智能网联汽车软件在线升级安全风险分析及管理对策建议*

吴胜男[1]　朱云尧[1]　冀浩杰[2]　付兴坤[3]

（1. 中国汽车工程研究院股份有限公司，重庆 404100；2. 北京信息科技大学，北京 100192；3. 泰安北航科技园信息科技有限公司，泰安 271000）

【欢迎引用】吴胜男，朱云尧，冀浩杰，等. 智能网联汽车软件在线升级安全风险分析及管理对策建议[J]. 汽车文摘, 2023(3): 15-20.

【Cite this paper】WU S N, ZHU Y Y, JI H J, et al. Analysis of Software Online Updating Safety Risks and Suggestions for Intelligent Connected Vehicles [J]. Automotive Digest (Chinese), 2023(3): 15-20.

【摘要】智能网联是我国汽车产业重大战略方向，软件定义汽车成为行业发展方向的重要特征。智能网联汽车软件在线升级可实现全新功能导入、产品性能迭代、用户体验改善，具备经济、高效的显著特征。近年来，在应用规模、范围等方面均大幅提升。但是，汽车软件在线升级涉及升级前、升级中、升级后过程状态，对原有汽车管理模式带来新的挑战，需要综合分析国内外汽车创新管理经验，针对智能网联汽车软件在线升级潜在的安全风险，从管理方面提出针对性对策建议。

主题词：智能网联汽车　软件在线升级　安全风险　对策建议

中图分类号：U463.6；F426.471　　**文献标识码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20220191

Analysis of Software Online Updating Safety Risks and Suggestions for Intelligent Connected Vehicles*

Wu Shengnan[1], Zhu Yunyao[1], Ji Haojie[2], Fu Xingkun[3]

(1. China Automotive Engineering Research Institute Co. Ltd., Chongqing 404100; 2. Beijing Information Science & Technology University, Beijing 100192; 3. Beihang Taishan Science and Technology Innovation Park, Taian 271000)

【Abstract】Intellectualization and networking are the significant strategic development direction of the automobile industry in our country. Software defining vehicle has become an important feature of the development direction of the industry. With online upgrading of software for Intelligent and Connected Vehicle (ICV), the introduction of new functions, the iteration of product's performance, and the improvement of user experience can be realized economically and efficiently. In recent years, the scale and scope of its application have both been expanded. However, the online upgrading of ICV software involves process states before, during and after the upgrading process, which brings new challenges to the original pattern of managing the automobile. This paper comprehensively analyzes both domestic and foreign experience of innovative management of vehicles, and puts forward targeted solutions and proposals towards the potential security risks of ICV software's online upgrading from the aspect of management.

Key words: Intelligent and Connected Vehicle(ICV), Software online updating, Safety risk, Suggestion

1　引言

远程在线升级（Over-The-Air, OTA）是基于移动通信网络接口完成对移动终端产品的软件数据升级管理的技术，包含软件远程升级（Software Over The Air, SOTA）和固件远程升级（Firmware Over The Air, FOTA），主要用于智能手机行业[1]。对于汽车行业而言，2000年后，日本汽车制造厂商开始对配置T-BOX车载控制单元的汽车进行T-BOX系统的OTA远程升级。在此以后，部分汽车制造厂商开始对具备远程通信功能的车载信息娱乐系统（In-Vehicle Infotainment, IVI）进行OTA远程升级，如导航地图、应用音乐等，从OTA远程升级的功能内容范围分析，此时汽车行业主要针对车载信息娱乐系统和简单的电器部件控制功

*青年基金项目：车联网先导应用环境构建及场景测试验证平台建设项目（2020-0101-1-1）。

能，属于SOTA的范畴。从汽车OTA远程升级更新内容上分析，特斯拉Model S是一款真正搭载FOTA技术的汽车，通过远程升级修复安全漏洞、提升产品性能、改善用户体验[2]。自2018年以来，国内汽车OTA远程升级在功能搭载率、升级内容等方面均实现快速提升，OTA远程升级发展逐渐扩大化，并催生一批功能选装、硬件免费+软件收费等新型商业模式。由于智能化、网联化技术的赋能，OTA远程升级技术将成为未来汽车产品软件数据更新的主要方式，逐渐成为汽车智能化、网联化的标准配置，汽车产业将迎来“越用越新”的时代。

本文主要从汽车软件在线升级架构、流程、最新管理实践方面，研究汽车软件在线升级的潜在风险和发展重点。

2 国内外汽车软件在线升级管理最新进展

智能网联汽车OTA远程升级的软件数据内容不仅包含智能座舱、车联网，还扩展到汽车行车系统控制层和自动驾驶（图1）[3]。OTA远程升级将深度变革汽车产品定义、开发、验证、销售、服务全过程。当前，汽车OTA远程升级范围，已从信息娱乐系统逐渐扩展至制动能量回收系统、电池管理系统、智能座舱、辅助驾驶功能等领域，不同功能域的性能参数均发生变更，产品缺陷修复方式更加灵活多样[4-5]。从一定程度来看，属于汽车“再造”属性，升级后的汽车产品如何满足生产一致性管理要求，如何进行汽车安全影响评估，如何界定消除汽车产品缺陷和性能改进的边界等，均对传统汽车静态固化的管理模式带来新的挑战。

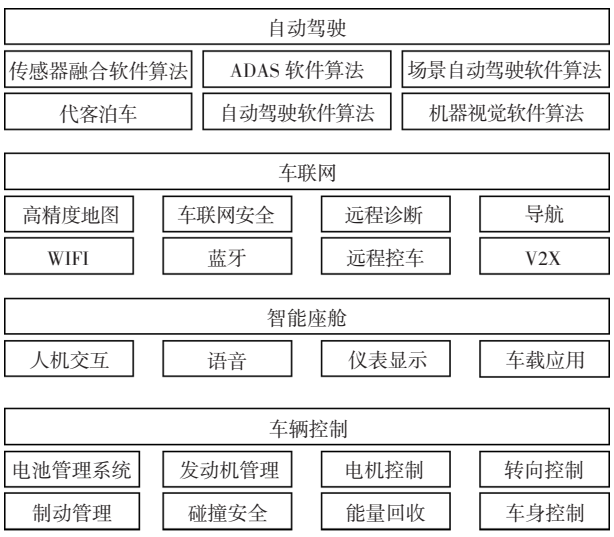

图1 智能网联汽车应用软件[3]

国外以联合国和日本为代表，已出台具体法规要求对汽车OTA进行管理。目前，联合国世界车辆法规协调论坛发布3项涉及智能网联汽车信息安全的重要法规UN Regulation No.155、UN Regulation No.156、UN Regulation No.157，其中UN Regulation No.155和UN Regulation No. 156法规要求销售到58协约国的汽车制造企业必须获得政府监管部门的汽车信息安全管理认证和汽车软件升级管理体系认证，汽车软件升级管理体系认证要求汽车制造企业从软件更新过程，软件更新的安全性要求、已安装软件的标识等方面建立软件升级管理体系，政府监管部门会保持认证结果不定期复审。

日本对于汽车OTA远程升级管理处于领先位置，为促进自动驾驶产业的快速落地，先后出台或修订了《道路车辆运输法》《车辆特定改造许可制度》《道路运输车辆保安基准》《审查事务规程》等文件，从上位法、管理制度、法规要求等维度，对汽车OTA在线升级申请、审查、验证、许可等关键环节构建了较为完善的管理体系[6-8]。日本将汽车OTA远程升级作为汽车制造企业对已销售车型改装应用的一种技术方式，针对具备OTA远程升级改装的汽车制造企业，其需要建立软件升级和网络安全等制度管理体系，并且国家监管部门不定期审查已建立的软件升级和网络安全等制度管理体系的执行状态，此外汽车制造企业在OTA升级前需向日本国土交通部提交汽车软件升级申请材料，经国土交通部批准后方可执行汽车OTA远程升级。

此外，国际相关标准组织为减少汽车OTA远程升级质量问题，先后发布了SAE J3061（2016）、Uptane IEEE-ISTO 6100.1.0.0（2018）、ISO/SAE 21434（2021）等行业标准，从信息安全工程体系建设、安全测试技术和汽车安全防护框架等方面提供标准化OTA远程升级产品解决方案。另外，国际标准化组织为支撑UN Regulation No. 156 - Software update and software update management system法规在企业体系的实施，ISO 24089《道路车辆软件升级工程》已正式立项，旨在提出车载软件更新所涉及的功能安全和信息安全方面的要求，明确软件升级管理系统、车辆、电子电气架构和软件包的设计开发流程，支撑相关法规的实施。综合来看，国际上已出台的法规和标准从OTA远程升级前对车况的正确感知，到OTA远程升级结果完整性、功能性验证、升级内容防篡改机制，再到升级失败后车辆自动还原到可用状态、更新内容和过程可追溯，以及完备的安全监控和审计机制、告知车主更新

内容及保护措施等方面，对汽车OTA远程升级安全均强化了管理要求。

我国行业主管部门高度重视汽车OTA远程升级管理。总体来看，我国以备案方式开展汽车OTA管理，对汽车OTA升级进行规范管理。具体来看，从新车准入和在用车管理角度先后出台了《市场监管总局办公厅关于进一步加强汽车远程升级（OTA）技术召回监管的通知》《关于开展汽车软件在线升级备案的通知》等管理政策。其中，《市场监管总局办公厅关于进一步加强汽车远程升级（OTA）技术召回监管的通知》提出对OTA远程升级追溯、对OTA远程升级技术服务活动和OTA远程升级召回备案进行管理。《关于开展汽车软件在线升级备案的通知》对企业远程升级过程进行管理，主要体现在OTA远程升级过程管理、安全应急响应、升级版本、信息记录等。此外，工信部发布的《关于加强智能网联汽车生产企业及产品准入管理的意见》也提到准入测试应开展OTA远程升级安全测试和升级过程测试。《关于开展汽车数据安全、网络安全等自查工作的通知》提出要对OTA远程升级安全和网络安全状态进行评估检验。市场监管总局等部委联合发布的《关于试行汽车安全沙盒监管制度的通告》，提出对使用远程升级等新功能模式的车辆开展深度测试，更早发现质量安全问题，保障安全底线。

从标准法规来看，我国在2022年6月已发布了强制性国家标准《汽车软件升级通用技术要求》（征求意见稿），该标准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、说明书要求等，从技术法规角度进一步完善汽车OTA远程升级管理要求。

3　汽车软件在线升级存在的主要安全问题

汽车OTA远程升级系统架构主要由远程升级云服务器端、云端数据传输和汽车产品应用终端组成[9-10]。远程升级云服务器端和汽车产品应用终端采用一对多的方式，部署在汽车制造企业数据中心的私有云服务平台为远程升级云服务器端，利用公有云的内容分发技术（Content Delivery Network, CDN）实现位于不同地区的不同汽车同时更新[11]。远程升级系统架构见图2。

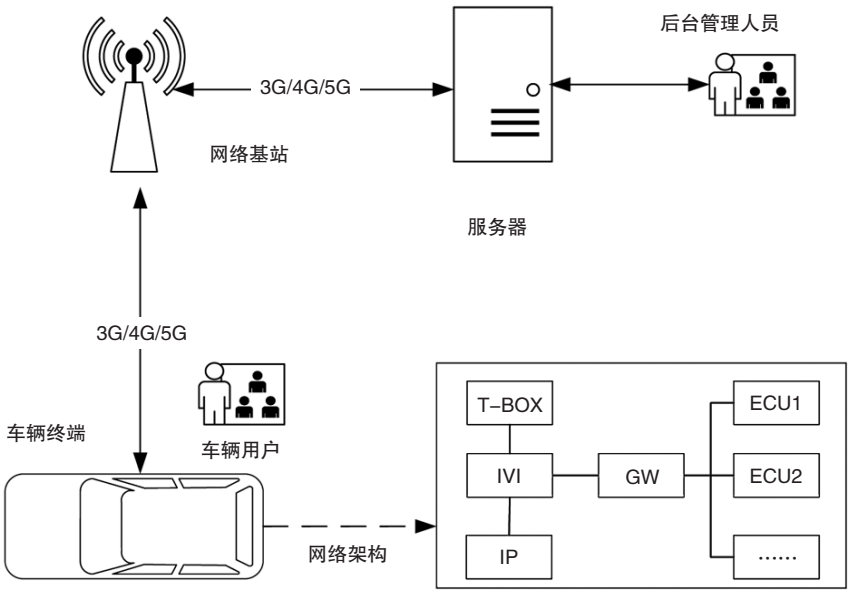

图2　汽车OTA系统架构[11]

通过功能测试的汽车软件远程升级数据包，在OTA远程升级云服务器完成刷写验证流程，经远程升级云服务器工程设计人员在远程升级云服务器部署车端控制器的软件数据包，建立远程升级任务，利用车载远程升级主控单元执行端与远程升级服务器的无线通信链路，匹配和下载远程升级软件数据文件，实现待升级车载控制单元的远程软件数据下载、软件数据安装过程[12-14]，OTA远程升级主要流程见图3。

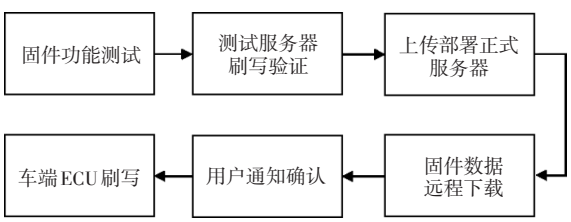

图3　汽车OTA升级流程

从汽车OTA远程升级的系统框架分析，在远程升级的每个流程中均存在安全风险，常见的安全风险包

含远程在线升级云服务器风险、软件数据传输风险、远程在线升级服务器与车载远程在线升级控制单元之间的通讯协议风险、车内通信网络风险、软件在线升级数据包被篡改风险[15-16]。据统计，利用OTA远程升级端口的攻击方式已成为汽车产品当前面临的最高风险，如果出现安全事件，其影响范围包含汽车运行状态、车主隐私数据泄露、车主财务损失，更为严重的安全事件会涉及到车主的人身伤亡[17]。如何在软件快速迭代进程中确保软件质量和升级成功率、如何准确评估识别复杂电子电器系统升级必要性和升级软件准确性、如何确保软件在线升级合规等关键问题，均对程序可靠性、数据完整性、系统安全性和传输连通性方面提出了更高要求。

从用户使用来看，OTA远程升级可涉及产品技术参数和控制策略调整，安全风险有待评估，一定程度上影响用车安全；部分OTA远程升级并未明确告知车主远程在线升级的理由，以及远程在线升级的内容和升级后对汽车的影响，侵犯用户合法权益；OTA远程升级过程中还可获取智能网联汽车位置信息和汽车使用数据等个人隐私数据，面临着数据安全风险及车主隐私数据保护问题。

从汽车产品来看，频繁的OTA远程升级导致先期投发车型配置与不断自动升级的软件系统不相匹配，车载控制单元的硬件能力不足，软件系统运行速度慢，将影响产品正常运行，不利于可持续发展。

从产业生态来看，智能网联汽车OTA远程升级产品的使用条件和环境十分复杂，OTA远程升级升级生态系统涉及实体包括智能网联汽车、OTA远程升级云服务器、手机、汽车制造商、备件OEM、软件经销商、车主、汽车服务中心、保险公司、执法人员等，明确各方权责利弊是一项系统工程，需要各方持续探索行业解决方案。

4 对策与建议

总体来看，OTA远程升级的发展与汽车的智能化和网联化推进息息相关，未来在自动驾驶域、底盘域及动力域的OTA远程升级将不断增多，需要政府机构、整车企业、关键零部件供应商与IT、生产制造、市场和相关测试机构协同配合[18]，打造完整的OTA远程升级生态系统，共同保障智能网联汽车产业高质量发展。

4.1 完善OTA远程升级管理体系

OTA远程升级涉及后市场车辆的再设计更新过程。建议在现有备案管理基础上，进一步建立汽车OTA远程升级技术审查和测试机制，具体建设如下。

（1）开展升级包一致性比对分析，发现对升级包内容不一致的情况，开展功能安全、网络安全和数据安全测试。

（2）对企业因OTA远程升级后产生重大安全问题或对车辆一致性产生较大影响的，建议对企业相关能力开展核实，并对该类企业后续涉及安全或重要参数变更等OTA远程升级活动，重点开展升级过程及升级后的测试验证，确保产品生产一致性[19]。

（3）基于缺陷线索收集，对于OTA远程升级后投诉较多车型，开展OTA远程升级后的车辆的功能抽检验证，包括不限于升级日志读取以及功能测试。

4.2 建立健全OTA远程升级管理标准体系

在已有OTA远程升级技术要求基础上，可参考传统数据安全和网络安全体系架构，梳理目前已有的智能网联汽车数据安全和网络安全相关标准，以标准属性作为主要分类维度的标准体系框架（图4），从规范类、技术类、管理类3个方面建设面向汽车OTA远程升级监管流程的标准体系，坚持标准体系适度超前，逐步起到发展引领作用。其中，规范类标准包括基本术语、缺陷判定、OTA远程升级分类等标准，基于OTA远程升级的行业术语、OTA远程升级的缺陷定义以及OTA远程升级的分类标准等方面，规范OTA远程升级的行业术语和行业流程标准，推进OTA远程升级管理过程专业化。技术类标准包含安全测试（测试用例、测试流程、测试机构资质要求、测试场地等环境要求）、风险评估等标准，并将标准内容划分为终端、网络、业务场景等测试、评估对象。针对OTA远程升级过程中的多场景、多产品的安全测试方法、测试流程以及漏洞等级判定方法等测试技术方面进行系统化、标准化的管理，为企业开展检测业务或第三方实验室检测单位提供基本标准依据。管理类标准则包括漏洞库标准规范、应急处置和追溯管理（包括OTA升级管理标准等），从OTA远程升级产品漏洞库的建设管理、企业应急处理管理机制和质量缺陷可追溯的开发流程开展标准化建设，让汽车制造企业将重点聚焦在技术研发和产品设计上，提高企业核心竞争力。其次，现行法规（如UN Regulation No.156、ISO 24089标准）均是从整车角度出发，部件系统供应商需要完全适应下游主机厂要求，沟通成本和后期维护成本大大增加。建议未来将主机厂和零部件厂商资源进行有效整合，构建符合行业发展需求、涵盖云-管-端[20-21]全要素的OTA远程升级标准体系。最后，围绕标准中难

点、热点问题，协调各标委会和相关科研机构组织力量开展OTA远程升级标准化的研究工作，针对不同标委会所覆盖的相关技术标准进行归口管理，指导和支撑汽车OTA远程升级监管工作。

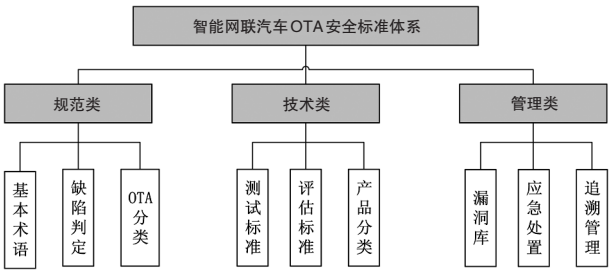

图4　智能网联汽车OTA安全监管标准体系框架

4.3　完善汽车OTA远程升级安全测试体系

首先，基于网络安全和数据安全风险评估理论基础、汽车网络安全和数据安全领域现有的威胁分析以及实践经验，结合汽车本身的复杂特性，建立以资产为核心的汽车OTA远程升级安全风险评估模型，包括资产识别、脆弱性分析，威胁分析、影响评估、攻击路径分析、攻击可行性分析、风险值判断等方面。

其次，汽车OTA远程升级系统本身是完整的生态系统，检测方向包括汽车远程升级车载终端安全检测、车载终端-远程升级云服务器平台-移动设备App间通信，以及与远程升级业务交互安全检测、移动设备App安全检测以及远程升级云服务器云平台安全检测，为此定期针对以上5部分内容进行安全检测非常必要。

再次，汽车OTA远程升级是一个复杂的系统工程，涉及到的安全包括网络安全、数据安全、功能安全等多方面，重点推动软件数据模拟仿真验证测试，网络安全和数据安全的合规检测等服务。从模拟仿真测试体系、测试评价体系以及功能安全验证体系方面制定汽车远程在线升级测试规范。

最后，梳理并汇集OTA远程升级监管技术需求，梳理共性和核心关键技术，围绕技术需求通过部际会商、设立产业基金等形式，以重点研发计划、国家自然科学基金、国际合作项目等为牵引，汇聚国内外创新资源形成合力，特别是针对智能网联汽车快速迭代发展形势下，建立常态化的关键技术协同攻关模式，有效打破壁垒，形成从基础理论-共性关键技术-集成示范应用全链条、一体化的创新群体。

4.4　强化OTA远程升级安全基础保障能力

首先，深入研究汽车产品安全风险评估/缺陷研判等关键技术，健全安全评价和缺陷研究机制，为国家监管机构监管汽车产品安全方面提供有效技术支持。整合行业资源，构建安全基线，基于大数据有效识别安全漏洞，提升安全缺陷识别能力，持续开展产品信息安全缺陷安全测试、风险评估，利用技术和检验手段分析判断缺陷，并对标准符合性问题进行调查。

其次，针对具备OTA远程升级配置的汽车产品及相关零部件系统的关键软件数据，针对其功能可靠安全方面进行检测认证，建立多层级的远程升级检测认证服务体系。

再次，由于升级车辆的控制器芯片和操作系统、零部件和车型的差异较大，由此造成了具体车型适配分散化难题，亟需构建一套统一、通用的测试验证平台和测试工具，解决软件落地中的标准化问题。进一步保障不同车型的OTA远程升级体系标准化过程的稳定性和高效性。

建议以高校、科研院所等“第三方”，建立“共研、共建、共享、共营”的技术支撑平台，服务于OTA远程升级监管，提供有效的技术保障。最后，促进汽车OTA远程升级行业构建自律规范。目前，由于时间、成本、功能、安全风险等综合因素考量，大部分主机厂将考虑直接向OTA远程升级供应商购买服务，OTA远程升级供应商通过多种方式实现软件刷写，但是由于是新兴模式和新兴技术，行业内存在OTA远程升级产品质量参差不齐等现象，建议由行业第三方机构牵头，联合主要生态要素主体，共同建立智能网联汽车OTA远程升级创新联盟，构建统一评价标准，探索行业领跑者机制，鼓励优胜劣汰，规范行业自律发展。

综上所述，汽车OTA远程升级是智能网联汽车产业的重要趋势，即将迎来大规模应用。但在OTA远程升级的每个流程中均存在安全风险，影响车辆性能、安全和用户权益，如不加以妥善管理，不利于行业可持续发展。汽车OTA远程升级需要在检测认证、一致性抽查、分级备案、数据化监管、测评技术、缺陷研判、风险评估、标准制定等方面进一步强化和健全管理体系。

参　考　文　献

[1] 武翔宇, 赵德华, 郝铁亮. 浅谈汽车OTA的现状与未来发展趋势[J]. 汽车实用技术, 2019(3): 214-216.

[2] 宋伟, 胡巧声, 唐俊安. 空中下载技术在商用车上的应用[J]. 汽车电器, 2019(12): 8-11.

[3] 万开明, 洪雷. 车载OTA技术研究[J]. 时代汽车, 2020(11): 10-11.

[4] SUBKE P, MOSHREF M, ERBER J. In-Vehicle Diagnostic

System for Prognostics and OTA Updates of Automated /Autonomous Vehicles[C]//WCX SAE World Congress Experience, 2020.

[5] FIZZA K, AULUCK N, AZIM A, et al. Faster OTA Updates in Smart Vehicles using Fog Computing[C]// the 12th IEEE/ACM International Conference. ACM, 2019.

[6] 田端祥, 段晖, 陈洁, 等. 远程升级技术在汽车智能网联系统中的运用[J]. 内燃机与配件,2022(5): 2014-216.

[7] 武智, 刘天宇, 贾先锋. 智能网联汽车OTA升级安全设计[J]. 汽车实用技术, 2022(3): 38-40.

[8] 尹超. 软件定义汽车时代车辆公告管理制度的挑战与对策[J]. 汽车工业研究, 2021(3): 26-28.

[9] 张进华. 汽车领域"监管沙盒"的国际经验及启示[EB/OL].(2022- 04- 11) [2023- 02- 27].https//baijiahao.baidu.com/s?id=1729778912273146858&wfr=spider&for=pc.

[10] 王栋梁, 汤利顺, 陈博, 等. 智能网联汽车整车OTA功能设计研究[J]. 汽车技术, 2018(10): 29-33.

[11] HAIBO Z, YAN C, KAIJIAN L, XIAOFAN H. The Mobility Management Strategies by Integrating Mobile Edge Computing and CDN in Vehicular Networks[J]. Journal of Electronics & Information Technology, 2020, 42(6): 1444-1451.

[12] 周媛媛. 车联网信息安全测试技术分析及应用[J]. 北京汽车, 2020(2): 23-27.

[13] ZHI W, TIANYU L, XIANFENG J, et al. Security design of OTA upgrade for intelligent connected vehicle[C]// Proceedings of the 2021 International Conference on Control and Intelligent Robotics, 2021: 736-739.

[14] HE K X, WANG C Y, HAN Y Y, et al. Research on cyber security Technology and Test Method of OTA for Intelligent Connected Vehicle[C]// 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). Fuzhou, China: IEEE: 2020.

[15] HALDER S, GHOSAL A, CONTI M. Secure Over-The-Air Software Updates in Connected Vehicles: A Survey[J]. Computer Networks, 2020, 178(9):107343.

[16] KIM K, KIM J S, JEONG S, et al. Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense[J]. Computers & Security, 2021, 103(4): 102150.

[17] FENG S, FENG Y, YAN X, et al. Safety assessment of highly automated driving systems in test tracks: A new framework[J]. Accident Analysis & Prevention, 2020, 144.

[18] Society of Automotive Engineers(SAE). Cybersecurity guide book for cyber physical vehicle systems: SAE J3061_202112[S/OL]. (2021-12-15)[2023-01-16]. https://www.sae.org/standards/content/j3061_202112/.

[19] UPSTREAM SECURITY. Global Automotive Cybersecurity Report 2022[EB/OL]. [2022- 01- 17].https://upstream.auto/2022report.

[20] 刘健皓. 智能网联汽车的威胁分析与发展建议[J]. 智能网联汽车, 2019(1): 79-79.

[21] NEERAJ K, RAHAT I, SUDIP M, et al. An intelligent approach for building a secure decentralized public key infrastructure in VANET[J]. Journal of Computer and System Sciences, 2015, 81(6): 1042-1058.

【作者简介】

吴胜男(1988-),女,硕士研究生,中国汽车工程研究院股份有限公司政研中心产业发展研究室主任,中级工程师,主要研究方向为智能网联汽车产业政策战略。

E-mail: wushengnan@caeri.com.cn