ICS 93.080.10
CCS R80/90

团 体 标 准

T/ITS 00**-20**

自主式交通系统协同感知信息安全技术要求

Technical Requirements for Information Security in Cooperative Perception of Autonomous Transportation Systems

20**-**-**发布 20**-**-**实施

中国智能交通产业联盟 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。

本文件由中国智能交通产业联盟（C-ITS）提出并归口。

本文件起草单位：东南大学、交通运输部公路科学研究院、南京莱斯网信技术研究院有限公司、南京莱斯信息技术股份有限公司、北京航空航天大学、东软集团股份有限公司、苏州智加科技有限公司、中南大学、武汉理工大学、联通智网科技股份有限公司、兴唐通信科技有限公司、中国信息通信科技集团有限公司、北京万集科技股份有限公司。

本文件主要起草人：付华、高春宵、李大韦、陈峻、胡爱群、谌仪、齐志峰、贲伟、丁维昊、王朋成、王琦、曹莹琦、刘东润、刘文、巩金亮、吕晓晨、杨天、房家奕、徐智凯、马晓彤。

自主式交通系统协同感知信息安全技术要求

1 范围

本文件规定了自主式交通系统中协同感知信息系统的数据安全、通信安全、样本安全、模型安全、异常行为合理性检测以及运行维护与测试验证要求。

本文件适用于车辆、路侧单元、边缘节点、平台节点，以及参与协同感知信息采集、处理、融合、推理、传输、存储和发布的相关系统的设计、开发、部署、测试和运营。

本文件不替代现有网络安全、密码应用、个人信息保护、功能安全和通信协议等方面的标准。与其他标准配套使用时，应结合业务风险评估结果统筹实施。

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。

YD/T 3750-2020 车联网无线通信安全技术指南

YD/T 3751-2020 车联网信息服务数据安全技术要求

YD/T 3978-2021 基于车路协同的高等级自动驾驶数据交互内容

YD/T 4774-2024 车辆C-V2X异常行为管理技术要求

ETSI TS 103 324 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Collective Perception Service

ETSI TS 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats

ISO/SAE 21434:2021 Road vehicles-Cybersecurity engineering

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

自主式交通系统 autonomous transportation system

自主式交通系统是以自感知、自适应、自学习、自组织为特征的高度自治的交通系统。

3.1.2

协同感知 collaborative perception

通过交通主体之间的数据共享机制，实现超视距范围内交通环境信息的感知融合，提升自主式交通系统的感知准确性、鲁棒性与安全性。

3.2 缩略语

下列缩略语适用于本文件。

CPM：协同感知消息（Cooperative Perception Message）

CPS：协同感知业务（Cooperative Perception Service）

C-V2X：蜂窝车联网通信（Cellular Vehicle to Everything）

ITS-S：智能交通站点（Intelligent Transport System Station）

OBU：车载单元（On-Board Unit）

RSU：路侧单元（Road-Side Unit）

PKI：公钥基础设施（Public Key Infrastructure）

TEE：可信执行环境（Trusted Execution Environment）

4 协同感知安全总体架构

协同感知安全总体架构宜围绕“感知采集、消息生成、消息传输、融合处理、模型训练与更新、模型推理输出、异常处置与闭环管理”七个环节进行设计。

协同感知系统的安全对象至少包括数据、样本、模型、消息、证书与密钥、算力与运行环境以及日志审计。

协同感知系统面临的主要安全威胁包括但不限于：伪造或重放感知消息、样本篡改、坐标或时间同步欺骗、异常行为注入、训练数据投毒、后门触发、模型窃取、参数篡改、拒绝服务和日志擦除。

协同感知安全防护应形成“身份可信、数据可验、样本可检、模型可控、行为可判、事件可追、风险可处置”的闭环机制。

表1 不同感知环节的典型风险和控制重点

感知环节	主要对象	典型风险	控制重点
数据采集	原始传感器数据	伪造采样、传感器故障、时间漂移	采样完整性、源可信、时间同步
消息生成	CPM/感知结果	目标伪造、字段异常、坐标欺骗	格式校验、合理性约束、签名保护
消息传输	广播或单播链路	重放、篡改、伪装、窃听	认证、完整性、防重放、加密
融合处理	多源输入与融合结果	对抗样本、异常节点放大	多源一致性、置信度评估、隔离降权
训练与更新	数据集、标签、模型包	投毒、后门、版本回退	溯源、审计、完整性校验
推理与发布	在线模型和接口	模型窃取、参数篡改、输出操纵	访问控制、查询监测、TEE/签名

5 总体安全要求

协同感知信息系统应结合业务场景、运行区域、接入主体数量、自动驾驶等级和网络暴露面开展信息安全风险评估，并形成分级防护策略。

系统应建立覆盖设计、开发、测试、部署、运营、更新和退役等全生命周期的安全管理机制，安全过程宜与功能安全、预期功能安全和质量管理过程协同实施。

系统应对参与协同感知的主体建立可信身份与权限体系，明确车端、路侧端、平台端和运维端的最小权限边界。

涉及安全关键业务的时间、位置、目标轨迹、目标类别、置信度和传感器健康状态等字段，应具备来源可验证、内容可校验和处理可追踪的能力。

系统应支持安全事件告警、日志留存、追溯分析和策略联动处置；日志至少应覆盖消息接收、校验结果、模型版本、检测告警、处置动作和恢复结果。

当任一安全机制失效时，系统应支持降级运行，例如降低协同感知权重、隔离可疑节点、限制模型接口输出粒度，或切换为本地感知优先策略。

6 样本安全要求

6.1 通用要求

系统应针对数据级样本、特征级样本和决策级样本分别建立检测策略，并支持分层记录检测结果和处置结果。

样本安全检测应兼顾实时性和准确性；用于在线推理的检测机制不应给安全关键业务带来不可接受的时延累积。

样本安全检测输出至少应包括样本标识、检测时间、检测类型、风险等级、定位结果、处置动作和关联节点信息。

6.2 数据级和特征级样本要求

系统应对原始数据和中间特征开展统计特征检测，检测内容宜包括频谱分布、像素或点云数值分布、稀疏度、熵值、通道相关性以及历史偏离度。

系统应通过压缩、去噪、随机平滑、输入重采样或多视角重投影等预处理一致性方法识别潜在对抗扰动。

系统应对模型中间层激活值、特征图分布和输出置信度进行异常监测，识别与正常样本显著偏离的异常输入。

对于来自外部主体的特征级样本，系统应校验特征维度、坐标系、时间戳、版本号和生成模型标识的一致性，防止格式兼容攻击和跨版本注入。

6.3 决策级样本要求

系统应对目标位置、速度、航向角、尺寸、类别、置信度和轨迹连续性进行合理性检查。

决策级样本应结合高精地图、车道约束、道路拓扑、交通规则和静态设施信息进行场景一致性校验。

当多个感知主体上报同一目标时，系统应开展跨主体一致性评估，并结合时间差、空间差和类别差确定融合权重。

对判定为高风险的决策级样本，系统应至少支持丢弃、隔离、降权和请求复核等处置动作。

7 异常行为合理性检测要求

7.1 车辆异常行为检测

车辆节点发送的消息在通过安全协议校验后，系统仍应对其内容开展合理性检测，避免利用合法证书发送误导性数据。

车辆异常行为检测应至少覆盖消息频率异常、轨迹跳变、超物理约束速度或加速度、重复目标异常、相邻时刻目标消失/出现异常和地图不一致异常。

当车载传感器出现失准、遮挡、失焦、标定漂移或故障告警时，车辆节点应下调共享信息的可信等级，必要时停止外发高风险感知结果。

7.2 路侧系统异常行为检测

路侧节点应建立与安装位置、视场范围、道路设施和目标覆盖区域相匹配的合理性规则。

针对路侧节点发送的消息，系统应检查固定设施坐标、检测覆盖范围、目标生成位置、上报方向和时间同步状态是否满足部署基线。

路侧节点的异常行为检测应结合设备健康状态、边缘计算负载、传感器联动关系和历史稳定性进行综合判断。

7.3 异常行为处置

系统应建立异常行为分级规则，并与证书吊销、消息隔离、节点降权、运维告警和人工复核流程联动。

对持续发生或跨区域传播的异常行为，系统应具备生成异常行为报告并向上级管理实体或安全管理平台上报的能力。

8 数据安全要求

8.1 数据采集与标注安全

训练、验证和测试数据集应建立来源登记、采集时间、采集地点、设备标识、标注责任人和版本信息等溯源记录。

标注数据应采用双人复核、规则抽检或自动一致性校验等方式控制标签质量；涉及高风险类别时宜增加专家复核环节。

用于模型训练的外部数据集在接入前应完成格式校验、恶意文件扫描、内容合理性评估和授权合规审查。

8.2 数据投毒检测要求

系统应通过样本分布检测识别与基线数据明显偏离的数据簇，检测维度宜包括空间位置分布、类别比例、天气时段覆盖和传感器统计特性。

系统应通过特征空间聚类分析识别异常密集样本、离群样本和与标签不一致样本。

系统应开展标签一致性检测，识别同一对象在不同视角、不同节点或不同时间窗口下标签冲突的情况。

发现疑似投毒数据后，系统应支持样本隔离、训练集回滚、增量重训、影响范围评估和审计留痕。

8.3 后门攻击检测要求

系统应具备触发器反演或等效分析能力，用于识别模型对局部图案、特定区域、特定频域特征或组合条件的异常敏感反应。

系统应通过特征空间异常分析、类别激活响应分析和推理行为对比分析识别潜在后门行为。

模型上线前应开展后门检测；模型更新、迁移学习或持续学习后，宜重新开展检测。

8.4 数据存储与共享安全

数据集、标注文件和训练配置文件应按照敏感程度实施分级存储和访问控制。

共享数据应采用脱敏、最小化和授权控制原则；涉及可识别个人或车辆的信息时，应符合相关法律法规和行业规定。

关键数据应具备完整性校验、备份恢复和版本回滚能力。

9 通信安全要求

9.1 基本要求

协同感知消息的安全防护应覆盖身份认证、完整性保护、防重放、防伪造、密钥管理、证书管理和异常行为处置支撑等方面。

系统采用广播方式发送协同感知消息时，应保证接收方能够验证消息来源和完整性；采用单播或管理通道时，宜进一步提供保密性保护。

通信安全机制应与现有C-V2X或ITS消息安全框架兼容，不应破坏业务字段语义和时延约束。

9.2 消息保护要求

协同感知消息应携带可验证的安全头、签名或等效的完整性保护信息，并包含时间戳、消息类型标识、发送方标识或可追溯凭据。

接收方应校验消息格式、消息长度、签名有效性、证书有效期、证书状态和生成时间窗口，对超时消息或重复消息应予以丢弃或隔离。

当消息安全校验成功但业务合理性校验失败时，系统不应直接信任该消息，应转入异常行为检测与处置流程。

9.3 密钥与证书管理要求

系统应建立证书申请、签发、更新、吊销、黑名单同步和失效处置机制。

私钥应采用安全硬件、可信执行环境或等效安全措施进行保护，不应以明文形式长期存储在普通文件系统中。

证书与密钥更新过程应具备完整性校验和防回退能力。

9.4 抗攻击要求

系统应具备重放攻击检测能力，宜结合消息序列号、时间戳、短期缓存和空间约束进行综合判断。

系统应对异常高频查询、异常消息风暴、跨区域重复广播和资源消耗型攻击进行限流、隔离或优先级调整。

管理接口和模型分发通道应采用双向认证和加密传输。

10 模型安全要求

10.1 模型资产管理

系统应建立模型台账，记录模型名称、功能用途、训练数据版本、参数摘要、依赖环境、发布责任人、发布时间和适用场景。

模型文件、推理配置文件、算子库和依赖组件应作为统一的模型资产进行保护，并建立相应的版本控制和发布审批机制。

10.2 模型窃取预防要求

模型接口应实施身份鉴别、访问控制、调用频率限制和异常查询行为监测。

对外暴露的推理结果宜遵循最小必要输出原则，避免过多暴露中间特征、精细置信度分布或可用于重建模型的信息。

系统宜通过查询指纹分析、诱骗样本检测、水印或指纹标识等手段识别模型窃取风险。

10.3 参数篡改防护要求

模型参数在存储、传输和加载过程中应进行完整性校验，校验方式宜采用数字签名、摘要比对或可信度量。

模型文件应支持加密存储，关键模型宜在可信执行环境或等效可信硬件环境中加载和运行。

系统应监测模型输出分布和关键性能指标的突变情况，识别参数被篡改或依赖环境被异常替换的风险。

10.4 模型更新与恢复要求

模型上线前应完成安全评估、基线性能评估和兼容性评估。

模型更新应支持灰度发布、回滚恢复和异常告警；发现模型异常后，应能够快速切换至可信版本。

采用在线学习、持续学习或联邦学习等机制时，应增加更新源身份校验、聚合前样本筛查和模型差异审计措施。

11 运行维护与测试验证要求

11.1 运行维护要求

运营单位应建立覆盖车端、路侧端、边缘端和平台端的统一安全监测机制，并定期评估样本安全、数据安全、通信安全和模型安全状况。

系统应支持安全策略远程更新，并在更新失败或状态异常时提供回退机制。

应定期开展攻击模拟、漏洞排查、证书状态核验、数据集抽检和模型安全复测。

11.2 测试验证要求

测试验证应覆盖功能正确性、检测效果、性能影响、处置闭环和恢复能力等内容。

样本安全测试至少应覆盖常见对抗扰动、伪造特征注入、决策级异常构造和多节点冲突信息注入场景。

数据安全测试至少应覆盖投毒样本注入、标签篡改、后门触发器注入、数据集版本回退和备份恢复场景。

通信安全测试至少应覆盖签名验证、证书失效、消息重放、字段篡改、时钟偏移和拒绝服务场景。

模型安全测试至少应覆盖未授权访问、批量查询、模型文件篡改、依赖库替换、更新包回退和异常输出监测场景。

T/ITS XXXX- XXXX

中国智能交通产业联盟
标准

自主式交通系统协同感知信息安全技术要求

T/ITS XXXX-XXXX

北京市海淀区西土城路 8 号（100088）
中国智能交通产业联盟印刷
网址：http://www.c-its.org.cn

20XX 年 X 月第一版　20XX 年 X 月第一次印刷