汽车软件在线升级关键技术及监管要求分析*

王婧璇　文海鸥　陈亚翔

（中国汽车工程研究院股份有限公司，重庆 401120）

【欢迎引用】王婧璇，文海鸥，陈亚翔. 汽车软件在线升级关键技术及监管要求分析[J]. 汽车文摘，2024(4): 19-27.

【Cite this paper】WANG J X, WEN H O, CHEN Y X. Analysis on Key Technology and Regulatory Requirement for Automotive Over the Air Update[J]. Automotive Digest (Chinese), 2024(4): 19-27.

【摘要】随着软件定义汽车时代的到来，汽车软件升级技术应用的必要性愈发突出，为了避免汽车软件在线升级中潜在的安全风险，车辆制造商需保证产品在线升级（OTA）的安全性。针对当前汽车OTA面临的挑战，从数据完整性及服务完整性2方面总结了OTA升级关键技术的发展现状，分析了现有软件升级管理法规要求，并在此基础上提出企业OTA能力建设方面的建议。

关键词：智能网联汽车；软件升级；OTA安全

中图分类号：U461.99；F426　　**文献标志码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20230196

Analysis on Key Technology and Regulatory Requirement for Automotive Over the Air Update

Wang Jingxuan, Wen Haiou, Chen Yaxiang

（China Automotive Engineering Research Institute Co., Ltd., Chongqing 404100）

【Abstract】With the advent of the software-defined automobile era, the necessity of the application of automobile software update technology becomes more and more prominent. To avoid potential security risks, vehicle manufacturer needs to ensure OTA security of the product. In view of the current challenges faced by OTA, the development status of key technologies for OTA update is summarized from the aspects of data integrity and service integrity. The requirements of existing software update management laws and regulations are analyzed, and the corresponding OTA capacity building suggestions are put forward to vehicle manufacturers.

Key words: Intelligent and connected vehicles, Software update, OTA security

0　引言

随着车辆高级功能的配置，智能网联汽车中软件数量日益增加，其代码量高达百万行[1-5]。软件漏洞和错误可能会带来系统崩溃、功能失效、信息泄露和安全漏洞等风险，影响驾驶体验甚至危害用户生命财产安全。同时，车辆对软件连接、控制和协调依赖程度增加，也加剧了对软件修复和漏洞修补的需求。因此，车辆制造商需要建立一个安全的软件更新机制，以便修复漏洞并应对不断变化的环境威胁。在传统的封闭系统车辆中，车辆故障是由硬件故障或软件安装中的错误造成的，对应的解决方案是召回问题车辆并进行修复，而该方式所需时间过长且为用户带来极大不便[6]。由于智能车辆具有网联无线网联通信功能，所以车辆制造商开始通过无线方式对汽车软件实现远程空中下载（Over The Air, OTA）升级，该方法无需物理召回过程，可向用户提供最方便、最快速的软件升级服务[7-8]。

OTA软件更新具有以下优势：（1）车辆可以在运行状态中及时对软件进行升级，大大缩短了软件升级的时间；（2）通过OTA软件升级可以降低车辆保修成本和物理召回成本；（3）通过实时升级，可以及时解决安全问题，提高汽车的安全性能，降低被攻击的风险；（4）通过OTA升级，用户可以享受个性化定制服务，如对音乐、导航等应用软件的更新[9-11]。2022年，全球支持OTA升级的车辆出货量将接近2.03亿辆[12]。因此，

*基金项目：汽车电子软件代码质量控制技术研究与工具开发（CSTB2022TIAD-STX0001）。

OTA升级具有巨大潜力，对汽车市场的未来发展具有重要的意义。

车辆制造商通过蜂窝网络实现智能网联车辆的OTA升级。同时，网络连接也给车辆带来了各种安全威胁和隐私挑战。有研究人员通过多种方式（车载诊断端口、Wi-Fi、蓝牙等）尝试对车载电子控制单元（Electronic Control Unit, ECU）进行攻击，结果发现ECU会被成功攻击，而网络攻击者可以通过被入侵的ECU向车载网络注入数据包，以控制车辆[13-16]。联网车辆面临被远程网络攻击的风险，使得建立端到端的OTA升级安全连接成为一个至关重要的问题，而由于复杂、多样的攻击手段以及不够成熟的技术，导致车辆在OTA过程中保持安全的连接十分具有挑战性。此外，OTA升级面临的另一个挑战是升级时保障车辆的安全及准确访问。由于每次OTA升级的对象满足特定限制，因此需限制云端仅能访问并仅向目标车辆推送对应升级包。为了避免OTA升级过程中由于车辆的网络可用性故障导致的升级中断或失败等问题，原始设备制造商（Original Equipment Manufacturer, OEM）和网络运营商需要确保升级过程中可有效利用无线电频谱，以最大限度地提高升级成功率，同时最小化车辆升级对其他网络用户的影响。因此，对于网络运营商而言，联网车辆的OTA升级成为一个重要的调度问题[17]。

为了解决OTA升级可能存在的问题，可采取多种措施，如通过完整性验证、身份验证和密钥管理等措施，防止车辆被远程攻击以及数据被篡改或窃取。为确保OTA升级过程的高效性和可靠性，OEM和网络运营商可以选择使用强大可靠的通信协议，建立云端与车辆之间的高效通信。此外，需要设计健壮的软件程序，满足升级中断时能够自动续传、自动检测和进行失败重启的需求[18-20]。为了最大程度地减少OTA升级对蜂窝网络的压力，同时保障升级包传输的完整性和稳定性，需要对OTA升级的程序和过程进行优化，尽可能降低升级过程对带宽和网络资源的消耗。同时，应优化网络连接和调度策略，以确保软件包下载过程中网络可用性，并确保对所有其他网络用户的影响最小，从而最大程度地提高更新成功率。

综上，智能网联汽车的软件升级趋势为OTA升级，为确保其实施的可靠性，需保证云端将真实完整的升级包安全传输至车端，且升级包的安装过程需不受攻击。除了技术要求之外，企业OTA体系也需满足监管要求。因此，本文主要总结了OTA升级的要求及其关键技术，并讨论了OTA升级面临的挑战，还研究了国内外现有OTA升级监管要求，并基于此对企业提出关于OTA升级能力的建设建议。

1 OTA升级安全关键技术

1.1 OTA升级流程

汽车OTA升级架构主要包括：OTA云服务器、无线网络传输端以及车端，如图1所示。其中，云端的升级包由软件供应商上传，车辆制造商负责升级任务的发布。车端通过无线网络从云端获取OTA升级任务及升级包，并向云端上报升级结果。

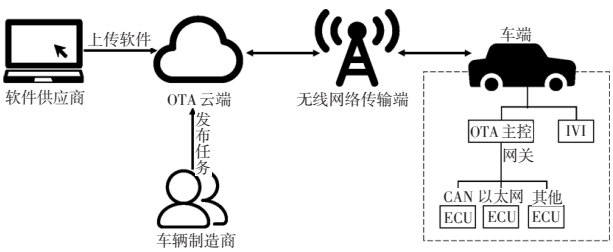

图1 OTA系统架构

OTA具体升级流程主要包括以下环节（图2）。

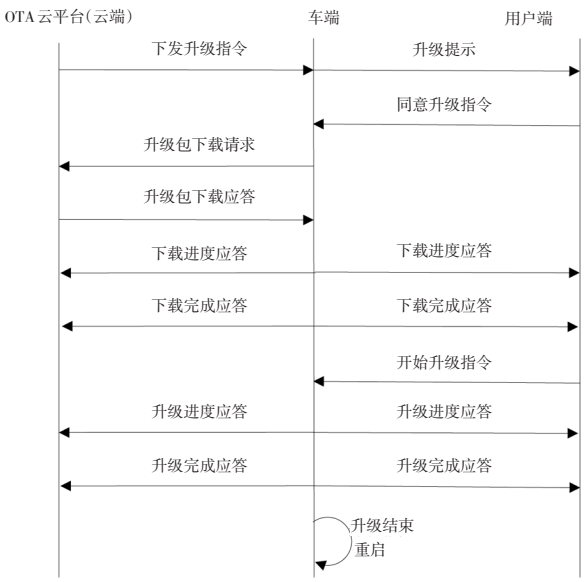

图2 OTA升级流程

（1）软件供应商向车辆制造商交付通过了功能测试的升级包，上传至OTA云平台，并完成升级包验证流程。

（2）车辆制造商通过OTA云平台向目标车辆发布升级任务。

（3）车辆制造商通过实体信件、电子邮件、社交媒体和车载通知等方式通知车辆用户升级信息，用户可选择拒绝或同意软件更新。若选择“拒绝”，则不会进行升级，若选择“同意”，车辆检查自身状态是否满足车

辆制造商规定的升级前置条件，满足则进行下一步。

（4）车辆向OTA平台请求软件升级，接收访问OTA平台中软件升级包的路径信息。

（5）车辆根据软件升级包的路径访问OTA平台的升级包，并进行升级包下载，下载过程中OTA平台或用户端可查看下载进度，直至下载完成。若下载中断，则在满足条件后继续下载。

（6）车辆端对下载的升级包进行验证后执行安装，OTA升级完成后，用户可接收升级结果告知。若升级失败，软件将回滚至上一可用版本；若升级成功，可进行后期验证，以确认已成功完成目标ECU的软件升级，并且本次升级未影响任何其他ECU或车辆功能。

1.2 OTA升级的安全要求

为保证完整稳定的OTA服务，需保证其数据完整性和服务完整性。数据完整性要求数据未经许可不被授权访问和篡改[21-22]。研究表明被篡改过的数据包可能会使车辆被远程攻击，威胁车辆及用户的安全[23]。服务完整性要求软件升级全过程（下载、安装）中未受恶意软件或其他恶意修改的干扰（DOS攻击、选择性转发、节点捕获等）[24-25]。从开始下载软件包到执行安装，服务完整性均可能会受到破坏。

为避免OTA服务的数据完整性和服务完整性被破坏，应在云端及车端均验证升级包的数据完整性，阻止对升级包未经授权的访问及篡改（新增，删减或修改）。此外，需构建OTA云平台与车辆间升级包分发的安全传输通道，并在各节点查验服务的完整性。因此，OTA升级的安全要求应包括：

（1）OTA升级任务发布后，需验证目标车辆的升级包访问权限。

（2）应确保升级包由OTA云平台下发至目标车辆的传输安全性，安全传输通道可最大程度地确保在传输过程中数据未经篡改，或具备数据修改点检测能力。

（3）在车辆从OTA云平台下载升级包完成且未开始执行安装之前，需将升级包安全储存，以保证待安装软件包的真实性及完整性不受破坏。

（4）为避免安装错误升级包带来的问题，升级包上传至OTA云平台后需通过平台的真实性、完整性验证后才可下发，车辆下载升级包后，需在执行安装前再次校验升级包的完整性。

（5）应保证OTA云平台的网络安全水平，以发现其漏洞并保证其免受网络攻击，保证上传至平台后升级包的数据完整性以及升级指令下发后OTA服务的完整性不受破坏。

1.3 OTA升级关键技术现状

1.3.1 保证数据完整性的技术

目前，OTA升级中的数据完整性保证主要通过哈希函数实现，数据真实性保证主要通过密钥加密技术实现。

1.3.1.1 哈希函数

哈希函数可以将任意长度的数据处理得到一个唯一的、具有固定长度的哈希值，常见的哈希函数有MD5、SHA-1、SHA-256等。Checkoway等[26]在升级中将二进制的固件升级包与哈希值打包传输，通过对哈希值的验证确保了固件数据的完整性，该研究的不足是验证数据占据内存过大。Nilsson等[27]提出了一种汽车OTA协议，通过该协议可以安全地进行固件升级。该协议采用了哈希链和预共享加密密钥技术来防止数据被窃听、拦截和篡改攻击。首先将升级包的二进制文件分成若干个数据片段，后通过反向散列为每个片段创建了一个哈希链，在OTA云平台将哈希链的每个片段传输到车辆端之前，使用预共享加密密钥对哈希链加密以保证数据的安全性。Byeon等[28]的研究提出一种使用哈希函数验证汽车ECU数据完整性的系统。该系统通过哈希函数对传输的数据进行验证，确保数据在传输和存储过程中的完整性，从而减少ECU数据被攻击和篡改的风险。服务器通过哈希函数对传输数据进行校验，若完整性无误则将哈希值和ECU元数据分别存储在区块链和链下分布式存储中。通过验证系统，用户可以对ECU数据的攻击和篡改进行验证。

1.3.1.2 密钥加密

（1）对称密钥加密

对称密钥加密是一种使用同一密钥进行加密和解密的技术。这种加密方式速度快，适合加密大量数据。常见的对称加密算法有DES、3DES、AES等。

Karim等[29]提出一种用于汽车软件无线升级的车辆制造商与车辆间的后台加密通信通道。该研究中，服务器只在用户最初请求的加密通道上经过用户批准后收集数据。该通道采用对称密钥加密技术，通过使用共同的密钥，双方可以实现安全通信，防止消息被第三方拦截和阅读。Mahmud等[30]提出了一种智能车辆安全软件升级技术。该技术的先决条件是，车辆制造商、软件供应商和车辆之间共享同一组密钥。每次软件升级之前，软件供应商和车辆会共享对称密

钥。此后，软件供应商将共享的对称密钥加密后的软件发送到车辆。该研究确保系统安全性和完整性的另一方式是随机时间间隔内向车辆发送多个软件副本，车辆在收到至少两个加密软件副本后才可进行解密和安装，以确保只有经过授权并已验证的软件得到安装，从而防止未经授权或恶意软件的入侵。

（2）对称及非对称结合密钥加密

Steger等[31]的研究中提出了用于安全高效的汽车OTA软件升级的SecUp框架，该框架通过使用对称和非对称密钥结合的技术来确保所有通信的保密性和完整性，并通过使用NFC智能卡和PIN码对设备进行身份验证来防止未经授权的个体进行操作。同时，使用组播通信技术可以在短时间内将多辆汽车的软件进行更新，从而提高了软件更新的效率。升级过程中，服务器生成会话密钥，并使用汽车公钥加密的数据包发送给每辆汽车，完成升级包的传输，由车辆完成对应升级包的安装。该框架的设计具有前瞻性和高效性，能够保证连接车辆的软件升级过程安全可靠。

（3）隐写术及密码学结合加密

隐写术和密码学结合可以提高通信的安全性和隐私保护有效性。隐写术可以隐藏信息，使之不易被探测和发现，避免被攻击者破解。密码学则提供了各种加密算法和安全协议，使信息在传输过程中得到保护，只有授权的用户才能访问和解密信息。

Mayilsamy等[32]提出一种集成了隐写和密码学的方法，用于验证数据完整性，并使用加密技术来保护云中的数据，以保证OTA升级安全进行。同时，密钥在控制环境中经过密钥交换程序后存储在受信任的平台模块中，并使用IEEE 802.11s网状网络作为通信媒介进行OTA升级的安全传输。

（4）硬件安全模块加密

基于硬件安全模块的密钥管理机制主要依靠硬件安全协议对密钥全生命周期执行操作与管理，包括密钥的生成、存储以及分发等。同时，该机制还能对外提供多种密钥服务，以满足不同应用场景下的安全需求。

有学者设计了可执行的FOTA系统，该系统中的密钥管理机制通过硬件安全模块实现升级中的密钥服务[18]。该模块的应用从物理层面保证了密钥的不可泄露，提高了系统对汽车客户端的安全性和隐私保护。

Petri及其团队[33]提出了一种基于硬件安全模块的OTA升级技术，该技术通过网关从OTA服务器下载升级包，并用预存在硬件安全模块中的哈希算法验证该升级包，若验证无误，则将升级包传输到目标ECU进行安装。这种技术的主要优点是硬件安全模块支持多种加密算法对升级包的加密和验证，从而防止分发给车辆的升级包被篡改或恶意注入。

1.3.2　保证服务完整性的技术

区块链是一种基于分布式网络节点和密码学安全技术的去中心化数据管理技术，具有强大的安全性、鲁棒性和可扩展性。其数据层采用了带有公钥的数字签名验证数据的真实性，同时通过哈希函数和数据块哈希链验证数据的完整性。

Steger等[34]在一项工作中引入了基于区块链（Blockchain, BC）的架构来解决汽车OTA升级中的数据安全问题。在该架构中的实体有OEM、管理系统、汽车、OTA服务器，其中各个实体分别作为端点与其他实体组成集群，各集群间通过覆盖网络相互连接，端头可以直接通信，系统不设中心节点，从而实现去中心化管理。软件升级任务下发前，管理系统向云服务器发送存储请求，请求通过验证后云服务器会向管理系统发送包含服务器签名及软件包上传所需信息的数据。当软件包上传至服务器后，管理系统会创建一条升级任务并写入区块链模块并使用OEM的密钥加密升级任务信息后广播给车辆。作者通过验证表明该体系结构具有优良的性能。

Dhakal等[35]提出了一种使用区块链的物联网设备固件升级模型，其中包含固件制造商、升级服务器、升级管理器和物联网设备4个主要部分。整个升级的流程为：固件制造商开发完成软件包后通过区块链对其元数据进行管理，并通过升级服务器下发升级任务。升级管理器将升级包的元数据从区块链中提取，分发到待升级的物联网设备后，对应设备接收软件包并启动升级任务后执行升级。研究表明这种使用区块链的物联网设备固件升级模型可以保障升级过程的安全性和可靠性，并且提高了升级的效率。

具有安全、分散式、灵活和可扩展特性的Uptane架构目前已被应用于汽车软件的安全升级。Uptane使用了多个TUF（The Update Framework）库，具有多个实体和一个管理系统，以支持不同实现之间的交互。Uptane架构采用多种措施来保护软件升级安全，包括额外的存储区域、元数据广播、车辆版本清单和时间服务器等机制[36]。软件的元数据由车辆主控广播到次ECU，以确保每个ECU具有相同的元数据。清单签名是使用OEM提供的对称密钥进行签名的，时间服务器可确保所有ECU的时间同步，从而确保车辆软件升级服务的完整性。

为解决大规模OTA软件升级对蜂窝网络带来的挑战，Amrita及其团队[37]提出一种OTA升级的新技术STRIDE。STRIDE可扩展到车辆中大量并发软件升级，并基于具有密文策略属性的加密确保端到端的安全性。为了实现更新包快速、可靠分发，该团队还开发了一种服务于动态数据流的软件更新调度算法，通过将蜂窝接入点的时隙动态分配给车辆，以实现最佳吞吐量。该研究通过仿真实验证明了所提出技术的适用性，结果表明该技术在现实场景下是可实现的。

目前，基于计算轻量级的对称密钥及哈希函数的OTA升级技术被广泛应用，区块链技术正在成为安全OTA升级的有效途径，而其高资源消耗的问题是制约其发展的重要原因，亟待进一步研究。具有分散式、灵活和可扩展特性的新架构已逐渐得到部分应用，未来有潜力成为OTA升级系统的重要实现方式。此外，实现从OTA云端到车端的高效、安全软件分发仍是一个需要深入研究的关键方向，还应重点关注OTA升级中的数据隐私保护策略及技术。总之，为实现充分安全、稳定、可靠的OTA升级，行业仍需攻克很多技术难题。

2 OTA标准法规分析

2.1 国外标准法规

2.1.1 UN R156

联合国欧洲经济委员会（UNECE）世界车辆法规协调论坛工作组（WP 29）于2020年6月发布法规《UN R156关于就软件更新与软件更新管理系统批准车辆的统一规定》，该法规适用于M类、N类、O类、R类、S类及T类车辆[38]。UN R156的要求分为软件升级管理体系（Software Upgrade Management System, SUMS）要求及车型认证（Vehicle Type Approval, VTA）要求两部分，如图3所示。

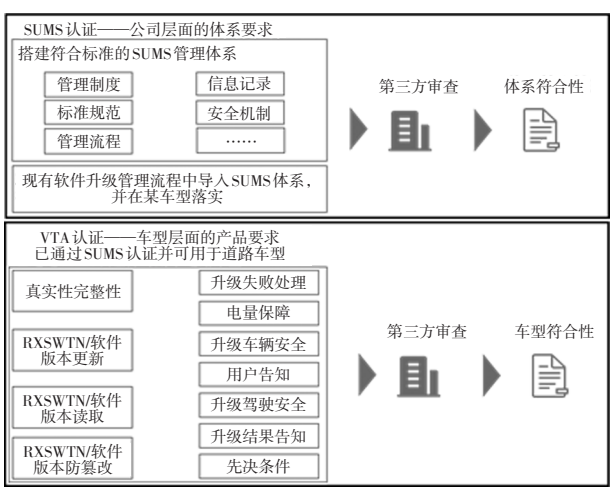

图3 UN R156认证要求

2.1.1.1 SUMS体系要求

SUMS体系是针对公司层面的体系要求，规定了过程要求、信息记录要求、安全相关要求、在线升级附加要求。

（1）过程要求：车辆制造商需确保与法规有关的信息得以记录和保留、所有软件版本信息需唯一可识别、可识别目标车辆、向监管部门提供软件识别码登记册及目标车辆配置文件。此外，还需评估升级系统与其他系统的相关性、与车辆配置的兼容性、升级对型式认证系统/功能/参数的影响以及对安全相关功能的影响。同时，升级需告知车辆用户。对于具有软件识别码（RX SoftWare Identification Number，RXSWIN）的车型，车辆制造商要可访问及更新其信息并且可验证型式批准系统组件上的软件版本信息与RXSWIN信息一致。

（2）信息记录要求：车辆制造商应记录和存储的关于软件升级的详细信息，包括用于软件升级流程和相关标准文件、相关型式认证系统配置的文件、对于每个RXSWIN的可审计的登记册、升级目标车辆的配置文件以及软件升级文档（应包含的信息有升级目的、可能影响的系统或功能、是否影响型式认证、升级先决条件等）。

（3）安全相关要求：车辆制造商应提供证明来确保软件升级的安全性，包括证明升级前，升级过程中受到保护的流程，以及验证车辆所用软件的软件功能和代码是合适的。

（4）在线升级附加要求：车辆制造商应演示OTA升级流程和程序，以确保升级不会影响到车辆安全，并需演示需特定或复杂操作的OTA升级过程。

2.1.1.2 VTA认证要求

车型认证要求是针对车型层面的产品要求，包括软件升级要求及在线升级附加要求。

（1）软件升级要求：软件升级包的真实性和完整性须受到保护。RXSWIN/软件版本须可通过标准接口读取、可更新并满足防篡改要求。

（2）在线升级附加要求：保证升级失败后系统可恢复到上一版本或车辆置于安全状态；满足升级电量条件的前提才会进行升级；升级前车辆状态满足先决条件才会执行升级；用户可获取相关升级信息及升级结果；升级不可对车辆安全及驾驶安全造成影响。

车型认证的流程包括以下4个步骤：

（1）车辆制造商向国家审批机构申请VTA，并提

交有关车辆的技术规格和相关文件。

（2）由认证机构/技术服务机构进行车辆测试，判断车辆是否符合UN R156法规要求。

（3）国家审批机构根据测试报告对车辆进行审批，以确定车辆是否符合UN R156法规要求。

（4）当车辆通过UN R156法规要求的所有测试，国家审批机构向车辆制造商颁发VTA证书。

2.1.2 ISO 24089

国际标准化组织道路车辆委员会软件升级工作组（ISO/TC 22/SC 32/WG 12）于2019年组织了ISO-24089《道路车辆 软件升级工程》标准的编制工作，标准预计2024年发布。标准适用于所有车辆软件升级工程的相关组织和供应商，而不仅限于OEM。标准所描述的软件升级方法包括有线升级、OTA升级以及硬件更换[39]。在实际应用中，组织和供应商可以根据需要对这些方法进行选择和组合，以满足特定的软件升级需求。

ISO 24089的整体框架如图4所示。标准的第4章、第5章分别从组织及项目层面对软件升级工程提出了相应的要求。组织层面的要求旨在于确保参与软件升级工程的组织能够高效管理项目，并在项目过程中进行适当地规划和监控，以确保软件升级能够按时完成并达到预期的目标和质量要求。同时，也要求组织之间合作和信息共享，以加强整个软件升级工程的有效性和效率。项目层面的软件升级要求主要覆盖了制定及实施软件升级项目的计划、管理并存储相关资料、提供裁剪行为的适用性原理并确保基础架构与车辆系统的互操作性。第6章、第7章分别提出了基础架构及车辆/车辆系统层面的功能要求。大致包括风险管理、车辆配置信息管理、软件升级活动信息管理及升级包管理。第8章、第9章分别规定了升级包装配发布及软件升级活动的相应流程。在执行软件升级操作之前，需要对获取用户同意；在软件升级期间，需要对软件升级过程进行记录和跟踪；在软件升级完成之后还需要对升级结果进行评估，并记录相关的证据以供审核和验证。

2.2 国内标准及要求

工业和信息化部装备工业发展中心发布的《关于开展汽车软件在线升级备案的通知》于2022年4月15日起正式实施[40]。对于汽车企业而言，备案要求企业加强技术能力，做好相关管理和控制，确保在线升级流程的安全性和稳定性，同时保障用户的隐私权和权益。备案内容主要包括企业管理能力、车型及功能以及具体升级活动3个方面。首先，企业需要证明具备OTA体系管理能力，包括在线升级的设计、开发、测试、验证和发布等环节的管理。其次，汽车企业需要明确车型和功能范围，识别能够进行OTA升级的功能和控制器，并且要评估升级对车辆安全、能效、环保、防盗等方面的影响。最后，企业需要提供具体升级活动的相关报告，确保升级活动的安全性和稳定性。

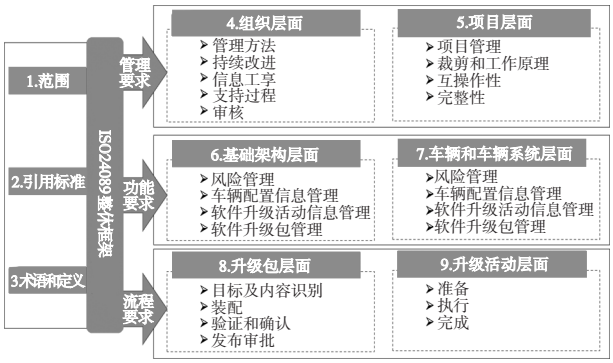

图4 ISO24089内容框架

标准方面，汽标委智能网联汽车分标委制定了《汽车软件升级通用技术要求》，该标准预计2024年发布[41]。该标准的内容参考了UN R156法规，主体要求包括软件升级管理体系要求和车辆要求，并在此基础上补充了车辆试验方法。《汽车软件升级通用技术要求》中软件升级管理体系要求包括一般要求、过程要求、信息记录要求、安全相关要求及在线升级附加要求。与UN R156法规要求相比，该标准明确指出了车辆制造商应具备软件升级管理体系，规定了信息存储的时限至少至车型停产后10年，并要求企业具备对于软件升级相关突发事件的应急处理能力。在车辆要求上，与UN R156法规要求相比，《汽车软件升级通用技术要求》中增加了用户确认以及车门防锁止两项要求。

对于国外主要OTA标准法规的分析可知，UN R156为车辆制造商建立汽车软件管理体系和进行具有软件升级功能的车型开发提供了指导；ISO24089则在工程开发层面上对企业OTA能力提出要求并给出示例。针对我国OTA监管现状，目前多部委监管的侧重点不同，备案的监管重点集中在升级过程的合规性及升级结果的符合性，而国标集中在系统升级策略的合理性。未来OTA升级标准法规体系将会向更加全面的方向发展，覆盖OTA产品级、系统级、部件级等多维度，如规范OTA云平台技术标准、增加用户体验相关标准、完善供应商管控规范等。软件升级相关标准的制定及实施，将对车辆制造商提出一定的要求，这有利于

确保汽车软件升级安全及其整体性能和操作稳定性，更有助于提高市场规范化程度，保障消费者权益。

3 企业OTA能力建设建议

OTA升级技术已经成为现代汽车技术发展的趋势之一，对于车辆制造商而言，OTA升级技术的应用可帮助企业快速响应市场变化和技术变革，提高汽车的质量和性能，为用户提供更好的用户体验。但同时，OTA升级技术也面临着安全性和隐私性等方面的挑战，需要企业加强技术研发，加强安全和隐私保护，落实法律法规和监管要求。

（1）软件升级管理体系建设方面：企业应建立、健全软件升级管理体系，覆盖软件升级全生命周期的管理制度及规范流程，并关注软件升级相关活动的策略及实施细节的信息记录与存储。企业还应设置相应的安全策略保证升级的可靠进行，并对软件升级进行全面性评估，评估重点主要包括其对型式认证相关参数/系统或车辆安全相关功能的影响，以及待升级系统/功能与其他车辆系统/功能的相关性和与车辆现有配置的兼容性等。为确保对软件升级突发事件得到有效处理，企业应专门建立针对软件升级事件的风险控制制度及应急响应流程。此外，软件升级管理体系合规有效的关键点是应用，因此企业在具体车型开发中需切实应用管理体系，实现制度的落地实施。企业应积极参与监管机构审查，以确保OTA升级应用符合法律法规和监管要求，并保持与行业伙伴的沟通。

（2）车型开发方面：根据相关OTA标准法规的要求，形成企业内部更为具体详细的OTA技术标准，开发过程中需加强OTA升级技术的研究和开发，重视技术安全问题，重点关注OTA数据完整性、服务完整性及通信安全3部分。应选用更先进的签名技术及密钥技术保护数据的真实性及机密性，采用更安全的架构保证升级服务的完整性，同时应采用更加安全的通信协议保证传输过程的安全性。应在升级过程中对数据进行监测和验证，防止出现数据泄露和恶意攻击等问题，且需加强用户隐私保护和数据安全管理，例如通过数据加密、权限控制和信息追踪，确保用户数据的安全性。企业还需构建完善的OTA测试能力，覆盖法规测试及研发阶段的软件升级全链条测试能力，建立丰富的测试用例库，测试内容应包括OTA信息安全检测、OTA性能检测、OTA压力测试、OTA健壮测试、OTA功能测试等。测评体系的建立有助于提高研发过程中的可控性，从而保证车辆OTA升级的质量和稳定性。

4 结束语

介绍了汽车OTA架构以及通用的升级流程，重点关注OTA软件更新服务的安全性和完整性问题，通过对OTA升级相关研究的分析，总结了目前OTA升级关键技术的特点。同时，对国内外的汽车软件升级相关法规及标准进行分析，并基于此为车辆制造企业提出OTA能力建设建议。总结如下：

（1）为保证完整稳定的OTA服务，需保证其数据完整性和服务完整性。

（2）保证OTA数据完整性的主要技术有哈希函数、密钥加密等，保证OTA服务完整性的主要手段有应用区块链技术、设计OTA新架构等。

（3）目前对OTA的监管主要集中在企业汽车软件升级管理体系及具体车型升级要求2方面。满足标准及法规提出的OTA能力要求可保障汽车软件升级的安全稳定性，进一步规范OTA市场。

参 考 文 献

[1] LE V H, HARTOG J D, ZANNONE N. Security and Privacy for Innovative Automotive Applications a Survey[J]. Computer Communications, 2018(132): 17-41.

[2] GUISSOUMA H, HOHL C P, LESNIAK F. Lifecycle Management of Automotive Safety- Critical Over the Air Updates: A Systems Approach[J]. IEEE Access, 2022(10): 57696.

[3] PHAM M, XIONG K. A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles, Computers & Security, 2021(109): 102269.

[4] CHATTOPADHYAY A, LAM K Y, TAVVA Y. Autonomous Vehicle: Security by Design[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22 (11): 7015-7029.

[5] DAJSUREN Y, MARK B. Automotive Systems and Software Engineering: State of the Art and Future Trends[M]. Springer, 2019.

[6] NILSSON D K, PHUNG P H, LARSON U E. Vehicle ECU Classification based on Safety-Security Characteristics[C]// IET Road Transport Information and Control and ITS United Kingdom Members' Conference, 2008: 1-7.

[7] RIGGS C, RIGAUD C, BEARD R, et al. A Survey on Connected Vehicles Vulnerabilities and Countermeasures[J]. Journal of Traffic and Logistics Engineering, 2019, 6(1): 11-16.

[8] 王栋梁, 汤利顺, 陈博. 智能网联汽车整车OTA功能设计研究[J]. 汽车技术, 2018, 517(10): 33-37.

[9] IDREES M S, SCHWEPPE H, ROUDIER Y, et al. Secure Automotive on-board Protocols: a Case of Over-the-air Firmware Updates[J]. Lecture Notes in Computer Science, 2011(6596): 224-238.

[10] KHURRAM M, KUMAR H, CHANDAK A, et al. Enhancing Connected Car Adoption: Security and over the Air Update Framework[C]// IEEE World Forum on Internet of Things, Reston, VA, 2016: 194-198.

[11] 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.

[12] ABI Research. Adoption of Automotive Software Over-the-Air Updates [EB/OL]. (2019-11-15) [2023-07-05]. https://www.abiresearch.com/press/abi-research-anticipates-accelerated-adoption-auto/.

[13] NIE S, LIU L, DU Y. Free-fall: Hacking Tesla From Wireless to Can Bus[C]// Black Hat USA, 2017.

[14] 汤伟强. 主动式汽车安全带控制系统开发及OTA远程升级研究[D]. 上海: 华东理工大学, 2022.

[15] HALDER S, CONTI M, DAS S K, A Holistic Approach to Power Efficiency in a Clock Offset based Intrusion Detection Systems for Controller Area Networks[J]. Pervasive and Mobile Computing, 2021(73): 101385.

[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, 14.

[18] 谭凡. 智能网联汽车FOTA系统安全机制的研究与实现[D]. 成都: 电子科技大学, 2020.

[19] 高洁,汪庆. 一种电动汽车软件OTA升级服务平台的设计方案[J]. 电脑知识与技术, 2017, 13(8): 209-211.

[20] 董晓慧. 面向车载域控制器架构的安全FOTA升级方法研究[D]. 长春: 吉林大学, 2022.

[21] FONGEN A. Identity Management and Integrity Protection in the Internet of Things[C]//International Conference on Emerging Security Technologies, Lisbon, Portugal, 2012.

[22] MATHUR R, AGARWAL S, SHARMA V. Solving Security Issues in Mobile Computing Using Cryptography Techniques-A Survey[C]//International Conference on Computing, Communication and Automation, 2015: 492-497.

[23] KNOCKEL J, CRANDALL J R. Protecting Free and Open Communications on the Internet Against Man-inthe-middle Attacks on Third-party Software: we're FOCI'd[C]// USENIX Workshop on Free and Open Communications on the Internet, Bellevue, WA, 2012.

[24] KUPPUSAMY T K, DELONG L A, CAPPOS J. Uptane: Security and Customizability of Software Updates for Vehicles[J]. IEEE Vehicular Technology Magazine, 2018, 13(1): 66-73

[25] 胡文, 姜立标. 智能网联汽车的多级安全防护方案设计和分析[J]. 网络安全技术与应用, 2017, 2(2): 136-138+140.

[26] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces[C]//Proceedings of USENIX Security Symposium, 2011: 77-92.

[27] NILSSON D K, LARSON U E. Secure Firmware Updates Over the Air in Intelligent Vehicles[C]//Proceedings of IEEE International Conference on Communications Workshops, 2008, 380-384.

[28] BYEON, SANG P, KIM, et al. ECU Data Integrity Verification System Using Blockchain[J], Journal of Industrial Convergence, 2022, 11(20): 57-63

[29] MANSOUR K, FARAG W, ELHELW M. AiroDiag: A Sophisticated Tool that Diagnoses and Updates Vehicles Software Over Air[C]//IEEE International Electric Vehicle Conference, Greenville, SC, USA, 2012: 1-7.

[30] MAHMUD S M, SHANKER S, HOSSAIN I. Secure Software Upload in an Intelligent Vehicle via Wireless Communication Links[C]//Proceedings of IEEE Intelligent Vehicles Symposium, 2005: 588-593.

[31] STEGER M, KARNER M, HILLEBRAND J, et al. Generic Framework Enabling Secure and Efficient Automotive Wireless SW Updates[C]//Proceedings of IEEE 21st International Conference on Emerging Technologies and Factory Automation, 2016: 1-8.

[32] MAYILSAMY K, RAMACHANDRAN N, RAJ V S. An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air[J]. Computers & Electrical Engineering. 2018(71): 578-593.

[33] PETRI R, SPRINGER M, ZELLE D, et al. Evaluation of Lightweight TPMs for Automotive Software Updates Over the Air[C]//Proceedings of 4th International Conference on Embedded Security in Car USA, 2016: 1-15.

[34] STEGER M, DORRI A, KANHERE S S, et al. Secure Wireless Automotive Software Updates Using Blockchains: a Proof of Concept[C]//Proceedings of 22nd International Forum on Advanced Microsystems for Automotive Applications, 2018: 137-149.

[35] DHAKAL S, JAAFAR F, ZAVARSKY P. Private Blockchain Network for IoT Device Firmware Integrity Verifica-

tion and Update[C]//IEEE Internationa Symposium on High Assurance Systems Engineering, 2019: 164-170.

[36] MAHMOOD S, NGUYEN H N, SHAIKH S A. Systematic Threat Assessment and Security Testing of Automotive Over-the-Air (OTA) Updates[J]. Vehicular Communications, 2022(35): 100468.

[37] GHOSAL A, HALDER S, CONTI M. Secure Over-the-Air Software Update for Connected Vehicles[J]. Computer Networks, 2022(218): 109394.

[38] UNITED NATIONS. Software Update and Software Update Management System, UN Regulation No. 156 [S/OL]. (2020-04-04) [2023-07-05]. https://unece.org/sites/default/files/2021-03/R156e.pdf.

[39] ISO/TC 22/SC 32. Road vehicles—Software update engineering, Standard ISO 24089 [S/OL]. (2023-02) [2023-07-05]. https://www.iso.org/obp/ui/en/#iso:std:iso:24089:ed-1:v1:en

[40] 工业和信息化部装备工业发展中心. 关于开展汽车软件在线升级备案的通知 [2022]229号[S/OL]. (2022-04-15) [2023-07-05]. http://www.miit-eidc.org.cn/art/2022/4/15/art_54_30478.html.

[41] 工业和信息化部装备工业一司.《汽车软件升级通用技术要求》征求意见稿[EB/OL]. (2022-06-17) [2023-07-05].https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2022/art_c1878e9460a74860a37bd3964436116d.html.

（责任编辑　**明慧**）

【作者简介】

王婧璇（1997—），女，中国汽车工程研究院股份有限公司，工程师，研究方向为汽车软件在线升级技术及法规。

E-mail：wangjingxuan@caeri.com.cn

《汽车技术》征稿启事

《汽车技术》杂志是中国第一汽车集团有限公司主办的国内外公开发行的汽车前瞻与应用技术类月刊，为我国高质量科技期刊分级目录入选期刊、中国科学引文数据库（CSCD）来源期刊、中文核心期刊、中国科技核心期刊、RCCSE中国核心学术期刊（A）、俄罗斯《文摘杂志》（AJ）收录期刊。

《汽车技术》杂志以报道汽车整车及其零部件设计、研究、试验等方面的前瞻与应用技术为主，并兼有理论研究内容，是中国汽车行业核心学术和知识传播与共享的平台。

《汽车技术》将在国家提出的“创新、协调、绿色、开放、共享”发展理念的指引下，把握《节能与新能源汽车技术路线图》和“低碳化、信息化、智能化”的汽车技术主流发展趋势，努力在传统内燃机汽车高效动力系统、轻量化、低阻力领域，新能源汽车和互联智能汽车技术领域，大力吸收优质稿源，为广大科研和工程技术人员服务，为我国汽车工程技术创新能力提升贡献力量。

《汽车技术》欢迎高等院校师生、研发工程技术人员、技术管理人员及相关人员不吝赐稿，反映国家重点扶持项目、自然科学基金项目和其他重点项目等研究成果的稿件将被优先选择刊登。

投稿要求：

1.文章字数最好控制在6 000~8 000字范围之内；

2.请按科技论文要求撰写文章摘要，摘要中文字数控制在180字左右；

3.文章必须附有公开发表的、体现本领域最新研究成果的参考文献，且在文中应标注文献引用处；

4.文章主要作者应提供其简介，包括出生年、性别、职称、学历、研究方向及技术成果等；

5.来稿的保密审查工作由作者单位负责，确保署名无争议，文责自负；

6.请勿一稿多投；

7.本刊使用网站投稿，请先登陆网站注册成功后投稿，详细投稿要求见本刊网站中“下载中心”栏的“作者指南”，网址：http://qcjs.cbpt.cnki.net。

《汽车技术》编辑部