

团 体 标 准

T/CMES XXXX—202X

代替 T/CMES XXXX—201X

道路车辆 线控制动系统功能安全概念阶段 S/E/C 参数量化评估规范

Specification for Quantitative S/E/C Parameter Assessment
in the Concept Phase of Functional Safety for
Brake-by-Wire Systems for Road Vehicles
(征求意见稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中国机械工程学会 发布

中国机械工程学会（英文简称 CMES）是具备开展国内、国际标准化活动资质的全国性社会团体。制定中国机械工程学会团体标准，以满足企业需要和市场需求，推动机械工业创新发展，是中国机械工程学会团体标准的工作内容之一。中国境内的团体和个人，均可提出制、修订中国机械工程学会团体标准的建议并参与有关工作。

中国机械工程学会团体标准按《中国机械工程学会标准化管理办法》进行制定和管理。

中国机械工程学会团体标准草案经向社会公开征求意见，并得到参加审定会议的 3/4 以上的专家、成员的投票赞同，方可作为中国机械工程学会团体标准予以发布。

在本标准实施过程中，如发现需要修改或补充之处，请将意见和有关资料寄给中国机械工程学会，以便修订时参考。

本标准版权为中国机械工程学会所有。除了用于国家法律或事先得到中国机械工程学会正式许可外，不许以任何形式复制、传播该标准或用于其他商业目的。

中国机械工程学会地址：北京市海淀区首体南路 9 号主语国际 4 座 11 层

邮政编码：100048 电话：010-68799027 传真：010-68799050

网址：www.cmes.org 联系人：袁俊瑞 电子信箱：yuanjr@cmes.org

目次

前言v

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 3

5 总则 3

 5.1 评估原则 3

 5.2 评估流程架构 4

 5.3 各步骤简要说明 4

 5.4 评估记录要求 5

6 线性制动系统与功能分析 5

 6.1 目的 5

 6.2 输入 5

 6.3 分析要求 5

 6.4 EHB 6

 6.5 EMB 8

 6.6 输出物要求 11

7 失效模式识别与量化 11

 7.1 目的 11

 7.2 输入 11

 7.3 分析方法 11

 7.4 分析步骤 12

 7.5 线控制动系统典型失效模式参考 13

 7.6 输出物要求 18

8 运行场景定义与量化 18

 8.1 目的 18

 8.2 输入准备 18

 8.3 场景定义框架 18

8.4 线控制动系统场景要素提取18

8.5 输出物汇总20

9 危害识别与定义20

9.1 目的20

9.2 输入准备20

9.3 分析步骤21

9.4 线控制动系统危害事件示例22

9.5 输出物汇总23

10 严重度（S）量化评估方法23

10.1 目的23

10.2 输入准备23

10.3 量化模型基础23

10.4 评估流程25

10.5 碰撞类型的确定26

10.6 碰撞速度的计算方法26

10.7 评估示例29

10.8 输出物汇总31

11 暴露率（E）量化评估方法31

11.1 目的31

11.2 输入准备31

11.3 量化模型基础31

11.4 评估流程34

11.5 评估示例35

11.6 输出物汇总36

12 可控性（C）量化评估方法36

12.1 目的36

12.2 输入准备36

12.3 量化模型基础36

12.4 评估步骤40

12.5 评估示例40

12.6 输出物汇总41

13 S/E/C 综合评估与 ASIL 等级确定41

13.1 目的41

13.2 输入准备 41

13.3 ASIL 等级判定 41

13.4 评估示例 42

13.5 输出物汇总 42

附 录 A （资料性附录） 功能-失效矩阵示例 43

附 录 B （资料性附录） 线控制动系统典型运行场景清单 49

附 录 C （资料性附录） 线控制动系统典型运行场景 S/E/C 评估与 ASIL 定级 58

参考文献 62

中国机械工程学学会标准征求意见稿

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。

本文件由中国机械工程学会提出并归口。

本文件起草单位：湖北文理学院、襄阳达安汽车检测中心有限公司、武汉理工大学、燕山大学、东风汽车集团有限公司研发总院、岚图汽车科技有限公司。

本文件主要起草人：陈运星、林凯、李梦林、钱闯、刘家杰、李亘、赵春来、夏冰、赵鼎晔、陈志军、闫梅、李海波、刘辉、吴华伟、张锐。

本文件首次制定。

中国机械工程学会标准征求意见稿

道路车辆 线控制动系统功能安全概念阶段 S/E/C 参数量化评估 规范

1 范围

本标准规定了线控制动系统（Brake-by-Wire, BbW）在功能安全（Functional Safety）概念阶段中，严重度、暴露率和可控性三个参数的量化评估方法、数据来源、评估流程及结果判定规则。

本标准适用于 M 类、N 类道路车辆的线控制动系统，包括 EHB、EMB 等，涵盖常规制动、紧急制动、AEB、ABS、EBD 等功能的危害分析与风险评估。

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/T 34590.3 2022 道路车辆 功能安全

GB/Z 42285 2022 道路车辆 电子电气系统 ASIL 等级确定方法指南

GB 21670 2025 乘用车制动系统技术要求及试验方法

T/CSAE 284.2 2022 自动驾驶乘用车 线控底盘性能要求及试验方法

3 术语和定义

GB/T 34590.1—2022 界定的以及下列术语和定义适用于本文件。

3.1

线控底盘系统 chassis-by-wire system

由线控驱动系统、线控制动系统、线控转向系统、线控驻车系统等一个或多个线控子系统组成，通过电信号传递驾驶员、驾驶辅助系统、自动驾驶系统或整车控制系统的控制指令，并由传感器、控制器、执行器、通信链路及电源系统协同实现车辆纵向、横向、驻车及相关底盘运动控制的系统。

3.2

线控制动系统 brake-by-wire system; BbW

通过电信号传递驾驶员、驾驶辅助系统、自动驾驶系统或整车控制系统的制动请求，由制动控制器控制制动执行器，实现制动力建立、分配、调节、反馈及故障响应的制动系统。

注：线控制动系统可包括电子液压制动系统、电子机械制动系统等技术路线。

3.3

电子液压制动系统 electro-hydraulic braking system; EHB

保留液压制动传递路径，由电子控制单元控制泵电机、电磁阀体等液压执行机构建立和调节制动压力，实现各轮制动力控制的线控制动系统。

3.4

电子机械制动系统 electro-mechanical braking system; EMB

取消传统液压制动回路，由电子控制单元直接控制各车轮处的电机卡钳或机电执行机构产生夹紧力，实现制动力建立、调节和反馈的线控制动系统。

3.5

中国典型场景库 China typical scenarios library

基于中国道路环境、交通状况及驾驶行为采集形成的标准化测试场景数据集。

3.6

自然驾驶数据 naturalistic driving data

在真实道路交通环境中，以不干预或低干预方式，通过车载传感器、车辆总线、定位设备、视频/雷达设备或数据记录系统持续采集的驾驶员操作、车辆状态、道路环境、交通参与者行为及系统运行状态等数据。

3.7

接管请求 takeover request

L3 级自动驾驶系统在其设计运行条件边界或发生系统故障时，向驾驶员发出的、要求其在规定时间内重新接管车辆控制权的强制性提示。

3.8

驾驶员接管能力 driver takeover capability

在系统失效或发出接管请求时，驾驶员恢复对车辆控制的有效性和及时性。

[基于 GB/T 40429—2021 相关术语扩展]

3.9

设计运行范围 operational design domain; ODD

驾驶自动化系统设计时确定的适用于其功能运行的外部环境条件。

注 1：典型外部环境条件包括道路、交通、天气、光照等。

[GB/T 40429—2021 规定了术语定义]

3.10

设计运行条件 operational design condition; ODC

驾驶自动化系统设计时确定的适用于其功能运行的各类条件的总称。

[GB/T 40429—2021 规定了术语定义；GB/T 45312—2025 规定了自动驾驶系统设计运行条件]

3.11

危害事件 hazardous event

危害与特定运行场景相结合后形成的事件。

3.12

严重度 severity; S

对特定运行场景中危害事件可能造成的人员伤害程度的预估等级。

注：本文件中，严重度等级用于S参数量化评估，通常可分为S0、S1、S2、S3。

[GB/T 34590.3—2022 规定了相关评估要求]

3.13

暴露概率/暴露率 exposure; E

车辆、驾驶员或其他交通参与者处于某一运行场景或运行条件中的概率、频率或时间占比。

[GB/T 34590.3—2022 规定了相关评估要求]

3.14

可控性 controllability; C

驾驶员或其他道路交通参与者在特定运行场景中避免事故或减轻危害后果的难易程度。

注：本文件中，可控性评估可综合考虑驾驶员反应时间、驾驶员接管能力、车辆动力学响应、制动系统剩余能力、人机交互提示有效性和道路附着条件等因素。

[GB/T 34590.3—2022 规定了相关评估要求，有修改]

3.15

汽车安全完整性等级 automotive safety integrity level; ASIL

用于表征安全相关电气/电子系统功能安全要求严格程度的等级，由危害事件的严重度、暴露概率和可控性组合确定。

[GB/T 34590.1—2022、GB/T 34590.3—2022 规定了术语定义和等级确定方法]

4 缩略语

下列缩略语适用于本文件。

CAN：控制器局域网（Controller Area Network）

CANFD：可变速率的控制器局域网（CAN with Flexible Data rate）

ETC：电子不停车收费（Electronic Toll Collection）

GNSS：全球导航卫星系统（Global Navigation Satellite System）

Lin：局域网互连网络（Local Interconnect Network）

MOST：面向媒体的系统传输总线（Media Oriented System Transport）

NFC：近距离无线通讯技术（Near Field Communication）

OBD：车载诊断（On-Board Diagnostics）

UDS：统一诊断服务（Unified Diagnostic Services）

USB：通用串行总线（Universal Serial Bus）

WLAN：无线局域网（Wireless Local Area Networks）

5 总则

5.1 评估原则

本标准规定的 S/E/C 量化评估遵循以下原则：

- a) 量化优先原则：在技术可行且数据可获取的条件下，应优先采用基于实测数据、仿真模型或统计分析的量化方法，减少对专家经验判断的单一依赖。量化方法应具有可复现性，即不同评估人员在相同输入条件下应得出相近的评估结果。对于线控制动系统，量化优先原则尤其重要，因为制动系统的失效后果与车速、减速度、路面附着等物理参数存在明确的函数关系，具备量化分析的基础条件。
- b) 场景驱动原则：评估应以典型运行场景为基础，充分考虑中国道路环境、交通状况及驾驶行为的本土化特征。场景的选择应覆盖线控制动系统实际运行中的典型工况，包括紧急制动、低速跟车、湿滑路面、坡道行驶等，避免因场景遗漏导致评估结果偏离实际风险水平。
- c) 数据支撑原则：评估结论应有明确的数据来源支撑，包括自然驾驶数据、场景库数据、交通事故统计、人因工程实验数据等。所有数据应注明来源、采集时间、样本量及版本信息，确保评估结论的可信度和可追溯性。对于线控制动系统，特别需要关注自动紧急制动（AEB）介入率、ABS 激活频率、路面附着分布等关键数据。
- d) 可追溯性原则：评估过程中的关键参数选取、假设条件设定及判定依据应完整记录，确保评估结果在后续审查或修订时能够追溯至原始输入和决策过程。任何基于专家经验的判断应有明确的理由说明。

5.2 评估流程架构

S/E/C 量化评估应按照图 5-1 所示的八个步骤依次进行。各步骤之间存在明确的输入输出关系，前一步骤的输出作为后一步骤的输入，确保评估过程的连贯性与可追溯性。

评估流程的设计体现了从“系统分析”到“风险量化”的逻辑递进关系。步骤 1 至步骤 4 完成基础分析工作，包括系统功能分析、失效模式识别、运行场景分析和危害事件定义；步骤 5 至步骤 7 分别对每个危害事件进行 S、E、C 三个参数的量化评估；步骤 8 综合前三步的结果，判定 ASIL 等级并形成评估报告。

各步骤的具体方法和要求详见第 6 章至第 13 章。

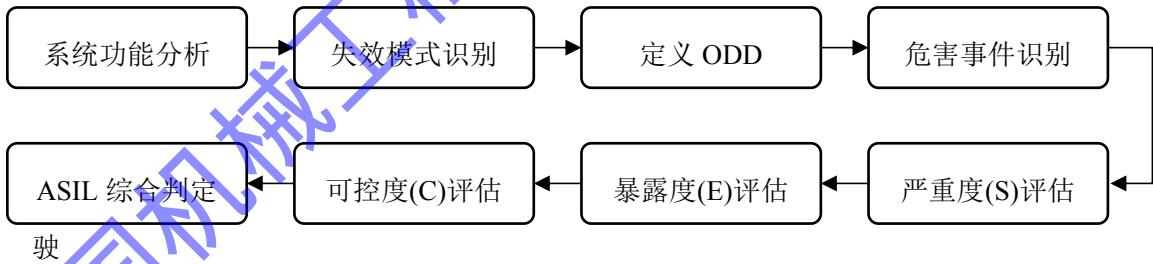


图 5-1 线控制动系统 S/E/C 量化评估总流程

5.3 各步骤简要说明

为便于理解评估流程的整体逻辑，以下对各步骤的核心内容进行简要说明：

步骤 1：线控制动系统与功能分析（详见第 6 章）

明确评估对象的系统边界、功能构成、系统间耦合关系及运行条件。输出组件清单和功能清单，为后续失效模式识别提供基础。

步骤 2：失效模式识别与量化（详见第 7 章）

识别线控制动系统可能发生的失效模式，分别针对线控制动的两种主要技术路线——EHB 与 EMB，识别其可能发生的失效模式。输出失效模式清单。

步骤 3：运行场景定义与量化（详见第 8 章）

识别可能触发或暴露失效模式的运行场景，并对场景的出现频率进行量化统计。重点场景包括紧急制动、低速跟车、湿滑路面、坡道行驶等。输出运行场景要素表和典型运行场景清单。

步骤 4：危害识别与定义（详见第 9 章）

将失效模式与运行场景结合，定义具体的危害事件。每个危害事件采用“在 X 场景下，Y 失效导致 Z 危害”的结构化描述，并明确驾驶模式。输出危害事件清单。

步骤 5：严重度 S 量化评估（详见第 10 章）

基于纵向碰撞能量模型，对每个危害事件量化严重度等级（S0~S3）。关键参数包括车速、减速度、路面附着、坡度、车辆载荷等。输出各危害事件的 S 等级。

步骤 6：暴露率 E 量化评估（详见第 11 章）

基于场景频率统计，对每个危害事件量化暴露率等级（E0~E4）。关键修正系数包括 AEB 介入率、ABS 激活频率、智驾模式占比、湿滑路面比例等。输出各危害事件的 E 等级。

步骤 7：可控性 C 量化评估（详见第 12 章）

综合评估驾驶员反应时间、车辆动力学响应、人机交互效果三个维度，对每个危害事件量化可控性等级（C0~C3）。输出各危害事件的 C 等级。

步骤 8：ASIL 等级综合判定与报告（详见第 13 章）

综合 S/E/C 评估结果，依据 ISO 26262-3 确定 ASIL 等级，处理多危害事件和组合危害，编制评估报告。输出各危害事件的 ASIL 等级、系统安全目标等级、评估报告。

5.4 评估记录要求

评估过程中应保留以下记录，确保评估结果可追溯、可复现：

- 各步骤输入数据的来源、采集时间、样本量及版本号；
- 各步骤输出结果及计算过程，包括中间计算值和最终判定结果；
- 关键假设及判定依据的详细说明，如假设的驾驶员反应时间等；
- 评估人员、审核人员、批准人员及日期；
- 评估报告的版本历史及修订说明，包括每次修订的内容、原因和日期。

6 线性制动系统与功能分析

6.1 目的

线控制动系统与功能分析是 S/E/C 量化评估的起点。本章旨在明确评估对象的系统边界、功能构成及功能描述，为后续的失效模式识别、场景分析和危害定义提供结构化、可量化的基础输入。

6.2 输入

开展系统与功能分析所需的主要输入包括：

- 线控底盘系统架构图（含硬件拓扑、软件架构、通信网络）；
- 系统功能需求文档；
- 系统接口定义文件（含内部接口与外部接口）；
- 冗余架构设计说明（如双电机、双控制器、双通信链路）；
- 系统运行条件定义（如车速范围、驾驶模式、环境条件）。

6.3 分析要求

线控制动系统依据执行器类型可分为两类架构：EHB 和 EMB。两类架构在组件构成、功能实现方式及失效模式上存在本质差异，需分别进行系统与功能分析。

6.4 EHB

EHB 保留液压传递路径，通过电控单元驱动泵电机建压，并由电磁阀体精确分配各轮制动压力，取消了传统真空助力器与机械式比例阀^[1]。其典型系统架构如图 6-1 所示。

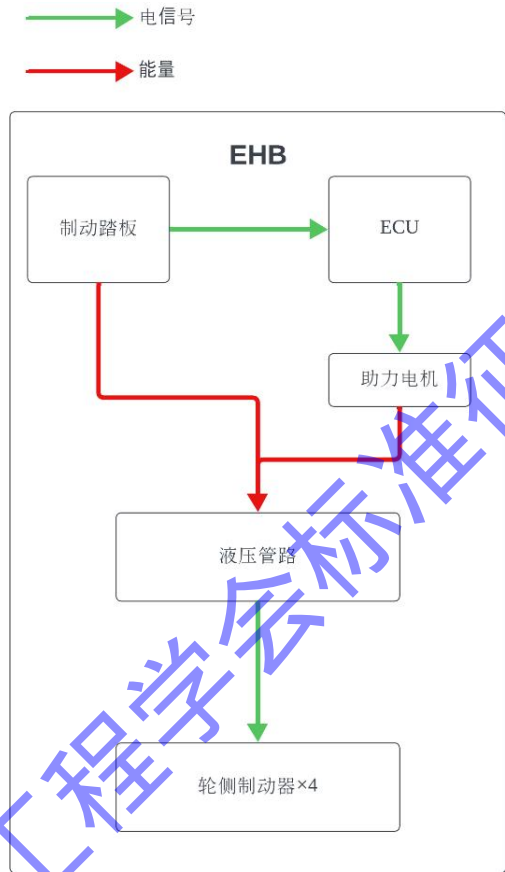


图 6-1 EHB 系统架构图

依据图 6-1 所示架构，评估人员应识别 EHB 系统的传感器、控制器、执行器与通信链路，形成组件清单，作为输出物 6-2 的组成部分。EHB 系统典型组件清单如表 6-1 所示。

表 6-1 EHB 系统典型组件清单

组件类型	组件名称	功能定位
传感器	制动踏板位移传感器	采集踏板行程，解析驾驶员制动意图
传感器	踏板力传感器	与位移信号共同用于制动意图解析
传感器	制动压力传感器	采集主缸及各轮缸液压压力，用于压力闭环控制
传感器	轮速传感器	采集各轮转速，用于 ABS/ESC/EBD 滑移率计算
传感器	加速度传感器（IMU）	采集纵向/侧向加速度及横摆角速度，用于动态稳定控制
控制器	制动域主控制器	执行制动力解算与主动安全功能控制
控制器	制动域备用控制器	主控制器失效时接管基础制动功能
执行器	电子液压制动单元（EHB）	驱动泵电机建立液压压力，通过电磁阀分配各轮制动压力

组件类型	组件名称	功能定位
执行器	制动泵电机	为液压回路建立高压制动液压
执行器	电磁阀体	控制各轮缸液压通断与压力调节
通信链路	CAN/CANFD	承载控制器与整车各域之间的控制指令与状态信号
通信链路	车载以太网	承载自动驾驶/ADAS 域与制动域之间的高带宽指令通信
通信链路	SENT	踏板及压力传感器至控制器的点对点高速数字信号传输

表 6-1 EHB 系统典型组件清单(续)

组件类型	组件名称	功能定位
通信链路	PSI5	轮速传感器至控制器的双向数字信号传输，支持传感器状态反馈

在完成组件识别后，评估人员应结合 EHB 系统功能需求文档，逐项梳理系统所支持的功能，形成功能清单，作为输出物 6-1 的组成部分。如表 6-2 所示。

表 6-2 EHB 系统典型功能清单

功能编号	功能名称	功能类别	功能说明
EHB-F-01	常规制动	基础制动	驾驶员踩踏制动踏板时，系统采集踏板位移与踏板力信号，解算目标制动力，通过 EHB 精确建立各轮液压压力，产生对应制动力矩
EHB-F-02	制动踏板感模拟	基础制动	系统通过踏板模拟器提供可调节的踏板力-位移特性，模拟传统液压制动的踏板感，满足驾驶员操控预期
EHB-F-03	制动压力精确控制	基础制动	依据目标压力与实际压力的偏差，动态调节电磁阀开度及泵电机转速，实现各轮制动压力的毫秒级精确跟随
EHB-F-04	防抱死制动（ABS）	主动安全	实时监测各轮轮速，识别车轮抱死趋势，通过增压/保压/减压循环调节各轮液压压力，防止车轮锁死
EHB-F-05	电子制动力分配（EBD）	主动安全	根据车辆载荷分布与轴荷转移，动态优化前后轴及左右轮制动力分配比例，防止后轴提前抱死
EHB-F-06	牵引力控制（TCS）	主动安全	检测驱动轮滑转，通过对滑转轮施加液压制动力矩并协调降低驱动力矩，抑制驱动轮过度打滑
EHB-F-07	电子稳定控制（ESC）	主动安全	识别转向不足/转向过度趋势，通过对单侧车轮施加差异液压制动力矩，修正车辆运动轨迹，抑制侧滑
EHB-F-08	制动辅助（BA）	主动安全	检测到紧急制动意图时，自动补充建立更高液压压力至 ABS 激活阈值，缩短制动距离
EHB-F-09	自动紧急制动执行（AEB） ^{[2][3][4]}	主动安全	接收 ADAS 或自动驾驶域控制器的紧急制动指令，自主建立高压液压制动力，执行完整制动至车辆停止
EHB-F-10	再生制动协调	能量管理	优先使用电机回馈制动力矩，不足部分由液压制动补充，在回馈能力变化时实现液压与回馈的平顺切换
EHB-F-11	制动能量回收模式管理	能量管理	根据电池 SOC、温度及驾驶模式，动态调整最大允许回收功率，协调再生制动与液压制动的分配策略
EHB-F-12	电子驻车制动（EPB）	驻车功能	驱动后轴卡钳夹紧制动盘并自锁，实现可靠驻车保持；释放时解除夹紧，可与自动驻车保持功能联动

EHB-F-13	自动驻车保持（Auto Hold）	驻车功能	车辆停止后自动维持液压压力防止溜动；检测到起步意图时平顺释放制动力
EHB-F-14	坡道辅助（HAC）	驻车功能	坡道起步时短暂保持液压制动压力，防止车辆后溜，待驱动力充分建立后平顺释放
EHB-F-15	液压系统自检	系统监控	系统上电及运行过程中定期验证电磁阀开关特性、泵电机建压能力及液压回路密封性

表 6-2 EHB 系统典型功能清单(续)

功能编号	功能名称	功能类别	功能说明
EHB-F-16	制动系统健康监测	系统监控	持续监测液压压力、传感器信号完整性、控制器状态及通信链路质量，识别异常并触发告警与降级响应
EHB-F-17	制动热管理	系统监控	监测制动盘及卡钳温度，在持续高强度制动工况下协调再生制动与液压制动分担比例，防止热衰退
EHB-F-18	冗余制动控制	功能安全	主控制器或主通信链路故障时，备用控制器接管制动功能，利用冗余液压回路维持基础制动能力
EHB-F-19	系统降级管理	功能安全	根据传感器故障、控制器异常、通信中断等故障类型，按预定策略切换工作模式，并输出故障状态信息
EHB-F-20	自动驾驶制动执行接口	系统集成	提供标准化减速度控制接口，接收自动驾驶系统的目标减速度指令，执行精确液压制动控制并反馈实际状态
EHB-F-21	制动信号输出与状态反馈	系统集成	向整车其他域控制器实时输出制动激活状态、各轮压力值、ABS/ESC 激活状态及系统故障状态等信息

6.5 EMB

EMB 完全取消液压回路，由控制器直接驱动每个车轮处的电机卡钳加进制动盘，实现纯电气化制动力传递。其典型系统架构图如 6-2 所示。

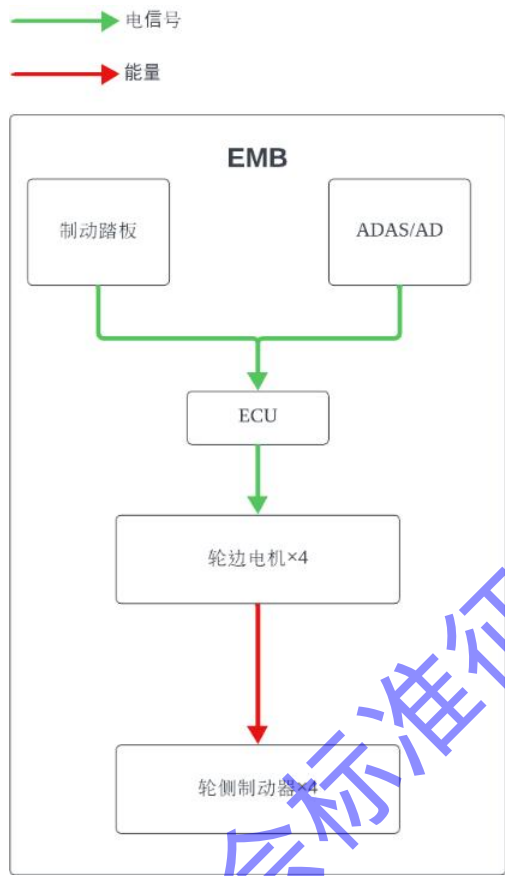


图 6-2 EMB 系统架构图

依据图 6-2 所示架构，评估人员应识别 EMB 系统的传感器、控制器、执行器与通信链路，形成组件清单，作为输出物 6-2 的组成部分。EMB 系统典型组件清单如表 6-3 所示。

表 6-3 EMB 系统典型组件清单

组件类型	组件名称	功能定位
传感器	制动踏板位移传感器	采集踏板行程，解析驾驶员制动意图
传感器	踏板力传感器	与位移信号共同用于制动意图解析
传感器	夹紧力传感器	采集卡钳实际夹紧力，用于制动力闭环控制
传感器	电机位置传感器	采集卡钳电机转角，用于位置闭环与夹紧力估算
传感器	轮速传感器	采集各轮转速，用于 ABS/ESC/EBD 滑移率计算
传感器	加速度传感器（IMU）	采集纵向/侧向加速度及横摆角速度，用于动态稳定控制
控制器	制动域主控制器	执行制动力解算、卡钳电机指令输出与主动安全功能控制
控制器	制动域备用控制器	主控制器失效时接管基础制动功能
执行器	电子机械制动卡钳（EMB）	集成电机、减速机构与夹紧机构，直接驱动制动盘产生制动力
执行器	卡钳电机驱动器	接收控制器指令，驱动卡钳电机输出目标力矩
通信链路	CAN/CANFD	承载控制器与整车各域之间的控制指令与状态信号
通信链路	车载以太网	承载自动驾驶/ADAS 域与制动域之间的高带宽指令通信
通信链路	SENT/PSI5	传感器至控制器的高速数字信号传输

在完成组件识别后，评估人员应结合 EMB 系统功能需求文档，逐项梳理系统所支持的功能，形成功能清单，作为输出物 6-2 的组成部分。如表 6-4 所示。

表 6-4 EMB 系统典型功能清单

功能编号	功能名称	功能类别	功能说明
EMB-F-01	常规制动	基础制动	驾驶员踩踏制动踏板时，系统采集踏板位移与踏板力信号，解算目标制动力，直接驱动各轮卡钳电机产生对应夹紧力
EMB-F-02	制动踏板感模拟	基础制动	系统通过踏板模拟器提供可调节的踏板力-位移特性，模拟传统制动的踏板感，满足驾驶员操控预期
EMB-F-03	夹紧力精确控制	基础制动	依据目标夹紧力与实际夹紧力的偏差，动态调节卡钳电机驱动电流与转角，实现各轮制动力的精确闭环跟随
EMB-F-04	电机位置控制	基础制动	通过电机位置传感器采集卡钳电机转角，实现卡钳行程的精确控制，支持夹紧力估算与快速响应
EMB-F-05	防抱死制动（ABS）	主动安全	实时监测各轮轮速，识别车轮抱死趋势，通过调节卡钳电机夹紧力循环，防止车轮锁死
EMB-F-06	电子制动力分配（EBD）	主动安全	根据车辆载荷分布与轴荷转移，动态优化前后轴及左右轮卡钳夹紧力分配比例，防止后轴提前抱死
EMB-F-07	牵引力控制（TCS）	主动安全	检测驱动轮滑转，通过对滑转轮卡钳施加夹紧力并协调降低驱动力矩，抑制驱动轮过度打滑
EMB-F-08	电子稳定控制（ESC）	主动安全	识别转向不足/转向过度趋势，通过对单侧车轮卡钳施加差异夹紧力，修正车辆运动轨迹，抑制侧滑

表 6-4 EMB 系统典型功能清单(续)

功能编号	功能名称	功能类别	功能说明
EMB-F-09	制动辅助（BA）	主动安全	检测到紧急制动意图时，自动提升卡钳夹紧力至 ABS 激活阈值，缩短制动距离
EMB-F-10	自动紧急制动执行（AEB）	主动安全	接收 ADAS 或自动驾驶域控制器的紧急制动指令，自主驱动各轮卡钳电机至最大夹紧力，执行完整制动至车辆停止
EMB-F-11	再生制动协调	能量管理	优先使用电机回馈制动力矩，不足部分由卡钳夹紧力补充，在回馈能力变化时实现电机制动与夹紧力的平顺切换
EMB-F-12	制动能量回收模式管理	能量管理	根据电池 SOC、温度及驾驶模式，动态调整最大允许回收功率，协调再生制动与卡钳夹紧力的分配策略
EMB-F-13	电子驻车制动（EPB）	驻车功能	驱动卡钳电机夹紧制动盘并通过自锁机构保持，实现可靠驻车；释放时反转电机解除夹紧
EMB-F-14	自动驻车保持（Auto Hold）	驻车功能	车辆停止后自动保持卡钳夹紧力防止溜动；检测到起步意图时平顺释放夹紧力
EMB-F-15	坡道辅助（HAC）	驻车功能	坡道起步时短暂保持卡钳夹紧力，防止车辆后溜，待驱动力充分建立后平顺释放
EMB-F-16	卡钳电机自检	系统监控	系统上电及运行过程中定期验证各轮卡钳电机驱动能力、位置

			传感器信号完整性及自锁机构状态
EMB-F-17	制动系统健康监测	系统监控	持续监测夹紧力传感器、电机位置传感器、控制器状态及通信链路质量，识别异常并触发警告与降级响应
EMB-F-18	制动热管理	系统监控	监测卡钳电机及制动盘温度，在持续高强度制动工况下协调再生制动与卡钳夹紧力分担比例，防止电机过热
EMB-F-19	冗余制动控制	功能安全	主控制器或主通信链路故障时，备用控制器接管制动功能，维持各轮卡钳基础夹紧力控制能力
EMB-F-20	系统降级管理	功能安全	根据传感器故障、控制器异常、通信中断等故障类型，按预定策略切换工作模式，并输出故障状态信息
EMB-F-21	自动驾驶制动执行接口	系统集成	提供标准化减速度控制接口，接收自动驾驶系统的目标减速度指令，执行精确卡钳夹紧力控制并反馈实际状态
EMB-F-22	制动信号输出与状态反馈	系统集成	向整车其他域控制器实时输出制动激活状态、各轮夹紧力值、ABS/ESC 激活状态及系统故障状态等信息

6.6 输出物要求

系统与功能分析完成后，评估人员应形成以下输出物：

输出物 6-1 组件清单：参考表 6-1、表 6-3，包含线控制动系统的硬件组成（传感器、控制器、执行器、通信链路）。

输出物 6-2 功能清单：参考表 6-2、表 6-4，包含线控制动系统的核心功能、功能类别及功能说明。评估人员应根据实际系统配置识别具体功能，并注明不同主机厂功能定义可能存在差异。该输出物用于失效模式识别，因为功能是失效模式的基础，需针对每个功能分析其可能发生的失效。

7 失效模式识别与量化

7.1 目的

本章旨在系统性地识别线控制动系统可能发生的失效模式，为后续运行场景分析、危害定义及 S/E/C 量化评估提供基础输入。失效模式的识别应采用系统化的分析方法，确保识别过程的完整性、可追溯性和可复现性。

7.2 输入

在开始本章分析前，评估人员应准备好以下输入资料：

表 7-1 输入准备规范、规程和指南的对比

资料名称	来源	说明
组件清单	第 6 章输出物 6-1	明确评估范围，识别硬件组成和冗余架构
功能清单	第 6 章输出物 6-2	明确系统有哪些功能，功能是失效模式的基础
系统架构设计文档	系统设计部门	了解各功能的实现原理、信号流和控制逻辑

7.3 分析方法

失效模式的识别采用“功能-失效矩阵”方法^[5]，该方法以系统功能为起点，从多个维度系统性

地分析每个功能可能发生的失效。示例矩阵详见附录 A。该方法具有以下特点：

- 系统性：覆盖所有功能，避免遗漏。
- 结构化：采用统一的分类维度，便于横向比较。
- 可追溯：每个失效模式均可追溯到其关联功能和失效原因。

7.4 分析步骤

评估人员应按照以下步骤完成失效模式的系统化识别。

7.4.1 确定分析对象

以第 6 章识别的功能清单为基础，将每个功能作为独立的分析对象。评估人员应列出所有需要分析的功能，并为每个功能分配唯一标识。

线控制动系统通常涉及以下功能域：

表 7-2 线控制动系统功能域

功能域	典型功能
常规制动功能	常规制动助力、电子制动力分配（EBD）
稳定性控制功能	防抱死制动（ABS）、车身稳定控制（ESC）
高级辅助制动功能	自动紧急制动（AEB）执行、自适应巡航（ACC）减速执行
坡道辅助功能	坡道辅助（HHC）、陡坡缓降（HDC）
驻车关联功能	自动驻车（Auto Hold）、电子驻车制动（EPB）执行
再生制动功能	再生制动协调
安全功能	故障诊断与响应、冗余切换

7.4.2 分析功能实现原理

针对每个分析对象，评估人员需理解其正常工作的实现原理，梳理功能实现的关键环节：

- a) 输入信号：功能执行所需的输入信号（如车速、轮速、踏板位移、制动压力、智驾指令等）
- b) 供电条件：功能执行所需的电源供应（如控制器供电、执行器供电）
- c) 通信链路：功能执行所依赖的通信通道（如 CAN 总线、以太网）
- d) 控制逻辑：功能执行的控制算法和判断逻辑
- e) 执行机构：功能执行所依赖的物理执行部件（如电机、泵、阀）

7.4.3 确定失效分类维度

失效模式的识别从以下三个核心维度展开：

表 7-3 失效模式分析维度

失效维度	定义	典型表现
功能丧失	功能完全无法执行或执行能力显著低于设计要求	制动力完全丧失、ABS 不工作
功能异常	功能执行但性能不符合设计要求	制动力不足、响应延迟、制动不平衡
非预期功能	系统产生了不属于该功能要求的输出	无制动指令时自行制动、ABS 误触发

7.4.4 系统化识别失效模式

评估人员应采用以下方法识别失效模式。当功能实现链条清晰时，宜采用方法一；方法二可单独使用，也可用于对方法一识别结果进行完整性验证。

方法一：基于功能实现环节分解

将功能的实现过程分解为多个关键环节，针对每个环节逐一分析可能发生的失效：

表 7-4 基于功能实现环节的失效原因识别

实现环节	可能失效
输入信号	信号丢失、信号偏差、信号延迟、信号噪声等
供电	电源中断、电压跌落、电源噪声等
通信	通信中断、数据错误、延迟超限等
控制逻辑	逻辑错误、计算错误、判断失误等
执行机构	卡滞、断线、性能下降、响应延迟等

方法二：基于失效维度逐项分析

针对每个功能，从“功能丧失”、“功能异常”、“非预期功能”三个维度逐项分析，记录所有识别到的失效模式，确保每个失效模式都能追溯到合理的失效原因。

7.4.5 整理形成失效模式清单

将识别出的所有失效模式进行汇总、归类，形成结构化的失效模式清单。清单应包含以下要素：

表 7-5 失效模式整理清单

要素	说明
失效编号	唯一标识，采用“BR-序号”格式
关联功能	指明该失效模式对应哪个功能

表 7-5 失效模式整理清单(续)

要素	说明
失效维度	功能丧失/功能异常/非预期功能
失效模式	简明扼要地描述失效现象
失效描述	详细说明失效的具体表现
可能的失效原因	列出导致该失效的典型原因

7.5 线控制动系统典型失效模式参考

以下列出了线控制动系统常见的失效模式，评估人员可参照本节的分析方法，根据实际系统配置进行调整：

表 7-6 线控制动系统经典失效模式参考表

失效编号	关联功能	失效模式	失效维度	适用架构	底层物理失效原因
BR-01	常规制动	制动力丧失/卡钳夹紧力丧失	功能丧失	ALL	EHB：液压管路严重破裂、制动液泄漏导致主回路无法建压。

					EMB: 轮端卡钳电机物理断电、高压/低压供电全面崩溃。
BR-02	常规制动	制动助力不足/夹紧力不足	功能异常	ALL	EHB: 泵电机建压能力下降、系统内部渗入空气。 EMB: 电机因长下坡过载引发发热衰退、驱动电流受限。
BR-03	常规制动	制动响应延迟	功能异常	ALL	控制器主任务周期过载、总线通信丢包、执行机构克服空行程/背隙时间过长。
BR-04	常规制动	制动拖滞(卡钳无法完全释放)	功能异常	ALL	EHB: 阀体卸压卡滞、机械回位弹簧断裂。 EMB: 滚珠丝杠背隙补偿错误、主动回位控制算法异常。
BR-05	常规制动	非预期制动	非预期功能	ALL	核心控制算法计算错误、踏板传感器信号突发严重正向漂移、总线突发恶意减速度指令。
BR-06	踏板感模拟	踏板感丧失	功能丧失	ALL	踏板模拟器内部机械断裂、行程反馈机构物理脱落。
BR-07	踏板感模拟	踏板感异常	功能异常	ALL	EHB: 模拟器隔离阀在常规制动时异常关闭。 EMB/ALL: 模拟器机械导向槽异物卡滞、弹簧刚度随寿命老化漂移。
BR-08	压力/夹紧力精确控制	压力控制失效/闭环控制失效	功能丧失	ALL	轮缸压力传感器(EHB)或夹紧力传感器(EMB)物理断线, 导致闭环控制链条彻底断开。
BR-09	压力/夹紧力精确控制	压力控制偏差过大/夹紧力控制偏差	功能异常	ALL	压力/夹紧力传感器发生线性漂移、底层执行器驱动芯片(MOSFET)发热导致电流控制不准。
BR-10	压力/夹紧力精确控制	压力控制振荡 / 夹紧力振荡	功能异常	ALL	底层 PID/调速器控制参数与当前制动盘刚度不匹配、传感器受高频电磁干扰导致反馈信号抖动。

表 7-6 线控制动系统经典失效模式参考表(续)

失效编号	关联功能	失效模式	失效维度	适用架构	底层物理失效原因
BR-11	电机位置控制	位置控制失效	功能丧失	EMB	卡钳电机位置传感器(如旋变或霍尔)物理损坏、信号传输线路断路。
BR-12	电机位置控制	位置控制偏差	功能异常	EMB	位置传感器正余弦信号调理电路增益失准、转子初始零位写入错误。
BR-13	电机位置控制	位置传感器信号失真	功能异常	EMB	轮端强电磁干扰、编码器磁环磨损或附着铁屑导致信号丢步。
BR-14	防抱死制动	ABS 功能丧失	功能丧失	ALL	轮速传感器物理损坏信号中断、底层滑移率控制算法锁死崩溃。
BR-15	防抱死制动	ABS 调压异常/夹紧力调节异常	功能异常	ALL	EHB: 高速高速开关阀响应迟缓。 EMB: 电机高频动态换向(正反转切换)性能因温升衰减。
BR-16	防抱死制动	ABS 误触发	非预期	ALL	轮速信号受电磁干扰产生严重瞬态噪声(误判为车

			功能		轮锁死)、车辆基准车速算法估算错误。
BR-17	电子制动力分配	EBD 功能丧失	功能丧失	ALL	轴荷估算算法死机、关键纵向加速度传感器故障。
BR-18	电子制动力分配	左右轮制动不平衡 / 轮间不均	功能异常	ALL	单侧执行机构特性差异(如 EHB 单侧阀门磨损、EMB 单侧卡钳摩擦非线性漂移)。
BR-19	牵引力控制	TCS 功能丧失	功能丧失	ALL	驱动轮滑移率计算逻辑错误、主动建压源 (EHB 泵电机/EMB 单轮执行器) 响应失效。
BR-20	牵引力控制	TCS 介入不及时	功能异常	ALL	软件诊断消抖时间设计过长、低附着路面识别算法逻辑存在迟滞。
BR-21	牵引力控制	TCS 误介入	非预期功能	ALL	常规路面行驶时, 由于轮速瞬态信号丢失, 算法误判驱动轮打滑而异常主动建压。
BR-22	电子稳定控制	ESC 功能丧失	功能丧失	ALL	IMU 完全失效、横摆角速度与侧倾角估算逻辑死锁。
BR-23	电子稳定控制	ESC 干预力矩异常/差异夹紧力异常	功能异常	ALL	SAS 发生零点漂移, 导致车辆目标轨迹预测算法计算出的修正力矩偏大或偏小。
BR-24	电子稳定控制	ESC 误激活	非预期功能	ALL	车辆平顺路面直线行驶时, IMU 受强振动干扰产生阶跃突变信号, 触发单侧车轮脉冲式主动制动。
BR-25	制动辅助	BA 功能丧失	功能丧失	ALL	踏板速度解析算法异常终止, 紧急制动意图无法被正确识别。
BR-26	制动辅助	BA 建压不足/夹紧力提升不足	功能异常	ALL	执行器极限建压速率 (Bar/s 或 kN/s) 受限、低电压工况大功率驱动受限。

表 7-6 线控制动系统经典失效模式参考表(续)

失效编号	关联功能	失效模式	失效维度	适用架构	底层物理失效原因
BR-27	制动辅助	BA 误触发	非预期功能	ALL	驾驶员快速松开并重踩踏板的常规操作, 被高频滤波算法误判为紧急避险制动, 触发最高系统增压。
BR-28	自动紧急制动	AEB 执行失效	功能丧失	ALL	车载以太网或智驾私有总线中断、智驾接口协议安全校验失败。
BR-29	自动紧急制动	AEB 执行延迟	功能异常	ALL	智驾接口数据网关转发队列积压、制动控制器接口任务优先级配置不当。
BR-30	自动紧急制动	AEB 非预期触发	非预期功能	ALL	智驾接口层软件逻辑异常, 将常规 ACC 减速度请求误解析为最高优先级的 AEB 硬制动指令。
BR-31	再生制动协调	再生制动协调功能丧失	功能丧失	ALL	动能回收私有 CAN/LIN 通信彻底中断, 制动系统无法获取电驱动反馈数据。

BR-32	再生制动协调	切换制动力突变	功能异常	ALL	电驱系统电机制动力矩反馈值精度超差，线控制动机械力矩未能同步实现高精度等额补偿。
BR-33	再生制动协调	液压过度介入 / 卡钳夹紧力过度介入	非预期功能	ALL	控制协调算法在电驱动回收能力充足时，因逻辑判断错误，额外输出机械制动力矩导致总制动力超标。
BR-34	再生制动模式管理	回收模式管理失效	功能丧失	ALL	回收模式状态机死锁，系统无法在强/弱回收模式之间进行动态切换。
BR-35	再生制动模式管理	回收功率偏离目标值	功能异常	ALL	电池 SOC 或环境温度数据读取错误，导致最大允许回收功率限制策略出现偏差。
BR-36	电子驻车制动	EPB 无法夹紧	功能丧失	ALL	EPB 驻车电机烧毁、断路，或者底层卡钳自锁螺杆/丝杠卡爪物理磨损断裂。
BR-37	电子驻车制动	EPB 夹紧力不足/自锁力不足	功能异常	ALL	驻车拉索疲劳拉伸、驻车电机限流保护阈值因温度误判定而提前触发。
BR-38	电子驻车制动	EPB 无法释放/电机无法反转释放	功能异常	ALL	控制器 H 桥驱动芯片故障无法实现电流反转、丝杠机械卡死在最紧端。
BR-39	电子驻车制动	EPB 误释放	非预期功能	ALL	车辆静态驻车时，EPB 开关信号线由于短路产生虚假释放脉冲，造成非预期解除自锁。
BR-40	自动驻车保持	驻车保持功能失效	功能丧失	ALL	EHB: 主缸保压电磁阀发生物理内漏、系统无法维持静止液压。 EMB: 轮端电机由于长时间静态保持过热而无法维持力矩。
BR-41	自动驻车保持	意外自动释放/意外释放夹紧力	非预期功能	ALL	车辆起步驱动力协调逻辑（根据离合器/油门开度）出现误判，在驱动力未建立时提前解锁。

表 7-6 线控制动系统经典失效模式参考表(续)

失效编号	关联功能	失效模式	失效维度	适用架构	底层物理失效原因
BR-42	坡道辅助	坡道辅助失效	功能丧失	ALL	坡度传感器（IMU）物理损毁，无法输出合法的坡度倾角信息。
BR-43	坡道辅助	制动/夹紧力保持时间异常	功能异常	ALL	系统的软件定时器周期溢出或时钟漂移，导致坡道起步 2 秒的延时保持功能过早或过晚释放。
BR-44	系统自检（液压/电机）	自检功能失效	功能丧失	ALL	自检状态机调度逻辑异常，上电后未能按时启动系统基础诊断。
BR-45	系统自检（液压/电机）	漏检故障	功能异常	ALL	诊断窗口期设置过短、故障诊断阈值由于算法迭代被错误放宽，导致微小泄压或断相未报出。
BR-46	系统自检	误报故障	非预期	ALL	自检滤波算法消抖时间过短，将低压电源暂态波动

	(液 压 / 电 机)		功能		(如起动瞬态跌落) 误判为硬件永久损坏。
BR-47	制动系统健康监测	故障检测失效	功能丧失	ALL	运行期在线故障矩阵配置表损坏(软失效), 导致严重运行时故障发生时无法触发降级。
BR-48	制动系统健康监测	告警输出延迟	功能异常	ALL	仪表盘 HMI 告警总线报文发送优先级过低, 告警发送时间超过安全容错时间(FTTI)。
BR-49	制动系统健康监测	虚假告警输出	非预期功能	ALL	软件诊断层逻辑互锁设计存在死角, 正常工况下误报 ASIL D 级别故障导致红灯亮起。
BR-50	制动热管理	热管理功能失效	功能丧失	ALL	热管理软件模块意外挂起、温升预测估算模型停止运行。
BR-51	制动热管理	温度监测偏差 / 电机温度监测偏差	功能异常	ALL	EHB: 制动盘温升数学估算模型参数未适配刹车片磨损。 EMB: 轮端卡钳电机内置 NTC 热敏电阻阻值随寿命发生严重漂移。
BR-52	冗余制动控制	冗余切换失效	功能丧失	ALL	冗余硬件心跳监测电路物理损坏、状态机切换存在逻辑互锁死角, 备用 ECU 无法接管。
BR-53	冗余制动控制	切换响应延迟	功能异常	ALL	主/备控制器同步握手协议超时, 导致切换接管时间超过了底盘动态 FTTI 安全要求。
BR-54	冗余制动控制	误切换至备用控制器	非预期功能	ALL	主控制器运行完全正常, 因冗余总线偶发性电磁干扰触发误判, 导致非预期切入备用基础制动。
BR-55	系统降级管理	降级切换失效	功能丧失	ALL	降级策略机状态跳转配置错误, 系统在发生重大故障后锁死在原状态, 拒绝进入跛行模式。
BR-56	系统降级管理	降级策略执行异常	功能异常	ALL	系统进入降级模式后, 输出的限定力矩或报警声音级别与既定的安全目标策略不符。

表 7-6 线控制动系统经典失效模式参考表(续)

失效编号	关联功能	失效模式	失效维度	适用架构	底层物理失效原因
BR-57	自驾制动执行接口	接口通信失效	功能丧失	ALL	智驾域与制动域之间的物理网线或总线断开, 智驾减速度目标报文接收中断。
BR-58	自驾制动执行接口	减速度执行偏差	功能异常	ALL	制动减速度闭环控制算法中, 未有效补偿整车车辆质量变化(空载 vs 满载), 导致执行差额过大。
BR-59	自驾制动执行接口	非预期执行制动指令	非预期功能	ALL	通信链路发生严重数据错位, 制动系统误将常规心跳报文中的特定字段解析为高减速度请求。
BR-60	信号输出与状态反馈	信号输出中断	功能丧失	ALL	状态反馈报文在发送总线发送缓冲队列中死锁, 导致动力域/车身域无法获取当前制动状态。
BR-61	信号输出与状态反馈	信号值错误	功能异常	ALL	控制器内部 RAM 发生单比特翻转(未配置 ECC 保护), 导致发送给整车的“实际各轮压力值/夹紧力”错误。

7.6 输出物要求

完成本章分析后，评估人员应形成以下输出物：

输出物 7-1 失效模式清单：包含失效编号、关联功能、失效维度、失效模式、失效描述、可能的失效原因。清单应通过系统化的分析方法生成，并根据实际系统配置进行调整。该输出物用于后续运行场景分析（第 8 章）和危害定义（第 9 章）。

8 运行场景定义与量化

8.1 目的

本章旨在基于 ODD 场景库的分层架构，定义线控制动系统在运行过程中可能触发的各类场景。通过系统性地识别场景要素，为后续危害识别与暴露率评估提供基础输入。

8.2 输入准备

在开始本章分析前，评估人员应准备好以下输入资料：

表 8-1 输入准备

资料名称	来源	说明
功能清单	第 6 章输出物 6-1 和 6-2	明确系统功能，帮助确定功能激活的场景
失效模式清单	第 7 章输出 7-1	明确失效模式，确定失效可能发生的场景
预期功能安全场景库	中国智能网联汽车产业创新联盟预期功能安全工作组（CAICV）	提供场景分层架构和要素分类

8.3 场景定义框架

本标准采用预期功能安全场景库的七层架构定义运行场景。该架构将场景要素划分为七个层级，每层包含影响制动系统功能的若干参数：

表 8-2 预期功能安全场景架构

层级	名称	说明
第 1 层	道路结构	道路几何形状、路面类型、车道配置
第 2 层	道路设施	交通标志、标线、护栏等
第 3 层	环境条件	天气、光照、附着条件
第 4 层	交通参与者	其他车辆、行人、非机动车
第 5 层	动态要素	本车运动状态、驾驶员操作
第 6 层	系统状态	驾驶模式、系统工作状态
第 7 层	数字信息	高精地图、V2X、定位信息

注：对于线控制动系统，场景的完整描述需包含上述七个层级的参数组合。评估人员应重点关注对制动功能有直接影响的层级（第1层、第3层、第4层、第5层、第6层），并结合系统功能特点选取关键要素。

8.4 线控制动系统场景要素提取

基于线控制动系统的功能特点，评估人员在定义场景时应系统性地从七个层级中选取对制动性能、失效触发或风险等级有显著影响的要素。以下对各层级要素进行说明，并汇总于表 8-3 中。

第 1 层：道路结构：道路结构直接决定制动系统的物理环境，影响制动力需求、稳定性以及坡道辅助等功能。评估人员应重点关注道路类型（城市、高速、乡村、停车场）、坡度（无坡、小坡、大坡）、曲率（直道、小弯、急弯）以及车道数（单车道、多车道）。坡度影响坡道起步和溜车风险，曲率影响弯道制动的稳定性，而道路类型和车道数则与交通密度、制动频率密切相关。

第 2 层：道路设施：道路设施如交通标志、标线、信号灯等，对驾驶员的制动决策及智驾系统的感知有重要影响。评估人员应关注交通标志（限速、让行、停止）、标线清晰度以及护栏位置等要素。这些要素虽不直接改变制动系统物理行为，但影响驾驶行为及系统对环境的理解，进而影响暴露率。

第 3 层：环境条件：环境条件直接影响制动效能和车辆稳定性。评估人员应重点考虑路面附着系数（高、中、低）、天气（晴、雨、雪、雾）以及光照（白天、夜晚、隧道、逆光）。低附着路面会显著延长制动距离、增加 ABS 介入频率；恶劣天气和不良光照会影响驾驶员视线和传感器性能，进而影响可控性和暴露率。

第 4 层：交通参与者：交通参与者的状态是决定制动需求和碰撞风险的关键因素。评估人员应重点关注前车状态（匀速、减速、静止、紧急制动）、前车距离（远、中、近）、行人/障碍物（无、行人横穿、行人静止、障碍物）以及相邻车道车辆（无、有并行、有切入）。这些要素直接影响 AEB 触发概率、追尾风险以及紧急制动的必要性。

第 5 层：动态要素：动态要素反映本车实时运动状态和驾驶员操作意图。评估人员应重点关注本车车速（低速、中速、高速）、制动踏板状态（未踩、轻踩、中度、紧急）、制动意图（无制动、减速、紧急停车）以及车辆载荷（空载、满载）。车速和制动意图直接决定制动能量和碰撞严重度，载荷则影响制动力分配和制动距离。

第 6 层：系统状态：系统状态反映制动系统自身的工作模式及车辆控制权归属。评估人员应重点关注驾驶模式（人工驾驶、智驾介入）、制动系统状态（正常、降级、故障）以及冗余状态（主控正常、备用待命、切换中）。这些要素直接影响失效后的系统能力以及驾驶员接管条件，对可控性评估至关重要。

第 7 层：数字信息：数字信息为智能驾驶功能提供先验知识，其质量影响系统决策的准确性。评估人员应重点关注定位精度（高、中、低）和地图信息（准确、过时、缺失）。对于依赖高精地图的坡道检测、弯道预判等功能，数字信息的质量直接影响功能激活和性能。

表 8-3 线控制动系统场景要素汇总

层级	要素	分级	对制动系统的影响
第 1 层：道路结构	道路类型	城市道路、高速公路、乡村道路、停车场	影响制动频率和紧急程度
	坡度	无坡（0°）、小坡（3°~10°）、大坡（>10°）	影响坡道辅助功能激活和溜车风险
	曲率	直道、小弯（半径>200m）、急弯（半径≤200m）	影响弯道制动稳定性
	车道数	单车道、多车道	影响交通密度和碰撞风险
第 2 层：道路设施	交通标志	限速、让行、停止	影响驾驶员制动决策
	标线清晰度	清晰、模糊、缺失	影响车道保持和智驾感知
	护栏位置	有、无	影响碰撞后防护
第 3 层：环境	路面附着系数	高附着（≥0.8）、中附着（0.4~0.8）、低	影响制动距离、ABS 介入、车辆稳

条件		附着 (≤ 0.4)	定性
	天气	晴天、雨、雪、雾	影响路面附着和能见度
	光照	白天、夜晚、隧道、逆光	影响传感器性能和驾驶员视线
第 4 层: 交通参与者	前车状态	匀速、减速、静止、紧急制动	影响追尾风险和 AEB 触发
	前车距离	远 ($>50\text{m}$)、中 ($20\sim 50\text{m}$)、近 ($<20\text{m}$)	影响制动需求强度
	行人/障碍物	无、行人横穿、行人静止、障碍物	影响碰撞对象类型和 AEB 触发
	相邻车道车辆	无、有 (并行)、有 (切入)	影响紧急制动时的避让空间
第 5 层: 动态要素	本车车速	低速 ($0\sim 30\text{ km/h}$)、中速 ($30\sim 80\text{ km/h}$)、高速 ($\geq 80\text{ km/h}$)	直接影响制动能量和碰撞严重度
	制动踏板状态	未踩、轻踩 ($<30\%$)、中度 ($30\%\sim 70\%$)、紧急 ($>70\%$)	反映驾驶员制动意图
	制动意图	无制动、减速、紧急停车	影响系统期望响应
	车辆载荷	空载、满载	影响制动力分配和制动距离
第 6 层: 系统状态	驾驶模式	人工驾驶、智驾介入	影响驾驶员接管能力和场景频率
	制动系统状态	正常、降级、故障	影响失效后的系统能力
	冗余状态	主控正常、备用待命、切换中	影响可控性
第 7 层: 数字信息	定位精度	高 ($<0.5\text{m}$)、中 ($0.5\sim 2\text{m}$)、低 ($>2\text{m}$)	影响依赖定位的功能 (如坡道检测)
	地图信息	准确、过时、缺失	影响坡度、曲率等预知信息

8.5 输出物汇总

完成本章分析后, 评估人员应形成以下输出物, 用于后续章节:

输出物 8-1 运行场景要素表: 即表 8-3, 汇总了七个层级的关键要素及其分级, 明确线控制动系统需要关注的场景参数。

输出物 8-2 典型运行场景清单: 基于上述要素组合, 形成线控制动系统的典型运行场景清单。典型场景清单详见附录 B。评估人员应根据实际系统功能和运行设计域, 在附录 B 的基础上补充或调整场景, 确保覆盖所有可能触发失效的情况。

9 危害识别与定义

9.1 目的

本章旨在将第 7 章识别的失效模式与第 8 章定义的运行场景相结合, 形成具体的危害事件, 并对每个危害事件进行结构化描述和严重性预判。危害事件是后续 S/E/C 量化评估的直接对象, 其定义的准确性和完整性直接影响评估结果。

9.2 输入准备

在开始本章分析前, 评估人员应准备好以下输入资料:

表 9-1 输入准备

资料名称	来源	说明
功能清单	第 6 章输出物 6-1 和 6-2	明确系统功能, 帮助理解危害发生的背景

失效模式清单	第 7 章输出物 7-1	提供失效模式及失效描述、可能原因
运行场景要素表	第 8 章输出物 8-1 和 8-2	提供场景要素及其分级

9.3 分析步骤

评估人员应按照以下步骤完成危害识别与定义。

9.3.1 确定危害事件的基本结构

每个危害事件应采用统一的结构化描述方式，确保信息完整、无歧义。本标准推荐采用以下描述结构：

“在[场景]下，由于[失效模式]导致 [危害后果]。”

其中：

[场景]：引用第 8 章定义的运行场景（如 SC-01：高速直线行驶中前车紧急制动），可包含关键参数组合。

[失效模式]：引用第 7 章识别的失效模式（如 BR-02：制动力丧失）。

[危害后果]：描述失效发生后对车辆运动状态或对交通参与者造成的具体影响（如“车辆无法有效减速，与前车发生追尾碰撞”）。

9.3.2 关联失效模式与运行场景

针对第 7 章识别的每个失效模式，评估人员应分析其在哪些运行场景下可能产生危害。关联分析应基于以下原则：

- a) 文失效模式与场景的组合必须具有物理可能性。例如，“制动力丧失”在需要制动的场景（如 SC-01、SC-03）下才会产生危害；在不需要制动的场景下，该失效可能不会立即导致危害。
- b) 同一失效模式可与多个场景关联，每个关联均产生独立的危害事件。
- c) 同一场景下可能关联多个失效模式，每个失效模式分别产生危害事件。

评估人员应建立“失效模式-场景”关联矩阵，明确哪些组合需要进一步定义危害事件。

9.3.3 定义危害事件

对于每个“失效模式-场景”关联组合，评估人员应按照步骤 1 的结构定义危害事件。危害事件的定义应满足以下要求：

- a) 唯一性：每个危害事件应有唯一编号，便于追溯。
- b) 完整性：描述应包含场景、失效模式、危害后果三个要素。
- c) 清晰性：描述应使用明确的技术语言，避免模糊表述。
- d) 可量化：危害后果应尽量与后续严重度评估的参数（如碰撞速度、偏移距离）相关联。

危害事件的编号可采用“HZ-序号”格式，HZ 代表危害（Hazard）。

9.3.4 明确危害发生条件

危害事件的发生通常需要满足特定的参数阈值组合。评估人员应明确每个危害事件的发生条件，即哪些参数在什么范围内时，危害实际会发生。

例如，对于“高速直线行驶中前车紧急制动”场景下“制动力丧失”的危害，其发生条件可定义为：车速≥80 km/h、前车距离≤30 m、制动力丧失比例≥50%。

上述参数阈值可来源于行业工程经验、同类项目积累或专家判断，评估人员应结合实际项目情况合理选取。

明确发生条件有助于后续暴露率评估时，准确统计满足条件的场景频率，避免将不满足条件的场景计入统计。

9.3.5 建立危害事件清单

将所有定义的危害事件汇总，形成结构化的危害事件清单。清单应包含以下要素：

表 9-2 危害事件清单列表

要素	说明
危害编号	唯一标识，采用“HZ-序号”格式
关联失效模式	引用第 6 章的失效编号
关联场景	引用第 7 章的场景编号
危害描述	结构化描述（场景+失效+后果）
发生条件	危害发生的参数阈值组合

9.4 线控制动系统危害事件示例

以下列出线控制动系统典型危害事件的示例，供评估人员参考。实际应用中，评估人员应根据实际系统功能、失效模式和场景，补充或调整危害事件。

表 9-3 线控制动系统危害事件示例

危害编号	关联失效模式	关联场景	危害描述	发生条件
HZ-01	BR-02（制动力丧失）	SC-01（高速直线行驶中前车紧急制动）	在高速直线行驶中前车紧急制动场景下，由于制动力丧失，车辆无法有效减速，与前车发生追尾碰撞	车速≥80 km/h、前车距离≤30 m、制动力丧失≥50%

表 9-3 线控制动系统危害事件示例(续)

危害编号	关联失效模式	关联场景	危害描述	发生条件
HZ-02	BR-02（制动力丧失）	SC-03（湿滑路面紧急制动）	在湿滑路面紧急制动场景下，由于制动力丧失，车辆制动距离显著延长，与前方障碍物或车辆发生碰撞	车速≥50 km/h、路面附着≤0.4、制动力丧失≥50%
HZ-03	BR-01（非预期制动）	SC-02（城市低速跟车）	在城市低速跟车场景下，由于非预期制动，车辆突然减速，导致后方车辆追尾	车速 20～50 km/h、交通密度高、非预期制动压力≥50 bar
HZ-04	BR-05（制动不平衡）	SC-08（弯道制动）	在弯道制动场景下，由于制动不平衡，车辆左右轮制动力差异导致跑偏，偏离车道与护栏或其他车辆碰撞	弯道半径≤200 m、车速≥60 km/h、左右轮制动力差≥30%
HZ-05	BR-13（坡道辅助失效）	SC-04（坡道起步）	在坡道起步场景下，由于坡道辅助失效，松开制动踏板后车辆溜车，与后方车辆或障碍物碰撞	坡度≥10%、坡道辅助失效、无驻车介入
HZ-06	BR-11（AEB 执	SC-06（自动紧急制动触	在自动紧急制动触发场景下，由于	车速≥50 km/h、AEB

	行失效)	发)	AEB 执行失效, 车辆未按指令减速, 与前方行人或静止车辆发生碰撞	指令有效、执行器无响应
HZ-07	BR-15 (再生制动协调失效)	SC-10 (再生制动介入)	在再生制动介入场景下, 由于再生制动与液压制动协调失效, 制动力突变导致车辆顿挫, 可能引发后车追尾	车速 30~80 km/h、轻制动、再生制动协调异常

9.5 输出物汇总

完成本章分析后, 评估人员应形成以下输出物, 用于后续章节:

输出物 9-1 线控制动系统危害事件清单: 参考表 9-3: 包含危害编号、关联失效模式、关联场景、危害描述、发生条件。该清单是后续 S/E/C 量化评估 (第 10~12 章) 的直接输入。

10 严重度 (S) 量化评估方法

10.1 目的

本章旨在建立线控制动系统危害事件严重度 (S) 的量化评估方法。通过基于整车动力学模型的解析计算, 综合考虑车辆参数、制动系统特性、路面条件、驾驶员行为等多重因素, 将危害后果转化为可量化的碰撞速度指标, 并根据碰撞速度确定严重度等级, 为后续 ASIL 等级判定提供依据。

10.2 输入准备

在开始本章评估前, 评估人员应准备好以下输入资料:

表 10-1 输入准备表

资料名称	来源	说明
危害事件清单	第 9 章输出物 9-1	包含危害编号、失效模式、场景参数、预判严重性

表 10-1 输入准备表(续)

资料名称	来源	说明
运行场景要素表	第 8 章输出物 8-1 和 8-2	提供场景要素及其分级
失效模式清单	第 7 章输出物 7-1	提供失效响应时间、失效幅值等参数
车辆动力学参数	整车技术文档	提供车辆质量、制动系统性能、轮胎特性等参数

10.3 量化模型基础

严重度 (S) 的量化以碰撞能量模型为核心理论依据。本节阐述该模型的理论基础、标准依据及关键参数的确定方法。

10.3.1 严重度评估标准

线控制动系统失效导致的严重度 (S) 应依据 SAE J2980:2023^[6]中定义的量化模型进行判定。该模型基于碰撞速度增量 (Delta-V, V) 与碰撞类型, 确立其与 AIS 定级伤害程度的映射关系。评估过程中, 应以碰撞时刻的瞬时速度及潜在碰撞方式作为关键评价要素。根据 SAE J2980:2023, 危害事件的 S 等级判定规则如下:

表 10-2 严重度 S 与碰撞类型及相对速度关系表

碰撞类型	范围	S0	S1	S2	S3
正碰	最小速度		>4-10km/h	>20-50km/h	>40-65km/h
	最大速度	<4-10km/h ^a	<20-50km/h	≤40-65km/h	
后碰	最小速度		>4-10km/h	>20-50km/h	>40-60km/h
	最大速度	<4-10km/h ^a	<20-50km/h	≤40-65km/h	
侧碰	最小速度		>2-10km/h	≥8-30km/h	>16-40km/h
	最大速度	<2-3km/h ^a	<8-30km/h	<16-40km/h	
注：上述清单是非穷尽的。在确定危害事件的严重度分级时，宜考虑潜在风险的参与者。这包括行人、骑自行车的人和和其他车辆上的乘客(无论车辆是否在公共道路上)。					
^a 某些分析中未定义。					

注：表中速度区间为推荐典型值，评估人员可结合具体车型和碰撞兼容性适当调整，但应在报告中说明[7]。当碰撞速度落在两个等级的重叠区时，取较严重的等级。

SAE J2980（2023 版）对严重度（S）的分类借鉴了医学上关于伤害程度的通用标准，特别是国际通用的伤害严重度评分（AIS）理念。AIS 是国际上广泛采用的伤害严重度分级标准，将人体伤害从轻到重划分为 6 个等级^[8]。SAE J2980 将其与功能安全的 S 等级进行了对应。

表 10-3 严重度等级与 AIS 分级对应关系

严重度等级	描述	受伤概率（死亡/重伤）	伤害类型	严重度等级与 AIS 等级
S0	无伤害	无	无伤害或轻微的、可忽略不计的伤害	S0(无伤害)对应 AIS 分级中的“无伤害”:AIS 分级中无伤害等级描述为未达到任何伤害标准，与 SAEJ2980 中的 S0 等级一致，均表示无伤害

表 10-3 严重度等级与 AIS 分级对应关系(续)

S1	轻伤	很低	轻微伤害，如擦伤、挫伤等，通常不需要住院治疗	S1(轻伤)对应 AIS 分级中的“轻度创伤”:AIS 分级中的轻度创伤通常指擦伤、挫伤等轻微伤害，与 SAEJ2980 中的 S1 等级相对应，都表示不需要住院治疗的轻微伤害
S2	重伤	低	严重伤害，可能导致人员残疾或危及生命，但死亡率较低	S2(重伤)对应 AIS 分级中的“中度创伤”到“严重创伤”:AIS 分级中的中度创伤到严重创伤涵盖了需要住院治疗的伤害，如骨折、内出血等。这与 SAEJ2980 中的 S2 等级对应，都表示可能导致残疾或危及生命的伤害
S3	危及生命/致命伤	中等	极其严重的伤害，很可能导致死亡或造成严	S3(危及生命/致命伤)对应 AIS 分级中的“危重创伤”和“极重创伤”AIS 分级中的危重创伤和极重创伤代表了极其严重的伤害，死亡风险极高，与 SAEJ2980 中的

			重的、永久性的伤害	S3 等级一致,都是指可能导致死亡或严重永久性后遗症的伤害。
--	--	--	-----------	--------------------------------

10.3.2 碰撞能量与人体伤害的关系

根据经典力学,运动物体的动能表达式为:

$$E_k = \frac{1}{2}mv^2 \dots\dots\dots 1$$

式中:
E_k: 动能 (J) ;
m: 物体质量 (kg) ;
v: 物体速度 (m/s) 。

当车辆发生碰撞时,动能会在极短时间内被吸收,转化为人体与车辆结构之间的相互作用力。人体组织(如骨骼、软组织、内脏)对冲击力的耐受程度有限,当冲击能量超过一定阈值时,就会造成伤害。

伤害机制: 人体伤害程度与碰撞过程中能量吸收的速率和分布密切相关。在车辆碰撞事故中,人体伤害主要表现为:

- a) 头部伤害: 与头部减速过程中产生的加速度峰值相关,常用头部伤害判据 HIC (Head Injury Criterion) 进行评估;
- b) 胸部伤害: 与胸部压缩量和加速度相关;
- c) 下肢伤害: 与腿部受到的冲击力相关。

研究表明,碰撞速度是预测人体伤害程度的最关键参数之一^[9]。这是因为在给定车辆结构条件下,碰撞速度与能量吸收量直接相关,进而与人体受到的冲击力相关。因此本标准采用碰撞速度作为伤害程度的量化依据。

10.3.3 碰撞速度的关键影响因素

碰撞速度的大小取决于以下多个因素的相互作用:

- a) 初始车速: 失效发生时的本车速度,直接决定碰撞能量的上限。
- b) 相对速度: 本车与前车(或障碍物)的速度差,是计算反应距离和制动距离的核心参数。
- c) 失效后剩余制动力: 线控制动失效后,车辆仍可能保留机械制动能力(通常减速度不低于 2.44 m/s²)^[10]。剩余制动力越大,碰撞速度越低。
- d) 驾驶员反应时间: 从失效发生到驾驶员开始制动的总时间(含感知、决策、肌肉响应)。反应时间越长,车辆在无有效制动状态下行驶的距离越长,碰撞速度越高。
- e) 制动系统响应时间: 从制动指令发出到制动力完全建立的时间(包括延迟时间和建立时间)。响应越慢,有效制动开始越晚。
- f) 路面附着系数: 低附着路面(冰雪、湿滑)会显著降低可实现的最大减速度,延长制动距离,从而升高碰撞速度。
- g) 坡度: 下坡时重力分量抵消部分制动力,使碰撞速度升高;上坡则相反。
- h) 空气阻力与滚动阻力: 高速工况下空气阻力对减速有一定贡献,但通常远小于制动力。

10.4 评估流程

严重度 S 的评估按以下三个步骤进行:

- a) 确定碰撞类型: 根据危害事件描述,判断碰撞属于正碰、后碰还是侧碰。
- b) 计算碰撞速度: 采用整车动力学仿真或解析计算方法,获得失效后本车与碰撞目标的相对

速度。

- c) 判定 S 等级：将碰撞速度和碰撞类型对照表 10-3，得出 S0～S3 等级。

10.5 碰撞类型的确定

碰撞类型直接影响表 10-2 中使用的速度阈值。评估人员应根据危害事件的描述，按以下原则判断：

表 10-4 碰撞类型确定表

碰撞类型	定义	典型危害事件示例
正碰	本车正面与前车或障碍物发生碰撞	制动力丧失导致本车追尾前车
后碰	本车尾部被后车碰撞	非预期制动导致后车追尾本车；坡道溜车碰撞后方车辆
侧碰	本车侧面与其他车辆或障碍物碰撞	制动不平衡导致车辆跑偏，与相邻车道车辆侧面碰撞

判断规则：

- a) 若本车是主动追尾前车（本车速度>前车速度），按正碰处理。
b) 若本车是被动被后车追尾（本车速度<后车速度或本车静止），按后碰处理。
c) 若本车偏离行驶车道或发生侧滑，与侧面物体碰撞，按侧碰处理。

10.6 碰撞速度的计算方法

碰撞速度是指碰撞瞬间本车与碰撞目标之间的相对速度。本标准推荐采用整车动力学仿真方法，同时提供解析计算公式作为备选。

10.6.1 整车动力学仿真

评估人员应在仿真软件（如 CarSim、Matlab/Simulink）中建立线控制动系统的整车动力学模型，输入以下关键参数：

- a) 车辆参数：质量、轴距、质心高度、轮胎特性、空气阻力系数、迎风面积等。
b) 制动系统参数：正常制动能力、失效模式下的剩余制动力、响应延迟（ t_{d1} ）、压力建立时间（ t_{d2} ）。
c) 场景参数：初始车速、前车或障碍物的运动状态（速度、减速度）、路面附着系数、坡度、初始距离。
d) 驾驶员模型：反应时间 t_{react} （人工模式取 0.5～1.5 s，智驾模式取 1.0～3.0 s），制动操作（紧急制动）。
e) 在仿真中设置失效发生时刻，运行模型直至碰撞或安全停止，输出碰撞时刻的相对速度。

10.6.2 碰撞速度解析计算模型

本节建立用于计算碰撞速度的解析模型。该模型基于整车纵向动力学，综合考虑车辆自身特性、制动系统响应、驾驶员行为以及外部环境因素，能够较为真实地反映失效后的车辆运动状态。以下对各部分进行详细说明^{[1][12]}。

整车纵向动力学方程

车辆在行驶过程中受到的合力决定了它的加速度，从而影响速度变化和制动距离。纵向动力学方程是描述这一关系的核心：

$$m \cdot \frac{dv}{dt} = F_{brake} + F_{drag} + F_{roll} + F_{grade} \dots\dots\dots 2$$

式中：

$m \cdot \frac{dv}{dt}$: 车辆惯性力, 即质量乘以加速度 (速度对时间的导数);

F_{brake} : 制动系统施加在车轮上的总制动力, 方向与行驶方向相反, 为负值;

F_{drag} : 空气阻力, 随车速增大而增大, 方向与行驶方向相反, 为负值;

F_{roll} : 滚动阻力, 由轮胎与路面接触变形产生, 方向与行驶方向相反, 为负值;

F_{grade} : 坡度力, 上坡时阻碍车辆前进 (正值, 帮忙减速), 下坡时推动车辆前进 (负值, 不利于减速)。

各力的具体表达式如下:

空气阻力:

$$F_{\text{drag}} = \frac{1}{2} \rho C_d A v^2 \dots\dots\dots 3$$

式中:

ρ : 空气密度 (标准大气压下取 1.225 kg/m^3);

C_d : 空气阻力系数 (反映车辆流线型程度, 轿车通常 $0.25 \sim 0.35$);

A : 车辆迎风面积 (m^2);

v : 瞬时车速 (m/s)。

空气阻力与车速的平方成正比, 在高速工况下对减速有显著贡献。

滚动阻力:

$$F_{\text{roll}} = -f_r m g \cos \alpha \dots\dots\dots 4$$

式中:

f_r : 滚动阻力系数 (与轮胎类型、路面材料有关, 通常取 $0.01 \sim 0.02$);

m : 车辆质量 (kg);

g : 重力加速度 (9.8 m/s^2);

α : 坡度角 ($^\circ$), $\cos \alpha$ 考虑坡道对法向载荷的影响。

滚动阻力与车速关系不大, 基本为恒定值。

坡度力:

$$F_{\text{grade}} = m g \sin \alpha \dots\dots\dots 5$$

式中:

m : 车辆质量 (kg);

g : 重力加速度 (9.8 m/s^2);

α : 坡度角 ($^\circ$), $\sin \alpha$ 考虑坡道对法向载荷的影响。

上坡时 $\alpha > 0$, $\sin \alpha > 0$, F_{grade} 为正, 相当于额外减速力。

下坡时 $\alpha < 0$, $\sin \alpha < 0$, F_{grade} 为负, 相当于额外减速力, 会增加碰撞风险。

制动系统动态响应模型

线控制动系统从接收到制动指令到产生最大制动力需要一定的时间, 该过程直接影响碰撞速度。因此必须建立制动力随时间变化的动态模型^[13]。

将制动力建立过程分为三个阶段:

反应延迟时间 ($t \leq t_{d1}$)

从制动指令发出到系统开始建压的时间 (通常 $0.01 \sim 0.05 \text{ s}$)。在此期间, 制动力为零:

$$F_{\text{brake}}(t) = 0 \dots\dots\dots 6$$

线性建立阶段 ($t_{d1} < t \leq t_{d1} + t_{d2}$)

制动力从零线性增长至最大值 F_{max} , 增长斜率为 F_{max}/t_{d2} :

$$F_{\text{brake}}(t) = -\frac{F_{\text{max}}}{t_{d2}}(t - t_{d1}) \dots\dots\dots 7$$

稳定输出阶段($t > t_{d1} + t_{d2}$)

制动力保持最大值:

$$F_{\text{brake}}(t) = -F_{\text{max}} \dots\dots\dots 8$$

式中 t_{d2} 为建立时间（通常 0.1~0.3s），反映制动系统的响应速度。不同失效模式会影响 t_{d1} 、 t_{d2} 和 F_{max} 的取值（见 9.5 节）。

实际可用最大制动力不仅受制动系统本身能力限制，还受路面附着条件制约：

$$F_{\text{max,actual}} = \min (F_{\text{mar,capable}}, \mu \cdot m \cdot g \cdot \eta_{\text{load}}) \dots\dots\dots 9$$

式中：

$F_{\text{max,capable}}$ ：制动系统（制动器、助力器等）能提供的最大制动力；

μ ：路面附着系数（干燥路面 0.8~1.0，湿滑路面 0.4~0.8，冰雪路面 0.2~0.4）；

η_{load} ：轴荷分配系数，考虑制动时轴荷转移的影响（通常取 0.9~1.1）。实际应用中可简化取 1.0。

制动系统动态响应模型

在制动过程中，前后轴制动力分配会影响整车的制动稳定性和最大可利用附着力。对于普通乘用车，制动力分配通常采用固定比例或根据载荷调整。

设前轴制动力占总制动力的比例为 β （ $0 < \beta < 1$ ），则：

前轴制动力： $F_{\text{brake,f}} = \beta \cdot F_{\text{brake}}$

后轴制动力： $F_{\text{brake,r}} = (1 - \beta) \cdot F_{\text{brake}}$

当制动系统正常工作时， β 取值通常使前后轮同时达到附着极限，以获得最大减速度。在失效模式下（如制动不平衡），前后轴分配可能偏离设计值，但在纵向碰撞速度计算中，可以忽略这种偏差，仅需关注总制动力 F_{brake} 的变化。

驾驶员模型

驾驶员从感知到危险到开始踩下制动踏板需要一定的反应时间 t_{react} 。在这段时间内，车辆按照失效模式继续行驶（可能无制动或已有非预期制动）。反应时间的长短直接决定了碰撞前的制动开始时刻，从而影响碰撞速度。

本标准根据驾驶模式推荐以下取值：

人工驾驶模式： $t_{\text{react}} = 0.5 \sim 1.5\text{s}$ ，典型值取 1.0s（参考 SAE J2980）。

智驾介入模式： $t_{\text{react}} = 1.0 \sim 3.0\text{s}$ ，典型值取 2.0s（包含接管时间）。

在反应时间内，驾驶员尚未采取任何制动操作。反应结束后，驾驶员施加紧急制动（阶跃输入），制动系统按动态响应模型执行。

纵向碰撞速度求解

碰撞速度的计算需要明确本车与前车（或障碍物）的相对运动。设初始时刻 $t = 0$ 时，本车速度为 v_0 ，前车速度为 v_{lead} ，两车初始距离为 d_0 。

本车位置随时间的变化通过对速度积分得到：

$$s_{\text{ego}}(t) = \int_0^t v_{\text{ego}}(\tau) d\tau \dots\dots\dots 10$$

前车位置（若为静止障碍物，则 $v_{\text{lead}} = 0$ ， $s_{\text{lead}}(t) = 0$ ）：

$$s_{\text{lead}}(t) = \int_0^t v_{\text{lead}}(\tau) d\tau \dots\dots\dots 11$$

碰撞时刻 t_c 满足两车距离为零：

$$s_{\text{ego}}(t_c) - s_{\text{lead}}(t_c) = d_0 \dots\dots\dots 12$$

若方程有解，则碰撞速度为：

$$v_c = v_{\text{ego}}(t_c) - v_{\text{lead}}(t_c) \dots\dots\dots 13$$

若方程无解（即本车始终无法追上），则判定为无碰撞风险（S0）。

数值求解方法：由于制动系统动态响应、空气阻力等均为非线性，通常无法直接给出解析解。评估人员可采用数值积分（如欧拉法或四阶龙格-库塔法）离散计算时间历程，直到满足碰撞条件或时间超出合理范围。步长建议取 0.01~0.02s，以保证精度。

10.6.3 典型失效模式的模型修正

针对不同失效模式，需要对上述模型中的参数进行相应调整。下表总结了常见失效模式对模型的影响：

表 10-5 线控制动系统典型失效模式参数修正

失效模式	模型修正	说明
制动力完全丧失	$F_{max} = 0$	无制动能力，仅靠阻力和坡度减速
非预期制动	制动指令在无驾驶员输入时自发产生	按系统响应模型执行，反应时间 t_{react} 可视为 0 或极短
制动力部分丧失	$F_{max} = \eta \cdot F_{max, capable}$	η 为剩余制动力比例（ $0 \leq \eta \leq 1$ ）
制动响应延迟	增加额外的延迟时间 t_{delay}	并入 t_{d1} ，即 $t'_{d1} = t_{d1} + t_{delay}$
制动建立时间延长	增大 t_{d2}	影响制动初期的减速效果，使碰撞速度升高
制动不平衡	仅影响侧向稳定性	对纵向碰撞速度影响较小，可忽略
ABS 功能丧失	最大制动力仍可达附着极限	模型可不调整，因为最大减速度仍受附着系数限制

10.6.4 关键参数汇总

表 10-6 关键参数汇总

参数	符号	单位	典型范围	数据来源
整车质量	m	kg	1300~2500	整车参数表
空气阻力系数	C_d	—	0.25~0.35	整车参数表
迎风面积	A	m ²	2.0~2.8	整车参数表

表 10-6 关键参数汇总(续)

参数	符号	单位	典型范围	数据来源
滚动阻力系数	f_r	—	0.01~0.02	轮胎参数表
最大制动力（系统）	$F_{max, capable}$	N	取决于制动器	制动系统参数表
制动反应延迟	t_{d1}	s	0.01~0.05	制动系统参数表
制动建立时间	t_{d2}	s	0.1~0.4	制动系统参数表
反应时间（人工）	t_{react}	s	0.5~1.5	人因工程数据、SAE J2980
反应时间（智驾）	t_{react}	s	1.0~3.0	接管研究数据
路面附着系数	μ	—	0.2~1.0	运行条件参数表
坡度角	α	°	0~20	运行条件参数表
初始车速	v_0	km/h	根据场景	运行条件参数表
初始距离	d_0	m	根据场景	场景定义

10.7 评估示例

示例场景：高速公路直线行驶，本车车速 80km/h，前车静止，距离 30m，发生制动力完全丧失。

表 10-7 示例场景参数表

参数	符号	取值	来源
整车质量	m	1500 kg	整车参数表
空气阻力系数	C_d	0.30	整车参数表
迎风面积	A	2.2 m ²	整车参数表
滚动阻力系数	f_r	0.012	轮胎参数表
最大制动力（系统）	$F_{max, capable}$	12000 N	制动系统参数表
失效模式修正	η	0（完全丧失）	失效特征参数表
实际最大制动力	F_{max}	0N	$F_{max} = \eta \times F_{max, capable}$
反应时间	t_{react}	1.0s	人工模式，SAE J2980
制动延迟	t_{d1}	0.02s	制动系统参数表
制动建立时间	t_{d2}	0.3s	制动系统参数表
路面附着系数	μ	0.8	运行条件参数表
坡度角	α	0°	运行条件参数表
初始车速	v_0	80km/h = 22.22m/s	运行条件参数表
初始距离	d_0	30m	场景定义

步骤 1：确定碰撞类型

本车追尾前车：正碰

步骤 2：计算碰撞速度

法 1：整车动力学仿真

在 CarSim 中建立整车模型，设置表 10-9 的参数：

仿真设置：本车初速 80 km/h，前车静止，两车初始距离 30 m，线控主制动功能失效，系统切换至机械备份模式，此时仅能提供 2.44 m/s²的剩余减速度，驾驶员反应时间 1.0 s 后踩下制动踏板。

仿真输出：本车在失效后约 1.35 s 与前车碰撞，碰撞速度为 79.8 km/h。

法 2：通过解析公式计算

步骤二：计算碰撞速度

由于制动力完全丧失（ $F_{max} = 0$ ），车辆仅受空气阻力和滚动阻力减速。

空气阻力：
$$F_{drag} = -\frac{1}{2} \times 1.225 \times 0.30 \times 2.2 \times v^2 = -0.404 \times v^2$$

滚动阻力：
$$F_{roll} = -0.012 \times 1500 \times 9.8 \times \cos 0^\circ = -176.4\text{N}$$

运动方程：
$$1500 \times \frac{dv}{dt} = -0.404v^2 - 176.4$$

采用欧拉法进行数值积分，时间步长 0.01s：

初始时刻 $t = 0$ ， $v = 22.22\text{m/s}$ ，行驶距离 $s = 0$

本车行驶至前车位置时， $s = 30\text{m}$

经数值积分计算，本车到达前车位置的时间 $t_c \approx 1.35\text{s}$ ，此时速度 $v_c \approx 22.18\text{m/s} \approx 79.8\text{km/h}$ 。

步骤三：判定 S 等级

碰撞速度为 79.8km/h，大于 60km/h，对照表 10-3，判定为 S3。

步骤四：记录评估数据
参数取值来源：整车参数表、制动系统参数表、失效特征参数表、运行条件参数表
计算过程：采用整车纵向动力学方程，考虑空气阻力、滚动阻力，采用欧拉法数值积分
计算结果：碰撞速度 79.8km/h
判定结果：S3

10.8 输出物汇总

输出物 10-1 严重度 S 评估记录表：包含危害编号、整车参数、制动系统参数、场景参数、失效模式修正、计算过程（含微分方程、数值积分方法）、碰撞速度、S 等级、评估依据（含参数来源和计算说明）。

11 暴露率（E）量化评估方法

11.1 目的

本章规定了线控制动系统危害事件暴露率（E）的量化评估方法。通过对中国典型场景库和自然驾驶数据的统计分析，获取各运行场景的出现频次或时间占比。根据场景频率分布，确定危害事件对应的暴露率等级，为 ASIL 等级判定提供量化依据。

11.2 输入准备

在开始本章评估前，评估人员应准备好以下输入资料：

表 11-1 输入准备

资料名称	来源	说明
危害事件清单	第 9 章输出物 9-1	包含危害编号、关联失效模式、关联场景
典型运行场景清单	第 8 章输出物 8-1	包含场景编号、场景名称、场景描述
中国典型场景库	CAICV	提供各类场景的频率统计数据（数据总结）

表 11-1 输入准备(续)

资料名称	来源	说明
自然驾驶数据库	实车采集数据	提供基于实际行驶数据的场景频率
车辆运行数据	用户使用统计	年平均运行时间、年平均行驶里程等
VDA 702 场景目录	德国汽车工业协会	提供标准化基础场景要素及其暴露概率参考

11.3 量化模型基础

11.3.1 暴露率的定义与评估框架

暴露率（E）是功能安全 HARA 中的三个核心参数之一，用于描述危险出现时，人员暴露于因系统失效而造成危害的场景中的概率。需要特别强调的是，暴露率与失效本身的发生概率无关，而与“失效能造成危害的场景”出现的概率有关。

ISO 26262- 3 为暴露率提供了基本的定义和分级框架，但该标准仅给出了定性的描述，未提供具体的量化取值方法。评估人员在实践中长期面临“如何客观确定 E 等级”的困扰。为解决这一问题，国际汽车工程领域发展出了两套重要的补充性标准——SAE J2980 和 VDA 702，它们与

ISO 26262- 3 共同构成了本标准暴露率评估的完整方法体系。

三者的逻辑关系可概括为：

- a) ISO 26262-3 提供顶层框架（E 等级定义、双维度判定表）；
- b) SAE J2980 提供量化方法（频率范围、场景分类维度）；
- c) VDA 702 提供工程工具（场景目录、要素概率参考值、乘积公式）。

11.3.2 GB/T 34590.3—2022 暴露率的定义与等级划分

根据 GB/T 34590.3—2022，暴露率（E）划分为 E0 至 E4 五个等级。其中，E0 对应于极低可能性的场景（通常不进行后续风险评估），E1 至 E4 对应于场景暴露概率的递增水平。本标准采用 GB/T 34590.3—2022 附录 B 中规定的量化判定准则，通过运行场景持续时间（占总驾驶时间的比例）或运行场景发生频率两个维度进行综合判定。根据 GB/T 34590.3—2022，暴露率（E）的量化定义及分级如表 11-2 和表 11-3 所示。

表 11-2 基于运行场景持续时间的暴露概率等级

运行场景暴露概率等级	E1	E2	E3	E4
描述	非常低的概率	低概率	中等概率	高概率
持续时间（平均运行时间的百分比）	无定义	<1%平均运行时间	1%-10%平均运行时间	>10%平均运行时间

表 11-3 基于运行场景频率的暴露概率等级

运行场景暴露概率等级	E1	E2	E3	E4
描述	非常低的概率	低概率	中等概率	高概率
场景发生的频率	对于绝大多数驾驶员小于一年发生一次	对于绝大多数驾驶员一年发生几次	对于一般的驾驶员一个月发生一次或多次	平均几乎发生在每次驾驶中

11.3.3 SAE J2980 暴露率的量化方法

SAE J2980 是由美国汽车工程师学会（SAE）发布的标准，旨在为汽车运动控制电气和电子（E/E）系统的 ASIL 确定提供指导。SAE J2980 作为 ISO 26262 的补充和细化，专注于运动控制系统。它遵循 ISO 26262 的基本原则和方法，为特定的运动控制系统提供更详细和具体的指导。该标准主要应用于汽车运动控制系统的功能安全分析，如车辆的转向系统、制动系统、推进系统等。通过该标准的指导，可以帮助工程师在设计阶段识别潜在的危险事件，并采取相应的安全措施，确保车辆在各种行驶条件下的安全。

表 11-4 暴露度边界条件（d）

	E1	E2	E3	E4
时间范围 d	-	<1%平均运行时间	1%-10%平均运行时间	>10%平均运行时间
运行时间 小时/年	<0.4 小时/年	0.4 小时/年≤x<4 小时/年	4 小时/年≤x≤4 小时/年	>10%平均运行时间

表 11-5 暴露度边界条件（f）

	E1	E2	E3	E4
频率范围 f	对于绝大多数驾驶员 小于一年发生一次	对于绝大多数驾驶员 一年发生几次	对于一般的驾驶员一 个月发生一次或多次	平均几乎发生在每次 驾驶中
基础形式循环数量/ 年	<1 次/年	1 次/年≤x<10 次/年	10 次/年≤x≤100 次/ 年	>100 次/年

注：本标准参照SAE J2980的频率范围建议，并结合中国典型场景库进行本土化校准。

11.3.4 VDA 702 场景目录与组合概率方法

VDA 702 由德国汽车工业协会（VDA）制定，专注于确定车辆行驶过程中的暴露度等级，为汽车功能安全中的危害分析和风险评估提供支持^[14]。该标准主要应用于汽车的功能安全分析中，特别是在危害分析和风险评估阶段。通过对车辆行驶场景的全面覆盖和暴露度等级的确定，为后续的安全措施制定和风险控制提供依据，提供了可操作的工程落地方法。

标准化的场景目录：将车辆运行场景分解为独立的基础要素（如道路类型、路面条件、驾驶操作等），并为每个要素给出了 E 参数参考值（基于轿车数据和专家评估）。

组合概率方法：危害场景由多个独立的基础场景要素组合而成，组合场景的暴露概率等于各要素概率的乘积。这是本标准暴露率量化的核心算法。

11.3.5 核心思想：场景要素的概率乘积

根据第 8 章定义的七层场景架构（道路结构、道路设施、环境条件、交通参与者、动态要素、系统状态、数字信息），一个完整的运行场景可以分解为多个相互独立的基础场景要素。例如，场景“高速直线行驶中前车紧急制动”可分解为：

- a) 道路类型：高速公路；
- b) 路面条件：干燥；
- c) 本车状态：高速行驶；
- d) 交通参与者：前车紧急制动

由于这些要素在统计上相互独立，组合场景的总暴露概率等于各要素概率的乘积：

$$P_E = P_{s1} \times P_{s2} \times P_{s3} \times \cdots \times P_{sn} \cdots \cdots \cdots 14$$

式中：

P_E ：组合场景的暴露概率（无量纲，最终转化为持续时间百分比或频率）；

P_{si} ：第 i 个基础场景要素的概率（持续时间百分比或年发生频率）。

注：这一方法遵循了VDA 702标准的核心思路。VDA 702已系统地将车辆运行场景分解为标准化基础要素，并为每个基础要素提供了暴露概率参考值（基于轿车数据和专家评估）。评估人员在获取基础要素概率时，可优先参考VDA 702提供的参考值，也可结合中国典型场景库或自动驾驶数据进行修正。

11.3.6 暴露率判定流程

评估人员应按照以下流程进行暴露率量化：

- a) 确定危害事件关联的运行场景，并按照七层架构分解为基础场景要素。
- b) 获取每个基础场景要素的暴露数据：
 - 对于持续时间型要素（如道路类型、路面条件、车辆状态），获取其占平均运行时间的百分比。
 - 对于频率型要素（如特定驾驶操作、交通参与者行为），获取其每年发生的次数。

数据来源优先采用中国典型场景库和自然驾驶数据，当缺乏本土数据时可参考 VDA 702 场景目录或 SAE J2980 推荐值。

- c) 计算组合场景的总暴露概率：
将各要素的概率（持续时间百分比或年频率）相乘。
若结果为持续时间百分比，则对照表 11-2 判定 E 等级。
若结果为年频率，则对照表 11-3 判定 E 等级。
- d) 取两个维度中较高的 E 等级作为最终结果。
- e) 记录评估依据：包括数据来源、要素分解、概率取值、计算过程和判定结果。

11.4 评估流程

步骤 1：场景要素分解

针对每个危害事件，评估人员应从第 8 章的典型运行场景清单中确定关联场景，并按照七层架构将场景分解为独立的基础要素。

示例：危害事件“湿滑路面紧急制动场景下制动力丧失”关联的场景“湿滑路面紧急制动”可分解为：

表 11-6 场景分解示例

层级	要素	取值
第 1 层：道路结构	道路类型	城市道路
第 1 层：道路结构	坡度	无坡
第 3 层：环境条件	路面附着	湿滑 ($\mu \leq 0.4$)
第 4 层：交通参与者	前车状态	紧急制动
第 5 层：动态要素	本车车速	≥ 50 km/h
第 6 层：系统状态	驾驶模式	人工

步骤 2：获取各要素的频率数据

评估人员应从以下数据来源中获取每个基础场景要素的持续时间百分比（占平均运行时间的比例）或年发生频率：

- a) 优先使用中国典型场景库或自然驾驶数据，以反映中国本土道路环境及驾驶行为。
- b) 可参考 VDA 702 场景目录中提供的参考值，并在评估报告中注明“参考 VDA 702 数据”。
- c) 对于车辆运行基本参数（如年平均运行时间、加速/制动踏板操作占比等），可使用用户统计数据或行业通用值。

步骤 3：计算组合场景的总暴露概率

根据场景要素的独立性假设，组合场景的总暴露概率为各要素概率的乘积。

a) 持续时间维度的计算

若所有要素均为持续时间百分比（无量纲），则乘积结果即为组合场景占平均运行时间的百分比按 14 式计算

b) 频率维度的计算

若要素中包含年发生频率（次/年），则乘积结果为组合场景的年发生频率：

$$P_{frequency} = P_{s1} \times P_{s2} \times \cdots \times P_{sn} \times N_{base} \cdots \cdots 15$$

式中：

N_{base} ：基准年行驶循环数（通常取 1000 次/年）。

c) 混合计算

当要素同时包含持续时间和频率时，应分别计算持续时间维度和频率维度的结果，然后各自判定 E 等级，最后取高者。

步骤 4：判定 E 等级

根据计算得到的持续时间百分比或年频率，分别对照表 11-4 和表 11-5，确定 E 等级。若两个维度判定的等级不同，取较高的等级。

表 11-7 E 等级判定规则

判定维度	计算公式	对照表	示例阈值
持续时间	$P_{duration}(\%)$	表 11-4	$<1\% \rightarrow E2; 1\% \sim 10\% \rightarrow E3; >10\% \rightarrow E4$
频率	$P_{frequency}(\text{次/年})$	表 11-5	$<1 \text{ 次/年} \rightarrow E1; 1 \sim 10 \text{ 次/年} \rightarrow E2; 10 \sim 100 \text{ 次/年} \rightarrow E3; >100 \text{ 次/年} \rightarrow E4$

注：当计算值处于边界时，取更保守（更高）的E等级。

步骤 5：记录评估依据

评估人员在评估报告中应完整记录以下信息：

- a) 数据来源：使用的场景库版本、自然驾驶数据里程、车辆运行统计周期，若参考了 VDA 702 数据需注明；
- b) 要素分解：按照七层架构列出的所有基础场景要素；
- c) 各要素概率：每个要素的取值及其数据来源；
- d) 计算过程：概率乘积的详细计算步骤；
- e) 判定结果：持续时间维度 E 等级、频率维度 E 等级、最终 E 等级。

注：若存在要素相关性或数据不确定性，应说明处理原则。

11.5 评估示例

危害事件：车辆在坡道起步时，由于坡道辅助功能失效，导致车辆后溜与后方车辆碰撞（关联场景：坡道起步）。

步骤 1：场景要素分解

根据第 8 章七层架构，将“坡道起步”场景分解为独立的基础要素：

表 11-8 示例场景要素分解

层级	要素	取值
第 1 层：道路结构	坡度	有坡（>3%）
第 5 层：动态要素	本车车速	0 km/h（静止）
第 5 层：动态要素	制动踏板状态	松开
第 6 层：系统状态	驾驶模式	人工

步骤 2：获取各要素暴露数据

表 11-9 典型场景库和自然驾驶数据的典型值

要素	概率类型	概率值	数据来源
有坡路段占比（>3%）	持续时间	10%	中国典型场景库/地图数据
车辆静止（车速为 0）占比	持续时间	20%	自然驾驶数据
制动踏板松开占比（静止时）	持续时间	30%	自然驾驶数据

注：上述概率均基于中国典型场景库和自然驾驶数据的典型值。若缺乏本土数据，可参考VDA 702中类似要素的参考值。

步骤 3：计算组合场景总暴露概率（持续时间维度）
该场景所有要素均为持续时间百分比，因此直接相乘：

$$P_{duration} = 0.10 \times 0.20 \times 0.30 = 0.006 = 0.6\%$$

步骤 4：判定 E 等级

计算得到的持续时间为 0.6%，小于 1%，对照表 11-2（基于运行场景持续时间），属于 E2（低概率，<1%的平均运行时间）。频率维度在此简单场景中不再单独计算，以持续时间结果为准。

步骤 5：记录评估依据

数据来源：中国典型场景库 v2.0，自然驾驶数据（10000 公里）

要素分解：坡度>3%（10%）、车辆静止（20%）、静止时制动踏板松开（30%）

计算过程： $0.10 \times 0.20 \times 0.30 = 0.006 = 0.6\%$

判定结果：E2

11.6 输出物汇总

输出物 11-1 暴露率 E 评估记录表：包含危害编号、关联场景、场景要素分解（七层架构各要素取值）、各要素概率类型及数值、数据来源（若参考 VDA 702 需注明）、持续时间乘积结果、频率乘积结果、持续时间维度 E 等级、频率维度 E 等级、最终 E 等级、评估依据。

12 可控性（C）量化评估方法

12.1 目的

本章旨在建立线控制动系统危害事件可控性（C）的量化评估方法。可控性衡量的是驾驶员或其他交通参与者通过及时反应避免危害事件发生或减轻伤害程度的可能性。根据 ISO 26262-3，可控性分为 C0 至 C3 四个等级，分别表示从“完全可控”到“难以控制”。本标准综合考虑驾驶员反应时间、车辆动力学响应、人机交互效果三个核心维度，建立量化评估模型，确定每个危害事件的可控性等级。

12.2 输入准备

表 12-1 输入准备

资料名称	来源	说明
危害事件清单	第 9 章输出物 9-1	包含危害编号、失效模式、场景参数
失效特征参数表	第 7 章输出物 7-1	提供失效响应时间、失效幅值等
车辆动力学参数	整车技术文档	车辆质量、制动性能、转向响应等
人因工程数据	行业研究/实验数据	驾驶员反应时间、接管成功率、预警有效性
系统设计文档	系统设计部门	冗余架构、故障响应策略、预警方式

12.3 量化模型基础

12.3.1 可控性定义与等级

可控性是指驾驶员或其他交通参与者通过及时反应避免危害事件发生或减轻伤害程度的能力。

根据 ISO 26262-3，可控性分为 C0 至 C3 四个等级，其含义如下：

表 12-2 可控性等级说明

可控性等级	C0	C1	C2	C3
描述	可控	简单可控	一般可控	难以控制或不可控
驾驶因素和场景	超过 99% 的普通驾驶员或交通参与者能够避免伤害	90% 到 99% 普通驾驶员或交通参与者能够避免伤害	不到 90% 的普通驾驶员或交通参与者能够避免伤害	超过 99% 的普通驾驶员或交通参与者能够避免伤害

12.3.2 可控性的影响因素

可控性取决于多个因素的相互作用。在车辆纵向碰撞场景中，最关键的影响因素包括：

- a) 驾驶员反应时间：从失效发生到驾驶员开始采取制动操作所需的时间。反应时间越长，车辆在无有效制动状态下行驶的距离越长，碰撞风险越高。
- b) 系统响应时间：从驾驶员踩下制动踏板到制动系统实际产生有效减速度的时间。响应时间越短，制动效果越早发挥。
- c) 相对速度：本车与前车（或障碍物）之间的速度差。相对速度越大，同样时间内接近的距离越大，所需的安全距离越长。
- d) 实际距离：失效发生时本车与前车（或障碍物）之间的空间距离。距离越近，可供反应和制动的余地越小。
- e) 失效后剩余制动力：线控制动系统失效后，车辆可能仍保留部分制动能力（如机械备份）。剩余制动力越大，制动减速度越高，越容易避免碰撞。

12.3.3 制动过程时序分解

从失效发生到车辆开始有效减速，整个制动过程可以分解为三个连续的时间段：

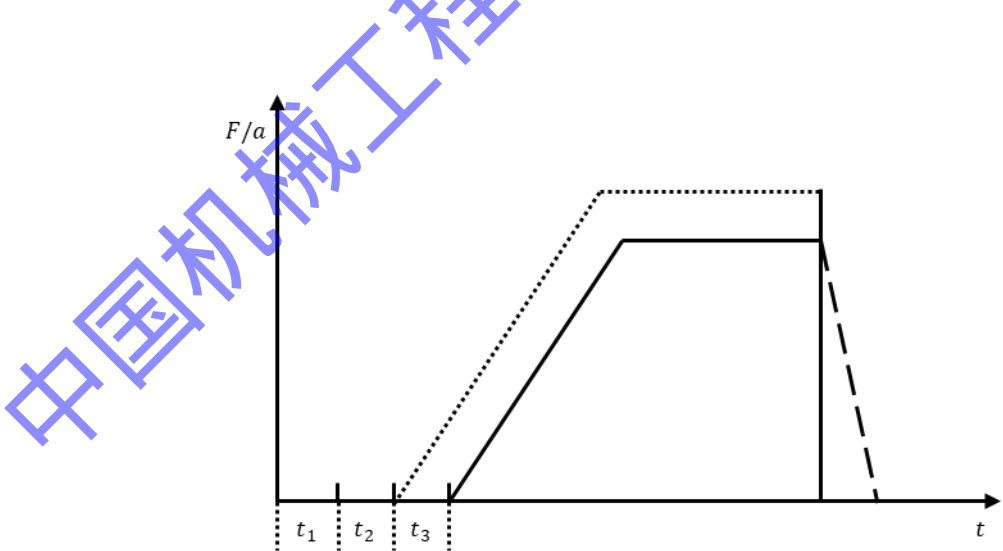


图 12-1 制动过程

驾驶员感知时间 t_1

失效发生后，驾驶员需要一定时间才能意识到危险的存在。这段时间包括视觉/听觉信号的接收、大脑对信息的处理以及对危险程度的判断。感知时间的长短受驾驶员警觉状态、预警方式、场景复杂程度等因素影响。在最严苛情况下（如驾驶员分心或无预警），感知时间可取典型最大值。

驾驶员控制响应时间 t_2

驾驶员意识到危险后，需要将决策转化为实际行动——将脚从加速踏板移动到制动踏板上但未踩下时。这段时间包括神经传导、肌肉收缩以及肢体运动的时间。控制响应时间与驾驶员的年龄、经验、身体状态有关。

系统响应时间 t_3

自驾驶员踩下制动踏板产生电信号触发起，至轮边执行机构建立起目标制动力（通常以达到90%目标压力为准）的时间总和。该指标涵盖了传感器信号采集延迟、总线传输延迟、控制算法处理时间以及执行器物理建压时间。系统响应时间与系统架构、硬件性能、软件算法密切相关。

总反应时间 $t_{total} = t_1 + t_2 + t_3$ ，即从失效发生到车辆开始产生有效减速度的总时间。在此期间，车辆基本维持失效发生前的运动状态（无有效制动），以相对速度继续接近前方目标。

12.3.4 关键距离定义

基于上述时序分解，可以定义三个关键距离：

反应距离 S_1 ：在总反应时间 t_{total} 内，车辆以相对速度 v_{rel} 行驶的距离。这段时间内驾驶员尚未采取有效制动，车辆继续接近前方目标。

$$S_1 = v_{rel} \cdot (t_1 + t_2 + t_3) \dots\dots\dots 16$$

式中：

v_{rel} ：本车与前车的相对速度（m/s）；

t_{total} ：总反应时间（s）。

反应距离 S_1 的意义在于：如果失效发生时两车的实际距离 S 小于或等于 S_1 ，则意味着在驾驶员尚未开始有效制动时，碰撞已经发生或不可避免。这种情况下，驾驶员完全没有反应的机会，可控性极差。

制动距离 S_2 ：从制动开始到两车速度相同（或本车停止）所需的距离。这段距离取决于相对速度和制动减速度。

$$S_2 = \frac{v_{rel}^2}{2a} \dots\dots\dots 17$$

式中：

a ：失效后车辆实际能达到的制动减速度（m/s²）。

制动距离 S_2 反映了在理想制动条件下，从开始减速到完全避免碰撞所需的最小空间。制动减速度 a 取决于失效后的剩余制动能力：若制动力完全丧失，则 a 取车辆机械制动或滑行减速度（通常不低于 2.44m/s²）；若部分丧失，则按剩余比例折算。

总安全距离 S_3 ：总安全距离是反应距离与制动距离之和，代表从失效发生到完全避免碰撞所需的最小初始距离。

$$S_3 = S_1 + S_2 \dots\dots\dots 18$$

总安全距离 S_3 的意义在于：如果失效发生时两车的实际距离 S 大于 S_3 ，则驾驶员有充分的反应时间和制动空间，可以通过单纯的制动操作避免碰撞；如果实际距离介于 S_1 和 S_3 之间，则仅靠制动可能不足，但驾驶员仍可能通过转向等其他操作避免碰撞。

12.3.5 可控性判定原理

将失效发生时的实际距离 S 与上述两个阈值 S_1 和 S_3 进行比较，可以得到可控性的定量判定：

表 12-3 可控性等级评估矩阵构建依据表

条件	物理含义	可控性等级	解释
----	------	-------	----

$S \leq S_1$	反应距离内已发生碰撞	C3	驾驶员尚未反应即已碰撞，无法避免
$S_1 < S \leq S_3$	反应后可开始制动，但仅靠制动可能不足	C2	驾驶员有反应时间，但需采取转向等额外操作才能避免，一般可控
$S > S_3$	有充分反应和制动空间	C1/C0	驾驶员可通过制动或转向完全避免，简单可控或完全可控

对于 $S > S_3$ 的情况，进一步区分 C1 和 C0：
若驾驶员可通过单纯的制动操作避免碰撞，且操作较为自然，通常判定为 C1。
若驾驶员极易避免（如极低相对速度、极大距离），或场景本身几乎不构成威胁，可判定为 C0。

12.3.6 典型参数取值

为便于工程应用，本标准推荐采用以下典型参数（基于行业通用数据，适用于最严苛评估）：

表 12-4 经典参数取值参考

参数	含义	推荐取值	说明
t_1	驾驶员感知时间 ^[15]	0.4s	神经延迟最大值
t_2	驾驶员控制响应时间	1.12s	肌肉延迟最大值
t_3	系统响应时间	0.2s	线控制动典型响应时间
t_{total}	总反应时间	1.72s	从失效到产生减速度的总时间
a （完全丧失）	失效后制动减速度	2.44m/s ²	纯机械制动减速度（GB 标准下限）

根据表 12-4 将数据带入公式进行计算，并细化车辆相对速度和相对距离，可以分析得出可控性评估矩阵，本矩阵列举了大部分情况。

表 12-5 可控度等级评估矩阵

相对距离 (m) 相对 车速 (km/h)		[0,5]	(5,10]	(10,20]	(20,30]	(30,40]	(40,50]	(50,60]	(60,70]	(70,80]	(80,90]	(90,100]
低速	$v \leq 5$	C1	C0	C0	C0	C0	C0	C0	C0	C0	C0	C0
	$5 < v \leq 10$	C2	C1	C0	C0	C0	C0	C0	C0	C0	C0	C0
	$10 < v \leq 15$	C3	C2	C1	C0	C0	C0	C0	C0	C0	C0	C0
	$15 < v \leq 20$	C3	C2	C1	C0	C0	C0	C0	C0	C0	C0	C0

速	20											
	< v	C3	C3	C2	C1	C0	C0	C0	C0	C0	C0	C1
	≤ 30											
	30											
	< v	C3	C3	C2	C2	C2	C1	C0	C0	C0	C0	C0
速	≤ 40											
	40											
	< v	C3	C3	C3	C2	C2	C2	C2	C1	C0	C0	C0
	≤ 50											
	40											
速	< v	C3	C3	C3	C2	C2	C2	C2	C1	C0	C0	C0
	≤ 50											
高	50											
	< v	C3	C3	C3	C2	C2	C2	C2	C2	C1	C0	C0
	≤ 60											
	60											
	< v	C3	C3	C3	C3	C2	C2	C2	C2	C2	C1	C0
速	≤ 70											
	70											
	< v	C3	C3	C3	C3	C2	C2	C2	C2	C2	C2	C1
	≤ 80											

12.4 评估步骤

评估人员只需三步即可完成可控性量化评估：

步骤 1：获取场景参数

从危害事件中提取：

相对车速 v_{rel} （km/h）

实际相对距离 S（m）

步骤 2：查表

将相对车速和相对距离按表 12-5 查找对应的 C 等级。

步骤 3：记录结果

在评估记录表中填写查表得到的 C 等级及依据。

12.5 评估示例

示例 1：城市跟车，相对车速 30 km/h，实际距离 20 m

查表：相对车速 30、距离 20 → C2

示例 2：高速行驶，本车 80 km/h，前车静止（相对车速 80 km/h），距离 50 m

查表：相对车速 80、距离 50 → C2

示例 3：低速泊车，相对车速 5 km/h，距离 5 m

查表：相对车速 5、距离 5 → C1

12.6 输出物汇总

输出物 12-1 可控性 C 评估记录表：包含危害编号、相对车速、实际距离、查表得到的 C 等级、特殊修正说明（如有）、评估依据。

13 S/E/C 综合评估与 ASIL 等级确定

13.1 目的

本章旨在根据第 10 章、第 11 章、第 12 章分别量化得到的严重度（S）、暴露率（E）、可控性（C）等级，综合判定每个危害事件的 ASIL 等级，确定系统的安全目标，并形成完整的评估报告。

13.2 输入准备

表 13-1 输入准备

资料名称	来源	说明
严重度 S 评估记录表	第 10 章输出物 10-1	每个危害事件的 S 等级（S0～S3）
暴露率 E 评估记录表	第 11 章输出物 11-1	每个危害事件的 E 等级（E0～E4）
可控性 C 评估记录表	第 12 章输出物 12-1	每个危害事件的 C 等级（C0～C3）
危害事件清单	第 9 章输出物 9-1	危害编号及描述

13.3 ASIL 等级判定

ASIL 等级由 S、E、C 三个参数共同决定，依据 ISO 26262-3 给出的 ASIL 判定表（见表 13-2）。表中 QM 表示“质量管理”，即无需按照 ASIL 要求进行功能安全开发，按常规质量管理即可。而 ASIL A、ASIL B、ASIL C 和 ASIL D 分别代表四个由低到高递增的安全完整性等级，其中 ASIL A 为最低安全要求等级，ASIL D 为最高安全要求等级。随着 ASIL 等级的提升，对线控制动系统在硬件随机失效概率、软件架构严谨性以及安全完整性指标等方面的要求越严苛，以确保系统在发生潜在失效时具备足够的风险预防与控制能力。

表 13-2 ASIL 等级判定表

S	E	C		
		C1	C2	C3
S1	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
	E1	QM	QM	QM
S2	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C

	E4	B	C	D
--	----	---	---	---

注：表中 A、B、C、D 分别指代 ASIL A、ASIL B、ASIL C 和 ASIL D。

查表方法：以S、E、C的等级组合在表中查找对应的ASIL等级。若表中未列出的组合（如S0、E1、C1），则按S0或E0处理，结果为QM。

13.4 评估示例

危害事件：高速直线行驶中前车紧急制动场景下制动力丧失

步骤 1：收集 S/E/C 评估结果

严重度 S：S2（碰撞速度 47.5 km/h）

暴露率 E：E4（持续时间 10.71% > 10%）

可控性 C：C2（相对车速 30 km/h，距离 20 m，查表得 C2）

步骤 2：查 ASIL 判定表

以 S2、E4、C2 查表 12-1，对应 ASIL D

步骤 3：系统安全目标确定

若该危害事件为系统最高等级，则系统安全目标为 ASIL D

注：典型场景评级详见附录C。

13.5 输出物汇总

输出物 13-1 ASIL 等级综合判定表：包含危害编号、S 等级、E 等级、C 等级、ASIL 等级、备注。

附 录 A
(资料性附录)
功能-失效矩阵示例

A.1 EHB 系统功能-失效模式矩阵（电子液压制动）

表 A-1 EHB 系统功能-失效模式矩阵（电子液压制动）

图例： ✓ 功能丧失 ✓ 功能异常 ✓ 非预期功能

功能编号	功能名称	失效模式	功能丧失	功能异常	非预期功能
EHB-F-01	常规制动	制动力丧失	✓		
		制动助力不足		✓	
		制动响应延迟		✓	
		制动拖滞		✓	
		非预期制动			✓
EHB-F-02	踏板感模拟	踏板感丧失	✓		
		踏板感异常（力-位移特性偏差）		✓	
EHB-F-03	制动压力精确控制	压力控制失效	✓		
		压力控制偏差过大		✓	
		压力控制振荡		✓	
EHB-F-04	ABS	ABS 功能丧失	✓		
		ABS 调压异常		✓	
		ABS 误触发			✓
EHB-F-05	EBD	EBD 功能丧失	✓		
		左右轮制动不平衡		✓	
EHB-F-06	TCS	TCS 功能丧失	✓		

功能编号	功能名称	失效模式	功能丧失	功能异常	非预期功能
		TCS 介入不及时		✓	
		TCS 误介入			✓
EHB-F-07	ESC	ESC 功能丧失	✓		
		ESC 干预力矩异常		✓	
		ESC 误激活			✓
EHB-F-08	BA	BA 功能丧失	✓		
		BA 建压不足		✓	
		BA 误触发			✓
EHB-F-09	AEB	AEB 执行失效	✓		
		AEB 执行延迟		✓	
		AEB 非预期触发			✓
EHB-F-10	再生制动协调	再生制动协调功能丧失	✓		
		液压与再生切换制动力突变		✓	
		液压过度介入			✓
EHB-F-11	制动能量回收模式管理	回收模式管理失效	✓		
		回收功率偏离目标值		✓	
EHB-F-12	EPB	EPB 无法夹紧	✓		
		EPB 夹紧力不足		✓	
		EPB 误释放			✓
		EPB 无法释放		✓	
EHB-F-13	自动驻车保持	驻车保持功能失效	✓		
		意外自动释放			✓
EHB-F-14	坡道辅助	坡道辅助失效	✓		

功能编号	功能名称	失效模式	功能丧失	功能异常	非预期功能
		制动保持时间异常		✓	
EHB-F-15	液压系统自检	自检功能失效	✓		
		漏检故障		✓	
		误报故障			✓
EHB-F-16	制动系统健康监测	故障检测失效	✓		
		告警输出延迟		✓	
		虚假告警输出			✓
EHB-F-17	制动热管理	热管理功能失效	✓		
		温度监测偏差		✓	
EHB-F-18	冗余制动控制	冗余切换失效	✓		
		切换响应延迟		✓	
		误切换至备用控制器			✓
EHB-F-19	系统降级管理	降级切换失效	✓		
		降级策略执行异常		✓	
EHB-F-20	自动驾驶制动执行接口	接口通信失效	✓		
		减速度执行偏差		✓	
		非预期执行制动指令			✓
EHB-F-21	制动信号输出与状态反馈	信号输出中断	✓		
		信号值错误		✓	

A.2 EMB 系统功能-失效模式矩阵（电子机械制动）

表 A-2 EMB 系统功能-失效模式矩阵（电子机械制动）

图例： ✓ 功能丧失 ✓ 功能异常 ✓ 非预期功能

功能编号	功能名称	失效模式	功能丧失	功能异常	非预期功能
EMB-F-01	常规制动	卡钳夹紧力丧失	✓		
		夹紧力不足		✓	
		制动响应延迟		✓	
		制动拖滞（卡钳无法完全释放）		✓	
		非预期制动			✓
EMB-F-02	踏板感模拟	踏板感丧失	✓		
		踏板感异常（力-位移特性偏差）		✓	
EMB-F-03	夹紧力精确控制	夹紧力闭环控制失效	✓		
		夹紧力控制偏差		✓	
		夹紧力振荡		✓	
EMB-F-04	电机位置控制	位置控制失效	✓		
		位置控制偏差		✓	
		位置传感器信号失真		✓	
EMB-F-05	ABS	ABS 功能丧失	✓		
		ABS 夹紧力调节异常		✓	
		ABS 误触发			✓
EMB-F-06	EBD	EBD 功能丧失	✓		
		轮间夹紧力分配不均		✓	
EMB-F-07	TCS	TCS 功能丧失	✓		
		TCS 介入不及时		✓	

功能编号	功能名称	失效模式	功能丧失	功能异常	非预期功能
		TCS 误介入			✓
EMB-F-08	ESC	ESC 功能丧失	✓		
		ESC 差异夹紧力异常		✓	
		ESC 误激活			✓
EMB-F-09	BA	BA 功能丧失	✓		
		BA 夹紧力提升不足		✓	
		BA 误触发			✓
EMB-F-10	AEB	AEB 执行失效	✓		
		AEB 执行延迟		✓	
		AEB 非预期触发			✓
EMB-F-11	再生制动协调	再生制动协调功能丧失	✓		
		电机制动与夹紧力切换突变		✓	
		卡钳夹紧力过度介入			✓
EMB-F-12	制动能量回收模式管理	回收模式管理失效	✓		
		回收功率偏离目标值		✓	
EMB-F-13	EPB	EPB 无法夹紧	✓		
		EPB 自锁力不足		✓	
		EPB 误释放			✓
		EPB 电机无法反转释放		✓	
EMB-F-14	自动驻车保持	驻车保持功能失效	✓		
		意外自动释放夹紧力			✓
EMB-F-15	坡道辅助	坡道辅助失效	✓		
		夹紧力保持时间异常		✓	

功能编号	功能名称	失效模式	功能丧失	功能异常	非预期功能
EMB-F-16	卡钳电机自检	自检功能失效	✓		
		漏检故障		✓	
		误报故障			✓
EMB-F-17	制动系统健康监测	故障检测失效	✓		
		告警输出延迟		✓	
		虚假告警输出			✓
EMB-F-18	制动热管理	热管理功能失效	✓		
		卡钳电机温度监测偏差		✓	
EMB-F-19	冗余制动控制	冗余切换失效	✓		
		切换响应延迟		✓	
		误切换至备用控制器			✓
EMB-F-20	系统降级管理	降级切换失效	✓		
		降级策略执行异常		✓	
EMB-F-21	自动驾驶制动执行接口	接口通信失效	✓		
		减速度执行偏差		✓	
		非预期执行制动指令			✓
EMB-F-22	制动信号输出与状态反馈	信号输出中断	✓		
		信号值错误		✓	

附 录 B
(资料性附录)

线控制动系统典型运行场景清单

B.1 说明

本附录为线控制动系统典型运行场景的完整清单，供危害识别与暴露率评估使用。评估人员应根据实际系统的运行设计域（ODD）在此基础上补充或调整场景。

B.2 场景编码规则

场景编号采用"SC-XX"格式，按功能域分组：

编号段	功能域
SC-01～SC-10	常规制动场景
SC-11～SC-18	自动/智驾制动场景
SC-19～SC-22	特殊工况场景
SC-23～SC-28	系统状态异常场景

B.3 典型运行场景清单

表 B-1 典型运行场景

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
SC-01	高速直线紧急制动	高速公路匀速行驶，前车突然紧急制动，驾驶员踩紧急制动踏板	高速公路；直道；多车道；无坡	标线清晰；无停车标志；有隔离护栏	晴天；白天；高附着（≥0.8）	前车紧急制动；前车距离近（<40m）；相邻车道有并行	高速（~80km/s）；踏板紧急（>70%）；制动意图：紧急停车；空载	人工驾驶；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-02	城市低速跟车	城市道路早晚高峰，低速跟车，频繁轻踩和	城市道路；直道；多车道；无坡	交通信号灯；标线清晰；无	晴天；白天；高附着（≥0.8）	前车减速/静止；前车距离近（<20m）；无相邻切	低速（~15 km/s）；踏板轻踩 / 中度（<30% ~	人工驾驶；制动系统正常；主控制器正常	定位精度高；地图信息准确

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
	车频繁启停	中踩制动踏板		护栏		入	70%)；制动意图：减速；空载		
SC-03	湿滑路面紧急制动	雨雪路面行驶，前方突现行人横穿，驾驶员紧急踩制动踏板，ABS介入	城市/乡村道路；直道；单/多车道；无坡	标线模糊；有限速标志；无护栏	雨雪；白天；低附着 (≤ 0.4)	行人横穿；前车距离中 (20 ~ 50m)；无相邻车辆	低速 (~15 km/s)；踏板紧急 (>70%)；制动意图：紧急停车；空载	人工驾驶；制动系统正常 (ABS 激活)；主控制器正常	定位精度中；地图信息准确
SC-04	坡道起步坡道辅助激活	坡道停车后起步，松开制动踏板，HAC短暂保持制动防溜车，随后平顺释放	城市/乡村道路；小坡 ($3^{\circ} \sim 10^{\circ}$)；单车道；上坡	无停车标志；标线清晰；无护栏	晴天；白天；高附着 (≥ 0.8)	无前车；无行人；无相邻车辆	车速为0；踏板释放；制动意图：无制动（起步）；空载	人工驾驶；制动系统正常 (HAC 激活)；主控制器正常	定位精度中；地图信息准确（坡度已知）
SC-05	下陡坡持续制动	山区陡坡下行，驾驶员持续中度踩制动踏板，制动热管理介入	山区道路；大坡 ($>10^{\circ}$)；单车道；下坡	有限速/陡坡警告标志；标线清晰；有护栏	晴天/雨；白天；中附着 ($0.4 \sim 0.8$)	无前车；无行人；无相邻车辆	中速 (~50 km/s)；踏板中度 (30% ~ 70%)；制动意图：减速；满载	人工驾驶；制动系统正常 (热管理激活)；主控制器正常	定位精度中；地图信息准确（坡度已知）
SC-06	弯道中等速	急弯路段行驶中驾驶员施加中度制动，ESC	城市/乡村道路；急弯（半径 $\leq 200\text{m}$ ）；	有弯道警告标志；标线清	晴天；白天；高附着 (≥ 0.8)	无前车；无行人；无相邻车辆	低速 (~15 km/s)；踏板中度 (30% ~ 70%)；制	人工驾驶；制动系统正常 (ESC 待命)；主	定位精度高；地图信息准确（曲率

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
	度制动	监控横向稳定性	单车道；无坡	晰；有护栏			动意图：减速；空载	控制器正常	已知）
SC-07	交叉路口前减速停车	城市路口前减速并停车等待红灯，行人从人行横道横穿	城市道路；交叉路口；多车道；无坡	交通信号灯；停止线；斑马线；标线清晰	晴天；白天；高附着（≥0.8）	行人横穿；对向车辆；前车距离中（20～50m）	低速（~15 km/s）；踏板中度（30%～70%）；制动意图：减速至停；空载	人工驾驶；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-08	高速公路变道后制动	高速变道完成后发现前方车辆减速，相邻车道有车辆切入，驾驶员中度制动	高速公路；直道；多车道；无坡	标线清晰；有限速标志；有隔离护栏	晴天；白天；高附着（≥0.8）	前车减速；前车距离中（20～50m）；相邻车道车辆切入	高速（~80km/s）；踏板中度（30%～70%）；制动意图：减速；空载	人工驾驶；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-09	停车场低速避让行人	停车场内低速行驶，前方行人静止或缓行，驾驶员轻踩制动减速	停车场；低速区；弯道/直道混合；无坡	停车标志；标线模糊；无护栏	夜晚/隧道；高附着（≥0.8）	行人静止/缓行；障碍物（车位隔离桩）；无相邻车辆	低速（~15 km/s）；踏板轻踩（<30%）；制动意图：减速；空载	人工驾驶；制动系统正常；主控制器正常	定位精度低（无GPS）；地图信息缺失
SC-10	再生制动介入	减速时再生制动优先介入，液压/电机夹紧力按需协调	城市道路；直道；多车道；无坡	交通信号灯；标线清晰；无护栏	晴天；白天；高附着（≥0.8）	前车减速；前车距离中（20～50m）；无相邻切入	中速（~40km/s）；踏板轻踩（<30%）；制动意图：减速；空载	人工驾驶；制动系统正常（再生制动激活）；主控制器	定位精度高；地图信息准确

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
	协调	补充						正常	
SC-1 1	AE B 触发——前方静止障碍物	城市道路中速行驶，智驾系统识别前方静止障碍物并判断碰撞不可避免，触发AEB	城市道路；直道；多车道；无坡	标线清晰；无护栏	晴天；白天；高附着（ ≥ 0.8 ）	障碍物静止（车辆/箱体）；前车距离近（ $< 20\text{m}$ ）；无相邻车辆	中速（ $\sim 40\text{km/s}$ ）；无踏板输入；制动意图：AEB自主制动；空载	智驾介入；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-1 2	AE B 触发——行人横穿	夜间城市道路中速行驶，行人突然横穿，智驾系统触发AEB，驾驶员未介入	城市道路；直道；多车道；无坡	斑马线（无信号灯）；标线清晰；无护栏	夜晚；高附着（ ≥ 0.8 ）	行人横穿；前车距离近（ $< 20\text{m}$ ）；无相邻车辆	中速（ $\sim 40\text{km/s}$ ）；无踏板输入；制动意图：AEB自主制动；空载	智驾介入；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-1 3	AE B 触发——前车紧急制动	高速公路行驶，前车突然紧急制动，TTC过短，智驾系统触发AEB制动	高速公路；直道；多车道；无坡	标线清晰；有隔离护栏；无限速标志	晴天；白天；高附着（ ≥ 0.8 ）	前车紧急制动；前车距离近（ $< 20\text{m}$ ）；相邻车道有并行	高速（ $\sim 80\text{km/s}$ ）；无踏板输入；制动意图：AEB自主制动；空载	智驾介入；制动系统正常；主控制器正常	定位精度高；地图信息准确

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
SC-14	自适应巡航跟车减速	高速公路ACC巡航，前车减速，智驾系统发出制动请求以维持安全跟车距离	高速公路；直道；多车道；无坡	标线清晰；有隔离护栏；有限速标志	晴天；白天；高附着（≥0.8）	前车减速；前车距离中（20～50m）；无相邻切入	高速（~80km/s）；智驾制动请求（轻到中度）；制动意图：减速；空载	智驾介入（ACC激活）；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-15	红灯前自动驻车激活	城市路口前停稳，Auto Hold自动激活，保持制动力直至检测到起步意图	城市道路；交叉路口；多车道；无坡	交通信号灯；停止线；标线清晰	晴天；白天；高附着（≥0.8）	无前车（已停车）；行人横穿（等待中）；无相邻切入	车速为0；踏板释放；制动意图：驻车保持；空载	智驾介入（Auto Hold激活）；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-16	智驾制动与驾驶员接管冲突	智驾系统发出减速制动指令时，驾驶员同时踩踏板，产生双输入叠加	城市道路；直道；多车道；无坡	标线清晰；交通信号灯；无护栏	晴天；白天；高附着（≥0.8）	前车减速；前车距离中（20～50m）；无相邻切入	中速（~50km/s）；踏板轻踩（驾驶员接管）；制动意图：双重输入；空载	智驾介入→驾驶员接管；制动系统正常；主控制器正常	定位精度高；地图信息准确
SC-17	自动驾驶检测异常	自动驾驶系统检测到内部异常（传感器或规划模块），发出紧急	高速公路；直道；多车道；无坡	标线清晰；有隔离护栏；有限速标志	晴天；白天；高附着（≥0.8）	无前车障碍；后方有跟随车辆；无行人	高速（~80km/s）；智驾制动请求（紧急）；制动意图：紧急停车；空载	智驾介入；制动系统正常；主控制器正常	定位精度高；地图信息准确

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
	常紧急停车	停车指令							
SC-18	满载陡坡持续制动热衰退	满载状态下长坡持续制动，制动器温度持续升高，热管理介入协调再生与摩擦分担	山区道路；大坡（>10°）；单车道；下坡	有陡坡警告标志；标线清晰；有护栏	晴天；白天；中附着（0.4~0.8）	无前车；无行人；无相邻车辆	中速（~50km/s）；踏板中度（30%~70%）；制动意图：减速；满载	人工驾驶；制动系统正常（热管理激活）；主控制器正常	定位精度中；地图信息准确（坡度已知）
SC-19	大雾低能见度高速制动	高速公路大雾天气能见度极低，驾驶员识别前方静止车辆延迟，紧急制动	高速公路；直道；多车道；无坡	雾区警告标志；标线清晰；有隔离护栏	大雾；白天；高附着（≥0.8）	前车静止；前车距离近（<20m）；无相邻车辆	低速（~10 km/s）；踏板紧急（>70%）；制动意图：紧急停车；空载	人工驾驶；制动系统正常；主控制器正常	定位精度高；地图信息准确（雾区预警）
SC-20	冰雪路面低附着ABS高频	冰雪路面低附着，驾驶员中度制动，ABS高频调压防止车轮锁死	城市/乡村道路；直道；单/多车道；无坡	标线模糊（积雪覆盖）；有限速标志；无护栏	冰雪；白天；低附着（≤0.4）	前车减速；前车距离中（20~50m）；无相邻车辆	低速（~10km/s）；踏板中度（30%~70%）；制动意图：减速；空载	人工驾驶；制动系统正常（ABS高频激活）；主控制器正常	定位精度中；地图信息准确

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
	介入								
SC-2 1	逆光行驶识别延迟紧急制动	逆光环境驾驶员识别前方行人横穿延迟，踏板从轻踩迅速切换为紧急制动	城市道路；直道；多车道；无坡	斑马线；标线清晰；无护栏	逆光；白天；高附着（≥0.8）	行人横穿；前车距离近（<20m）；无相邻车辆	中速（~40km/s）；踏板轻踩→紧急（快速切换）；制动意图：紧急停车；空载	人工驾驶；制动系统正常（BA激活）；主控制器正常	定位精度高；地图信息准确
SC-2 2	急弯湿滑路面ESC介入制动	急弯路段遇雨天湿滑路面，驾驶员制动叠加转弯，ESC检测侧滑趋势并介入	乡村道路；急弯（半径≤200m）；单车道；无坡	弯道警告标志；标线模糊；有护栏	雨天；白天；低附着（≤0.4）	无前车；无行人；无相邻车辆	低速（~10km/s）；踏板中度（30%~70%）；制动意图：减速；空载	人工驾驶；制动系统正常（ABS/ESC激活）；主控制器正常	定位精度中；地图信息准确（曲率已知）
SC-2 3	制动系统降级运行中制动	主控制器部分故障，系统切换至降级模式，驾驶员在城市道路中度踩制动	城市道路；直道；多车道；无坡	标线清晰；交通信号灯；无护栏	晴天；白天；高附着（≥0.8）	前车减速；前车距离中（20~50m）；无相邻切入	中速（~40km/s）；踏板中度（30%~70%）；制动意图：减速；空载	人工驾驶；制动系统降级（备用控制器接管）；冗余已切换	定位精度高；地图信息准确

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
SC-2 4	冗余切换过程中驾驶员制动	主控故障触发冗余切换期间, 驾驶员遭遇前车紧急制动, 踩紧急制动踏板	高速公路; 直道; 多车道; 无坡	标线清晰; 有隔离护栏; 有限速标志	晴天; 白天; 高附着 (≥ 0.8)	前车紧急制动; 前车距离近 ($< 20\text{m}$); 相邻车道有并行	高速 ($\sim 80\text{km/s}$); 踏板紧急 ($> 70\%$); 制动意图: 紧急停车; 空载	人工驾驶; 制动系统冗余切换中; 主控故障/备用接管中	定位精度高; 地图信息准确
SC-2 5	CAN通信中断后制动请求	CAN/CAN FD 总线通信中断, 制动域无法接收整车指令, 驾驶员踩制动踏板	城市道路; 直道; 多车道; 无坡	标线清晰; 交通信号灯; 无护栏	晴天; 白天; 高附着 (≥ 0.8)	前车静止; 前车距离近 ($< 20\text{m}$); 无相邻切入	中速 ($\sim 40\text{km/s}$); 踏板中度 ($30\% \sim 70\%$); 制动意图: 减速; 空载	人工驾驶; 制动系统故障 (通信中断); 主控制器供电正常	定位精度高; 地图信息准确 (通信层故障与此独立)
SC-2 6	轮速传感器失效后湿滑路制动	轮速传感器失效导致 ABS/EBD 功能丧失, 驾驶员在低附着路面制动	城市道路; 直道; 单/多车道; 无坡	标线模糊; 有限速标志; 无护栏	雨天; 白天; 低附着 (≤ 0.4)	前车减速; 前车距离中 ($20 \sim 50\text{m}$); 无相邻车辆	中速 ($\sim 40\text{km/s}$); 踏板中度 ($30\% \sim 70\%$); 制动意图: 减速; 空载	人工驾驶; 制动系统降级 (ABS/EBD 不可用); 轮速传感器故障	定位精度中; 地图信息准确
SC-2	供	车辆供电	城市道	标线	晴天;	前车静止;	低速	人工驾	定位精

场景编号	场景名称	场景描述	道路结构	道路设施	环境条件	交通参与者	动态要素	系统状态	数字信息
7	电电压异常下低速制动	电压异常跌落，制动执行器性能下降，驾驶员低速前踩制动	路；直道；多车道；无坡	清晰；交通信号灯；无护栏	白天；高附着（≥0.8）	前车距离近（<20m）；无行人	（~10km/s）；踏板中度（30% ~ 70%）；制动意图：减速；空载	驶；制动系统降级（供电电压不足）；执行器性能下降	度高；地图信息准确
SC-28	单侧执行器失效后高速紧急制动	单侧 EMB/EHB 执行器失效（如断线或驱动故障），驾驶员高速遭遇前车紧急制动	高速公路；直道；多车道；无坡	标线清晰；有隔离护栏；有限速标志	晴天；白天；高附着（≥0.8）	前车紧急制动；前车距离近（<20m）；相邻车道有并行	高速（~80km/s）；踏板紧急（>70%）；制动意图：紧急停车；空载	人工驾驶；制动系统降级（单侧执行器失效）；备用控制器正常	定位精度高；地图信息准确

B.4 使用说明

本清单为基础场景集，评估人员在使用时应注意：

- a) 根据实际系统的运行设计域（ODD）筛选适用场景，不在 ODD 范围内的场景可标注为"不适用"并说明原因。
- b) 评估人员可根据实际需要在各编号段内补充场景，补充场景应遵循本附录的场景描述格式。
- c) 每个场景在后续 HARA 分析中应明确对应的危害事件、严重度（S）、暴露率（E）及可控性（C）评估结论。

附录 C

(资料性附录)

线控制动系统典型运行场景 S/E/C 评估与 ASIL 定级

表 C-1 典型场景评级表

场景编号	场景名称	场景描述	S	S 定级依据	E	E 定级依据	C	C 定级依据	ASIL
SC-01	高速直线紧急制动	高速公路匀速行驶，前车突然紧急制动，驾驶员踩紧急制动踏板	S3	高速追尾/正面碰撞，致命风险高	E3	高速公路行驶属高频场景，每次长途驾驶均可遭遇	C2	高速下规避空间有限，控制难度大	B
SC-02	城市低速跟车频繁启停	城市道路早晚高峰，低速跟车，频繁轻踩和中踩制动踏板	S0	低速轻微碰撞，无或轻伤风险	E3	城市通勤场景高频，几乎每次驾驶均发生	C1	速度低，驾驶员有充足反应时间规避	QM
SC-03	湿滑路面紧急制动	雨雪路面行驶，前方突现行人横穿，驾驶员紧急踩制动踏板，ABS 介入	S0	雨雪低速碰撞，轻伤或无	E2	雨雪天气有一定频率，非每日发生	C0	多数驾驶员可通过常规操作规避	QM
SC-04	坡道起步坡道辅助激活	坡道停车后起步，松开制动踏板，HAC 短暂保持制动防溜车，随后平顺释放	S1	低速溜车碰撞，中轻度伤害	E2	坡道停车较常见但非极高频	C0	驾驶员可及时重踩制动控车	QM
SC-05	下陡坡持续制动	山区陡坡下行，驾驶员持续中度踩制动踏板，制动热管理介入	S2	陡坡失控碰撞，重伤风险高	E1	山区陡坡满载下坡场景频率较低	C0	热衰退渐进发生，有提前应对可能	QM
SC-06	弯道中等速度制动	急弯路段行驶中驾驶员施加中度制动，ESC 监控横向稳定性	S1	弯道失控侧滑，中轻度伤害风险	E2	急弯路段中频出现，山区/乡村道路常见	C0	多数驾驶员可通过修正方向控车	QM
SC-07	交叉路	城市路口前减速并停	S1	路口低	E3	城市路口	C0	速度较低，	QM

场景编号	场景名称	场景描述	S	S 定级依据	E	E 定级依据	C	C 定级依据	ASIL
	口前减速停车	车等待红灯，行人从人行横道横穿		速碰撞，中轻度伤害		停车为极高频日常场景		有转向规避空间	
SC-08	高速公路变道后制动	高速变道完成后发现前方车辆减速，相邻车道有车辆切入，驾驶员中度制动	S0	变道轻微碰撞，无或轻度伤害	E2	高速变道后跟车制动较常见	C2	高速变道跟车，规避难度大	QM
SC-09	停车场低速避让行人	停车场内低速行驶，前方行人静止或缓行，驾驶员轻踩制动减速	S0	停车场极低速碰撞，轻伤或无	E3	停车场使用频率较高	C2	视线或空间受限，有一定规避难度	QM
SC-10	再生制动介入协调	减速时再生制动优先介入，液压/电机夹紧力按需协调补充	S0	制动力突变，轻微不适或轻伤	E3	电动车每次减速均可能发生，极高频	C2	驾驶员可通过微调踏板力部分补偿	QM
SC-11	AEB 触发——前方静止障碍物	城市道路中速行驶，智驾系统识别前方静止障碍物并判断碰撞不可避免，触发 AEB	S2	中速碰撞障碍物，严重重伤风险	E2	城市道路静止障碍物场景中频出现	C3	无预警且接管窗口极短，极难控制	A
SC-12	AEB 触发——行人横穿	夜间城市道路中速行驶，行人突然横穿，智驾系统触发 AEB，驾驶员未介入	S2	中速碰撞行人，重伤或致死风险	E2	行人横穿场景中频，夜间城市道路常见	C3	夜间视线差，几乎无接管反应时间	A
SC-13	AEB 触发——前车紧急制动	高速公路行驶，前车突然紧急制动，TTC 过短，智驾系统触发 AEB 制动	S3	高速追尾碰撞，致命风险极高	E3	高速公路跟车行驶为高频场景	C3	高速短 TTC，驾驶员完全无法接管	C
SC-14	自适应巡航跟车减速	高速公路 ACC 巡航，前车减速，智驾系统发出制动请求以维持安全跟车距离	S0	巡航低速差碰撞，中轻度伤害	E3	高速公路 ACC 使用频率高	C2	驾驶员处于监控状态，可接管规避	QM
SC-15	红灯前自动驻车激活	城市路口前停稳，Auto Hold 自动激活，保持制动力直至检测	S0	驻车失效溜车，轻微碰	E3	城市路口停车极高频	C0	驾驶员极易感知并踩刹车控	QM

场景编号	场景名称	场景描述	S	S 定级依据	E	E 定级依据	C	C 定级依据	ASIL
		到起步意图		擦伤害				车	
SC-16	智驾制动与驾驶员接管冲突	智驾系统发出减速制动指令时，驾驶员同时踩踏板，产生双输入叠加	S0	人机冲突致制动异常，轻微伤害	E2	人机共驾切换有一定频率	C2	驾驶员主动参与，可通过调整踏板力修正	QM
SC-17	自动驾驶检测异常紧急停车	自动驾驶系统检测到内部异常（传感器或规划模块），发出紧急停车指令	S3	高速失控碰撞，致命风险高	E1	自动驾驶内部异常触发紧急停车频率较低	C1	弱监控状态，但仍有一定接管可能	QM
SC-18	满载陡坡持续制动热衰退	满载状态下长坡持续制动，制动器温度持续升高，热管理介入协调再生与摩擦分担	S2	满载长坡失控，严重碰撞风险	E1	满载山区长坡驾驶频率较低	C0	渐进式发生，驾驶员可提前应对	QM
SC-19	大雾低能见度高速制动	高速公路大雾天气能见度极低，驾驶员识别前方静止车辆延迟，紧急制动	S3	大雾高速追尾，致命风险极高	E1	大雾高速行驶频率较低，季节性	C1	能见度极低，发现危险到规避时间极短	QM
SC-20	冰雪路面低附着 ABS 高频介入	冰雪路面低附着，驾驶员中度制动，ABS 高频调压防止车轮锁死	S0	冰雪路面低速碰撞，轻微伤害	E1	冰雪路面季节性，频率较低	C0	多数驾驶员可通过常规滑行/控车应对	QM
SC-21	逆光行驶识别延迟紧急制动	逆光环境驾驶员识别前方行人横穿延迟，踏板从轻踩迅速切换为紧急制动	S2	碰撞行人风险，可能导致重伤致死	E2	逆光行驶较常见，早晚高峰每日均有	C3	视线受阻，几乎无接管和规避时间	A
SC-22	急弯湿滑路面 ESC 介入制动	急弯路段遇雨天湿滑路面，驾驶员制动叠加转弯，ESC 检测侧滑趋势并介入	S1	弯道侧滑碰撞，轻微伤害	E1	急弯湿滑同时发生频率较低	C0	常规极限路况，多数人可通过控车应对	QM
SC-23	制动系统降级运行中	主控制器部分故障，系统切换至降级模式，驾驶员在城市道	S0	降级后制动距离延长，	E0	系统降级为偶发故障状态，频	C2	需驾驶员明显加大踏板力进	QM

场景编号	场景名称	场景描述	S	S 定级依据	E	E 定级依据	C	C 定级依据	ASIL
	制动	路中度踩制动		轻微伤害		率较低		行人工补偿	
SC-24	冗余切换过程中驾驶员制动	主控故障触发冗余切换期间，驾驶员遭遇前车紧急制动，踩紧急制动踏板	S3	高速瞬间失去制动，致命风险极高	E0	冗余切换与前车紧急制动同时发生，概率极低	C3	突发瞬时失效，驾驶员完全无法应对	QM
SC-25	CAN 通信中断后制动请求	CAN/CANFD 总线通信中断，制动域无法接收整车指令，驾驶员踩制动踏板	S2	通信中断无制动，严重碰撞风险	E0	CAN 总线完全中断为极低概率故障	C2	突发系统故障，驾驶员规避难度大	QM
SC-26	轮速传感器失效后湿滑路制动	轮速传感器失效导致 ABS/EBD 功能丧失，驾驶员在低附着路面制动	S0	湿滑失控碰撞，轻微伤害	E0	传感器失效叠加湿滑路面为较低频组合	C2	丧失防抱死，驾驶员控车难度高	QM
SC-27	供电电压异常下低速制动	车辆供电电压异常跌落，制动执行器性能下降，驾驶员低速前踩制动	S0	低速故障碰撞，轻伤或无	E1	供电异常为偶发故障	C1	低速状态下，可通过转向或加大力规避	QM
SC-28	单侧执行器失效后高速紧急制动	单侧 EMB/EHB 执行器失效（如断线或驱动故障），驾驶员高速遭遇前车紧急制动	S3	高速单侧制动跑偏，致命碰撞风险高	E0	单侧执行器失效叠加高速紧急制动为低频事件	C3	跑偏窗口极短，驾驶员极难修正控制	QM

参考文献

- [1] ROBERT BOSCH GMBH. Bosch Automotive Handbook[M]. 10th ed. Hoboken: Wiley, 2018.
 - [2] Euro NCAP. AEB Car-to-Car Test Protocol[S]. Leuven: Euro NCAP, 2023.
 - [3] UNECE. UN Regulation No.152 Advanced Emergency Braking Systems[S]. Geneva: UNECE, 2020.
 - [4] NHTSA. Federal Motor Vehicle Safety Standards: Automatic Emergency Braking Systems Final Rule[S]. Washington DC: NHTSA, 2024.
 - [5] IEC. IEC 60812:2018 Failure Modes and Effects Analysis (FMEA and FMECA)[S]. Geneva: IEC, 2018.
 - [6] SAE International. Considerations for ISO 26262 ASIL Hazard Classification (道路车辆危害事件风险评估建议实践): SAE J2980:2023[S]. Warrendale: SAE International, 2023.
 - [7] KRAMPE D, JUNGE M. Deriving functional safety (ISO 26262) S-parameters for vulnerable road users from national crash data. Accident Analysis and Prevention, 2020, 150: 105884.
 - [8] ASSOCIATION FOR THE ADVANCEMENT OF AUTOMOTIVE MEDICINE. AIS 2015 Abbreviated Injury Scale[M]. Barrington: AAAM, 2015.
 - [9] ROSÉN E, STIGSON H, Sander U. Literature review of pedestrian fatality risk as a function of car impact speed[J]. Accident Analysis and Prevention, 2011, 43(1): 25-33.
 - [10] UNECE. UN Regulation No.13-H Uniform provisions concerning the approval of passenger cars with regard to braking[S]. Geneva: UNECE, 2023.
 - [11] GILLESPIE T D. Fundamentals of Vehicle Dynamics[M]. Warrendale: SAE International, 1992.
 - [12] RAJAMANI R. Vehicle Dynamics and Control[M]. 2nd ed. New York: Springer, 2012.
 - [13] TANELLI M, SAVARESI S M. Active Braking Control Systems Design for Vehicles[M]. London: Springer, 2010.
 - [14] Verband der Automobilindustrie. Scenario Catalog for the Assessment of Exposure (暴露率评估场景目录): VDA 702[S]. Berlin: VDA, 2023.
 - [15] GREEN M. How long does it take to stop? Methodological analysis of driver perception-brake times[J]. Transportation Human Factors, 2000, 2(3): 195-216.
-