DOI 10.15302/J-SSCAE-2019.03.006

智能网联汽车信息安全管理的实施对策

赵世佳[1]，徐可[1]，薛晓卿[2,3]，乔英俊[4]

（1. 工业和信息化部装备工业发展中心，北京 100846； 2. 中国软件评测中心，北京 100048；
3. 清华大学车辆与运载学院， 北京 100084；4. 中国工程院战略咨询中心，北京 100088）

摘要：新一轮科技和产业变革加速融合，智能网联汽车为消费者提供了便利的使用方式、丰富的应用内容和安全的驾驶环境，但同时，由智能化、网联化带来的信息安全问题也面临着多重风险。近年来黑客攻击频发，信息安全问题不仅会影响行车安全、造成用户数据泄露，更使国家安全受到威胁。安全问题已经引发各国政府的高度重视，美国、欧洲和日本等主要发达国家和地区都在积极行动。在此背景下，我国应尽快推动统筹智能网联汽车信息安全的发展和管理，积极布局、合理规划，全力保障智能网联汽车信息安全，推动智能网联汽车的稳步发展。

关键词：智能网联汽车；信息安全；汽车产业；管理

中图分类号：TM912　　**文献标识码：**A

Implementation Countermeasures for Information Security Management of Intelligent Connected Vehicles

Zhao Shijia[1], Xu Ke[1], Xue Xiaoqing[2,3], Qiao Yingjun[4]

(1. Ministry of Industry and Information Technology Equipment Industry Development Center, Beijing 100846, China;
2. China Software Test Center, Beijing 100048, China; 3. School of Vehicle and Mobility, Tsinghua University,
Beijing 100084, China; 4. Center for Strategic Studies, CAE, Beijing 100088, China)

Abstract: A new round of technological and industrial changes has accelerated technological integration. Intelligent connected vehicles (ICVs) have provided consumers with convenient use, rich application contents, and a safe driving environment. Meanwhile, multiple risks are also brought to information security by intelligentization and networking. In recent years, hacker attacks frequently occur, and information security not only affects driving safety and user data safety, but also threatens national security when being damaged. So, information security issues have attracted great attention from governments all over the world. Major developed countries and regions, such as the United States, Europe, and Japan, are taking active actions to safeguard information security. In this context, China should promote the development and management of the information security of the ICVs, take active measures, make rational planning, and make every effort to ensure the information security of ICVs, thus to promote the steady development of the ICVs.

Keywords: intelligent connected vehicles; information security; automotive industry; management

收稿日期：2019-05-06；**修回日期：**2019-05-09

通讯作者：乔英俊，中国工程院战略咨询中心助理研究员，研究方向为能源与交通、区域创新研究；E-mail: qiaoyj@cae.cn

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

在新一轮科技革命和产业变革背景下，智能网联汽车是新兴技术与汽车产业融合创新的重要组成部分，汽车已不再是孤立的单元，而逐步成为智能交通、智慧能源、智慧城市等系统的重要载体和节点，被视为可移动的智能网络终端。随着人工智能、信息通信技术加速发展和跨界融合，智能网联汽车与外界的交互手段不断丰富，智能网联汽车在积极融入网络时代的同时，也不可避免地面临信息安全问题。2015 年，两名黑客实现远程操控行驶中的切诺基，Uconnect 车载系统发送指令，能够操控车辆进行降速、关闭引擎、突然制动或制动失灵等行为，使车辆驶离道路，菲亚特克莱斯勒公司召回在美国受影响的 140 万辆汽车，包括吉普、道奇等品牌，这是全球汽车制造商首次因信息安全问题而召回车辆，美国高速公路安全管理局（NHTSA）高度关注，并且跟踪菲亚特克莱斯勒公司的软件升级方案能否解决问题。2016 年，日产聆风曝出 Nissan Connect 服务安全漏洞事件。2017 年，福特汽车有限公司、宝马集团、英菲尼迪汽车公司和日产汽车公司等企业的远程信息处理控制单元被爆出存在漏洞。智能网联汽车面临恶意攻击和威胁的概率不断提高，攻击方式和途径越来越难以预测。

智能网联汽车的信息安全威胁不仅能够造成个人隐私泄露、企业经济损失，还能造成车毁人亡的严重后果，甚至带来国家公共安全问题 [1,2]。美国独立研究机构 Ponemon 公布的汽车信息安全调查报告预测，未来由于信息安全漏洞被召回的车辆将高达 60%~70%，汽车受到信息安全攻击的威胁正逐步提升 [3]。智能网联汽车信息安全已经成为汽车产业甚至社会关注的焦点。据统计，56% 的消费者表示信息安全和隐私保护将成为未来购买车辆主要考虑的因素 [4]。

当前，汽车电动化、智能化、网联化、共享化成为全球汽车产业的重要发展趋势，欧洲、美国、日本等主要发达国家和地区加紧部署智能网联汽车，主要跨国车企、零部件巨头、互联网企业加快智能网联汽车及重点领域的投资布局。我国也将智能网联汽车作为重要的发展方向，并将其作为汽车强国建设的重要突破口之一 [5]。在大力发展智能网联汽车的同时，我国亟需将汽车信息安全上升为国家网络安全的重要组成部分，高度重视信息安全带来的风险，加快推进智能网联汽车信息安全技术的研发及应用、建立标准法规、制定相应的测试规范，有效实现多部门的协同机制，实现全方位的安全防护。

二、智能网联汽车面临多重信息安全风险

目前，智能网联汽车面临的信息安全风险主要来自于“云 – 管 – 端 – 外部链接”，即云平台、网络传输、车辆以及相关联的外部设备，如图 1 所示。

（一）车辆安全风险

终端主要是将车辆看作系统中的智能终端，随着车辆智能化、网联化水平不断增加，车辆自身面临的信息安全问题也日益增多。

车辆的信息安全风险主要包括三个方面：一是系统安全。一方面是软件系统安全，随着软件在汽车占比的逐步提升，软件安全面临较大的风险挑战，如主机厂将软件安装包（APK）开放下载，容易受到黑客攻击；另一方面是硬件系统安全，对于自动驾驶和自动巡航系统，通过伪造障碍物，干扰毫米波雷达判断，从而逼停车辆或干扰车辆前进，或控制超声波设备发送与汽车相同周期和频率的超声波，干扰汽车等，一旦被攻击，将存在车辆安全事故风险。二是密钥安全。通常采用数据加密的方式实现保护数据隐私，一旦密钥被泄露，加密数据的

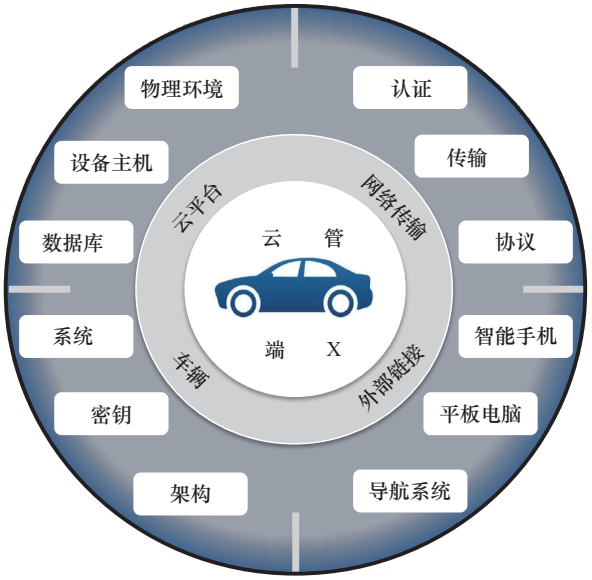

图 1　智能网联汽车信息安全风险架构

安全性将荡然无存。例如，通过在远离汽车时录制汽车钥匙信号，实现一次性开门，以及分析解码后通过计算使误差永远在合理范围内，实现无限次开门。攻击者通过插桩调试获取控制信息后逆向分析，从而获取控制流程，并利用脚本通过蓝牙钥匙控制汽车。三是架构安全。汽车内部相对封闭的网络环境也存在可被攻击的缺口，对于外部攻击的防御能力较弱，如车载诊断系统（OBD）接口、面向媒体的系统传输（MOST）总线、控制器局域网络（CAN）总线、串行通讯网络（LIN）总线、胎压监测系统等 [6]。由于 CAN 总线采用明文通信的机制，如果能够深入到控制 CAN 网络，就能够控制相关的电子控制单元（ECU），造成危险。

（二）云平台安全风险

云平台是智能网联汽车系统的重要组成部分，实现的功能日益丰富，从监督管理、提供娱乐服务、远程诊断故障到远程控制车辆、空中下载技术（OTA）升级等，由提供信息服务逐渐向车辆底层控制深入。云平台的安全主要包括物理环境、设备主机、接口、数据库、应用程序安全等。

云平台面临着多种恶意威胁，既有病毒防护、访问控制防护等，更有数据安全防护，尤其是防止云端数据（特别是隐私数据）的丢失和被窃取。目前大部分车联网数据使用分布式技术进行存储，主要面临的安全威胁包括黑客对数据恶意窃取和篡改、敏感数据被非法访问等。未来，通过云平台将可以实现多种形式的云服务，如跟踪和管理整个车队的车辆等。据 QYResearch 估计，到 2024 年全球 30% 的售出车辆将配备网络安全云服务，网络安全云服务的收入将达到 5.58 亿美元。随着智能网联汽车持续发展，数据安全、访问控制等方面的威胁也会逐步增多，云平台安全风险要予以足够的重视。

（三）网络传输安全风险

V2X 指智能网联汽车对外的通信连接，以长期演进（LTE）和第五代移动通信网络（5G）为主，目前国家也在加大力度推动通信技术及标准的发展。同时，专用短程通信技术（DSRC）作为一项成熟的技术，在车车通信方面也具有自身的优势。通信的安全主要包括通信的完整性，传输消息不能被非法篡改；防止伪装或者中间人攻击，确保消息来自合法的发送设备；防止洪泛攻击，保证通信的性能和可用性。

网络传输存在三大安全风险：一是认证风险，通过身份伪造、动态劫持等方式冒充验证者的身份信息。二是传输风险，车辆的传输信息在没有加密或强度不够的情况下，容易遭受攻击。三是协议风险，通信流程把一种协议伪装成另一种协议。例如，协议链路层的通信未加密，可以通过抓取链路层标识实现具体车辆的定位，进行跟踪；在自动驾驶情况下，汽车按照 V2X 通信内容制定行驶路线，攻击者通过伪消息诱导车辆发生误判，影响车辆控制 [7]。

（四）外部链接设备安全风险

随着智能网联汽车承载的功能逐步增多，操控 APP、充电桩等外部生态组件频繁接入车辆将带来新的安全风险。

消费者在购买和安装车辆的外部链接产品时，将带来外部病毒入侵攻击的风险。首先，便携设备参杂着大量仿制、山寨产品或恶意代码应用程序等，这些外联设备组件获取成本低且安全防护能力不足。其次，新能源汽车的充电桩存在安全风险，如充电桩控制模块通过以太网与管理系统连接，网络内部没有防护，可通过互联网入侵桩联网，控制充电电压、篡改充电金额等。同时，充电 APP 与移动支付相关，通过在手机内植入木马等方式可进行信息窃取、恶意吸费等攻击 [8]。最后，现有汽车的后装产品信息安全面临较大风险挑战，本身而言，现有车辆设计对信息安全的考虑不足，例如后装市场的 OBD 盒子、车机等具有潜在风险。综上所述，汽车企业在车辆研发过程中，必须重点考虑外接设备所带来的恶性信息安全攻击威胁 [9]。

三、加强智能网联汽车信息安全管理

由智能网联引发的汽车新的安全隐患已经得到各国政府的高度重视，美国、欧洲、日本等国家和地区积极推动信息安全相关标准和技术规范制定工作，加快形成智能网联汽车信息安全管理要求。

（一）美国的全方位信息安全法规标准

美国将汽车信息安全上升到国家安全层面，政

府主管部门通过制定政策、推动立法、发布安全实践等手段引导产业加快信息安全发展。在政策方面，2016 年 9 月，美国 NHTSA 正式发布联邦自动驾驶汽车政策 Federal Automated Vehicles Policy，高度自动车辆（HAV）评估包括 15 项安全性能，其中涉及隐私、整车网络安全等汽车网络安全相关内容。在法规方面，2017 年 3 月，美国国会通过汽车安全和隐私草案（Security and Privacy in Your Car Act，简称“SPY Car Act”），指示 NHTSA 制定机动车辆网络安全法规，要求在美国销售的机动车辆可以防止非授权入侵，包括电子控制及驾驶数据和数据传输安全。美国众议院通过《确保车辆演化的未来部署和研究安全法案》（《自动驾驶方案》）要求汽车企业必须制定详细的网络安全计划，否则将阻止其制造、销售或进口智能网联汽车系统及车辆。在标准方面，美国基于 ISO 26262 率先制定 SAE J3061《汽车系统网络安全指南》等系列标准，内容涉及汽车信息安全完整性等级、测试方法和测试工具等，以保证汽车在全生命周期中都可获得有效的信息安全保护，为整车企业和汽车零部件供应商提供了技术参考和建议。同时，美国汽车工程师协会（SAE）与 ISO/TC22 道路车辆技术委员会以联合工作组的形式成立了汽车信息安全工作组，正式启动 ISO 层面的国际标准法规制定工作。2016 年，NHTSA 发布了《现代汽车信息安全最佳实践》，针对快速发展的智能网联汽车信息安全及隐私保护等问题推出了最佳实践框架结构。汽车行业通过各种手段强化信息安全防护能力，通用汽车公司、特斯拉等多家汽车企业也通过公开招募安全人员或者与安全机构合作的方式，来应对汽车的信息安全问题。

（二）欧洲的汽车零部件及网络通信安全

欧洲网络和信息安全局将智能网联汽车列为物联网安全的重要组成部分，组建专家团队。同时，欧洲依托强大的汽车制造商和零部件供应商，自 2008 年开始分别开展了 EVITA、OVERSEE、PRESERVE 等项目，从汽车硬件安全、网络传输通信安全等方面提出了技术规范和解决方案，部分技术成果已实现产业化应用，如 EVITA 项目为汽车网络安全提供信息“攻击”场景、危险分析、建议性硬件系统结构等方面的技术指南。沃尔沃与瑞典查尔姆斯理工大学等合作 HEAVENS 项目，进行网络风险评估。大陆集团收购以色列安全公司 Argus，以期进一步加强并提高汽车网络安全方面的能力。英国公司 Cerberus 研发了 RISC–V 开源内核和定制加密、密码管理单元设计安全芯片，提高了无人驾驶汽车、物联网设备的网络安全防御能力。另外，欧洲电信标准协会（ETSI）针对智能网联汽车与智能交通系统制定了包括智能交通系统（ITS）安全服务架构、ITS 通信安全架构与安全管理、可信与隐私管理、访问控制和保密服务等方面的一系列信息安全标准，加强对智能网联汽车信息安全发展的规范和引导。

（三）日本的汽车生命周期信息安全保护措施

日本《网络安全战略》明确将汽车列入物联网系统安全领域。日本信息处理推进机构（IPA）从汽车可靠性的角度出发，通过对汽车安全的攻击方式和途径进行分析定义了汽车信息安全模型 IPA Car，其中，信息安全产生的威胁包括用户偶然引发的失误以及攻击者恶意造成的威胁两类，针对此类威胁提出了信息加密、判定用户程序合法性、对使用者操作权限和通信范围实施访问控制管理等策略 [10]。同时，IPA 遵循汽车的全生命周期制定了安全管理方针，设计阶段根据各项功能安全性的重要程度实施预算划拨，开发阶段根据编码标准采用防漏洞的安全编码，使用阶段为消费者构筑了信息安全快速应对的联络反馈机制，废弃阶段提供信息删除功能等，以保证用户的各项隐私，如图 2 所示。日本瑞萨电子推出“汽车功能安全和网络安全支持计划”，通过简化精密的汽车系统的设计复杂性，为实现安全的驾驶体验做出贡献。

四、我国智能网联汽车信息安全管理的实施对策

近年来，随着信息安全事件频发，我国政府对于信息安全防护逐渐加强，政策支持力度不断提高。网络安全成为“十三五”规划重点建设方向，《国家网络空间安全战略》以及《战略性新兴产业重点产品和服务指导目录》等多项政策密集出台，加速推动信息安全产品需求释放，《中华人民共和国网络安全法》的实施推动了我国网络安全水平跃

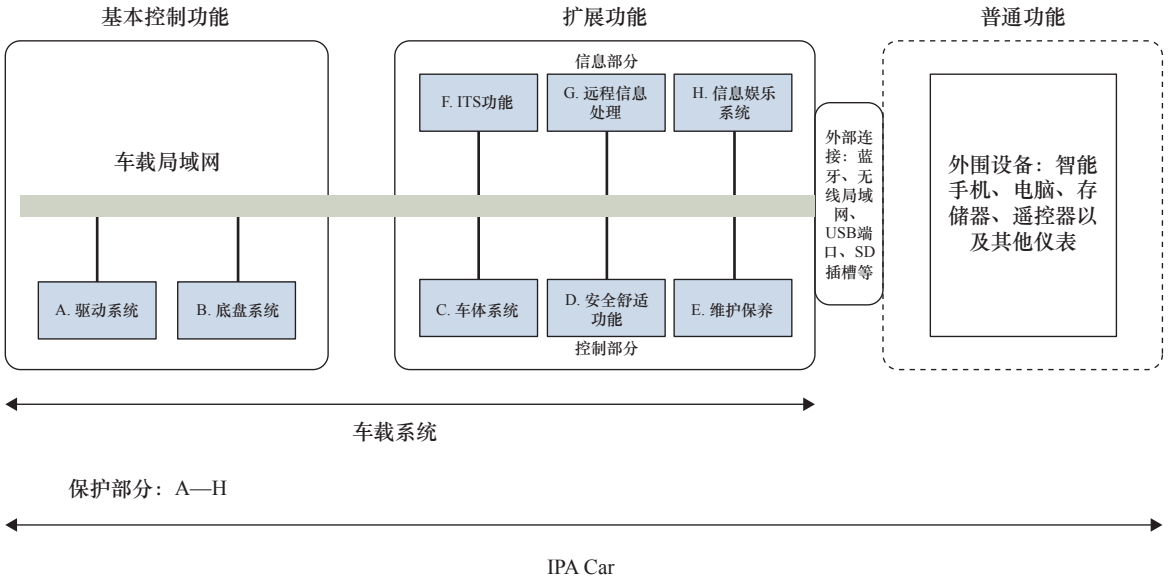

图 2　日本汽车信息安全模型 IPA Car [10]

升。我国信息安全产业规模不断扩大，从 2012 年的 157.26 亿元上升至 2016 年的 341.72 亿元，五年内年均复合增速达到 21.41%。

2016 年 4 月，全国汽车标准化技术委员会下设的智能网联汽车分技术委员成立了汽车信息安全工作组，负责跟进国际标准化工作、制定国内智能网联汽车信息安全相关的标准体系。《汽车产业中长期发展规划》将智能网联汽车的信息安全作为重要目标和任务。但是，我国汽车产业信息安全意识刚起步，需求尚不十分明确，自身安全防护能力薄弱，智能网联汽车信息安全技术要求和测试评价标准体系不完善，无法对企业形成有效的引导和促进，也无法对产品和服务的质量进行有效把控。规范的安全监管标准和测试流程缺失，各个企业依据自己的理解进行规划和实践，智能网联汽车信息安全管理机制尚不健全，无法对信息安全风险进行预测、感知、监督、反馈以及发布等。

综上所述，我国亟待加强智能网联汽车信息安全管理，在技术研发、标准法规、测试规范方面提出以下实施对策。

（一）推进智能网联汽车信息安全技术研发与应用

智能网联汽车的发展对信息安全技术提出了新的要求。除了要有基本的安全功能需求，例如抵御网络攻击、检测扫描软件漏洞、防止数据篡改和实时检测异常行为等，还有对车辆功能的特殊需求，包括车辆行驶安全保证、车辆信息交互功能保证以及隐私信息安全保证。由于传统车辆是相对封闭的个体，因此，车辆的功能设计以实时性和功能安全为主，较少考虑信息安全。但随着车辆智能化和网联化的发展，使得信息安全领域衍生出众多与车辆相关的威胁风险。因此，为保障未来智能网联汽车信息安全，需要对基础元件到整个产品，从设计研发到生产整个过程当中，考虑加入信息安全元素，并且建立信息安全闭环，提高车辆的信息安全防护能力。

一是加强顶层设计，通过制定政策、发布指南等形式对行业进行规范指导，建立智能网联汽车信息安全防护体系，支持智能网联汽车信息安全技术的研发和推广应用，设立课题，强调部门协作进行关键技术公关。二是从全生命周期的维度加强智能网联汽车信息安全防护，重点加强关键芯片、软件、通信协议和系统应用等创新，提升安全可控水平，研发芯片加密技术、应用软件安全防护技术、安全隔离架构技术、云平台数据加密安全防护技术等。在国家级及企业级远程监控平台中，尽快导入信息安全监控模块，对于车辆、外部链接设备等安全隐患进行实时监控和预警，压制恶意攻击在系统内部网络的扩散传播，及时上报漏洞或攻击，不仅要在第一时间弥补安全漏洞，更要注重升级自身的安全性，杜绝二次威胁的引入。三是通过搜集国内外网络安全事件及工具，总结智能网联汽车信息安全问

题，引导前端企业探索可行的解决方案，同时加强对个人信用记录、违法失信行为等数据的收集与分析，降低攻击发生的可能性。四是构建智能网联汽车基础数据交互管理平台，推动各车企平台、服务提供商平台信息数据的实时接入，统一监管，以保证监管和服务的可靠性和稳定性。

（二）建立智能网联汽车信息安全标准法规

由于智能网联汽车信息安全属于新兴领域，监管主体、内容、方法、手段均没有出台相应的法律法规或规程进行明确。虽然已经颁布《中华人民共和国网络安全法》，但是缺乏针对行业细分领域的解读和细则制定，导致监管缺乏一定的法律依据以及规章措施的保护。我国应在充分借鉴国外在汽车信息安全标准法规发展经验的同时，结合我国智能网联汽车发展的特点以及信息安全方面的问题，加强我国智能网联汽车信息安全行业规范。

一是加强智能网联汽车信息安全立法工作，明晰信息安全框架下对汽车企业、零部件企业的要求，明确由于信息安全系统被破坏引发恶性事件的责任判定和处罚。二是跟踪全球智能网联汽车信息安全标准化动态，联合标准化机构加快制定信息安全防护标准，包括《汽车信息安全防护通用技术条件》《汽车网关信息安全技术要求》《汽车信息安全通用技术规范》《车载 T-BOX 信息安全技术要求》《电动汽车充电信息安全防护规范》等。三是制定智能网联汽车数据安全技术标准，通过对数据进行分级，确定保护级别，建立“云 – 管 – 端 – 外部链接”数据安全标准框架。

（三）制定智能网联汽车信息安全测试规范

传统汽车更多地聚焦于功能安全，而信息安全逐步成为智能网联汽车关注的焦点。通过测试可以有效衡量信息安全保护措施是否符合防护需求，利用测试排查信息安全隐患和薄弱环节，有助于大幅提升安全防护能力。

一是建立健全智能网联汽车信息安全技术要求以及测评标准体系，搭建智能网联汽车检测和评估平台。二是依据车辆的应用场景，分析车辆的信息安全威胁面、风险等级，建立不同智能化水平下的车辆信息安全威胁模型，依托第三方测评机构开展检测与评估服务，对产品可能存在的缺陷和弱点进行安全检测。三是推动低等级智能网联汽车通过国家信息认证体系实现自愿认证，对高等级智能网联汽车要求实施强制安全认证。

参考文献

[1] 钟志华, 乔英俊, 王建强, 等. 新时代汽车强国战略研究综述(一) [J]. 中国工程科学, 2018, 20(1): 1–10.
Zhong Z H, Qiao Y J, Wang J Q, et al. Summary of strategy research on automobile power in new era (I) [J]. Strategic Study of CAE, 2018, 20(1): 1–10.

[2] 钟志华, 乔英俊, 王建强, 等. 新时代汽车强国战略研究综述(二) [J]. 中国工程科学, 2018, 20(1): 11–19.
Zhong Z H, Qiao Y J, Wang J Q, et al. Summary of strategy research on automobile power in new era (II) [J]. Strategic Study of CAE, 2018, 20(1): 11–19.

[3] Ponemon Institute. Car cybersecurity: What do the automakers really think? [R]. Traverse City: Ponemon Institute, 2015.

[4] IBM 商业价值研究院. 加速车辆信息安全: 赢得车辆完整性和数据隐私性竞争 [R]. 北京: IBM 商业价值研究院, 2017.
IBM Business Value Research Institute. Accelerating vehicle information security: Winning vehicle integrity and data privacy competition [R]. Beijing: IBM Business Value Research Institute, 2017.

[5] 赵福全, 刘宗巍, 郝瀚, 等. 中国实现汽车强国的战略分析和实施路径 [J]. 中国科技论坛, 2016 (8): 45–51.
Zhao F Q, Liu Z W, Hao H, et al. Analysis of China’s strategy for a stronger automotive country and its implementation pathway [J]. Forum on Science and Technology in China, 2016 (8): 45–51.

[6] 于赫. 网联汽车信息安全问题及CAN 总线异常检测技术研究 [D]. 吉林: 吉林大学(博士学位论文), 2016.
Yu H. Research on connected vehicle cyber security and anomaly detection technology for in-vehicle CAN Bus [D]. Jilin: Jilin University (Doctoral dissertation), 2016.

[7] 李逸瀚. 电动汽车信息安全网关研制与 wolfSSL 协议研究 [D]. 合肥: 中国科学技术大学(硕士学位论文), 2017.
Li Y H. Research of the information security gateway of electric vehicle and research on wolfSSL protocol [D]. Hefei: University of Science and Technology of China (Master’s thesis), 2017.

[8] 赵世佳, 赵福全, 郝瀚, 等. 中国新能源汽车充电基础设施发展现状与应对策略 [J]. 中国科技论坛, 2017 (10): 97–104.
Zhao S J, Zhao F Q, Hao H, et al. The current situation and countermeasures in Chinese charging infrastructure of new energy vehicles [J]. Forum on Science and Technology in China, 2017 (10): 97–104.

[9] 冯志杰, 何明, 李彬, 等. 汽车信息安全攻防关键技术研究进展 [J]. 信息安全学报, 2017, 2(2): 1–14.
Feng Z J, He M, Li B, et al. Research on car information security attack and protection technology [J]. Journal of Cyber Security, 2017, 2(2): 1–14.

[10] 印曦, 魏冬, 黄伟庆, 等. 日本车联网信息安全发展现状与分析 [J]. 中国信息安全, 2017 (1): 98–101.
Yin X, Wei D, Huang W Q, et al. Current situation and analysis of information security of vehicle networking in Japan [J]. China Information Security, 2017 (1): 98–101.