ICS 03.220.01
CCS R82

团　　体　　标　　准

T/KJDL 021—2024

商用车高级辅助驾驶系统终端与远程平台安全技术要求

Technical Requirements On Commercial-Vehicle ADAS And Remote Platform Security

2024－01－31 发布　　2024－03－01 实施

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。

本文件的某些内容有可能涉及专利，本文件的发布机构不应承担识别这些专利的责任。

本文件由珠海骏驰智联科技有限公司提出。

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、广东产品质量监督检验研究院、移动通信国家工程研究中心、广州优保爱驾科技有限公司、广东沐华科技发展有限公司、深圳市交投科技有限公司、高新兴科技集团股份有限公司、广州小鹏汽车科技有限公司、广东省电子商务认证有限公司、暨南大学、江苏大学、信阳师范大学、西安邮电大学、兰州理工大学、湛江市泰康投资有限公司、深圳市朗庭技术服务有限公司、中科先进智联（杭州）科技有限公司、广东省车联网产业联盟。

本文件主要起草人：刘化龙、石光明、罗广、谢孟思、庄杰、柯涛、温水泉、李大成、肖磉、严日骞、曾少旭、刘志全、张义、刘可儿、李永春、冯霞、胡斌、陈树乐、岳浩、张嵩、赖成喆、成玉丹、刘玉娟、杨文凤、肖薇薇、姚岚、黄斐然。

商用车高级辅助驾驶系统终端与远程平台安全技术要求

1 范围

本文件规定了商用车高级辅助驾驶系统(ADAS)与远程平台的安全要求，包含数据采集、传输与存储安全要求，身份确认、控制命令及远程交互信息的安全技术要求。

本文件适用于安装有ADAS的运营车辆、特种车辆（环卫车、救护车、消防车等）及管理系统，其他商用车辆系统可参照执行。

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。

GB/T 3730.1-2022 汽车、挂车及汽车列车的术语和定义 第1部分:类型
GB 7258-2017 机动车运行安全技术条件
GB 20263-2006 导航电子地图安全处理技术基本要求
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
GB/T 25069-2022 信息安全技术 术语
GB/T 32960.2-2016 电动汽车远程服务与管理系统技术规范 第2部分：车载终端
GB/T 32960.3-2016 电动汽车远程服务与管理系统技术规范 第3部分：通信协议及数据格式
GB/T 36625.3-2021 智慧城市 数据融合 第3部分：数据采集规范
GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求
GB/T 37376-2019 交通运输 数字证书格式
GB/T 38186-2019 商用车辆自动紧急制动系统（AEBS）性能要求及试验方法
GB/T 38671-2020 信息安全技术 远程人脸识别系统技术要求
GB/T 39263-2020 道路车辆 先进驾驶辅助系统(ADAS) 术语及定义
GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
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
GB/T 40861-2021 汽车信息安全通用技术要求
GB/T 42012-2022 信息安全技术 即时通信服务数据安全要求
YD/T 3492-2019 视频监控系统网络安全技术要求
YD/T 3750-2020 车联网无线通信安全技术指南
YD/T 3751-2020 车联网信息服务 数据安全技术要求
YD/T 3752-2020 车联网信息服务平台安全防护技术要求
T/KJDL 020-2022 商用车辆辅助驾驶安全及数据平台
ISO/IEC 27001 信息安全、 网络安全和隐私保护

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069-2022、GB/T 38186-2019和T/KJDL 020-2022界定的以及下列术语和定义适用于本文件。

3.1.1

视频监控 video surveillance
利用视频技术探测、监视设防区域并实时显示。

3.1.2

安全漏洞 security vulnerability

系统和平台在需求分析、设计、实现、配置、测试、运行、维护等过程中,无意或有意产生的、能够被威胁利用的缺陷或弱点。

3.1.3

位置轨迹 position trajectory

车辆在地图上的定位和途径路径。

3.2 缩略语

下列符号适用于本文件。

ADAS：高级辅助驾驶系统（Advanced Driver Assistance Systems）
DMS：驾驶员状态监测系统（Driver monitoring systems）
FTP：文件传输协议（File Transfer Protocol）
HTTP：超文本传输协议（Hypertext Transfer Protocol）
IC卡：集成电路卡（Integrated Circuit Card）
JTAG：联合测试工作组（Joint Test Action Group）
PKI：公钥基础设施（Public Key Infrastructure）
SSL：安全套接字层（Secure Sockets Layer）
TLS：传输层安全（Transport Layer Security）
USB：通用串行总线（Universal Serial Bus）
VIN：车辆识别码（Vehicle Identification Number）
VPN：虚拟专用网络（Virtual Private Network）

4 概述

4.1 一般要求

商用车ADAS应包含终端与远程平台两个方面，关注身份认证与访问控制、数据传感与实时处理、通信与系统安全、安全审计与监控等要素，确保系统的安全性和可靠性。

本项要求包含但不限于以下项目：

a) 应经过多层身份验证，授权后才能访问系统，维护终端和远程平台的安全；
b) 应具备高精度的数据传感装置，确保对车辆周围环境的实时感知；
c) 应采用可靠的决策算法，进行障碍物检测、路径规划和车辆控制；
d) 应经过严格的验证和测试，包括仿真测试、闭环道路测试和实际道路测试；
e) 使用 ADAS 提供驾乘服务的车辆应使用脱敏的匿名通讯技术建立司乘专用联系通道，保护个人信息；
f) 应封禁调试接口和非加密远程接入方式，提高安全性；
g) 应具备抗对抗样本攻击能力。

4.2 终端安全要求

4.2.1 数据采集要求

本项要求包含但不限于以下项目：

a) 数据采集应满足 GB/T 36625.3-2021 中数据采集质量控制的规定；
b) 应根据不同应用场景下的数据价值和合规需求来判断数据的敏感度；
c) 应采用具备安全措施的采集工具和方法，并确保采集过程未被恶意干扰；
d) 应对不同的采集对象采取针对性的采集保护要求，如采集车外数据时，应匿名化处理或者处理完成立即删除；
e) 应按照合法、正当、必要原则采集数据，不得超过业务功能范围采集数据。

4.2.2 数据传输要求

a) 所有在终端间的数据传输都应该使用安全协议进行，例如 SSL/TLS 等，以确保数据传输的安全性和私密性；
b) 终端设备需要支持认证与身份验证机制，确保只有经过授权的用户或设备可以访问和传输数据；
c) 在数据传输过程中，应使用加密算法对数据进行加密，以防止未经授权的窃听；
d) 为了确保终端数据传输的稳定性和可靠性，应该采用冗余传输机制和错误纠正码等技术，以减少数据传输中的丢失和损坏；
e) 终端设备应具备安全审计和监控功能，记录和监测数据传输的过程，及时发现异常行为和安全事件，并采取相应的措施进行处理。同时，也需要保护这些审计和监控数据的安全性，防止被篡改或删除。

4.2.3 数据存储要求

本项要求包含但不限于以下项目：
a) 存储在车载终端内的数据应满足 GB/T 32960.2-2016 的加密规定；
b) 为了防止未经授权的篡改，终端存储设备应该具备防篡改保护措施。例如，使用数字签名或哈希算法来验证数据的完整性；
c) 为了防止数据丢失或损坏，终端存储设备上的数据应定期备份到可靠的存储介质上。备份过程应该是安全的，并且备份数据应加密存储；
d) 终端存储设备应具备安全认证功能，确保只有经过授权的用户可以访问和修改存储数据。例如，使用身份认证和访问控制机制。

4.2.4 身份认证与访问控制要求

本项要求包含但不限于以下项目：
a) 身份认证应满足 GB/T 38671 中的功能规定；
b) 访问控制应满足 GB/T 38671 中对用户数据保护的规定；
c) 应引入多因素身份认证，结合用户密码、智能卡、生物识别等多种因素，提高身份验证的安全性，确保只有合法用户能够登录系统；
d) 应建立 PKI 体系，使用数字证书对终端进行身份验证，确保终端的身份合法有效，维护系统整体的安全性；
e) 应启用登录审计功能，监控用户的登录行为，及时检测异常活动，提高对潜在风险的感知，以及提高对安全威胁的响应速度。

4.2.5 车辆数据安全要求

本项要求包含但不限于以下项目：
a) 车辆数据安全应满足 GB/T 42012—2022 中数据安全的规定；
b) 应对不同隐私级别的数据进行分类安全保护，以实现高安全要求和低经济效益；
c) 应关注车内数据存储安全和车外交互数据在车企管理平台存储安全；
d) 应采取相应的措施保证数据访问者的合理访问，如身份鉴别和访问控制；
e) 应保证数据传输链路的安全性和终端设备身份的合法性与唯一性，使得高精度定位数据具有完整性和可检验性。

4.3 远程平台安全要求

4.3.1 报警及响应时间要求

本项要求包含但不限于以下项目：
a) 预警触发条件应包含 GB/T 39263-2020 中触发报警的项目；
b) 响应时间应满足 GB 7258-2017 中对车辆应急制动中对预警响应的时间要求；
c) 应设定精确的报警触发条件，确保系统能够准确地识别潜在危险情况并及时发出警示信号；
d) 应根据报警的严重性和紧急程度，设定不同的报警级别，确保驾驶员能快速察觉到危险情况并采取行动。

4.3.2 网络与通信安全要求

本项要求包含但不限于以下项目：

a) 网络与通信安全应满足 ISO/IEC 27001 中相应等级的规定；
b) 应实施恶意软件防护措施，并定期进行恶意软件扫描和漏洞修复，确保免受恶意软件的威胁；
c) 建立有效的安全监控和事件日志记录机制，全面监测系统的网络活动。及时检测并记录异常行为，以便进行实时响应和后续安全审计。

4.3.3 操作系统安全要求

本项要求包含但不限于以下项目：

a) 操作系统安全应满足 ISO/IEC 27001 中相应等级的规定；
b) 应部署有效的防病毒和恶意软件的保护机制，确保远程平台的操作系统免受病毒和恶意软件的侵害，及时应对新的威胁；
c) 应定期接受安全更新和维护，及时修补已知漏洞，提高系统的整体抗攻击性，确保操作系统和相关软件的安全性是持续得到维护和升级的。

4.3.4 平台访问与数据安全要求

本项要求包括但不限于以下项目：

a) 访问控制与数据安全应满足 GB/T 22239-2019 中相应等级的规定；
b) 应在数据的收集、传输和存储过程中，采取适当的措施，保护消费者的个人信息和隐私；
c) 应采取措施保护系统的保密性和完整性，以防止未经授权的访问和潜在攻击以及因意外故障导致数据丢失。

4.3.5 平台等保要求

本项要求包括但不限于以下项目：

a) 平台等保要求应满足 GB/T 22239-2019 中对入侵防范及设备安全的规定；
b) 应制定清晰的安全等级划分标准，确保远程平台根据其重要性和风险程度得到适当的安全等级分类；
c) 确保平台的设计、实施和运维符合相关的法律和合规性要求，以保障系统的合法性和可信度。

5 终端安全技术要求

5.1 终端数据源

5.1.1 终端车辆收集的数据信息

终端车辆收集信息参考表 1。

表1 终端收集信息表

数据类别	主要范围
驾驶人有关的行为数据	驾驶人身份信息、驾驶习惯、驾驶状态(可能含眼球、脉搏等生物信息)、位置信息、交通及路况信息等
主机运行有关的硬件数据	车辆识别码(VIN)、设备配置及运行情况 车辆通信内容、维保记录、位置信息等
车载/移动终端有关的数据	车载终端(车机屏、车上娱乐等)收集的数据，车载终端系统及应用收集的收据，以及车机联网 APP 收集的数据等
其他数据	路边收集数据、车主数据、乘客数据、气象数据、远程协助收集的数据等

结合《网络安全法》、《信息安全技术 个人信息安全规范》及相关行业实践，智能车辆收集的上述数据绝大多数属于个人信息，其中包括可以直接识别自然人身份的车主姓名、身份证号、生物识别信息，也包括可以与其他信息结合识别自然人身份的车牌号、车辆行踪轨迹和车辆识别码（VIN），以及车辆本身的技术数据（如各部件运行参数、驾驶习惯等）。并且，其中的身份信息、生物信息、轨迹及位置信息等信息属于个人敏感信息。

5.1.2 位置轨迹数据

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车辆定位和途径路径相关的数据。

5.1.3 座舱数据

座舱数据指的是通过摄像头、红外传感器、指纹传感器、雷达传感器、麦克风等传感器从车辆座舱采集的数据，以及对其进行加工后产生的数据，座舱数据。不包括对车辆采集数据处理产生的操控记录数据。

5.1.4 车外数据

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。车外数据包括人脸、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。

5.1.5 控制指令

控制指令指的是具有控制汽车功能特性的指令、动作、功能。

5.1.6 诊断指令

诊断指令指的是具有远程对商用车辆进行调试诊断能力的指令数据。

5.2 终端通用要求

不得基于商用车辆所采集数据及经其处理得到的数据开展与车辆管理、行驶安全无关的数据处理活动。

针对疲劳监测、语音识别、远程测控等ADAS功能收集的个人敏感信息基于数据全生命周期，包含：收集个人信息需征得同意、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ADAS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络通道，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。

ADAS应尽可能封禁USB、JTAG等调试接口以及隐藏的免授权非加密远程接入方式。

ADAS算法应具有抗对抗样本攻击能力。

5.3 车端数据的安全要求

应保留最少的个人敏感数据，并限制数据存储量和保留时间，禁止本地明文存储客户重要信息数据，关键及敏感数据应加密存储。

处理个人数据应遵循以下原则：

a) 车内处理原则；
b) 匿名化处理原则；
c) 最小保存期限原则；
d) 精度范围适用原则；
e) 默认不收集原则。

车辆数据存储安全需关注车内数据存储安全和车外交互数据在车企管理平台存储安全。针对车内数据，应对数据访问者采取身份鉴别和访问控制措施，防止未经授权访问，且数据存储时间满足业务场景需要的最短时间即可，不进行长期保存。可考虑基于指纹识别或者人脸识别的方式验证数据访问主体身份，按照“最小必要”原则限制数据存储时间，统筹考虑安全与功能需要对存储数据进行加密。

高精度定位数据应满足如下安全要求：

f) 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。
g) 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。

h) 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 20263-2006 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。
i) 高精度定位数据需具备完整性和可检验性。

5.3 车载终端的数据存储的安全要求

车载终端数据存储要求如下：
a) 应保证按照 GB/T 32960.3-2016 要求所存储的远程服务与管理数据的保密性和完整性；
b) 车载终端的安全重要参数在存储以及使用过程中，应只允许被授权的应用以授权方式读取和修改。

5.3.1 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。

5.3.2 车载终端的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。

5.4 数据传输的安全要求

车载终端的数据传递应遵循以下原则:
a) 应能够检测到数据在传输过程中完整性受到破坏。
b) 应采用技术措施保证数据传输的保密性。
c) 应能够检测到数据在传输过程中完整性受到破坏时，采取必要的措施恢复或重新获取完整的数据。

车载终端的数据传递应注意以下：

未经被收集者的单独同意，商用车辆不得通过网络、物理接口向车外传输包含个人信息的数据。将清晰度转换为120万像素以下且已擦除可识别个人身份的人脸、车牌等信息的视频、图像数据除外。

商用车辆不得通过网络、物理接口向车外传输车辆采集的音频、视频、图像等数据及经其处理得到的数据。

5.4.1 数据传输一般要求

商用车辆的远程服务与管理系统应满足传输数据的保密性、完整性和可用性要求。商用车辆远程服务与管理系统在客户端平台进行平台登入之前，应和服务端平台进行双向身份鉴别。

5.4.2 通信协议栈要求

商用车辆远程服务与管理系统通信协议栈应包含安全通信协议,在客户端平台和服务端平台之间建立安全通信连接，保障GB/T 32960.3-2016定义的业务应用层通信的安全性。

5.4.3 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、中间人攻击及窃听、监听等安全风险。

5.4.4 数据传输完整性保护

在进行个人信息传输时是否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。

5.4.4 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。

5.4.5 数据传输网络通道

诊断指令、控制指令应采用专用的VPN网络。

5.5 身份信息鉴别的安全要求

身份鉴别应满足GB/T 38671中的要求

开展人脸识别时，应至少满足以下要求：

a) 非人脸识别方式安全性或便捷性显著低于人脸识别方式。

b) 原则上不应使用人脸识别方式对不满十四周岁的未成年人进行身份识别。

c) 应同时提供非人脸识别的身份识别方式，并提供数据主体选择使用。

d) 应提供安全措施保障数据主体的知情同意权。

e) 人脸识别数据不应用于除身份识别之外的其他目的。

在人脸识别使用过程中：

f) 应在完成验证或辨识后立即删除人脸图像。

g) 应生成可更新、不可逆、不可链接的人脸特征。

h) 应具备防护呈现干扰攻击的能力。

i) 在本地和远程人脸识别方式均适用时，应使用本地人脸识别。

5.5.1 敏感数据访问身份认证

进行敏感个人信息访问前应依次优先采用人脸识别、IC卡、指纹识别、声纹识别、用户口令识别、IC卡等认证方式，认证后可具有一定时效，时效内身份认证有效，过期或者重新点火后需要重新进行身份认证。

5.5.2 控制指令访问身份认证

进行敏感个人信息传输前应采用公开密钥基础设施等方式对通信两端进行双向身份认证。

5.5.3 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。

5.6 数据采集和存储的安全要求

应根据商用车ADAS不同应用场景下的数据价值和合规需求来判断数据的敏感度，并根据敏感度进行分类分级（敏感度分级划分为 一般数据、重要数据、敏感数据）。

ADAS的数据分类：基础属性数据、车辆工况类数据、环境感知类数据、车辆控制类数据、应用服务类数据（如报表、数据挖掘结果等）。

分类分级同时对数据源的真实性进行验证，并在此基础上，对数据源做身份验证并记录。

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。

a) 数据分级，可分为一般数据、重要数据；

b) 针对不同级别的数据采取不同程度的安全防护措施；

c) 基于知情同意和充分授权原则进行数据采集；

d) 按照合法、正当、必要原则采集数据，不得超过业务功能范围采集数据；

e) 鉴别采集数据的完整性、准确性，保证数据质量。

5.6.1 车外数据采集安全要求

采集车外数据时，应进行匿名化或者处理完成立即删除。

5.6.2 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。

5.6.3 ADAS 传感采集安全要求

ADAS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等辅助驾驶系统在车内的控制器中完成识别功能。

5.6.4 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。

5.6.5 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。

5.7 车载终端日志功能

车载终端日志功能要求如下：

a) 应记录车载终端在远程服务过程中发生的信息安全相关事件，如检测受到网络攻击行为等；
b) 应使每个日志信息记录的内容包括但不限于：日期和时间（精确到秒）、车辆唯一识别码、事件类型；
c) 应保证所存储日志信息的保密性和完整性；
d) 车载终端日志应只允许被授权的应用以授权方式读取；
e) 应具有日志的上传机制，并使用安全通信协议将日志信息发送到企业平台。

5.8 车载终端系统安全

车载终端不应存在由权威漏洞平台公开发布6个月及以上且未经处置的高危安全漏洞。

6 远程平台网络安全要求

6.1 物理和环境安全

用于维护远程平台的建筑或场所应满足如下安全要求：

a) 应符合 GB/T 39786-2021 中相应等级规定；
b) 应符合 GB/T 22239-2019 中相应等级的规定；
c) 设置有人值守的接待区或其他控制物理通道的方式以限制人员进入，仅授权人员可以进入建筑物或操作远程平台的现场；
d) 远程平台运营设施在无人值守的情况下，应保持闭锁且设置警报；
e) 要求所有员工佩戴可见标识，鼓励员工对未佩戴的人进行质询；
f) 进出远程平台运营设施及设施内部的活动均有视频监控。

6.2 通信和网络安全

6.2.1 安全通信基本要求

远程平台的网络安全防护应满足如下安全要求：

a) 应符合 GB/T 22239-2019 中相应等级的规定；
b) 应按照 GB/T 39786-2021 中相应等级规定，保证通信实体身份及传输数据的安全。

6.2.2 远程平台网络访问控制

远程平台的网络访问控制还应满足如下安全要求：

a) 外部系统对远程平台的远程访问（已授权）需要进行身份验证；
b) 远程平台访问外部系统应采用技术手段来保证目标系统的正确性和真实性；
c) 远程平台的监测端口的访问应被安全控制；
d) 应建立控制措施（如防火墙）以保护远程平台内部网络区域不接受其他任何非授权访问；
e) 按照远程平台访问控制策略来建立控制措施以保证可用的服务（如 HTTP，FTP 等）仅对授权用户开放，远程平台所有网络服务的安全属性以文档形式描述。

6.2.3 网络设备管理要求

远程平台应按如下要求对网络设备开展管理：

a） 建立路由管理以确保计算机（网络）连接和信息流不会违反远程平台的访问控制策略；

b） 平台运营机构应在物理安全的环境中维护本地网络组件（如防火墙和路由器），并定期审核其配置是否符合配置要求。

使用规则配置每个网络边界控制（防火墙、交换机、路由器、网关或其他网络控制设备或系统），这些规则仅支持确定为其操作所必需的服务、协议、端口和通信。

6.3 设备和技术安全

远程平台应用的设备及相关辅助设备应满足如下安全要求：

a） 应符合 GB/T 39786-2021 中相应等级规定；

b） 应符合 GB/T 22239-2019 中相应等级的规定；

c） 应建立并维护相关设备的清单；

d） 设备应被妥善的安置且受到保护，以降低受到环境威胁的风险和非授权访问的概率；

e） 设备应受到保护以免遭供电故障和其他电气异常的危害；

f） 设备应按照制造商提供的操作指南或规定流程来进行维护；

g） 应对设备的所有存储介质（包括固定和可移动的）进行检查，以确保它们在处置前不包含敏感数据。

6.4 应用和数据安全

6.4.1 身份鉴别与访问控制

a） 应满足 GB/T 39786-2021 中相应等级规定；

b） 对登录远程平台的人员应实施多因素身份验证；

c） 对可信角色授予访问远程平台的权限时应遵守“最小权限”原则。

6.4.2 系统应用安全要求

远程平台的应用安全应满足如下安全要求：

a） 应根据远程平台访问控制策略限制对信息和应用系统功能的访问；

b） 登录远程平台的管理人员应在访问远程平台的关键应用或执行特权操作前，应对远程平台操作人员进行额外的身份验证。

6.5 管理安全

远程平台数据安全要求，如下：

a） 应符合 GB/T 39786-2021 中相应等级规定；

b） 应按照 GB/T 22239-2019 中相应等级的规定对采集的个人信息进行保护；

c） 在需要将个人信息向可信第三方转移时（如依赖第三方开展人脸生物特征识别），应与可信第三方签订协议保证对个人信息的处理满足相关法律法规的要求；

d） 在公共或非受信网络（环境）进行敏感数据交换时，应将数据加密。

附 录 A
（资料性）
ADAS 行业分析研究报告

2023-2028年汽车驾驶辅助系统(ADAS)行业市场深度分析及发展策略研究报告(内容概况)。

汽车驾驶辅助系统(ADAS)行业研究报告主要分析了汽车驾驶辅助系统(ADAS)行业的国内外发展概况、行业的发展环境、市场分析(市场规模、市场结构、市场特点等)、竞争分析(行业集中度、竞争格局、竞争组群竞争因素等)、产品价格分析、用户分析、替代品和互补品分析、行业主导驱动因素、行业渠道分析、行业赢利能力、行业成长性、行业偿债能力、行业营运能力、汽车驾驶辅助系统 (ADAS)行业重点企业分析、子行业分析、区域市场分析、行业风险分析、行业发展前景预测及相关的经营、投资建议等。报告研究框架全面、严谨，分析内容客观、公正、系统，真实准确地反映了我国汽车驾驶辅助系统(ADAS)行业的市场发展现状和未来发展趋势。

该研究咨询报告由中研普华咨询公司领衔撰写，在大量周密的市场调研基础上，主要依据了国家统计局、国家商务部、国家发改委、国家经济信息中心、国务院发展研究中心、全国商业信息中心、中国经济景气监测中心、中国行业研究网、全国及海外多种相关报刊杂志的基础信息以及专业研究单位等公布和提供的大量资料。对我国汽车驾驶辅助系统(ADAS)行业作了详尽深入的分析，是企业进行市场研究工作时不可或缺的重要参考资料，同时也可作为金融机构进行信贷分析、证券分析、投资分析等研究工作时的参考依据。

参 考 文 献

[1] JT/T 794 道路运输车辆卫星定位系统车载终端技术要求
[2] JT/T 883-2014 运营车辆行驶危险预警系统技术要求和试验方法
[3] JT/T 1242-2019 营运车辆自动紧急制动系统性能要求与测试规程
[4] T/SCJA 13-2022 商用车盲区预警制动系统后装性能要求和测试规程