



中华人民共和国国家标准化指导性技术文件

GB/Z 265—2026

“人工智能+交通运输”应用安全指引

Application security guidelines for“ artificial intelligence+transportation”

2026-08-27 发布

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 III

1 范围1

2 规范性引用文件1

3 术语和定义1

4 总则2

5 生命周期安全要素3

6 应用场景安全风险防范11

附录 A(规范性) 交通运输人工智能应用常见安全风险防范12

附录 B(资料性) 交通运输典型应用场景突出安全风险防范示例15

参考文献25

前 言

本文件为规范类指导性技术文件。

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。

本文件由交通运输部和中國民用航空局提出。

本文件由全國智能運輸系統標準化技術委員會(SAC/TC 268)和全國網絡安全標準化技術委員會(SAC/TC 260)共同歸口。

本文件起草單位：中國交通通信信息中心、交通運輸部公路科學研究所、中國電子技術標準化研究院、交通運輸信息安全中心有限公司、中國交通信息科技集團有限公司、青島港國際股份有限公司、中國遠洋海運集團有限公司、中國南方航空集團有限公司、上海機場(集團)有限公司、中國民航信息网络股份有限公司、中國民航大學、華為技術有限公司、交通運輸部規劃研究院。

本文件主要起草人：杜漸、戴明、陳朴、齊志峰、羅慶勇、何峰、吳宇震、王楹、李飛、吳勇、李金良、耿慶仁、王力、許智宇、張碩、夏威、郝春亮、劉長輝、馮森、張妍婷、陳振東、霍曉宇、孫碩、賀林佳、黃偉鍵、張卓劍、常鑫宇、曾佩佩。

“人工智能+交通运输”应用安全指引

1 范围

本文件给出了交通运输人工智能应用安全的总则和生命周期安全要素,提供了交通运输人工智能典型应用场景安全风险防范的指导和建议。

本文件适用于交通运输人工智能全生命周期的应用安全工作。

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 20839 智能运输系统 通用术语
- GB/T 25069 信息安全技术 术语
- GB/T 41867 信息技术 人工智能 术语
- GB 45438 网络安全技术 人工智能生成合成内容标识方法

3 术语和定义

GB/T 20839、GB/T 25069 和 GB/T 41867 界定的以及下列术语和定义适用于本文件。

3.1

交通运输人工智能应用 transportation artificial intelligence application

人工智能在公路、水路、铁路、民航、邮政、城市客运、综合交通运输等交通运输领域,以及政务服务、业务服务、安全监管等场景中的应用,以实现检索增强、感知认知、推理决策、任务调度等方面的预期结果。

注:包括交通运输基础大模型、交通运输垂直领域大模型、智能体等人工智能应用形式。

3.2

交通运输基础大模型 transportation foundation large scale model

在通用大模型的基础上,基于交通运输行业通识高质量数据集和语料库进行训练的大模型。

注:高质量数据集是经过采集、分析、标注、转换、过滤、标准化、去标识化、质量检查、采样、增强、标记等数据处理,能直接用于开发和训练人工智能模型,有效提升模型性能的数据集合。

3.3

交通运输垂直领域大模型 transportation specific large scale model

在交通运输基础大模型的基础上,基于交通运输领域专识高质量数据集进行训练的大模型。

3.4

智能体 artificial intelligence agent

能够自主感知环境、制定决策、采取行动实现特定目标的智能系统。

注:一般具有记忆、规划、使用工具等基本能力。