CS
CCS 点击此处添加 CCS 号

# DB11

# 北　京　市　地　方　标　准

DB 11/T XXXX—XXXX

# 车路云一体化
# 车载单元应用技术要求

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

（征求意见稿）

**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。**

XXXX－XX－XX 发布　　XXXX－XX－XX 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：

本文件主要起草人：

# 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 车载单元应用技术要求

## 1 范围

本文件规定了车路云一体化技术路线下车载单元（OBU）应用系统交互要求、功能要求和安全要求。

本文件适用于车路云一体化技术路线下车载单元（OBU）的设备选型和服务场景应用。

## 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 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

YD/T 2394.2-2012 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

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**云控平台 cloud control platform**

由云控基础平台以及云控应用组成。云控基础平台汇聚车辆和道路交通动态信息，融合地图、交管、气象和定位等平台的相关数据，进行综合处理后，以标准化分级共享的方式支撑不同时延要求下的云控应用需求。在此基础上建立面向智能网联汽车产业的云控应用，可以为车辆增强安全、节约能耗以及提升区域交通效率提供服务。

3.2

**车载单元 on-board unit, OBU**

指安装在智能网联汽车上，搭载一定应用系统及功能模块，具备EUHT、C-V2X(直连通信 PC5)、4G/5G蜂窝的联网功能、高精度定位功能、数据采集、数据存储、数据传输、安全防护等功能的车载单元OBU设备。产品形态可以是单体式或集成式车载单元。单体式车载单元指单独设计为独立的装置或系统的车载单元；集成式车载单元指集成设计在车辆其它装置或系统的车载单元。

3.3

**增强型超高吞吐 enhanced ultra-high throughput(EUHT)**

物理层及媒体接入控制层满足YD/T 2394.2-2012规定的无线通信技术。

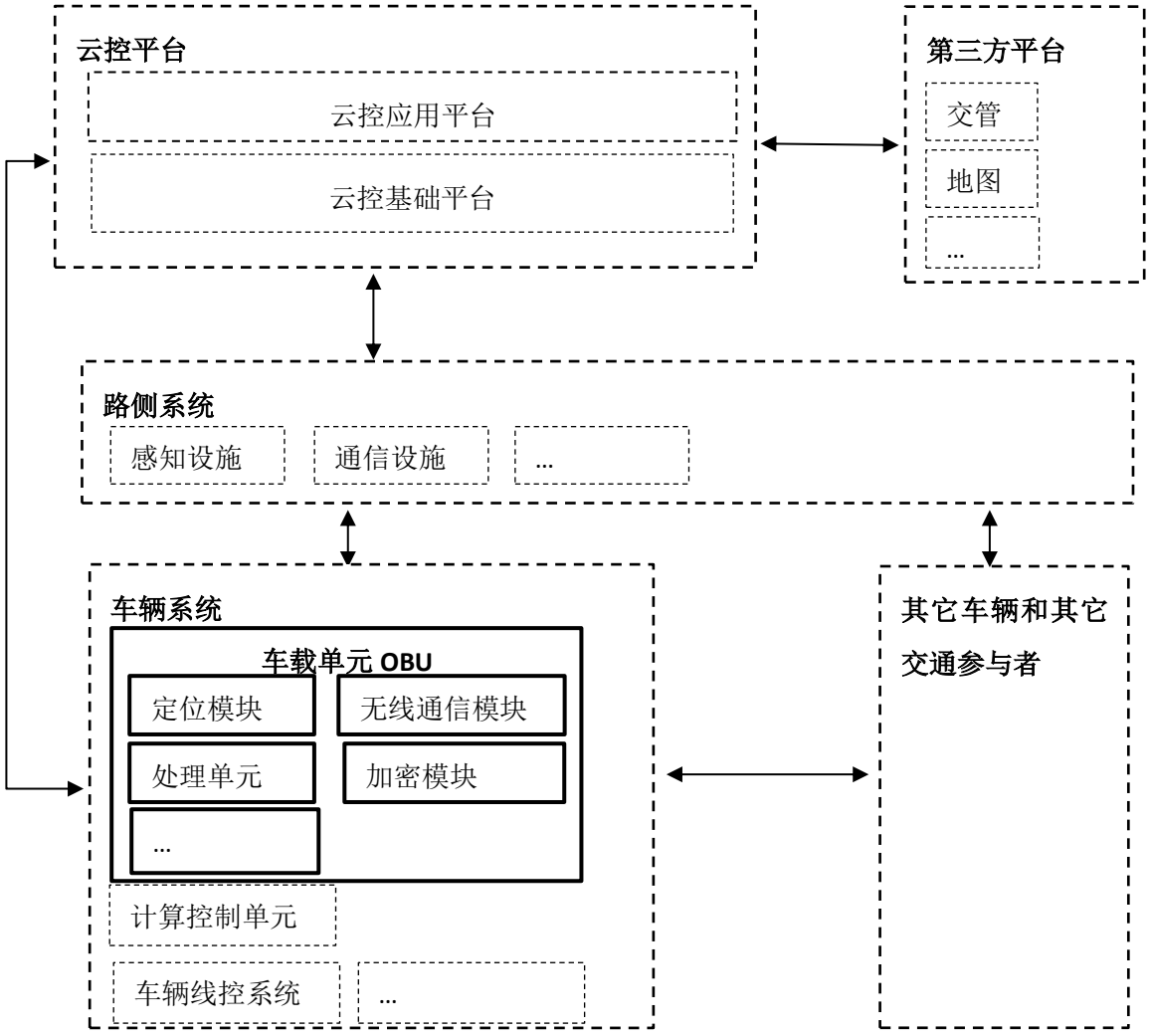
## 4 缩略语

下列缩略语适用于本文件。

AP：无线接入点（Access Point）
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）
CC攻击: 挑战黑洞(Challenge Collapsar)攻击
DDoS 分布式拒绝服务攻击(Distributed Denial of Service)
DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）
DNS：域名解析系统（Domain Name System）
EUHT：增强型超高吞吐（Enhanced Ultra High Throughput）
ICMP: 因特网控制报文协议（Internet Control Message Protocol）
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）
GNSS：全球导航卫星系统（Global Navigation Satellite System）
GPS：全球定位系统（Global Positioning System）
HTTP: 超文本传输协议（Hyper Text Transfer Protocol)
JSON: JS对象简谱（JavaScript Object Notation）
MAC 媒体接入控制（Media Access Control）
MQTT: 消息队列遥测传输协议（Message Queuing Telemetry Transport）
OBU：车载单元（On-Board Unit）
OTA：空中下载技术（Over-the-Air Technology）
PCB: 印制电路板（Printed Circuit Board）
Protobuf: 一种序列化数据描述语(Protocol Buffers)
RTK：实时差分定位（Real - time kinematic）
RTMP：实时消息传输协议（Real Time Messaging Protocol）
RTSP：实时流传输协议（Real-Time Streaming Protocol）
TCM 可信密码模块（Trusted Cryptography Module）
TCP 传输控制协议（Transmission Control Protocol）
TLS：安全传输层协议（Transport Layer Security)
TPM: 可信平台模块（Trusted Platform Module）
TPCM: 可信平台控制模块（Trusted Platform Control Module）
TLCP: 传输层密码协议（Transport layer cryptography protocol）
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）
SSH: 安全外壳协议（Secure Shell）
UDP 用户数据报协议（User Datagram Protocol）
UDS：统一诊断服务（Unified diagnostic services）
3GPP：第三代合作伙伴计划(3rd Generation Partnership Project)

## 5 系统架构

车路云一体化系统架构示意图如图1所示，主要包括云控平台、路侧系统、车辆系统等部分。本文件针对车辆系统中的车载单元OBU的应用技术提出要求，支撑基于OBU的业务应用。车载单元OBU主要包括定位模块、无线通信模块、处理单元、加密模块等。车载单元OBU作为车辆系统的一部分，支撑车辆系统与云控平台、路侧系统、其它车辆和其它交通参与者等之间通信。




**注：**实线框表示车载单元的组成;虚线框表示与车载单元有关的系统。

**图1 车路云一体化系统架构示意图**

# 6 系统交互要求

## 6.1 车云交互

车载单元 OBU 使用 EUTH、4G/5G 蜂窝等通信链路，与云控平台通信，车载单元 OBU 应满足以下要求：

a) 支持通过 CAN、以太网采集车辆运行状态数据（数据采集频率不小于 10Hz），并将采集的车辆运行状态数据实时上传至云控平台，应用协议宜采用 JSON、Protobuf 等数据格式。

b) 支持至少 2 路视频数据采集，并将采集的视频数据实时上传至云控平台，实时视频流符合 GB/T 28181 规定或符合 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。

c) 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。

d) 支持 TCP/UDP、HTTP/HTTPS、MQTT 等不同层级通信协议。

e) 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，并进行数据重传。

## 6.2 车路、车车等交互

车载单元 OBU 使用 C-V2X（直连通信 PC5)、EUHT 等通信链路，与其他车辆、路侧智能基础设施进行 V2V、V2I 等车路协同应用通信。车载单元 OBU 应支持表 1 所述应用场景，宜支持表 2 所述应用场景，并能够支持扩展自定义场景。表 1、表 2 中应用场景的交互协议根据应用方实际情况确定，其中表 2 中的部分应用场景可参考 YD/T 3978 实现。

**表1 第一阶段 V2X 应用场景列表**

| 序号 | 主要通信方式 | 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-Event | 紧急制动预警 |
| 7 | V2V-Event | 异常车辆提醒 |
| 8 | V2V-Event | 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 |
| 14 | V2I | 车内标牌 |
| 15 | V2I | 前方拥堵提醒 |
| 16 | V2V | 紧急车辆提醒 |

表2　第二阶段 V2X 应用场景列表

| 序号 | 主要通信方式 | 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 |
| 13 | V2V/V2I | 协同式感知 |
| 14 | V2I | 基于路侧协同的无信号交叉口通行 |
| 15 | V2I | 基于路侧协同的自动驾驶车辆脱困 |
| 16 | V2I | 高精地图版本对齐及动态更新 |
| 17 | V2I | 自主泊车 |
| 18 | V2I | 基于路侧感知的“僵尸车”识别 |
| 19 | V2I | 基于路侧感知的交通状况识别 |
| 20 | V2V/V2I | 基于协同式感知的异常驾驶行为识别 |

# 7　功能要求

## 7.1　通信功能

### 7.1.1　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、GB/T 36454的规定；
b)　支持5725-5850MHz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，支持非法广播的抑制；
e)　支持终端入网鉴权认证，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；
f)　支持网络传输指标的单向时延低于10ms、丢包率小于0.1%；
g)　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%。

### 7.1.2　C-V2X 直连通信

C-V2X直连通信应能满足如下基本要求：

a) 通信距离：≥400m（空旷无遮挡环境下,丢包率小于 10%）；
b) 工作频段：5905-5925 MHz；
c) 工作带宽：20 MHz；
d) 发送功率：最大 23±2 dBm。

整体来说，C-V2X 接入层应满足 YD/T 3756 的要求，网络层应满足 YD/T 3707 的要求，消息层应满足 YD/T 3709 的要求。

### 7.1.3 4G/5G 通信

4G/5G通信应满足如下要求：
a) 支持4G或5G通信，具备向下兼容能力；
b) 支持监控连接状态、延时监控、运营商信息（运营商/信号强度/网络类型/网络频段/信道）等内容。

### 7.1.4 Wi-Fi 通信

Wi-Fi通信应满足如下要求：
a) 支持IEEE802.11 b/g/n/ac协议，支持2.4GHz、5GHz频段通信；
b) 支持将Wi-Fi切换为AP模式、以便提供访问OBU设备局域网的服务；
c) 支持将Wi-Fi切换为STA模式、以便OBU设备局域网内设备可以访问连接的本地网络。

## 7.2 空口链路选择

支持车云业务时，为保证业务的连续性，OBU空口链路选择应满足以下要求：
a) OBU应支持使用EUHT或4G/5G与云控平台建立通信链路；
b) 支持优先选择EUHT链路；
c) 基于当前的链路信号质量状态，选择最优网络链路；
d) EUHT、4G/5G链路切换过程，业务中断间隔小于1s；
e) OBU宜支持使用EUHT、4G/5G双链路同时进行某些车端数据传输。

## 7.3 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，应符合下列要求：
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 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) 车载单元 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。

## 7.4 定位

OBU应具备定位功能，应满足以下要求：
a) 应至少支持BDS、GPS；
b) 提供经度、纬度、高程、速度、方向以及时间等关键参数，更新频率不小于10HZ；
c) 宜支持GCJ-02坐标系；
d) 车载单元OBU应能实现分米级或厘米级定位精度；
e) 车载单元OBU应能输出三轴加速度、三轴角速度参数信息；
f) 应支持应支持无/弱GNSS定位。

### 7.5 时间同步

车载单元OBU应具备时间步功能，应满足以下要求：

a) 时间格式遵循 UTC 标准时间格式，时间起始为 1970 年 1 月 1 日 0 点 0 分；

b) 支持设备自身时间的保持和维护，支持通过北斗、GPS 进行校时，时间精度不大于 1ms；通过 NTP 周期校时，时间精度不大于 10ms。

### 7.6 配置管理

OBU应具备本地和远程管理维护功能，支持参数配置与查询、恢复出厂设置、软件升级、运维管理及日志等系统管理功能，满足以下要求：

a)应支持IP、DNS地址、路由及日志等参数配置；

b)应支持出厂初始参数的恢复设置；

c)应支持固件、软件升级，升级后设备无需人为操作应能正常工作。升级过程中出现因网络或其原因出现他中断时，应能回退到旧版本，重启后能正常工作；

d)应支持对OBU运行状态的查询、监测；

e)应支持日志导出；

f)应支持OBU自身故障诊断。

### 7.7 自检

车载单元OBU应具备自检能力，同时具备故障存储能力，支持故障实时上报至云控平台。

### 7.8 物理接口

#### 7.8.1 以太网通信接口

以太网通信应满足如下要求：

a) 不少于 2 路 100/1000Base-Tx 通信；

b) 每个 LAN 口可单独配置 IP/DNS/DHCP Server&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，为重要车载部件的高级别通信要求提供保障；

e) 支持通信链路的连接检测及故障恢复。

#### 7.8.2 CAN 通信接口

CAN通信应具备CAN接口。ISO CAN、CAN-FD至少各一路。

## 8 安全要求

### 8.1 通信安全

#### 8.1.1 车车、车路通信

使用直连通信（C-V2X PC5 接口）时，应满足以下安全要求：

a) 应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，证书格式遵循 YD/T 3957；

b) 应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有效性，及签名有效性，并且只对

通过验证的数据进行进一步的处理；未通过验证的消息将被丢弃。

### 8.1.2 车云通信

与云控平台之间的网络通信时，应满足如下网络传输安全要求：

a) 宜采取安全传输协议，例如 TLCP、TLS 1.2、TSL 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。

## 8.2 网络安全

### 8.2.1 防火墙

OBU需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可通过源/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。

### 8.2.2 Ethernet-IDPS

OBU设备应具备以下IDPS网络攻击检测防御功能：

a) 防御常见的网络攻击：DDoS攻击（TCP(SYN)、UDP、ICMP三大类）检测、端口扫描、密码爆破、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) 支持攻击事件的日志记录。

### 8.2.3 CAN IDPS

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，支持UDS会话检查。

## 8.3 数据安全

### 8.3.1 数据完整性与真实性

OBU应能保证数据的完整性和真实性，应满足以下要求：

a) 可采用身份鉴别等机制，保证采集数据来源的真实性；

b) 可采用数据校验等机制，保证采集数据的完整性；

c) 可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) 应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。

### 8.3.2 数据机密性

OBU应能保证数据机密性，应满足以下要求：

a) 应保证采集数据的机密性，可采用加密等机制；

b) 应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) 重要数据应存储在安全区域或以密文形式存储；

e） 应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。

## 8.4 系统安全

### 8.4.1 安全启动

OBU应能保证安全启动，应满足以下要求：

a） 可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，防止刷机，防止离线注入、篡改；

b） 可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 TPM、TCM、TPCM 等。

### 8.4.2 安全调试

具备安全机制用于保护对OBU设备的调试，包括但不限于以下方面：

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。

## 8.5 安全 OTA

在线升级安全要求：

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设备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设备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设备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设备升级失败时，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。

离线升级安全要求：

a） 若 OBU 设备使用升级系统进行离线升级，应对离线升级包真实性和完整性进行校验；

b） 若 OBU 设备不使用升级系统进行离线升级，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 设备升级失败时，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。