ICS
CCS

团　　体　　标　　准

T/KJDL 020-2022

商用车辆辅助驾驶安全及数据平台

Commercial Vehicle Assisted Driving Safety and Data Platform

2022 -12-30 发布　　2022-12-30 实施

广 东 省 车 联 网 产 业 联 盟
广州市空间地理信息与物联网促进会　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。

本文件由珠海骏驰智联科技有限公司和广州市空间地理信息与物联网促进会提出。

本文件由广州市空间地理信息与物联网促进会归口。

本文件起草单位：珠海骏驰智联科技有限公司、移动通信国家工程研究中心、广州市晶华精密光学股份有限公司、名商科技有限公司、广州通达汽车电气股份有限公司、北京驭安科技有限公司、广东产品质量监督检验研究院、联通智网科技股份有限公司、涟漪位置（广州）科技有限公司、中电车联信安科技有限公司、广州大道信息科技有限公司、东莞市粤熙实业有限公司、奇安信科技集团、广州市空间地理信息与物联网促进会、广东省车联网产业联盟。

本文件主要起草人：刘化龙、罗广、江志洲、曹绍芬、罗高翔、石光明、胡义发、连春央、陈智杰、宋海娜、宋鑫、胡文祥、秦涤、雷明、岳浩、谢俊彤、刘可儿、阙秀震、许斯亮。

商用车辆辅助驾驶安全及数据平台

1 范围

本文件规定了商用车辆辅助驾驶安全监管数据要求，包含车端的辅助驾驶数据安全要求和远程平台的网络安全要求。

本文件适用于安装有高级辅助驾驶系统的运营车辆、特种车辆（环保车、救护车、消防车等）及管理系统，其他商用车辆系统参照执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的，凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本适用于本文件。

GB/T 38186-2019 商用车辆自动紧急制动系统性能要求及试验方法

GM/T 0064 基于数字证书的身份接口规范

JT/T 808-2019 道路运输车辆卫星定位系统终端通信协议及数据格式

JT/T 1242-2019 营运车辆自动紧急制动系统性能要求及测试方法

TC260-001 汽车采集数据处理安全指南

T/GDRTA 001-2020 道路运输车辆智能视频监控报警系统终端技术规范

T/KJDL 001-2019 营运车辆智能网络终端通用技术规范

3 术语和定义、缩略语

下列术语和定义适用于本文件。

3.1 术语和定义

3.1.1

自动紧急制动系统 advanced emergency braking system

实时监测车辆前方行驶环境，并在可能发生碰撞危险时自动启动车辆制动系统使车辆减速，以避免碰撞或减轻碰撞的系统。

[来源：JT/T 1242-2019，3.1.1]

3.1.2

被试车辆 subject vehicle

按照本文件的要求，进行试验的车辆。

[来源：GB/T 38186-2019,3.2]

3.1.3

目标 target

路上行驶的所有机动车辆，非机动车辆且适合辅助驾驶传感探测特征的代表物体。

[来源：GB/T 38186-2019,3.3]

3.1.4

移动目标 moving target

在被试车辆行驶前方同一车道中央，以恒定速度同向移动的目标。

[来源：GB/T 38186-2019,3.4]

3.1.5

静止目标 stationary target

在被测试车辆行驶前方同一车道中央保持不动的目标。

[来源：GB/T 38186-2019,3.5]

3.1.6

柔性目标 soft target

用于模拟普通乘用车且在发生碰撞时对自身及被试车辆危害最小的目标。

[来源：GB/T 38186-2019,3.6]

3.1.7

碰撞预警阶段 collision warning phase

从车辆向驾驶发出前方可能发生碰撞的预警开始到车辆紧急制动以前的阶段。

[来源：GB/T 38186-2019，3.8]

3.1.8

自检 self-check

在高级辅助驾驶系统启动以前通过半连续方式对辅助驾驶系统失效进行自动检查、测试其功能的行为。

[来源：GB/T 38186-2019,3.10]

3.1.9

预计碰撞时间 time to collision TTC

被试车辆与目标之间的距离除以被试车辆与目标瞬间相对车速所得出的时间。

[来源：GB/T 38186-2019,3.11]

3.1.10

完好性 completeness

完好性是当高级辅助驾驶系统由于故障而不能提供满足要求的功能时，系统能够在系统自检完成后5S 内向用户告警的能力。

3.1.11

位置轨迹数据 location track data

位置轨迹数据指的是基于卫星定位、通信网络等方式获取的汽车定位和途径路径相关的数据。

[来源：TC260-001,4 d）]

3.1.12

座舱数据 cockpit Data

座舱数据指的是通过摄像头、红外传感器、指纹传感器、麦克风等传感器从汽车座舱采集的数据，以及对其进行加工后产生的数据；座舱数据包含驾驶员和乘员的人脸、声纹、心率等敏感个人信息，不包括对汽车采集数据处理产生的操控记录数据。

[来源：TC260-001,4 b）]

3.1.13

车外数据 out-of-vehicle data

车外数据指的是通过摄像头、雷达等传感器从汽车外部环境采集的道路、建筑、地形、交通参与者等数据，以及对其进行加工后产生的数据。交通参与者指参与交通活动的人，包括机动车、非机动车、其他交通工具的驾驶员与乘员，以及其他参与交通活动相关的人员。车外包括人脸、车牌等个人信息以及车辆流量、物流等法律法规规定的重要数据。

[来源：TC260-001 4 a）]

3.1.14

运行数据 operation data

运行数据指的是通过车速传感器、温度传感器、轴转速传感器、压力传感器等从动力系统、底盘系统、车身系统、舒适系统等电子电气系统采集的数据。

[来源：TC260-001 4 c）]

3.1.15

控制指令 control commands

控制指令指的是具有控制汽车功能特性的指令、动作、功能。

3.1.16

诊断指令 diagnostic Instructions

诊断指令指的是具有远程对车机进行调试诊断能力的指令数据。

3.2 缩略语

AEBS:自动紧急制动系统（advanced emergency braking system）
TTC：预计碰撞时间 （time to collision）
ADAS:高级辅助驾驶系统（Advanced Driving Assistance System）
SSL:数字证书（Secure socket layer）
SIP:会话初始协议（Session Initiation Protocol）
VPC:虚拟机（Virtual PC）
EIP:企业信息门户（Enterprise Information Portal）

4 一般要求

4.1 商用车辆辅助驾驶系统

商用车辆辅助驾驶系统（Advanced Driving Assistance System）是利用安装在车上的各式各样传感器（毫米波雷达、激光雷达、单\双目摄像头以及卫星导航），在汽车行驶过程中感应周围环境与驾驶员的面部特征、收集数据，进行静态、动态物体的辨识、侦测与追踪，并结合导航地图数据，进行运算与分析，预先让驾驶者察觉到可能发生的危险，执行降速保距，变道避险等有效增加汽车驾驶的舒适性和安全性。行驶过程中触发的前向目标风险数据、右侧目标风险数据、驾驶员行为数据、系统执行数据上传到数据平台，为车辆的安全管理提供闭环佐证。典型框图如图 1 所示。

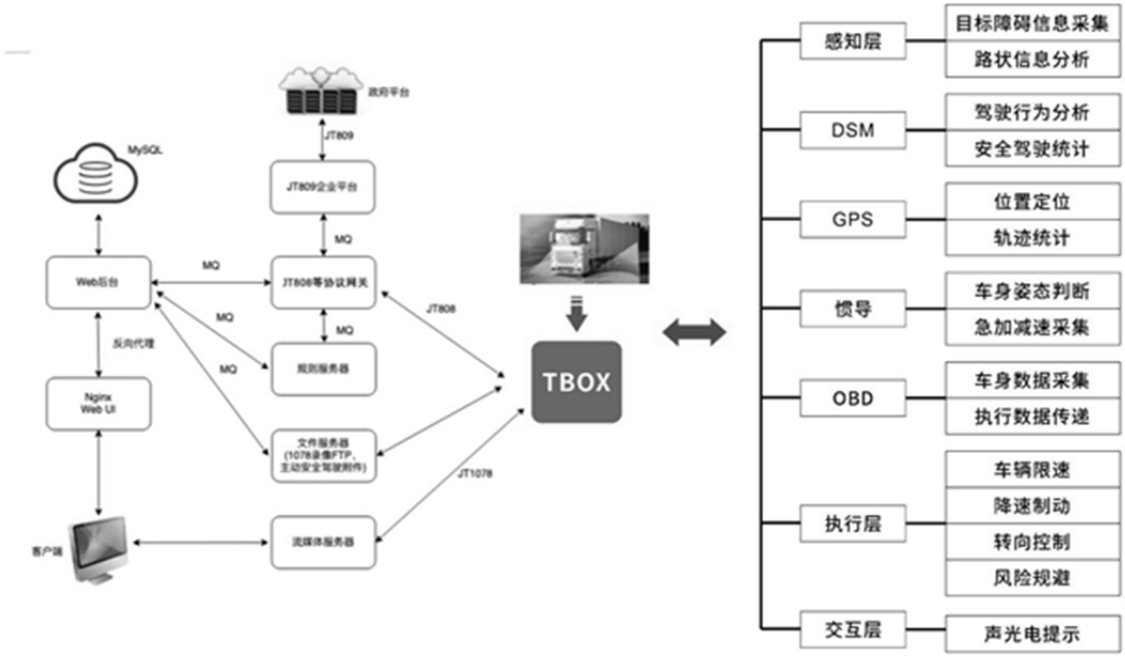


图1 辅助驾驶系统功能框图

针对疲劳监测、语音识别、远程控车等高级辅助驾驶系统功能收集的个人敏感信息基于数据全生命周期应采用技术手段进行保护，包含：收集个人信息征得同意、传输加密保护、双向认证、人脸车牌匿名化处理、存储加密等技术手段。

针对使用高级辅助驾驶系统提供驾乘服务的车辆，需使用脱敏的匿名通讯技术建立司乘专用联系通道，既可以达成完成服务的目的，又可以实现对司乘手机号等个人信息的保护，如使用临时第三方号码通信。

高级辅助驾驶系统应尽可能封禁 USB、JTAG 等调试接口以及其它隐藏的免授权非加密远程接入方式。

4.1.1 商用车辆辅助驾驶安全设备应满足《GB/T 38186-2019 商用车辆自动紧急制动系统（AEBS）性能要求及测试方法---第四部分技术要求》。

4.1.2 商用车辆辅助驾驶安全设备应满足前方探测的传感器为 77G 毫米波、算法视觉镜头、多线激光

中的任意两种；探测的最大距离不小于 160m，探测的最小距离不应大于 2m，对行人的探测距离不应小于 60m。

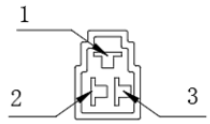
4.1.3　商用车辆辅助驾驶安全设备应满足《T/GDRTA 001-2020 道路运输车辆智能视频监控报警系统终端技术规范》5.2 高级驾驶辅助功能、5.3 驾驶员状态监测与报警功能的要求。

4.1.4　商用车辆辅助驾驶安全设备应满足《T/GDRTA 001-2020　道路运输车辆智能视频监控报警系统终端技术规范》5.4.6 右盲区监测报警制动功能的要求，商用车辆右盲区通过安装角雷达与视觉镜头检测盲区的行人与非机动车辆，当行人出现在 1m—2m 之间启动报警,行人出现在车辆盲区 1m 范围以内，设备启动制动降速（要求车速必须小于 30km/h,且向右转弯的前提），车外通过声光报警器驱离行人。

4.1.5　商用车辆辅助驾驶安全设备可以通过 CAN 信号与汽车行驶记录仪兼容，商用车辆辅助驾驶安全设备通过 CAN 的协议将设备被触发的报警数据上传给汽车行驶记录仪，由汽车行驶记录仪统一上传平台，商用车辆辅助驾驶安全设备对接汽车行驶记录仪指定 CAN 接口 CANH,CANL 。

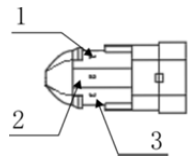
4.1.6　商用车辆辅助驾驶安全设备对接原车或者汽车行驶记录仪的电源端口如表 1：电源端口定义。

表1　电源端口定义

端口图片	端子型号	脚位	功能	规格	备注
	DJ7031-6.3-11	1	电源-	线径1mm^2	电流≥4A
		2	电源+	线径1mm^2	电流≥4A
		3	ACC	线径0.5mm^2	电流≥2A

商用车辆辅助驾驶安全设备对接原车的车身转向触发的端口如表二:转向触发端口定义。

表2　转向触发端口定义

端口图片	端子型号	脚位	功能	规格	备注
	282105-1	1	右转向信号	线径0.5mm^2	电流≥1A
		1	右转向信号	线径0.5mm^2	电流≥1A
		1	右转向信号	线径0.5mm^2	电流≥1A

4.1.7　商用车辆辅助驾驶安全设备上传数据平台的信息至少包括：自车车速、目标车距、车辆轨迹、报警点的车辆定位、前向 ADAS 图片及 10s 小视频，DSM 图片及 10s 小视频，开始触发报警的时间及车速、结束报警的时间及车速、事件类型、AEBS 制动时长、盲区触发图片等。

4.1.8　商用车辆辅助驾驶安全设备具备本地存储功能，针对触发车辆制动的信息要求保存 10 万条。

4.1.9　商用车辆辅助驾驶安全设备具备后向来车提醒功能，后向来车进入到探测的报警范围，设备触发后向报警指示牌，提醒后方车辆保持安全距离；设备自动切屏显示后向场景，提醒驾驶员后方危险。

4.1.10　商用车辆辅助驾驶安全设备本地存储的 SD 卡、TF 卡必须具备防拆卸设计，未经许可或授权无法获取数据。

4.2　车辆安装布线

4.2.1　取电原则

车辆常火线取电在 ACC 之前，不受仪表盘上所有开关控制，考虑到终端负载要求，要求在主电源上取电。控火线受 ACC 开关控制，搭铁线在车辆的主搭铁线上取电。

4.2.2　布线原则

应和原车线路一致并固定做到整套线路布置整洁和隐蔽，并用防潮绝缘胶布将功能线包好，禁止误接或错接，确保终端的每个功能正常工作。根据连接信号、电源接线的位置，把主机信号线接好并固定牢靠。外接引线必须加波纹套管随汽车线路走向固定，避免接触汽车发动机等高温部位。连接线时需要

将线穿孔绞接，缠绕圈数不少于 5 圈，包胶布时要防止线芯刺穿胶布导致短路。要求接线要结实，不能起削，不能松散，以防线路发热引发后患。每个接线头不能紧靠线的根部，至少距离 20 厘米，保留维护修理的空隙。

4.2.3 接线要求

终端报警时所对应的触发报警速度阈值与分级报警速度阈值均采用以脉冲速度为主，卫星定位速度为辅，同时车道偏离报警应关联左、右转向灯信号，终端接线要求至少接常电、ACC、地线、脉冲速度、左转向灯、右转向灯、刹车、等信号线。

4.2.4 安装后检验

终端安装标定完成后，应在空旷场地对设备进行上电测试，检测应遵循以下原则：

a) 终端安装完成后，不应增加车辆状态异常，异常包含车辆不能正常启动，发动机故障以及其它车辆功能性故障；
b) 终端自身工作正常，可正常定位，并连接到监控中心，监控中心可接收终端定位数据，查看设备实时视频；
c) 终端智能视频监控报警功能工作正常。

4.2.5 标定方法

安装完成后，按照辅助驾驶安全系统的要求，将雷达或激光与镜头的位置关联关系按图 2 标定正视图、图 3 标定侧视图进行配置，配置完成后将生成的文件升级到镜头，重启系统。

图2 标定正视图

图3　标定侧视图

4.2.6　功能测试

商用车辆辅助驾驶安全系统功能测试应满足：T/GDRTA 001—2020 中 8.2 高级驾驶辅助系统测试 、8.3 驾驶员状态监测与报警测试，GB/T38186-2019 中 5.4、5.5 的功能测试要求。

4.3　远程平台

远程平台基于无线网络对各类车辆进行集中管理,监控的系统;以高品质，高效率的集中化,分布式网络管理为架构,以视频,音频,数据等多媒体信息的网络传输为基础,为用户执行实时监视,GPS 定位,录像存储,车辆调度及报警预警,AEBS 制动降速的安全防范工作,满足车辆用户对车辆在地图上的实时监控,提供历史轨迹数据的查询和回放,对报警和处警进行统一管理,分析和呈现用户需要的各种报表;作为企业平台接入到政府平台,为上级平台需要的各种数据提供上行下发的通道。图 4 为商用车辆辅助驾驶系统远程平台框图。

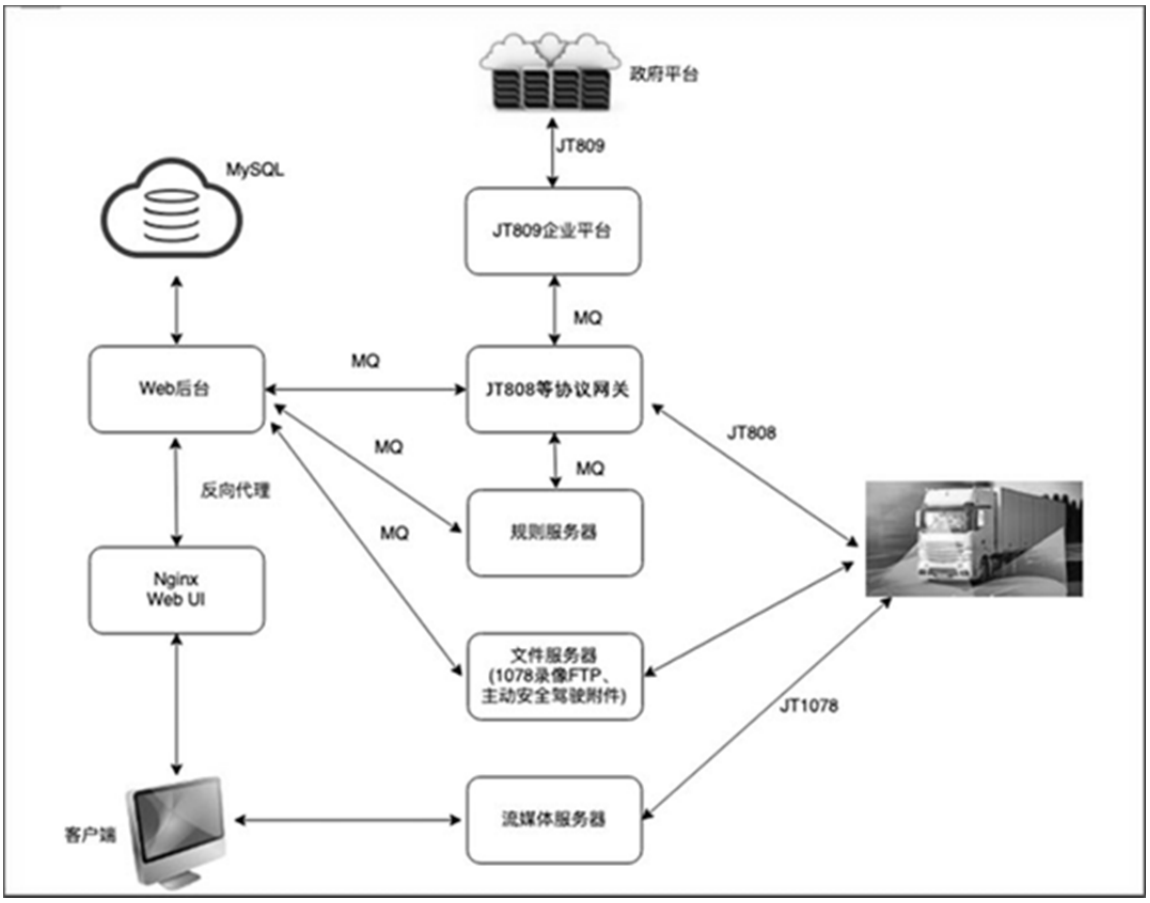


图4　商用车辆辅助驾驶系统远程平台框图

5　辅助驾驶数据安全要求

5.1　车端数据的安全要求

5.1.1　高精度定位数据应满足如下安全要求

a)　身份认证安全要求。车端设备应基于高精度定位服务商提供的数字证书完成身份认证接收高精度定位数据，保证终端设备身份的合法性与唯一性；
b)　数据传输网络安全要求。通过网络传输数据产品时，应保证数据传输链路加密，避免网络攻击；

c） 地理信息安全要求。车端高精度定位数据采集、处理、应用应符合 GB 20263 的标准要求，车端高精度定位数据存储应保存在车端本地，保证地理信息安全；
d） 高精度定位数据完好性要求。高精度定位数据需具备完好性和可检验性。

5.1.2 应尽可能少的本地存留个人敏感数据，并限制该部分数据的存储量和保留时间，禁止本地明文存储支付密码等个人关键及敏感信息数据；关键及敏感个人数据应加密存储。

5.1.3 数据传输的安全要求

a） 进行数据传输前，应建立双向 SSL 通道；
b） 所有数据传输应在 SSL 通道中加密传输；
c） SSL 协议版本不低于 TLS1.2。

5.1.4 身份鉴别的安全要求

a） 应采用口令、密码技术、生物技术中的两种或两种以上组合的鉴别技术进行身份鉴别，且其中至少一种鉴别技术应采用密码技术实现；
b） 如果采用数字证书方式进行身份鉴别，应遵循《基于数字证书的身份鉴别接口规范》。

5.2 数据采集的安全要求

5.2.1 敏感个人信息存储安全要求

需采用加密等安全措施存储个人信息：
a） 对结构化的个人信息采取字段加密方式进行存储；
b） 对非结构化数据，如包含个人信息的敏感文档、图片、视频等，对整个文件进行加密。

5.2.2 敏感个人信息访问安全要求

需提供用户个人授权同意方式，经用户授权同意后才可以对车辆上敏感个人信息进行访问、修改和删除等操作。应禁止非授权访问敏感个人信息。

5.3 数据传输的安全要求

5.3.1 数据传输保密性

进行个人信息传输时应根据数据分类分级情况采用适合强度加密算法对传输通道和内容进行安全保护，并保证加密机制可防止重放、篡改、仿冒、中间人攻击及被窃听、监听等安全风险。
a） 进行数据传输前，应建立双向 SSL 通道；
b） 所有数据传输应在 SSL 通道中加密传输；
c） SSL 协议版本不低于 TLS1.2。

5.3.2 数据传输完整性保护

在进行个人信息传输时使用校验技术或密码技术，并保证可有效防止数据篡改、替换、删除、插入等非法行为。

5.3.3 数据传输可用性保护

进行个人信息传输时需采用数据真实性校验技术保证数据的可用性。

5.3.4 数据传输出境要求

车外数据、座舱数据、位置轨迹数据不应出境；运行数据如需出境，应当通过国家网信部门组织开展的数据出境安全评估。

5.3.5 数据传输网络通道

诊断指令、控制指令应采用专用的 APN 网络。

5.4 身份鉴别的安全要求

5.4.1 敏感数据访问身份认证

进行敏感个人信息访问前应优先采用人脸识别、指纹识别、声纹识别、用户口令识别、IC 卡等一种或多种认证方式，认证后可具有一定时效，时效内身份认定有效，时效过期或者主机重新点火加电后需要重新进行身份认证。

5.4.2 控制指令访问身份认证

进行控制指令功能访问前应优先采用人脸识别、指纹识别、声纹识别、用户口令识别、IC 卡等一种或多种认证方式。

5.4.3 敏感数据传输身份认证

进行敏感个人信息传输前应采用 PKI 等方式对通信两端进行双向身份认证。

5.5 数据采集的安全要求

应采用具备身份认证、访问控制、加密等安全措施的采集工具和方法，并确保数据采集过程可有效防止恶意代码或污染数据注入。

应规范数据采集渠道、数据格式、采集流程、采集方式，以免数据因不符合规范或无效，导致无法有效使用。

5.5.1 车外数据采集安全要求

采集车外数据时，应进行匿名化处理或者使用完成即行删除。

5.5.2 座舱数据采集安全要求

采集座舱数据时，需提供驾驶员和乘客同意的方式，并取得明示同意，而且个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的意愿表示。

5.5.3 高级辅助驾驶系统传感采集安全要求

高级辅助驾驶系统所需采集的车内影像、生物特征信息等，采用车端本地化处理，不上传不留存的方式处理个人信息。车企 DMS(驾驶员状态监测系统)等辅助驾驶系统功能完全在车内的控制器中完成识别。

5.5.4 位置轨迹数据采集安全要求

采集的位置轨迹数据，应采用匿名化技术防止轨迹位置信息泄露。

5.5.5 远程控制指令及诊断信息采集安全要求

车辆收集远程控制、远程诊断等功能场景下所发送的指令数据时，需提供明确告知等方式并得到用户的授权同意。

6 远程平台网络安全要求

6.1 物理和环境安全

弹性云服务器本身已初步具备可靠、安全、弹性、易用的特点。后续还可根据业务的拓展来进行云服务器的扩容、集群等操作，动态依据不同的安全要求，定制相应的安全防护机制。在默认情况下，已基本实现网络隔离、安全组规则保护、DDoS 攻击、漏洞扫描等。

6.2 通信和网络安全

图 5 说明，其主旨是通过虚拟私有云，通过 VPC 进行内部访问控制，通过 EIP 进行公网访问，每一个层级都可以依据需求创建合适的安全组规则。

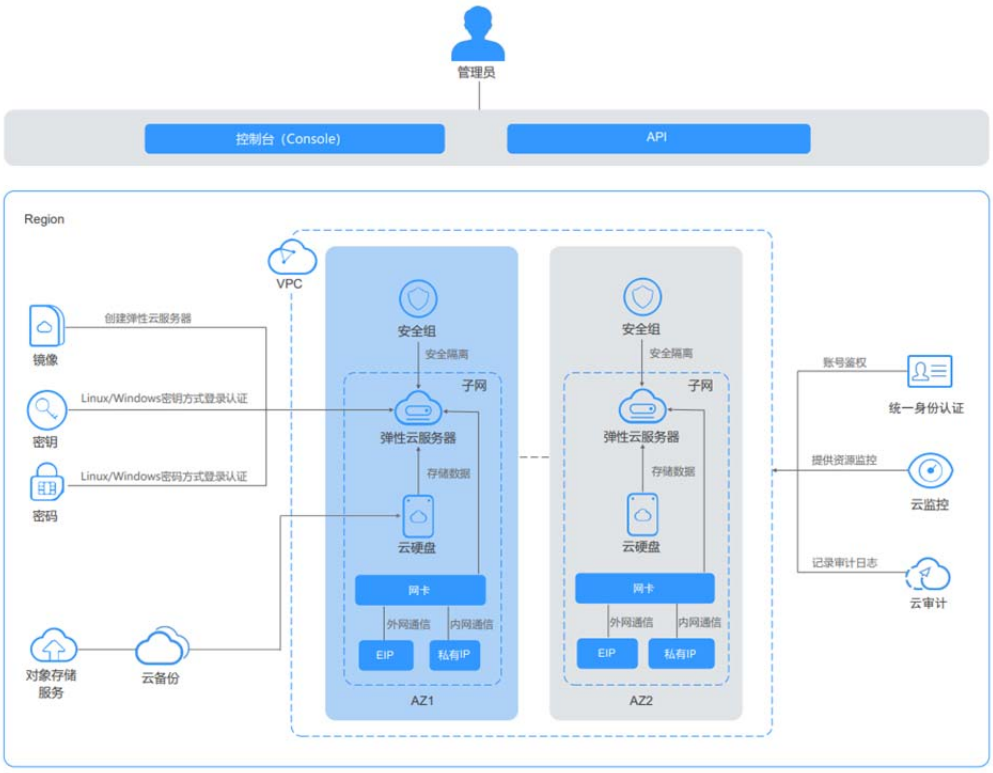


图5　网络管理拓普图

6.2.1　网络架构

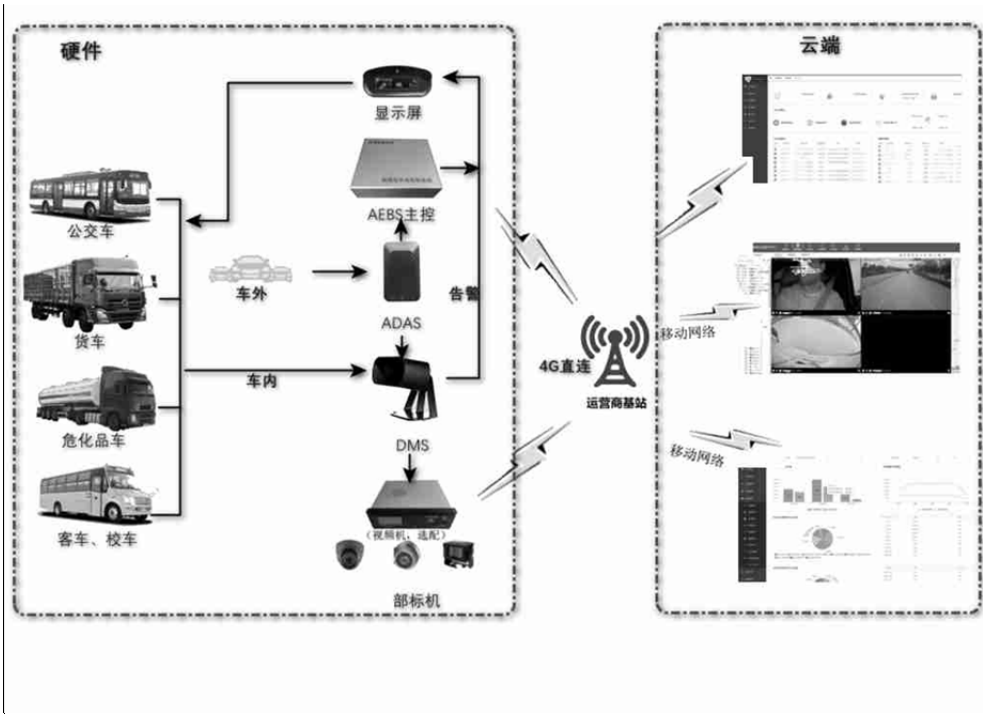


图6　网络连接图

6.2.2　通信传输

应满足如下要求:

a) 公共网络、无线网络采用传输层安全(例如 TLS)协议来保证传输的安全；
b) 对于重要行业或敏感部门，应构建可信网络环境，保证通信传输的可信性。

6.2.3 无线使用控制

本项应满足如下要求:

a) 应确保终端设备无线网络通过受控的边界防护设备接入内部网络；
b) 对于通过无线方式连接的远程监控设备，连接上采用满足相关安全标准的加密算法等，启用安全性不低于 WPA2-PSK 的安全模式，并设置连接强口令或绑定用于连接的终端（比如手机等），保证通信链路的安全性以及连接终端的合法性。

6.2.4 接入安全

本项应满足如下要求：

a) 应对接入设备采取接入身份认证措施，保证接入监控网络的设备身份合法性；
b) 应具备对非授权的远程监控设备私自联到内部网络的行为进行限制或检查的能力，一旦有未经认证的的设备试图接入时，应能够及时发现非法接入的设备源地址，向网络管理员告警， 并及时阻挡；
c) 应具备接入认证失败的处理能力，当认证应答超过规定时限时，应能终止与待接入对象之间的当前会话；当经过一定次数的认证失败后，应能终止认证会话的尝试，并在一定的安全时间间隔后才能恢复；
d) 应支持对接入设备的远程配置管理，应对设备接入通信网采取访问控制机制和安全策略，应通过 ACL 方式控制接入设备对通信网的访问；
e) 接入设备应根据不同情况采用不同的认证方式；
f) 对非 SIP 设备，宜通过设备代理来进行认证；
g) 对标准 SIP 可信设备，应采用数字证书的认证方式；
h) 对于各生产厂商设计的私有接入协议，宜符合 JT/T 808 中的相关要求。
i) 应对设备接入安全事件进行日志审计，日志内容应至少包含日期和时间、事件类型，事件主体和事件描述，成功或失败信息。

6.3 应用和数据安全

6.3.1 数据保密性

对于信令数据的加密采用SIP 所支持的安全协议进行处理。

6.3.2 人脸车牌图像视频数据存储安全要求

车联网云端对人脸及车牌等敏感个人信息的图像视频应进行匿名化处理和存储。

6.3.3 个人敏感信息数据安全要求

车联网云端对个人敏感信息应进行脱敏处理和存储，对于个人敏感信息的操作和访问应进行审计记录。

6.3.4 车外及轨迹数据存储安全要求

车外数据、位置轨迹数据在远程信息服务平台等车外位置中保存时间后不应超过14d。以下条件的数据例外：

a) 为优化行驶安全功能而存储的特定场景数据，每车每天不超过 3 个连续时间的数据片段，每个片段不应超过 2 分钟；
b) 为用户远程监控车内外情况、使用云盘存储用户数据等直接服务于用户的功能，通过传输安全保障和访问控制措施保障的用户传输到云端平台的数据；
c) 采集训练数据的专用采集车辆或特定区域行驶的专用测试车辆采集的数据，车辆外部有“测试车辆”或“数据采集车辆”及所属单位的显著表示，驾驶人员为具备授权的特定人员。
d) 新能源汽车、道路运输车辆、网络预约出租汽车依据行政管理要求进行存储的数据。

e） 用于生产经营的汽车产生的，生产经营者可控的位置轨迹数据。

6.3.5 敏感数据分享安全要求

车外数据、位置轨迹数据、个人敏感数据进行分享和公开时，应采用区块链等技术保证数据的访问授权、透明、不可篡改、可回溯。

6.3.6 控制指令和诊断指令安全要求

云平台对车端发起的控制指令和诊断指令应采用高强度加密算法对传输通道和内容进行安全保护，并保证加密机制可防止重放、篡改、仿冒、中间人攻击及窃听、监听等安全风险。

用户发起控制指令和诊断指令的功能应进行审批、身份认证、操作审计。

6.4 管理安全

6.5.1 资产管理

a） 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
b） 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题；
c） 应定期对系统进行漏洞评测，并形成报告；
d） 应采取必要的措施验证安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补；
e） 应建立漏洞管理制度和漏洞全生命周期管理系统，落实漏洞责任制，并对漏洞进行跟踪，高危漏洞进行报送。应建立威胁预警与应急响应制度，按要求进行加固和防护。

6.5.2 密码管理

远程监控系统的口令应符合《智能联网设备口令保护指南》的要求，不存在弱口令、空口令或默认口令等。

本项应满足如下要求:

a） 口令不得与用户名相同；
b） 口令长度不得低于 8 个字符；
c） 口令至少包含数字、大小写字母、特殊字符混合组成的三类字符；
d） 口令不得以明文方式进行传输；
e） 口令加密存储；
f） 口令应定期更换；
g） 口令不得以程序硬编码；
h） 输入框中口令应掩盖显示；
i） 禁止从输入框中复制口令；
j） 应采用技术手段对口令强度进行校验；
k） 所有针对口令的操作均记录日志，日志内容包括用户 ID、IP 地址、操作时间、操作内容、操作结果等信息。

附 录 A
（资料性）
远程平台参数要求

CMS主要包括登录服务器、网关服务器、流媒体服务器、用户管理服务器、WIFI自动下载服务器，存储服务器、WEB服务器及远程监控客户端八个部分。

服务器部分由一个或两个数据库服务器、一个或两个登录服务器、多个网关服务器、多个流媒体服务器、多个用户管理服务器向车载DVR及客户端提供GPS、视频、报警等服务。

A.1 服务器基本要求

操作系统	Microsoft Windows Server 2003 或者更高
CPU	英特尔四核至强，且主频不小于 Xeon 5410(2.33GHz)
网卡	2 个 Gigabit Ethernet
内存	4G(或者更高)
硬盘	1TB
光驱	DVR-ROM
其它	支持 VGA 显示；支持普通键盘口，推荐使用 USB 键盘口；需要有电脑、运行、硬盘等状态指示灯

A.2 流媒体服务器

性能规格	
要求	最大可支持 256 路入口视频流的分发，入口媒体流带宽最大 128Mbps
	单路媒体流最大复制输出 6 路，出口媒体带宽最大 512Mbps
	千兆网口的速率下，20Mbps 输出码流，平均转发时延小于 5 ms 千兆网口的速率下，100Mbps 输出码流，平均转发时延小于 40 ms 千兆网口的速率下，512Mbps 输出码流，平均转发时延小于 200 ms
视频带宽	
要求	按每路 CIF 格式视频每秒 320Kbit 数据量，256 路视频需要 320*256 = 81,920 Kbit 带宽 说明：目前 MDVR 设备在 3G 网络环境下，受网络带宽限制，最高上传 CIF 分辨率视频。