强制性国家标准

GB 44495—2024《汽车整车信息安全技术要求》第1号修改单

（征求意见稿）

编制说明

标准起草项目组

二〇二五年八月

目 次

GB 44495—2024《汽车整车信息安全技术要求》第 1 号修改单（征求意见稿）编制说明

一、工作简况

（一）任务来源

根据国家标准化管理委员会《关于下达<包装机械安全要求>等 31 项强制性国家标准制修订计划及相关标准外文版计划的通知》（国标委发〔2021〕27 号）中项目编号 20214422-Q-339 的强制性国家标准制定项目，制定强制性国家标准《汽车整车信息安全技术要求》。

（二）主要工作过程

受工业和信息化部委托，全国汽标委智能网联汽车分标委根据单位申请情况成立标准起草项目组，确定中国汽车技术研究中心有限公司、国汽（北京）智能网联汽车研究院有限公司和电子科技大学为标准起草项目组牵头单位，并在此基础上明确了任务和分工，积极开展标准的预研、起草及征求意见等工作。

自标准制定工作启动以来，牵头单位多次组织项目组成员单位召开项目组会议，分析了联合国等国际标准法规组织的汽车标准法规现状，讨论确定了适应中国汽车产业发展现状的汽车整车信息安全的技术要求并编写了标准草案，最终完成了标准的征求意见稿。

2019 年 11 月启动标准编制工作，成立项目组，召开第 1 次会议。

2019 年 12 月就标准边界及制定思路等内容征集各单位意见。

2020 年 3 月项目组第 2 次会议（线上），围绕制定思路及框架展开讨论。

2020 年 4 月～5 月确定框架、征求参编意向并分工编写。

2020 年 6 月～9 月形成标准草案并提交立项申请。

2020 年 10 月项目组第 3 次会议，持续完善标准草案。

2021 年 3 月～4 月根据行业管理需求和主管部门要求，将原推荐性国家标准项目调整为强制性国家标准项目。

2021 年 4 月项目组第 4 次会议，完成本标准与 UNWP.29R155 法规的对比分析。

2021 年 5 月～7 月组织多次封闭写稿和专题研讨会议，持续完善标准草案。

2021 年 7 月项目组第 5 次会议，充分参照 R155 法规及解释文件形成标准草案。

2021 年 8 月～9 月组织多次封闭写稿和专题研讨会议，持续完善标准草案。

2021 年 10 月项目组第 6 次会议，对草案进行详细讨论，确定技术要求框架，形成试验方法。

2022 年 1 月～6 月组织行业开展标准验证试验工作，包括企业信息安全管理审核、车辆技术要求及试验方法验证。

2022 年 7 月～8 月在汽车信息安全标准工作组进行征集意见，收集反馈意见并召开意见协调会，形成意见处理结论。

2022年9月根据意见反馈修改形成公开征求意见稿和编制说明。

2023年5月~7月在工信部、国标委和汽标委网站进行公开征求意见，并向一汽、东风、百度、上检等国内主要整车厂、供应商、试验机构、科研机构等69家委员单位定向征求意见，共收集到来自133家单位的反馈意见，共计987条。秘书处组织项目组成员单位及主要意见提出单位召开意见处理会议，其中170条采纳，418条部分采纳，399条不采纳，并根据反馈意见优化完善标准草案。

2023年8月汽标委秘书处组织召开强标预审会议，收到来自一汽、中国汽研、襄阳达安、德赛西威、小鹏汽车等单位的意见，根据反馈意见修改形成送审稿和编制说明。

2023年9月汽标委智能网联汽车分标委组织对该标准进行技术审查，经全体参会委员及委员代表共同审议，一致同意该标准通过审查，并形成审查意见。会后标准起草组按照审查意见修改完善草案，形成标准报批稿。

2024年7月5日-12日，工信部装备一司根据标准涉及的主管部门，征求了国家市场监管总局认证监督管理司意见，截至2024年7月12日，暂未收到反馈意见。

1.项目组第一次会议

汽车整车信息安全技术要求标准项目组第一次会议于2019年11月5日在杭州召开，正式启动标准制定工作。会议就标准的制定背景、范围、目标、框架、进度计划、研制思路等进行了讨论，对一些共性问题进行了探讨，会议明确标准撰写的整体思路按照整车开发流程V字型的架构来设计，需要和《汽车信息安全通用技术要求》的安全原则及需求相结合，综合考虑标准的对象，并在会后对标准框架开展进一步总结与梳理。

2.项目组第二次会议

汽车整车信息安全技术要求标准项目组第二次工作会议于2020年3月4日在线上召开，会议进一步围绕标准背景及项目计划、编写思路、框架等展开讨论。会议明确了标准定位是从整车视角出发综合考量，不包括对零部件单独的安全要求，技术要求和测试对象以整车为主；标准不区分不同的驾驶自动化级别，而是适用于道路车辆的通用基本要求。会议就标准下一步编制工作的分工进行了安排，由威胁分析与风险评估、外部访问点安全、内部网络通信安全、基于业务的安全、基于功能的安全、数据安全要求等7个部分分工编写，形成V1.0版草案。

3.项目组第三次会议

汽车整车信息安全技术要求标准项目组第三次工作会议于2020年10月21日在北京召开。会议讨论了标准的总体框架、编制思路，并由整车威胁分析与风险评估、外部访问点安全、内部网络通信安全、基于业务的安全、基于功能的安全、数据安全要求等7个部分对各章的编写思路和遇到的问题进行了交流与讨论，基于讨论进一步协调统一了标准框架、编写方式及要求力度等，并在会后面向项目组内广泛征集各章节的编写意见。

4.项目组第四次会议

汽车整车信息安全技术要求标准项目组第四次工作会议于2021年4月26日在天津召开。会议对本标准转为强标的背景进行了介绍，增进项目组全体成员对现有标准内容的理解；明确了整体的时间进度计划、各节点任务，明确各章节任务分工、工作思路和计划。会议明确本标准作为国家强制标准，不一定代表技术先进性，而侧重考量技术的广泛性和通用性，每条技术要求的提出都应力求必要、精简凝练，并且要着重考虑与UNR155法规的国际协调；围绕法规原文对标准框架设置和章节内容进行了对应的优化与调整。

5.作为强制性国家标准重新立项

2021年7月，为贯彻落实《网络安全法》《数据安全法》等，应对智能网联汽车信息安全风险与挑战，主管部门出于产业安全发展及行业管理需要，将该推荐性国家标准项目调整为强制性国家标准项目，为保障产业健康可持续发展划定信息安全基线要求。

6.项目组第五次会议

汽车整车信息安全技术要求标准项目组第五次工作会议于2021年7月26-29日在厦门召开。本次会议扩大了项目组成员的参与范围，主要针对车辆技术要求部分进行封闭写稿及讨论，并就各章节内容的编写情况逐一进行介绍和全体讨论，基本确定了标准的框架及主体内容，形成第二版草案，并参考GB 40050等信息安全行业重点标准的行文表述方式，统一梳理标准内容及行文。

7.项目组第六次会议

汽车整车信息安全技术要求标准项目组第六次工作会议于2021年10月12-13日在成都召开。本次会议在项目组内对标准的技术要求条款进行逐条地讨论、完善及确认，并初步讨论了管理章节的内容及试验开展的思路，为试验方法编写提供参考。会议形成的标准草案第三版，主要包括管理要求、车型技术要求、试验方法三部分内容，同时，明确了本标准不提出唯一限定的技术要求和试验方法，希望企业在充分的风险评估的基础上开展。后续将重点解决各章节存在内容交叉、重复的问题，进一步优化完善技术要求，增加相应的试验方法，部署标准验证试验工作。

8.标准验证试验

2022年1月-6月，汽标委智能网联汽车分标委秘书处根据标准编制工作计划开展本标准验证试验，验证试验项目包括：汽车信息安全管理体系审核，在申请企业所在地及线上同步开展；车辆技术要求及试验方法验证，在相关试验机构开展。秘书处面向汽车信息安全标准工作组广泛征集参与企业及试验车辆，由于本标准试验验证条款数量较多、准备工作复杂、体系验证需大量相关方配合、整体试验周期较长、试验验证资源有限，按照整车产品安全开发程度及企业信息安全管理体系建设完备程度，从征集到的24家汽车生产企业中最终选取了12家企业随机分配至6家检测机构共同开展验证试验。以线上线下相结合的方式先后完成所有车辆的标准验证试验及信息安全管理体系审核工作，总结试验过程中的经验和问题，进一步完善标准草案。

9.试验工作专题启动会

汽车整车信息安全技术要求的试验工作专题启动会于2022年3月1日以线上会议召开。本次会议由秘书处及6家试验机构共同参与，本次会议部署了开展验证试验的工作要求，并重点研讨确定标准验证试验实施方案及具体工作计划。明确了以验证标准草案中各条要求的合理性和可实施性为出发点，核查标准要求是否为基线要求。

10.工作组意见协调会

2022年7月31日，形成工作组征求意见稿，并面向汽标委智能网联汽车分标委汽车信息安全标准工作组100余家单位征求意见。本次反馈意见共计收到78家单位的意见反馈，标准项目组于8月30日至9月6日召开意见处理协调会议，根据反馈意见进行了逐条讨论处理，并根据相关意见对标准公开征求意见稿和编制说明进行了修改。

11.公开征求意见协调会

2023年5月，形成公开征求意见稿，并启动面向社会公开征求意见。2023年5月-7月，正式在工信部、国标委和汽标委网站进行公开征求意见和WTO通报，并向一汽、东风、百度、上检等国内主要整车厂、供应商、试验机构、科研机构等69家委员单位定向征求意见，共收集到来自133家单位的反馈意见，共计987条。2023年7月25~27日，秘书处组织项目组成员单位及主要意见提出单位召开意见处理会议，其中170条采纳，399条不采纳，418条部分采纳，并根据反馈意见优化完善标准草案。

12.强标预审会

2023年8月汽标委秘书处组织召开强标预审会议，收到来自一汽、中国汽研、襄阳达安、德赛西威、小鹏汽车等单位的意见，根据反馈意见修改形成送审稿和编制说明。

13.标准审查会

2023年9月，全国汽车标准化委员会智能网联汽车分技术委员会秘书处召开强制性国家标准《汽车整车信息安全技术要求》审查会议。经过讨论和现场表决，全体到会委员及委员代表一致同意该标准通过审查，并根据反馈意见优化形成标准报批稿。

14.标准第1号修改单

2025年4月，根据工作要求，项目组起草单位研究提出了GB 44495—2024第1号修改单（征求意见稿），主要修改了3个方面：

一、全文将“信息安全管理体系”“信息安全管理体系要求”均修改为“信息安全保障要求”。具体涉及的条款如下：

1、将“1 范围”修改为：本文件规定了汽车信息安全保障要求、信息安全基本要求、信息安全技术要求及同一型式判定，描述了相应的检验与试验方法。本文件适用于M类、N类车辆。

2、将“术语和定义 3.2”删除。

3、将第5章标题修改为：5 汽车信息安全保障要求。

4、将5.1的第一句修改为：车辆制造商应满足车辆全生命周期的汽车信息安全保障要求。

5、将 5.2 的第一句修改为：汽车信息安全保障要求应包括以下内容。

6、将 6.1 修改为：车辆产品开发流程应遵循汽车信息安全保障要求。

7、将 8.1 的第一句修改为：检验及试验方法包括汽车信息安全保障要求检验、基本要求检验和技术要求测试。

二、全文将“检查”修改为“检验”。具体涉及的条款如下：

1、将第 8 章标题修改为：8 检验与试验方法。

2、将 8.1 的内容修改为：检验及试验方法包括汽车信息安全保障要求检验、基本要求检验和技术要求测试：

——针对车辆制造商信息安全保障要求相关的文档进行检验，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验，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。

3、将 8.2 章节修改为：8.2 信息安全基本要求检验

8.2.1 检验要求

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，完成检验后应对留存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的文档与车辆的一致性、可追溯性做出自我声明。

8.2.2 检验方法

8.2.2.1 检验车辆制造商提交的文档，确认检验方案，包括检验范围、检验方式、检验日程、现场检验必要的证明文件清单。

8.2.2.2 应依据 8.2.2.1 确认的检验方案，在车辆制造商现场检验留存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。

4、将 8.3.2.2.1 b）修改为：伪造、篡改并发送远程车辆控制指令，检验是否可伪造、篡改该指令，车辆是否执行该指令。

5、将 8.3.2.2.3 a）修改为：触发车辆远程控制功能，检验是否存在安全日志，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。

6、将 8.3.2.2.3 b）修改为：检验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。

7、将 8.3.3.1 b）修改为：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，检验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。

8、将 8.3.3.3 修改为：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，检验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。

9、将 8.3.3.4 修改为：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，检验是否可操作、清除和写入数据，判定车辆是否满足 7.2.4 的要求。

10、将 8.3.3.5 修改为：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，检验车辆是否做出响应，判定车辆是否满足 7.2.5 的要求。

11、将 8.3.3.6 修改为：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，检验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。

12、将 8.3.3.7 修改为：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，检验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。

13、将 8.3.3.12 a）修改为：构建并触发车辆关键通信信息安全事件，检验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；

14、将 8.3.3.12 b）修改为：检验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。

15、将 8.3.4.2.1 b）修改为：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，检验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，检验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。

16、将 8.3.4.2.2 b）修改为：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，检验车辆是否满足 7.3.2.2 的要求。

17、将 8.3.4.2.3 a）修改为：构造升级安全事件，检验是否存在在线升级信息安全事件日志；

18、将 8.3.4.2.3 b）修改为：检验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。

19、将 8.3.5.1 b）修改为：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，检验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；

20、将 8.3.5.1 c）修改为：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，检验是否安全存储密钥。

21、将 8.3.5.6 修改为：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，检验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。

22、将 8.3.5.7 修改为：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 3600s，解析通信报文数据，检验目的 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。

三、将第 9 章 同一型式判定 9.1 和 9.2 中的第一条列项“汽车信息安全管理体系有效”均修改为：汽车整车信息安全技术要求检验检测报告中的汽车信息安全保障要求相关内容有效且其签发日期未超过三年。。

修改后形成征求意见稿并提交全国汽车标准化技术委员会公示征求意见。

二、编制原则、强制性国家标准主要技术要求的依据及理由

本文件编写符合 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。起草过程，充分考虑国内外现有相关标准的统一和协调；标准的要求充分考虑了国内当前的行业技术水平，对草案内容进行多次征求意见和充分讨论。

（一）适用范围

本文件规定了汽车信息安全保障要求、信息安全基本要求、信息安全技术要求及同一型式判定，描述了相应的检验与试验方法。

本文件适用于M类、N类车辆。

（二）主要技术内容

以下选择标准技术要求的部分重点内容进行说明：

第5章 汽车信息安全保障要求

基于国内行业技术发展现状，参考R155法规第7.2章节的内容，针对如下方面提出要求：

（1）车辆制造商应满足车辆全生命周期的汽车信息安全保障要求。

说明：本标准条款所要求的汽车信息安全保障要求以车辆产品为核心，应覆盖车辆的全生命周期。若流程、规定等仅与企业经营管理、组织自身运营相关，并不涉及车辆产品信息安全相关话题，则不在本标准所要求的范围内。

（2）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。

说明：本条款要求汽车生产企业针对车辆的信息安全风险进行识别、评估、分类、处置等相关管控活动，并建立相应的流程。此处的流程应能够应对车辆全生命周期的风险管控，企业可自行定义实施路线。

（3）应包含漏洞管理机制，明确漏洞收集、分析、报告、处置、发布、上报等活动环节。

说明：本条款明确要求企业建立漏洞管理机制，并且需涵盖收集、分析、报告、处置、发布等关键环节。

第6章 车辆信息安全一般要求

基于国内行业技术发展现状，参考R155法规中第7.3章节的内容，及附录5中的部分相关内容（表A14.3.4、4.3.7有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表B3、B5中有关的缓解措施），针对如下方面提出要求：

（1）车辆产品开发流程应遵循汽车信息安全保障要求。

说明：车辆产品应按照汽车信息安全保障要求中定义的相关流程、制度开展开发工作。

（2）车辆制造商应识别和管理车辆与供应商相关的风险。

说明：此处“供应商”关注与车辆产品风险相关的供应商，包括合同供应商、服务提供商等。

（3）车辆制造商应针对车辆实施相应措施，以识别针对该车辆的网络攻击，并为车辆制造商在识别与车辆相关的网络攻击、网络威胁和漏洞方面提供监测能力，以及为分析网络攻击、网络威胁和漏洞提供数据取证能力。

说明：车辆产品端应实施相应的措施，与企业在汽车信息安全保障要求中建立的网络攻击、网络威胁和漏洞的监测和响应流程进行协同，从而保障企业可以针对车辆产品进行网络攻击、网络威胁和漏洞方面的监测，并且支持数据取证。

第 7 章 车辆信息安全技术要求

7.1 外部连接安全要求

基于国内行业技术发展现状，参考 R155 法规附录 5 中的相关内容（表 A14.3.1、4.3.5 有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表 B4 中有关的缓解措施），针对如下方面提出要求：

（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。

（2）车辆应关闭非业务必要的网络端口。

（3）应对远程控制指令信息进行真实性和完整性验证。

（4）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。

（5）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。

（6）应对车端具备远程控制功能的系统进行完整性验证。

（7）应对授权的第三方应用的真实性和完整性进行验证。

（8）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。

（9）应对车辆外部接口进行访问控制保护，禁止非授权访问。

（10）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，只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。

（11）车辆应具备抵御 USB 接口接入设备中的病毒程序和携带病毒的媒体文件和应用软件的能力，如识别且不执行病毒文件。

（12）通过诊断接口发送车辆关键配置及标定参数的写操作指令时，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

基于国内行业技术发展现状，参考 R155 法规附录 5 中的相关内容（表 A14.3.2 有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表 B1、B5 中有关的缓解措施），针对如下方面提出要求：

（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。

说明：本文件并未强制要求双向认证、也未强制要求必须使用证书保护机制。

（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。

说明：本条款主要是针对 V2X 场景提出的要求。

（3）车辆应采用完整性保护机制保护除射频、NFC 之外的外部无线通信通道。

说明：本条款主要针对能够在通信协议层面实现完整性保护机制的外部通信通道。某些外部通信通道例如 RFID、NFC 等，不适用此条款；无线传感器与车载设备之间的通信、语音交互也不适用于本条款；对于企业采用的完整性保护技术类型和强度，本文件不做具体要求。

（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。

说明：本文件旨在对车辆的信息安全风险提出安全要求，具体“敏感个人信息”的定义以汽车数据安全相关管理要求和标准规定为准。

（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。

说明：本条款仅包含与外部直接通信的零部件，利用 T-BOX，车载信息交互系统间接与外部通信的零部件不适用于本条款的要求；射频、NFC 等短距离无线通信的传感器也不适用于本条款要求；身份识别机制包括基于密码的认证机制、DTC 记录、日志记录、异常提醒等，对外部通信零部件进行身份识别的技术可通过云端来实现。

（6）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。

说明：恶意的诊断数据包括非法诊断请求、非法诊断应答、暴力请求认证、非法开启 DTC 主动上传、恶意连续复位等；本条款使用“数据”而不是消息或指令等表述方式，是为了全文统一考虑，其本身是广义的概念，可指代原文的“恶意消息”具；体恶意数据的定义由厂家决定并提供清单作为测试的输入。

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

说明：本条款对车辆通信信息安全事件日志记录提出了要求，安全日志防护应满足第 7.4 章数据代码章节的要求。

7.3 软件升级安全要求

基于国内行业技术发展现状，参考 R155 法规附录 5 以及 R156 法规中的相关内容（表 A14.3.3 有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表 B2 中有关的缓解措施），针对如下方面提出要求：

（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。

说明：车载软件升级系统在行业和某些企业也被称为车端 OTA Master，包括系统软件和硬件；该条款的正常启动是指车载软件升级系统默认加载程序的启动；本文件中将除默认加载程序的启动之外，均视为非正常启动。

（2）车载软件升级系统应不存在由权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。注：处置方式包括消除漏洞、制定减缓措施等方式。

说明：本条款的说明参见第 7.1 章的相关说明。

（3）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。

说明：该条款是对在线软件升级场景（OTA场景）提出的要求；在线升级包在解包和分发之前，需要由车载软件升级系统校验其真实性和完整性，以保证在线升级包的真实来源和未受修改，其他环节是否进行校验不在本文件中进行要求。

（4）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。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，且验证升级包的真实性和完整性。

说明：若车辆不使用车载软件升级系统进行离线升级，主要有以下两类升级方式：a）使用诊断仪等基于OBD端口的设备进行刷写升级；b）使用USB端口进行直刷（不经过车载软件升级系统）。如果采用a）方式，要求车端刷写准入端采用如27服务等防护措施对诊断仪等设备进行认证之后，才能进行刷写操作；如果采用b）方式，要求ECU在被刷写之前对离线升级包的真实性和完整性进行校验。

7.4 数据安全要求

基于国内行业技术发展现状，参考R155法规附录5中的部分相关内容（表A14.3.6有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表B5、B7、C3中有关的缓解措施），针对以下方面提出要求：

（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。

说明：常见的安全的存储方式包括存储在HSM、SE、TEE等安全模块，也包括安全的软件存储形式。

（2）车辆应采取安全防御机制保护存储在车内的车辆识别代号（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。

说明：此条要求中用于身份识别的数据由企业自行确定，包括直接用于身份识别的数据和组合起来间接识别身份的数据。

（3）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。

说明：关键数据由企业根据车型的业务场景和风险评估来确认。

（4）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的必须保留的个人信息。

说明：国家要求存储在车内不允许修改的数据除外，例如DSSAD、EDR内存储的数据，防恢复机制在本标准中不提出强度要求，未来以数据安全相关标准的要求为准。

（5）车辆不应直接向境外传输数据。

说明：此条款主要是避免车型设计时预留了数据出境的功能或接口，导致大批量的车辆避开管理部门的监管向境外直传数据。车辆通过国内云平台中转间接向境外传递数据，用户个人行为的跨境数据传输均不受本条款的要求。

（五）主要试验（或）验证情况分析

根据工作安排，中国汽车技术研究中心有限公司、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、上海机动车检测认证技术研究中心有限公司、中国汽车工程研究院股份有限公司、招商局检测车辆技术研究院有限公司、襄阳达安汽车检测中心有限公司等6家检测机构以及上海汽车集团股份有限公司、重庆长安汽车股份有限公司、广州汽车集团股份有限公司、吉利汽车研究院（宁波）有限公司、东风汽车集团有限公司、上海蔚来汽车有限公司、广州小鹏汽车科技有限公司、北京车和家汽车科技有限公司、梅赛德斯—奔驰集团股份公司、宝马（中国）服务有限公司、一汽—大众汽车有限公司、一汽解放汽车有限公司等进行了试验方法验证，以下选择有代表性的验证内容对验证主要情况进行说明。

1.汽车信息安全保障要求

在检验期间，汽车生产企业依据秘书处发出的《审核表》进行材料准备，采取文件展示、现场演示等方式，通过现场/远程方式进行，评估企业是否满足本标准草案中的要求。经总结发现，所有参与验证活动的整车生产企业均建立汽车信息安全保障要求，初步形成面向汽车产品的信息安全管理制度，能够覆盖本标准第5章的条款要求，但不同企业的落地执行方式不同、所执行颗粒度有所差异。为便于行业理解以及加强企业落地可操作性，特作如下说明：

（1）车辆制造商应满足车辆全生命周期的汽车信息安全保障要求。

说明：ISO 21434《道路车辆 信息安全工程》可作为证明和评估汽车信息安全保障要求所需阶段的依据。第9章“概念阶段”、第10章“产品开发”和第11章“信息安全验证”可用于评估汽车信息安全保障要求的开发阶段。第12章“生产”可用于评估汽车信息安全保障要求的生产阶段。第7章“持续的信息安全活动”、第13章“操作和维护”以及第14章“报废”可用于评估汽车信息安全保障要求的后生产阶段；

（2）应建立企业内部管理信息安全的流程。

说明：本条款中提及的企业内部管理信息安全的流程，指在组织层级与车辆信息安全强相关的流程，对于组织本身的信息安全流程，如：针对企业IT系统的信息安全管理流程等不在本标准考虑范围内。此外，本条款可参考ISO 21434《道路车辆 信息安全工程》中第五章“组织信息安全管理”中的要求，从治理文化、信息共享、安全审核、工具管理、持续改进等方面进行开展。

（3）应建立识别、评估、分类、处置车辆信息安全风险及核实已识别风险得到适当处置的流程，并确保车辆风险评估保持最新状态。

说明：本条款中提及的风险指车辆全生命周期中的信息安全风险，覆盖研发阶段、生产阶段、后生产阶段。企业根据实际需求与业务场景，定义车辆全生命周期中的信息安全风险管控流程。此外，ISO 21434《道路车辆 信息安全工程》中第十五章提及的威胁分析与风险评估方法论可供参考，企业可自行选择是否采用。

（4）应建立针对车辆的网络攻击、网络威胁和漏洞的监测和响应流程，要求如下：

a）应包含确保已识别的网络威胁和漏洞得到响应，且在合理的时限内得到处置的流程；

说明：本条款中提及的“合理时限”当前可由企业结合实际情况自行定义，“处置”包括采取缓解措施、修复、持续监测等方式。

此外发现：针对于合资企业和外资企业，其部分文档（尤其是车辆产品开发相关制度）保存在国外，且供应商来自于各个国家，存在无法提供资料或提供的资料难以审查（非中英版本）的情况，需在标准中进行明确约束。

2.信息安全基本要求

经总结发现，汽车生产企业针对部分新车型已开展信息安全活动，但由于车型项目尚处于概念阶段，无法依据所建立的汽车信息安全保障要求开展全部活动。且部分企业执行的信息安全活动与建立的流程规定并不一致。考虑到目前汽车生产企业的汽车信息安全保障要求亦正处于建设过程中，需预留充足时间供其新款车型研发验证。同时发现，对于风险评估活动而言，企业开展形式不一；对于供应商管理而言，汽车企业能够提出明确的信息安全技术要求，但针对于职责划分、工作内容等，企业开展形式不一等等。总体来说，参与的汽车生产企业对于本标准的第六章条款要求理解无明显偏差。

此外，由于合资企业属性，车辆产品由国内外团队共同完成，但国外团队并不会向国内团队提供完整的风险评估和相关处置文档，因此，存在车型产品开发完成后，但实际风险评估不充分的可能性，车型产品的安全性存在较大风险。

3.信息安全技术要求试验结果

测试开始前，需结合信息安全基本要求的检验结果确认适用于该车型的测试项，并获取必要的测试输入信息。

测试输入信息并不一定需要提供完整的文本材料，车辆生产企业针对不同的测试输入信息可以采用不同的方式提供测试输入，不同的测试输入信息提供方式如下：

（1）测试人员和车辆生产企业技术人员通过会议沟通确认：测试车辆远程控制功能，包括远程控制指令应用场景和使用权限；测试车辆授权第三方应用真实性和完整性验证方式；测试车辆非授权第三方应用的访问控制机制；测试车辆外部接口；与测试车辆通信的车辆生产企业云平台；测试车辆通信方法，包括采用的通信协议类型；测试车辆 V2X 功能；测试

车辆向外传输敏感个人信息的通信通道；测试车辆与外部直接通信零部件；测试车辆个人信息清除功能及防恢复机制。

（2）车辆生产企业技术人员先提供目录清单，然后测试人员在车辆生产企业现场确认测试必须的详细信息：远程控制指令审计方式及审计日志记录地址、车辆记录异常指令的地址；测试车内通信方案及通信矩阵样例，包括专用数据通信矩阵样例；测试车辆对称密钥和私钥的存储方式及说明文档；测试车辆内部存储敏感个人信息存储地址；测试车辆内存储的车辆识别代号和用于身份识别的数据清单及存储地址；测试车辆内存储的关键数据清单及存储的地址。

（3）车辆生产企业安排技术人员携带相应的工具在检测机构现场协助完成测试，测试结束后工具收回：测试车辆车载软件升级系统可信根、引导加载程序、系统固件的访问方式和地址；测试车辆实现离线软件升级的方式及工具。

按照2021年10月项目组第6次会议形成的文件开展了验证测试，不同车辆测试项目并不完全相同（全覆盖为80项测试项），下表中给出了标准验证的总体情况。

序号	标准条款	通过情况	不可行/未通过试验主要原因
1	外部连接安全要求对应15项测试项	通过数量：11 不通过数量：2 未试验数量：2	完成13项测试项的验证，剩余2项测试项被GB 34660-2017覆盖未开展验证试验；13项测试项中有11项测试方法得到认可，2项测试方法需进行调整。
2	通信安全要求对应40项测试项	通过数量：25 不通过数量：8 未试验数量：7	完成33项测试项的验证，剩余7项与V2X相关，由于本次送检车型均不具备V2X功能，未开展验证试验；33项中有25项测试方法得到了认可，8项测试方法需要进行调整。
3	软件升级安全要求对应13项测试项	通过数量：7 不通过数量：6 未试验数量：0	完成了全部测试项的验证；13项测试项中有7项方法得到了认可，6项测试方法需进行调整。
4	数据代码安全要求对应12项测试项	通过数量：11 不通过数量：1 未试验数量：0	完成了全部测试项的验证；12项测试项中有11项方法得到了认可，1项测试方法需进行调整。

测试验证情况总体总结及重点问题说明：

（1）车型流程检验是开展车型技术要求试验验证的基础，车型技术要求试验验证是对车型流程检验结果的补充确认。

（2）测试验证时发现测试项可能无法完全覆盖技术要求，若企业风险评估后的缓解措施多于技术要求，多出来的企业自定义安全措施需进行评估确认，不再进行测试。

（3）部分测试方法可能会影响企业平台运行。示例：标准原文7.2.2车辆与车辆、路侧单元、云平台等的通信，应实施身份认证。测试项8.3.3.1与云平台通信的身份认证试验方法：

a）若车辆与云平台通信采用公有通信协议，采用网络数据抓包工具进行数据抓包，解析通信报文数据，检查是否采用如 TLSV1.2 同等安全级别或以上要求的安全通信层协议；

b）若车辆与云平台通信采用私有通信协议，对私有通信协议方案进行审核，采用网络数据抓包的方法进行数据抓包，解析通信报文数据中加密密钥衍生、更新及存储策略，检查是否支持以安全方式进行定期更新，并以安全的方式存储加密密钥。

c）依据车辆端通信部件清单，使用车辆端设备和云平台的合法证书，检测双方是否能够完成身份认证以进行后续通信；

d）分别替换伪造的车辆端设备和云平台的证书，测试是否能够通过身份认证并进行后续通信。

说明：送检车辆连接的平台均为实际生产平台，进行证书替换，采用私有 APN 通讯的认证方式可能影响已售车辆运行。

（4）部分企业产品采取的防护技术可能会影响测试项执行，将通过审核的方式补充证明。示例：测试项 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，并按照以下测试方法依次开展测试，测试已存储敏感个人信息的车辆是否满足 7.4.2 的要求：

a）启动车辆，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；

b）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；

c）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。

说明：标准技术要求“7.2.2 车辆与车辆、路侧单元、云平台等的通信，应实施身份认证”，企业为满足此条款要求，采用了 TLS 1.2 以上安全通讯协议时，测试人员无法通过技术测试验证的方式核查此时传输的数据消息体本身是否依照声明的算法进行数据加密；

（5）通过本次标准验证试验，对部分测试方法进行优化调整：

a）若基于第 7 章安全技术要求的风险处置措施与企业所识别的风险不相关，无需对不相关的条款开展测试，仅需开展评估确认。

b）若基于第 7 章安全技术要求的风险处置措施无法覆盖企业所识别的风险，应在按照附录 A 开展测试验证的基础上，对企业实际所使用的处置措施开展评估确认。

c）若基于第 7 章安全技术要求的风险处置措施适用于企业所识别的风险，按照 8.3 试验方法开展验证，其中适用于现场测试的条款依照文件中列出的条款开展测试进行确认，不适用于现场测试的条款通过审核研发阶段的第三方测试报告进行确认。

三、与有关法律、行政法规和其他标准的关系

本标准是我国智能网联汽车管理的重要内容；与现行相关法律、法规、规章及相关标准没有冲突或矛盾。

四、与国际标准化组织、其他国家或者地区有关法律法规和标准的比对分析

本标准未采用国际标准，基于国内行业发展现状和管理需求自主制定。

2020 年 6 月，联合国世界车辆法规协调论坛（UN WP.29）发布 R155《关于信息安全和信息安全管理体系的汽车型式批准统一规定》，在信息安全管理体系的符合性证明、信息安全管理体系要求、车型要求、车型修改及扩展、生产一致性等方面做出规定，并在其附录中给出了主要的汽车信息安全风险及缓解措施。该法规已于 2021 年 1 月 1 日生效，欧盟、日本等计划从 2022 年 7 月起，所有新车型需要满足 R155 法规，以获取车辆型式批准 WVTA（Whole Vehicle Type Approval）证书后上市销售，计划 2024 年 7 月起制造的所有车辆均必须满足 R155 法规的要求。

本标准的制定借鉴联合国世界车辆法规协调论坛（UN WP.29）已发布《关于信息安全和信息安全管理体系的汽车型式批准统一规定》法规的思路，在满足政府管理需求和符合行业发展现状的基础上自主制定。

五、重大分歧意见的处理过程、处理意见及其依据

本标准修订过程中无重大分歧。

六、对强制性国家标准自发布日期至实施日期之间的过渡期的建议及理由

由于汽车信息安全保障要求及信息安全技术的应用涉及企业保障能力构建、车辆安全设计开发、检测机构试验开展等方面，建议预留一段时间的过渡期，为各相关方预留充分准备时间。

本标准建议实施日期：2026-01-01

实施过渡期：

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。

七、与实施强制性国家标准有关的政策措施

本标准的实施监督管理部门是工业和信息化部、国家市场监督管理总局。对于违反强制性国家标准的行为，应按照下列法律、行政法规、部门规章相关规定进行处理：

（一）《中华人民共和国标准化法（2017修订）》

第二十五条不符合强制性标准的产品、服务，不得生产、销售、进口或者提供。

第三十六条生产、销售、进口产品或者提供服务不符合强制性标准，或者企业生产的产品、提供的服务不符合其公开标准的技术要求的，依法承担民事责任。

（二）《中华人民共和国产品质量法（2018年修订）》

第十三条可能危及人体健康和人身、财产安全的工业产品，必须符合保障人体健康和人身、财产安全的国家标准、行业标准；未制定国家标准、行业标准的，必须符合保障人体健康和人身、财产安全的要求。

禁止生产、销售不符合保障人体健康和人身、财产安全的标准和要求的工业产品。具体管理办法由国务院规定。

（三）工业和信息化部《车辆生产企业及产品生产一致性监督管理办法》（工产业〔2010〕第109号）

第十条对于不能保证产品生产一致性的车辆生产企业，工业和信息化部将视情节轻重，依法分别采取通报、限期整改、暂停或撤销“免予安全技术检验”备案、暂停或撤销其相关产品《公告》等措施。实施监督管理部门以及对违反强制性国家标准的行为进行处理的有关法律、行政法规、部门规章依据等。

八、是否需要对外通报的建议及理由

本标准为强制性国家标准，在标准适用范围为本文件适用于M类、N类车辆，涉及进口车，需对外通报。

九、废止现行有关标准的建议

无。

十、涉及专利的有关说明

本标准不涉及专利。

十一、强制性国家标准所涉及的产品、过程或者服务目录

本标准涉及产品包括本文件适用于M类、N类车辆。

十二、其他应当予以说明的事项

无。