ICS 03.220.20
CCS R85

团 体 标 准

T/ITS XXXX-**

自主式交通系统 信息安全分级规范

Autonomous transportation system—
Information security classification specification

（征求意见稿）

本稿完成日期：2026 年 4 月 3 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。

中国智能交通产业联盟

20**-**-**发布 20**-**-**实施

中国智能交通产业联盟 发布

中国智能交通产业联盟

目　　次

中国智能交通产业联盟

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：北京邮电大学、交通运输部公路科学研究院、北京奇虎科技有限公司、同济大学、北京航空航天大学、联通智网科技股份有限公司、北京万集科技股份有限公司。

本标准主要起草人：袁开国、李灵慧、杨皓博、袁泉、丁川、赵慧敏、李响、黄爱玲、张永生、奇格奇、蒋永雷、周光涛、辛亮、于朝阳、杨广宇、孙剑、唐克双、朱宏、由林麟、沈峰、李强、吉静。

中国智能交通产业联盟

自主式交通系统 信息安全分级规范

1 范围

本文件规定了基于风险评估的自主式交通信息安全等级划分规则和分级方法，提出了等级划分模型和分级要素，包括自主式交通系统资产的重要程度、潜在风险影响程度以及需抵御的信息安全威胁程度，并提出了自主式交通信息安全四个等级的特征。

本文件适用于自主式交通系统的建设、运营单位以及相关行业监管部门，为自主式交通信息安全等级的划分提供指导，并为自主式交通系统信息安全的规划、设计、运行维护、评估与管理提供依据。

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 22080-2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 31722-2015 信息技术 安全技术 信息安全风险管理

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

生产安全事故报告和调查处理条例 国务院第493号令

突发环境事件信息报告办法 环境保护部令第17号

3 术语、定义和缩略语

3.1 术语和定义

GB/T 22080-2016界定的以及下列术语和定义适用于本文件。

3.1.1

英文名称信息安全风险 information security risk

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

注:它以事态的可能性及其后果的组合来度量。

[GB/T 31722-2015,定义3.2]

3.1.2

影响 impact

中国智能交通产业联盟

事件的后果,对已达到的业务目标水平的不利改变。在信息安全中,一般指不测事件的后果。

[GB/T 31722-2015,定义3.1]

3.1.3

威胁 threat

可能导致对系统或组织的损害的不期望事件发生的潜在原因。

[GB/T29246-2012,定义2.45]

3.1.4

安全属性 security attribute

主体、用户(包括外部的IT产品)、客体、信息、会话和/或资源的某些特性,这些特性用于定义安全。

3.2 缩略语

下列缩略语适用于本文件

ATS：自主式交通系统（autonomous transportation systems）

AV：自动驾驶车辆（Autonomous Vehicle）

ITS：智能交通系统（Intelligent Transportation System）

V2X：车联网通信(Vehicle-to-Everything)

ECU：电子控制单元（Electronic Control Unit）

ADV：对抗样本（Adversarial Example）

BAP：感知模型后门攻击（Backdoor Attack on Perception）

MPA：模型投毒攻击（Model Poisoning Attack）

DPA：数据投毒攻击（Data Poisoning Attack）

MSA：模型萃取攻击（Model Stealing Attack）

PIA：提示注入攻击（Prompt Injection Attack）

Trojan：通用后门攻击（Trojan Attack）

AUC：曲线下面积（Area Under Curve）

TPR：真正率（True Positive Rate）

FPR：假正率（False Positive Rate）

MAD：模型归因距离（Model Attribution Distance）

RTA：实时审计机制（Real-Time Audit）

SDR：安全部署准备度（Safe Deployment Readiness）

LLM：大语言模型（Large Language Model）

中国智能交通产业联盟

PFD：提示过滤与防御（Prompt Filtering and Defense）

PGD：投影梯度下降（Projected Gradient Descent）

RLHF：人类反馈强化学习（Reinforcement Learning with Human Feedback）

SAR：安全保障率（Security Assurance Rate）

OTA：远程更新（Over the Air Update）

RSU：路侧单元（Road Side Unit）

CAN：控制器局域网总线（Controller Area Network）

V2I：车与基础设施通信（Vehicle-to-Infrastructure）

V2V：车与车通信（Vehicle-to-Vehicle）

IMU：惯性测量单元（Inertial Measurement Unit）

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

DoS：拒绝服务攻击（Denial of Service）

VPN：虚拟专用网络（Virtual Private Network）

CRC：循环冗余校验（Cyclic Redundancy Check）

API：应用程序编程接口（Application Programming Interface）

APT：高级持续性威胁（Advanced Persistent Threat）

IDS：入侵检测系统（Intrusion Detection System）

IPS：入侵防御系统（Intrusion Prevention System）

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

TPM：可信平台模块（Trusted Platform Module）

PKI：公钥基础设施（Public Key Infrastructure）

DSRC：专用短程通信（Dedicated Short-Range Communications）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

4 自主式交通系统概论

4.1 自主式交通系统基本构成

中国智能交通产业联盟

自主式交通系统是一个典型的、具有复杂结构和功能的新一代交通运输系统群，其融合了多个领域的相关技术。自主式交通系统是在交通运输系统与智能、驱动技术（人工智能、网络，计算、数据、材料能源）和系统学科（心理、认知、行为）深度融合的基础上构建和发展的。自主式交通的设计初衷是以高安全性、高质量和高效率完成交通运输活动。自主式交通系统的每个组成部分具有自感知，自决策，自重构和和谐操作的能力，系统整体具有高度智能化、高度适应性、高度开放性、高度鲁棒性的特征。

从系统工程的角度出发，自主式交通系统可以按照如下进行定义：

（1）自主式交通系统组成

自主式交通系统通常由载具（车）、路（道路与路侧系统）、云（云端系统）以及外部环境共同构成。为进行更细粒度的信息安全分级与防护要求的识别，自主式交通系统组成应从物理实体维度和功能模块维度进行规范描述：

自主式交通系统在物理实体维度上主要包括下列三类实体：1.载具：载具是参与交通活动的相对完整的载体，其包括了车辆本身（如车身、动力系统、转向与制动系统等）以及为实现自主交通和车联网功能而配置的车载系统。车载系统通常包括车载传感器与采集设备、车载电子控制单元（ECU）或域控制器、执行机构驱动单元、车载网络与通信单元、人机交互终端等，是完成环境感知、自身状态评估、局部决策与车辆机动控制的直接执行主体。2.路：路是承载交通活动的道路及其附属设施，以及部署于其上的路侧系统。路侧系统通常包括路侧感知设备（如视频监控、毫米波雷达、激光雷达、地磁线圈等）、路侧控制器（如交通信号控制机、道闸控制器等）、路侧单元（RSU）、边缘计算与通信节点等，用于感知道路运行状态、实施交通协同管控，并为车提供辅助决策信息和安全约束。3.云：云是部署于数据中心或云平台的系统集合，通常包括数据采集与存储平台、运行监测与安全审计平台、全局调度与优化决策系统、远程运维与软件/模型在线更新平台等，用于实现跨区域数据融合分析、全局策略生成以及统一运维管理，是车-路协同运行的核心支撑。

自主式交通系统在功能维度模块上，可以根据车、路、云内部普遍包含的功能进行规范描述：1.感知与传感器模块：包括部署于车和路的各类传感器及环境/状态采集设备，用于获取车辆运行状态、道路与交通参与者状态、环境与基础设施状态等信息，是系统获取外部和自身信息的基础。2.网络与通信模块：包括车载总线、车载以太网、工业以太网、V2X 通信设备、蜂窝移动通信网络、专用通信网络及相关网关设备等，用于实现车、路、云之间以及各内部组件之间的数据传输与协议转换，是系统联接与协同的基础。3.智能模型模块：包括部署在车、路、云上的各类人工智能模型、规则引擎及其支撑软件，用于完成环境理解、自身状态评估、风险预测、路径规划和行为决策等，是自主式交通系统智能行为与自主能力的核心。4.控制器与执行模块：包括车载电子控制单元（ECU）、域控制器、路侧控制器、执

中国智能交通产业联盟

行机构驱动单元等，用于将决策结果转化为制动、转向、加减速、信号灯控制、道闸控制等具体物理动作，是保障交通活动安全、有序运行的关键环节。在具体工程实现中，以上功能模块可以按域控制、平台化、虚拟化等方式进行集成，或部署于同一物理设备。其信息安全分级与防护要求应结合其在车、路、云整体架构中的角色、处理数据的重要性以及受攻击后对系统安全的影响进行综合分析。

（2）自主式交通系统控制过程

自主式交通系统的运行可抽象为由感知–传输–决策–控制闭环支撑的自动控制过程，并辅以人机交互机制和远程管理支持工具。在具有自主运行能力的场景下，车、路、云及其内部的多个模块协同工作，构成系统的主要控制主体，同时保留必要的人为监控与干预接口。在感知阶段，部署于载具和路侧的各类传感器获取车辆状态、道路与交通参与者状态及环境信息，形成对交通场景的基础描述；在传输阶段，车载总线、V2X、蜂窝通信等网络与通信模块在车、路、云之间及其内部可靠传递感知数据和运行状态；在决策阶段，部署在车、路、云上的智能模型对多源数据进行融合分析与风险评估，生成路径规划、行为选择和协同控制策略；在控制阶段，车载 ECU、域控制器、路侧控制器及执行机构驱动单元据此对车辆和基础设施实施制动、转向、加减速、信号控制等动作，闭合控制回路。同时，车载人机交互终端为驾驶员或值守人员提供状态监视和必要接管能力，云端运维与 OTA 平台实现运行监测、故障诊断与软件/模型更新，从而保障系统的安全、稳定和可持续运行。

整个控制过程依赖多模块信息流实时协同，易受数据篡改、通信中断或决策劫持，识别对抗与投毒攻击等信息安全威胁影响。

（3）自主式交通系统结构层次

由于部署场景、技术路径或业务定位不同，不同自主式交通系统的架构存在差异。但总体上，可在车–路–云一体化架构基础上，将完整的自主式交通系统按功能与技术栈纵向划分为若干层次，例如：第1层：物理与设备层（载具本体、路侧感知与控制设备、云端计算与存储基础设施等）；第2层：网络与通信层（车载总线、车路协同 V2X、蜂窝及专用通信网络等）；第3层：基础软件与操作系统层（车载、路侧与云端操作系统、虚拟化与中间件平台等）；第4层：业务与应用层（感知处理、协同控制、调度管理、人机交互与远程运维等应用服务）；第5层：数据层（运行数据、日志与审计数据、模型训练与更新所需的数据资源等）；第6层：智能与决策层（部署在车、路、云上的智能模型、决策引擎和策略管理模块等）。其中，物理与设备层、网络与通信层和基础软件与操作系统层为支撑感知–传输–决策–控制闭环安全可靠运行的基础系统构成部分，构成信息安全防护的核心范围。实际工程中，物理上相邻层可能由同一设备或平台承载，并不影响依据上述层次划分合理识别安全边界并部署差异化安全防护措施。

中国智能交通产业联盟

（4）自主式交通系统分级对象

自主式交通系统的信息安全分级对象应为在特定区域或场景内部署运行的完整自主式交通系统工程。分级时，应在 4.1（1）～4.1（3）所确定的组成、控制过程、结构层次和安全区域基础上，从系统工程视角对车、路、云各实体及其内部功能模块进行整体识别与分析。完整自主式交通系统分级对象一般包括：以载具（车）为核心的车载系统及其感知与传感器模块、网络与通信模块、智能模型模块和控制器与执行模块；以道路及路侧系统为核心的各类路侧感知与控制设备、通信与边缘计算节点；以及以云端系统为核心的运行监测、数据存储与分析、全局调度与优化决策、远程运维与软件/模型在线更新等平台及其支撑设施。同时，应将支撑感知–传输–决策–控制闭环运行的人机交互机制和远程管理支持工具纳入同一分级对象范围，并结合物理层、网络层、操作系统层、应用层、数据层和智能层等结构层次以及各安全区域和跨域通信通道，对系统在机密性、完整性、可用性等方面的重要性和面临的威胁进行综合评估，确定该完整自主式交通系统的统一信息安全等级。

4.2 自主式交通系统自主水平划分

针对自主式交通系统的自主水平进行划分，应综合评估载具、路、云三类实体及其内部感知与传感器模块、网络与通信模块、智能模型模块、控制器与执行模块在“感知－传输－决策－控制”闭环中的自动化与智能化程度，以及人类在系统运行过程中的参与方式和职责边界。根据人类参与程度、载具、路、云协同能力、系统在感知、决策、控制各环节的自主完成度及其可稳定覆盖的运行设计域和场景复杂度，自主式交通系统可划分为四个自主水平等级：

（1）人工主导协同阶段（Level 0）——人在环中

系统不具备或仅具备极有限的自主能力，“感知–传输–决策–控制”闭环主要由人完成。载具、路、云侧的感知与传感器模块、网络与通信模块、智能模型模块和控制器与执行模块仅提供信息显示、风险告警和局部控制辅助，无法独立完成连续的自动控制；人需要在整个运行过程中持续参与并直接操作，对系统行为承担主要责任。

（2）条件自主协同阶段（Level 1）——人在环上

系统能够在限定或大部分预设场景下由载具、路、云侧协同闭合控制闭环，完成大部分感知、决策与控制操作。人从直接操控转为监视与兜底角色，无需持续执行具体操作，但需持续或按系统请求关注运行状态，并在系统能力边界被触及、出现复杂或异常情形时及时介入。该阶段综合了原“部分自主”和“请求介入”的特征，体现为具备一定自组织能力但仍依赖人工监督和接管。

（3）高自主协同阶段（Level 2）——人在环外

中国智能交通产业联盟

系统在预先限定的运行设计域内具备完全自主运行能力，载具、路、云侧可独立完成全流程感知、决策与控制，人不再直接参与具体操作，仅在策略配置和运行审计等层面保持宏观关注。路侧与云端具备对动态微观交通信息的自主感知和判断能力，可与载具形成高层次协同，实现系统级安全保障与效率优化。

（4）全域自主协同阶段（Level 3）——人离环

系统可在各类交通场景下实现完全自主运行，载具、路、云具备全域感知、全局决策与全程执行能力，在系统群体层面实现协同感知、协同决策与协同控制。运行过程中不再依赖人工参与控制环节，仅保留规划配置和监管等职能，该阶段代表自主式交通系统的最高自主水平与“完全自动化”运行模式。

根据实际部署形态和风险评估需求，可分别对完整的自主式交通系统及其局部子系统进行自主水平分级。通常情况下，局部子系统的自主水平不应高于其所属整体系统的自主水平。

5 自主式交通系统信息安全等级划分规划

5.1 自主式交通系统覆盖范围划分规则

本条规则用于定义自主式交通系统覆盖的场景。规则制定参考网络安全等级保护要求，对于自主交通的覆盖区域进行定义。通过明确交通系统的覆盖范围，结合自主式交通系统的自主水平，可以明确自主式交通系统应具备的安全水平。在自主式交通系统资产重要程度要素构成中，覆盖范围是指自主式交通系统在空间布局和服务对象上的地理与行政层级范围，反映系统在运行规模、影响半径及管理复杂度等方面的特征。该维度可分为全国级、省部级、地市级、区县级四个等级，具体划分条件如下：

全国级自主式交通系统：指在全国范围内统一规划、部署和运行的自主式交通系统，服务对象跨越多个省份或覆盖国家级交通主干网络，通常承担国家级交通调度、运行监测、应急指挥或战略支撑任务。示例：国家级智能高速网联平台、跨省区自主交通干线运输系统、全国多场景融合的车路云协同运行体系等。此类系统若遭受攻击或被破坏，可能直接影响国家关键交通枢纽的指挥调度与运行安全，造成跨区域甚至全国范围的交通瘫痪，严重危及国家安全、经济运行和社会秩序。攻击还可能导致战略性运行数据泄露或被篡改，影响国防保障、能源运输和应急物资调配等关键职能，后果极其严重。

省部级自主式交通系统：指在省、自治区、直辖市或部委管理范围内统一规划和运行的自主式交通系统，服务范围覆盖多个地市或重点交通枢纽节点，承担区域级交通调度、管理与协调任务。示例：省域高速自主交通管控系统、省级城市群智能公交网络等。此类系统受到攻击后，可能导致大范围区域交通运行中断或指挥失灵，引发重大经济损失和社会混乱，影响区域应急响应和跨市协同作业。若关键信息或调度数据被篡改，还可能导致运营失控或错误决策，造成重大安全事故和社会影响。

中国智能交通产业联盟

地市级自主式交通系统：指在地级市行政区域内部署和运行的自主式交通系统，主要服务于城市道路交通、公共运输、港口、机场或城市物流等场景。系统的运行与管理由市级交通主管部门或运营单位负责。示例：城市主干道智能信号控制系统、快速公交自动调度平台、城市级自主交通公交系统、城市物流协同配送网络等。若系统遭受攻击或出现安全故障，可能导致城市交通信号错乱、道路拥堵加剧、公交及地铁系统停运，进而影响居民日常出行、城市物流与应急服务，造成显著的经济损失与公共服务中断。信息泄露或恶意操控还可能引发市域范围的舆情风险与信任危机。

区县级自主式交通系统：指服务于特定区域、园区或区县范围内的自主式交通系统，通常覆盖范围有限，运行环境相对封闭或半封闭，系统功能以乡道，县道等少交通设施或无交通设施、局部交通运行、园区物流或末端运输为主。示例：产业园区自主交通接驳系统、封闭园区智能配送车系统、区县级公路等。此类系统受到攻击后，其影响范围相对有限，主要表现为局部运行中断、作业效率下降或数据泄露。虽然一般不会对社会整体秩序造成重大影响，但若系统被长期控制或数据被篡改，可能导致交通设备异常运行、局部事故风险增加，并在特定情况下影响区域公共安全与管理稳定。

本条规则用于定义自主式交通系统在空间范围和管理层级上的覆盖场景，是自主式交通系统安全分级的重要依据之一。规则的制定参考了《网络安全等级保护基本要求》等国家标准的分级原则，结合自主式交通系统的结构特点和运行模式，对其覆盖区域进行了分层定义。通过明确系统的地理覆盖范围与服务层级，并与系统自主水平相结合，可科学评估其在运行规模、信息交互复杂度以及安全风险暴露面的差异，进而确定系统应具备的相应安全防护等级和管理要求。

在自主式交通系统资产重要程度要素构成中，覆盖范围反映了系统在空间布局、服务对象及管理半径上的广度，是衡量系统安全影响范围和防护要求的重要维度。覆盖范围划分为全国级、省部级、地市级和区县级四个等级，分别对应不同的运行层级、服务范围及潜在安全影响程度。通过对覆盖范围的分级定义，可为后续的风险评估、等级确定及安全控制措施配置提供依据，确保自主式交通系统的安全防护能力与其运行规模、重要性和潜在影响相匹配。

5.2 自主式交通系统信息安全分级要素

5.2.1 概述

a）自主式交通系统的信息安全分级应基于两个核心要素：自主化水平等级与覆盖范围。

b）分级方法应采用二维矩阵判定法，以自主化水平为一要素轴，以覆盖范围为另一要素轴，综合确定建议安全等级。

c）本条款适用于完整系统及其相对独立部分的分级；当两者同时存在时，分级结果应保持一致性与可追溯性。

中国智能交通产业联盟

5.2.2 **要素一：自主化水平等级（见 4.2）**

a）自主化水平等级反映人机关系、系统智能能力及感知-传输-决策-控制闭环的自动化程度，取值应为L0～L3。

b）自主化水平越高，人工补救空间越小、误触发风险与级联风险越高；分级时应相应提高安全防护要求。

c）自主化水平的判定依据应包括功能说明、测试报告与运行验证材料；当自主化水平发生变更时，应重新开展分级评估。

5.2.3 **要素二：覆盖范围（见 5.1）**

a）覆盖范围反映系统在空间布局与服务对象上的地理及行政层级，取值应为区县级、地市级、省部级、全国级。

b）覆盖范围越广，影响半径与管理复杂度越高；分级时应相应提高可用性、完整性与保密性保障要求。

c）覆盖范围的判定依据应包括行政覆盖清单、联网规模、服务量级及运行组织边界等文档。

5.2.4 **自主式交通系统信息安全分级矩阵**

分级采用二维矩阵判定法进行：以自主化水平（L0～L3）为横轴、覆盖范围（区县/地市/省部/全国）为纵轴，生成建议安全等级对照表（见表5-1）。自主式交通系统安全分级标签取值范围为1～4，表格中用S1～S4表示。

矩阵计算得到的建议等级应作为分级基准；确有必要调整时，宜按照本节修正规则在同一坐标系内统一执行，并在结论中标明调整理由与条款编号。矩阵的选点、判定与（如有）调整过程应形成完整留痕，汇总为《分级结论单》和《分级依据清单》，内容包括矩阵坐标、建议等级、最终等级、引用条款、证据材料编号、评审人及日期等，以保证分级结论的可追溯与可审计；当自主化水平、覆盖范围或系统边界发生变更时，分级结果应按照同一矩阵与规则及时复评并更新。分级矩阵如下表所示：

表 1 自主式交通系统安全分级表

覆盖范围					
全国	S2	S3	S4	S4	
省部	S2	S3	S3	S4	
地市	S1	S2	S2	S3	
区县	S1	S1	S2	S3	
	L0	**L1**	**L2**	**L3**	**自主水平**
注：表格中标签代表当前自主水平的交通系统在覆盖范围内的安全标签分级					

根据本标准，安全分级S1～S4对应的受攻击后果说明如下：

中国智能交通产业联盟

S1级（一般保护）对象遭受攻击时，影响通常局限于局部范围，可能造成短时服务中断、少量数据泄露或被篡改，对个人或单一单位的合法权益产生不利影响，但对社会秩序影响有限且可在较短时间内恢复；

S2级（重要保护）对象一旦受攻击，可能导致城市或区域范围业务能力显著下降或阶段性中断，运行调度受扰并存在一定人员伤亡或较大财产损失风险，公共利益与社会秩序受到较大影响，但通过应急处置在规定时间内应能恢复主要功能；

S3级（关键保护）对象遭受攻击，可能对社会秩序和公共利益造成严重危害，甚至对国家安全产生不利影响，表现为跨区域系统瘫痪或长时间不可用、重大经济损失与群体性安全事件风险攀升，核心数据被破坏将引发系统性失效，恢复难度大、周期长，需省部级以上统筹处置；

S4级（战略保护）对象受攻击时，将严重危及国家安全或造成特别重大的社会影响，可能使国家级交通指挥与应急保障失灵，出现大范围、长时间瘫痪或失控，战略运行数据泄露或篡改会引发连锁风险并影响国防、能源与物资保障体系，通常需启动国家层面的应急响应与恢复。

修正规则与从严规则

a）就高不就低原则：当两要素分别指向不同建议等级时，分级结果应取较高者。

b）重大场景加权：涉及危化品运输、大客流集散、应急保障、战略通信等场景时，分级结果应上调至少一级。

c）互联耦合上浮：当系统与上级平台或外部网络形成强耦合、级联系统无法实现安全隔离时，分级结果宜上调一级

d）复核与回退：当通过技术隔离、冗余设计与组织措施经验证可显著降低系统性风险时，分级结果可在风险评估报告支持下回退一级，但不得低于矩阵给出的基准等级。

e）系统/子系统一致性：子系统分级通常不应高于其所依附整体系统的分级；如业务风险客观需要上调时，整体系统分级与控制要求应同步评估与调整。

证据与判断要求

a）分级所需证据应至少包括：系统边界与架构说明、自主化功能与安全能力清单、覆盖范围与服务对象清单、运行规模与依赖关系、历史事件与应急恢复能力评估等。

b）分级判据应与相关标准中的“影响后果、可用性、完整性与保密性”要求相匹配，并在分级结论单中逐项对应说明。

c）当关键参数（自主化水平、覆盖范围、运行组织边界）发生变化时，分级结论应触发复评。

5.2.5 分级结论与应用

中国智能交通产业联盟

分级结论应形成单一文件并完整载明：最终安全等级（S×）、采用的矩阵坐标（覆盖范围×自主化水平）、修正规则应用情况（上调/回调结论及条款编号与依据），以及对应的安全控制域与扩展要求集合。该结论应作为安全建设、运维管理、合规测评与持续改进的统一输入；当系统发生扩容、迁移、跨域互联或场景扩展等重大变更时，应依据同一矩阵与修正规则组织复核并同步更新结论及控制清单。分级结论的有效期与复评周期宜结合系统变更频度、重大事件发生率、业务重要性与外部合规要求综合确定，并在管理制度中明确，同时保留结论形成与复评过程的留痕材料以支持审计与追溯。

6　自主式交通系统信息安全分级评估模型

6.1　目的与适用范围

本节旨在明确自主式交通系统不同安全分级（S1～S4）对抗攻击能力测试的要求。测试通过多个预设攻击场景评估系统在遭受网络和物理攻击时的抗毁伤和持续运行能力，为系统分类分级提供依据，同时形成整改闭环。此类测试针对自主式交通系统的整体进行，涵盖载具，路，云等自主式交通系统内的各个参与单位。测试结果将作为系统当前安全等级复核的重要参考，并为后续的安全漏洞整改与复测提供数据支撑。本节内容参考了《中国智能交通协会自主式交通系统信息物理系统总体架构》等行业文档及智能网联汽车安全研究成果编写。

6.2　测试对象与边界

测试对象： 涵盖自主式交通系统中的关键组成部分，包括车端、路侧和云端的关键组件（如决策控制单元和AI模型、车载网络和ECU、路侧单元RSU及交通信号控制系统、云控平台等）。同时考虑外部环境因素（如GNSS信号、道路标志、物理场景）以及各部分之间的接口和交互，如车辆与车辆、车辆与路侧之间的通信，人机交互接口等。目的与适用范围

6.2.1　攻击内容

车端：着重模拟车载感知与决策控制系统受到的攻击。通过对摄像头、雷达、激光雷达等传感信号进行对抗性干扰或伪装，生成“对抗样本”欺骗感知系统，诱导其产生虚假环境语义（例如伪造障碍物或道路标志），从而使自主交通参与车辆做出错误决策。同时，在训练或更新模型阶段加入有毒数据或后门植入，可能使攻击者在特定输入下远程控制车辆行为。还包括对车载控制策略的劫持或注入恶意策略，以及破坏车端信任根和加密密钥（如篡改硬件安全模块或恶意提取私钥），以绕过认证和数据完整性保护。针对车载网络和电子控制单元，模拟对 CAN 总线、FlexRay、车载以太网等内部通信网络的入侵，例如利用 CAN 总线缺乏安全机制的特点实施篡改、消息重放和拒绝服务攻击；对车载 ECU 及其固件进行篡改、植入后门或恶意更新，甚至通过物理访问调试接口重新烧录固件，使车辆执行部件（如制

中国智能交通产业联盟

动器、转向器、油门执行器等）发生异常行为；在传感器总线（如 GPS 串口、IMU 接口）上实施伪报或回放攻击，使车辆获取错误的位置信息或运动状态。

路侧：重点考虑路侧基础设施的安全威胁。包括路侧单元（RSU）、交通信号控制器、路侧感知设备等被攻击者入侵，控制或篡改交通信号广播和道路状态发布；在 V2I/V2V 通信中实施伪造、重放和中间人攻击，例如利用 LTE-V2X 系统的开放性假冒合法终端发布虚假交通信息、重放正常消息或窃听敏感数据；通过物理或网络手段篡改路侧感知与控制逻辑，诱导大范围交通行为异常。

云端：主要关注云控平台、OTA 服务器及相关后台系统的安全威胁。包括利用服务器漏洞或不安全的 OTA 通道注入恶意升级包，造成系统植入后门；对调度与管控平台实施渗透，篡改全局调度策略或指令下发内容；通过供应链攻击破坏云端软件组件的完整性。同时需要关注账户管理和审计机制的绕过攻击，如攻击者通过权限提升或禁用审计日志来隐藏入侵行为，削弱云端对车路系统的统一安全管控能力。

环境与外部信号：涉及对车外环境因素及外部信号源的干扰。模拟 GNSS 信号被欺骗或干扰的场景，例如攻击者广播虚假卫星信号导致车辆定位错误；对地图和电子围栏数据实施篡改或攻击（如修改高精地图中的道路属性），使自主交通参与车辆在规划路径时产生偏差。针对物理道路设施的攻击，包括在真实交通标志、信号灯或标线上施加恶意贴纸、遮挡或伪装，使感知系统识别错误；以及设置物理诱饵（如伪造障碍物）或构造干扰场景，以迷惑自主交通系统感知。

车－路－云跨域级联：设计综合性的跨域攻击场景，实现从路侧或云端到通信链路再到车端控制单元和执行机构的连锁破坏。例如，先入侵交通信号控制系统或云控平台（路侧/云端域），再通过被污染的信息或指令广播影响车载感知与决策（通信域），进一步进入车辆控制单元，最终危害执行器，形成多级联动攻击，验证车－路－云一体化系统在复杂攻击链路下的承受能力与阻断能力。

6.2.2 攻击等级

攻击者等级按能力和资源划分，一般从低到高包括：

T1 基础对手： 使用公开的攻击工具，实施单点、短时的局部攻击，对系统造成有限影响且难以持久驻留；

T2 小型组织： 拥有一定定制开发能力和资源，可跨域实施协同攻击，进行中期潜伏并协调攻击手段；

T3 有组织团体： 掌握零日漏洞或供应链攻击资源，能在多个域内联合攻击，长期潜伏并造成数据破坏或大面积功能丧失；

T4 国家级/战略： 拥有全谱资源和多矢量攻击手段，可跨区域发动系统性瘫痪攻击，导致战略级后果并难以防范。

该分级方法参考了工业网络安全等相关标准中对攻击者能力的分类思路。每个安全等级对应的测试内容和深度应基于此等级属性进行设计，以验证系统的抗攻击能力。

6.3 测试分域与项目框架

6.3.1 分域测试对象与关键能力覆盖

车端安全：评估车辆侧感知与决策模块在对抗攻击下的鲁棒性，包括对抗样本与感知欺骗测试；检查车载 AI 模型与推理过程的安全性，防范模型篡改、后门攻击等威胁；验证车端密钥和敏感数据（如地图片段、车辆状态信息）在存储与计算过程中的保护措施；测试车端系统在感知功能损失或降级情况下的容错策略，确保车辆在部分能力受损时仍能保持安全行为。对车载网络与 ECU 进行安全测试，检查 CAN/FlexRay/以太网总线的消息过滤、访问控制与拒绝服务防护；评估控制链路与执行器安全机制，包括通信链路完整性、物理接口安全以及执行机构的故障安全（Fail-safe）设计；验证在网络或硬件故障、攻击环境下的隔离与降级策略，确保关键控制功能安全退出或触发紧急制动等应急措施。

路侧安全：针对车-路协同链路的安全需求，测试 RSU 与路侧信号控制系统的认证与加密机制，验证其对伪造、重放、中间人攻击的防护能力；评估路侧感知设备（如相机、雷达、融合节点）的数据完整性保障能力，对控制广播、交通诱导信息等关键数据进行篡改检测；检查路侧设备的固件更新、访问控制、安全审计等机制，确保配置、策略与状态变更可溯源，异常操作可被及时发现与响应。

云端安全：对云控平台、OTA 服务、调度与后台系统开展安全审计与渗透测试，验证升级包签名、访问控制、账户体系与权限管理的可靠性；检查云端指令下发链路的完整性校验与认证机制，防止恶意指令注入；评估云端日志的完整性、留存与取证能力，确保远程操作与系统变更可追踪；通过供应链安全测试验证云端组件的可信性，防止后门、恶意更新或篡改。

环境安全：验证 GNSS 与定位系统的抗干扰和防欺骗能力（如多源定位融合验证）；对高精地图、电子围栏及道路设施（标线、标志、交通灯等）的抗篡改能力进行评估，包括通过仿真或实物测试验证车端感知系统对物理诱骗与道路环境干扰的识别能力；模拟各种电磁、光学、气象等外部环境干扰场景，检测车端传感器在极端环境下的安全性能与降级策略。

车-路-云跨域测试：组织多层级、多链路的联动攻击演练，通过构造从云端/路侧至车辆的级联攻击路径评估系统整体安全防护能力；验证系统在车端、路侧与云端安全区域分隔条件下对跨域攻击的抵抗能力与最小割效果，确保局部故障不能迅速跨越不同安全域而引发系统性失效；同时检验跨域告警联动、事件关联分析、快速隔离与协同恢复机制的有效性。

6.3.2 测试维度构成与能力要求

中国智能交通产业联盟

为保证测试用例在技术栈层面的覆盖性，除按车端、路侧、云端及跨域分域组织测试外，测试用例还应按物理、计算、网络、应用、数据、智能六个维度进行归类与统计。六维度与本标准第4章所述系统结构层次保持一致，用于明确用例构成与能力验证范围。各维度的构成与能力要求如下：

物理维度：覆盖载具本体、路侧设备、机柜与现场接口、传感器与执行器等实体对象；重点验证物理接口防护、设备防拆与访问控制、物理篡改检测、故障安全（Fail-safe）与应急处置触发能力等；

计算维度：覆盖车端/路侧/云端的计算平台、操作系统与虚拟化/容器运行环境（含关键配置与权限边界）；重点验证最小权限、系统加固、可信启动/完整性度量（如适用）、进程隔离与资源滥用防护、关键服务异常恢复能力等；

网络维度：覆盖车载总线、车载以太网、V2X/蜂窝/专用网络及网关边界；重点验证身份认证与密钥协商（如适用）、通信加密与完整性保护、重放/伪造/中间人防护、DoS与拥塞下的降级与隔离能力等；

应用维度：覆盖感知处理、协同控制、调度管理、人机交互、远程运维与OTA业务流程；重点验证鉴权授权、输入校验与接口安全、关键指令完整性校验、业务逻辑滥用防护、审计与可追溯能力等；

数据维度：覆盖运行数据、日志与审计数据、配置与策略数据、模型训练与更新相关数据等；重点验证数据分类分级与最小化、存储与传输保护、完整性校验与防篡改、备份恢复、数据投毒与污染检测（如适用）等；

智能维度：覆盖车、路、云端智能模型、决策引擎与策略模块；重点验证模型完整性与防篡改、后门/对抗鲁棒性、推理链路可信与异常检测、模型更新与回滚控制、智能决策在受扰条件下的安全约束与可解释审计（如适用）等。

测试大纲应给出“分域×六维度”的用例映射关系与覆盖说明；当某维度在特定测试对象中不适用时，应在测试大纲中说明不适用依据及风险替代验证方式。

6.4 系统安全分级矩阵

系统安全等级与攻击承受测试之间应建立对应关系：

S1 级：系统通过T1级别攻击测试，覆盖车、路、云、环境等基本项，确保基本安全防护措施到位；

S2 级：在通过T2级别攻击测试的基础上，重点检查关键接口和子系统的安全性，使系统对单域或简单跨域的小规模组织攻击具有足够抵御能力；

S3 级：必须通过T3级别攻击测试，测试场景应包括跨域联动和长时潜伏的攻击，验证系统在面对有组织攻击团体时的检测和响应能力；

中国智能交通产业联盟

S4 级：通过T4级别的全面测试，考核系统对多矢量联合攻击和级联故障的承受能力，以及在遭受战略级破坏后的恢复能力。多域联合作战和长时间连续攻击是S4级别重点评估的内容。

每个等级测试需形成覆盖矩阵，从单一攻击到综合场景逐级加强，以确保测试结果可用于安全等级复核与后续改进。分级矩阵如下表所示：

表 2 自主式交通系统安全分级适用表

		攻击强度			
		T1级	T2级	T3级	T4级
安全等级	S1级	√			
	S2级	√	√		
	S3级	√	√	√	
	S4级	√	√	√	√

6.5 测试方法与判据

6.5.1 测试方法

本标准针对自主式交通系统信息安全能力评估，定义以下四种主要测试方法及其适用条件和目标：

仿真注入测试：适用于系统开发初期或难以在真实环境中复现的攻击场景。通过建立虚拟仿真环境，将网络入侵、恶意控制等攻击手段注入系统，对系统的检测、识别和防御能力进行评估。仿真注入测试可以覆盖高危和边缘场景，对安全策略有效性进行定量分析。该方法目标是验证系统在虚拟场景下的安全事件响应能力，包括及时发现威胁、生成告警和触发安全机制等。

台架联调测试：适用于将系统组件（如传感器、控制器、通信模块等）集成到硬件测试台架进行测试的阶段。在受控实验室环境下，通过台架集成模拟车辆及路侧基础设施的工作状态，并对系统接口、通信协议和软件逻辑进行联调测试。该方法旨在验证系统在综合硬件环境下的安全性能，例如验证加密通信、鉴权机制和故障隔离功能是否有效，以及评估系统在模拟攻击下的稳定性。

封闭场地测试：适用于系统硬件集成完毕并可搭载到车辆或固定场景时，在封闭测试场地内进行验证。在真实或仿真交通场景中设置安全障碍物和攻击信号（如GPS欺骗、无线信号干扰等），对系统的端到端安全能力进行测试。根据相关研究，封闭场地测试通过真实车辆和实际环境要素的控制，能够有效测试系统在现实条件下的性能。本方法目标是综合验证系统对物理攻击和环境干扰的抵御能力、告警机制及安全恢复功能。

中国智能交通产业联盟

在役受控演练：适用于系统正式部署后的运行环境中进行的安全演练。在保障车辆安全的前提下，模拟真实运行过程中可能遇到的网络攻击或系统故障，对在役系统进行应急演练和安全验证。此阶段侧重考察系统在实际道路条件下的安全监测与响应，据报道，通过收集运营中车辆相关数据，可以评估系统在道路运行时的安全性。其目标是验证系统在实际使用中的检测告警能力、事件隔离与快速恢复能力，以及后续取证能力。

针对不同安全等级的系统，可采用多种测试方法组合以满足要求。一般建议如下：对于安全等级 S1 的系统，至少应进行仿真注入测试，以验证系统的基本检测能力；对于 S2 级系统，可在此基础上增加台架联调测试，评估集成环境下的安全性；对于 S3 级系统，应进一步增加封闭场地测试，验证系统在真实环境下的安全防护能力；对于 S4 级系统，则应综合采用上述所有测试方法，在仿真、实验室和现场多层次场景中全面验证系统的安全性能。

6.5.2 判据

测试评估采用“发现—抵御—告警—隔离—恢复—取证”六阶段闭环模型进行。针对每个测试场景，应收集各阶段的安全响应信息（如日志、告警、状态指标等），并形成最小证据集。测试判定按以下原则进行：

测试合格：系统在预设攻击或异常场景中，应能够对事件进行完整处置。在“发现”阶段及时识别异常；在“抵御”阶段启动防护措施；在“告警”阶段生成正确告警信息；在“隔离”阶段将威胁或故障控制在局部；在“恢复”阶段有效恢复功能；在“取证”阶段产生可用审计证据。若每个阶段均有对应响应且记录了最小证据集，则判定该测试项为合格。

测试不合格：若系统在任意关键阶段未触发预期响应，或未生成必要证据，即认定该阶段失败，则整个测试项判定为不合格。例如检测未发现攻击、隔离机制失效或无审计日志等情形。

限改要求：若系统在大多数阶段响应正常，但存在部分功能缺陷或证据不足，可视具体情况要求限期整改。限改判定意味着整体安全性不致危及系统运行，可在规定期限内完善相关功能和日志记录，以满足合格判据。

判定过程中应严格依据“最小证据集”原则：仅当系统提供的证据足以覆盖整个处置闭环的关键环节并证明功能有效时，才视为通过；否则根据缺陷性质确定整改或判为不合格。

6.5.3 安全保障率判据

为对测试结果进行量化评估并形成可追溯的达标依据，采用安全保障率作为补充判据，其要求如下：

a) 测试对象描述：测试对象应与 6.2 规定的测试对象与边界一致，明确对象范围（车端/路侧/云端/环境及车-路-云跨域链路）、版本与配置基线、测试域与接口边界，并在测试大纲中固化；

b) 计算方式：安全保障率按通过测试用例数占总测试用例数的比例计算，安全保障率应不低于 99.5%；

中国智能交通产业联盟

c) 调整机制：当安全保障率不满足要求时，应在保持可追溯与可审计的前提下采取以下一种或多种调整措施：1.调整测试对象等级目标或能力边界：可下调拟满足的安全等级（例如 S4 调整为 S3），或按 4.2 重新界定测试对象的自主化水平边界（例如 L3 调整为 L2），并同步更新分级结论引用条款与证据链；2.用例剪裁：仅可剪裁实操性低、与测试对象边界不匹配或重复度高的用例，剪裁比例不应超过总用例数的 5%，剪裁应经评审并形成书面结论；3.重新测试：完成上述调整后应重新组织测试，直至满足安全保障率要求；所有调整理由、范围与影响分析应在测试报告中说明；

d) 结果记录：应留存并归档测试大纲、用例清单与版本、执行记录与日志证据、复测记录、评审结论及最终判定结果，作为安全保障率达标依据，并满足审计与复现要求。

6.6 方案设计与实施要求

6.6.1 测试环境构建与数据集要求

测试环境应模拟自主式交通系统运行的典型应用场景，并保持高度可控。仿真环境需涵盖多种交通场景及安全威胁场景，确保场景多样性、覆盖性和典型性，以提升测试结果的有效性和可靠性。仿真场景库应遵循从概念设计到建模仿真的框架要求，建立完善的场景用例库。数据集方面，应包括：常见和极端交通场景下的仿真数据、多类型 V2X 消息库，以及专门的对抗样本库。V2X 消息库需涵盖标准通信协议下的合法消息及可模拟攻击的异常消息，如虚假位置广播、格式错误数据等。对抗样本库应收集针对感知、决策等模块的已知攻击样本，用以评估系统对对抗性攻击的鲁棒性。测试数据和场景应能够复现真实运行条件下的复杂度，并满足信息安全测评需求。

6.6.2 工具合规性、数据留痕与实验复现要求

测试所用工具应符合国家或行业标准规范，工具版本、配置及使用过程需进行合规性验证。所有测试活动必须完整留存数据留痕，包括测试脚本、执行日志、捕获流量和系统状态等，以保证结果可追溯并可验证。参考相关研究要求，仿真工具链的使用过程应作出说明和记录，保证所用模型、算法和数据均受控且可核查；同时，充分注意工具链标准化缺失导致的复现实验困难。测试结果与环境配置信息应同步归档，支持后续审计与重现，从而确保测试的可复现性和可信度。

6.6.3 安全回退机制与现场应急处置要求

测试方案应包括安全回退（fallback）设计，即当系统检测到关键安全事件或无法正常运行时，能够自动或人工切换到预定义的安全模式，以保障核心功能和人员安全。系统上线前应验证回退机制的可靠性，确保在网络中断、攻击入侵等情况下能够迅速断开风险连接或进入安全状态。现场应急处置要求包括制定详细的应急预案和操作流程：当监测到重大安全事件时，应立即启动应急机制，对受影响的组件实施隔离或下线，通知应急响应团队，并开始取证和恢复操作。企业需证明系统在投入使用时具备安全监测能力，并对异常事件能够及时进行紧急处置，确保事件发生时快速响应、及时处理并恢复业务。

中国智能交通产业联盟

6.7 报告与结论

完成测试后，根据“部件×攻击等级×测试用例”的覆盖情况和通过率，形成完整的测试报告和评估矩阵，明确系统在各测试场景下的表现。报告中列出发现的关键安全缺陷及建议的整改措施，并跟踪整改后的复测结果以闭环管理。最终将测试数据和分析结果作为系统安全等级分级或复审的依据，形成分级结论建议，同时提出下一年度的复评计划，持续推进系统安全能力提升。报告中应给出安全保障率计算过程、统计结果及（如有）调整与复测记录，并将相关留痕材料编号归档。

7 自主式交通系统安全分级评估规范

7.1 自主式交通系统安全分级流程

本标准基于风险评估过程，规定了自主式交通系统信息安全等级的分级流程。依据《GB/T 31722—2015 风险管理指南》的基本框架，风险管理过程应首先建立语境，然后进入风险评估与风险处置阶段。其中，风险评估包括风险分析与风险评价两类活动，而风险分析又包含风险识别与风险估算环节。

上述过程与本标准中自主式交通系统的信息安全等级分级方法保持一致。确定自主式交通系统信息安全等级的一般流程如图1所示：

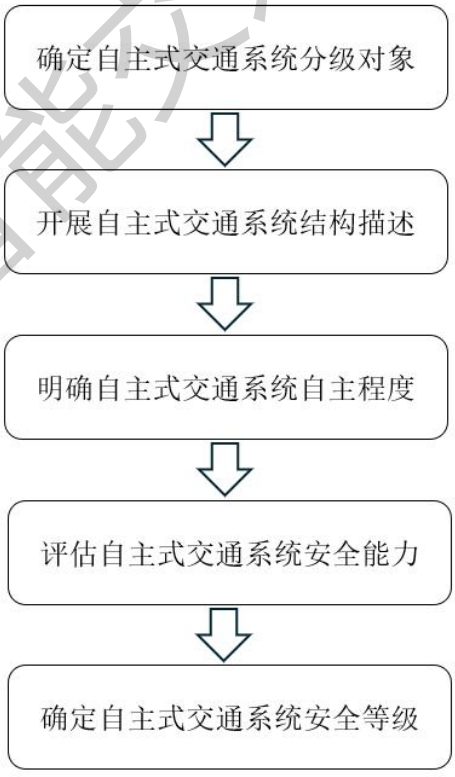

图 1 自主式交通信息安全分级流程

中国智能交通产业联盟

7.2 确定自主式交通系统分级对象

7.2.1 分级对象的确认条件

确认一个自主式交通系统作为分级对象，应满足以下基本条件：

a）一个具体的完整自主式交通系统：

业务应用：承载单一交通业务应用，例如城市自主交通公交线路系统、高速公路V2X协同控制系统、机场内部无人接驳系统等，具备明确的运行任务与业务边界；

独立性：系统的车端、路端和云端各功能模块相互独立，控制流程与信息处理设备具备清晰边界，无深度嵌套或交叉控制。例如，独占的感知融合平台、决策控制模块、车路通信节点等；

构成：自主式交通系统由车端控制系统、云端调度平台或边缘计算节点主构成，系统由多个车载单元、控制服务器、通信模块、传感器系统和路侧设备组成，形成完整的感知-传输-决策-执行闭环系统结构。

b）自主式交通系统中的相对独立部分：

为便于在系统工程视角下开展分级，自主式交通系统中的相对独立部分，可结合物理部署形态和功能定位，按照“车端－路侧－云端/通信”进行划分。符合下列条件的子系统，可作为单独分级对象：

车端子系统：指部署在车辆上的控制与感知执行系统，如车载控制器、车载感知与融合模块、执行机构及其内部通信网络（如车载以太网、CAN 总线等）。此类子系统通常围绕单车或车队形成完整的感知－决策－执行－通信闭环，具备相对独立的控制流程和运行逻辑，但可通过 V2X 等方式与路侧或云端进行数据交换或控制联动。

路侧子系统：指部署在道路基础设施上的控制与感知系统，如特定路段或交叉口的 V2I 节点、智能红绿灯控制子系统、路侧感知与诱导设备等。此类子系统以道路设施为物理载体，承担局部交通状态感知、信号控制和协同管控等功能，在地理或功能上具有相对清晰的边界，可按道路区段、管控区域或安全区域进行划分。

云端与通信基础子系统：指用于统一调度、管控和数据处理的云控平台，以及支撑车－路－云互联的基础通信系统，如专用蜂窝通信网、V2X 通信网络、专用 VPN/专线等。此类子系统为车端与路侧提供统一的业务支撑和数据通道，虽不直接承担全部物理控制动作，但在决策计算、数据汇聚、指令下发等方面具有高度集中性和独立的安全控制需求，在必要时可作为单独分级对象。

c）自主式交通系统的基本要素与完整性要求：

无论分级对象属于车端、路侧或云端/通信子系统，均应满足以下基本要求，方可作为独立分级对象：

中国智能交通产业联盟

功能闭环与物理实体：分级对象应由自动化控制组件（如车载控制器、交通信号控制器、云端调度模块）与感知/执行组件（如激光雷达、摄像头、执行机构等）按照统一的控制目标和控制逻辑组合而成，能够在本物理或逻辑边界内形成清晰的感知－决策－执行－通信功能闭环，构成可识别的物理实体或虚拟实体。

功能协同与业务完整性：一个自主式交通系统或其子系统可以由多个厂商提供的软硬件模块共同构成，只要车端、路侧与云端/通信各功能模块能够协同工作，并在其责任边界内形成统一的交通自动化运行能力，即可作为整体分级对象。

组件独立性限制：不得将单一组件（如某一服务器、单个通信终端、单个传感器节点等）单独作为分级对象，除非该组件在特定车端、路侧或云端场景中，已在功能和运行上实质具备完整系统特征，能够独立承担感知－决策－执行－通信闭环中的主要职责，并对安全风险承担可识别的责任边界。

d）唯一确定的安全责任单位：

分级对象的自主式交通系统应能明确其安全责任归属单位，责任单位需对该系统的信息安全规划、建设、运维、管理负全部或主责；

若下属部门承担系统建设、运行维护及安全运营职责，则该下属单位可认定为安全责任单位；

若多个下属单位分别承担系统设计、开发、运维等职责，则应由其共同上级单位明确系统整体安全管理与评估责任，作为最终责任单位。

7.2.2 分级对象的系统描述

对分级对象进行系统描述的目的是识别自主式交通系统的核心任务与安全使命，即该系统所承担的运行目标、业务功能及其能力要求。系统描述内容应涵盖其执行功能、所需接口与支撑能力、处理信息种类、运行结构、面临威胁等关键因素，以便支撑后续信息安全等级的科学划分。

a）自主式交通系统的基本信息：

总体目标与业务使命：明确自主式交通系统及其所属的业务平台或交通场景的总体目标、运行任务与业务使命。例如，智能公交系统、自主交通车道等；

控制流程与信息流动：描述系统的控制流程、覆盖范围、逻辑边界及信息流向，特别是车-路-云之间的交互关系；例如，智能体与载具、基础设施之间的数据与命令交互；

系统架构：系统的技术架构及管理组织体系，如是否集成云边协同结构、平台控制逻辑集中或分布式部署；

资产清单与业务映射：列出构成该系统的关键软硬件资源清单，并明确每项资产在交通调度、控制、感知等业务中的作用与关联性。

b）系统的网络及设备部署情况：

中国智能交通产业联盟

物理运行环境：描述系统所在的物理运行环境，如城市道路、高速公路、园区、机场等；

通信拓扑结构：说明系统所采用的通信拓扑结构（如V2X、5G、车载以太网等）；

设备与边界划分：列明控制设备（如车载计算平台、路侧单元RSU）、传感器、执行器、服务器、通信链路的部署与边界划分方式。

c）系统的业务种类与运行特性：

核心业务：包括系统涉及的核心业务，如路径规划、调度优化、协同感知等；

车辆与路段数量：明确系统覆盖的车辆数量、路段数量等；

信息安全需求：明确系统对信息安全属性（可用性、实时性、可操作性、完整性、保密性）的需求强度，是否属于闭环控制系统、是否支持连续运行、是否具备自主学习能力等。

d）系统提供的服务功能：

列出自主式交通系统为实现任务目标所提供的操作、控制与服务能力，如交通信号调控、障碍识别处理、路径再规划等；

评估各类服务在可用性、完整性与保密性方面的重要性等级。

e）系统处理的业务数据：

列出系统处理的主要数据类型（如实时图像、车辆状态、指令流、路侧感知数据），并明确这些数据的传输协议（如DSRC、MQTT、HTTP/HTTPS等）；

标注这些数据在保密性、完整性、可用性等维度上的信息安全等级要求。

f）系统与外部信息系统的连接关系：

明确系统是否与外部系统（如城市交通管理平台、公安联网系统、调度指挥中心、云平台等）互联互通；

列明接口方式（如API、网关、VPN等）、控制机制、传输内容类型，以及连接的用户范围与类型（如管理人员、驾驶员、平台开发者等）。

g）管理框架与职责划分：

说明该自主式交通系统的组织管理结构、安全管理策略、设置的管理部门及其职责；

明确不同岗位（如系统运维、数据安全员、安全策略制定人员）的安全角色和责任划分。

h）安全区域划分与通信网络依赖：

对于结构较大或具备多区域部署的自主式交通系统，应明确其安全区域（如感知区、控制区、通信区）与通信网络（如专用5G、V2I、V2V链路）之间的依赖与安全边界划分；

为系统分层分级提供依据，确保各区域的安全性与防护能力得到充分考虑。

中国智能交通产业联盟

8 自主式交通系统各等级安全防护能力描述

8.1 引言

自主式交通系统按照影响范围和安全需求划分为四个安全等级：S1级至S4级（见5.2.4）。同时，攻击者能力也分为四个等级（见6.3.2），从使用公开工具的基础对手（T1）到国家级/战略攻击者（T4）。系统安全等级与攻击强度之间建立对应关系：S1级系统应能抵御基础对手（T1）级攻击，S2级在此基础上增强以抗小型组织（T2）级别的跨域攻击，S3级须通过有组织团体（T3）级别的复合攻击测试，S4级则面向国家级（T4）多矢量联合攻击和级联故障测试。本文按照等保标准风格，逐级描述S1–S4系统的定义、抗攻击能力及防护要求，为各级系统设计、测试和升级提供参考。

8.2 S1 级安全系统的抗攻击能力

定义：S1级系统通常部署在区县级或封闭园区等小范围场景，自主交通功能级别较低（如L0–L1级别）。S1级系统遭受攻击时，影响通常局限于局部，可能导致短时服务中断或少量数据泄露，但可快速恢复。

抗攻击能力：

对T1级攻击：针对基础对手发动的单点、短时攻击（如简单的GPS信号欺骗、CAN报文注入、蓝牙重放或无线干扰等），S1系统应具备基本检测和拦截能力。系统通过传感器数据完整性校验、基础入侵检测和基础加密/校验措施，将攻击成功率降至极低（典型＜5%），检测真阳性率＞95%。例如，启用基本的消息认证码或CRC校验可有效防止伪造控制指令，GPS伪信号干扰可通过多源定位对比发现异常。攻击发生后，系统能够进行故障隔离或安全降级，预计最大恢复时间可控制在数秒级。

对T2级攻击：面对小型组织发动的跨域协同攻击（如联合对OBU/RSU进行DOS，或复杂的GPS欺骗+CAN篡改组合攻击），S1系统缺乏专门强化措施，防护能力有限。此类攻击可能导致S1系统局部功能失效或持续中断。一般情况下，攻击成功率明显高于5%，需要通过升级安全补丁或加强检测策略才能进一步降低风险。

对T3级攻击：对于有组织团体/APT发动的长期潜伏攻击（例如利用零日漏洞进行OTA升级包篡改、对车载系统秘密植入后门、恶意提取硬件安全模块秘钥等），S1级系统的防护能力不足。此时攻击可能导致关键模块控制权丧失或核心数据被破坏，严重时需人工干预重启或修复。

对T4级攻击：面对国家级多矢量攻击（如跨区域联动攻击同时打击车路云各域，或直接针对安全硬件实施高级渗透），S1级系统基本无法抵御，可能造成广泛失效。此级别攻击超出S1能力范畴，属于一级退级范畴。

防护要求：为实现以上防护能力，S1级系统应至少具备基本安全机制：

中国智能交通产业联盟

安全引导和硬件保护：启用安全启动（Secure Boot），确保所有固件和软件经过完整性校验后才能运行；禁止未授权的调试接口和ROOT访问，采用最小权限设计，开启SELinux等强制访问控制。

数据加密与密钥保护：敏感数据应避免明文存储或硬编码；密钥与凭据应使用操作系统安全存储能力（如系统密钥库/安全存储）进行管理。离线或OTA升级包需实施数字签名校验，防止篡改升级包导致非预期升级或升级失败。

基础网络安全：对车载网络进行简单隔离，仅开放必要服务；在CAN网关等关键节点设置访问控制和流量滤波，防止简单的数据注入和消息重放。通信协议（如车载以太网、Wi-Fi、蓝牙）应启用基础加密与认证配置（例如TLS、WPA2/WPA3、蓝牙安全连接等），降低嗅探和重放风险。

基本认证与审计：对设备和用户实行基本身份认证与权限控制，对远程接口和OTA通道实施强口令/证书校验、访问频控等基础防护。建立基础的日志审计和安全告警，当检测到异常时能够即时提示并启动保护策略。

8.3 S2级安全系统的抗攻击能力

定义：S2级系统通常用于城市级（地市级）交通场景，具备部分高级自动化功能（如L1－L2级别）和更广的覆盖范围。S2级系统的安全影响范围较S1大，一旦受攻击可能导致城市级业务能力下降或阶段性中断，需要通过应急处置在规定时间内恢复主要功能。

抗攻击能力：

对T1级攻击：针对基础对手的局部攻击（如GPS欺骗、CAN重放、无线干扰），S2系统具备完善的检测和防御机制。系统会利用多源融合感知和入侵检测，联合多传感器信息过滤异常信号，将此类攻击成功率控制在极低水平（＜5%），检测率＞95%。基础网络攻击（如简单端口扫描、Wi-Fi弱口令攻击）可由访问控制和加密通信机制阻断。

对T2级攻击：对于小型组织的跨域攻击（如结合车路协同消息伪造、中级规模的Bluetooth重放攻击或CAN网关注入），S2系统在S1的基础上加强关键子系统的安全性。通过域间隔离、防火墙和安全网关，系统可以识别并隔离跨域攻击路径。在此级别攻击下，应通过行为分析和安全策略使攻击成功率降低到可接受范围（建议＜10%）且检测率保持在90%以上。典型攻击如“对RSU信号重放导致交通指挥错误”或“注入伪造制动命令”都应能被安全模块发现并阻断。

对T3级攻击：面对APT团体的复杂攻击（如长期针对车联网系统的多阶段钓鱼、中间人和后门攻击），S2系统需要部署入侵检测系统(IDS)和安全事件关联分析。系统应在检测阶段及时发现跨域威胁（例如连续多域传感器数据不一致、OTA升级包签名异常），并启动防御策略。在这一等级攻击下，目标是确

中国智能交通产业联盟

保核心服务能够降级运行，不发生系统性瘫痪；典型要求如对车辆网络恶意数据的检出率高于90%、主要功能连续性保持在可控范围。

对T4级攻击：对于国家级攻击，S2系统只有有限防护能力，需要紧急启动事故预案。此时可能出现区域内长时间的大范围中断。S2级不会作为设计时防护T4的目标，仅需保证自身基本安全域能在攻击后实现隔离或紧急停用。

防护要求：为了实现上述防护能力，S2级系统需在S1级基础上增加以下安全机制：

强化认证与访问控制：采用双因素或更高级的身份认证机制，确保对远程接口（如OTA服务器、远程诊断）和设备登录的双重验证。

体系化加密通信与信任体系：在S1基础加密配置之上，建立更完备的加密认证体系，采用证书体系与密钥生命周期管理（如PKI）实现车路协同链路的双向认证与完整性保护；对V2X消息进行签名验证与证书校验。

网络隔离与边界防护：对车载网络、道路设施网络和运营后台网络进行清晰的分区隔离。关键ECU和控制器应通过防火墙或网关与辅助系统分离，禁止非授权数据流通。支持VPN或专网访问，避免车辆信息终端接入不安全的公网。

入侵检测与防御：部署基于规则和行为分析的IDS/IPS，对CAN总线、以太网等内部总线实施流量监测，对异常报文（如异常刷写帧频）进行拦截。结合安全日志和审计数据实现多级关联分析，快速定位攻击源。

安全更新和应急恢复：所有更新包必须通过安全签名验证，且优先使用安全可信固件。系统应具备故障降级与冗余能力，必要时启动安全模式（如只保留最小控制功能）。定期开展安全演练，确保在遭受攻击或异常后能够快速隔离故障域并恢复主要业务。

8.4 S3级安全系统的抗攻击能力

定义：S3级系统适用于省部级或跨区域的大规模自主交通系统，自主交通功能高度发达（如L2有条件自主交通）。此级别系统具有重要关键保护属性，受到攻击时可能对社会秩序造成严重危害。S3系统需要支持跨域联动的复杂场景，并强调检测与响应能力。

抗攻击能力：

对T1/T2级攻击：S3系统自然能够轻松抵御基础对手和小型组织发起的普通攻击，几乎所有基础攻击都会被安全防护机制察觉。基础攻击成功率近乎为零，系统设计要求基本功能持续可用。

对T3级攻击：S3级着重考核系统对有组织团体的攻击承受力。此时攻击场景将包括跨域联动和长期潜伏。例如攻击者可能联合对车辆感知、控制和路侧基础设施进行多阶段攻击：如先对交通信号控制器

中国智能交通产业联盟

实施入侵，再通过受控信号影响车载视觉系统，最终篡改制动指令。S3系统需具备多模态感知融合与安全审计能力，能够在“发现→抵御→告警→隔离→恢复”六阶段模型中完整处置异常。具体要求包括：威胁发现率高（TPR≥90%）、误报率低；在隔离阶段能将威胁局限在单一域内；恢复阶段能够有效重建受影响功能。典型指标可定为：复杂攻击链路最终致功能损失的概率极低（攻击成功率≪10%），检测与响应时间在可控范围内（例如几秒级内触发应急策略）。

对T4级攻击：面对国家级连续攻击，S3系统必须展现强大的容灾和恢复能力。虽然可能出现多域功能暂时失效，但系统设计要求快速切换到冗余系统或触发安全停驶，避免造成战略性级别后果。系统需在攻击结束后较短时间内恢复核心功能，确保交通系统整体稳定。

防护要求：S3级系统的安全防护应达到较高标准：

全局监控与决策：构建贯穿车、路、云的安全监控体系，实现多域数据汇聚与联动分析。对跨域攻击采用最小割原则设计，确保单域故障无法导致全系统瘫痪。

设备级信任与隔离：关键控制器和执行器使用硬件安全模块或可信平台模块(TPM)存储秘钥；车辆重要ECU和智能体处在可信执行环境(TEE)中运行；关键域间采用严格的分级隔离和网关认证。

高级攻击防御机制：针对感知欺骗攻击，使用高精度地图和环境多样本验证检测虚假标志；对AI模块实施对抗样本防护和模型完整性校验。网络层面，采用防DDoS设备、行为基线分析、信号时序检测等技术，针对OTA、后台和供应链进行深度渗透测试和签名验证。

应急响应与取证：建立完善的安全应急机制，攻击发生后能自动隔离受影响组件并通知安全团队，启动应急恢复流程。所有操作留存可用的审计日志，以便事后取证和改进；并在组织层面定期开展跨域联动处置演练，验证机制有效性。

8.5 S4 级安全系统的抗攻击能力

定义：S4级系统面向全国范围的交通枢纽和关键基础设施，自主交通功能接近完全自动化（L3全域自主交通）。S4级为战略保护对象，攻击后果极其严重，可能影响国家安全和全局交通稳定。

抗攻击能力：

对T1－T3级攻击：S4系统集成了S1－S3所有防护措施，对普通和中高级攻击几乎零容忍。任何单一攻击都能被系统自动阻断和隔离，核心功能始终保持可用。

对T4级攻击：国家级攻击将采取多矢量、长时间连续方式打击交通系统。S4系统设计要求能够承受此类极端条件。系统必须能够在GPS欺骗、通信链路全面拦截、供应链攻击等联合攻击下保障重要控制权。如先后对路侧单元、V2X链路、车载网络和云端同时攻击，S4系统仍需保证关键传感器故障时进行安全降级、保证紧急制动等核心功能可用。量化目标为：多域联合攻击下系统功能失效概率极低（攻击

中国智能交通产业联盟

最终成功率接近0%），综合检测和告警准确率接近100%。在重击之下，系统应快速切换冗余系统或进入安全模式，恢复时间控制在秒级至十秒级以内。

防护要求：S4级系统要求最为严格，需实施多层次、全方位的防护：

国家级认证和政策支撑：遵循相关国家安全法规，系统设计和运维需通过国家或行业安全认证。与国家应急和监控中心联网，在遭受攻击时启动国家级应急响应机制。

全域加固与冗余：从硬件到软件均采用最严密的安全方案：安全芯片、存储加密和运行环境保护；关键软件使用多版本、多厂商冗余实现（如至少两套独立的决策系统）；建立地理隔离的备份数据中心。

深度安全技术应用：对车路云的每个环节引入高强度安全技术体系，强化硬件根信任、全域证书与密钥治理、深度威胁检测与跨域联动处置能力。对V2X通信实施高级加密与完备PKI信任体系支撑下的消息签名、验证与撤销机制。

国家级统筹的持续攻防演练与联动处置：在S3已建立的应急响应机制与演练基础上，开展国家级或跨区域的常态化攻防演练与联动处置演习，模拟极端条件下的联合攻击（如多点GPS欺骗+网络封锁+物理破坏组合），验证跨域指挥、资源调度与全局恢复能力，确保系统安全防护能力能够持续升级和演进。

8.6 提升与演进办法

随着安全等级的提升，系统的防护目标和能力也逐级增强。S1级强调基本感知和控制的完整性，对抗单点、局部攻击；S2级增加了跨域接口保护和小规模组织攻击防御能力；S3级需应对跨域联动和长期潜伏攻击，具备高级检测与响应手段；S4级则针对全谱国家级攻击，通过最深层的安全加固和冗余设计保证系统整体稳定。各级区别主要体现在攻击成功率阈值、检测率要求和恢复能力上：高级系统对攻击成功率的容忍度极低（接近0%），响应和恢复要求更及时彻底。对于自主式交通系统安全分级测试，在设计和测试时应采用分级防护思路：S1级系统通过仿真测试验证基本检测能力，S2级加入实验台架联调测试评估集成环境安全，S3级增加封闭场地实车测试检验真实环境中的防护效果，S4级则在仿真、实验室和现场多层次场景中进行全面攻防演练。同时，各级系统应根据实际场景不断迭代和升级安全措施。例如S2系统可加强接口级认证和日志分析，S3系统加强多域融合防御，S4系统则建立国家级响应机制和实时威胁情报。自主式交通系统应建立持续安全生命周期管理机制。需根据新兴威胁和攻击手段及时修订防护策略，引入先进技术来增强系统韧性。定期进行安全评估和演练，使系统具备快速更新与适应能力，形成“发现—抵御—告警—隔离—恢复—取证”的闭环安全机制，确保在面对不断演变的威胁时能够快速响应并恢复正常运行。

中国智能交通产业联盟

T/ITS XXXX-XXXX

中国智能交通产业联盟

中国智能交通产业联盟

标准

自主式交通系统 信息安全分级规范

T/ITS 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