ICS 43.040.10
CCS T 36

DB11

北 京 市 地 方 标 准

DB11/T 2345—2024

车路云一体化系统车载单元应用技术要求

Technical requirements for on-board unit application of Vehicle-Road-Cloud Integration System

2024 - 12 - 25 发布　　2025 - 04 - 01 实施

北京市市场监督管理局　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。

本文件由北京市经济和信息化局提出并归口。

本文件由北京市经济和信息化局组织实施。

本文件起草单位：北京车网科技发展有限公司、中信科移动通信技术股份有限公司、北京云驰未来科技有限公司、云控智行科技有限公司、联想（北京）有限公司、新石器慧通（北京）科技有限公司、东软集团股份有限公司、新岸线（北京）科技集团有限公司、北京智慧城市网络有限公司、北京市智慧交通发展中心。

本文件主要起草人：孙宁、李峰、杨烨、高景伯、陈瀚、鲁鹏、于士超、王运、王林涛，王昶淳、刘蛟、田亮、钟严军、吴雅南、常雪阳、杨梦燕、黄杰、李滋、李水旺、郜冲、冯俊涛、黄含笑、马飙、李昕、刘浩、葛启彬、马凌飞。

引　言

本文件是为支持北京市高级别自动驾驶示范区建设，以示范区1.0和2.0技术方案为基础，复制推广已有技术经验成果，统筹建设全市统一云控平台，接入智能网联路侧设备和车端数据，提供车路云一体化服务，开展自动驾驶车辆运行监管，为智慧城市建设进行数据赋能而制定。考虑到车路云一体化涉及到的车端部分，本文件针对车载单元应用编写。

车路云一体化系统车载单元应用技术要求

1 范围

本文件规定了车载单元（OBU）应用的交互要求、功能要求和安全要求。

本文件适用于车路云一体化系统中车载单元（OBU）的应用。

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 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 31024.2 合作式智能运输系统 专用短程通信 第2部分：媒体访问控制层和物理层规范

GB/T 36454 信息技术 系统间远程通信和信息交换 中高速无线局域网媒体访问控制和物理层规范

GB/T 43187 车载无线通信终端

YD/T 2394.2 高频谱利用率和高数据吞吐的无线局域网技术要求 第2部分：增强型超高速无线局域网媒体接入控制层（MAC）和物理层（PHY）

YD/T 3707 基于LTE的车联网无线通信技术 网络层技术要求

YD/T 3709 基于LTE的车联网无线通信技术 消息层技术要求

YD/T 3756 基于LTE的车联网无线通信技术 支持直连通信的车载终端设备技术要求

YD/T 3957 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 基于车路协同的高等级自动驾驶数据交互内容

DB11/T 2329.1 车路云一体化信息交互技术要求 第1部分：路侧设施与云控平台

3 术语和定义

DB11/T 2329.1界定的以及下列术语和定义适用于本文件。

3.1

车载单元 on-board unit（OBU）

指安装在智能网联汽车上，支持EUHT、C-V2X、4G/5G通信，可实现V2X应用的硬件单元。产品形态可为独立的装置或系统、也可为与车辆其它部件集成在一起的装置或系统。

注：EUHT指物理层及媒体接入控制层满足YD/T 2394.2规定的无线通信技术。

4 缩略语

下列缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）

BDS：北斗卫星导航系统（BeiDou Navigation Satellite System）

CAN：控制器局域网络（Controller Area Network）

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

DNS：域名解析系统（Domain Name System）
EUHT：增强型超高吞吐（Enhanced Ultra High Throughput）
GNSS：全球导航卫星系统（Global Navigation Satellite System）
GPS：全球定位系统（Global Positioning System）
IDPS：入侵检测和防御系统（Intrusion Detection and Prevention Systems）
IP：因特网互连协议（Internet Protocol）
MAC：媒体接入控制（Media Access Control）
OBU：车载单元（On-Board Unit）
OTA：在线升级（Over-the-Air Update）
PCB：印制电路板（Printed Circuit Board）
TCP：传输控制协议（Transmission Control Protocol）
TLS：安全传输层协议（Transport Layer Security）
UDP：用户数据报协议（User Datagram Protocol）
UDS：统一诊断服务（Unified diagnostic services）
V2I：车载单元与路侧单元通信（Vehicle to Infrastructure）
V2P：车载单元与行人设备通信（Vehicle to Pedestrians）
V2V：车载单元之间通信（Vehicle to Vehicle）
V2X：车载单元与其他设备通信（Vehicle to Everything）

5 交互要求

5.1 交互架构

OBU集成在车辆中，支撑车辆与云控平台、路侧基础设施、其它车辆和其它交通参与者等之间通信。图1为OBU交互架构示意图。

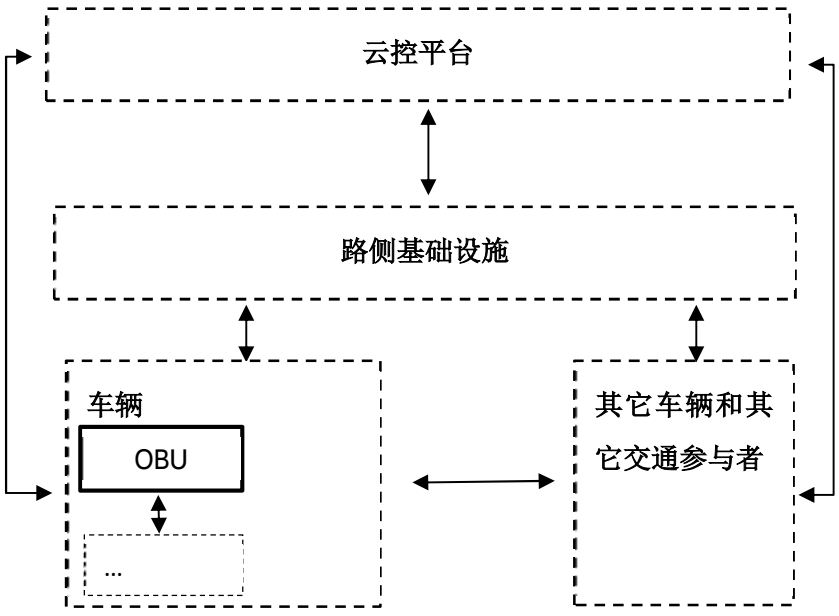

图1 OBU 交互架构示意图

5.2 车云交互

OBU 支持车云交互时，要求如下：

a) 应使用 EUHT、4G/5G 蜂窝等通信链路与云控平台通信；
b) 应支持 TCP/UDP、超文本传输协议（HTTP）/超文本传输安全协议（HTTPS）、消息队列遥测传输协议（MQTT）等不同层级通信协议；
c) 交互数据格式宜采用 JS 对象简谱（JSON）、Protobuf 等格式；
d) 应能按照不小于 10Hz 的频率采集车辆运行数据，并实时上传云控平台；
e) 应支持至少 2 路视频数据采集，并将采集的视频数据上传至云控平台，实时视频流应符合 GB/T 28181 规定或符合实时消息传输协议（RTMP）协议，支持按照云控平台指令上传指定时间段内的本地存储的视频数据文件；
f) 应支持从云控平台接收交通路况、安全预警、协同决策控制等信息数据，并能将接收数据通过 CAN、以太网转发给车载计算单元或域控制器等车端装置；
g) 应具备数据重传机制，能够本地存储或缓存未及时上传云控平台的数据，并能进行数据重传。

5.3 车路、车车交互

OBU 支持车路、车车交互时，要求如下：

a) OBU 应使用 C-V2X 直连通信、EUHT 等通信链路与其他车辆、路侧基础设施等进行 V2V、V2I、V2P 等 V2X 通信。
b) OBU 应支持表 1 所述应用场景，宜支持表 2、表 3 所述应用场景，可支持扩展自定义场景。表 1、表 2 中应用场景由应用方根据实际情况确定应用层及应用数据交互标准，表 3 中应用场景按照 YD/T 3978 实现。

表1 车辆辅助驾驶 V2X 应用场景列表

序号	通信模式	应用名称
1	V2V	前向碰撞预警
2	V2V/V2I	交叉路口碰撞预警
3	V2V/V2I	左转辅助
4	V2V	盲区预警/变道预警
5	V2V	逆向超车预警
6	V2V	紧急制动预警
7	V2V	异常车辆提醒
8	V2V	车辆失控预警
9	V2I	道路危险状况提示
10	V2I	限速预警
11	V2I	闯红灯预警
12	V2P/V2I	弱势交通参与者碰撞预警
13	V2I	绿波车速引导

表1　车辆辅助驾驶V2X应用场景列表（续）

序号	通信模式	应用名称
14	V2I	车内标牌
15	V2I	前方拥堵提醒
16	V2V	紧急车辆提醒

表2　车辆协同驾驶 V2X 应用场景列表

序号	通信模式	应用名称
1	V2V/V2I	感知数据共享
2	V2V/V2I	协作式变道
3	V2I	协作式车辆汇入
4	V2I	协作式交叉口通行
5	V2I	差分数据服务
6	V2I	动态车道管理
7	V2I	协作式优先车辆通行
8	V2I	场站路径引导服务
9	V2I	浮动车数据采集
10	P2X	弱势交通参与者安全通行
11	V2V	协作式车辆编队管理
12	V2I	道路收费服务

表3　基于车路协同的典型 V2X 应用场景列表

序号	通信模式	应用名称
1	V2V/V2I	协同式感知
2	V2I	基于路侧协同的无信号交叉口通行
3	V2I	基于路侧协同的自动驾驶车辆“脱困”
4	V2I	高精地图版本对齐及动态更新
5	V2I	自主泊车
6	V2I	基于路侧感知的“僵尸车”识别
7	V2I	基于路侧感知的交通状况识别
8	V2V/V2I	基于协同式感知的异常驾驶行为识别

6　功能要求

6.1　通信功能

6.1.1　EUHT 通信

EUHT通信应满足如下要求：

a) 支持EUHT通信协议，符合YD/T 2394.2、GB/T 31024.2、GB/T 36454的要求；
b) 支持5725MHz~5850MHz频段，带宽20/40MHz，带宽、时隙配比可配置；
c) 支持网络状态、信号质量等EUHT网络情况监测；
d) 支持业务数据的广播/组播；
e) 支持网络传输指标的单向时延低于10ms、丢包率小于0.1%；
f) 支持移动性管理，包括链路质量检测、切换，系统内切换成功率大于99.9%。

6.1.2 C-V2X 直连通信

C-V2X直连通信接入层应符合YD/T 3756的要求，网络层应符合YD/T 3707的要求，消息层应符合YD/T 3709的要求。

6.1.3 4G/5G 通信

4G/5G通信应满足GB/T 43187 规定的无线通信性能要求。

6.2 空口链路选择

OBU空口链路选择仅用于车云业务，要求如下：
a) 应支持使用EUHT或4G/5G与云控平台建立通信链路；
b) 应支持优先选择EUHT链路；
c) EUHT、4G/5G链路切换过程（基于EUHT信号质量判定是否切换）业务中断间隔应小于1s；
d) OBU宜支持使用EUHT、4G/5G双链路同时进行车端数据传输。

6.3 数据存储

数据存储功能应支持本地存储视频数据、车辆运行状态数据，应满足以下要求：
a) 至少能存储 2GB 大小的视频数据，数据具有可读性；
b) 至少能存储 100MB 大小的参数类数据（从整车 CAN、以太网、OBU 采集的参数类数据）；
c) 内部存储介质存储满时，能自动循坏覆盖；
d) OBU 断电停止工作时，断电前已保存的数据不丢失；
e) 能够通过本地数据接口对存储数据导出。

6.4 定位

定位功能应满足以下要求：
a) 至少支持GNSS中的BDS、GPS；
b) 能提供经度、纬度、速度、航向、三轴加速度、三轴角速度等关键参数，更新频率不小于10Hz；
c) 能实现分米级或厘米级定位精度；
d) 支持无/弱GNSS定位。

6.5 时间同步

时间步功能应满足以下要求：
a) 时间格式遵循 UTC 标准时间格式；
b) 支持设备自身时间的保持和维护，支持通过 BDS、GPS 进行校时，时间精度优于 1ms，通过 NTP 周期校时，时间精度优于 10ms。

6.6 配置管理

OBU应具备本地和远程管理维护功能，应满足以下要求：

a）支持IP、DNS地址、路由及日志等参数配置；

b）支持出厂初始参数的恢复设置；

c）支持固件、软件升级，升级后设备无需人为操作应能正常工作；

d）支持对OBU运行状态的查询、监测；

e）支持日志导出；

f）支持OBU自身故障诊断。

6.7 自检

OBU应具备自检能力，同时具备故障存储能力，应支持故障上报云控平台。

6.8 物理接口

6.8.1 以太网通信接口

OBU以太网通信应满足以下要求：

a) 支持不少于 2 路 100/1000Base-Tx 通信；

b) 每个 LAN 口能单独配置 IP、DNS、动态主机配置协议（DHCP）Server 和 Address Pool；

c) 支持多网段配置，不同网段之间可设置数据交换或隔离；

d) 支持静态路由、策略路由，支持多路由表和规则优先级；

e) 支持通信链路的连接检测及故障恢复；

f) 支持采集车辆运行状态数据（采集频率不小于 10Hz）、车载摄像头视频数据。

6.8.2 CAN 通信接口

OBU应具备CAN接口，ISO CAN、CAN-FD至少各一路。应支持采集车辆运行状态数据（采集频率不小于10Hz）。

7 安全要求

7.1 通信安全

7.1.1 车云通信

OBU与云控平台通信时，要求如下：

a) 宜采取安全传输协议，例如传输层密码协议（TLCP）、TLS 1.2、TLS 1.3 等，保障通信数据的机密性、完整性和真实性；

b) 应具有针对网络传输的访问控制功能，例如根据源地址、目的地址、源端口、目的端口和协议等进行检查；

c) 采用的通信协议不应存在后门，应及时进行安全更新。

7.1.2 车路、车车通信

7.1.2.1 使用 C-V2X 直连通信

OBU使用C-V2X直连通信时，应满足以下安全要求：

a) 采用基于数字证书的签名机制保证直连通信消息的真实性和完整性，证书格式应符合 YD/T 3957 的规定；

b) 验证所接收到的其它直连通信设备发送的数据消息的证书、签名有效性，并且只对通过验证的数据进行处理，丢弃未通过验证的消息。

7.1.2.2 使用 EUHT 通信

OBU使用EUHT通信时，应进行终端入网鉴权认证，应通过国产商用密码算法对控制信令和数据报文进行加解密，保证控制平面关键信令以及数据平面用户报文的安全传输。

7.2 网络安全

7.2.1 防火墙

OBU应具备基于防火墙提供的网络隔离和访问控制能力，网络隔离和访问控制应能通过源/目的地址、协议、端口、MAC地址、zone等基本元素，实现对流量的允许和阻断操作。

7.2.2 Ethernet-IDPS

OBU应具备以下IDPS网络攻击检测防御功能。

a) 防御常见的网络攻击：分布式拒绝服务（DDoS）攻击（TCP（SYN）、UDP、因特网控制报文协议（ICMP）三大类）检测、端口扫描、密码爆破、挑战黑洞（CC）攻击、网络蠕虫攻击、畸形报文攻击、应用层安全漏洞攻击等攻击行为。
b) 防御ARP攻击：基于IP、MAC、端口绑定，以及MAC地址学习等机制，防范ARP欺骗和ARP拒绝服务攻击。
c) 支持记录攻击事件。

7.2.3 CAN IDPS

宜支持基于报文定义、收发关系、信息熵、帧间隔等进行报文检测与行为检测，宜支持统一诊断服务（UDS）会话检查。

7.3 数据安全

7.3.1 数据完整性与真实性

OBU应能保证数据的完整性和真实性，要求如下：

a) 采用身份鉴别等机制，保证采集数据来源的真实性；
b) 采用数据校验等机制，保证采集数据的完整性；
c) 采用附加消息鉴别码或数字签名方式实现数据传输的完整性保护；
d) 采用有效校验技术和密码技术确保重要数据存储过程中的完整性，并在检测到完整性错误时采取必要的恢复措施。

7.3.2 数据机密性

OBU应能保证数据机密性，要求如下：

a) 保证采集数据的机密性，可采用加密等机制；
b) 采用密码技术实现系统管理数据、鉴别数据和其他重要数据传输的机密性；
c) 鉴别数据如采用密码技术，应采用安全机制（如安全芯片或密码模块等）进行保护；
d) 重要数据存储在安全区域或以密文形式存储；
e) 对数据发送方和接受方实施身份认证，在建立连接前，利用密码技术进行初始化会话验证，必要时采用专用传输协议或安全协议服务（TLS 1.2 及以上），避免来自基于协议的攻击和破坏。

7.4 系统安全

7.4.1 安全启动

OBU应能安全启动，要求如下：

a) 基于可信根对系统引导程序、系统程序等进行可信验证，确保加载的固件是可信的，以防止刷机、离线注入、篡改；
b) 通过可信根实体对安全启动所使用的可信根进行保护，可信根实体包括可信平台模块（TPM）、可信密码模块（TCM）、可信平台控制模块（TPCM）等。

7.4.2 安全调试

具备安全机制保障对OBU的调试，要求如下：

a) 硬件 PCB 不应存在后门或隐蔽接口；
b) 硬件 PCB 的调试接口应禁用或设置安全访问控制；
c) 安全芯片或硬件密码模块应与单个设备唯一绑定，防止恶意拆解。

7.5 软件升级安全

7.5.1 OTA 安全

OTA安全要求如下：

a) OTA通道应加密，并通过可信的OTA升级包和可信的签名信息进行安全升级；
b) OBU和在线升级服务器应进行身份认证，验证身份的真实性；
c) OBU的升级系统应对下载的在线升级包进行真实性和完整性校验；
d) OBU的升级系统应记录在线升级过程中发生的失败事件日志；
e) OBU升级失败时，应确保将系统恢复到最近的可用版本或将系统置于安全状态。

7.5.2 本地连接升级安全

OBU通过本地连接升级时，安全要求如下：

a) 若 OBU 使用升级系统进行本地连接升级，应对升级包真实性和完整性进行校验；
b) 若 OBU 不使用升级系统进行本地连接升级，应采取防护措施保证刷写接入端的安全性，或者校验被刷文件的真实性和完整性；
c) OBU 升级失败时，应确保将系统恢复到最近的可用版本或将系统置于安全状态。