ICS 35.240.60
CCS R 87

团　　体　　标　　准

T/CSAE 289—2022

车路协同　智能路侧设备接入网络安全技术要求

Vehicle-infrastructure cooperation—Cybersecurity technical requirements of intelligent road side equipment access

2022－12－30 发布　　2022－12－30 实施

中国汽车工程学会　　发 布

中国汽车工程学会标准（以下简称：CSAE 标准），是由中国汽车工程学会按照明确的程序、规则，遵循公开、透明、协商一致原则组织制定的，供市场自由选择、自愿采用的规范性技术文件。CSAE 标准旨在发挥市场自主制定标准优势，着眼企业竞争力提升，推动汽车产业创新技术的加速发展和广泛应用。

在本标准实施过程中，如发现需要修改或补充之处，欢迎将意见反馈至中国汽车工程学会，以便修订时参考。

中国汽车工程学会地址：
北京市大兴区融兴北三街39号行知楼；
电话：010-50911954；邮编：100176；邮箱：wwq@sae-china.org。

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　系统框架 2
6　连接技术要求 3
7　身份认证技术要求 4
8　数据访问控制技术要求 4
9　接入网络安全管理要求 5
参考文献 6

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这些专利的责任。

本文件由中国汽车工程学会汽车智能共享出行工作委员会提出。

本文件起草单位：北京航空航天大学、上海国际汽车城（集团）有限公司、北京百度智行科技有限公司、北京信息科技大学、北京奇虎科技有限公司、中国软件评测中心、国汽（北京）智能网联汽车研究院有限公司、中国汽车工程学会、泰安北航科技园信息科技有限公司、湖南大学、湖南大学无锡智能控制研究院、上海淞泓智能汽车科技有限公司。

本文件主要起草人：于海洋、任毅龙、沈理容、冀浩杰、彭伟、赵亚楠、孙宁、付兴坤、罗承刚、严敏睿、吕欣鸿、朱科屹、邹博松、廖亚男、孙东、路宏、王淼、武元丰、宁友良、薛宇、胡满江、边有钢、秦洪懋、徐彪、秦晓辉、秦兆博、吴俊贤、霍燕燕。

车路协同　智能路侧设备接入网络安全技术要求

1　范围

本文件规定了车路协同 智能路侧设备接入系统框架、身份认证技术要求、证书和密钥管理技术要求、数据访问控制技术要求、监控安全技术要求。

本文件适用于智能路侧设备接入网络安全的设计、开发和管理。

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 21053—2007　信息安全技术　公钥基础设施PKI系统安全等级保护技术要求
GB/T 28421—2012　电子收费　基于专用短程通信的电子收费交易
GB/T 29111—2012　道路交通信息服务　通过蜂窝网络发布的交通信息
GB/T 30276—2020　信息安全技术　网络安全漏洞管理规范
GB/T 37935—2019　信息安全技术　可信计算规范 可信软件基
YD/T 3340—2018　基于LTE的车联网无线通信技术　空中接口技术
YD/T 3707—2020　基于LTE的车联网无线通信技术　网络层技术要求
YD/T 3847—2021　基于LTE的车联网无线通信技术　支持直连通信的路侧设备测试方法
YD/T 3957—2021　基于LTE的车联网无线通信技术　安全证书管理系统技术要求
YD/T 3978—2021　基于车路协同的高等级自动驾驶数据交互内容

3　术语和定义

下列术语和定义适用于本文件。

3.1

智能路侧设备　intelligent roadside equipment

设置于道路两侧或龙门架等位置，实现道路交通感知、通信、计算、控制与服务等路侧功能的设备，由通信单元、定位单元、路侧感知单元、边缘计算单元、交通控制与服务单元等组成。

3.2

通信单元　communication unit

设置于道路路侧或龙门架等位置，具备无线或有线连接方式的产品或功能集成产品。

3.3

定位单元　positioning unit

设置于道路路侧或龙门架等位置，具备卫星定位数据的采集、跟踪、记录等功能的产品。

3.4

路侧感知单元　roadside sensing unit

设置于道路路侧或龙门架等位置，具备感知功能的传感器或传感器集，用于对道路交通运行情况、交通参与者、交通事件等检测识别，包括但不限于激光雷达、摄像头、毫米波雷达等产品。

[来源：YD/T 3978—2021，8]

3.5

边缘计算单元　edge computing unit

设置于道路路侧或龙门架等位置，具备强大计算功能的产品，用于实现多源信息融合、目标识别、事件检测、数据存储、高精度定位计算、智能协同、资源调度、信息安全等功能。

3.6

交通控制与服务单元 traffic control and service unit

设置于道路路侧或龙门架等位置，包含交通信号灯、交通标志线、可变情报板等电子设施，用于实现交通管理与控制功能。

3.7

车路协同云平台 vehicle-infrastructure cooperation cloud platform

设置于云端，实现车路协同的道路数据、车辆状态数据、路网状态数字化特征显示以及与自动驾驶汽车配合实现交通调度、交通管控等服务。

3.8

可信根实体 entity of trust root

设置于智能路侧设备产品内部,用于支撑可信计算平台信任链建立和传递以及可对外提供完整性度量、安全存储、密码计算等服务的功能模块。

[来源：GB/T37935—2019,3.12]

3.9

蜂窝网络 cell network

将移动电话服务区划分为若干个彼此相邻的小区，每个小区设立一个基站的网络结构。由于每个小区呈正六边形，又彼此相连，从整体上看，形状酷似蜂窝，所以人们称蜂窝网。

[来源：GB/T 29111—2012,3.1]

4 缩略语

下列缩略语适用于本文件。

DSRC：专用短程通信技术（Dedicated Short Range Communication）

PC5：直连通信接口（Proximity Services Communication）

PKI：公钥基础设施（Public Key Infrastructure）

RJ45：标准8位模块化接口（Registered Jack45）

5 系统框架

5.1 连接方式

5.1.1 有线连接应采用光纤、双绞线等传输方式，应支持以太网光纤、双绞线 RJ45 等接口方式。

5.1.2 无线连接应采用蜂窝网、PC5、DSRC 等传输方式。

5.2 系统框架

智能路侧设备与车路协同云平台、智能路侧设备、智能网联汽车的接入系统框架，如图1所示：

——智能路侧设备与车路协同云平台实现数据双向传输，如智能路侧设备将道路环境数据及交通状态数据传输到车路协同云平台，车路协同云平台发送交通道路管控数据到智能路侧设备，实现车路协同云平台的交通场景显示、交通预警显示、交通调度等功能；

——智能路侧设备与智能路侧设备实现数据双向传输，用于智能路侧设备的多源信息融合、智能协同等功能；

——智能路侧设备与智能网联汽车实现数据单向传输，用于车辆预警、决策控制信息的交互等功能；

——智能路侧设备内路侧感知单元、定位单元、边缘计算单元、通信单元实现数据双向传输，用于智能路侧设备道路交通感知、通信、计算、控制与服务等功能。

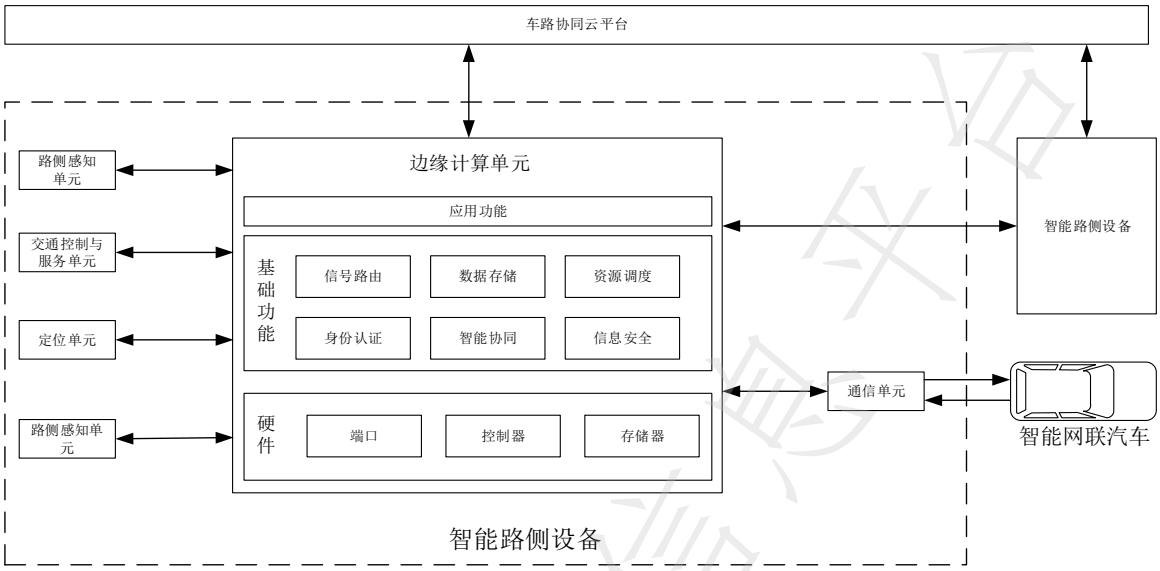

图1　智能路侧设备接入系统框架图

6　连接技术要求

6.1　安全接入要求

有线连接宜采用专用网络或建立加密通道方式。

无线连接宜采用专用无线网络或通道方式。

6.2　传输类型

6.2.1　智能路侧设备与车路协同云平台、智能路侧设备之间数据传输应采用 TCP/IP 协议。

6.2.2　智能路侧设备与智能网联汽车之间通信应采用 PC5、DSRC 等协议，PC5 通信应满足 YD/T 3340—2018、YD/T 3707—2020 的规定，DSRC 通信应符合 GB/T 28421—2012 的规定。

6.3　接口类型

6.3.1　智能路侧设备与车路协同应具备证书注册、交通控制、设备管理等会话接口；

6.3.2　智能路侧设备与智能路侧设备应具备证书认证、交通事件等会话接口。

6.4　接入会话要求

智能路侧设备应具备身份认证机制，验证接入会话满足以下要求：

——智能路侧设备与车路协同云平台接入，应采用双向身份认证；

——智能路侧设备与智能路侧设备接入，应采用双向身份认证；

——智能路侧设备与智能网联汽车接入身份认证应满足 YD/T 3957—2021 标准规定。

6.5　通信安全要求

智能路侧设备接入车路协同云平台、智能网联汽车、智能路侧设备时，智能路侧设备不应旁路。智能路侧设备应采用国密算法，加密方式应满足以下要求：

——与车路协同云平台应采用端到端信道加密；

——与智能路侧设备应采用端到端信道加密。

注：智能路侧设备接入网络后串行通信，不能存在并行通信通道。

6.6 安全启动要求

智能路侧设备在安全启动过程中，可信根实体、引导程序、系统固件应满足以下要求：
——不被篡改；
——若被篡改，智能路侧设备无法正常启动。

7 身份认证技术要求

7.1 唯一标识识别

智能路侧设备应具备唯一识别、不可篡改、不可伪造、统一管理的身份标识。

7.2 认证失败机制

身份认证过程失败后应满足以下要求：
——终止认证超时的当前会话；
——终止规定次数认证失败的接入会话的尝试。

7.3 证书和密钥管理技术要求

7.3.1 证书管理

智能路侧设备应具备数字证书的申请、存储、更新等功能。

7.3.2 密钥管理

智能路侧设备应具备密钥管理功能，满足以下要求：
——支持创建、存储、更新和删除接入会话密钥等操作，具备访问控制和密码保护功能；
——采用离线分发方式将预共享密钥分配至智能路侧设备；
——密钥管理支持多级生成和更新机制，主密钥的管理应支持密钥更新和注销安全策略；
——支持密钥隔离存储。
注：密钥隔离存储指密钥单独放置隔离区域，比如硬件存储，软件加密保护区等方法均属于密钥隔离存储。

7.4 PKI 安全

为智能路侧设备颁发证书的PKI系统应符合GB/T 21053—2007的规定，满足不低于3级安全等级保护。

8 数据访问控制技术要求

8.1 访问控制策略

智能路侧设备应具备访问控制策略，访问控制策略应满足以下要求：
——智能路侧设备的应用软件、数据等资源应具备访问控制验证，禁止非授权终端访问；
——智能路侧设备应支持车路协同云平台、智能网联汽车、智能路侧设备访问控制安全策略的配置和执行，智能路侧设备应根据不同终端配置不同的数据资源访问控制策略。

8.2 强制访问控制

智能路侧设备应具备强制访问控制策略，强制访问控制策略应满足以下安全要求：
——智能路侧设备的应用软件，数据等资源设置敏感标记；
——支持基于敏感标记和访问控制策略的强制访问控制。

8.3 隐私保护

智能路侧设备数据处理过程中应满足GB/T35273—2017的规定。

9 接入网络安全管理要求

9.1 异常行为检测

智能路侧设备应具备异常行为检测能力，异常行为检测能力应满足以下要求：

——支持对特定通信协议、数据格式的数据包过滤检查，丢弃不符合过滤要求的数据包；

——支持对恶意攻击和异常行为的检测，具备入侵告警功能。

9.2 漏洞安全

智能路侧设备不存在由权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞，漏洞管理应符合GB/T30276—2020的规定。

9.3 日志要求

智能路侧设备应支持记录存储车路协同云平台、智能路侧设备、智能网联汽车的接入行为数据，接入行为数据应至少包含日期、时间、接入设备类型、接入设备主体、接入事件描述、接入成功/失败的信息，日志保存期限应不少于6个月。

9.4 审计要求

审计运行事件检查、服务器状态记录、系统重要策略设置等数据，审计记录不得进行修改和删除，审计记录保存期限不少于6个月。

9.5 升级功能

智能路侧设备应具备升级功能，应满足以下要求：

——具备升级包校验机制，满足升级包完整性和真实性的安全要求；

——具备不同软件版本的唯一标识符。

参 考 文 献

[1] GB/T 35592—2017 公安物联网感知终端接入安全技术要求
[2] GB/T 40856—2021 车载信息交互系统信息安全技术要求及试验方法
[3] DB50/T 10001.4—2001 川渝智慧高速标准
[4] DB50/T 10001.4—2001 智慧高速公路 第四部分：车路协同系统数据交互
[5] DB50/T 10001.3—2021 DB51/T 10001.3—2021 智慧高速公路 第3部分：路侧设施设置规范