《智能网联汽车软件升级技术要求》（送审稿）编制说明

一、项目背景

（一）国内外现行相关法律、法规和标准情况

2020年6月，联合国世界车辆法规协调论坛（WP29）通过并发布R 156《关于软件升级和软件升级管理系统的汽车型式批准统一规定》，在软件升级管理体系证书、软件升级管理体系要求、车型要求、车型修改及扩展、生产一致性等方面做出规定。欧盟计划从2022年7月起所有新车型如果不满足R156将无法获取WVTA（Whole Vehicle Type Approval）证书，无法上市销售，2024年7月起制造的车辆必须满足该要求方可出厂销售。同时日本也将R 156纳入其汽车法规体系。

汽标委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《汽车软件升级通用技术要求》国家标准，该标准属于通用的技术要求，已于2022年6月份公开征求意见。国内目前尚无与软件升级相关的省市地方标准。

（二）必要性和意义

随着技术的不断发展，汽车通过软件升级的方式进行功能、性能的优化已成为一种常态，也是车辆的卖点之一。但也带来一系列安全问题，很多企业通过软件升级私自锁电或更改车辆的重要参数。深圳市的机动车保有量位居全国前列，几乎所有品牌的车辆都在深圳市内销售，如何对汽车的软件升级进行有效管理是当前的燃眉之急。软件升级对现行汽车管理制度带来挑战，现行汽车产品管理制度是基于型式的许可（或认证）管理，要求车辆参数须符合相关国家标准和规定，且实际生产产品性能参数应与准入型式保持一致。但在软件升级广泛应用的情况下，汽车生产企业很容易绕开现有汽车产品管理制度而对汽车安全、排放、能耗等准入相关参数进行大量调整，势必引发产品一致性问题，对现行汽车管理制度带来挑战。目前国家相关部委已出台了一系列政策，但有必要根据深圳市的实际情况出台相关标准，对具有软件升级功能的车辆进行测试和管理，保证安全。

二、工作简况

（一）任务来源

2022年8月24日，深圳市市场监督管理局下达文件《深圳市市场监督管理局关于下达2022 年第二批深圳市地方标准计划项目任务的通知》，通知中指出，决定对《智能网联汽车软件升级技术要求》等12项标准予以立项。

（二）主要起草过程

受深圳市市场监督管理局委托，中汽研软件测评（天津）有限公司根据申请情况成立标准起草项目组，确定中汽研软件测评（天津）有限公司为牵头单位，并在此基础上明确了任务和分工，积极开展标准的预研立项、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软件升级标准法规现状和国内强制性国家标准《汽车软件升级通用技术要求》内容，编写了标准草案，最终完成了标准的送审稿。

1. 预研立项阶段

2022 年 1 月～2 月 组建标准工作组，完成标准框架编写。

智能网联汽车软件升级技术要求标准项目组第一次会议于 2022 年 2 月 16 日在线上召开，正式启动标准制定工作。会议就标准的制定背景、范围、框架、技术现状进行了详细的讨论。会议明确：该标准以深圳市地方标准进行立项；该标准将参考国内正在制定的强制性国家标准《汽车软件升级通用技术要求》草案进行编制。

2. 组织起草阶段

2022 年 3 月～7 月 进行标准草案的编制，参考强制性国家标准《汽车软件升级通用技术要求》征求意见稿，形成标准的主体内容。

智能网联汽车软件升级技术要求标准项目组第二次工作会议于 2022 年 7 月 26 日在线上召开，会议明确参考《汽车软件升级通用技术要求》征求意见稿进行草案的修改和完善，并且分工进行。2022 年 9 月，秘书处面向深圳市企业征集试验车辆，计划开展标准验证工作。2022 年 10 月组织开展标准验证工作。

3. 意见征求阶段

智能网联汽车软件升级技术要求标准项目组第三次工作会议于 2022 年 8 月 26 日在线上召开，会议就标准草案进行讲解讨论，并征集工作组成员意见。

2022 年 12 月 5 日～2022 年 12 月 9 日，通过电子邮件的方式征求了深圳市交通运输局、深圳市公安局交通警察局、深圳市发展和改革委员会、深圳市市场监督管理局、中国银行保险监督管理委员会深圳监管局、深圳市政务服务数据管理局、深圳市住房和建设局、深圳市人民政府国有资产监督管理委员会、深圳市前海深港现代服务业合作区管理局、各区政府（福田区、罗湖区、南山区、宝安区、龙岗区、坪山区、龙华区、光明区、大鹏新区、深汕特别合作区）的意见，并根据意见修改标准草案。

三、主要内容的依据以及与国内领先、国际先进标准的对标情况

（一）主要内容的依据

本文件以强制性国家标准《汽车软件升级通用技术要求》征求意见稿（计划号：20214423-Q-339）（2022 年 6 月版本）为基础制定，主要用于支持深圳市智能网联汽车准入管理工作的实施，原标准由中华人民共和国工业和信息化部提出，全国汽车标准化技术委员会（SAC/ TC114）归口。

（二）与国内领先、国际先进标准的对标情况

本标准未采用国际标准。

本标准主要技术内容包括汽车软件升级管理体系要求、车辆要求、试验方法。本标准的

制定借鉴强制性国家标准《汽车软件升级通用技术要求》征求意见稿（计划号：20214423-Q-339）（2022年6月版本）。

四、主要条款的说明以及主要技术指标、参数、试验验证的论述

（一）范围

给出了本文件规定的内容和适用的范围。

本文件规定了汽车软件升级的管理体系要求、车辆要求、试验方法、车辆型式的变更和扩展、说明书。

本文件适用于M类、N类汽车，其他车辆类型可参照执行。

（二）规范性引用文件

给出了本文件规范性引用文件的情况。本文件主要引用了强制性国家标准《汽车软件升级通用技术要求》征求意见稿（计划号：20214423-Q-339）（2022 年 6 月版本）和《智能网联汽车整车信息安全技术要求》。

（三）术语和定义

给出了本文件涉及的术语和定义的情况。

本文件主要规定了“软件”“软件升级”“软件识别码”“软件升级管理体系”“在线升级”“升级包”“执行”“安全状态”“完整性验证数据”“系统”“车辆用户”11 个术语。

“软件”是指电子控制系统中由数字数据和指令组成的部分。

“软件升级”是指将某版本的软件更新到新版本或更改配置参数的过程。

“软件识别码”是指由车辆制造商定义，用于表示与型式批准相关系统中软件信息的专用标识符。

“软件升级管理体系”是指为完成软件升级而制定的一种规范组织的过程和程序的系统方法。

“在线升级”是指通过无线方式而不是使用电缆或其他本地连接进行数据传输的软件升级。

“升级包”是指用于进行软件升级的软件包。

“执行”是指安装和激活已下载升级包的过程。

“安全状态”是指当软件升级中断或失败时，一种没有不合理风险的运行模式。

“完整性验证数据”是指用以检测数据中的错误或变化的值。

“系统”是指用于实现功能的一组车辆部件和/或子系统。

“车辆用户”是指操作、驾驶、拥有或管理车辆的人。

（四）主要条款及说明

4.1 软件升级管理体系要求

4.1.1 一般要求

规定了车辆制造商建立软件升级管理体系的一般要求，包括信息存储要求、是否存储软件识别码 的要求。为了证明信息得到安全保存，可以使用国家/行业/国际标准。所提供的信息可能包括访问控制（物理和个人）、确保保存信息的服务器安全的控制措施、监测控制措施、配置控制措施、质量控制措施/所采用的质量管理体系。车辆制造商应演示并证明如何为给定车型生成软件识别码，并保证软件识别码的唯一性；每个软件识别码与其相应的型式批准要求存在对应关系，以及如何识别该对应关系；当型式批准相关系统进行软件升级时，如何保障同步更新软件识别码。无论车型是否具备软件识别码，只要车辆未存储识别码，车辆制造商应演示并证明辆的哪些电子控制单元（ECU）与型式批准有相关性，以及如何识别对应关系，当型式批准相关系统进行软件升级时，如何保障同步更新声明。

4.1.2 过程要求

规定了配置管理过程要求、软件识别码访问更新过程要求、相关性识别过程要求、目标车辆识别过程要求、兼容性确认过程要求、型式批准和安全相关影响评估过程要求、用户告知过程要求。对于在软件升级前后，能访问软件识别码相关信息的过程和在软件升级后，能更新软件识别码相关信息的过程，至少更新所有相关软件的版本及完整性验证数据，车辆制造商能够证明可以访问和更新软件识别码相关的信息，信息至少应存储在车辆制造商处。当系统发生了会导致车辆型式扩展或变更的软件升级时，软件识别码应改变；如果软件升级不会导致车辆型式扩展或变更，则该软件识别码应保持不变。

4.1.3 信息记录要求

规定了车辆制造商应记录用于描述进行软件升级所使用的所有过程信息以及以上过程如何应用于各种车型的说明。车辆制造商应至少能够记录与软件升级相关的车辆系统的所有配置，可能有一系列的历次配置或版本。“配置”包括系统的硬件、软件以及任何相关车辆或系统的参数。车辆制造商应记录关于目标车辆的信息，且应提供到车辆 VIN 码的层级。应记录检测目标车辆最新已知配置与软件升级的兼容性的方法、过程、结果的文件。

4.1.4 安全相关要求

规定了升级包安全要求、升级过程安全要求、功能和代码安全要求、应急管理要求。车辆制造商应能够证明其有适当的过程来控制向车辆推送哪些升级包，并确保只向车辆推送已知和有效的升级包。这可能包括保证供应商提供的保障软件升级安全的过程。车辆制造商应能够证明其有适当的过程来确保升级机制不会被操纵用于提供未经授权的升级。针对软件升级过程中可能突然发生的意外事件（例如升级中断或失败，以及升级过程中因车辆或人为因素导致的意外事件），车辆制造商应具备应急管理机制用于处理相应事件。

4.1.5 在线升级的附加要求

规定了驾驶过程中在线升级和在线升级需要特定的技能或复杂操作的要求。车辆制造商应对在驾驶过程中进行的软件升级进行安全评估，保障在线升级不会影响车辆安全。车辆制造商应建立过程确保车辆用户不需要做任何需要技术或复杂的事情来启动或完成软件升级。

当软件升级可能需要复杂操作时，需要有一个过程来确保只有当具备合适技能或训练有素的人员在场或者在远程执行时控制该过程时才进行这种软件升级。

4.2 车辆要求

4.2.1 一般要求

规定了升级包的真实性和完整性要求、软件识别码和/或软件版本更新读取要求、软件识别码和/或软件版本防篡改要求。要求在车辆上实施有效的真实性与完整性保护机制，以确保仅有效的升级包可被下载和执行，真实性和完整性应该由车辆进行有效验证。如果软件识别码在车辆上存储时，软件识别码应具备更新机制，且便于从车辆读取。如果软件识别码未在车辆上存储，则应将与型式批准相关的所有软件版本存储在车辆上，且具备更新机制，并便于从车端读取，并声明与型式批准相关系统的相关性。对于车辆存储软件识别码的，应同时保护软件识别码和软件版本，对于车辆未存储软件识别码的，应保护软件版本。软件识别码和/或软件版本只有授权方可以更新，且仅当在车辆上执行相关软件升级时才会发生此情况。

4.2.2 在线升级的附加要求

规定了用户告知要求、车辆用户确认要求、先决条件要求、电量保障要求、车辆安全要求、驾驶安全要求、车门防锁止要求、升级结果告知要求、级失败或中断要求。车辆制造商应说明如何得到车辆用户的确认。车辆制造商应定义软件升级要满足的先决条件，并确认每当软件升级开始时，这些条件都得到满足。保障车辆具备完成软件升级所需的电量，且具备在升级失败后恢复到以前版本/使车辆进入安全状态所需的电量，该要求不限制技术路线，例如电量检测、电压检测等。要求车辆制造商对执行软件升级是否影响车辆安全进行评估和识别，并通过技术手段确保车辆安全。要求车辆制造商对执行软件升级是否影响驾驶安全进行评估和识别，对于影响驾驶安全的软件升级项目，应采用技术手段确保车辆不能被驾驶，同时为了保障车辆安全和软件升级成功执行，还应限制部分车辆功能的使用。要求车辆在执行软件升级的过程中，至少保障车辆用户可以从车内解除车门锁止状态，避免一些紧急情况下，车内用户无法下车，技术方案不限行。要求车辆制造商在软件升级执行后，应将软件升级的结果及附加信息告知车辆用户，对于具有车载电子用户手册的，应及时更新手册内容避免对车辆用户造成误导。

4.3 试验方法

4.3.1 升级包真实性完整性试验

本试验是为了验证标准中 5.1.1 的要求。

对于在线升级，按照《智能网联汽车整车信息安全技术要求》 A.6.2.2 开展试验，试验结果符合 5.1.1 的要求;对于离线升级,按照《智能网联汽车整车信息安全技术要求》A.6.3 开展试验，试验结果符合 5.1.1 的要求。

4.3.2 软件识别码/软件版本更新及读取试验

本试验是为了验证标准中 5.1.2 和 5.1.3 的要求。

如果车辆上存储了软件识别码，车辆制造商应提供相应升级包，并提供软件识别码的标准接口的读取方式，包括通信协议、读取的诊断服务、诊断 DID 等。对比软件升级前后的软件识别码，符合车辆制造商的更新规则，则试验通过。

如果车辆上没有使用软件识别码，车辆制造商应提供相应升级包，并提供各相关软件版本的标准接口的读取方式，包括通信协议、读取的诊断服务、诊断 DID 等。对比软件升级前后的软件版本，符合车辆制造商的更新规则，则试验通过。

4.3.3 软件识别码/软件版本防篡改试验

本试验是为了验证标准中 5.1.4 的要求。

按照《智能网联汽车整车信息安全技术要求》 A.7.4 开展试验。

4.3.4 用户告知试验

本试验是为了验证标准中 5.2.1 的要求。本试验针对在线升级。

4.3.5 车辆安全试验

本试验是为了验证标准中5.2.2的要求。本试验针对在线升级。

4.3.6 驾驶安全试验

本试验是为了验证标准中 5.2.3 的要求。本试验针对在线升级。

根据车辆制造商提供的先决条件说明，在满足所有先决条件情况下，触发软件升级，查看是否能执行软件升级；在不满足先决条件情况下，触发升级，查看是否能执行软件升级。在满足所有先决条件情况下能执行软件升级，且在不满足先决条件情况下不能执行软件升级，则试验通过。

4.3.7 车门防锁止试验

本试验是为了验证标准中 5.2.4 的要求。本试验针对在线升级。

根据车辆制造商提供的电量保障措施的说明文件，在满足电量保障情况下，触发软件升级，查看是否能执行软件升级；在不满足电量保障情况下，触发软件升级，查看是否能执行软件升级。在满足电量保障情况下能执行软件升级，且在不满足电量保障情况下不能执行软件升级，则试验通过。

4.3.8 结果告知试验

本试验是为了验证标准中 5.2.5 的要求。本试验针对在线升级。

当车辆制造商声明该车型不涉及会影响车辆安全的软件升级项目，则本试验不适用。

当存在影响车辆安全的软件升级项目，根据车辆制造商提供的影响车辆安全的软件升级项目说明开展相应试验。如果车辆制造商设定的技术保护手段均被实施，则试验通过。

4.3.9 升级失败处理试验

本试验是为了验证标准中 5.2.6 的要求。本试验针对在线升级。

当车辆制造商声明该车型不涉及会影响驾驶安全的软件升级项目，则本试验不适用。

当存在影响驾驶安全的软件升级项目，根据车辆制造商提供的影响驾驶安全的软件升级项目说明开展相应试验。如果在执行软件升级中，车辆不能被驾驶，且影响车辆安全和影响软件升级成功执行的车辆功能不能被使用，则试验通过。

4.3.10 车门防锁止试验

本试验是为了验证标准中5.2.7的要求。本试验针对在线升级。

4.3.11 结果告知试验

本试验是为了验证标准中5.2.8的要求。本试验针对在线升级。

4.3.12 失败或中断处理试验

本试验是为了验证标准中 5.2.9 的要求。本试验针对在线升级。

4.4 车辆型式的变更和扩展

按本文件通过型式检验的车型，其结果可扩展到符合标准中7.2判定条件的其他车型。车型获得扩展后，此扩展车型不可再扩展到其他车型。

4.5 说明书

具备软件升级功能的车辆，其产品说明书至少应包含：“本车具备软件升级功能”等内容的说明；软件升级失败或中断后，车辆安全状态的说明；软件升级操作方法的说明。

（五）主要试验验证情况

5.1 试验综述

本标准验证情况参照强制性国家标准《汽车软件升级通用技术要求》，同时另征集一款车型进行验证，体系部分验证 17 家整车生产企业、车辆部分验证 15 款车型；

5.2 试验结果

软件升级管理体系要求：所有条款均被进行验证，不存在无法满足的要求。大部分企业均具备软件开发和软件升级管理的过程，但大多企业的过程比较分散，需要以软件升级为中心进行过程优化整合。另外，准入和认证相关参数或子系统相关过程要求需要企业根据自身的系统和产品进行分析完善，经过整改后可以支撑并通过本系统的评审。

车辆要求与试验方法：所有要求和试验方法均被验证，不存在无法满足的条款和无法进行的试验。升级包真实性和完整性试验、软件识别码/软件版本号防篡改试验等需要企业配合度高，涉及其信息安全的审批，该部分试验可以与信息安全相关标准同步开展。

五、涉及专利的有关说明

本标准不涉及专利。

六、重大意见分歧的处理依据和结果

本标准修订过程中无重大分歧。

七、实施地方标准的措施建议

由于汽车软件升级涉及企业软件升级管理体系调整、车辆功能开发、检测机构特殊试验开展等问题，建议本标准自发布日期至实施日期之间给予12个月过渡期。

本标准的实施日期为：

（1）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；

（2）对于已获得车辆型式批准的车型，自本文件实施之日起第13个月开始执行。