ICS ××.×××.××
× ×××
备案号：

DB50

重　庆　市　地　方　标　准

DB 50/T ×××—202×
代替：DB 50/T ×××—202X

自动驾驶接驳巴士运营技术规范

（征求意见稿）

202×-××-××发布　　202××-××-××实施

重庆市市场监督管理局发 布

前　言

本文件按照GB/T 1.1-2020给出的规则起草。

为进一步落实自动驾驶接驳巴士运营技术规范，推动相关产品功能与性能标准化，保障自动驾驶接驳巴士快速应用推广，根据T/ITS XXXX.1—XXXX《自动驾驶公交车-车辆运营技术要求》，制定本标准。

本规范适用于所有自动驾驶接驳巴士。

本文件由×××提出。

本文件由×××归口。

本文件起草单位：×××、×××、×××。

本文件主要起草人员：×××、×××、×××、×××、×××。

自动驾驶接驳巴士运营技术规范

1. 范围

本文件规定了自动驾驶接驳巴士的基本要求、运营功能要求和信息安全要求。

本文件适用于具备 L4 或 L5 自动驾驶能力，提供载客运营服务的中小型客车。其他车型参照执行。

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。

GA802—2008 机动车类型术语和定义

GB 4785 汽车及挂车外部照明和光信号装置的安装规定

GB 7258—2017 机动车运行安全技术条件

GB 13094 客车结构安全要求

GB 14166 机动车乘员用安全带、约束系统、儿童约束系统和 ISOFIX 儿童约束系统

GB 15741 汽车和挂车号牌板(架)及其位置

GB 17675 汽车转向系 基本要求

GB12676-2014 商用车辆和挂车制动系统技术要求及试验方法

GB 34655 客车灭火装备配置要求

GB/T 40429-2021 汽车驾驶自动化分级

GA 36 中华人民共和国机动车号牌

3. 术语、定义和缩略语

3.1 术语和定义

GB/T 1.1 界定的以及下列术语和定义适用于本文件。

3.1.1

自动驾驶接驳巴士 automated driving bus

具备L4或L5自动驾驶能力的中小型客车。中小型客车为GA802—2008中所规定的中小型客车。

3.1.2

高级自动驾驶系统 advanced autopilot system

GB/T 40429-2021 中所规定的 4 级或 5 级驾驶自动化系统。

3.1.3

在线升级 Over-The-Air update

通过无线网络，从服务器下载更新文件以确保软件系统等处于最新状态。

3.1.4

智能车载监控终端 intelligent monitoring terminal for automated driving system

智能车载监控终端是指安装在车辆上满足工作环境要求，具备行车记录仪、卫星定位、车载视频监控、驾驶员状态监测等其中多项功能，并支持与其他车载电子设备进行通信，提供主动安全管理与服务所需信息的车载设备。

3.1.5

远程驾驶状态监测 remote driving state monitoring

利用安装在远程驾驶舱的传感器，在远程驾驶过程中，通过接触或非接触的方式，实时监控安全员、驾驶舱运行状态，能够检测到危险驾驶行为、异常状态事件，并将异常状态上报企业监管平台。

3.1.6

安全员状态监测 safety driver state monitoring

利用安装在车辆的传感器，在安全员驾驶过程中，通过接触或非接触的方式，实时监控安全员的状态，能够检测到安全员危险驾驶行为，并将异常状态上报企业监管平台。

3.1.7

运营管理平台 operation management platform

支持用户终端及车辆内外屏幕及 HMI 等日常运营管理工作的后端平台。

3.1.8

监控平台 real time monitoring platform

对车辆运营关键指标、车辆线路运营状态进行实时监控的可视化监管平台。

3.1.9

最高设计运行速度 maximum design operational speed

车辆在自动驾驶模式下可运行的最高速度。

3.2 缩略语

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）
DoS：拒绝服务（Denial of Service）
ECU：电子控制单元（Electronic Control Unit）
EDR：事件数据记录系统（Events Data Recorder）
IMSI：国际移动用户识别码（International Mobile Subscriber Identity）
ODC：设计运行条件（operational design condition）
OTA：在线升级 （Over-The-Air update）
RTSP：实时流传输协议（Real Time Streaming Protocol）
TCP：传输协议控制（Transmission Control Protocol）
TLS：传输层安全性协议（Transport Layer Security）

UDP：用户数据报协议（User Datagram Protocol）
V2X：车辆与其他设备通讯（Vehicle to Everything）
VIN：车辆识别码（Vehicle Identification Number）

4. 车辆基本要求

4.1 整车要求

4.1.1 标志标牌

4.1.1.1 在车身前部外表面的易见部位上应至少装置一个能永久保持、且与车辆品牌相适应的商标或厂标。
4.1.1.2 车辆应留有安装前后号牌的位置，号牌板（架）位置应能满足 GB 7258 和 GB 15741 的要求；号牌板外廓尺寸和号牌板（架）的号牌安装孔尺寸应符合 GA 36 的要求。
4.1.1.3 车内应设置满足 GB 7258-2017 中 4.1.2 要求的产品标牌。
4.1.1.4 车辆尾部和车身两侧外表面易见部位应设置自动驾驶专用标识。

4.1.2 核载要求

4.1.2.1 最大允许总质量应按照 GB 7258—2017 中 4.4.1 的要求进行核定。
4.1.2.2 额定载客人数应按照 GB 7258—2017 中 4.4.3 和 GB 13094 中 4.2.2 的要求核定，司机或安全员的质量按 75 kg 计算。

4.1.3 最高设计车速

车辆的最高设计车速应不大于 70 km/h，且不小于 20 km/h。

4.1.4 静态横向稳定性

按 GB/T 14172 规定的方法，在空载、静态条件下，向左和右侧倾斜的侧倾稳定角均应不小于 35°。

4.1.5 信号及照明

车辆可不配备远光灯，若配备，应满足 GB 4785 要求。 车辆喇叭、灯光、车门实现线控功能，能够响应控制端发送的开关指令，并能正确响应。

4.1.6 转向要求

车辆的转向性能应满足 GB 17675 的要求。 转向系统实现线控功能，能够实现控制端发送的目标转角及角速度指令，并能正确响应。

4.1.7 制动要求

车辆的制动性能应满足 GB 12676 的要求。 制动系统实现线控功能，能够实现控制端发送的目标减速度等减速指令，并能正确响应。

4.2 安全配置

4.2.1 安全带

车辆所有座椅应配备安全带，且应符合 GB 14166 的规定。

4.2.2 灭火装备

车辆应配备灭火装备，且应符合 GB 34655 的规定。

4.2.3 火灾监测报警系统

车辆应具备火灾检测自动报警功能，能够检测到动力电池、发动机舱、驾驶舱、车厢的起火情况，并能发出声学和光学报警信号。

4.2.4 紧急制动装置

车辆应具备紧急制动装置，确保车辆在人工驾驶和自动驾驶模式下，均能够触发紧急制动并停止。

4.3 专用设备

4.3.1 车内信息交互设备

4.3.1.1 车辆应配备向车内乘客提供信息交互的设备，宜提供包括车辆驾驶模式、开门状态、BMS 状态在内信息。
4.3.1.2 如车辆设有安全员，应配备向安全员提供信息交互的设备。

4.3.2 车外信息交互设备

4.3.2.1 车辆应配备向车外交通参与者提供信息交互的功能，宜提供包括车辆驾驶模式、转向状态、到站状态在内信息。
4.3.2.2 车外信息交互设备可安装在车辆前侧、右侧或后侧的上方。

4.3.3 车内监控设备

4.3.3.1 车辆应配备车内监控设备。
4.3.3.2 监控设备安装位置应保证车内监控无死角。

5. 车辆运营要求

5.1 身份验证

5.1.1 乘客验证

车辆或车辆预约系统应具备乘客身份识别与验证功能，具体根据车辆运营模式选择验证方式，如 APP 车辆扫码认证或人脸识别，此功能应满足个人信息保护要求。

5.1.2 安全员验证

5.1.2.1 如车辆设有安全员，车辆应具备安全员身份识别与验证功能。
5.1.2.2 车辆对安全员身份识别与验证应有明确的基准，且基准应绑定个人身份信息。 此功能应满足个人信息保护要求。

5.2 车内信息交互

5.2.1 乘客信息交互

5.2.1.1 车辆面向乘客的交互功能应包括但不限于下列内容：
a) 线路名、起终点、途径站点在内的线路基础信息；

b) 车辆行驶路径、驾驶模式、实时位置、实时车速、剩余里程在内的车辆运行信息；
c) 车辆周围交通参与者、道路标志标线信息、信号灯信息；
d) 语音报站、安全提醒、紧急停车提醒。
5.2.1.2 车辆面向乘客的交互功能宜包括下列内容：
a) 车内温度、湿度、天气预报等信息；
b) 自动驾驶车辆周边实时感知信息及安全风险。

5.2.2 安全员信息交互

5.2.2.1 如车辆设有安全员，车辆应具备面向安全员的交互功能，且功能实现应通过安全机制验证，确保经过授权的安全员才能使用。
5.2.2.2 车辆面向安全员的交互功能应包括但不限于下列内容：
a) 识别并记录安全员上、下岗时间信息；
b) 面向安全员提供班次计划、调度指令信息；
c) 面向安全员的安全确认操作；
d) 线路名、起终点、运营时间、班次间隔、途径站点在内的线路基础信息；
e) 车辆行驶路径、实时位置、实时车速、剩余里程在内的车辆运动学信息；
f) 车辆周围交通参与者、道路标志标线信息；
g) 语音报站、安全提醒、紧急停车提醒；
f) 车辆故障信息。

5.3 车外信息交互

5.3.1 应用交互

5.3.1.1 车辆转向及制动时，应发出提示信息，提示信息从车辆后方应可清晰辨别。
5.3.1.2 车辆进出站时，应具备进出站报站安全提示。

5.3.2 公益交互

5.3.2.1 车辆宜具备向其他道路使用者显示前方信号灯信息的能力。
5.3.2.2 车辆宜具备向其他道路使用者显示车辆感知到的道路异常信息的能力，如施工等。
5.3.2.3 车辆宜具备公共信息宣传能力。

5.3.3 车云交互

车辆宜具备与云端交互的能力，交互信息宜包括协同感知、决策信息、远程控制信息等。

5.3.4 V2X 信息

车辆宜具备接收或发送 V2X 消息的能力，如交通信息、天气信息、信号灯信息和路侧感知信息等。

5.4 外部响应

5.4.1 运营管理平台

5.4.1.1 车辆应具备接入自动驾驶接驳巴士运营管理平台的能力，运营管理平台应对车辆的全生命周期进行管理。
5.4.1.2 车辆运营管理平台应至少上传以下内容：
a) 车辆基础性数据，包括车辆电子档案、维修保养信息、OTA 升级等信息；

b) 车辆运营相关的数据，包括车辆实时位置、驾驶模式、行驶轨迹、乘车人次、行驶里程等。

5.4.2 监控平台

5.4.2.1 车辆应具备接入监控平台的能力。
5.4.2.2 监控平台应能对车辆位置、驾驶模式、行驶轨迹的实时可视化监控。
5.4.2.3 监控平台对超速、偏离路线、长时间不上报路线等车辆异常情况进行报警。

5.4.3 配套设施

5.4.3.1 车辆如需配套使用智慧站台等设施，应具备向配套设施的信息输出能力。
5.4.3.2 车辆面向智慧站台等配套设施的输出信息，宜包括车辆位置及到站信息。

5.5 安全监测

5.5.1 超员监测

车辆或车辆预约系统应具备乘车人数识别能力，在车辆超员时应进行预警并提示乘客换乘其他车辆。

5.5.2 安全带监测

车辆应能对所有乘员安全带的使用状态进行监测，并配备满足 GB/T 24551 要求的安全带提醒装置。

5.5.3 乘员状态监测

车辆应具备提示乘客安全乘车的功能，及对车内乘员的危险动作的监测功能。

5.6 数据记录

5.6.1 功能要求

车辆应具备自动驾驶数据记录功能，并配备满足 GB 7258-2017 要求的 EDR，用于事故分析及责任判定。

5.6.2 记录存储

自动驾驶系统开启时，车辆应采用实时记录的方式记录数据，且记录数据的能力不低于 48 小时。

5.6.3 数据元素

车辆记录的数据应包括符合附录 A 的车辆及系统基本信息、车辆状态及动态信息、自动驾驶系统运行信息、行车环境信息、驾乘人员操作及状态信息。

5.7 其他要求

5.7.1 车门防夹

车辆应具备识别乘员上下车动作的能力，且具备防夹功能。

5.7.2 远程控制

5.7.2.1 车辆宜具备远程控制能力。
5.7.2.2 若车辆具备远程控制能力，当车辆出现故障、驶出 ODC 或遇到难以通过的场景，车辆应能主动发起远程控制请求，请求远程驾驶员协助控制。

6. 信息安全要求

6.1 自动驾驶车辆

6.1.1 硬件安全要求

6.1.1.1 自动驾驶车载终端的芯片调试接口应禁用或设置安全访问控制且不存在后门或隐蔽接口。
6.1.1.2 自动驾驶车载终端所使用的关键芯片，包含但不限于处理器、存储模块、通讯 IC 等用于处理、存储和传输敏感信息的芯片以及安全芯片，应减少暴露管脚。
6.1.1.3 自动驾驶车载终端的芯片之间应减少通信线路的数量，例如：使用多层电路板的车载信息交互系统可采用内层布线方式隐藏通信线路。
6.1.1.4 自动驾驶车载终端的电路板及芯片不宜暴露用以标注、端口和管脚功能的可读丝印。
6.1.1.5 自动驾驶车载终端能够对抗针对加解密操作的密码分析攻击、侧信道攻击、故障注入攻击等破坏数据保密性和完整性的安全威胁，保证车载端所存储的关键数据不被泄露或篡改、芯片功能可以正常使用。
6.1.1. 6 自动驾驶车载终端具备车载网络检测能力，并在终端受到攻击时，将攻击上报至 SOC 平台。

6.1.2 软件安全要求

6.1.2.1 操作系统、固件系统、应用软件和配置文件的升级、加载和安装时，应验证提供方的身份真实性和来源的合法性。
6.1.2.2 操作系统应验证登录用户身份的真实性和合法性。
6.1.2.3 应用软件应具备针对安全威胁的防护措施，防止被逆向分析、反编译、篡改、非授权访问等，宜采用代码混淆或加壳等措施。
6.1.2.4 操作系统、固件系统和配置文件的升级、加载和安装时，应验证其完整性。
6.1.2.5 软件系统、固件系统启动和运行时，应验证其完整性。
6.1.2.6 操作系统、固件系统、应用软件、配置文件和数据资产的访问可控性应满足:
a) 能验证对操作系统、固件系统、应用软件、配置文件和数据资产的访问、操作和使用的权限；
b) 能验证操作系统、固件系统、应用软件和配置文件的升级、加载和安装的权限。
6.1.2.7 操作系统、固件系统、应用软件应满足以下安全日志要求:
a) 对包括不限于用户活动和操作指令的重要信息安全事件进行记录，记录内容宜包含事件的时间、用户、事件类型、事件成功情况的信息；
b) 应采取访问控制机制管理日志读取和写入的权限；
c) 应对日志文件进行安全存储；
d) 涉及个人敏感信息的，应进行脱敏等防护后，才能写入日志文件。
6.1.2.8 操作系统、固件系统、应用软件应具备对自身受到信息安全攻击的感知能力，当受到信息安全攻击时，宜进行信息安全告警或攻击阻止的响应。
6.1.2.9 车辆应搭载网络入侵检测防御系统（NIDPS）与主机入侵检测响应系统（HIDS），对网络攻击进行检测和防御。并在车辆受到攻击时，将该攻击上报至 SOC 平台。
a) 应包括 L3-L7 层网络攻击行为的检测和防御、L5-L7 层网络协议（HTTP、DNS、TLS）深度包检测、L5-L7 层网络协议（SomeIP、DoIP）深度包检测；
b) 网络入侵检测防御系统（NIDPS）应对车辆的网络报文、蓝牙报文等数据进行检测与拦截，NIDPS 组件至少应具备防护墙检测引擎，流量检测引擎，网络检测引擎，深度包检测引擎四个检测组件；
c) 主机入侵检测响应系统（HIDS）应基于主机纬度的 IDS、对系统的状态进行分析，HIDS 至少应具备系统资源检测能力、系统服务检测能力、远程连接检测能力、文件安全检测能力，并依赖日志系统作为

数据分析源，同时对事件进行审计。
d) 网络入侵检测防御系统（NIDPS）占用 RAM 资源 40MB 以内，ROM 资源 15MB 以内；主机入侵检测响应系统（HIDS）占用 RAM 资源 40MB 以内，ROM 资源 15MB 以内。

6.2 路侧设备

6.2.1 安全要求

6.2.1.1 路侧终端应具备车载网络检测能力，并在终端受到攻击时，将攻击上报至 SOC 平台。
6.2.1.2 路侧终端应搭载路端入侵检测系统，路端入侵检测系统至少包括防火墙检测，流量检测，网络检测，深度包检测等多个检测能力。
a) 防火墙检测应具有端口和 IP 的黑/白名单功能、URL/URI 转换、默认规则、默认白名单功能；
b) 流量检测应对网络数据流量进行统计与阈值检测；
c) 网络检测应基于规则检测各类网络报文头异常，或报文内容异常，以守护进程方式运行；
d) 深度包检测应具备应用层协议识别和报文内容匹配功能。

6.2.2 性能要求

6.2.2.1 路侧安全系统不应对路侧设备功能造成影响，占用 RAM 资源 40MB 以内，ROM 资源 20MB 以内；
6.2.2.2 路端入侵检测系统各组件应支持 Android、Linux、Qnx 系统部署，应支持 ARM(32/64) X86(32/64)等多种硬件架构。

6.3 通信安全要求

6.3.1 车云平台通信

6.3.1.1 各通信单元应基于数字证书提供安全的认证服务；
6.3.1.2 蜂窝络层之上应支持独立的加密机制，应采用 TLS1.2 版本及以上的安全协议进行加密。
6.3.1.3 蜂窝移动通信网络层之上应支持独立的完整性机制，应采用 TLS1.2 版本及以上安全协议进行完整性保护，并满足
a) 与外部通信的部件应 DoS/DDoS 攻击；
b) 与外部通信的部件应支持抗无线干扰；
c) 车外远距离通信应具备对通信报文进行访问控制的能力，白名单访问控制、报文过滤、防通信流量过载机制等；
d) 车外远距离通信应确保蜂窝移动通信网络层通信 ID（如：国际移动用户识别码 IMSI 等）的唯一性；
e) 车外远距离通信应具备对通信报文的安全监控能力和攻击行为的感知能力，当受到信息安全攻击时，宜进行报文清洗、流量控制或阻止攻击行为的响应。

6.3.2 车内通信

6.3.2.1 车内通信应验证通信 ECU 双方身份的真实性。
6.3.2.2 车内通信数据应进行加密。
6.3.2.3 车内通信数据应采用完整性保护。
6.3.2.4 车内通信应具备通信流量控制能力，例如当受到恶意软件感染或者服务拒绝攻击而造成车内通信流量异常时，仍然有能力提供可接受的通信。
6.3.2.5 应将车内网络划分为不同的信息安全区域，每个信息安全区域之间宜进行网络隔离。
6.3.2.6 信息安全区域间应采用边界访问控制机制对来访的报文进行控制，例如采用报文过滤机制、报

文过载控制机制和用户访问权限控制机制等。

6.3.2.7 车内通信应具备日志记录的能力，例如记录流量过载、高频率的收到异常报文等现象。

6.3.2.8 车内通信应对异常报文具有感知能力，当感知到异常报文时，宜具有告警或者其他安全响应 的能力，例如接收到高频率的重放报文或者被篡改过的报文等异常现象。

6.4 OTA 要求

6.4.1 安全要求

6.4.1.1 自动驾驶系统升级时，车载网络设备和远程服务器之间应采用双向认证。

6.4.1.2 升级包的传输应采用加密措施。

6.4.1.3 自动驾驶系统接收升级包后，应对升级包的数字签名信息进行验证，校验升级包的完整性。

6.4.2 管理要求

6.4.2.1 车辆 OTA 时，应具备 OTA 管理功能，包括但不限于版本管理、版本备份、升级失败回滚，以保证正在 更新的系统能够从失败或者中断的更新中恢复。

6.4.2.2 OTA 安全应基于密码模块，通过实施数据加密和数字签名，对升级包文件进行机密性、完整性及真实性防护，以防止因升级包在传输、存储过程中被窃取、篡改给系统带来的安全风险。

附录 A
(规范性)
自动驾驶接驳巴士数据记录元素集

A.1 车辆及自动驾驶数据记录系统基本信息

表 A.1 给出了车辆及自动驾驶数据记录系统基本信息。

表 A.1 车辆及自动驾驶数据记录系统基本信息

序号	数据信息
1	车辆识别代号（VIN）
2	车辆型号
3	实现自动驾驶数据记录系统功能的硬件版本号
4	自动驾驶数据记录系统序列号
5	自动驾驶数据记录系统软件版本号
6	事件类型编码
7	事件触发时间
8	事件触发地点
9	行驶里程

A.2 车辆状态及动态信息

表 A.2 给出了车辆状态及动态信息。

表A.2 车辆状态及动态信息

序号	数据信息
1	驾驶模式
2	车辆位置（经纬度）
3	车辆速度
4	车辆加速度
5	车辆航向角
6	方向盘转角

A.3 自动驾驶系统运行信息

表 A.3 给出了自动驾驶系统运行信息。

表 A.3 自动驾驶系统运行信息

序号	数据信息
1	自动驾驶系统请求挡位
2	自动驾驶系统请求的加速度
3	自动驾驶系统请求的方向盘转向角
4	自动驾驶系统请求的转向曲率

5	自动驾驶系统请求的前轮转角
6	自动驾驶系统请求的转向小齿轮转向角
7	自动驾驶系统请求的方向盘转向力矩
8	自动驾驶系统请求的车速
9	自动驾驶系统请求的油门踏板开度比例
10	自动驾驶系统请求的刹车踏板开度比例
11	自动驾驶系统请求的驱动电机转矩
12	自动驾驶系统请求的驱动电机转速
13	自动驾驶系统请求的轮端扭矩
14	自动驾驶系统请求的车辆灯光信号状态
15	自动驾驶系统请求的车辆雨刮状态
16	自动驾驶系统故障状态

A.4 行车环境信息

表A.4给出了行车环境信息。

表A.4 行车环境信息

序号	数据信息
1	外部图像
2	感知目标物类型
3	感知目标物相对位置
4	感知目标物相对速度
5	信号灯信息

A.5 驾乘人员操作及状态信息

表A.5给出了驾乘人员操作及状态信息。

表A.5 驾乘人员操作及状态信息

序号	数据信息
1	后援用户接管能力
2	后援用户是否系安全带
3	后援用户是否在驾驶位
4	加速踏板开度
5	刹车踏板开度
6	刹车踏板状态
7	转向盘角度（如有转向盘）
8	转向扭矩
9	转向扭矩
如果已经记录刹车踏板开度，那么可不记录刹车踏板状态。转向盘与转向扭矩任选其一进行记录。	