ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL　—2026

车载工程系统信息安全防护技术要求

Technical Requirements for Information Security Protection of Vehicle-mounted Engineering Systems

（工作组讨论稿）

（本草案完成时间：2026-01-29）

2026 - - 发布　　2026 - - 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。

车载工程系统信息安全防护技术要求

1 引言

随着我国汽车智能化、网联化产业持续升级，车载工程系统已发展成为复杂信息物理系统，广泛应用于特种作业等国家重点领域，是培育新质生产力、推进交通强国建设的重要支撑。当前，该系统面临的网络攻击、数据泄露等安全风险日趋突出，直接关系国家安全、公共安全及人身安全。为落实《网络安全法》等相关法律法规要求，践行车联网安全国家战略，提升车载工程系统信息安全防护能力，筑牢关键信息基础设施安全防线，特制定本标准。本标准明确车载工程系统信息安全防护的技术与管理规范，为相关产品设计、开发、生产、运维全流程提供权威技术依据，引领行业安全有序发展，助力产业实现自主可控。

2 范围

规定了车载工程系统信息安全防护的基本原则、总体框架、技术防护要求、安全管理要求及测试评价方法，为网络安全等级保护在车载领域的落地实施提供支撑。适用于车载工程系统设计、开发、生产、运营、维护等相关组织及管理部门，涵盖国家重点领域应用的车载工程系统，为相关产品市场准入、合规审查提供技术支撑。

3 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，仅所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（包括所有修改单）适用于本标准。

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

GB/T 25069-2022 信息安全技术术语

GB/T 35273-2020 信息安全技术个人信息安全规范

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 18336.3-2022 信息技术安全技术 IT 产品安全评估准则第 3 部分：评估方法

GB/T 40856-2021 车载信息交互系统信息安全技术要求

YD/T 3746-2020 车联网信息服务用户个人信息保护要求

ISO/SAE 21434:2021 道路车辆-网络安全工程

（注：本标准立足我国车载工程系统发展实际，参考国内外相关技术与标准最新动态，结合国家安全战略部署，形成符合我国国情的信息安全防护规范。）

4 术语和定义

GB/T 25069-2022 界定的以及下列术语和定义，适用于本标准。

4.1 车载工程系统

指车辆上用于实现特定工程功能的电子、电气、软件及通信系统的集合，涵盖国家重点领域应用的相关系统，功能超越常规乘用车范畴，是我国智能交通、制造业数字化转型的重要组成部分。

4.2 信息安全防护

为保护车载工程系统硬件、软件及数据安全，防范各类信息安全风险，符合国家相关法律法规要求，所采取的各类技术与管理措施的总称，兼顾国家安全、公共安全与个人合法权益。

4.3 安全要素

构成车载工程系统信息安全的核心组成部分，包括但不限于硬件安全、软件安全、通信安全、数据安全，是落实网络安全等级保护要求的关键载体。

4.4 安全生命周期

指车载工程系统从概念设计、开发、生产、运维至报废的全流程，需全面融入信息安全活动，落实数据安全全生命周期管理要求，建立常态化、规范化安全管控机制。

5 基本原则

5.1 安全与功能并重原则

立足国家产业发展与安全战略，信息安全防护与车载工程系统功能同步规划、同步设计、同步实施、

同步运维，实现安全防护与工程效能协同提升。

5.2 纵深防御原则

契合网络安全等级保护核心要求，在车载工程系统各层次（边界、网络、主机、应用、数据）部署多层异构安全防护措施，构建协同联动的防御体系，提升系统抗攻击能力。

5.3 最小权限原则

遵循国家安全管控要求，对用户、进程及系统组件仅授予执行其任务所必需的最小访问权限，严格限制超额权限，从源头防范权限滥用带来的安全风险。

5.4 默认安全原则

落实“安全优先”部署，车载工程系统默认配置需处于安全状态，规范默认账号、密码管理，从源头降低安全隐患。

5.5 生命周期管理原则

对接国家相关标准要求，安全防护覆盖车载工程系统全生命周期，建立持续风险管理与安全更新机制，实现安全防护长效化。

6 信息安全防护总体框架

立足国家安全战略部署，以保障国家安全、公共安全和个人信息权益为核心，构建涵盖技术防护与安全管理的一体化信息安全防护体系，引领行业标准化发展，支撑关键信息基础设施安全保障工作。

6.1 资产识别与分类

全面识别车载工程系统内各类关键资产，重点识别涉及国家安全的核心资产，依据资产价值及安全影响程度实施分类分级管理，符合国家数据分类分级保护要求。

6.2 威胁分析与风险评估

结合我国车载工程系统面临的网络安全威胁态势，系统性识别潜在威胁与系统脆弱性，重点防范境外网络攻击、数据窃取等风险，科学评估风险发生概率及影响程度，明确风险处置优先级，形成完整风险评估报告。

6.3 防护策略与要求

基于风险评估结果，结合国家相关法律法规及标准规范，制定并实施针对性安全防护策略与要求，优先保障核心资产安全，将安全风险降至国家认可的可接受水平。

6.4 安全监控与事件响应

建立车载工程系统安全状态监控、安全事件检测、预警及应急响应机制，对接国家网络安全态势感知平台，规范安全事件上报流程，最大限度降低安全事件造成的损失。

6.5 持续改进

对接国家网络安全漏洞通报机制，跟踪国内外车载工程系统信息安全技术发展趋势，结合安全监控结果、事件处置经验及测试评估结论，持续优化安全防护措施，完善标准落地实施路径，助力产业实现自主可控。

7 技术防护要求

7.1 硬件安全

7.1.1 安全启动：关键控制单元需具备国家商用密码管理局认可的安全启动功能，确保系统固件与引导代码的完整性、真实性，未经授权的代码不得执行；优先采用我国自主研发的信任锚技术，提升硬件安全自主可控水平。

7.1.2 硬件信任根：关键安全域需配备硬件信任根（如安全芯片、硬件安全模块 HSM），优先采用国产产品，符合国家商用密码及网络安全等级保护要求，用于安全存储密钥、执行密码运算及提供可信执行环境。

7.1.3 物理防护：对安全芯片、调试接口等关键硬件组件，采取高强度物理防护措施，防止物理篡改与非授权物理访问，防范境外势力通过物理手段窃取核心信息。

7.1.4 硬件接口安全：对 JTAG、UART 等调试接口及生产测试接口，实施严格访问控制机制，规范访问流程；重要接口需具备失效后安全恢复能力，接口访问日志需完整留存、可追溯，符合网络安全等级保护要求。

7.2 软件安全

7.2.1 安全设计与开发：将安全实践全面融入软件开发生命周期，符合网络安全等级保护要求，开展安全需求分析、安全架构设计、安全编码（遵循 MISRA C 等编码规范）、代码安全审查及静态/动态应用安全测试（SAST/DAST），建立软件安全缺陷分级管理机制。

7.2.2 软件完整性保护：运行在关键部件上的软件需具备完整性校验能力，防止恶意篡改；采用国家商用密码算法实现数字签名与验签机制，软件更新包必须经过签名验证，确保更新包的真实性、完整性，防范恶意更新攻击。

7.2.3 最小化与隔离：软件开发遵循最小功能原则，剔除冗余功能以减少安全攻击面；采用内存保

护、访问控制、虚拟化或容器化等技术，实现不同安全等级、不同功能模块间的有效隔离，防范攻击跨模块扩散，保障核心软件功能安全。

7.2.4 安全更新：建立安全可靠的无线（OTA）及有线软件更新机制，保障更新包的机密性、完整性、真实性和可用性，防止回滚攻击、中间人攻击；支持更新失败后的安全恢复功能，更新日志完整留存、可追溯。

7.3 通信安全

7.3.1 车内通信安全：对 CAN、CAN FD、Ethernet 等车内关键总线的安全相关报文，实施身份认证、消息认证码（MAC）或加密等保护措施，采用国家商用密码算法，防止重放、篡改、伪造等攻击，保障车内通信安全。采用访问控制、防火墙或入侵检测/防御系统（IDS/IPS）等技术，对动力域、信息娱乐域等车内不同网络域实施逻辑隔离或物理隔离，规范域间数据传输，防范攻击跨域扩散。

7.3.2 车外通信安全：所有 V2X、蜂窝网络、Wi-Fi、蓝牙等车外通信连接，需采用符合国家商用密码标准的强加密协议（如 TLS 1.2 及以上版本、IPSec）实施端到端或链路保护，确保传输数据的机密性、完整性，应对境外网络监听、数据窃取风险。建立严格的接入认证机制，采用多因素认证及基于国家商用密码的认证方式，验证远程服务端或对等节点身份，防止非法接入，防范境外非法节点攻击系统。加强 OBD-II 端口、T-Box 接口等外部通信接口的访问控制与安全监测，规范接口使用权限及流程，完整留存接口访问日志，防范通过外部接口实施的网络攻击，符合网络安全等级保护边界防护要求。强化跨境通信安全管控，涉及核心数据、重要数据的车外通信，需符合国家数据出境安全管理相关要求，严禁核心数据非法出境，防范境外势力窃取我国车载工程系统核心信息。

7.4 数据安全

7.4.1 数据分类分级：对车载工程系统处理、存储、传输的各类数据实施分类分级管理（分为公开数据、内部数据、敏感数据、重要数据、核心数据），严格遵循国家数据分类分级保护要求，明确各级数据的保护标准与管控措施，重点加强敏感数据、重要数据、核心数据的安全防护，保障国家关键数据安全。

7.4.2 数据机密性：用户身份信息、地理轨迹、控制指令、密钥等敏感数据，在存储与传输过程中需采用符合国家密码管理规定的密码算法加密保护；密钥实施全生命周期安全管理，遵循国家商用密码密钥管理相关标准，防范密钥泄露、滥用。

7.4.3 数据完整性：关键配置数据、安全日志、程序数据等需实施完整性保护，采用国家商用密码算法实现的完整性校验机制，防止未授权修改，确保数据真实有效，为安全事件追溯、系统故障排查提供可靠依据。

7.4.4 数据可用性：建立关键安全功能所需数据的备份、恢复机制，定期开展数据备份演练，防止因网络攻击、系统故障导致的数据丢失或不可用，保障车载工程系统核心功能正常运行。

7.4.5 个人信息保护：严格遵循《个人信息保护法》《数据安全法》及 GB/T 35273-2020、YD/T 3746-2020 相关要求，依法处理车主、驾驶员、乘客等个人信息，遵循合法、正当、必要、诚信原则，明示收集使用规则，保障个人的知情权、同意权、访问权、更正删除权等合法权益，严禁非法收集、滥用、泄露个人信息。

7.4.6 日志与审计：完整记录访问尝试、配置变更、异常行为、数据操作等关键安全事件日志，日志内容需包含时间戳、事件类型、主体、客体、结果等足够信息，确保日志自身不被篡改、非法删除；涉及国家安全、公共安全的核心日志留存时间不少于 365 天，普通日志留存时间不少于 180 天，日志可对接国家网络安全态势感知平台，满足国家审计、监管要求。

7.5 身份认证与访问控制

7.5.1 身份认证：对访问车载工程系统资源（如诊断服务、管理后台、关键数据）的用户、设备、应用程序，全面实施强身份认证，符合网络安全等级保护身份认证相关要求；采用多因素认证或基于国家商用密码的认证机制，严禁使用弱口令、默认口令，防范身份伪造、冒用风险。

7.5.2 访问控制：实施基于角色的访问控制（RBAC）或属性基访问控制（ABAC）机制，严格遵循最小权限原则，明确各级角色的访问范围与权限，建立权限动态调整与定期审计机制，及时撤销冗余权限，防范权限滥用。

7.6 漏洞与风险管理

7.6.1 漏洞管理：建立健全漏洞管理全流程机制，对接国家网络安全漏洞通报机制，及时获取各类漏洞信息，开展漏洞分析、风险评估、修复及验证工作；对已知高危漏洞，需在获取相关信息后 90 天内制定修复方案并启动修复，中低危漏洞需在合理期限内完成修复，修复后需进行安全验证，确保漏洞彻底消除。

7.6.2 安全配置：制定明确的车载工程系统安全配置基线，符合网络安全等级保护安全配置相关要求，确保所有系统组件均按照安全基线配置；定期开展安全配置检查，及时发现并整改配置偏差；建立安全配置变更管理机制，配置变更需经过审批、完整记录，确保配置变更可追溯、可审计，持续维持系统安全状态。

8 安全管理要求

8.1 组织与职责

设立或明确负责车载工程系统信息安全管理的组织或岗位，明确其职责与权限，接受国家网络安全、数据安全监管部门的指导与监督；配备专业信息安全管理人员，建立健全信息安全管理制度与工作流程，确保信息安全管理工作常态化、规范化开展。

8.2 安全生命周期管理

建立并严格实施覆盖车载工程系统概念设计、开发、集成、验证、生产、运维及报废全阶段的信息安全管理流程，符合 ISO/SAE 21434:2021 基本原则，结合我国网络安全、数据安全相关要求，细化各阶段安全管理措施；重点加强核心数据、密钥的全生命周期管理，系统报废阶段需规范开展数据销毁、硬件处置工作，防范信息泄露。

8.3 供应链安全管理

落实国家供应链安全战略要求，建立健全车载工程系统供应链安全管理体系，对供应商、外包开发方提出明确信息安全要求并实施严格安全评估；开展供应商安全准入、持续监控及退出管理，重点管控境外供应商带来的安全风险，确保其提供的产品、服务符合本标准及国家相关要求，防范供应链攻击，保障供应链安全、自主可控。

8.4 安全开发流程

建立并严格执行符合网络安全等级保护要求的安全软件开发流程，将安全活动全面融入需求分析、设计、编码、测试等各个环节；建立软件安全缺陷管理机制，规范缺陷发现、上报、修复、验证流程，确保开发的软件符合本标准技术要求，从源头提升软件安全质量。

8.5 安全测试与评估

制定完善的安全测试计划，委托具备国家认可资质的第三方测试机构，开展渗透测试、模糊测试、漏洞扫描等各类安全测试，验证安全措施的有效性；每年至少开展一次安全风险评估，系统发生重大变更时需额外补充评估，形成测试报告、风险评估报告，针对发现的问题及时整改，测试与评估结果需报相关监管部门备案，作为合规审查、市场准入的重要依据。

8.6 应急响应与处置

制定符合国家网络安全事件应急处置相关要求的信息安全事件应急预案，明确事件分类分级标准、处置流程、恢复措施及报告机制，对接国家网络安全应急响应体系；每年至少开展一次应急演练，持续优化应急预案，提升应急处置能力；发生重大信息安全事件时，需按照国家相关规定及时上报，快速开展处置工作，减少事件造成的损失，防范事件扩大蔓延，保障国家安全、公共安全。

8.7 安全意识与培训

定期组织相关员工开展信息安全意识教育与技能培训，结合国家网络安全、数据安全相关法律法规及本标准要求，开展针对性培训，提升员工信息安全意识与安全操作技能；重点加强核心岗位人员的安全培训与考核，建立培训档案，确保员工具备相应的安全防护能力，防范人为因素带来的安全风险。

9 测试与评价方法

9.1 测试目标

验证车载工程系统是否符合本标准规定的各项信息安全技术要求与安全管理要求，是否满足国家网络安全、数据安全相关法律法规及战略部署需求；评估系统信息安全防护能力，识别安全隐患，为系统合规审查、市场准入、安全整改提供权威技术依据，保障系统安全可靠运行，筑牢国家关键信息基础设施安全防线。

9.2 测试环境

测试需在能够模拟车载工程系统真实运行环境或接近真实运行环境的测试平台上开展，测试环境需符合国家信息安全测试相关要求，具备安全性、独立性、可重复性，避免测试过程对真实系统、数据造成影响；同时需具备模拟各类网络攻击、安全事件的能力，全面检验系统安全防护效果。

9.3 测试内容与方法

9.3.1 审查与访谈：审查安全设计文档、系统配置文档、信息安全管理制度、测试报告、风险评估报告等相关资料，核实资料的完整性、规范性，确认其符合本标准及国家相关要求；访谈相关管理人员、技术人员，核实安全措施落地情况，评估信息安全管理工作的有效性。

9.3.2 静态分析：对软件代码、系统固件开展静态应用安全测试及二进制分析，检测代码中的安全缺陷、漏洞，评估软件编码质量，验证软件安全设计的合理性与合规性，防范因代码缺陷带来的安全风险。

9.3.3 动态测试：开展渗透测试（涵盖车内网络、外部接口、无线通信、Web/APP 后端等场景）、模糊测试、通信协议安全测试，模拟各类网络攻击行为，检验系统的抗攻击能力，识别系统脆弱性，评估通信安全防护效果。

9.3.4 功能验证：验证安全启动、安全更新、加密解密、身份认证、访问控制、数据保护、日志审计等各类安全功能的正确实现，确保各项安全功能符合本标准技术要求，能够有效防范各类信息安全风险，保障系统、数据安全。

9.3.5 漏洞扫描：使用专业漏洞扫描工具，对车载工程系统硬件、软件、网络设备等各类组件进行

已知漏洞扫描，对接国家漏洞数据库，及时发现系统存在的已知漏洞，评估漏洞风险等级，为漏洞修复工作提供依据。

9.4 评价准则

根据测试结果，对照本标准第 7 章技术防护要求、第 8 章安全管理要求及国家相关法律法规、标准规范，逐项评价车载工程系统的符合性。本标准中所有“应”条款均为强制性要求，任何一项不满足，即判定系统不符合本标准要求；对于涉及国家安全、公共安全的高风险项，实行一票否决制，直接判定系统不符合本标准要求。测试与评价结果需形成正式测试评价报告，明确评价结论、存在问题及整改建议，作为国家监管、合规审查的重要依据，推动车载工程系统信息安全防护水平持续提升，助力我国智能网联汽车产业高质量、安全有序发展。

10 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，有赖于各级医疗机构、主管部门、技术服务商和各相关方的共同努力，通过规范智慧医院数据互联互通共享技术，推动医疗健康数据资源有效整合与安全共享，提升医疗服务质量和效率，促进智慧医院建设规范化发展，为推进健康中国建设提供技术支撑。