

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

（报批稿）

编制说明

二〇二五年十二月

## 目 次

一、 工作简况 .....	1
二、 编制原则、强制性国家标准主要技术要求的依据及理由 .....	2
三、 与有关法律、行政法规和其他标准的关系 .....	6
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 .....	6
五、 重大分歧意见的处理过程、处理意见及其依据 .....	6
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 .....	6
七、 与实施强制性国家标准有关的政策措施 .....	6
八、 是否需要对外通报的建议及理由 .....	7
九、 废止现行有关标准的建议 .....	7
十、 涉及专利的有关说明 .....	7
十一、 强制性国家标准所涉及的产品、过程或者服务目录 .....	7
十二、 公平竞争审查情况说明 .....	7
十三、 其他应当予以说明的事项 .....	8

# GB 44495—2024《汽车整车信息安全技术要求》

## 第1号修改单

### （报批稿）

### 编制说明

#### 一、工作简况

##### 1.1 任务来源

2025年4月，工业和信息化部委托全国汽车标准化技术委员会智能网联汽车分技术委员会组织制定《汽车整车信息安全技术要求》国家标准第1号修改单。

##### 1.2 制定背景

智能网联汽车面临产业链长、通信方式多、攻击面广、数据量大等复杂多样的安全挑战，其信息安全贯穿车辆的研发、生产和在用运维，覆盖车辆的全生命周期，也涉及云平台、整车、部件、芯片和操作系统等组件。随着汽车智能化、网联化的不断发展与应用，车辆的信息安全问题日益严峻，一旦遭受网络攻击则可能导致用户个人信息泄露及远程入侵控车等严重后果，影响车辆用户的隐私、财产、生命等多方面安全，甚至危害社会与国家安全。近年来，汽车信息安全已成为汽车安全体系的重要一环。传统安全强调一般安全，主动安全和被动安全；新型安全则是指智能网联汽车的四维综合安全体系，包括功能安全、预期功能安全、网络安全和数据安全，是智能网联汽车安全层面的显著特征。因此，基于汽车的复杂应用环境，以车端为核心，运用纵深防御理念，制定汽车信息安全强制性技术标准已成为我国发展智能网联汽车的必然要求。

##### 1.3 起草过程

2024年8月，《汽车整车信息安全技术要求》等三项智能网联汽车领域首批强制性国家标准由市场监管总局（国家标准委）批准发布。依据智能网联汽车标准化工作的整体部署，全国汽车标准化技术委员会智能网联汽车分技术委员会提交修改单立项，2025年9月形成征求意见稿。2025年9月至2025年11月在工信部、国标委和汽标委网站进行公开征求意见，并向东风汽车集团有限公司、上海汽车集团股份有限公司乘用车分公司、惠州市德赛西威汽车电子股份有限公司、深圳引望智能技术有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、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、比亚迪汽车工业有限公司、吉利汽车研究院（宁波）有限公司、重庆长安汽车股份有限公司、北京车和家汽车科技有限公司、上汽通用五菱汽车股份有限公司、长城汽车股份有限公司、中国第一汽车集团有限公司、广州汽车集团股份有限公司、泛亚汽车技术中心有限公

司、上汽大众汽车有限公司、北京汽车研究总院有限公司等整车厂、供应商、检验检测机构、科研机构等 69 家委员单位定向征求意见，修改单在征求意见期间同步征求了公安部、市场监管总局、国家消防救援局等相关部门意见。

公开征求意见期间共收到 9 家单位和 1 位个人的 30 条意见建议，公安部交通管理局、交通运输部科技司、国家消防救援局政策法规司回函，无意见。2025 年 11 月，组织项目组成员单位及主要意见单位协调意见，其中 9 条意见与本次修改单相关，其余 21 条意见与本次修改单无关，相关意见中采纳 2 条，部分采纳 3 条，不采纳 4 条，并根据反馈意见及研讨结论形成送审稿和编制说明。2025 年 12 月 10 日，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。

本标准主要起草单位包括：中国汽车技术研究中心有限公司、电子科技大学、国汽（北京）智能网联汽车研究院有限公司、工业和信息化部装备工业发展中心、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、上海机动车检测认证技术研究中心有限公司、泛亚汽车技术中心有限公司、北京车和家信息技术有限公司、中国汽车工程研究院股份有限公司、中国标准化研究院、襄阳达安汽车检测中心有限公司、东风汽车集团有限公司、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、重庆长安汽车股份有限公司、一汽解放汽车有限公司、招商局检测车辆技术研究院有限公司、一汽大众汽车有限公司、上海蔚来汽车有限公司、广州小鹏汽车科技有限公司、上海汽车集团股份有限公司技术中心、中国第一汽车集团有限公司、长城汽车股份有限公司、上汽大众汽车有限公司、梅赛德斯—奔驰（中国）投资有限公司、宝马（中国）服务有限公司、通用汽车（中国）投资有限公司、深圳引望智能技术有限公司、三六零数字安全科技集团有限公司、北京百度网讯科技有限公司、北京梆梆安全科技有限公司、国家计算机网络应急技术处理协调中心、中国信息通信研究院、国家工业信息安全发展研究中心、比亚迪汽车工业有限公司、安徽江淮汽车集团股份有限公司、北京汽车研究总院有限公司、东风商用车有限公司、中国重型汽车集团有限公司、上海工业控制安全创新科技有限公司、北汽福田汽车股份有限公司、东软集团股份有限公司、联合汽车电子有限公司、沃尔沃汽车（亚太）投资控股有限公司、大众汽车（中国）投资有限公司、博世汽车部件（苏州）有限公司、日产（中国）投资有限公司、丰田汽车（中国）投资有限公司、本田技研工业（中国）投资有限公司。

## 二、 编制原则、强制性国家标准主要技术要求的依据及理由

### 2.1 编制原则

（1）规范性原则：在标准的起草过程中，严格按 GB/T 1.1—2020 的要求规划标准内容。在条款表述上，准确按照 GB/T 1.1—2020 的规定表述。

（2）科学性原则：本标准在编写过程中，充分吸收和听取国内外车辆生产企业、检测

机构的意见和建议，通过权衡试验结果的准确性和试验时长的节约成本两方面因素，确定科学合理的缩短法测试规程。

## 2.2 主要内容

本次修改单主要内容如下：

（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，不适用于基于已获得型式批准的二类底盘或整车改装的专用汽车。

2、将“术语和定义 3.2”删除。

3、将第 5 章标题及目录修改为：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”均修改为“检验”。具体涉及的条款如下：

1、将第 8 章标题及目录修改为：检验与试验方法。

2、将 8.1 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 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 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。

（四）将第 10 章中的“对于新申请车辆型式批准的车型，自本文件实施之日起开始执行。”修改为：对于新申请型式批准的车型，自本文件实施之日起第 7 个月开始执行。

### 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

本标准修改单在起草过程中，无重大分歧意见。

### 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

结合行业现状和技术发展趋势，经行业研究讨论，建议本修改单发布即实施。

### 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为工业和信息化部、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“免于安全技术检验”备案、暂停或撤销其相关产品《公告》等措施。

## 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，标准适用范围为适用于 M 类、N 类车辆，不适用于基于已获得型式批准的二类底盘或整车改装的专用汽车。涉及对外贸易，依据《强制性国家标准管理办法》与世界贸易组织的要求，需要进行 WTO/TBT 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

本标准涉及的产品为 M 类、N 类车辆，不适用于基于已获得型式批准的二类底盘或整车改装的专用汽车。

## 十二、 公平竞争审查情况说明

本标准已完成公平竞争审查，并填写了《公平竞争审查表》。本标准起草过程中无限制或者变相限制市场准入和退出、商品要素自由流动等情况，未对经营者生产经营成本、生产经营行为造成不利影响，不存在违反《公平竞争审查条例》规定的情况，符合公平竞争审查

标准。

### 十三、 其他应当予以说明的事项

无。

《汽车整车信息安全技术要求》第 1 号修改单 标准项目组

2025 年 12 月 10 日