

GB 44495—2024《汽车整车信息安全技术要求》

国家标准第 1 号修改单

(报批稿)

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。
