



中华人民共和国国家标准

GB/T XXXXX—XXXX

基于远程升级技术的汽车产品召回实施 要求

Recall implementation requirements of motor vehicle products
based on Over-The-Air update technology

(点击此处添加与国际标准一致性程度的标识)

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 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..... II

1 范围..... 3

2 规范性引用文件..... 3

3 术语和定义..... 3

4 基本原则..... 5

 4.1 合规原则..... 5

 4.2 分类原则..... 5

 4.3 视同原则..... 5

 4.4 安全原则..... 5

5 备案要求..... 5

 5.1 OTA 技术服务活动备案..... 5

 5.2 OTA 召回活动备案..... 5

 5.3 升级信息备案说明资料..... 6

6 召回实施过程要求..... 6

 6.1 召回通知..... 6

 6.2 升级日志要求..... 6

 6.3 升级失败解决方案..... 7

 6.4 OTA 过程监督..... 7

7 召回效果评估要求..... 7

 7.1 评估方法..... 7

 7.2 召回措施验证评估..... 8

 7.3 召回措施验证不通过项评估..... 8

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。

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。

本文件由全国产品缺陷与安全管理标准化技术委员会（SAC/TC 463）提出并归口。

本文件起草单位：

本文件主要起草人：

基于远程升级技术的汽车产品召回实施要求

1 范围

本文件给出了基于远程升级技术的汽车产品召回实施的基本原则、备案要求、实施过程要求和效果评估要求。

本文件适用于生产者开展的基于远程升级技术的汽车产品技术服务活动和召回活动。

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 43387 产品召回 术语

GB/T 34402-2017 汽车产品安全 风险评估与风险控制指南

GB/T XXX 汽车产品召回 信息缺陷评估指南

GB/T 39603-2020 缺陷汽车产品召回效果评估指南

GB/T 40914-2021 汽车产品召回 预警规则

GB 44495 汽车整车信息安全技术要求

GB 44496 汽车软件升级通用技术要求

3 术语和定义

GB/T 43387、GB/T 39603、GB 44496界定的以及下列术语和定义适用于本文件。

3.1

软件 software

电子控制系统中由数字数据和指令组成的部分。

[来源：GB 44496-2024，3.1]

3.2

软件下载 software download

将软件从一个计算机系统（例如：车辆或后台服务器）复制到另一个计算机系统。

3.3

软件升级 software updates

将某版本的软件通过升级包更新到新版本（包括更改软件的配置参数）的过程。

注1：“软件升级”也称“软件更新”。

注2：“软件升级”包含在线升级和离线升级。

注3：“软件升级”包含固件升级、应用软件升级或参数配置升级等。

[来源：GB 44496-2024，3.2]

3.4

远程升级 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：“远程升级”也称“在线升级”。

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]

3.5

升级包 update packages

用于进行软件升级的软件包。

3.6

回滚 rollback

将车辆内的软件或数据恢复到以前可用版本的过程。

3.7

OTA 召回 recall based on Over-The-Air update technology

生产者通过OTA方式对其已售出的汽车产品采取措施消除缺陷的活动。

3.8

技术服务活动 technical service activities

生产者提供与软件升级相关的技术服务，包括发布形式、升级内容、升级范围等。

3.9

升级范围 update scope

升级所解决问题涉及到产品的界限。

注1：如产品生产起止日期、生产批号或批次等。

[来源：GB/T 43387-2023, 5.22]

3.10

召回部件 recall parts

通过OTA召回方式来解决缺陷的ECU及软件。

3.11

召回提示 recall notes

提供给用户的召回升级内容描述。

3.12

升级包证书校验 certificate verification for the update package

升级包对应证书的有效性验证。

3.13

升级包措施验证 update package measure verification

升级流程措施、内容有效性措施以及缺陷解决措施验证。

3.14

车辆用户 vehicle user

操作、驾驶、拥有或管理车辆的人。

示例：车辆所有者、车辆运营方的授权代表或雇员、车辆制造商的授权代表或雇员。

[来源：GB 44496-2024, 3.11]

3.15

车载 OTA 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]

3.16

措施次生影响 additional effect of measures

生产者采取的召回措施实施后使汽车的部分性能或功能受到影响的情况，但未产生新的缺陷。

[来源：GB/T 39603-2020, 3.11]

4 基本原则

4.1 合规原则

生产者开展基于远程升级技术的召回实施活动，应满足《缺陷汽车产品召回管理条例》、《缺陷汽车产品召回管理条例实施办法》等法规和召回主管部门发布的政策性文件要求。

4.2 分类原则

4.2.1 生产者采用 OTA 方式解决非缺陷问题时，需按技术服务活动执行。

4.2.2 生产者采用 OTA 方式解决缺陷或排放危害问题时，需按召回活动执行。

4.3 视同原则

4.3.1 生产者采用 OTA 方式新增功能或提升性能，需进行安全或排放性能评估。

4.3.2 若评估不影响整车安全或排放性能变化，视同按技术服务活动执行。

4.3.3 若评估影响整车安全或排放性能变化，需进行缺陷或排放危害判定。

a) 判定不存在缺陷或排放危害的，视同按技术服务活动执行；

b) 判定存在缺陷或排放危害的，应及时向召回主管部门报告，视同按召回活动执行。

4.4 安全原则

4.4.1 生产者应建立与升级活动相适应的管理制度和保障能力，确保升级过程及升级后的车辆安全。

4.4.2 对可能在车辆行驶过程中进行的远程升级，应确保在远程升级不会影响车辆安全。

4.4.3 当执行远程升级可能影响车辆安全时，在执行远程升级时，应通过技术措施确保车辆安全。

4.4.4 当远程升级失败时，应确保及时将车辆系统回滚至以前的可用版本或将车辆置于安全状态。

5 备案要求

5.1 OTA 技术服务活动备案

5.1.1 生产者需在 OTA 发布前 5 个工作日内完成技术服务活动备案。

5.1.2 备案的 OTA 技术服务活动信息发生变化的，需在 20 个工作日内进行更新。

5.1.3 OTA 技术服务活动备案内容包括车辆基本信息、升级服务基本信息、升级包信息、云平台信息、安全防护信息等。

5.2 OTA 召回活动备案

5.2.1 OTA 召回活动备案包括召回计划备案和升级信息备案。

5.2.2 生产者需在确认缺陷或排放危害后 5 个工作日内按召回主管部门要求完成召回计划备案。

5.2.3 生产者需在召回实施前完成升级信息备案，相关要求及内容与第 5.1 节一致。

5.2.4 当生产者备案召回计划时尚未完成 OTA 升级信息准备的，需明确 OTA 召回措施的原理、措施有效性证明后，发布召回公告。

5.2.5 生产者备案召回计划时，需明确线上、线下召回涉及的车辆数量、计划完成率等内容。

5.3 升级信息备案说明资料

5.3.1 备案升级信息时，除第 5.1.3 条内容外，还需提供升级策略、升级包、升级部件和 OTA 系统车端要求等的说明资料。

5.3.2 升级策略说明资料，

- a) 提供升级策略，明确分批次或分区域等实时计划和目标；
- b) 提供升级策略有效性评估方案、灰度定义、成功率定义、配套售后策略及应急响应措施。

5.3.3 升级包说明资料，包括以下内容：

- a) 提供升级包命名规则、数据格式，升级前后对应的控制器版本、涉及的关键参数变化。
- b) 若为差分升级，需要提供原始升级包、差分算法、还原方法、签名验证方法。
- c) 提供升级包安全策略，包含证书信息、加密算法和模式（若加密）。
- d) 软件包信息安全要求符合《汽车整车信息安全技术要求》，提供升级包安全测评报告和漏洞安全测试报告，可由生产者自行提供，或由第三方检测机构给出。

5.3.4 升级部件说明

- a) 提供升级部件信息，包括软硬件信息（至少包括主 MCU 信息、操作系统、软件版本）及其功能变化内容。
- b) 提供与升级部件相关控制器的软硬件信息，及其功能变化内容。
- c) 提供升级部件涉及系统相关的电子电气架构信息，包括网络拓扑、车内网络通信方式。
- d) 提供升级部件及相关系统的单元、子系统及整车功能和信息安全测试报告。

5.3.5 OTA 系统车端要求

- a) 提供远程升级系统车端信息，包括车端远程升级主节点功能相关信息（至少包括升级功能信息以及安全方案信息）。
- b) OTA 系统车端要求符合《汽车软件升级通用技术要求》，提供远程升级系统车端安全测评报告，可由生产者自行提供，或由第三方检测机构给出。

5.3.6 生产者需确保升级信息材料的客观准确性和完整性，至少包括以下要求：

- a) 确保升级包内容对缺陷升级的措施有效性，以及测试验证报告的一致性。
- b) 核验升级包证书信息，确保该证书真实有效。
- c) 开展 OTA 系统车端评估，内容包含信息安全评估与可靠性评估。

6 召回实施过程要求

6.1 召回通知

6.1.1 召回通知内容应至少包括升级涉及部件、缺陷问题描述、缺陷可能造成的后果、升级时长、升级时需满足的车况条件、升级失败的处置措施。

6.1.2 除挂号信外，生产者可采取以下方式进行召回通知，但需确保通知可记录、可追溯：

- a) 通过车载 HMI、车载 IVI、仪表、HUD 等车端方式通知；
- b) 通过手机短信、手机 APP 等车端外方式通知。

6.1.3 生产者确认通知五次后，用户仍然不升级，可发布标志性警示提醒。

6.2 升级日志要求

6.2.1 生产者需及时将升级日志上传到智能网联汽车安全大数据云平台。

6.2.2 升级日志应包含如下内容：

- a) 云服务平台系统管理日志，包括升级完成情况、升级失败原因信息和升级过程中发生的信息安全日志。
- b) 车云交互日志，包括车端收到云端远程升级请求的信息、时间、车端上传升级前版本号信息、升级结果、完成升级时间信息。
- c) 车端待升级控制器的执行日志，包括待升级控制器升级前版本信息、升级执行时间、升级次数、升级结果、升级结果判定、升级后控制器版本信息。
- d) 用户 HMI 确认日志，包括用户 HMI 确认信息显示时间、显示方式、用户确认车辆停靠状态（是否在安全区域停车升级）、用户确认远程升级时间、确认远程升级结果信息。
- e) 车内远程升级通信日志，包括升级范围确认、升级包下载时间、远程升级车辆状态（电源电压状态，车速状态，刹车状态等）、升级所用时长信息。

6.3 升级失败解决方案

6.3.1 对于部分车辆出现升级失败的情况，生产者应提供升级失败后的解决方案。

6.3.2 对于多次尝试升级仍然失败的，由生产者需及时与用户联系，为用户提供远程协助，帮助用户及时前往就近的厂家指定维修点进行线下升级。

6.4 OTA 过程监督

6.4.1 生产者按召回主管部门提交召回阶段性报告和召回总结报告，提供线上升级已完成车辆、升级失败车辆的升级日志和线下升级完成车辆的证明材料。

6.4.2 召回主管部门通过对生产者提交的升级日志进行实施执行过程的审查，判断过程是否符合召回计划。

6.4.3 过程监督内容包括：

- a) 验证生产者所发布召回信息是否符合召回主管部门要求；
- b) 验证车辆用户是否能够收到本次 OTA 召回信息；

6.4.4 监督 OTA 召回实施过程的关键信息，包括但不限于升级包下载结果、用户确认结果、OTA 升级结果、车辆 VIN、车辆状态信息、召回部件版本信息。如升级结果为失败，则还应提交失败原因。

6.4.5 生产者应提供总结报告，包含下载成功率数量，下载失败数量，安装成功数量，安装失败数量，失败原因统计等。

6.4.6 生产者应分别统计线上、线下召回的完成情况，计算实际完成率，并以升级日志、召回维修工单等方式保存相应的证明材料。

6.4.7 OTA 云服务平台与智能网联汽车安全大数据云平台应通过 PKI 认证体系确保传输数据的真实性、完整性和机密性，智能网联汽车安全大数据云平台应该具备数据分析功能，可对 OTA 日志文件分析统计。

6.4.8 生产者需将 OTA 升级日志从 OTA 云服务平台上传至智能网联汽车安全大数据云平台。

6.4.9 监督的方法可以分为定期审核、抽查审核。

- a) 定期审核：对阶段性报告进行审核(是否按时提交报告，以及内容是否完整)；
- b) 抽查审核：对召回实施具体情况进行审核。

7 召回效果评估要求

7.1 评估方法

7.1.1 召回效果评估方法参照《缺陷汽车产品召回效果评估指南》开展，包括线上升级、线下升级综合完成情况评估。必要时，开展召回措施验证评估。

7.2 召回措施验证评估

7.2.1 OTA 召回实施后，若发生大量用户投诉，需进行措施有效性验证评估。

7.2.2 措施有效性验证评估包括功能验证与信息安全验证。

7.2.3 可采用如下验证方法之一或组合，进行功能验证：

- a) 边界值法：根据测试经验，对边界数据着重测试。
- b) 错误推测法：根据测试者的经验，对可能出现错误的地方多进行测试。
- c) 等价法：把输入条件划分为若干等价类，在每一个等价类中取一个数据作为测试的输入条件。
- d) 其他方法。

7.2.4 可采用如下验证方法之一或组合，进行信息安全验证：

- a) 漏洞扫描，确认测试对象是否存在漏洞。
- b) 渗透测试，通过模拟对系统的实战攻击，验证测试对象能够有效地实施相应的安全措施。
- c) 模糊测试，通过大量的数据或信号，对测试对象的功能进行压力测试，判断测试对象是否会在设定的情况下产生漏洞或出现异常行为。
- d) 其他方法。

7.3 召回措施验证不通过项评估

7.3.1 对于功能措施验证的不通过项，参考《汽车产品安全风险评估与风险控制》进行风险评估，识别功能次生影响。

7.3.2 对于信息安全措施验证的不通过项，参考《汽车产品召回信息缺陷评估指南》进行风险评估，识别信息安全次生影响。