电动汽车电机控制器功能安全设计研究

马伏韬[1]，马超文[2]，王坤俊[1]，钟雄武[1]，王双娥[1]
（1. 中车时代电动汽车股份有限公司，湖南 株洲 412007；
2. 湖南中车时代电驱科技有限公司，湖南 株洲 412001）

摘 要：本文基于ISO 26262《道路车辆功能安全》，以电动汽车电机控制器为研究对象，通过功能识别、相关项定义、危害分析与风险评估等方法确定其功能安全目标以及所对应的相关指标和功能安全要求，以作为后续开展系统详细设计的输入。

关键词：电动汽车；电机控制器；功能安全；ISO 26262
中图分类号：U463.6 **文献标志码**：A **DOI**：10.15917/j.cnki.1006-3331.2025.03.004

Research on the Function Safety Design of Electric Vehicle Motor Controller

MA Futao[1], MA Chaowen[2], WANG Kunjun[1], ZHONG Xiongwu[1], WANG Shuang'e[1]
(1. CRRC Times Electric Vehicle Co., Ltd., Zhuzhou 412007, China;
2. Hunan CRRC Times Electric Drive Technology Co., Ltd., Zhuzhou 412001, China)

Abstract: Based on ISO 26262 *Road Vehicles Functional Safety*, this paper takes the electric vehicle motor controller as the research object which determines the functional safety goals and the corresponding indicators and functional safety requirements through methods such as function identification, definition of the item under consideration, and hazard analysis and risk assessment. These results serve as the input for the subsequent detailed system design.

Key words: electric vehicle; motor controller; function safety; ISO 26262

随着汽车产业新能源化和智能化程度的不断提高，车用电子电气系统及其零部件功能日益复杂，如何确保车辆全生命周期的安全可靠，已成为当下亟需重点考虑的问题。为此，国际标准化组织于2011年正式颁布了ISO 26262系列标准，并于2018年更新[1]；国内也于2017年正式发布了GB/T 34590系列标准[2]。

在电动汽车中，电机控制器根据挡位、油门、刹车等指令，将动力电池的电能转化为驱动电机所需的电能，从而控制车辆的启动、运行、进退速度及爬坡力度；同时在车辆刹车时提供辅助，并将部分制动能量回收至动力电池中。本文从电机控制器的基本功能出发，详细分析其功能失效和整车层面的故障可能导致的危害，并基于此导出功能安全目标及其对应的相关指标和功能安全需求[3-7]。

1 功能识别及相关项定义

图1为电动汽车驱动系统示意图，其中整车控制器（Vehicle Control Unit，VCU）负责获取驾驶员意图，根据油门、刹车以及挡位信息判断当前工作模式，并计算期望的转矩指标；电机控制器（Motor Control Unit，MCU）负责电机驱动，并根据VCU发送的逆变器工作模式指令以及转矩指令来控制电机的转矩输出；高压电池负责为电机驱动提供能源。

功能识别的目的是定义和描述相关项，以及其对其他相关项和环境的依赖与相互作用。为实现这一目标，需进一步描述功能需求、非功能需求、系统边界及接口，同时明确与其他系统相互作用的假定条件。

收稿日期：2024-12-25。

第一作者：马伏韬（1996—），男，助理工程师，主要从事道路车辆、轨道交通功能安全研究工作。E-mail：402352686@qq.com。

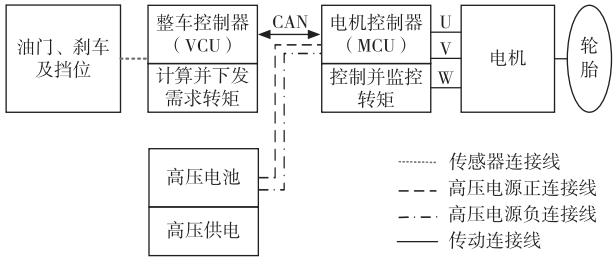

图 1　电动汽车驱动系统示意图

为完成电机控制器的功能安全设计，确定其运行的假定条件如下：①驱动环节只有单个电机且传动比固定；②系统包含差速器但不含离合器；③转矩指标由整车控制器计算；④直流储能系统采用高压电池；⑤逆变器作为电机控制的能量转换装置[8-9]。

基于整车需求，电机控制器的基本功能如下：提供转矩驱动力、回馈制动、提供特定转速输出、防溜车控制、蠕行控制、主动防抖动控制、紧急控制、主动放电、休眠控制、最大运行能力估计、电机控制器壳体盖板闭合状态监测、电机参数辨识、旋转变压器软解码、故障诊断。限于篇幅，本文以“电机控制器提供转矩驱动力”这一基本功能为例，进行相关项定义和后续分析[10]，其有关描述见表 1 和图 2。

表 1　电机控制器提供转矩驱动力基本功能描述

功能	输入	输出
当 MCU 接收到“转矩模式”请求时，MCU 根据 VCU 转矩指令控制电机输出指定转矩。	逆变器模式请求、逆变器转矩命令、旋转变压器信号、三相电流传感器信号（来自电机）。	三相电流（去往电机）

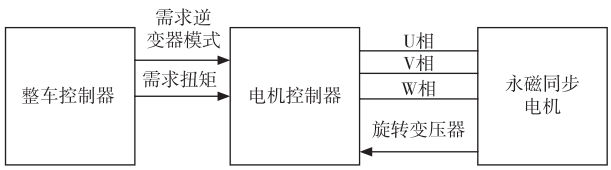

图 2　电机控制器提供转矩驱动力示意图

2　危害分析与风险评估

危害分析与风险评估（Hazard Analysis and Risk Assessment，HARA）的主要目的是识别由相关故障行为引起的危害事件，并对其进行分类，进而制定出能够预防或减轻这些危害事件的安全目标及对应的汽车安全完整性等级（Automotive Safety Integrity Level，ASIL）。该等级确定了汽车为避免不合理的安全风险所需满足的具体指标要求。具体分析步骤如下：首先，使用“危害与可操作性”分析方法对基本功能的故障情况进行分析；然后，根据这些故障情况确认可能引起的整车故障；接着，结合不同场景，确定这些整车故障可能导致的最坏结果；最后，根据这些结果进行评分并计算，从而导出功能安全目标。限于篇幅，下面以“电机控制器提供转矩驱动力”这一基本功能及其相关故障项为例进行分析[11]。

2.1　危害与可操作性分析

危害与可操作性分析（Hazard and Operability Study，HAZOP）是 HARA 的重要环节，其通过结合六类引导词，确定功能本身可能产生的故障，以此作为后续确定整车故障的必要输入[12]。

根据表 1 对“电机控制器提供转矩驱动力”功能的描述，结合 HAZOP 的六类引导词：功能丢失、错误执行（过大）、错误执行（过小）、错误执行（反向）、非预期启动功能、输出卡滞在固定值，可以分别导出该功能的六类故障行为，具体如下：非预期失去转矩驱动功能、转矩驱动力过大、转矩驱动力过小、转矩驱动力反向、非预期启动转矩模式、转矩驱动力卡滞。

2.2　整车故障推导分析

功能安全目标是基于整车危害分析和风险评估得出的，因此需要从上述零部件（电机控制器）的故障行为推导出可能引起的整车故障行为。电机控制器提供转矩驱动力的六类功能故障行为可能引起的整车故障行为见表 2。

表 2　整车故障推导分析

电机控制器故障行为	可能引起的整车故障行为
非预期失去转矩驱动功能	非预期滑行
转矩驱动力过大	非预期加速度过大、非预期偏航
转矩驱动力过小	非预期加速度减小
转矩驱动力反向	非预期减速、非预期偏航、非预期车辆倒退、非预期车辆前行
非预期启动转矩模式	非预期加速度减小、非预期加速度过大、非预期减速
转矩驱动力卡滞	非预期加速度减小、非预期加速度过大、非预期偏航

2.3 对应场景分析

如果整车出现故障但没有对应的场景,则无法准确判断其危害程度。因此,需要将整车故障与对应场景(集合为场景库)相结合,才能最终计算并导出功能安全目标[13]。依据 SAE J2980[14] 标准确定的电机控制器功能安全设计目标场景库见表 3。

表 3 运行场景库

地点	路面情况	驾驶行为
乡村道路、城市公路、行人区域、停车场、维修厂、高速公路	干燥、潮湿、冰雪、坡道	启动、前行、倒车、直行、停车、超车、转弯

根据电动客车可能的运行情况,将地点、路面情况、驾驶行为进行组合,本文共得出 18 种常见运行场景,如:高速公路(干燥、超车)、高速公路(干燥、变道)、乡村道路(潮湿、前行)等。

2.4 危害分析

依据 ISO 26262 标准要求,汽车安全完整性划分为 5 个等级:QM、ASIL A、ASIL B、ASIL C 和 ASIL D。其中,QM 为安全完整性最低的等级,对系统的功能安全性要求最低;ASIL D 为安全完整性最高的等级,对系统的功能安全性要求最严格。需要注意的是,当汽车安全完整性等级为 QM 时,虽然存在一定的危害风险,但该风险相对较小,通过质量管理(QM)措施即可有效管控,无需完全遵循 ISO 26262 的全部规定。

ASIL 的分数与各维度分数的对应关系由 ISO 26262-3:2018[15] 可知,为:

$$\mathrm{ASIL}=\mathrm{S}+\mathrm{E}+\mathrm{C} \tag{1}$$

式中:ASIL 表示汽车安全完整性等级;S 为危险事件所导致伤害或损失的潜在严重性,其分数通常依据 ISO 26262-3:2018[15] 和简明损伤定级(Abbreviated Injury Scale,AIS)确定;E 为人员暴露在系统失效后造成危害的场景中的概率,简称为暴露度,其分数通常由 ISO 26262-3:2018[15] 和 SAE J2980-2018[14] 确定;C 为危险所涉及的驾驶员和其他交通人员通过及时的反应避免特定伤害或损失的能力,简称为可控性,其分数通常由 ISO 26262-3:2018[15] 和设计测试经验确定。ASIL 等级与分数对应的关系如下:

$$\begin{cases}\mathrm{S}+\mathrm{E}+\mathrm{C}<7\rightarrow\mathrm{QM}\\ \mathrm{S}+\mathrm{E}+\mathrm{C}=7\rightarrow\mathrm{ASIL\ A}\\ \mathrm{S}+\mathrm{E}+\mathrm{C}=8\rightarrow\mathrm{ASIL\ B}\\ \mathrm{S}+\mathrm{E}+\mathrm{C}=9\rightarrow\mathrm{ASIL\ C}\\ \mathrm{S}+\mathrm{E}+\mathrm{C}=10\rightarrow\mathrm{ASIL\ D}\end{cases} \tag{2}$$

限于篇幅,下面仅展示“电机控制器提供转矩驱动力”这一功能在出现转矩驱动力过大故障时的两个危害分析。

1)由于“电机控制器提供转矩驱动力”功能故障导致转矩驱动力过大,当车辆在干燥的高速公路上行驶并进行变道时,整车非预期加速度过大并偏航,最坏的情况是车辆撞击路边物体。根据 ISO 26262、SAE J2980 标准和事故推测,该危害的暴露度为 E4(4 分)、严重度为 S3(3 分)、可控制度为 C1(1 分)。因此,其 ASIL 得分为 8 分,对应为 ASIL B 等级。

2)由于“电机控制器提供转矩驱动力”功能故障导致转矩驱动力过大,当车辆在冰雪覆盖的高速公路上行驶时,整车非预期加速度过大并偏航,最坏的情况是车辆追尾、撞击路边物体。根据 ISO 26262、SAE J2980 标准、简明损伤定级(AIS)和设计测试经验,该危害的暴露度为 E3、严重度为 S3、控制度为 C3。因此,其 ASIL 得分为 9 分,对应为 ASIL C 等级。

基于上述方法,可以完成电机控制器所有基本功能在不同故障模式和不同场景下的危害分析,并确定对应的 ASIL 等级。

2.5 合并导出功能安全目标

经上述分析可知,当“电机控制器提供转矩驱动力”这一功能出现转矩驱动力过大故障时,车辆在不同场景下会出现多种危害情况,并对应不同的 ASIL 等级要求。因此,需设定功能安全目标,从以下两个方面来满足所有危害分析子项:

1)制定功能安全技术要求,以检测、避免或减轻所有危害分析子项所导致的危害。

2)将危害分析子项中的最高 ASIL 等级作为本功能安全目标的 ASIL 等级,以确保满足所有危害分析子项的功能安全要求。

比如 2.4 节分析 1)中“避免在干燥高速公路上变道时转矩驱动力过大”的等级为 ASIL B;2.4 节分析 2)中“避免在冰雪高速公路上行驶时转矩驱动力

过大”的等级为 ASIL C。则其功能安全目标的功能安全技术要求及其等级可确定为：电机转矩的大小和方向应与转矩需求相符，且实际转矩与需求转矩的偏差需控制在一定范围内，等级为 ASIL C。

3　确定功能安全相关指标及需求

1）通过分析可以看出，以下因素都可能导致功能安全目标被违反：

①整车控制器运行错误。如驾驶员踩下或松开加速踏板时转矩指令错误，或者约束条件估计错误（可能导致驱动轴抱死）。

②通过现场总线，从整车控制器传输给电机控制器的转矩信号出现错误。

③电机控制器运行错误，如输出错误的蠕行或防溜坡转矩命令，或者实际输出转矩信号与需求转矩信号偏差较大。

④电机运行错误，如电机线圈短路。

因此，为防止违反功能安全目标，需确保电机控制器能计算出正确的转矩命令并监控实际输出转矩。具体而言，需要一个能准确计算驾驶员需求转矩指令的本质安全整车控制器，一个能监控实际转矩的本质安全电机控制器，并且两者之间具备端对端通信保护机制。

本质安全是指通过设计措施，使系统能够从根本上按照预期功能运行，或切换到一个安全状态，即便发生故障，系统也不会造成事故。安全状态是指电机轴上没有驱动转矩（当前旋转方向）。对于永磁同步电机，若通过主动短路能够达到并维持安全状态，那么在低速时，存在可由驾驶员控制的制动转矩是可以接受的。

2）对于 ASIL B 级及以上的硬件架构，有定性和定量的功能安全指标要求，详见表 4。

表 4　不同 ASIL 等级的硬件架构度量指标

度量指标	ASIL B	ASIL C	ASIL D
SPFM	≥90%	≥97%	≥99%
LFM	≥60%	≥80%	≥90%
PMHF	$<10^{-7}\ h^{-1}$	$<10^{-7}\ h^{-1}$	$<10^{-8}\ h^{-1}$

①单点故障度量（Single－Point Fault Metric，SPFM）指标反映硬件安全机制或设计对单点故障（指未被安全机制覆盖，且直接导致违背安全目标的故障）和残余故障（指硬件要素中未被安全机制覆盖的故障）的覆盖是否足够。SPFM 值越高，表示相关硬件的单点和残余故障所占比例越低，系统可靠性越高。其计算公式[16]为：

$$S_{\mathrm{PFM}} = 1 - \sum_{\mathrm{SRHW}} (\lambda_{\mathrm{SPF}} + \lambda_{\mathrm{RF}}) / \sum_{\mathrm{SRHW}} \lambda \tag{3}$$

式中：S_{PFM} 表示 SPFM 值；λ 表示安全相关故障失效率；λ_{SPF} 表示单点故障失效率；λ_{RF} 表示残余故障的失效率；SRHW 表示与安全相关的硬件。

②潜伏故障度量（Latent Fault Metric，LFM）指标用于反映硬件安全机制和设计对潜伏故障的覆盖情况。LFM 值越高，表示硬件潜伏故障所占比例越低，系统可靠性越高。其计算公式[16]为：

$$L_{\mathrm{FM}} = 1 - \sum_{\mathrm{SRHW}} \lambda_{\mathrm{MPF\_Latent}} / \sum_{\mathrm{SRHW}} (\lambda - \lambda_{\mathrm{SPF}} - \lambda_{\mathrm{RF}}) \tag{4}$$

式中：L_{FM} 表示 LFM 值；$\lambda_{\mathrm{MPF\_Latent}}$ 表示多点潜伏故障失效率（多点故障是指多个独立故障组合后导致多点失效的故障）。

③硬件故障度量（Probabilistic Metric for Hardware Failure，PMHF）指标用于反映硬件随机失效导致违背安全目标的残余风险是否足够低。PMHF 值越低，表示系统可靠性越高。其计算公式[16]为：

$$P_{\mathrm{MHF}} = \lambda_{\mathrm{SPF}} + \lambda_{\mathrm{RF}} + \lambda_{\mathrm{DPF\_det}} \times \lambda_{\mathrm{DPF\_latent}} \times T_{\mathrm{Lifetime}} \tag{5}$$

式中：P_{MHF} 表示 PMHF 值；$\lambda_{\mathrm{DPF\_det}}$ 表示被探测并被告知的双点故障失效率（双点故障是指两个独立故障组合后导致双点失效的故障）；$\lambda_{\mathrm{DPF\_latent}}$ 表示潜伏双点故障失效率（潜伏故障是指安全机制未能探测到，且在故障探测时间区间内不能被驾驶员察觉的故障）；$T_{\mathrm{Lifetimet}}$ 表示整车生命周期。

基于上述方法导出的功能安全目标和功能安全要求，可用于指导和规范后续的系统设计、软件设计和硬件设计。

4　结束语

本文通过对电动汽车电机控制器基本功能的识别与相关项定义、风险分析及危害评估，确定了以“电机控制器提供转矩驱动力”这一基本功能为例的总体

功能安全目标。限于篇幅,仅以此功能为例,确定了功能安全目标(电机转矩的大小和方向需与转矩需求相符,且实际转矩与需求转矩的偏差需控制在一定范围内)、等级(ASIL C),并据此确定了其功能安全相关指标及需求。后续将以上述目标、等级、指标及需求作为系统、软件、硬件及其测试阶段的输入,开展设计和确认工作。

参考文献:

[1] 郭建. 汽车电子 ISO 26262:2018 标准概述(一)[Z/OL]. (2023-07-28)[2024-12-20]. https://mp.weixin.qq.com/s/jFvas24s3JKmZx-67KTgdQ.

[2] 中汽研科技. 汽车芯片功能安全 GB/T 34590《道路车辆功能安全》标准解读[Z/OL]. (2024-08-09)[2024-12-20]. https://mp.weixin.qq.com/s/OKxl4glth-bm6MlXuZD9yg.

[3] 李勇,汪伟,彭再武,等. 新能源商用车控制软件质量提升研究[J]. 客车技术与研究,2020,42(3):12-15.

[4] 伍理勋,陈建明,陈磊,等. 电动汽车电机驱动控制器功能安全架构研究[J]. 控制与信息技术,2018(3):1-5.

[5] 邵海贺,付越. 基于 GB/T 34590 标准的电动汽车用电池管理系统功能安全概念设计研究[J]. 中国汽车,2024(2):7-9.

[6] 邬肖鹏,刘飞,熊璐,等. ISO 26262 标准下永磁同步电机故障对整车安全性的影响分析[J]. 汽车技术,2013(2):13-18.

[7] 庄兴明,张琴. 基于 ISO 26262 标准的车用驱动电机系统设计研究[J]. 汽车零部件,2016(12):18-21.

[8] 刘佳熙,郭辉,李君. 汽车电子电气系统的功能安全标准 ISO 26262[J]. 上海汽车,2011(10):57-61.

[9] 杨晓彤,何放,黄德健. 基于 ISO 26262 的电子换挡系统功能安全概念阶段研究[J]. 企业科技与发展,2019(9):125-128.

[10] 文凯,夏珩,裴锋,等. 基于 ISO 26262 的电动四驱混合动力系统功能安全概念设计[J]. 机电工程技术,2012(12):74-76.

[11] 童菲. 基于 ISO 26262 的整车电源模式管理系统功能安全概念设计[J]. 机电一体化,2015,21(7):63-67.

[12] 葛鹏,陈勇,罗大国,等. 基于道路车辆功能安全标准 ISO 26262 的 7DCT 电控系统设计[J]. 汽车技术,2014(9):21-23.

[13] 朱叶. 基于 ISO 26262 的动力电池系统高压功能安全概念[J]. 汽车零部件,2013(10):97-100.

[14] SAE International. Considerations for ISO 26262 ASIL Hazard Classification:J2980_201804[S]. Rev. ed. New York:SAE International,2018:1-53.

[15] International Organization for Standardization. Road Vehicles-Functional Safety Part 3: Concept phase:ISO 26262-3:2018[S]. 2nd ed. Geneva:ISO,2018:1-34.

[16] International Organization for Standardization. Road Vehicles-Functional Safety Part 5: Product development at the hardware level:ISO 26262-5-2018[S]. 2nd ed. Geneva:ISO,2018:1-90.