的丧失。

8.3.1.2 确认对象

确认对象为驱动电机系统。

8.3.1.3 确认要求

确认应满足如下要求：

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，至少包含真实的驱动电机系统，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，如不能输出驱动转矩。

d） 确认应对驱动电机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） 确认应对驱动电机系统的状态进行监控；

f） 确认应对驱动电机系统退出安全状态的条件进行监控。

8.3.1.4 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，并且警示驾驶员车辆处于驱动力丧失状态；

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。

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，并且警示驾驶员车辆处于驱动力丧失状态。

8.3.2 防止电机非预期的输出驱动转矩过大

8.3.2.1 目的

确认安全目标“防止电机非预期的输出驱动转矩过大”得到正确实现，并能够有效预防由于电机非预期的输出驱动转矩过大导致车辆加速度过大。

8.3.2.2 确认对象

确认对象为驱动电机系统。

8.3.2.3 确认要求

确认应满足如下要求：

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，至少包含真实的驱动电机系统，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，如电机非预期的输出驱动转矩过大。

d） 确认应对驱动电机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） 确认应对驱动电机系统的状态进行监控。

f） 确认应对驱动电机系统退出安全状态的条件进行监控。

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，且警示驾驶员车辆处于终止转矩输出状态；

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。

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，且警示驾驶员车辆处于终止转矩输出状态。

8.3.3 防止电机转矩输出方向反向

8.3.3.1 目的

确认安全目标“防止电机转矩输出方向反向”得到正确实现，并能够有效预防由于电机转矩输出方向反向导致车辆加速度方向相反。

8.3.3.2 确认对象

确认对象为驱动电机系统。

8.3.3.3 确认要求

确认应满足如下要求：

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，至少包含真实的驱动电机系统，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，如电机转矩输出方向反向。

d） 确认应对驱动电机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） 确认应对驱动电机系统的状态进行监控；

f） 确认应对驱动电机系统退出安全状态的条件进行监控。

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，并且警示驾驶员且车辆处于终止转矩输出状态；

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。

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，并且警示驾驶员且车辆处于终止转矩输出状态。

8.3.4 防止电机非预期的输出驱动转矩

8.3.4.1 目的

确认安全目标“防止电机非预期的输出驱动转矩”得到正确实现，并能够有效预防由于电机非预期的输出驱动转矩导致车辆从静止状态非预期启动、车辆非预期的加速。

8.3.4.2 确认对象

确认对象为驱动电机系统。

8.3.4.3 确认要求

确认应满足如下要求：

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，至少包含真实的驱动电机系统，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，如电机非预期的输出驱动转矩。

d) 确认应对驱动电机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) 确认应对驱动电机系统的状态进行监控；

f) 确认应对驱动电机系统退出安全状态的条件进行监控。

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，并且警示驾驶员且车辆处于终止转矩输出状态；

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。

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，并且警示驾驶员且车辆处于终止转矩输出状态。

8.3.5 防止电机无法输出制动转矩

8.3.5.1 目的

确认安全目标“防止电机无法输出制动转矩”得到正确实现，并能够有效预防由于电机无法输出制动转矩导致车辆制动力降低。

8.3.5.2 确认对象

确认对象为驱动电机系统。

8.3.5.3 确认要求

确认应满足如下要求：

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，至少包含真实的驱动电机系统，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，如电机无法输出制动转矩。

d） 确认应对驱动电机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） 确认应对驱动电机系统的状态进行监控；
f） 确认应对驱动电机系统退出安全状态的条件进行监控。

8.3.5.4 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，并且警示驾驶员车辆处于制动力降低状态；
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。

8.3.5.5 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，并且警示驾驶员车辆处于制动力降低状态。

8.3.6 防止电机非预期的输出制动转矩过大

8.3.6.1 目的

确认安全目标“防止电机非预期的输出制动转矩过大”得到正确实现，并能够有效预防由于电机非预期的输出制动转矩过大导致车辆减速度过大。

8.3.6.2 确认对象

确认对象为驱动电机系统。

8.3.6.3 确认要求

确认应满足如下要求：
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，至少包含真实的驱动电机系统，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，如电机非预期的输出制动转矩过大。

d） 确认应对驱动电机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） 确认应对驱动电机系统的状态进行监控；
f） 确认应对驱动电机系统退出安全状态的条件进行监控。

8.3.6.4 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，且警示驾驶员车辆处于终止转矩输出状态；
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。

8.3.6.5 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，且警示驾驶员车辆处于终止转矩输出状态。

8.3.7 防止电机非预期的输出制动转矩

8.3.7.1 目的

确认安全目标“防止电机非预期的输出制动转矩”得到正确实现，并能够有效预防由于电机非预期的输出制动转矩导致车辆非预期倒车。

8.3.7.2 确认对象

确认对象为驱动电机系统。

8.3.7.3 确认要求

确认应满足如下要求：

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，至少包含真实的驱动电机系统，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，如电机非预期的输出制动转矩。

d) 确认应对驱动电机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；确认应对驱动电机系统的状态进行监控；

e) 确认应对驱动电机系统退出安全状态的条件进行监控。

8.3.7.4 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，且警示驾驶员车辆处于终止转矩输出状态；

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。

8.3.7.5 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，且警示驾驶员车辆处于终止转矩输出状态。

附 录 A
（资料性）
以驱动电机系统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 输出驱动转矩

该功能旨在驱动电机控制器基于整车控制器给出的驱动转矩指令，结合驱动电机当前转速、负荷等状态控制驱动电机输出给定的驱动转矩。

A.1.1.2 输出制动转矩

该功能旨在驱动电机控制器基于整车控制器给出的制动转矩指令，结合驱动电机当前转速、负荷等状态控制驱动电机输出给定的制动转矩。

A.1.2 驱动电机系统的边界和接口

按照GB/T 34590.3-XXXX中5.4.2的要求，定义驱动电机系统相关项与其他相关项的边界和接口。

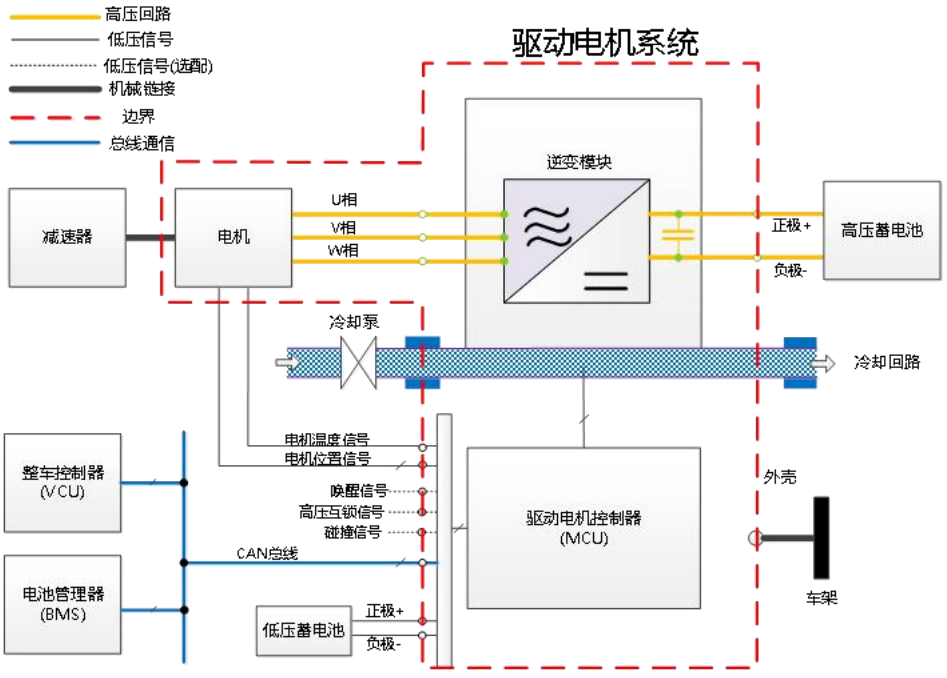

图 A.1 驱动电机系统相关项边界和接口参考示例

注1：图A.1中的示例所示系统为由蓄电池、电机控制器、电机和单减速器构成的动力总成系统，此系统可用于将电能转换为机械能驱动汽车行进的纯电动汽车，同时该动力总成系统具备制动能量回收功能。

注2：图A.1中的示例以搭载在A级乘用车上的驱动电机系统为例，其他车型可参考本附录示例进行分析。

注3：图A.1中的示例使用VCU作为独立的整车控制单元，接收油门、制动、档位等信息，并转换为所需要的转矩输出请求。该示例不考虑VCU与MCU集成等新型或特殊的整车控制架构形式。

注4：图A.1中的示例使用CAN通信作为驱动电机系统的通信形式为例，采用如CAN-FD、FlexRay等其他通信形式的车型可参考本文件。

注5：本附录中的电机仅以电动汽车常用的永磁同步电机为例，对使用如异步电机、电励磁同步电机等电机类型的车型可参考本附录分析。电机控制器的工作模式仅考虑转矩控制模式，不考虑转速控制和电压控制的工作模式。

A.2 相关项在整车层面上的危害识别

A.2.1 识别驱动电机系统的功能异常表现

按照GB/T 34590.3-XXXX第6章的要求，应用危害与可操作性分析（HAZOP）方法识别驱动电机系统的功能异常表现，见表A.1。

表 A.1 HAZOP 分析示例

功能	引导词					
	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）		
输出驱动转矩（含零转矩）	不能输出驱动转矩	实际输出驱动转矩大于期望值	实际输出驱动转矩小于期望值	输出转矩方向与期望值反向	非预期输出驱动转矩	输出转矩量无法更新
输出制动转矩	不能输出制动转矩	实际输出制动转矩大于期望值	实际输出制动转矩小于期望值	输出转矩方向与期望值反向	非预期输出制动转矩	输出转矩量无法更新

A.2.2 分析驱动电机系统的功能异常表现导致的整车层面危害

按照GB/T 34590.3-XXXX第6章的要求，根据A.2.1中驱动电机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），见表A.2。

表 A.2 整车层面危害（最严重的情况）

驱动电机系统功能异常表现的影响	整车层面的危害（最严重的情况）
不能输出驱动转矩	车辆驱动力丧失
实际输出驱动转矩大于期望值	车辆加速度过大
实际输出驱动转矩小于期望值	车辆加速能力不足
非预期输出驱动转矩	车辆从静止状态非预期启动、车辆非预期的加速
不能输出制动转矩	车辆制动力降低
实际输出制动转矩大于期望值	车辆减速度过大
实际输出制动转矩小于期望值	车辆制动力降低
非预期输出制动转矩	车辆非预期倒车
输出转矩方向与期望值反向	车辆加速度方向相反
输出转矩量无法更新	车辆非预期加、减速或车辆运动反向

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，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
1	正常行驶（高速路、城市或乡村道路、住宅区或人口密集区等）
2	超车行驶（高速路或城市多车道路、乡村或单车道路等）
3	转弯行驶（十字路口、匝道等）
4	静止起步（十字路口、停车场、坡道等）
5	高速匝道并入
6	坡道行驶（上下坡、坡道驻车等）

A.4 ASIL 等级的导出

以驱动电机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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
HZD_01_1a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	车辆在高速或城市多车道道路上超车运行时突然丢失动力（踩油门无响应），后方或侧方有车辆	在与后方或侧方车辆相对车速较小的情况下(ΔV＜20km/h)，与后方或侧方车辆发生碰撞	S1	碰撞时两车的相对速度偏低，可能造成驾驶员轻度或中度受伤，但不会危及生命	E4	正常驾驶过程中，前后车保持较低相对车速的持续时间大于10%平均驾驶时间	C1	由于丢失动力发生时前后车相对车速较低，大于99%驾驶员可以控制车辆减速或完成停车	QM
HZD_01_1b	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与后方或侧方车辆相对车速中等的情况下(20km/h≤ΔV≤40km/h)，与后方或侧方车辆发生碰撞	S2	碰撞时两车的相对速度中等，可能造成驾驶员较为严重的受伤，但不会危及生命	E3	正常驾驶过程中，前后车保持中等相对车速的持续时间在1%到10%平均驾驶时间内	C2	由于丢失动力发生时前后车相对车速中等，大于90%驾驶员可以控制车辆减速或完成停车	A
HZD_01_1c	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与后方或侧方车辆相对车速较高的情况下(ΔV＞40km/h)，与后方或侧方车辆发生碰撞	S3	碰撞时两辆车的相对速度较高，可能造成驾驶员较为严重的受伤，甚至危及生命	E2	正常驾驶过程中，前后车保持较高相对车速的持续时间小于1%平均驾驶时间	C2	由于丢失动力发生时前后车相对车速较高，大于90%驾驶员可以控制车辆减速或完成停车	A
HZD_01_2a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	车辆正常驾驶过程中突然丢失动力（踩油门无响应），后方有车辆跟随	在与后车相对车速较小的情况下(ΔV＜20km/h)，与后车发生碰撞	S1	碰撞时两辆车的相对速度偏低，可能造成驾驶员轻度或中度受伤，但不会危及生命	E4	正常驾驶过程中，前后车保持较低相对车速的持续时间大于10%平均驾驶时间	C1	由于丢失动力发生时前后车相对车速较低，大于99%驾驶员可以控制车辆减速或完成停车	QM
HZD_01_2b	输出驱动转矩	不能输出驱动	驱动力丧失	无		在与后车相对车速中等的情况下(20km/h≤ΔV≤	S2	碰撞时两辆车的相对速度中等，可能造成	E3	正常驾驶过程中，前后车保持中等相对车	C2	由于丢失动力发生时前后车相对车速	A

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
	（含零转矩）	转矩				40km/h），与后车发生碰撞		驾驶员较为严重的受伤，但不会危及生命		速的持续时间在1%到10%平均驾驶时间内		中等，大于90%驾驶员可以控制车辆减速或完成停车	
HZD_01_2c	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与后车相对车速较高的情况下（ΔV＞40km/h），与后车发生碰撞	S3	碰撞时两辆车的相对速度较高，可能造成驾驶员较为严重的受伤，甚至危及生命	E2	正常驾驶过程中，前后车保持较高相对车速的持续时间小于1%平均驾驶时间	C2	由于丢失动力发生时前后车相对车速较高，大于90%驾驶员可以控制车辆减速或完成停车	A
HZD_01_3a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	车辆在十字路口转向过程中突然丢失动力（踩油门无响应），对向有来车	对向车道车辆以相较于左转车辆较低的相对车速驶过路口（ΔV＜20km/h），左转车辆无法按照预期的速度通过对向车道，可能导致发生碰撞	S1	碰撞时两辆车的相对速度偏低，可能造成驾驶员轻度或中度受伤，但不会危及生命	E2	穿越十字路口左转，对向车辆与转弯车辆保持较低相对车速的持续时间小于1%平均驾驶时间	C1	由于丢失动力发生时对向车辆和左转车辆相对车速较低，大于99%驾驶员可以控制车辆减速或完成停车	QM
HZD_01_3b	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		对向车道车辆以相较于左转车辆中等的相对车速驶过路口（20km/h≤ΔV≤40km/h），左转车辆无法按照预期的速度通过对向车道，可能导致发生碰撞	S2	碰撞时两辆车的相对速度中等，可能造成驾驶员较为严重的受伤，但不会危及生命	E2	穿越十字路口左转，对向车辆与转弯车辆保持中等相对车速的持续时间小于1%平均驾驶时间	C2	由于丢失动力发生时对向车辆和左转车辆相对车速中等，大于90%驾驶员可以控制车辆减速或完成停车	QM
HZD_01_3c	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		对向车道车辆以相较于左转车辆较高的相对车速驶过路口（ΔV＞40km/h），左转车辆无法按照预期的速度通过对	S3	碰撞时两辆车的相对速度较高，可能造成驾驶员较为严重的受伤，甚至危及生命	E2	穿越十字路口左转，对向车辆与转弯车辆保持较高相对车速的持续时间小于1%平均	C1	由于丢失动力发生时前后车相对车速较高，大于99%驾驶员可以控制车辆减	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
						向车道，可能导致发生碰撞				驾驶时间		速或完成停车	
HZD_01_4a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	在城市或乡村道路借道超车运行时，在借道过程中突然丢失动力（踩油门无响应），对向车道有来车	在与对向车道车辆相对车速较小的情况下（ΔV＜20km/h），与对向车道车辆发生碰撞	S1	碰撞时两辆车的相对速度偏低，可能造成驾驶员轻度或中度受伤，但不会危及生命	E2	借道超车，对向车辆与借道车辆保持较低相对车速的持续时间小于1%平均驾驶时间	C1	由于丢失动力发生时对向车辆和左转车辆相对车速较低，大于99%驾驶员可以控制车辆减速或完成停车	QM
HZD_01_4b	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与对向车道车辆相对车速中等的情况下（20km/h≤ΔV≤40km/h），与对向车道车辆发生碰撞	S2	碰撞时两辆车的相对速度中等，可能造成驾驶员较为严重的受伤，但不会危及生命	E2	借道超车，对向车辆与借道车辆保持中等相对车速的持续时间小于1%平均驾驶时间	C2	由于丢失动力发生时对向车辆和左转车辆相对车速中等，大于90%驾驶员可以控制车辆减速或完成停车	QM
HZD_01_4c	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与对向车道车辆相对车速较高的情况下（ΔV＞40km/h），与对向车道车辆发生碰撞	S3	碰撞时两辆车的相对速度较高，可能造成驾驶员较为严重的受伤，甚至危及生命	E2	借道超车，对向车辆与借道车辆保持较高相对车速的持续时间小于1%平均驾驶时间	C2	由于丢失动力发生时对向车辆和左转车辆相对车速中等，大于90%驾驶员可以控制车辆减速或完成停车	A
HZD_01_5a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	在高速入口匝道并道过程中突然丢失动力（踩油门无响应），后方有来车	在与后车相对车速较小的情况下（ΔV＜20km/h），与后车发生碰撞	S1	碰撞时两辆车的相对速度偏低，可能造成驾驶员轻度或中度受伤，但不会危及生命	E2	高速匝道并道，前后车保持较低相对车速的持续时间小于1%平均驾驶时间	C1	由于丢失动力发生时前后车相对车速较低，大于99%驾驶员可以控制车辆减速或完成停车	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
HZD_01_5b	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与后车相对车速中等的情况下(20km/h≤ΔV≤40km/h)，与后车发生碰撞	S2	碰撞时两辆车的相对速度中等，可能造成驾驶员较为严重的受伤，但不会危及生命	E2	高速匝道并道，前后车保持较低相对车速的持续时间小于1%平均驾驶时间	C2	由于丢失动力发生时前后车相对车速中等，大于90%驾驶员可以控制车辆减速或完成停车	QM
HZD_01_5c	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与后车相对车速较高的情况下(ΔV＞40km/h)，与后车发生碰撞	S3	碰撞时两辆车的相对速度较高，可能造成驾驶员较为严重的受伤，甚至危及生命	E2	高速匝道并道，前后车保持较低相对车速的持续时间小于1%平均驾驶时间	C2	由于丢失动力发生时前后车相对车速较高，大于90%驾驶员可以控制车辆减速或完成停车	A
HZD_01_6a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	车辆在陡坡爬坡运行时，突然丢失动力（踩油门无响应，后方有行人穿过	在与后方行人相对距离较近的情况下，由于丢失动力导致后遛，与后方行人发生碰撞	S3	由于距离较小，相对速度较小，可能造成后方轻度或中度受伤，但是考虑到可能产生碾压，最坏情况下可能造成较为严重的受伤，甚至危及生命	E2	爬坡驾驶，且后方有来车的持续时间小于1%平均驾驶时间	C2	由于丢失动力导致车辆后遛且于后车距离较近，大于90%驾驶员可以控制车辆制动、鸣笛等	A
HZD_01_6b	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与后方行人相对距离较远的情况下，由于丢失动力导致后遛，与后方行人发生碰撞	S3	由于距离较远，相对速度较大，可能造成后方较为严重的受伤，甚至危及生命	E2	爬坡驾驶，且后方有行人穿越的持续时间小于1%平均驾驶时间	C1	由于丢失动力导致车辆后遛且于后方行人距离较远，大于99%驾驶员可以控制车辆制动、鸣笛等	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
HZD_01_7a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	车辆在陡坡爬坡运行时，突然丢失动力（踩油门无响应），后方有来车	在与后车相对距离较近的情况下，由于丢失动力导致后遛，与后车发生碰撞	S1	由于距离较小，相对速度较小，可能造成后车驾驶员轻度或中度受伤，但不会危及生命	E2	爬坡驾驶，且后方有来车的持续时间小于1%平均驾驶时间	C2	由于丢失动力导致车辆后遛且于后车距离较近，大于90%驾驶员可以控制车辆制动、鸣笛等	QM
HZD_01_7b	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无		在与后车相对距离较远的情况下，由于丢失动力导致后遛，与后车发生碰撞	S2	由于距离较远，相对速度较大，可能造成后车驾驶员轻度或中度受伤，但不会危及生命	E2	爬坡驾驶，且后方有来车的持续时间小于1%平均驾驶时间	C1	由于丢失动力导致车辆后遛且于后车距离较近，大于99%驾驶员可以控制车辆制动、鸣笛等	QM
HZD_01_8a	输出驱动转矩（含零转矩）	不能输出驱动转矩	驱动力丧失	无	车辆运行，通过铁路交叉路口，突然丢失动力（踩油门无响应），列车后续经过铁道交叉路口	车辆将会与列车相撞	S3	车辆通过铁路交叉路口等危险路况时丢失动力，产生特别严重或致命伤害	E1	车辆经过铁路交叉口在平均驾驶时间中的占比小于1%	C2	由于丢失动力导致车辆滞留在铁道交叉口，大于90%驾驶员可以尽快离开车辆以避免伤害	QM
HZD_02_1a	输出驱动转矩（含零转矩）	实际输出驱动转矩大于期望值	加速度过大	车辆在人员较为密集处低速行驶	与车辆附近行人发生碰撞	人员较为密集处低速行驶时非预期的加速	S3	可能对行人造成危及生命的伤害，严重度取决于电机产生非预期加速的能力	E4	大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于 10%	C2	在碰撞发生之前，大多数司机可能无法正确控制车辆，避免伤害	C
HZD_02_2a	输出驱动转矩	实际输出驱动	加速度过大	在城市道路/高速公路	与车道外对象（行人/车辆/设施）碰	弯道行驶时非预期的加速，偏航	S3	可能以较高速度撞向行人/车辆/设施，严	E4	大多数驾驶员每天都会遭遇此驾驶场景，	C2	驾驶员可以通过踩制动降低车速，在	C

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
	（含零转矩）	转矩大于期望值		等处正常行驶时转向，进入弯道行驶	撞			重度取决于电机产生非预期加速的能力		其在平均驾驶时间中的占比大于10%		大多数情况下，驾驶员的反应时间足够避免伤害的发生	
HZD_02_3a	输出驱动转矩（含零转矩）	实际输出驱动转矩大于期望值	加速度过大	在城市道路/高速公路等处正常直行，前方有其他车辆	与前面车辆追尾	中高速行驶时非预期的加速	S2	追尾撞击时的速度差较低，通常认为不会对驾乘人员造成危及生命的伤害。	E4	大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足够避免伤害的发生	B
HZD_02_4a	输出驱动转矩（含零转矩）	实际输出驱动转矩大于期望值	加速度过大	山路，前边没有交通状况，以小于60km/h的正常速度下坡；或者山路，前边没有交通状况，以小于60km/h的正常速度下	车辆撞到其他车辆或物体、或者车辆离开路面掉落山下	车辆中低速山路行驶时，非预期加速，车辆稳定性丧失	S3	车辆撞到其他车辆或物体、或者车辆离开路面掉落山下，会发生人员生命危险	E2	一般的驾驶员和车辆遇到此驾驶场景可能性较低(绝大多数驾驶员一年发生几次（基于运行场景频率） 绝大多数车辆在山路带有不安全的陡峭斜波的平均运行时间小于1%)	C3	对于一般的驾驶员，此场景很难控制，此时由于故障可能会导致ESP功能受限(遇到非预期加速，驾驶员会比较慌乱，尤其是自行车/行人比较近的时候。少于90%的驾驶员能够避免危害的发生)	B
HZD_02_4b	输出驱动转矩（含零转矩）	实际输出驱动转矩大于期望	加速度过大	坡；或者山路，有雪，以小于40km/h低速	车辆撞到其他车辆或物体、或者车辆离开路面掉落山下	车辆中低速山路行驶时，非预期加速，车辆稳定性丧失	S3	车辆撞到其他车辆或物体、或者车辆离开路面掉落山下，会发生人员生命危险(车	E3	山区驾驶中可能性相对较高(山区中车辆在山路带有不安全的陡峭斜坡的路面平均	C2	山区驾驶员具有较丰富的经验，可以降低可控度(山区驾驶员具有较丰富	B

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
		值		下坡				辆中速侧面碰撞到一个狭窄的静止物体，如树干、路边突出护栏等，影响到乘员舱；中速和其他车辆碰撞；自行车/行人事故、或者车辆离开路面掉落山下，会发生人员生命危险）		运行时间介于1%~10%之间）		的经验，可保持既定行驶线路）	
HZD_03_1a	输出驱动转矩（含零转矩）	实际输出驱动转矩小于期望值	加速度过小	高速超车	高速路超车运行，在超车过程中后方有重型卡车	后方车辆车距过小时，将会发生碰撞	S2	发生后碰，S3：ΔV＞40km/h；S2：ΔV＞20km/h；S1：ΔV＞6km/h	E3	根据GB/T 34590.3-XXXX,表B.3,	C0	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足够避免伤害的发生	QM
HZD_03_2a	输出驱动转矩（含零转矩）	实际输出驱动转矩小于期望值	加速度过小	高速正常行驶	高速上正常驾驶时，后方有来车	后方车辆车距过小时，将会发生碰撞	S2	发生后碰，S3：ΔV＞40km/h；S2：ΔV＞20km/h；S1：ΔV＞6km/h	E4	根据GB/T 34590.3-XXXX,表B.3,正常行驶为E4,	C0	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足够避免伤害的发生	QM
HZD_03_3a	输出驱动转矩（含零转矩）	实际输出驱动转矩小于期望值	加速度过小	城市道路转向	车辆在十字路口转向时，对向有来车，与对向车辆发生碰撞	车辆在十字路口左转，车速较慢，通过对向车道时车辆丢失动力使车辆停止在对向车道上。对向车道车辆以正常速度驶过路口，左转车辆	S3	发生碰撞，S3：ΔV＞40km/h；S2：ΔV＞20km/h；S1：ΔV＞6km/h	E3	大多数驾驶员平均每月都会遭遇此驾驶场景，其在平均驾驶时间中的占比处于1%-10%	C0	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足够避免伤害的发生	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
						无法按照预期的速度通过对向车道，可能导致发生碰撞。							
HZD_03_4a	输出驱动转矩（含零转矩）	实际输出驱动转矩小于期望值	加速度过小	城市或乡村道路超车	在城市或乡村道路超车运行时，在超车或并道过程中后方有来车	后方车辆车距过小时，将会发生碰撞	S2	发生后碰，S3：ΔV＞40km/h；S2：ΔV＞20km/h；S1：ΔV＞6km/h	E3	大多数驾驶员平均每月都会遭遇此驾驶场景，其在平均驾驶时间中的占比处于1%-10%	C0	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足够避免伤害的发生。	QM
HZD_03_5a	输出驱动转矩（含零转矩）	实际输出驱动转矩小于期望值	加速度过小	爬坡	车辆陡坡爬坡运行时，后方道路有行人穿过，车距较小	车辆发生后溜与后车发生碰撞	S1	发生后碰，S3：ΔV＞40km/h；S2：ΔV＞20km/h；S1：ΔV＞6km/h	E1	大多数驾驶员平均每月都会遭遇爬坡驾驶场景，但考虑后方有行人穿越	C0	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足够避免伤害的发生。	QM
HZD_03_5b	输出驱动转矩（含零转矩）	实际输出驱动转矩小于期望值	加速度过小		车辆陡坡爬坡运行时，后方有来车，车距较大	车辆发生后溜与后车发生碰撞	S1	发生后碰，S3：ΔV＞40km/h；S2：ΔV＞20km/h；S1：ΔV＞6km/h	E3	大多数驾驶员平均每月都会遭遇此驾驶场景，其在平均驾驶时间中的占比处于1%-10%	C0	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足够避免伤害的发生。	QM
HZD_03_6a	输出驱动转矩（含零转矩）	实际输出驱动转矩小于期望	加速度过小	通过铁路	车辆运行，通过铁路交叉路口	车辆将会与列车相撞	S3	发生侧碰，S3：ΔV＞40km/h；S2：ΔV＞20km/h；S1：ΔV＞6km/h	E1	大多数驾驶员平均1年会遭遇此驾驶场景，其在平均驾驶时间中的占比小于1%	C0	驾驶员可以通过踩制动降低车速，在大多数情况下，驾驶员的反应时间足	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
		值										够避免伤害的发生。	
HZD_04_1a	输出驱动转矩（含零转矩）	转矩输出方向与期望值反向	加速度方向相反	车辆静止	车辆静止起步，行人从车前或者车后面穿过或邻近有停放其他车辆	车辆与前后方邻近的行人或其它车辆发生碰撞	S3	在车辆静止起步时，反向转矩输出将会导致低速碰撞邻近的行人或其它车辆，产生特别严重或致命伤害的概率大于10%	E3	车辆静止且前后方有行人或车辆的场景较为常见，其在平均驾驶时间中的占比介于1% ~ 10%。	C3	反向车辆运动违背驾驶员以及邻近行人的预期，小于90%的驾驶员可以避免伤害	C
HZD_04_1b	输出驱动转矩（含零转矩）	转矩输出方向与期望值反向	加速度方向相反		上坡道驻车，后方有行人穿过或邻近的其它车辆（相对距离较远）	车辆溜坡，与后方邻近的行人或其它车辆发生碰撞	S3	在车辆坡道驻车时，反向转矩输出将导致车辆溜坡撞到后方邻近的行人或其它车辆，相对距离较远发生碰撞时的车速较高，产生特别严重或致命伤害的概率大于10%	E2	坡道驻车且后方有邻近的行人或其它车辆的场景大多数驾驶员平均一年会遭遇多次，其在平均驾驶时间中的占比小于1%	C2	反向车辆运动违背驾驶员以及邻近行人的预期，由于相对距离较远，大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动来控制车辆避免发生碰撞	A
HZD_04_1c	输出驱动转矩（含零转矩）	转矩输出方向与期望值反向	加速度方向相反		上坡道驻车，后方有行人穿过或邻近的其它车辆（相对距离较近）		S2	在车辆坡道驻车时，反向转矩输出将导致车辆溜坡撞到后方邻近的行人或其它车辆，相对距离较近发生碰撞时的车速较低，产生严重的和危	E2	坡道驻车且后方有邻近的行人或其它车辆的场景大多数驾驶员平均一年会遭遇多次，其在平均驾驶时间中的占比小于1%	C3	反向车辆运动违背驾驶员以及邻近行人的预期，由于相对距离较近，小于90%的驾驶员或其他道路使用者可以避免伤害	A

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
								及生命的伤害（有存活的可能）					
HZD_04_2a	输出驱动转矩（含零转矩）	转矩输出方向与期望值反向	加速度方向相反	高速公路潮湿路面	雨雪天车辆在高速公路上行驶	在潮湿路面行驶时，突然转矩驱动力反向，类似制动，可能导致偏航并撞上其它车辆或公共设施	S3	车辆在高速行驶过程中，反向转矩输出将导致车辆偏航并撞上其它车辆或公共设施，产生特别严重或致命伤害的概率大于10%	E3	雨雪天在高速上行驶的场景较为常见，其在平均驾驶时间中的占比介于1%~10%。	C3	在低附路面上非预期横向运动较难控制，小于90%的驾驶员可以避免伤害	C
HZD_04_3a	输出驱动转矩（含零转矩）	转矩输出方向与期望值反向	加速度方向相反	中高速	高速上驾驶员踩油门超车并道	超车过程中，突然转矩驱动力反向，类似于制动，导致车辆减速并与后车相撞	S3	车速较高时，并道过程中与后方车辆碰撞，产生特别严重或致命伤害的概率大于10%	E4	在高速上超车并道，大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动来控制车辆避免发生碰撞	C
HZD_04_4a	输出驱动转矩（含零转矩）	转矩输出方向与期望值反向	加速度方向相反	低速	车辆在人员较为密集处低速行驶	车辆在城市或城镇、商业或住宅区低速行驶时，附近有行人或其它车辆，当发生意外的反向加速时，可能会与邻近的行人或其它车辆发生碰撞	S3	车辆低速行驶时，反向转矩输出将会导致低速碰撞邻近的行人或其它车辆，产生特别严重或致命伤害的概率大于10%	E4	人员或交通密集区域低速行驶，大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C0	车辆会先减速到零然后再反向运动，可控时间较长，绝大部分驾驶员都可以避免伤害	QM
HZD_04_5a	输出驱动转矩（含零	转矩输出方向与期望	加速度方向相反	倒车时	车辆倒车时，车头前方有行人或其它车辆经过	车辆在倒车过程中，突然转矩驱动力反向，车辆反向往前开，可能会撞到前方经过	S2	车辆倒车时通常速度较低，与周围的行人发生碰撞，产生严重	E4	低速倒车大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾	C0	车辆会先减速到零然后再反向运动，可控时间较长，绝	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
	转矩）	值反向				的行人或其它车辆		的和危及生命的伤害（有存活的可能）		驶时间中的占比大于10%		大部分驾驶员都可以避免伤害	
HZD_05_1a	输出驱动转矩	非预期驱动转矩输出	车辆从静止状态非预期启动	车辆无蠕行功能	车辆静止停于斑马线前，驾驶员在车上，车辆前方较远处有行人或其他车辆经过。	车辆与前方行人或车辆发生碰撞（远距离）	S3	由于与行人或车辆距离较远，故障车辆将会以中速撞上邻近行人或车辆，产生特别严重或致命伤害的概率大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	C
HZD_05_1b	输出驱动转矩	非预期驱动转矩输出	车辆从静止状态非预期启动	车辆有蠕行功能	车辆静止停于斑马线前，驾驶员在车上，并且车辆退出可行驶模式，车辆前方较远处有行人或其他车辆经过。	车辆与前方行人或车辆发生碰撞（远距离）	S3	由于与行人或车辆距离较远，故障车辆将会以中速撞上邻近行人或车辆，产生特别严重或致命伤害的概率大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	C
HZD_05_1c	输出驱动转矩	非预期驱动转矩输出	车辆从静止状态非预期启动	车辆有蠕行功能	车辆静止停于斑马线前，驾驶员在车上，并且车辆退出可行驶模式，车辆前方较近处有行人或其他车辆经过	车辆与前方行人或车辆发生碰撞（近距离）	S2	由于与行人距离较近，车辆行驶速度较低，产生特别严重或致命伤害的概率不大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C3	小于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	C
HZD_05_2a	输出驱动转矩	非预期驱动转	车辆从静止状		车辆静止，在交叉路口或环形路口	车辆与前方/侧方车辆发生碰撞	S3	在交叉路口或环形路口准备汇入车流时突	E4	大多数驾驶员平均每天都会遭遇此驾驶场	C2	大于90%的驾驶员或其他道路使用者	C

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
		矩输出	态非预期启动		准备汇入车流。			然加速，将会以中高速撞上其他车辆，产生特别严重或致命伤害的概率大于10%		景，其在平均驾驶时间中的占比大于10%		可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	
HZD_05_2b	输出驱动转矩	非预期驱动转矩输出	车辆非预期的加速	新能源汽车滑行时处于回馈制动模式	车辆运行过程中，以中高车速直线滑行	车辆与前方车辆追尾	S2	追尾撞击时的速度差较低，通常产生特别严重或致命伤害的概率不大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	B
HZD_05_2c	输出驱动转矩	非预期驱动转矩输出	车辆非预期的加速	新能源汽车滑行时处于回馈制动模式	车辆运行经过弯道时，以中高车速滑行通过弯道；	车辆与前方车辆追尾	S3	车速较高，由于弯道碰撞，导致偏置碰撞，通常产生特别严重或致命伤害的概率大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	C
HZD_06_1a	输出制动转矩	不能输出制动转矩	制动力降低	车辆再生制动等级中等(大于0.3g)	车辆在高速公路上跟随前车行驶，前方车突然急刹	驾驶员踩下制动踏板后，驱动系统再生制动力意外未输出，车辆未提供预期制动力，导致减速不及时或制动距离过长而与前车相撞	S2	由于制动系统与驱动系统的再生制动不同步，混合制动功能会受到影响。由于车辆再生制动等级中等，车辆减速度不足或制动距离过长与前方车辆发生碰撞，可能造	E4	大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C1	在碰撞发生之前，司机可以加大制动踏板深度，大于99%的驾驶员或其他道路使用者可以避免伤害。	A

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
								成驾驶员较为严重的受伤，但不会危及生命					
HZD_06_1b	输出制动转矩	不能输出制动转矩	制动力降低	车辆再生制动等级较低（小于等于0.3g）	车辆在高速公路上跟随前车行驶，前方车突然急刹	驾驶员踩下制动踏板后，驱动系统再生制动力意外未输出，车辆未提供预期制动力，导致减速不及时或制动距离过长而与前车相撞	S1	由于制动系统与驱动系统的再生制动不同步，混合制动功能会受到影响。由于车辆再生制动等级较低，车辆减速度不足或制动距离过长与前方车辆发生碰撞，可能造成驾驶员轻度或中度受伤，但不会危及生命	E4	大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C0	在碰撞发生之前，司机可以加大制动踏板深度，绝大部分驾驶员或其他道路使用者可以避免伤害。	QM
HZD_06_2a	输出制动转矩	不能输出制动转矩	制动力降低	车辆再生制动等级中等(大于0.3g)	车辆在城市道路或人员密集区行驶，前方车辆制动减速，或车辆要在斑马线前停止	驾驶员踩下制动踏板后，驱动系统再生制动力意外未输出，车辆未提供预期制动力，导致减速不及时或制动距离过长而与前车或斑马线上行人相撞。	S2	由于制动系统与驱动系统的再生制动不同步，混合制动功能会受到影响。由于车辆再生制动等级中等，车辆减速度不足或制动距离过长与前方车辆或行人发生碰撞，可能造成驾驶员较为严重的受伤，但不会	E4	大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C1	在碰撞发生之前，司机可以加大制动踏板深度，大于90%的驾驶员或其他道路使用者可以避免伤害。	A

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
								危及生命					
HZD_06_2b	输出制动转矩	不能输出制动转矩	制动力降低	车辆再生制动等级较低（小于等于0.3g）	车辆在城市道路或人员密集区行驶，前方车辆制动减速，或车辆要在斑马线前停止	驾驶员踩下制动踏板后，驱动系统再生制动力意外未输出，车辆未提供预期制动力，导致减速不及时或制动距离过长而与前车相撞	S1	由于制动系统与驱动系统的再生制动不同步，混合制动功能会受到影响。由于车辆再生制动等级较低，车辆减速度不足或制动距离过长与前方车辆发生碰撞，可能造成驾驶员轻度或中度受伤，但不会危及生命	E4	大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C0	在碰撞发生之前，司机可以加大制动踏板深度，绝大部分驾驶员或其他道路使用者可以避免伤害。	QM
HZD_07_1a	输出制动转矩	实际输出制动转矩大于期望值	减速度过大	在高速公路正常行驶时转向，进入弯道行驶	与车道外设施碰撞或坠毁	弯道行驶时非预期的制动力过大，偏航	S3	可能导致车辆撞毁，产生特别严重或致命伤害	E3	大多数驾驶员平均一年会遭遇此驾驶场景，其在平均驾驶时间中的占比小于1%	C3	驾驶员在制动力过大造成偏航导致车辆脱离弯道时难以控制车辆	C
HZD_07_2a	输出制动转矩	实际输出制动转矩大于期望值	减速度过大	高速公路且湿滑路面正常行驶	撞向公共设施或其他车辆	高速公路（湿滑路面）行驶时，有制动转矩请求时，非预期的制动力过大，偏航	S3	可能导致车辆失稳，高速撞向公共设施或其他车辆	E3	在高速公路（湿滑路面）行驶对于一般的驾驶员较为常见，可认为持续时间占平均运行时间的百分比介于1% ~ 10%。	C3	由于制动力的非预期增大导致的车辆失稳，一般驾驶员很难进行判断，可能会进一步踩制动加剧失稳现象，难以控制	C

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
HZD_07_3a	输出制动转矩	实际输出制动转矩大于期望值	减速度过大	高速公路上正常行驶时轻点制动	与后车相撞	高速上轻点制动时，制动转矩超过预期值，急减速	S2	高速公路，车速较高，与后方来车轿车正碰	E4	高速公路行驶对于一般的驾驶员非常常见	C3	在符合交通法规的前提下，车辆间距够大，前车有制动灯显示，常规可控（电动汽车能量回馈运行制动转矩较小时，有可能不会亮制动灯。后车驾驶员可能来不及制动，90%或小于90%驾驶员可以及时制动。）	C
HZD_07_4a	输出制动转矩	实际输出制动转矩大于期望值	减速度过大	在城市道路等处正常行驶时转向，进入弯道行驶	与车道外对象（行人/车辆/设施）碰撞	弯道行驶时非预期的制动力过大，偏航 (弯道行驶时制动转矩超过预期值，偏航)	S3	与摩托/自行车/行人参与者发生碰撞	E3	大多数驾驶员每天都会遭遇此驾驶场景，但需有摩托/自行车/行人在车周边	C3	驾驶员在制动力过大造成偏航导致车辆脱离弯道时难以控制车辆	C
HZD_08_1a	输出制动转矩	实际输出制动转矩小于期望值	制动力降低	车辆运行，车辆临停，前方有车辆或行人经过	车辆与邻近区域内的行人或车辆发生碰撞	车辆在下陡坡临停时制动力降低	S3	车辆在下陡坡临停时制动力降低，将撞上前方车或行人，产生特别严重或致命伤害的概率大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C0	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过机械制动或方向盘控制车辆避免发生碰撞（驾驶员可控）	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
HZD_08_2a	输出制动转矩	实际输出制动转矩小于期望值	制动力降低	车辆直线通过十字路口，减速行驶；	车辆邻近区域内有行人或其他车辆；	与邻近区域的行人或其他车辆发生碰撞；	S3	车辆正常减速时制动力降低，可能高速撞上车辆或邻近行人，致人员伤亡；	E4	每个驾驶循环都会经历此驾驶场景，其在平均驾驶时间中的占比大于10%；	C0	车辆减速过程中制动力过小，大部分驾驶员可以踩制动，通过机械制动力降低车速；驾驶员可以通过鸣笛警示行人避让；	QM
HZD_08_3a	输出制动转矩	实际输出制动转矩小于期望值	制动力降低	车辆转弯/掉头行驶；	转弯区域内有行人或其他车辆；	与邻近区域的行人或其他车辆发生碰撞；	S3	车辆转弯/掉头时制动力降低，可能高速撞上车辆或邻近行人，致人员伤亡；	E4	每个驾驶循环都会经历此驾驶场景，其在平均驾驶时间中的占比大于10%；	C0	车辆转弯时制动力过小可能会引起非预期偏航，部分驾驶员可通过制动或方向盘有效控制车辆，避免发生碰撞，驾驶员也可以通过鸣笛警示行人避让；	QM
HZD_09_1a	输出制动转矩	转矩输出方向与期望值反向（与驱动转矩反向相同）	加速度方向相反	车辆静止	车辆减速至静止，行人从车前穿过或邻近有停放其他车辆	车辆与前方邻近的行人或其它车辆发生碰撞	S3	在车辆减速至静止时，反向转矩输出将会导致低速碰撞邻近的行人或其它车辆，产生特别严重或致命伤害的概率大于10%	E3	车辆减速至静止且前方有行人或车辆的场景较为常见，其在平均驾驶时间中的占比介于1% ~ 10%。	C3	反向加速违背驾驶员以及邻近行人的预期，小于90%的驾驶员可以避免伤害	C

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
HZD_09_1b	输出制动转矩	转矩输出方向与期望值反向（与驱动转矩反向相同）	加速度方向相反		下坡道驻车，前方有行人穿过或邻近的其它车辆（相对距离较远）	车辆溜坡，与前方邻近的行人或其它车辆发生碰撞	S3	在车辆坡道驻车时，反向转矩输出将导致车辆溜坡撞到前方邻近的行人或其它车辆，相对距离较远发生碰撞时的车速较高，产生特别严重或致命伤害的概率大于10%	E2	坡道驻车且前方有邻近的行人或其它车辆的场景大多数驾驶员平均一年会遭遇多次，其在平均驾驶时间中的占比小于1%	C2	反向车辆运动违背驾驶员以及邻近行人的预期，由于相对距离较远，大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动来控制车辆避免发生碰撞	A
HZD_09_1c	输出制动转矩	转矩输出方向与期望值反向（与驱动转矩反向相同）	加速度方向相反		下坡道驻车，前方有行人穿过或邻近的其它车辆（相对距离较近）	车辆溜坡，与前方邻近的行人或其它车辆发生碰撞	S2	在车辆坡道驻车时，反向转矩输出将导致车辆溜坡撞到前方邻近的行人或其它车辆，相对距离较近发生碰撞时的车速较低，产生严重的和危及生命的伤害（有存活的可能）	E2	坡道驻车且前方有邻近的行人或其它车辆的场景大多数驾驶员平均一年会遭遇多次，其在平均驾驶时间中的占比小于1%	C3	反向车辆运动违背驾驶员以及邻近行人的预期，由于相对距离较远，小于90%的驾驶员或其他道路使用者可以避免伤害	A
HZD_09_2a	输出制动转矩	转矩输出方向与期望值反向（与驱动转矩	加速度方向相反	高速公路潮湿路面	雨雪天车辆在高速公路上行驶	在潮湿路面行驶时，突然转矩驱动力反向，类似非预期加速，可能导致偏航并撞上其它车辆或公共设施	S3	车辆在高速行驶过程中，反向转矩输出将导致车辆偏航并撞上其它车辆或公共设施，产生特别严重或致命伤害的概率大于	E3	雨雪天在高速上行驶的场景较为常见，其在平均驾驶时间中的占比介于1% ~ 10%。	C3	在低附路面上非预期横向运动较难控制，小于90%的驾驶员可以避免伤害	C

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
		反向相同）						10%					
HZD_09_3a	输出制动转矩	转矩输出方向与期望值反向（与驱动转矩反向相同）	加速度方向相反	中高速	高速上前车突然制动，驾驶员踩制动踏板	制动过程中，突然转矩驱动力反向，类似于非预期加速，导致车辆减速不足并与前车相撞	S3	车速较高时，制动过程中与前方车辆碰撞，产生特别严重或致命伤害的概率大于10%	E4	在高速上前车突然制动，大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动来控制车辆避免发生碰撞	C
HZD_09_4a	输出制动转矩	转矩输出方向与期望值反向（与驱动转矩反向相同）	加速度方向相反	低速	车辆在人员较为密集处踩制动踏板	车辆在城市或城镇、商业或住宅区低速行驶过程中踩制动踏板，附近有行人或其它车辆，当发生意外的反向加速时，可能会与邻近的行人或其它车辆发生碰撞	S3	车辆低速行驶时，反向转矩输出将会导致低速碰撞邻近的行人或其它车辆，产生特别严重或致命伤害的概率大于10%	E4	人员或交通密集区域低速行驶，大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过深踩制动踏板来控制车辆避免发生碰撞	C
HZD_09_5a	输出制动转矩	转矩输出方向与期望值反向（与驱动转矩	加速度方向相反	倒车时	车辆倒车时，车尾后方有行人或其它车辆经过	车辆在倒车过程中，突然转矩驱动力反向，车辆突然加速往后开，可能会撞到后方经过的行人或其它车辆	S2	车辆倒车时通常速度较低，与周围的行人发生碰撞，产生严重的和危及生命的伤害（有存活的可能）	E4	低速倒车大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过深踩制动踏板来控制车辆避免发生碰撞	B

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
		反向相同）											
HZD_10_1a	输出制动转矩	非预期制动转矩输出（与非预期转矩反向类似）	非预期倒车	车辆有蠕行功能	车辆静止，驾驶员在车上，退出可行驶模式，车辆后方有行人或其他车辆经过	车辆与后方邻近行人或停放车辆发生碰撞（远距离）	S3	建议描述更改为由于与行人距离较远，车辆将会以中速撞上邻近行人或车辆，产生特别严重或致命伤害的概率大于10%	E4	大多数驾驶员每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C2	大于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	C
HZD_10_1b	输出制动转矩	非预期制动转矩输出（与非预期转矩反向类似）	非预期倒车	车辆有蠕行功能	车辆静止，驾驶员在车上，退出可行驶模式，车辆前方有行人或其他车辆经过	车辆与后方邻近行人或停放车辆发生碰撞（近距离）	S2	由于与行人距离较近，车辆行驶速度较低，产生特别严重或致命伤害的概率不大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C3	小于90%的驾驶员或其他道路使用者可以避免伤害，驾驶员可通过制动或方向盘控制车辆避免发生碰撞	C
HZD_10_2a	输出制动转矩	非预期制动转矩输出（与非预期转矩反向类似）	车辆非预期的减速	N档滑行处于0Nm命令状态，但行车时N档滑行的暴露度较低。带档滑行的暴露度较高，新	车辆运行过程中，以中高车速滑行；	车辆行驶中非预期减速，导致后面车辆追尾	S2	追尾撞击时的速度差较低，通常产生特别严重或致命伤害的概率不大于10%	E4	大多数驾驶员平均每天都会遭遇此驾驶场景，其在平均驾驶时间中的占比大于10%	C0	通常状态下可控，其等效于制动	QM

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－考虑最严苛场景）	ASIL						
							S	理由	E	理由	C	理由	ASIL
				能源汽车滑行时处于回馈制动模式。									
注：“卡滞”相关的功能异常功能表现为转矩输出量无法更新，其危害分析和风险评估会被非预期的加速和非预期的减速覆盖。													

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，见表A.5。

表 A.5 安全目标和安全状态

序号	安全目标	ASIL	安全状态	FTTI	HARA编号	整车危害
SG-01	防止电机无法输出驱动转矩	A	发出警示	参见7.1.3	HZD_01_1b、HZD_01_1c、HZD_01_2b、HZD_01_2c、HZD_01_3c、HZD_01_4c、HZD_01_5c、HZD_01_6a、HZD_01_8a	车辆驱动力丧失
SG-02	防止电机非预期的输出驱动转矩过大	C	发出警示，终止转矩输出	参见7.2.3	HZD_02_1a	车辆加速度过大
SG-03	防止电机转矩输出方向反向	C	发出警示，终止转矩输出	参见7.3.3	HZD_04_1a、HZD_04_2a、HZD_04_3a、HZD_09_1a、HZD_09_2a、HZD_09_3a、HZD_09_4a、HZD_09_5a	车辆加速度方向相反
SG-04	防止电机非预期的输出驱动转矩	C	发出警示，终止转矩输出	参见7.4.3	HZD_05_1a、HZD_05_1b、HZD_05_1c、HZD_05_2a、HZD_05_2c	车辆从静止状态非预期启动、车辆非预期的加速
SG-05	防止电机无法输出制动转矩	A	发出警示	参见7.5.3	HZD_06_1a、HZD_06_2a	车辆制动力降低
SG-06	防止电机非预期的输出制动转矩过大	C	发出警示，终止转矩输出	参见7.6.3	HZD_07_1a、HZD_07_2a、HZD_07_4a	车辆减速度过大
SG-07	防止电机非预期的输出制动转矩	C	发出警示，终止转矩输出	参见7.7.3	HZD_10_1a、HZD_10_1b	车辆非预期倒车

附 录 B
（资料性）
故障容错时间间隔（FTTI）确定方法示例

B.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B.1所示。

以驱动电机系统为例，FTTI为从故障发生到驱动电机系统产生不可接受的危害的最短时间间隔。例如，驱动电机从非预期的输出驱动转矩过大故障发生到整车非预期的加速过大的最短时间间隔。

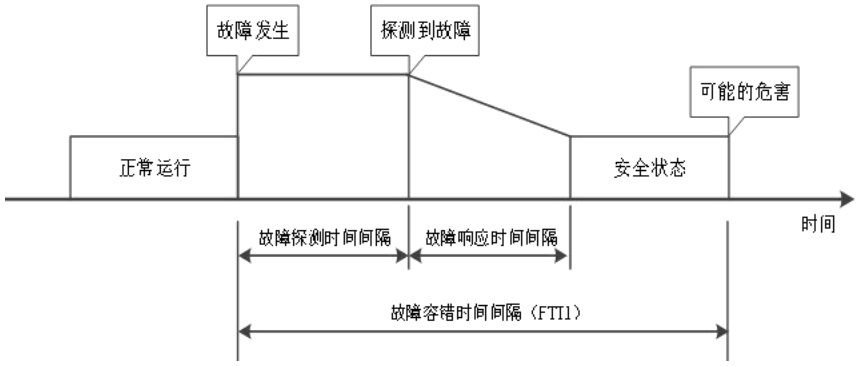

图 B.1 故障容错时间间隔

如图B.1所示，在定义驱动电机系统的FTTI时，需要明确以下几点：

a) FTTI 需要在驱动电机系统来定义；
b) 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；
c) 故障指违背安全阈值，例如：电机非预期的输出驱动转矩过大故障发生意味着非预期输出驱动转矩过大的安全阈值被违背；
d) 可能的危害是不能接受的驱动电机系统危害，危害必须是明确的且可识别的，可由整车制造商和驱动电机系统供应商协商确定，如非预期输出驱动转矩过大、非预期输出制动转矩过大等；
e) 从故障发生到产生危害的时间之内，驱动电机系统应以最严苛情况或整车制造商和驱动电机系统供应商确认的工况运行。

B.2 电机非预期的输出驱动转矩过大故障 FTTI 定义示例

B.2.1 总则

本附录给出电机非预期的输出驱动转矩过大故障FTTI的确定方法及过程示例，示意图如图B.2所示。

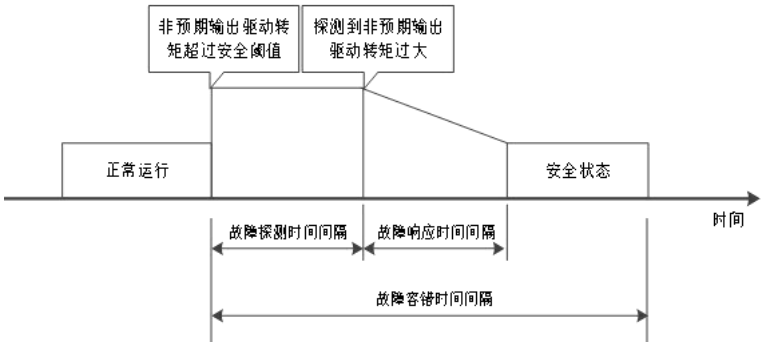

图 B.2 电机非预期输出驱动转矩过大故障容错时间间隔

B.2.2 确定整车非预期加速度过大的安全阈值

整车制造商和驱动电机系统供应商应在不同的HARA分析场景下，通过故障注入的方式，评估驾驶员在无故障注入预期的情况下，在不同非预期加速度下对整车的控制程度，从而确定整车非预期加速度过大的安全阈值。

对整车的控制程度的衡量，主要考虑整车非预期加速是否对驾驶员造成惊吓，从而发生一些错误的操作，例如：

a) 不合适的制动、加速操作（踩错或松开）；

b) 不合适的转向操作（紧锁或松开）；

c) 无响应驾驶行为。

该评估应尽可能减少由于驾驶员对故障注入的心理预期而产生的影响，可以通过在评估过程中实施认知分心任务的方式来实现。

该评估应考虑目标市场驾驶员性别、年龄、地域等因素对测试结果的影响。

B.2.3 确定驾驶员平均响应时间

整车制造商和驱动电机系统供应商应在不同的HARA分析场景下，通过故障注入的方式，评估不同驾驶员在无故障注入预期的情况下，从注入故障到做出动作响应（正确响应或错误响应）的平均响应时间。

平均响应时间一般由场景感知时间和动作执行时间两部分组成，应尽可能减少动作执行时间的影响。

该评估应尽可能减少由于驾驶员对故障注入的心理预期而产生的影响，可以通过在评估过程中实施认知分心任务的方式来实现。

该评估应尽可能考虑性别、年龄、地域等因素的差别，并记录尽可能多的样本。

B.2.4 计算电机非预期输出驱动转矩过大的安全阈值

电机非预期驱动转矩过大的安全阈值需要根据整车的非预期加速度过大安全阈值、整备质量、轮胎半径及减速比等整车参数来进行计算，违背该阈值意味着此时整车发生非预期的加速度过大危害。

B.2.5 确认电机非预期输出驱动转矩过大的FTTI

基于B.2.3中确定的驾驶员平均响应时间，来设置非预期加速度注入持续时间，即在驾驶员平均响应时间内撤销故障注入，再次评估驾驶员对整车的控制程度，确保可控性在目标范围内。该持续时间即为整车非预期加速度过大的FTTI。

根据不同的整车电子架构，在去除其他模块的通信延迟后（例如整车控制器VCU的处理时间和通信频率等），可得到电机非预期输出驱动转矩过大的FTTI。