

《汽车远程升级（OTA）信息安全测试规范》编制说明

一、工作简况

1.1 任务来源

《汽车远程升级（OTA）信息安全测试规范》团体标准是由中国汽车工程学会批准立项。文件号中汽学函【2022】145号，任务号为2022-66。本标准由中国智能网联汽车产业创新联盟提出，国汽（北京）智能网联汽车研究院有限公司、惠州市德赛西威汽车电子股份有限公司、陕西重型汽车有限公司、博世汽车部件（苏州）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）、北京百度网讯科技有限公司、北汽福田汽车股份有限公司、北京航迹科技有限公司、北京汽车研究总院有限公司、重庆长安汽车股份有限公司、浙江长三角车联网安全技术有限公司、北京赛目科技股份有限公司、招商局检测车辆技术研究院有限公司、苏州挚途科技有限公司、中汽研软件测评（天津）有限公司、江苏智能网联汽车创新中心有限公司、中国标准化研究院长三角分院、襄阳达安汽车检测中心有限公司、中国汽车工程研究院股份有限公司、北京经纬恒润科技股份有限公司、北京万集科技股份有限公司、国汽智端（成都）科技有限公司、国家金融科技测评中心、中国信息通信研究院、紫光国芯微电子股份有限公司、国家工业信息安全发展研究中心、一汽奔腾轿车有限公司、江铃汽车股份有限公司、南德认证检测（中国）有限公司上海分公司、宁波谦川科技有限公司等单位起草。

1.2 编制背景与目标

随着汽车行业快速向智能化、网联化、电动化的方向发展，车载电子器件在整车系统中逐渐增多，整车和ECU已经实现从物理方式到软件升级（OTA）的更新迭代。当前针对汽车的黑客攻击事件频发，OTA升级的信息安全成为了重点关注方向，也称为黑客重点攻击的对象。攻击者通过劫持、篡改、替换等攻击方法对OTA网络升级中涉及到的云端、车端、通讯端安全进行攻击。

有统计显示，2021年，中国主流智能汽车产品的OTA更新平均周期大约仅为两周。一方面，这些OTA升级为用户带来了新的功能体验，让人们对于“智能汽车常用常新”“软件定义汽车”的憧憬成为现实；但另一方面，由于汽车OTA相关的标准规范尚不健全，车企没有具体的实用性标准参考，导致车企无据可循。

2021 年 8 月，工信部发布《关于加强智能网联汽车生产企业及产品准入管理的意见》：明确了汽车生产企业实施升级的管理能力要求和升级活动备案要求，OTA 升级活动应保障产品安全性和生产一致性。

2022 年 4 月，工信部装备中心发布《关于开展软件在线升级备案的通知》：明确获得道路机动车辆生产准入许可的汽车整车生产企业及其生产的具备 OTA 升级功能的汽车整车产品，在开展 OTA 升级活动前，应进行备案。

《关于开展软件升级备案的通知》的要求主要有以下五点：

第一，企业实施 OTA 升级活动应当确保汽车产品符合国家法律法规、技术标准及技术规范等相关要求，保障汽车产品生产一致性；

第二，企业应按要求依次完成企业管理能力备案、车型及功能备案和具体升级活动备案后，才能实施 OTA 升级活动；

第三，根据升级活动的影响评估，具体升级活动应采取分级备案；

第四，企业是 OTA 升级活动安全 and 产品生产一致性的责任主体。企业应履行告知义务；

第五，企业应识别升级活动所影响的电子控制系统，并保存软件初始和升级版本（集），支持实施升级追溯管理。相关备案信息应真实、准确和完整。

上述一系列举措都意味着针对汽车远程升级（OTA）的政策法规正在逐步完善，同样相应技术标准亟需制定。

因此设立汽车远程升级（OTA）信息安全测试规范项目，制定一套结合企业实际生产需要的，覆盖汽车远程升级（OTA）前系统验证、升级中的访问控制和密码技术应用和升级后的处置过程中的安全技术要求与测试方法。填补了该领域内的标准空白，对补齐汽车远程升级（OTA）测试规范的缺失环节，推动行业各方共同加强汽车远程升级（OTA）信息安全具有积极意义。

1.3 主要工作过程

本标准于 2022 年 5 月开始进行前期研究及调研，国汽智联联合行业知名检测机构、整车厂商、研究院所、安全技术服务商等单位成立《汽车远程升级（OTA）信息安全测试规范》标准项目组。项目组成员系统分析了汽车远程升级（OTA）中存在的信息安全问题，并调研车辆在实际使用 OTA 升级中云端、车端、通讯端的工作方式及对服务平台的信息安全需求，以此确定汽车远程升级（OTA）信息安全测试方法。

2022 年 6 月 8 日，向项目组成员单位发送第一次会议通知，并发送标准草案征集参编单位意见。会前共收集反馈意见 21 条。

2022 年 6 月 15 日，组织召开项目组第一次会议。会上首先对远程升级（OTA）国内外相关政策标准情况进行介绍，接着向参会代表介绍了本标准的编制开展计划及标准定位，其次进行标准参编单位及人员介绍，最后项目组成员对标准文本内容以及反馈意见进行讨论。会后根据讨论结果，向项目组成员发送修订后的标准草案并继续征集意见。

2022 年 7 月 1 日，根据前期收集的 33 条反馈意见，组织召开项目组第二次会议。会上经项目组成员讨论后达成一下共识：1）修改标准范围；2）补充测试项目中的前置条件；3）增加服务平台、测试服务平台术语定义；4）统一全文件中的名词表述。

2022 年 8 月，本标准由中国汽车工程学会批准立项，文件号中汽学函【2022】145 号，任务号为 2022-66。同时，标准在中国汽车工程学会、中国智能网联汽车产业创新联盟等平台进行参编单位征集，进一步扩大项目组成员。

2022 年 10 月 13 日，向全体项目组成员进一步对标准文本进行征集意见，共收集反馈意见 163 条。2022 年 11 月 24 日，召开项目组第三次会议。会议中对收集到的 163 条意见全部处理完毕，并达成以下共识：1）统一并完善标准中对密码算法的要求与表述；2）统一并完善标准中对服务平台与升级设备的数据处理活动安全测试的要求与表述；3）将 OTA 升级包安全测试放在规范性附录 A 中，不做强制性测试。会后根据讨论结果，向项目组成员发送修订后的标准草案并继续征集意见。

2023 年 2 月 22 日，召开项目组第四次会议，会上对收集到的 46 条意见全部处理完毕，并增加了密钥生成策略测试项。会上向项目组成员说明下一步工作计划，即公开征集意见、标准验证试验。

二、标准编制原则和主要内容

2.1 标准制定原则

在充分总结和比较了国内外对汽车远程升级（OTA）的基础上，参考了 WP. 29/R155（信息安全与信息安全管理系统）、WP. 29/R156（软件升级与软件升级管理系统）、GB《汽车整车信息安全技术要求》、GB《汽车软件升级通用技术要求》等标准内容。本标准对汽车远程升级（OTA）过程中，服务平台安全、通信链路安

全、车载设备安全、升级过程安全等方面的测试要求进行梳理与归纳总结，给出相应的测试目的、测试方法、前置条件、通过标准。

2.1.1 通用性原则

本标准提出的汽车远程升级（OTA）信息安全测试规范适用于 M 类、N 类汽车远程升级（OTA）的信息安全设计开发、验证和生产工作。

2.1.2 指导性原则

本标准提出的汽车远程升级(OTA)信息安全测试方法,可为汽车远程升级(OTA)的信息安全设计开发、验证和生产工作提供指导。

2.1.3 协调性原则

本标准提出的测试方法与目前使用的国家标准中的方法协调统一、互不交叉。仅作为一种更便捷、精确度更高、更高效的方法对目前使用的方法进行补充。

2.1.4 兼容性原则

本标准提出的汽车远程升级（OTA）信息安全测试规范，具有普遍适用性。

2.2 标准主要技术内容

本标准共分为 10 章，规定了汽车 OTA 升级前的服务平台验证、升级中的访问控制和密码技术应用，及升级后的处置过程中的测试方法。

内容包括：

- （1） 范围
- （2） 规范性引用文件、
- （3） 术语和定义
- （4） 缩略语
- （5） 测试条件

本章节中，规定了测试环境要求、测试工具要求、测试服务平台要求、测试通信链路要求、测试车载设备要求。

（6） 服务平台安全测试

本章节中，规定了托管环境的安全测试、服务平台公开安全漏洞、服务平台访问控制机制测试、服务平台用户凭据安全测试、服务平台认证失败处理安全测试、服务平台数据处理活动安全测试、服务平台会话安全机制测试、服务平台随机数生成机制安全测试、服务平台日志机制安全测试等要求。

（7） 通信链路安全测试

本章节中规定了升级前访问认证安全测试、通信数据传输安全测试、密钥生成策略测试、密钥强度与算法安全测试、密钥存储安全测试、通信协议安全测试等要求。

（8） 车载设备安全测试

本章节中规定了升级设备计算环境（安全基线）安全测试、升级设备密码模块安全测试、升级设备数据处理活动安全测试、非授权软件安全校验机制测试、系统访问控制（权限管理）机制安全测试等要求。

（9） OTA 过程安全测试

本章节规定了用户提示及交互过程测试、升级启动前安全检查机制测试、升级启动后自检机制安全测试、升级失败回滚机制安全测试、升级成功功能自检和审计机制测试、数据及隐私保护机制测试、升级过程日志与存储安全测试、断电保护安全测试、升级中断恢复机制测试、低版本升级阻断测试等要求。

（10） OTA 升级包安全测试

本章节规定了升级包组件安全漏洞测试、升级包签名测试、升级包隐藏调试接口与函数测试、升级包保护机制测试、升级包签名密钥安全测试等要求。

2.3 关键技术问题说明

本标准的主要技术内容分为服务平台安全（托管环境、公开安全漏洞、访问控制机制、用户凭据、认证失败处理、数据处理活动、会话安全机制、随机数生成机制、日志机制），通信链路安全（升级前访问认证、通信数据传输、密钥生成策略、密钥强度与算法、密钥存储、通信协议），车载设备安全（计算环境、密码模块、数据处理活动、非授权软件校验机制、系统访问控制机制），OTA 升级过程安全（用户提示及交互过程、升级启动前安全检查机制、升级启动后自检机制、升级失败回滚机制、升级成功功能自检和审计机制、数据及隐私保护机制、升级过程日志与存储、断电保护、升级中断恢复、低版本升级阻断）。

2.4 标准主要内容的论据

编制内容主要基于细化完善 OTA 信息安全测试的测试目的、测试方法及通过标准，主要内容包括服务平台、通信链路、车载设备、升级过程、升级包的安全测试。编制内容主要参照的法规及标准内容如下：

WP.29/R156（软件升级与软件升级管理系统）及 GB《汽车软件升级通用技术要求》，参考了 R156 法规及强标中信息安全相关部分，包括汽车软件升级的管理体系要求、车辆要求、试验方法。

WP.29/R155（信息安全与信息安全管理系统）及 GB《汽车整车信息安全技术要求》，参考了 R155 法规附录 5（表 A1 4.3.3 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），基于国内行业发展现状，GB《汽车整车信息安全技术要求》对“软件升级安全要求”提出具体技术要求及测试方法，在团体标准《汽车远程升级（OTA）信息安全测试规范》中均有参考。

GB/T 40861-2021《汽车信息安全通用技术要求》，参考了标准中规定的软件升级活动应确保软件和近距离、远距离通信的真实性、保密性、完整性、可用性、访问可控性、抗抵赖性、可核查性及可预见性。以及列举的软件升级活动可能带来的固件覆写、升级包重放、非法软件安装及拒绝正常软件升级等信息安全风险。

2.5 标准工作基础

编制组主编单位国汽（北京）智能网联汽车研究院有限公司，目前已具备汽车远程升级（OTA）信息安全测试能力并完成相关测试工具开发。公司的信息安全实验室已承接各种整车或零部件的信息安全测试项目，测试经验丰富。在标准制定方面，牵头或参与了多项国家标准、行业标准及团体标准，其中包括 GB《汽车整车信息安全技术要求及测试方法》、GB/T《汽车信息安全应急响应管理规范》、GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》、GB/T 40861-2021《汽车信息安全通用技术要求》、YD/T《C-V2X 车辆异常行为管理技术要求》等。

主要起草单位有惠州市德赛西威汽车电子股份有限公司、陕西重型汽车有限公司、博世汽车部件（苏州）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）、北京百度网讯科技有限公司、北汽福田汽车股份有限公司、北京航迹科技有限公司、北京汽车研究总院有限公司、重庆长安汽车股份有限公司、浙江长三角车联网安全技术有限公司、北京赛目科技股份有限公司、招商局检测车辆技术研究院有限公司、苏州挚途科技有限公司、中汽研软件测评（天津）有限公司、江苏智能网联汽车创新中心有限公司、中国标准化研究院长三角分院、襄阳达安汽车检测中心有限公司、中国汽车工程研究院股份有限公司、北京经纬恒润科技股份有限公司、北京万集科技股份有限公司、国汽智端（成都）科技有限公司、国家金融科技测评中心、中国信息通信研究院、紫光国芯微电子股份有限公司、国家工

业信息安全发展研究中心、一汽奔腾轿车有限公司、江铃汽车股份有限公司、南德认证检测（中国）有限公司上海分公司、宁波谦川科技有限公司等。主要成员单位囊括了行业内知名检测机构、整车企业、零部件厂商、安全公司及研究院所，具备应用 OTA 技术整车升级或零部件升级、OTA 产品研发或提供 OTA 解决方案 OTA 测试经验或测试工具产品等参编条件。

三、主要试验（或验证）情况分析

中国智能网联汽车产业创新联盟（CAICV）在 2023 年 3 月至 4 月期间开展标准验证工作。

验证内容主要包括：汽车远程升级（OTA）软件升级服务平台安全、通信链路安全、车载设备安全及 OTA 升级过程安全等内容。

验证形式主要在国家智能网联汽车创新中心信息安全实验室现场验证或参与单位所在地现场验证。

验证企业包括：具备应用 OTA 技术整车升级或零部件升级的整车企业；具备 OTA 产品研发或提供 OTA 解决方案的供应商企业；具备 OTA 测试经验或测试工具产品的检测机构、安全技术服务厂商等。

验证情况分析（待标准验证试验结束后进行总结分析）：

四、标准中涉及专利的情况

无。

五、预期达到的社会效益、对产业发展的作用的情况

本标准的编制，提出了汽车 OTA 升级前的服务平台验证、升级中的访问控制和密码技术应用，及升级后的处置过程中的测试方法。标准发布后，可以为智能网联汽车产品准入测试评价、沙盒监管测试评价提供参考、支撑中国特色第三方智能网联汽车测试评价体系、引导产品测试评价优化提供输入。

六、采用国际标准和国外先进标准情况，与国际、国外同类标准水平的对比情况，国内外关键指标对比分析或与测试的国外样品、样机的相关数据对比情况

尚无。

七、在标准体系中的位置，与现行相关法律、法规、规章及相关标准，特别是强制性标准的协调性

本标准符合国家有关法律、法规和相关强制性标准的要求,与现行的国家标准、行业标准相协调。

八、重大分歧意见的处理经过和依据

尚无。

九、标准性质的建议说明

本标准为中国汽车工程学会标准,属于团体标准,供协会会员和社会自愿使用。

十、贯彻标准的要求和措施建议

严格按照本标准提出的试验方法对材料的卤素含量进行检测,对试验人员进行理论学习和操作培训,保证检测方法操作的准确性。

十一、废止现行相关标准的建议

无。

十二、其他应予说明的事项

无。

标准起草工作组
2023年2月24日

(注:具体内容可以结合项目本身撰写,如不涉及的可填写无)