ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL 177—2025

汽车工程 自动驾驶数据记录与传输安全技术标准

Technical Standard for Autonomous Vehicle Data Recording and Transmission Security

征求意见稿

2025 - - 发布　　2025 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

汽车工程 自动驾驶数据记录与传输安全 技术标准

一、引言

随着自动驾驶技术的快速发展，数据记录与传输安全成为保障自动驾驶汽车安全运行的关键环节。当前，自动驾驶汽车数据记录与传输存在标准不统一、安全要求不完善、隐私保护措施不足等问题。为解决这些问题，系统规范自动驾驶汽车数据记录与传输安全技术要求，特制定本标准。本标准聚焦自动驾驶汽车数据记录与传输安全的基本要求、数据记录、数据传输、数据存储、隐私保护等关键环节，为自动驾驶汽车数据记录与传输安全提供技术指导。

二、范围

本标准系统规定了自动驾驶汽车数据记录与传输安全的技术要求、安全规范和管理流程，涵盖了从数据采集、处理、存储到传输、销毁的全生命周期安全管理要求。本标准适用于所有在中国境内生产和销售的L3级及以上自动驾驶汽车的数据记录与传输系统，包括乘用车、商用车、特种车辆等各类自动驾驶车辆。在系统层面，本标准适用于自动驾驶数据记录系统（DDR）、事件数据记录器（EDR）、远程信息处理系统等关键子系统。在数据类型方面，本标准适用于车辆运行数据、环境感知数据、驾驶决策数据、车辆控制数据、用户行为数据等所有与自动驾驶相关的数据类别。具体技术内容包括数据采集规范、数据加密标准、传输协议要求、存储安全规范、隐私保护机制、安全审计要求、应急响应流程等。适用对象包括汽车整车制造商、自动驾驶系统供应商、零部件供应商、软件开发商、数据服务提供商等相关企业。需要特别说明的是，本标准不适用于军事用途的自动驾驶车辆，也不适用于非道路使用的工程机械车辆，这些应参照相应的专项标准执行。各相关企业在执行过程中可根据具体产品特性和应用场景，在本标准框架下制定更详细的技术实施方案，但核心安全要求和技术指标不得低于本标准规定。

三、规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

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

《中华人民共和国网络安全法》（2017年6月1日起施行）

《中华人民共和国数据安全法》（2021年9月1日起施行）

GB/T 40429-2021 汽车驾驶自动化分级

GB/T 39263-2020 道路车辆 网络安全工程

GB/T 37337-2019 汽车信息安全通用技术要求

ISO/SAE 21434:2021 道路车辆网络安全工程

UN R157 自动车道保持系统（ALKS）法规

四、术语和定义

下列术语和定义适用于本标准。

（一）自动驾驶数据记录系统

专门用于持续记录和存储自动驾驶系统运行期间各类数据的完整系统，通常由数据采集模块、数据处理单元、存储设备、安全保护模块等组成。该系统必须具备持续记录至少30天运行数据的能力，数据存储容量不低于2TB，应具备抗冲击、防火、防水等物理防护特性，确保在事故发生后数据可完整恢复。系统采样频率应不低于100Hz，时间同步精度误差不超过1毫秒。

（二）事件数据记录

当检测到特定事件时自动触发的数据记录过程，包括但不限于碰撞事件、系统故障、紧急制动、车道偏离等关键事件。事件触发阈值应设置合理，碰撞事件检测加速度阈值应设置在3g-5g范围内，系统故障检测应覆盖所有关键子系统。事件记录应包括事件前30秒至事件后15秒的完整数据，数据记录完整性必须达到99.9%以上。

（三）数据安全传输

采用密码学技术和管理措施，确保数据在传输过程中的机密性、完整性和可用性的全过程。必须使用国家密码管理局批准的商用密码算法，数据传输加密强度不低于 128 位，支持端到端加密。传输协议应具备前向安全性，密钥更新周期不超过 24 小时，数据传输丢包率应控制在 0.1%以内，网络延迟不超过 100 毫秒。

（四）隐私保护

在数据采集、存储、处理和传输全过程中，采取技术和管理措施保护个人隐私信息不被非法获取、使用和泄露的系统性保护机制。包括数据匿名化处理、差分隐私保护、访问权限控制、数据最小化采集等具体措施。个人身份信息的去标识化处理必须达到 k-匿名（k≥10）标准，敏感地理位置信息的模糊化处理精度不应高于 100 米。

（五）数据安全事件

导致自动驾驶相关数据遭到未经授权的访问、篡改、破坏、泄露或丢失的意外事件。根据影响程度分为三个等级：一般事件（影响单个车辆）、重大事件（影响特定车型）、特别重大事件（影响整个品牌或行业）。安全事件应急响应时间要求：一般事件不超过 4 小时，重大事件不超过 1 小时，特别重大事件必须立即响应并启动应急预案。

（六）数据完整性验证

通过数字签名、哈希校验等技术手段，验证数据在传输和存储过程中未被篡改的技术过程。必须使用国家密码管理局批准的 SM3 哈希算法进行数据完整性校验，校验失败的数据必须自动隔离并启动数据恢复流程。完整性验证周期不超过 24 小时，校验失败率应控制在 0.01%以内。

（七）安全审计日志

记录所有数据访问和操作行为的系统日志，用于安全事件追溯和责任认定。审计日志必须包含时间戳、操作类型、操作用户、数据范围、操作结果等关键信息，日志记录时间精度不低于 1 毫秒。审计日志保存期限不少于 3 年，且必须采用防篡改技术进行保护，任何修改操作都必须被记录。

（八）数据分类分级

根据数据的重要性和敏感程度，对自动驾驶相关数据进行分类和定级的管理措施。数据至少应分为四个安全级别：公开级、内部级、秘密级和绝密级。不同级别的数据应采取不同的保护措施，秘密级及以上数据必须加密存储和传输，访问权限必须严格管控，并建立详细的访问日志。数据分类准确率应达到 95%以上，分级更新周期不超过 6 个月。

五、基本要求

（一）安全原则

数据记录与传输应遵循以下原则：最小必要原则，仅采集和处理必要数据；安全可控原则，确保数据全生命周期安全；隐私保护原则，充分保护用户隐私；可追溯原则，确保数据可追溯和可审计。

（二）技术要求

系统应满足以下技术要求：数据记录完整性不低于 99.9%；数据传输实时性延迟不超过 100ms；数据存储可靠性不低于 99.99%；系统可用性不低于 99.9%。

（三）管理要求

建立完善的数据安全管理体系：制定数据安全管理制度；明确数据安全责任；建立数据安全培训机制；完善应急响应预案。安全培训覆盖率 100%，应急演练每年不少于 2 次。

六、数据记录

（一）记录内容

数据记录应包括以下内容：车辆状态数据，包括速度、加速度、位置等；环境感知数据，包括传感器原始数据、目标识别结果等；决策控制数据，包括规划轨迹、控制指令等；系统状态数据，包括软硬件状态、故障信息等。数据记录时间精度不低于 10ms。

（二）记录要求

数据记录应满足以下要求：事件触发记录响应时间不超过 50ms；连续记录数据保存时长不低于 30 天；事件数据永久保存；数据记录完整性验证周期不超过 24 小时。

（三）数据质量

数据质量应满足以下要求：数据准确性不低于 99.9%；数据完整性不低于 99.99%；时间同步精度不超过 1ms；数据格式符合标准规范。

七、数据传输

（一）传输安全

数据传输应满足以下安全要求：采用国密算法加密传输，加密强度不低于 SM4；建立双向认证机制，认证失败率不超过 0.1%；实施完整性保护，使用 HMAC-SM3 算法；支持前向安全，密钥更新周期不超过 24 小时。

（二）传输性能

传输性能应满足以下要求：传输速率不低于 100Mbps；传输延迟不超过 100ms；数据包丢失率不超过 0.1%；网络中断恢复时间不超过 5 秒。

（三）传输协议

传输协议应符合以下规范：采用 TLS 1.3 及以上安全协议；支持 MQTT、HTTP/2 等标准协议；实现数据压缩，压缩率不低于 50%；具备流量控制机制。

八、数据存储

（一）存储安全

数据存储应满足以下安全要求：采用加密存储，加密强度不低于 SM4；实施访问控制，权限分级不少于 4 级；建立审计日志，日志保存时间不少于 3 年；实现数据备份，备份周期不超过 24 小时。

（二）存储性能

存储性能应满足以下要求：存储容量可扩展，支持 PB 级存储；读写速度不低于 500MB/s；数据持久性不低于 99.999%；存储系统可用性不低于 99.9%。

（三）存储管理

存储管理应实现以下功能：自动数据分类分级；智能生命周期管理；快速数据检索，检索响应时间不超过 1 秒；安全数据销毁，销毁后数据不可恢复。

九、隐私保护

（一）隐私数据识别

应建立隐私数据识别机制：自动识别个人身份信息；分类处理敏感数据；实施去标识化处理；建立隐私数据清单。隐私数据识别准确率不低于 95%。

（二）数据脱敏

数据脱敏应满足以下要求：采用差分隐私技术，隐私预算 ε 不超过 1；实施 k-匿名处理，k 值不小于 10；支持同态加密，支持密文运算；实现数据扰动，扰动比例不超过 5%。

（三）权限控制

权限控制应实现以下功能：基于角色的访问控制；最小权限原则；多因素认证；操作审计追踪。权限变更审批率 100%。

十、安全监测

（一）实时监测

建立实时安全监测系统：监测数据访问行为；检测异常操作模式；预警安全威胁；实时阻断攻击。威胁检测准确率不低于 99%，误报率不超过 1%。

（二）安全审计

安全审计应满足以下要求：记录所有数据操作；审计日志完整性保护；异常行为分析；安全事件追溯。审计记录保存时间不少于 3 年。

（三）应急响应

应急响应应达到以下标准：安全事件 5 分钟内响应；1 小时内完成初步处置；24 小时内提交分析报告；重大问题 7 日内整改完成。

十一、测试验证

（一）安全测试

安全测试应包括：渗透测试每季度不少于 1 次；漏洞扫描每月不少于 1 次；代码审计覆盖率 100%；安全测试通过率 100%。

（二）性能测试

性能测试应验证：系统并发支持不低于 1000 连接；数据处理延迟不超过 100ms；存储吞吐量不低于 1GB/s；网络带宽利用率不低于 90%。

（三）合规验证

合规验证应确认：符合国家法律法规要求；满足行业标准规范；通过第三方认证；完成监管备案。合规项完成率 100%。

十二、质量管理

（一）质量保证

建立质量保证体系：制定质量标准；实施过程管控；开展质量评审；持续改进优化。产品出厂合格率 100%。

（二）文档管理

文档管理应做到：文档齐全完整；版本受控管理；变更规范有序；归档及时准确。文档齐套率 100%。

（三）变更管理

变更管理应实现：变更申请审批率 100%；变更影响分析覆盖率 100%；变更测试通过率 100%；变更记录完整率 100%。

十三、附则

本标准由广西电子商务企业联合会负责解释。本标准自发布之日起试行，试行期为一年。试行期满后，根据实施反馈情况进行修订和完善。各相关单位可依据本标准制定具体的实施细则。若本标准与国家新颁布的法律法规或强制性标准有不一致之处，应以国家法律法规和强制性标准为准。本标准所引用的规范性引用文件如有更新，其最新版本适用于本标准。广西电子商务企业联合会将根据技术发展和应用需求，适时组织对本标准的复审与修订工作，以保障其持续的先进性和适用性。本标准的有效实施，有赖于汽车制造商、零部件供应商、技术服务商和各相关方的共同努力，通过规范自动驾驶汽车数据记录与传输安全技术要求，保障自动驾驶汽车数据安全，促进自动驾驶技术健康发展，保护用户隐私和公共利益，推动智能网联汽车产业高质量发展。