ICS 43.020
CCS T 40

中华人民共和国国家标准

GB 44495—2024

汽车整车信息安全技术要求

Technical requirements for vehicle cybersecurity

2024-08-23 发布　　2026-01-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件技术内容参考了联合国技术法规UN R155《关于批准车辆信息安全和信息安全管理体系的统一规定》。

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。

本文件由中华人民共和国工业和信息化部提出并归口。

汽车整车信息安全技术要求

1 范围

本文件规定了汽车信息安全管理体系要求、信息安全基本要求、信息安全技术要求及同一型式判定，描述了相应的检查与试验方法。

本文件适用于M类、N类及至少装有1个电子控制单元的O类车辆。

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 40861 汽车信息安全通用技术要求

GB/T 44373 智能网联汽车 术语和定义

GB/T 44464—2024 汽车数据通用要求

GB 44496 汽车软件升级通用技术要求

3 术语和定义

GB/T 40861、GB/T 44373、GB 44496界定的以及下列术语和定义适用于本文件。

3.1

汽车信息安全 vehicle cybersecurity

汽车的电子电气系统、组件和功能被保护，使其资产不受威胁的状态。

[来源：GB/T 40861—2021，3.1]

3.2

汽车信息安全管理体系 cybersecurity management system；CSMS

基于风险的系统方法。

注：包括组织流程、责任和治理，以处理与车辆网络威胁相关的风险并保护车辆免受网络攻击。

[来源：GB/T 44373—2024，3.11，有修改]

3.3

风险 risk

车辆信息安全不确定性的影响。

注：风险用攻击可行性和影响表示。

3.4

风险评估 risk assessment

发现、识别和描述风险，理解风险的性质以及确定风险级别，并将风险分析的结果与风险标准进行比较，以确定风险是否可接受的过程。

3.5

威胁 threat

可能导致系统、组织或个人受到损害的意外事件的潜在原因。

3.6

漏洞　vulnerability

在资产或缓解措施中，可被一个或多个威胁利用的弱点。

3.7

车载软件升级系统　on-board software update system

安装在车端并具备直接接收、分发和校验来自车外的升级包等用于实现软件升级功能的软件和硬件。

[来源：GB 44496—2024，3.12]

3.8

在线升级　over-the-air update

通过无线方式而不是使用电缆或其他本地连接方式将升级包传输到车辆的软件升级。

注 1："在线升级"也称"远程升级"。

注 2："本地连接方式"一般指通过车载诊断(OBD)接口、通用串行总线(USB)接口等进行的物理连接方式。

[来源：GB 44496—2024，3.3]

3.9

离线升级　offline update

除在线升级外的软件升级。

[来源：GB 44496—2024，3.13]

3.10

敏感个人信息　sensitive personal information

一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息。

注：包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

4　缩略语

下列缩略语适用于本文件。

CAN：控制器局域网络(Controller Area Network)

ECU：电子控制单元(Electronic Control Unit)

HSM：硬件安全模块(Hardware Security Module)

NFC：近场通信(Near Field Communication)

OBD：车载诊断(On-Board Diagnostics)

RFID：射频识别(Radio Frequency Identification)

USB：通用串行总线(Universal Serial Bus)

VLAN：虚拟局域网(Virtual Local Area Network)

VIN：车辆识别代号(Vehicle Identification Number)

V2X：车辆与车外其他设备之间的无线通信(Vehicle to Everything)

WLAN：无线局域网(Wireless Local Area Networks)

5　汽车信息安全管理体系要求

5.1　车辆制造商应具备车辆全生命周期的汽车信息安全管理体系。

注：车辆全生命周期包括车辆的开发阶段、生产阶段及后生产阶段。

5.2 汽车信息安全管理体系应包括以下内容。

——建立企业内部管理汽车信息安全的过程。

——建立识别、评估、分类、处置车辆信息安全风险及核实已识别风险得到处置的过程，并确保车辆风险评估保持最新状态。

——建立用于车辆信息安全测试的过程。

——建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：

- 包含漏洞管理机制，明确漏洞收集、分析、报告、处置、发布、上报等活动环节；
- 建立针对网络攻击提供相关数据并进行分析的过程，如通过车辆数据和车辆日志分析和检测网络攻击、威胁和漏洞；
- 建立确保对网络攻击、网络威胁和漏洞进行持续监控的过程，且车辆纳入监控范围的时间应不晚于车辆注册登记的时间；
- 建立确保已识别的网络攻击、网络威胁和漏洞得到响应，且在时限内得到处置的过程；
- 建立评估所实施的信息安全措施在发现新的网络攻击、网络威胁和漏洞的情况下是否仍然有效的过程。

——建立管理企业与合同供应商、服务提供商、车辆制造商子组织之间汽车信息安全依赖关系的过程。

6 信息安全基本要求

6.1 车辆产品开发流程应遵循汽车信息安全管理体系要求。

6.2 车辆制造商应识别和管理车辆与供应商相关的风险。

6.3 车辆制造商应识别车辆的关键要素，对车辆进行风险评估，并管理已识别的风险。

注 1：风险评估的范围包含车辆的各个要素及其相互作用，并进一步考虑与外部系统的相互作用。

注 2：关键要素包括但不限于有助于车辆安全、环境保护或防盗的要素，以及提供连接性的系统部件或车辆架构中对信息安全至关重要的部分等。

6.4 车辆制造商应采取基于第 7 章要求的处置措施保护车辆不受风险评估中已识别的风险影响。若处置措施与所识别的风险不相关，车辆制造商应说明其不相关性。若处置措施不足以应对所识别的风险，车辆制造商应实施其他的措施，并说明其使用措施的合理性。

6.5 如有专用环境，车辆制造商应采取措施，以保护车辆用于存储和执行后装软件、服务、应用程序或数据的专用环境。

注：如沙箱专用环境等。

6.6 车辆制造商应通过测试来验证所实施的信息安全措施的有效性。

6.7 车辆制造商应针对车辆实施相应措施，以确保具备以下能力：

——针对车辆网络攻击的识别能力；

——针对与车辆相关的网络攻击、网络威胁和漏洞的监测能力及数据取证能力。

6.8 车辆制造商应使用公开的、已发布的、有效的密码算法，应根据不同密码算法和业务场景，选择适当的参数和选项。

6.9 车辆制造商应满足以下密码模块要求之一：

——采用符合国际、国家或行业标准要求的密码模块；

——未采用国际、国家或行业标准要求的密码模块，说明使用的合理性。

6.10 车辆应采用默认安全设置，如 WLAN 的默认连接口令应满足复杂度的要求。

6.11 汽车数据处理活动中的数据车内处理、默认不收集、精度范围适用、脱敏处理、个人同意及显著告知等要求，应符合 GB/T 44464—2024 中 4.2.2 的规定。

7 信息安全技术要求

7.1 外部连接安全要求

7.1.1 通用安全要求

7.1.1.1 车端具备远程控制功能的系统、授权的第三方应用等外部连接系统不应存在由汽车行业权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞。

注1：汽车行业权威漏洞平台如车联网产品专用漏洞库NVDB-CAVD等政府主管部门认可的其他漏洞平台。

注2：处置包括消除漏洞、制定减缓措施等方式。

7.1.1.2 车辆应关闭非业务必要的网络端口。

7.1.2 远程控制安全要求

7.1.2.1 应对远程控制指令信息进行真实性和完整性验证。

7.1.2.2 应对远程控制指令设置访问控制，禁用非授权的远程控制指令。

7.1.2.3 应具备记录远程控制指令的安全日志功能，安全日志记录的内容至少包括远程控制指令的时间、发送主体、远程控制对象、操作结果等，留存相关的安全日志应不少于6个月。

7.1.2.4 应对车端具备远程控制功能的系统进行完整性验证。

7.1.3 第三方应用安全要求

7.1.3.1 应对授权的第三方应用的真实性和完整性进行验证。

注：第三方应用是指车辆制造商及其供应商之外的其他实体提供的面向用户提供服务的应用程序，包括第三方娱乐应用等。

7.1.3.2 应对非授权的第三方应用的安装进行提示，并对已安装的非授权的第三方应用进行访问控制，限制此类应用直接访问系统资源、个人信息等。

7.1.4 外部接口安全要求

7.1.4.1 应对车辆外部接口进行访问控制保护，禁止非授权访问。

注：外部接口包括USB接口、诊断接口和其他可直接接触的物理接口。

7.1.4.2 应对车辆USB接口、SD卡接口接入设备中的文件进行访问控制，仅允许读写指定格式的文件或安装执行指定签名的应用软件。

7.1.4.3 车辆应对USB接口接入设备中的病毒风险进行处置。

7.1.4.4 通过诊断接口向车辆发送关键配置及标定参数的写操作指令时，车辆应采用身份鉴别或访问控制等安全策略。

7.2 通信安全要求

7.2.1 车辆与车辆制造商云平台通信时，应对其通信对象的身份真实性进行验证。

7.2.2 车辆与车辆、路侧单元、移动终端等进行V2X直连通信时，应进行证书有效性和合法性的验证。

7.2.3 车辆应采用完整性保护机制保护除RFID、NFC之外的外部无线通信通道。

7.2.4 车辆应具备对来自车辆外部通信通道的数据操作指令的访问控制机制。

注：来自车辆外部通信通道的数据操作指令包括代码注入、数据操纵、数据覆盖、数据擦除和数据写入等指令。

7.2.5 车辆应验证所接收的外部关键指令数据的有效性或唯一性。

示例：针对远程控制服务器发送的车控指令，车端可通过网关验证该类指令的有效性或唯一性。

注：关键指令数据是指可能影响行车和财产安全的指令数据，包括但不限于车控指令数据。

7.2.6 车辆应对向车外发送的敏感个人信息实施保密性保护措施。

7.2.7 车辆应具备安全机制防御物理操纵攻击，至少具备与外部直接无线通信的零部件的身份识别机制。

注：与外部存在直接无线通信的零部件包括但不限于车载信息交互系统等，不包括短距离无线传感器。

7.2.8 车辆与外部直接无线通信的零部件应具备安全机制防止非授权的特权访问。

注：非授权用户可能通过调试接口获得系统的根用户或特权用户权限。

7.2.9 车辆应对内部网络进行区域划分并对区域边界进行防护。车辆内部网络跨域请求应进行访问控制，并遵循默认拒绝原则和最小化授权原则。

注：区域边界防护措施包括物理隔离、逻辑隔离（如采用白名单、防火墙、VLAN）等。

7.2.10 车辆应具备识别车辆通信通道遭受拒绝服务攻击的能力，并对攻击进行相应的处理。

注 1：对攻击的处理包括对攻击数据包的拦截或丢弃、受影响系统的自动恢复、日志记录等。

注 2：车辆通信通道包括移动蜂窝通信、V2X、CAN 总线、车载以太网等。

7.2.11 车辆应具备识别恶意的 V2X 数据、恶意的诊断数据的能力，并采取保护措施。

注：V2X 数据包括路侧单元发送到车辆的数据、车辆与车辆之间的数据。

7.2.12 应具备记录关键的通信信息安全事件日志的功能，日志存储时长应不少于 6 个月。

注：关键的通信信息安全事件由车辆制造商根据风险评估的结果确定，日志记录内容包括事件时间、事件原因等。

7.3 软件升级安全要求

7.3.1 通用安全要求

7.3.1.1 车载软件升级系统应通过安全保护机制，保护车载软件升级系统的可信根、引导加载程序、系统固件不被篡改，或在被篡改后，通过安全保护机制使其无法正常启动。

7.3.1.2 车载软件升级系统不应存在由汽车行业权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。

注 1：汽车行业权威漏洞平台如车联网产品专用漏洞库 NVDB-CAVD 等政府主管部门认可的其他漏洞平台。

注 2：处置包括消除漏洞、制定减缓措施等方式。

7.3.2 在线升级安全要求

7.3.2.1 车辆和在线升级服务器应进行身份认证，验证其身份的真实性，并在下载中断恢复时重新验证。

注：常见的认证方式包括使用证书进行身份认证。

7.3.2.2 车辆应对下载的升级包进行真实性和完整性验证。

7.3.2.3 应对在线升级过程中发生的信息安全事件日志进行记录，日志存储时长应不少于 6 个月。

7.3.3 离线升级安全要求

7.3.3.1 若车辆使用车载软件升级系统进行离线升级，车辆应对离线升级包真实性和完整性进行验证。

7.3.3.2 若车辆不使用车载软件升级系统进行离线升级，应采取保护措施保证刷写接入端的安全性，或验证升级包的真实性和完整性。

7.4 数据安全要求

7.4.1 车辆应采取安全访问技术或安全存储技术保护存储的对称密钥和非对称密钥中的私钥，防止其被非授权访问和获取。

7.4.2 车辆应采取安全访问技术、加密技术或其他安全技术保护存储在车内的敏感个人信息，防止其被非授权访问和获取。

7.4.3 车辆应采取安全防御机制保护存储在车内的 VIN 等用于车辆身份识别的数据，防止其被非授权删除和修改。

注：防止数据被非授权删除和修改的安全防御机制包括安全访问技术、只读技术等。

7.4.4 车辆应采取安全防御机制保护存储在车内的关键数据，防止其被非授权删除和修改。

注：关键数据包括制动参数、安全气囊展开阈值、动力电池参数等关键配置参数，以及其他车辆运行过程中产生的可能影响行车安全的数据。

7.4.5 车辆应采取安全防御机制保护存储在车内的安全日志，防止其被修改和非授权删除。

7.4.6 车辆应具备个人信息删除功能，该功能可删除的信息不应包括法律、行政法规、强制性国家标准中规定必须保留的个人信息。

7.4.7 车辆不应直接向境外传输数据。

注：用户使用浏览器访问境外网站、使用通信软件向境外传递消息、自主安装可能导致数据出境的第三方应用等用户自主行为不受本条款限制。

8 检查与试验方法

8.1 总则

检查及试验方法包括汽车信息安全管理体系检查、基本要求检查和技术要求测试：

——针对车辆制造商信息安全保障能力相关的文档进行检查，确认车辆制造商满足第 5 章的要求；

——针对车辆在开发、生产等过程中信息安全相关的文档进行检查，确认测试车辆满足第 6 章的要求；

——基于车辆所识别的风险以及第 7 章车辆技术要求处置措施的相关性，依据 8.3 确认车辆信息安全技术要求的测试范围，并依据测试范围开展测试，确认车辆满足第 7 章的要求。

注：测试范围包括第 7 章与待测试车辆的适用条款、各适用条款对应的测试对象等。

8.2 信息安全基本要求检查

8.2.1 检查要求

8.2.1.1 车辆制造商应具备文档来说明车辆在开发、生产等过程的信息安全情况，文档包括提交的文档和留存备查的文档。

8.2.1.2 提交的文档应为中文版本，并至少包含如下内容：

——证明车辆满足第 6 章要求的总结文档；

——写明文档版本信息的留存备查文档清单。

8.2.1.3 车辆制造商应以安全的方式在本地留存车辆信息安全相关过程文档备查，完成检查后应对留存备查的文档进行防篡改处理。

8.2.1.4 车辆制造商应对提交和留存备查的文档与车辆的一致性、可追溯性做出自我声明。

8.2.2 检查方法

8.2.2.1 检查车辆制造商提交的文档，确认检查方案，包括检查范围、检查方式、检查日程、现场检查必要的证明文件清单。

8.2.2.2 应依据 8.2.2.1 确认的检查方案，在车辆制造商现场检查留存备查的信息安全相关过程文档，确认车辆是否满足第 6 章的要求。

8.3 信息安全技术要求测试

8.3.1 测试条件

8.3.1.1 测试环境要求

涉及无线短距离通信的测试，应保证车辆在无信号干扰的测试环境中进行。

8.3.1.2 测试状态要求

测试样件包括整车及 8.1 确定的测试范围中涉及的零部件，应满足以下要求：

——测试样件可正常运行；

——整车信息安全相关功能处于开启状态；

——测试过程中，若测试车辆速度大于 0 km/h 或测试车辆可能发生非预期启动，则将测试车辆置于整车转毂试验台或保证车辆安全运行的道路环境中开展测试。

8.3.1.3 测试输入要求

车辆制造商应依据 8.1 确定的测试范围，提供必要的测试输入支持完成测试。

8.3.2 外部连接安全测试

8.3.2.1 通用安全测试

8.3.2.1.1 系统漏洞安全测试

测试人员应使用漏洞扫描工具对车辆外部连接系统进行漏洞扫描，并将测试结果与汽车行业权威漏洞平台 6 个月前公布的高危及以上的安全漏洞清单和车辆制造商提供的车辆外部连接系统漏洞处置方案进行比对，判定车辆是否满足 7.1.1.1 的要求。

8.3.2.1.2 非业务必要网络端口安全测试

测试人员应依据车辆制造商提供的车辆业务端口列表，通过 WLAN、车载以太网、蜂窝网络等通信通道将测试车辆与扫描测试设备组网，使用扫描测试设备测试车辆所开放的端口，并将测试得到的车辆开放端口列表与车辆业务端口列表进行比对，判定车辆是否满足 7.1.1.2 的要求。

8.3.2.2 远程控制安全测试

8.3.2.2.1 真实性和完整性验证安全测试

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足 7.1.2.1 的要求：

a) 登录车辆远程控制程序账户，测试是否可触发正常的远程车辆控制指令；

b) 伪造、篡改并发送远程车辆控制指令，检查是否可伪造、篡改该指令，车辆是否执行该指令。

8.3.2.2.2 远程控制指令权限控制安全测试

测试人员应依据车辆制造商提供的车辆远程控制指令应用场景和使用权限文件，构造并发送超出权限的远程控制指令，判定车辆是否满足 7.1.2.2 的要求。

8.3.2.2.3 安全日志记录安全测试

测试人员应按照以下测试方法依次开展测试，判定是否满足 7.1.2.3 的要求：

a） 触发车辆远程控制功能，检查是否存在安全日志，安全日志记录的内容是否包含远程控制指令的时间、发送主体、远程控制对象、操作结果等信息；

b） 检查安全日志记录的时间跨度是否不少于 6 个月或是否具备留存安全日志不少于 6 个月的能力。

8.3.2.2.4 完整性安全测试

测试人员应根据车辆制造商提供的车辆远程控制功能系统完整性验证功能的证明文件，判定车辆是否满足 7.1.2.4 的要求。

8.3.2.3 第三方应用安全测试

8.3.2.3.1 真实性完整性验证安全测试

测试人员应获取授权的第三方应用，使用工具篡改其代码，并安装、执行篡改后的授权第三方应用，判定车辆是否满足 7.1.3.1 的要求。若篡改后的授权第三方应用被限制访问超出访问控制权限的资源，视为应用非正常运行，满足要求。

8.3.2.3.2 访问控制安全测试

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足 7.1.3.2 的要求：

a） 安装非授权的第三方应用，测试车辆是否进行提示；

b） 使用已安装的非授权第三方应用访问超出访问控制权限的资源，测试是否可访问控制权限外的资源。

8.3.2.4 外部接口安全测试

8.3.2.4.1 外部接口访问控制安全测试

测试人员应依据车辆制造商提供的车辆外部接口的总结文档或车辆外部接口清单，使用非授权的用户或工具访问车辆的外部接口，判定车辆是否满足 7.1.4.1 的要求。

8.3.2.4.2 USB 接口、SD 卡接口访问控制安全测试

测试人员应依据车辆制造商提供的 USB 接口、SD 卡接口的总结文档或 USB 接口、SD 卡接口支持的文件类型清单，分别在具备 USB 接口、SD 卡接口的移动存储介质中注入指定格式文件、指定签名的应用软件和其他非指定格式文件和非指定签名的应用软件，将移动存储介质分别连接到车辆 USB 接口、SD 卡接口，尝试执行非指定格式文件和非指定签名的应用软件，判定车辆是否满足 7.1.4.2 的要求。

8.3.2.4.3 USB 防病毒安全测试

测试人员应在具备 USB 接口的移动存储介质中注入病毒文件，将移动存储介质连接到车辆 USB 接口，尝试执行病毒文件，判定车辆是否满足 7.1.4.3 的要求。

8.3.2.4.4 诊断接口身份鉴别安全测试

测试人员应按照以下两种测试方法中适用的测试方法开展测试，判定车辆是否满足 7.1.4.4 的要求：

a） 使用非授权用户或工具在诊断接口发送车辆关键配置及标定参数的写操作指令，测试车辆是否执行该操作指令；

b） 使用工具在诊断接口发送车辆关键配置及标定参数的写操作指令，测试车辆是否存在访问控

制机制。

8.3.3 通信安全测试

8.3.3.1 云平台通信身份真实性验证安全测试

测试人员应依据车辆制造商提供的云平台清单及采用的通信协议类型，并按照如下三种测试方法中适用的测试方法开展测试，判定车辆是否满足 7.2.1 的要求。

a) 若车辆与车辆制造商云平台采用专用网络或虚拟专用网络环境进行通信，测试人员应根据企业提供的车辆云平台通信身份真实性的证明文件，确认车辆是否满足 7.2.1 的要求。

b) 若车辆与车辆制造商云平台采用公共网络环境进行通信，且使用公有通信协议，测试人员应使用网络数据抓包工具进行数据抓包，解析通信报文数据，检查车辆是否对车辆制造商云平台进行身份真实性验证。若采用网络数据抓包工具无法进行数据抓包，测试人员应根据企业提供的车辆云平台通信身份真实性的证明文件，确认车辆是否满足 7.2.1 的要求。

c) 若车辆与车辆制造商云平台采用公共网络环境进行通信，且使用私有通信协议，测试人员应根据企业提供的车辆云平台通信身份真实性的证明文件，确认车辆是否满足 7.2.1 的要求。

8.3.3.2 V2X 通信身份认证安全测试

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足 7.2.2 的要求：

a) 依照 8.3.1.2 的要求处置车辆，由测试设备向测试车辆下发合法证书并与测试车辆进行正常通信，测试车辆是否能够接收测试设备的直连通信消息；

b) 分别构造失效证书和身份伪造证书，并向车辆发送通信消息，测试车辆是否能够识别失效证书和身份伪造证书。

8.3.3.3 通信通道完整性安全测试

测试人员应依据车辆制造商提供的车辆移动蜂窝通信、WLAN、蓝牙等外部通信通道清单，依次触发车辆外部无线通信数据传输，并使用测试设备对车辆外部无线通信通道数据进行抓包，检查通道是否采用完整性保护机制，判定车辆是否满足 7.2.3 的要求。若使用测试设备无法对车辆移动蜂窝通信的数据进行抓包，测试人员应根据企业提供的车辆移动蜂窝通信通道完整性保护证明文件，判定车辆是否满足 7.2.3 的要求。

8.3.3.4 防非授权操作安全测试

测试人员应使用非授权身份通过车辆外部通信通道对车辆的数据依次进行超出访问控制机制的操作、清除和写入，检查是否可操作、清除和写入数据，判定车辆是否满足 7.2.4 的要求。

8.3.3.5 关键指令数据有效性或唯一性验证安全测试

测试人员应依据车辆制造商提供的关键指令数据列表，使用测试设备录制关键指令数据，重新发送录制的指令数据，检查车辆是否做出响应，判定车辆是否满足 7.2.5 的要求。

8.3.3.6 敏感个人信息保密性安全测试

测试人员应依据车辆制造商提供的车辆向外传输敏感个人信息的功能清单，触发车辆向外传输敏感个人信息的功能，使用车辆制造商提供的端口和访问权限抓取传输的数据包，检查是否对车辆传输的敏感个人信息进行加密，判定车辆是否满足 7.2.6 的要求。

8.3.3.7 防御物理操纵攻击安全测试

测试人员应依据车辆制造商提供的测试车辆与外部直接无线通信的零部件清单，使用和测试车辆与外部直接无线通信零部件型号相同但未授权的零部件替换安装在测试车辆相同的位置，启动车辆，检查零部件是否功能异常或车辆是否有异常部件连接告警，判定车辆是否满足 7.2.7 的要求。

8.3.3.8 车辆与外部直接通信零部件防非授权特权访问安全测试

测试人员应依据车辆制造商提供的对外直接无线通信零部件系统权限设计方案，并按照以下两种测试方法中适用的测试方法开展测试，判定车辆是否满足 7.2.8 的要求：

a) 若系统只存在特权访问的用户，测试是否能非授权登录进入系统；

b) 若系统存在或可配置多种权限用户，依据非特权用户登录系统方式进入系统，使用系统提权方法对非特权用户进行提权，测试进行提权操作后的用户是否能进行特权访问。

8.3.3.9 车内安全区域隔离安全测试

测试人员应依据车辆制造商提供的通信矩阵和访问控制列表样例，并按照以下两种测试方法中适用的测试方法开展测试，判定车辆是否满足 7.2.9 的要求：

a) 若使用物理隔离措施，验证车辆制造商提供的物理隔离方案是否有效；

b) 若使用逻辑隔离措施，依据车辆制造商提供的逻辑隔离策略，发送不符合策略的数据帧，在指定的目的端口，测试是否可接收到不符合策略的数据帧。

8.3.3.10 拒绝服务攻击识别防护安全测试

测试人员应依照 8.3.1.2 的要求处置车辆，使车辆分别处于静止和运动状态，使用拒绝服务攻击测试设备依次攻击车辆移动蜂窝通信、V2X、CAN 总线、车载以太网等通信通道，判定车辆是否满足 7.2.10的要求。

8.3.3.11 恶意数据识别安全测试

测试人员应依照 8.3.1.2 的要求处置车辆，向车辆发送当前车况非预期的恶意数据，判定车辆是否满足 7.2.11 的要求。

8.3.3.12 通信信息安全日志安全测试

测试人员应依据车辆制造商提供的车辆关键通信信息安全事件日志记录机制及其存储路径，并按照以下测试方法依次开展测试，判定是否满足 7.2.12 的要求：

a) 构建并触发车辆关键通信信息安全事件，检查是否按照关键通信信息安全事件日志记录机制记录该事件；

b) 检查日志记录的时间跨度是否不少于 6 个月或是否具备留存日志不少于 6 个月的能力。

8.3.4 软件升级安全测试

8.3.4.1 通用安全要求测试

8.3.4.1.1 安全保护机制测试

测试人员应依据车辆制造商提供的车载软件升级系统的可信根、引导加载程序、系统固件的安全保护机制的安全证明文件，判定车辆是否满足 7.3.1.1 的要求。

8.3.4.1.2 漏洞安全测试

测试人员应使用漏洞扫描工具对车载软件升级系统进行漏洞扫描，并将测试结果与汽车行业权威漏洞平台6个月前公布的高危及以上的安全漏洞清单和车辆制造商提供的车载软件升级系统漏洞处置方案进行比对，判定车辆是否满足7.3.1.2的要求。

8.3.4.2 在线升级安全测试

8.3.4.2.1 服务器身份认证安全测试

测试人员应依据车辆制造商提供的在线升级服务器清单及采用的通信协议类型，并按照以下三种测试方法中适用的测试方法开展测试，判定车辆是否满足7.3.2.1的要求。

a) 若车辆与在线升级服务器采用专用网络或虚拟专用网络环境进行通信，测试人员应根据企业提供的在线升级服务器身份认证安全功能的证明文件，确认车辆是否满足7.3.2.1的要求。

b) 若车辆与在线升级服务器采用公共网络环境进行通信，且使用公有通信协议，测试人员应使用测试设备进行数据抓包，解析通信报文数据，检查车辆是否对在线升级服务器进行身份真实性验证；中断下载并恢复，使用测试设备进行数据抓包，解析通信报文数据，检查是否重新进行身份真实性验证。若使用测试设备无法进行数据抓包，测试人员应根据企业提供的在线升级服务器身份认证安全功能的证明文件，确认车辆是否满足7.3.2.1的要求。

c) 若车辆与在线升级服务器采用公共网络环境进行通信，且使用私有通信协议，测试人员应根据企业提供的在线升级服务器身份认证安全功能的证明文件，确认车辆是否满足7.3.2.1的要求。

8.3.4.2.2 在线升级包真实性和完整性验证安全测试

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足7.3.2.2的要求。

a) 使用车辆制造商提供的正常升级包触发在线升级，测试升级功能是否正常。

b) 确认在线升级功能正常后，构造真实性和完整性被破坏的升级包，并依据车辆制造商提供的方法和权限，将真实性和完整性被破坏的升级包下载或传输到车端，执行软件升级，测试是否升级成功。若车辆的信息安全防护机制不支持将真实性和完整性被破坏的升级包下载或传输到车端，则依据车辆制造商提供的在线升级信息安全防护机制证明文件，检查车辆是否满足7.3.2.2的要求。

8.3.4.2.3 在线升级信息安全事件日志安全测试

测试人员应按照以下测试方法依次开展测试，判定是否满足7.3.2.3的要求：

a) 构造升级安全事件，检查是否存在在线升级信息安全事件日志；

b) 检查日志记录的时间跨度是否不少于6个月或是否具备留存日志不少于6个月的能力。

8.3.4.3 离线升级安全测试

8.3.4.3.1 使用车载软件升级系统的离线升级安全测试

测试人员应分别构造被伪造、被篡改的升级包，使用离线升级工具将该升级包下载或传输到车载端，执行离线升级，判定车辆是否满足7.3.3.1的要求。

8.3.4.3.2 不使用车载软件升级系统的离线升级安全测试

测试人员应按照如下测试方法中适用的测试方法开展测试，判定车辆是否满足7.3.3.2的要求：

a) 将非认证的刷写接入端接入车辆刷写接口并执行离线升级，测试车辆是否能识别非认证的刷写接入端；
b) 分别构造被伪造、被篡改的升级包，使用刷写接入端接入车辆刷写接口，执行离线升级，测试是否执行升级或升级是否成功。

8.3.5 数据安全测试

8.3.5.1 密钥防非法获取和访问安全测试

测试人员应依据车辆密码使用方案，确认测试零部件，并按照以下三种测试方法中适用的测试方法开展测试，判定车辆是否满足 7.4.1 的要求：

a) 若采取安全访问技术存储密钥，通过零部件访问接口进行破解、提取等攻击操作，测试是否可对密钥非授权访问和获取；
b) 若采取 HSM 等硬件安全模块存储密钥，应依据硬件安全模块安装位置说明文档，检查车辆是否在文档标识位置安装了硬件安全模块来保护密钥；
c) 若采取安全的软件存储形式存储密钥，应依据车辆制造商提供的保证车辆密钥安全存储证明文件，检查是否安全存储密钥。

8.3.5.2 敏感个人信息防泄露安全测试

测试人员应依据敏感个人信息功能清单和存储地址清单，确认测试零部件，依次触发车辆记录敏感个人信息的功能，并按照以下测试方法依次开展测试，判定车辆是否满足 7.4.2 的要求：

a) 若采用安全访问技术保护存储的敏感个人信息，依据敏感个人信息存储区域和地址范围说明，通过零部件调试接口，使用未添加访问控制权限的用户访问存储的敏感个人信息，测试是否能非授权访问敏感个人信息；
b) 若采取加密技术保护存储的敏感个人信息，依据敏感个人信息存储区域和地址范围说明，通过零部件调试接口，使用软件分析工具提取存储的敏感个人信息，测试是否为密文存储；
c) 依次触发车辆记录敏感个人信息的功能，然后依据系统登录方式进入系统，对测试零部件进行敏感个人信息检索，测试是否可检索出不在敏感个人信息功能清单和存储地址清单中存储的敏感个人信息。

8.3.5.3 车辆身份识别数据防非授权删除和修改安全测试

测试人员应依据车辆内存储的 VIN 等用于车辆身份识别的数据清单及存储地址，确定测试零部件，使用软件分析工具非授权删除和修改存储在车辆内的 VIN 等用于车辆身份识别的数据，判定车辆是否满足 7.4.3 的要求。

8.3.5.4 关键数据防非授权删除和修改安全测试

测试人员应依据车辆内存储的关键数据清单及存储的地址，确定测试零部件，通过零部件调试接口，使用软件分析工具修改存储在车内的关键数据，判定车辆是否满足 7.4.4 的要求。

8.3.5.5 日志文件防修改和非授权删除安全测试

测试人员应依据车辆内存储的安全日志清单及存储的地址，确定测试零部件，并按照以下测试方法依次开展测试，判定车辆是否满足 7.4.5 的要求：

a) 依据车辆内存储的安全日志清单及存储的地址，通过零部件调试接口，修改安全日志文件，测试是否可修改安全日志文件；

b) 依据车辆内存储的安全日志清单及存储的地址，通过零部件调试接口，使用软件分析工具测试是否可非授权删除安全日志文件。

8.3.5.6 个人信息清除功能测试方法

测试人员应使用测试车辆个人信息清除功能，确认测试零部件，依次触发车辆记录个人信息的功能，清除车辆内存储的个人信息，依据车辆制造商提供的车辆内存储的个人信息清单及存储的地址，通过零部件调试接口检索，检查个人信息是否被完全删除，判定车辆是否满足 7.4.6 的要求。

8.3.5.7 防数据直接出境测试方法

测试人员应开启车辆全部移动蜂窝通信通道和 WLAN 通信通道，依次模拟测试车辆处于未上电、仅上电、各项预装的数据传输功能正常启用的状态，并使用网络数据抓包工具对对外通信网络通道同时抓包，且总抓包时长不少于 3 600 s，解析通信报文数据，检查目的 IP 地址中是否包含境外 IP 地址，判定车辆是否满足 7.4.7 的要求。

9 同一型式判定

9.1 信息安全直接视同判定条件

如符合下述规定，则视为同一型式：

——汽车信息安全管理体系有效；

——车辆整车电子电气架构相同且信息安全处置措施相同；

——车辆中央网关的硬件型号和软件版本号（不影响信息安全的除外）相同；

——车辆车载软件升级系统硬件型号和软件版本号（不影响信息安全的除外）相同；

——车辆具备蜂窝移动通信系统功能的零部件硬件型号和软件版本号（不影响信息安全的除外）相同；

——车辆无线通信方式所使用的协议类型、协议版本、接口类型、接口数量相同或减少；

注：无线通信方式包含 WLAN、蓝牙、NFC、蜂窝通信、V2X 等。

——车辆外部接口的类型、数量相同或减少；

——与车辆直接连接并产生数据交互的车辆生产企业云平台 IP 地址或域名相同。

9.2 信息安全测试验证后视同判定条件

如车型发生涉及 9.1 的变更，在符合下述规定时，仅需对变更参数相关的技术要求进行补充测试，经审批许可后获得扩展：

——汽车信息安全管理体系有效；

——车辆整车电子电气架构相同且信息安全处置措施相同；

——车辆无线通信方式所使用的协议类型和接口类型相同或减少；

——车辆外部接口的类型相同或减少。

9.3 数据处理功能直接视同条件

如符合下述规定，则视为同一型式：

——车辆匿名化算法生产企业和版本相同；

——车辆实现匿名化算法的控制器硬件型号、软件版本号（不影响匿名化处理策略除外）和生产企业相同；

——车辆用于实现匿名化功能相关的摄像头等采集设备硬件型号、主要参数配置（采样分辨率、采

样视场角、采样帧率)和生产企业相同；

——车辆匿名化功能触发规则相同。

10 标准的实施

对于新申请型式批准的车型，自本文件实施之日起开始执行。

对于已获得型式批准的车型，自本文件实施之日起第25个月开始执行。

参 考 文 献

[1] UN R155 关于批准车辆信息安全和信息安全管理体系的统一规定