2021

智能网联汽车信息安全发展报告

ANNUAL REPORT ON THE DEVELOPMENT OF INTELLGENT CONNECTED VEHICLE INFORMATION SECURITY（2021）

精华版

中国汽车工程研究院股份有限公司
车联网安全联合实验室
主编

智能网联汽车信息安全发展报告

2021

(精华版)

蓝皮书官方微信群

中国汽研北京分院官微

中国汽研官微

——欲了解智能网联汽车信息安全产业发展、蓝皮书相关动态，以及参与皮书编制工作组，请扫码关注公众号/加入官方群!!

编 委 会

支 持 单 位

- 工业和信息化部装备工业发展中心
- 国家计算机网络与信息安全管理中心
- 中国工业互联网研究院信息安全所
- 中国电子信息产业发展研究院
- 中国电子技术标准化研究院
- 中国信息通信研究院
- 华东师范大学
- 北京邮电大学
- 北京航空航天大学
- 北方工业大学
- 长安大学
- 重庆邮电大学
- 华为技术有限公司
- 浙江长三角车联网安全技术有限公司
- 深圳市纽创信安科技开发有限公司
- 上海犬安科技有限公司
- 上海工业控制安全创新科技有限公司
- 杭州安恒信息技术股份有限公司
- 北京天融信网络安全技术有限公司
- 北京中电华大电子设计有限责任公司
- 北京智芯微电子科技有限公司
- 安谋科技（中国）有限公司
- 天津国芯科技有限公司

- 广州小鹏汽车科技有限公司
- 恒大汽车科技（广东）有限公司
- 长城汽车股份有限公司
- 重庆长安汽车股份有限公司
- 国汽（北京）智能网联汽车研究院有限公司
- 江苏智能网联汽车创新中心
- 北京安杰律师事务所
- 上海伊世智能科技有限公司
- 中汽创智科技有限公司

编辑说明

本蓝皮书由中国汽车工程研究院股份有限公司（简称：“中国汽研”）、车联网安全联合实验室策划编撰，旨在以年度报告的形式，通过对智能网联汽车信息安全产业政策、标准、技术、产品、企业等多维度分析，洞察智能网联汽车信息安全领域发展现状及趋势，为广大读者提供这一新兴领域的产业立体图景以了解行业发展规律，进而推动中国智能网联汽车产业健康有序发展。

中国汽车工程研究院股份有限公司（简称“中国汽研”）成立于 1963 年，是国家一类科研院所。近年来，中国汽研聚焦“安全”、“绿色”、“体验”三大技术领域，形成了集检测中心、工程中心、智能中心、新能源中心、数据中心、孵化中心及装备产业于一体的集群体系，提供解决方案、软件数据、装备工具三类产品。在车联网信息安全方面，中国汽研先后承担了车联网安全综合服务平台、智能网联汽车安全检测平台、车联网身份认证平台、智能网联汽车车载安全网关等四项国家课题，获工信部授牌"2020 年车联网安全应用试点示范项目”，已在通信安全、数据安全和隐私安全检测、OTA 应用安全检测和渗透测试等方面形成检测能力，并为行业主管部门政策标准制定提供技术支撑。

车联网安全联合实验室由中国汽研与国家互联网应急中心（CNCERT）于 2019 年 11 月联合成立。依托国家互联网应急中心独特的网络安全资源能力以及中国汽研在汽车领域的专业能力、产业经验与资源，通过建立车联网安全支撑体系、技术体系和服务体系等国家级车联网安全应急保障体系，开展车联网测评技术、攻防技术、仿真平台等关键技术和装备等联合研究，以及创新平台建设及标准制定，逐步拓展车联网安全生态构建，为国家在车联网安全渗透攻击、检测认证、安全防护架构、安全加密体系、安全漏洞库、安全标准等方面提供创新成果，旨在建设国内一流的车联网安全技术支撑平台，为车联网安全攻防与检测提供技术服务，形成引领行业的技术支撑力量。

本蓝皮书内容上分为总报告、调研篇、产业篇、技术篇、政策法规篇、专题篇及附录。通过对智能网联汽车信息安全行业多维度分析，洞察智能网联汽车信息安全领域发展现状及趋势，为广大读者提供这一新兴领域的产业立体图景。

本蓝皮书是行业首部论述汽车信息安全的专著，是汽车领域适应国家《中华

人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等上位法信息安全要求的系统性思考。

本蓝皮书以“智能网联汽车信息安全”为主题，系统介绍了智能网联汽车信息安全产业格局、技术路线，梳理了技术体系和产品体系，特别是对比各国标准、法规、政策的进展，为行业监管方向和思路提出了建设性意见。

本蓝皮书能够为行业管理者提供极具价值的决策性参考，为整车企业、零部件企业、安全服务商等行业主体提供指导性发展建议和风险规避性提示，为社会公众提供客观公正的行业画像，并发挥信息安全教育和舆论引导作用。

目　录

I 总报告

导读：本报告深度剖析了智能网联汽车信息安全的重要性和必要性，分析了智能网联汽车信息安全新形势，介绍了智能网联汽车信息安全的最新进展，提出了智能网联汽车信息安全面临的问题与挑战，并从政策、标准、产业协同、整车企业等方面提出了智能网联汽车信息安全相关对策与建议。

一、智能网联汽车信息安全的重要性和必要性

（一） 智能网联汽车信息安全是国家安全的重要防线

统筹安全与发展是新时期我国经济社会发展的指导思想而网络空间安全已上升至国家安全战略层面。不但汽车的研发设计、生产制造及流通使用各个环节集成了大量影响国家安全的重要敏感信息，而且车辆的互联互通也使得其行驶中的控制权和决策权更多地依赖于路边基础设施及云平台并易受攻击，本产业的重要战略意义上升到保障我国能源安全、实现碳达峰、碳中和、建设交通强国、拉动国民经济增长领域。

（二） 智能网联汽车信息安全事关行业的可持续健康发展

智能网联汽车是传统汽车工业与新兴信息通信技术融合的重要载体。智能网联汽车信息安全产业具有链条长、层级深、技术融合复杂且市场空间巨大等新兴产业特征。智能网联汽车信息安全产业的发展，能够促进包括基础科学、前沿技术、应用技术等在内的多层次自主科技创新能力提升。同时，信息安全产品的市场化推广、服务的商业化落地，将加速推动传统汽车工业技术与互联网信息技术的融合应用，吸引跨界和新兴主体入局，促进产业链、价值链重构，进而为产业转型升级与高质量发展提供动力。同时，通过参与信息安全技术相关的国际标准的制定工作，我国智能网联汽车产业在全球范围内的主导权和话语权逐渐增强。

（三） 智能网联汽车信息安全与个人隐私保护息息相关

智能网联汽车所产生的数据既涵盖与车辆信息安全运行关联的数据，也包括用户数据、汽车应用服务相关数据。这些数据使用户的线上和线下信息相结合，因此一旦其出现泄露情况，汽车用户的个人隐私将难以得到保障。同时，智能网

联汽车或 TSP 云平台一旦遭受非法入侵和攻击，将导致车辆被远程解锁以及启动，甚至其动力系统和转向系统都可能会被恶意控制，从而造成车辆行驶安全事故或车辆被窃取的严重后果。

二、智能网联汽车信息安全发展新形势

（一） 智能网联汽车产业发展迈向新速度

随着人工智能、5G 通信、大数据及云计算架构等新一代信息技术产业的飞速发及其与传统汽车工业的融合创新，汽车的电动化、智能化、网联化、共享化将成为未来行业发展的新趋势。到 2025 年、2030 年，部分自动驾驶、有条件自动驾驶智能网联汽车销量占当年汽车总销量的比例分别为 50%、70%。

（二） 智能网联汽车信息安全面临新风险

在智能移动终端时代汽车产品形态全面革新，边界不断延展，汽车成为万物互联的节点。安全风险既涉及车辆零部件、总线，又涉及无线通信、软件，还包括交通路侧设备、云管理平台、物联网终端等。

智能网联汽车的信息安全风险主要包括车外网络安全风险(包括短距离无线网络、远距离移动网络、V2X 网络、OBD、TSP 云平台、App 等安全风险)、车内网络安全风险(包括 CAN 总线、T-BOX、IVI、OTA 等安全风险)和其他网络安全风险(包括车辆数据安全风险、充电桩安全风险)。

三、智能网联汽车信息安全面临的问题和挑战

（一） 政策法规标准尚未健全，体系化与可落地性亟须加强

法律法规方面，目前国内外智能网联汽车信息安全形势十分严峻，各国政府部对智能网联汽车信息安全的战略部署投入了大量精力，各项工作已步入实质性阶段。我国尚未出台专门的智能网联汽车信息安全法律法规。

标准方面，新领域标准的缺失必将阻碍技术的量产，建立符合行业发展的一系列标准及配套政策，形成一个科学统一的有机体，对于产业的健康有序发展而言至关重要。

（二） 部分核心技术需加强自主可控，融合与创新应用成为关键

目前，完整的、系统级的智能网联汽车信息安全解决方案建设与应用存在一

定难度安全技术缺口依然存在。车联网检测技术方面尚未形成覆盖应用的场景的车联网安全保障体系；企业的漏洞发掘水平有待进一步提高，针对新业务场景的信息安全风险评估技术还需加强；汽车电子稳定性控制技术、零部件程序代码信息校验和安全“写保护”机制、网络安全传输中的加密技术，以及可信计算、终端设备的认证机制等需要实现国产的自主可控；另外，功能安全、信息安全的融合方法还在研究中。

（三） 产业主体协同性不足，安全方案无法有效落地

目前，车企在跨部门、跨组织的协同方面存在障碍，无法实施明确的产品网络安全职责定义和规划；普遍尚未建立起完善的管控生产过程中网络安全风险的防护制度；欠缺处置和应对在整个生命周期内网络安全风险的能力；缺乏与供应商协同管控供应链网络安全风险的保障机制。

（四） 数据资源难以互通共享，管理联动机制尚未建立

目前，工业和信息化部网络安全管理局为贯彻落实《网络安全法》《车联网（智能网联汽车）产业发展行动计划》，建立车联网的网络安全通报机加强车联网网络安全资源、汇聚、威胁信息共享、安全态势研判、风险隐患预警，增进网络安全技术经验交流促进网络安全事件协同处理，提升车联网网络安全防护水平，还处于成立成员单位阶段。

（五） 商业模式尚不清晰，市场化价值仍需探索

由于智能网联汽车尚未大规模普及、社会公众的信息安全意识较为薄弱、信息安全技术在汽车领域的融合应用成熟度不高等因素，智能网联汽车信息安全的市场价值尚未得到广泛认可，价值转化方式也并不明确，而为了保障智能网联汽车信息安全，相关主体需投入相当大，这使得产业发展的内生力和持久力存在不确定性，成为现阶段阻碍产业化进程的重要瓶颈。

四、智能网联汽车信息安全对策建议

（一） 政策方面

1、强化顶层设计

智能网联汽车涉及多个产业及其主管部门，相关政策法规需要从国家战略和行业发展层面做好顶层设计。制定我国智能网联汽车信息安全发展专项规划，对

智能网联汽车信息安全进行统一、有效的统筹管理和规范指引。通过专项规划来协调管理相关行业内企业行为，避免企业间各行其是、价格战;提供贷款、担保、贴息和信用保险等方面的多项政策，加强金融、财税等支持，促进智能网联汽车的信息安全头部企业快速成长，形成技术创新格局。

2、设立重大专项

近几年，随着国家对网络空间安全的重视程度逐步提高，国家相关部委对网络空间安全的相关重大专项给予了专项财政资金的支持。然而，由于智能网联汽车信息安全属于新兴细分领域，目前相关指南中并没有针对智能网联汽车信息安全相关的项目，建议国家在各部委重大专项中专门设立智能网联汽车信息安全专项。

3、鼓励推广应用

我国需积极借鉴欧美等国家智能网联汽车先进地区的经验，在具备足够基础条件的城市推进建设智能网联汽车相关的测试基地、示范运营区，扩大智能网联汽车应用范围。一旦智能网联汽车大规模普及，市场将倒逼整车企业遵循相关智能网联汽车信息安全系列标准，执行严格的供应链管理体制机制，定期进行渗透测试，持续监控信息安全风险建立健全整车企业的智能网联汽车信息安全体系。

4、建立健全整车企业的智能网联汽车信息安全体系。

平衡安全与发展作为新兴产业，体系不健全、标准不完善、技术不成熟、业态不健康往往会是其发展初期的常态。在这样的常态下，产业的发展容易"一管就死、一放就乱"。如何平衡智能网联汽车信息安全产业的安全要求与发展节奏成为新的课题。建议采用"沙盒监管"的方式对智能网联汽车信息安全进行示范验证，总结发展经验，并逐步在全国普及。

（二） 标准方面

1、明确标准体系构建原则

智能网联汽车信息安全标准体系建设应遵从《网络安全法》这一根本性文件《网络安全法》是指导我国各行业、各领域网络安全工作的纲领性文也是我国智能网联汽车信息安全标准体系建设的根本性参考文件。《网络安全法》对网络安全事故的责任主体进行了明确说明在智能网联汽车信息安全方面对整车制造商、车载信息系统提供商及网络服务运营商提出了法律层面的要求，使得汽车行业在

智能网联汽车信息安全功能产品的生产和运营上实现"有法可依"。

智能网联汽车信息安全标准体系建设是一个系统工程应统筹考虑车辆以及车辆与外部信息交互的所有渠道、方式与环节。安全智能网联信息安全标准体系建设必须从广义和狭义两个角度进行考察。广义上，应从信息交互方式、所涉及的节点以及所使用的渠道等方面确保车辆信息在传输、存储和处理过程中不存在泄露和非法访问的威胁;狭义上，则应确保车辆建立安全可靠的车内信息安全防护机制，能够防止车辆相关敏感信息泄露并抵御外界非法入侵。

智能网联汽车信息安全标准体系建设应以汽车行业为主，发挥各相关行业专长共同进行。智能网联汽车的信息安全标准研究、制定应以智能网联汽车为主体，利用相应的信息安全防护技术满足其各类应用场景下的安全需求，由汽车、计算机、通信等各行业发挥各自专长、共同协作开展。

2、协同建立适合产业需要的标准体系

加快智能网联汽车网络安全相关标准的制定。目前我国智能网联汽车信息安全相关标准法规较少且不成体系，各责任部门要统筹规划围绕智能网联汽车系统架构和信息安全产业发展目标推动成立全国智能网联汽车信息安全标准化委员会，推进跨部门、跨行业、跨领域的统筹协调机制的建立，制定智能网联汽车信息安全标准体系及相关指南。针对行业应用广泛、产业急需的智能网联汽车信息安全标准，尽快组建标准制定起草工作组，并设置标准制定绿色通道。全面参与智能网联汽车信息安全国际标准法规的制定工作，吸收相关国际标准制定和实施的经验，鼓励国家标准向国际标准转化，为国际标准的制定带来中国智慧。

（三） 产业协同方面

1、行业各方紧密配合共同解决信息安全问题

智能网联汽车信息安全属于跨产业融合产业，包括通信产业、汽车产业、IT产业、信息安全服务产业、大数据产业、法律行业等，需要对其进行全面融合创新。目前，智能网联汽车信息安全产业并未形成发展合力，产业依旧处于较为分散的状态。建议从行业层面成立智能网联汽车信息安全产业联盟，统筹智能网联汽车信息安全产业达成共识，促进智能网联汽车信息安全产业健康有序发展。

2、加快智能网联汽车网络安全防护技术突破

关键共性基础技术成为智能网联汽车信息安全产业发展的基础支撑，如安全

通信技术、安全检测技术、安全认证技术、安全芯片技术、安全运营技术等。建议行业内相关企业根据自身优势，充分理解智能网联汽车应用场景及发展趋势，共同攻关关键共性基础技术，为行业发展提供技术保障。加大对车载智能操作系统、云计算平台、5G 网络的研究投入，促进代码校验、数据容错防护、传输校验以及安全"写保护"等核心技术领域的蓬勃发展，提升智能网联汽车在遇到重大信息安全事件时的应急处理能力。加强对网络加密技术、可信计算技术、终端设备认证技术的研究保证终端设备的可信度，防止非认证终端接入汽车进而对汽车的安全构成威胁。

3、提高智能网联汽车的网络安全保障水平

加快构建复杂通信环境下高效可靠的检测保护和响应恢复系统。通过对多域分层入侵检测和主动防护的信息安全模型的研究，建立无线通信安全防护与攻击的协调机制，设计不同安全级别的响应机制和恢复策略，构建针对智能网联汽车的软硬件集成保护体系，形成网联智能汽车"检测保护响应恢复"全生命周期的完整安全体系。

4、保障智能网联汽车的车路协同传输安全

参考智能网联汽车的需求，加快 LTE-V 等通信网络设施建设，推进 5G 通信网络系统的建设，不断优化车道宽度、道路限速等设施参数，提高路侧通信单元的信息化和标准化水平，建设高精度 GPS 定位系统和视频监控系统，利用公有云平台共享测试和监控数据，构建智能化、网联化的智慧路网基础设施。

5、建立健全教育体系与人才培养机制

作为新兴产业，智能网联汽车信息安全产业人才体系与产业发展存在供需矛盾。传统信息安全人才对汽车的理解不足，相比之下汽车人才对信息安全的理解不足，然而智能网联汽车信息安全产业的发展需要既精通信息安全又要深刻理解汽车的相关内容。因此，建立健全智能网联汽车信息安全教育体系以及人才培养机制是当前亟待解决的问题之。建议通过校企合作，建立产学研用闭环人才培养机制，为智能网联汽车信息安全产业源源不断地输送高素质人才。

（四） 整车企业方面

1、提升智能网联汽车信息安全重视程度

智能网联汽车信息安全防护具有全生命周期性特征，但在所有的信息安全环

节中，整车企业担负着系统集成、功能实现、售后维护等职责，是信息安全全生命周期防护中最重要的环节。目前多数整车企业对智能网联汽车信息安全的重视程度不足，还未意识到信息安全对产品以及企业发展的重要性。建议整车企业树立信息安全意识，通过事件复现、信息安全事件攻防等手段提升内部重视程度。

2、将智能网联汽车信息安全开发体系嵌入整车开发流程

整车企业已经建立了相对完善、成熟的整车开发体系和开发流程。目前针对智能网联汽车信息安全的开发流程和体系相对不健全。建议整车企业联合行业相关机构，根据智能网联汽车信息安全的技术特点与要求制定适合智能网联汽车信息安全发展趋势的开发体系和流程，并将该体系融入整车开发流程和体系。

（五） 测试评价方面

1、建立第三方安全测评公共服务平台

近年来，我国对网络安全逐步重视，建立了较为完善的信息安全认证、检测、培训体系。然而，由于智能网联汽车信息安全的特殊性，现有的测试方法和工具难以对其进行有效的测试和认证。建议尽快推进相关服务、测试和认证等制度标准的建立健全，由国家指定的第三方安全评估机构实施智能网联汽车信息安全评估；在现有经认可的信息安全评估机构中增加智能网联汽车信息安全服务，设立专门针对智能网联汽车信息安全的授权评估机构，对车辆内部总线、车载设备、服务平台和移动终端安全等进行全面分析。

2、鼓励开发智能网联汽车信息安全测试工具

智能网联汽车信息安全测试与评价是智能网联汽车安全水平提升的重要驱动力，目前，在智能网联汽车安全检测技术方面，缺乏完善的安全测试方法和专业检测工具，车联网运行过程中产生的数据没有得到有效利用。智能网联汽车的相关服务平台已经具备较多的通用和移动终端测试工具，但对于汽车总线和车载非智能设备的测试工具则仍欠缺成熟的测试方法。因此，建议智能网联汽车信息安全相关企业、测试认证设备企业等研究开发智能网联汽车信息安全相关的专用测试设备。随着智能化的推进，未来的智能网联汽车信息安全防护系统将朝着主动防护、自动检测、智能识别的方向发展，面向智能汽车的自动化检测工具的开发是未来发展的重点内容之一，其发展目标为具备监测、防护的基本功能，实时监控车辆的安全状态，防止攻击者的非法入侵。

II 行业调研

导读：对国家主管部门、行业机构、整车企业、零部件企业、信息安全服务商、检测认证机构及用户相关主体开展调研，基于基本信息、认知程度、现状分析、未来预测及需求分析五个维度，形成了智能网联汽车信息安全调查问卷，并进行了调查结果分析，挖掘不同群体的痛点、诉求及解决方案。

一、智能网联汽车信息安全调研基本信息

1、调研样本归属类型覆盖全面

本次智能网联汽车信息安全调研样本分布较为合理均匀。其中，国家主管部门占比 2%，行业机构占比 21%，车企业占比 22%，零部件企业占比 17%，信息安全服务商占比 11%，检测认证机构占比 16%，用户占比 11%。

2、调研样本地域分布覆盖广

调研群体分布在全国 21 个省、自治区和直辖市。其中重庆市、北京市、江苏省、上海市为样本地域分布排前四的省市，总样本数量达到 168 个，占总样本的 80.8%。从实际来看，这四个地域聚集了国内的成渝汽车产业集群、京津冀汽车产业集群、长三角汽车产业集群，如长安汽车、北汽集团、上汽集团等，具有代表性。

二、智能网联汽车信息安全调研认知程度

1、在认为整车企业对智能网联汽车信息安全重视程度方面，整体来说，调研群体认为整车企业对智能网联汽车信息安全的重视程度较高。

2、在认为零部件企业对智能网联汽车信息安全重视程度方面，22%的认为零部件企业对智能网联汽车信息安全非常重视，29%的认为零部件企业对智能网联汽车信息安全较为重视，37%的认为零部件企业对智能网联汽车信息安全一般重视。

3、认为信息安全服务商能力在一般及以下的占比超过 50%，这说明行业内对信息安全服务商的能力持相对保守和谨慎的态度。

4、认为检测认证机构对智能网联汽车信息安全较为重视及以上的占比为77%，说明行业内对检测认证机构对智能网联汽车信息安全的重视程度认可度较高。

5、用户关注汽车信息安全的驱动力是信息安全产业要重点突出或解决的内容。通过调研发现，驱动用户关注汽车信息安全的因素较为分散，未出现集中分布的现象。

三、智能网联汽车信息安全调研现状分析

1、从智能网联汽车信息安全产业链需要提升的领域排序来看，安全服务技术、安全芯片以及检测认证位列前三，其后依次是整车、零部件及其他。

2、行业组织上各企业针对智能网联汽车信息安全的重视度依然不足，部分企业仍抱着尝试的态度在应对汽车信息安全发展。

3、从国家安全、社会安全以及个人安全的角度考量，未来智能网联汽车信息安全产业仍将以国内企业为主，这也是国家安全可控、自主高效的基本原则。

四、智能网联汽车信息安全调研未来预测

1、通过对行业内相关人员的调研，未来汽车信息安全面临的挑战排序依次为体系安全、黑客攻击、技术迭代、人才培育及其他。

2、80%的行业内人员认为智能网联汽车信息安全会在一定程度上阻碍汽车产业的发展，表现出对智能网联汽车信息安全产业发展的担忧大于乐观。

五、智能网联汽车信息安全调研需求分析

1、用户对智能网联汽车信息安全的最低容忍度阈值不高。这需要整车企业、零部件企业、信息安全服务企业、第三方检测认证机构形成强联动协同机制，保证智能网联汽车信息安全可靠、可信。

2、行业内对信息安全解决方案的需求最大，说明智能网联汽车信息安全是新鲜事物，企业研发经验相对不足，用户希望获取交钥匙性质的全方位的信息安全解决方案。这也从侧面表明了，对于信息安全服务企业，当前阶段全链条服务

是智能网联汽车信息安全的供求方式。

六、智能网联汽车信息安全调研结论

智能网联汽车信息安全产业作为新兴产业，体系不健全、标准不完善、技术不成熟，政府、行业机构、整车企业、零部件企业、信息安全服务商、检测认证机构及用户等相关方还没有形成供需之间的有序配合，产业依旧处于较为分散的形态，未来如何平衡车联网信息安全产业的安全要求与发展节奏成为新的课题。

III产业发展

导读：从安全芯片、关键零部件、安全服务商、整车企业、第三方检测行业等角度介绍了十几年来各主体在产业组织、商业模式、软硬件开发、服务产品、体系与质量保证等方面探索构建信息安全产业生态的实践。

一、智能网联汽车信息安全芯片行业发展分析

安全芯片即安全单元，是一种内部集成了密码算法并具备物理防御攻击设计的集成电路 。安全芯片具有数据的加解密、身份认证鉴权、安全存储密钥的功能和防攻击设计。基于安全芯片全方位、高可靠、功能强大的安全机制，可为各类物联网设备提供身份认证、数据传输加密、敏感信息保护等安全服务。随着汽车的智能化、网联化，汽车内部越来越广泛地使用各类安全芯片。汽车电子应用中的安全芯片又需要具备产品设计“高安全性和高可靠性”、批量生产“高稳定性”的特点。本小节总结安全芯片的关键技术、产品形态和应用，介绍当前国内外主流安全芯片企业的动态，预测未来安全芯片的行业发展趋势，并给出安全芯片产业的发展启示。

芯片内部主要集成了微处理器、程序存储器、数据存储器、数据与程序、安全电路与传感器管理模块、密码运算协处理器等功能部件，根据使用者对芯片性能的不同要求，微处理器的性能、存储器的容量、芯片的性能均有所不同。安全芯片的防御技术主要包括加密算法实现、防侧信道攻击、防故障攻击、防物理攻击、高安全 CPU、存储设备防护和总线防护技术，配合其他软件可实现安全启动、安全存储、身份认证、密码算法实现等功能，可应用于关键组件系统加固、传感器安全防护、T-box 安全隔离、OTA 安全升级、车云通信安全防护、V2X 通信安全防护等场景。

智能安全芯片行业中游企业运营模式主要分为 IDM 模式与 Fabless 模式。IDM 模式，是集 IC 设计、制造、封测甚至下游电子终端产品生产于一体的模式，是早期多数集成电路企业采用的运营模式，代表企业有紫电集团、NXP，英飞凌等；Fabless 模式，只负责芯片的电路设计与销售环节，将生产、测试、封装等环节

向其他企业外包，代表企业有握奇数据、瑞达信安、晨元数据等。由于涉及国家安全，国内的安全芯片行业倾向于生产带国密算法的产品代表性的厂商有华大电子、华虹集成、大唐微电子、同方微电子、天津国芯、国民技术、复旦微电子公司，而智能卡成卡供应商则数量众多，主要有握奇数据、东信和平、华虹、华大、恒宝、明华公司等企业。

随着电子电器在汽车产业的应用范围逐渐扩大，2017-2022 年全球汽车电子市场规模将以 6.7%的复合增速保持增长态势，预计至 2022 年全球市场规模将超过 2 万亿元，而国内市场规模将接近万亿元大关。而技术发展将呈现功能日趋融合、高性能、自主可控等趋势，安全芯片需求开始受到车厂的重视。目前国内厂商紫光同芯、天津国芯、上海芯钦均推出了车规级安全芯片，芯片产品获得 AEC-Q100 认证，应用于 V2X、ECU 控制、车机控市、车载 eSIM、ETC 电子收费等领域，其竞争亦日趋激烈。

随着国际芯片市场竞争的加剧，安全芯片的发展直接关系到国家信息安全，为了国家的“信息主权”研制采用国产密码算法的、自主可控的安全芯片势在必行。从信息技术和控制技术发展的角度来看，物联网应用领域对安全芯片的发展具有极大的战略意义，也是安全芯片未来应用机会最多、潜力最大的主要市场。

二、智能网联汽车信息安全关键零部件行业发展分析

目前汽车零部件主要分为传统汽车零部件与新兴汽车零部件。智能网联汽车信息安全零部件是指汽车内部涉及网络连接与通信数据交互的软件和硬件。从现阶段看，智能网联汽车关键零部件信息安全主要包括车载信息娱乐系统、电子控制单元、域控制器、车载网联通信终端、车载网关、无线通信、App 等方面安全防控。

车载信息娱乐系统是采用车载专用中央处理器、基于车身总线系统和互联网服务形成的一类车载综合信息处理系统，该领域代表性的操作系统有黑莓公司的 QNX、阿里的 YunOS 及百度的小度 OS 等。其面临的主要威胁包括软硬件攻击两方面：一是攻击者可通过软件升级的方式，在升级期间获得访问权限进入目标系统；二是攻击者可拆解 IVI 的众多硬件接口，通过对车载电路进行窃听、逆向等获取 IVI 系统内信息，进而采取更多攻击。因此，其信息安全要求包括硬件安全要求、

通信协议与接口安全要求、操作系统安全要求、应用软件安全要求、数据安全要求等。

电子控制单元由微处理器、存储器、输入/输出接口、模数转换器(A/D)以及整形、驱动等大规模集成电路组成。为了控制总线长度、降低 ECU 数量，分散的小传感器被逐渐集成为功能更强的单个传感器，将分散的控制器按照功能域划分、集成为运算能力更强的域，即将汽车电子系统划分为若干个功能块，每个功能块内部的系统架构以域控制器为主导搭建，利用处理能力更强的多核 CPU/GPU 芯片相对集中地对每个域进行控制，以取代分布式电子电气架构。代表性的 ECU 厂商有 ST 公司、德赛西威、映驰科技和福瑞泰克等。该部件面临的信息安全威胁包括：1）主流的 CAN/CAN-FD 协议具有字节长度有限、仲裁机制不完善、无源地址域和无认证域等问题；2）ECU 硬件可能存在可读丝印和暴露调试口，容易遭受逆向分析等攻击；3）ECU 中的敏感数据在存储、访问过程中，缺少加密存储和访问控制等防护措施，可能导致数据被篡改或泄露；4）ECU 恶意代码植入；5）ECU 虚假信息干扰等问题。

T-BOX 主要用于和后台系统及移动端 App 通信，实现车辆信息的显示与控制，代表性的厂商有博世、大陆、法雷奥、LG、哈曼、联友科技、经纬恒润等。其面临的信息安全威胁包括：1）固件内部代码没有加密等保护措施容易被攻击者利用泄露消息内容；2）部分出厂时会预留调试接口，如果完整分析 T-BOX 的硬件结构、调试引脚、Wi-Fi、系统、串口通信等研究点，就能轻易破解 T-BOX 的软硬件内部信息的保护措施，因此，其应具备的信息安全要求包括数据安全性、固件安全性、OTA 升级安全性等。

网关的主要功能是在网络和 ECU 之间提供安全、无缝的通信，包括在车辆的许多内部网络与外界的外部网络之间建立桥梁，代表性的设备厂商有博士、NXP、TI、恒润科技、芯驰科技等。其面临的信息安全威胁如下：1）利用 CAN、Ethernet 总线路由功能，向车内其他控制器发送非法报文、消息；2）利用 UDS 协议功能，向车内 ECU 进行配置变更、写入恶意代码、读取敏感信息；3）利用 OTA 主控节点功能，非法篡改车内 ECU 固件、获取 OEMIP，使 OTA 功能异常；4）利用关键敏感的车控功能，对车控业务进行恶意决策控制。因此，其应具有机密性、身份认证能力和抗攻击能力。

车载无线通信技术由车载导航模块、车载无线通信模块、安全报警模块、行车状态记录模块、多媒体播放模块、数据采集模块、语音识别模块、地理信息系统模块等八个模块组成，代表性的厂商包括高通、联发科、华为等。其主要存在认证风险、传输风险及协议风险三方面信息安全威胁，因此，其应具备的信息安全要求为信息的真实性与完整性、身份安全性、信息时效性及条件性隐私保护等四点。

智能网联汽车相关的移动终端 App 按照用途可大致分为车控类、查询类、服务类，代表性的 app 厂家包括宝马的 MyBMW App、奔驰的 Mercedes me、Mercedes me Store 和 Mercedes me Service，奥迪汽车的“My Audi” App、比亚迪汽车 app、蔚来 App 等。其面临的信息安全威胁包括客户端安全、数据安全、通信安全及业务安全等；因此，其应具备的信息安全要求为本地数据安全、恶意行为检测上传、用户进行身份标识和鉴别、认证风险检验等。

三、智能网联汽车信息安全服务行业发展分析

信息安全服务的实现要素主要包括服务人才、服务工具及服务流程。其中，服务人才在服务流程的驱动下，使用服务工具协助客户构建体联动的主动安全防御体系，围绕业务活动场景，实现安全监测、预警、分析、响应的运营管理闭环，有效抵御内外部威胁，保障业务安全、稳定地运行。

根据研究内容将信息安全服务场景分为传统场景和新场景。传统场景是指传统 IT 架构下的安全服务场景。新场景主要是指大数据、云计算、物联网、区块链、人工智能、5G 等新技术催生的全新架构下的安全服务场景。在此基础上，对新场景下的新服务、新场景下的传统服务、传统场景下的新服务、传统场景下的传统服务进行了分析，并针对车联网的信息安全服务中的安全测试、安全咨询、安全培训、安全开发、态势感知、应急、响应等内容进行了介绍。

随着全球数字经济快速发展，国外市场的各大公司纷纷加入网络安全服务市场分一杯，包括 Symantec、CrowdStrike、埃森哲、Palo AltoNetworks、Proofpoint 等。国内安全服务市场也持续增长，安全厂商在安全服务领域的布局逐步拓展。在新兴安全服务领域，以安恒信息、绿盟科技、深信服、天融信、启明星辰、山石网科、奇安信、360 等为代表的网络安全厂商凭借自身的前沿技术创新优势，

持续开拓在各自优势领域的安全服务能力。

从信息安全服务行业的市场趋势预测方面，目前中国是世界上除美国以外在网络安全产业支出最多的国家，中国网络安全投入在 IT 行业整体投入中的占比也一直保持着稳步提升。在竞争格局趋势方面，综合型厂商、咨询公司以及电信运营商是欧美安全服务市场的主要参与者，而国内市场则由安全厂商占据主导地位。未来各厂商在渠道资源投入以及渠道管理能力方面的差异将带来其市场份额的此消彼长，需要加大对产业微观层面变化的持续跟踪。

信息安全服务发展启示从服务人才培养体系化、服务流程标准化以及服务平台及工具专业化三方面进行说明。其中，针对服务人才培养体系化，应系统化地建立网络信息安全服务人才体系，构建专业安全服务人才梯队。针对服务流程标准化，为了能够提升市场的竞争力，要不断地创新，基于安全服务的管理流程进行服务模式及服务内容的创新。针对服务平台及工具，新兴安全服务工具除了要满足人才梯队的工作需求外还要符合新兴安全服务的发展趋势，只有这样才能保障新兴安全服务的服务效率和质量。

四、智能网联汽车整车信息安全发展分析

智能网联汽车信息安全是国家安全范畴中重要的领域之一。目前整车的汽车安全不单单是功能安全，还需要考虑到信息安全。由于自动化能力要求的升级，智能网联汽车信息安全需要最少包含“云、管、端”三方面。云端安全主要包括：整车云如 TSP 以及 OTA 服务等，第三方云如零部件厂家的云等，管端安全主要包括 4/5G 蜂窝网络的通信信道、蓝牙、NFC、RFID、Wi-Fi、外部智能硬件等；车端安全主要包括：总线、T-BOX、IVI、OBD 以及终端 App 等。

从整车企业信息安全布局情况来看，国外主要对奔驰、奥迪、宝马、特斯拉、福特汽车、博世、大陆集团等公司的信息安全布局进行介绍，从多方面防护汽车信息安全。在我国整车企业中，主要包括北汽新能源、小鹏汽车、蔚来汽车等，上述企业不仅在合作共赢中优势互补，在信息安全相关建设中也各自积极探索。除此之外，华为、腾讯、百度、360 等各大互联网企业也积极加快车联网和智能网联汽车信息安全相关建设。

随着汽车发展日趋电动化、智能化、自动化，信息安全问题是汽车智能化和

网联化发展的必然产物。为了保证整车安全的更高要求，不仅需要保证车辆的功能安全，也需要保障车云的安全，即车内和车外网络以及云端安全。然而，由于车联网存在技术痛点、人才痛点以及管理痛点，就需自上而下，由内向外去加强技术防护、人才培养以及智能网联汽车信息安全相关的标准体系。

相较于传统的信息安全体系，针对智能网联汽车的信息安全问题，需制定整车企业信息安全发展思路。首先，构建以”检测-保护-响应-恢复”为体系的全生命周期智能网联汽车信息安全体系，以及制定针对智能汽车不同安全等级的响应机制和恢复策略，这是未来智能网联汽车信息安全的主要发展方向。从长远来看，智能网联汽车信息安全已经成为汽车产业甚至全社会关注的焦点，其信息安全防护需要从端、管、云多个角度进行考虑，分析汽车所面临的威胁，加强数据在全生命周期的访问控制，完善车辆使用过程中的身份认证体系，搭建贯通“端管云”三个层面的信息安全主动防护体系。

五、智能网联汽车信息安全第三方检测行业发展分析

智能网联汽车是智能汽车与车联网的结合，随着技术的不断进步，它搭载的车载传感器更为先进、控制器更为智能、执行器更为高效，并且融合了互联网以及通信技术的先进成果。为了应对智能汽车产业兴起带来的信息安全成果以及产生的问题，国内外整车厂都在提升自身的信息安全能力，随着智能网联汽车信息安全相关标准与测试规范的完备，第三方检测机构成为了智能网联汽车信息安全不可或缺的一部分。

第三方检测机构是处于买卖利益之外的第三方，以公正、权威的非当事人身份，根据有关法律、标准或合同进行商品检验活动。独立第三方检测企业能为产业转型升级提供支持，为产业的发展提供强有力的服务平台等。本报告分国内和国外检测机构进行介绍，内容包括各个智能网联汽车信息安全检测机构的主营业务、检测服务及战略方向等。

国外检测机构中 TUV 南德、TUV 莱茵、通标标准技术服务有限公司（SGS）、德凯集团等都有着自己的测试服务。其中，德国 TUV 南德是一家独立的第三方技术服务机构，在汽车工业安全领域有逾百年的经验。TUV 南德专注于汽车信息安全领域，提供测试与认证、技术支持与顾问、知识服务等一站式解决方案。德国

TUV 莱茵提供测试&评估、认证、审核、培训、咨询等服务，在信息安全领域聚焦网络风险管理、智能设备和物联网的隐私与安全、功能安全及信息安全认证等方面。SGS 提供信息安全方面提供云服务认证、EuroPrivacy 数据保护认证、ISO/IEC27001：2013 培训与认证等多维度服务。德凯集团致力于保障信息安全为客户提供定制化的安全评估解决方案。

国内检测机构中，主要介绍了中汽院汽车技术有限公司、中国软件评测中心、中国信息通信研究院、中汽研软件测评(天津)有限公司等公司的背景及测试服务。其中，中汽院汽车技术有限公司是中国汽研的全资子公司，中国汽研是经国家科委批准成立的国家类科研院所，是权威的第三方汽车研发与检测机构。在汽车“新四化”发展趋势下，车联网信息安全成为公司发展的战略方向，已开展多项重要布局。中国软件评测中心是工业和信息化部一类科研事业单位，中国评测承担了多个国家科研项目的研究以及国家产业技术服务平台和重点实验室的建设工作，开发了具有自主知识产权的 30 余种专业测试工具，拥有近百项专利和软件著作权，主持或参与了数十项信息技术领域国家标准和行业标准的制定，具备车载终端信息安全测评、整车信息安全测评、V2X 安全测评、电动汽车通信协议及数据格式一致性及安全测评以及源代码测评等服务。中国信息通信研究院具有丰富的安全评估及评测经验，可提供安全定级、安全评测、风险评估、安全加固等网络信息安全服务。此外，中国信通院打造集操作系统安全检测、应用软件安全检测、信息内容安全检测为一体的远程用户定制多引擎安全测试平台“泰尔安测云”。中汽研软件测评(天津)有限公司提供产品检测、产品及体系认证、产品研发、委托测试、场地服务、品牌推广等一站式综合技术服务，具备国家认监委检验检测机构资质认定(CMA)、中国合格评定国家认可委(CNAS)实验室认可资质。

Ⅳ技术体系

导读：从端管云的基础通信架构入手，围绕感知-控制-决策提出车辆驾驶系统的安全防护技术，并从终端（车辆）安全延伸至应用安全、数据安全领域、前瞻性地提出面向服务的架构、零信任、数字孪生、可信人工智能、联邦学习、隐私计算等前沿技术。

一、智能网联汽车信息安全技术架构

（一）云-管-端技术架构

智能网联汽车的信息安全防护不只是保障车辆本身的信息安全，而是一个由通信、云平台和外部的新兴生态系统组成的整体性生态安全预警和防护。这种安全预警需要长期地进行，需要定期地对整个生态系统做好安全性检测，以便于发现潜在的危害性。因此，智能网联汽车的信息安全整体架构可以依据国际普遍采用的“云”“管”“端”“路侧单元”信息安全架构四个方面进行描述。

云平台肩负着控制指令的下达、信息汇集和存储等重要职责，其中对于信息安全进行防护的手段主要包括：利用成熟云平台安全技术保障车联网服务平台安全；部署云平台集中管控能力，保障云平台数据安全。车联网通信信息安全防护主要针对“车-云”通信，以加强访问控制并开展异常流量监测为主，主要防护手段有：加强车载端访问控制、实施分域管理，降低安全风险；基于 PKI 和通信加密，构建可信“车-云”通信，网络侧进行异常流量监测，提升车联网网络侧信息安全防护能力。

车端的信息安全防护工作主要从硬件安全、操作系统安全、应用安全和对内对外通信安全四个层面开展，主要的防护措施有：利用硬件安全模块，保障车端硬件安全；通过身份权限管理和访问控制机制，保证操作系统层面安全；应用层具备安全更新、抵抗攻击、数据加密存储能力；对内对外通信层面保证数据的保密性、完整性及通信质量。路侧单元信息安全架构主要防护手段包括：对 RSU 配置专用的硬件加密模块并实施通信加密，保障设备安全管理，对 PC5 接口上的 C-V2X 消息认证鉴权以及保障业务功能安全管理。

（二）纵深防御技术架构

对于智能网联汽车的防御可以划分为五个主要的层次分别针对核心控制器、车载内部网络、外部网络接入、V2X 泛在网络通信安全防护以及云端安全持续监控和应急响应。

核心控制器：域控制器的概念最早由以博世、大陆为首的 Tier1 提出，它的出现是为了解决信息安全以及 ECU 瓶颈问题。基于强大的硬件计算能力与丰富的软件接口支持，更多核心功能模块集中于域控制器内，系统功能集成度大大提高，这样对于功能的感知与执行的硬件要求降低。加之数据交互的接口标准化，会让这些零部件变成标准零件，从而降低这部分零部件的开发/制造成本。

车载内部网络：车载内部网络的安全防护主要由汽车网关信息安全和电子控制单元安全通信组成。汽车网关是允许车辆与外界通信的车辆入口点，其不仅与外界通信、提供可靠和安全的无线通信，更重要的是车辆功能和特征的发展也必须通过车辆网关增加各种网络接口。车辆的网关必须能够与所有的独特的协议及其范围跨度很大的不同数据速率进行有效通信。为了达到期望的安全性，单纯的软件解决方案往往是不足的。对于电子控制单元层级的安全而言，硬件安全模块是关键，其能够提高嵌入式系统对更复杂攻击的抵抗能力，并且可以为密钥数据及针对软件篡改提供保护。

外部网络接入：T-BOX 和 IVI 系统通常连接到公共网络域，因此对车载网和信息服务域使用网络隔离来增强安全控制管理是最有效的方法，形成两个具有不同安全级别的访问控制域可以避免未经授权的访问。此外，在车载网中使控制单元和非控制单元被安全地分开，并且为控制单元模块制定更高级别的访问控制策略也是行之有效的方法，增加访问 IP 白名单以避免干扰也是加强网络访问控制的有效方法。

V2X 泛在网络通信：V2X 的设施架构建立在安全、可靠、双向的消息传递的基础上，这些信息通过双重认证在车辆和交通设施之间传递。V2X 技术可提高道路安全性，让车辆能够与其他车辆、道路使用者和道路基础设施进行通信，帮助司机防止道路碰撞并避免危险状况，其主要防护重点包括车云通信的通信链路安全、车车通信的路侧设施安全和人车通信的移动终端安全。

云端安全持续监控和应急响应：当前大多数车联网远程服务与管理系统平台

均采用公有云技术进行云端服务器部署，在享受公有云便利的同时也将云端威胁引入，部署在云端的车联网远程服务与管理系统平台对于自身和依赖环境的安全而言至关重要，需要将传统 IT 防护与车联网应用场景进行有机结合。

二、智能网联汽车信息安全重点技术最新进展

（一）终端安全

计算机终端安全大致分为计算机终端的物理安全和计算机终端的系统安全。计算机终端的物理安全主要就是计算机所在物理环境的安全与计算机自身硬件的安全，而计算机终端的系统安全是针对操作系统的相关技术。面向芯片安全，欧洲整车厂推动成立 ISO26262 标准，该标准已获得汽车界的广泛认可，成为汽车供应链厂商的准入门票。面向系统安全，汽车也将拥有专属的操作系统。根据汽车的需求及实际情况，未来汽车 OS 主要有两种：一种是注重开放性、兼容性，以提高驾驶员驾驶体验的智能座舱 OS，另一种则是更关注汽车驾驶安全，保障汽车稳定驾驶的自动驾驶 OS。

（二）网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。网络安全通常指计算机网络的安全，实际上也可以指计算机通信网络的安全。其主要包括移动通信网络安全、车载通信网络安全、无线通信网络安全、卫星通信网络安全。

（三）应用安全

应用安全即保障应用在运行过程中和输出结果的安全，防止数据在应用运行过程中出现数据错误、被篡改、被泄露等问题。

嵌入式软件安全：随着复杂嵌入式攻击的数量增加，嵌入式系统需要更高水准的安全措施。与标准 PC 不同，嵌入式系统旨在执行一组指定的任务。其同样面临硬件攻击和软件攻击，针对硬件木马的防范主要集中在检测方法上，比如强化功能测试。针对车载终端软件系统的安全对策方面，现有的安全解决方案是从虚拟化、操作系统、应用层和网络传输层几个方面，通过资源、隔离、安全审计、

应用防护和流量加密方案的角度对其进行安全加固。

Web 软件安全：随着科技的发展，社会已进入大数据时代，指数量级的数据在互联网中传播，包括各类敏感数据。因此 Web 安全也成为当今社会信息安全的重点。Web 应用安全漏洞通常可分为服务器端漏洞和客户端漏洞两大类。其面临着注入 Injection、失效的身份认证和会话管理、XML 外部实体(XXE)、安全配置错误和跨站脚本(XSS)等安全问题。目前针对 Web 软件安全的检测和防护方案主要有代码审计、应用防火墙、基于规则的检测技术、基于算法的检测技术、基于自学习的检测技术、蜜罐技术等。

移动 App 软件安全：随着移动互联网的高速发展，越来越多的车型具备了通过手机等移动设备进行远程控制的功能，而针对手机 App 进行远程攻击已经成为黑客入侵汽车的重要手段之一。由于车联网 App 大多数都是基于 Android 平台开发的，依托 Android App 面临的风险威胁介绍车辆 App 所面临的三大安全威胁：恶意代码、二次打包和信息泄露。针对三大安全威胁，现有的检测和防护方法包括应用监控、恶意代码分析、相似性检测、应用沙盒和加固技术等。

（四）数据安全

在互联网通信交互过程中，涉及海量数据的传递，这些数据包含各种各样的重要信息，要保障这些数据的安全，就要保证数据的完整性、可用性和实时性，确保在通信过程中，数据不被篡改、丢失、泄露等。目前针对数据发布安全的技术能够避免链接攻击，同时保证发布数据的完整性。数据匿名技术是指以 K 匿名为基础的一系列数据匿名发布技术，能保证发布数据的真实性和安全性，避免遭受链接攻击而泄露隐私。数据脱敏技术能够去除数据所包含的敏感信息。数据扰乱技术通过添加噪声的方式对原始数据进行随机扰动，使敏感数据失真，但扰动的过程保持数据的统计不变性，以便可继续对其进行统计分析数据有损技术是指通过损失部分数据的方式来保护整个敏感数据集，适用于数据集的全部数据汇总后才构成敏感信息的场景，其中的技术方法有限制返回行数和限制返回列数。

三、前沿技术预见和影响分析

（一）面向服务的架构

面向服务的架构是一种软件架构，也是一种软件设计方法和理念，在 IT 领域已有数十年的应用经验。SOA 具备“松耦合”、“接口标准可访问”和“易于扩展”等特点，使得开发人员能以最小的软件变更应对迭代多变的客户需求。将 SOA 引入当前汽车软件设计中，车辆功能被以面向服务的设计理念架构为不同的服务组件，有别于面向信号的传统架构，SOA 中的每个服务部具有唯一且独立互不影响的身份标识，并通过服务中间件完成自身的发布、对其他服务的订阅以及与其他服务的通信工作。由此，SOA 较好地解决了传统架构中因个别功能增减/变更而导致整个通信矩阵与路由矩阵都要变更的问题。更进一步，由于其“接口标准可访问”的特性，服务组件的部署不再依赖于具体特定的操作系统和编程语言，在一定程度上实现了组件的“软硬分离”。SOA 不仅仅是从技术角度来看的服务体系结构，而且是确保提供和使用正确服务的策略、实践和框架。

（二）零信任

零信任最早是由约翰·金德瓦格（John Kindervag）担任 Forrester Research 副总裁兼首席分析师期间创建的。零信任代表了新一代的网络安全防护理念，它的关键在于打破默认的“信任”，用一句通俗的话来概括就是“持续验证，永不信任”。默认不信任企业网络内外的任何人、设备和系统，基于身份认证和授权重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信。基于零信任原则，可以保障办公系统的三个“安全”：终端安全、链路安全和访问控制安全。

（三）数字孪生

数字孪生是充分利用物理模型、传感器更新、运行历史等数据，集成多学科、多物理量、多尺度、多概率的仿真过程，在虚拟空间中完成映射，从而反映相对应的实体装备的全生命周期过程。相较于设计图纸，数字孪生体最大的特点在于对实体对象的动态仿真。数字孪生体是动态的，它的改变依据来自本体的物理设计模型，还有本体上

传感器反馈的数据，以及本体运行的历史数据。本体的实时状态，还有外界

环境条件，都会复现到“孪生体”上。如果需要做系统设计改动，或者想要知道系统在特殊外部条件下的反应，工程师们可以在孪生体上进行“实验”。这样既避免了对本体的影响，也可以提高效率、节约成本。除此之外，数字孪生还有三个特点，分别是“全生命周期”、“实时/准实时”和“双向”。

（四）可信人工智能

人工智能的内生安全：人工智能系统相似于一般信息系统，难以避免地会存在脆弱性，这种脆弱性被称为人工智能的内生安全问题，一旦这些脆弱性在物理空间暴露，就可能引发安全事故。即使这些脆弱性未暴露，也可能被不法分子恶意利用，从而使得人工智能系统载体具备特定的破坏能力，这种由脆弱性衍生出来的安全问题又被称为人工智能的衍生安全问题。

数据集对算法鲁棒性的影响：有了上述对人工智能内生安全(脆弱性)的基本概念，下文主要以自动驾驶中的人工智能技术为例，说明数据集对它的影响。在自动驾驶的训练过程中，主要考虑训练样本的完备性、均衡性及准确性。训练样本的完备性是说，在自动驾驶场景中，要充分考虑所有可能的驾驶场景以及场景中存在的物体，以防没有被训练到的场景直接被用于真实驾驶中，产生无法识别、识别错误等后果，从而做出错误的决策并引发安全事故。数据集的均衡性是指数据集包含的各种类别的样本在数量上的均衡程度，数据集越均衡，数据样本分布偏差越小，人工智能算法效果越好。数据标注是构建数据集很重要的一步，在这个过程中，如果数据不完整，将导致算法不能正确识别导致严重的后果。

数据投毒与对抗样本：通过上述数据集对算法执行的影响可知，不法分子可以通过对数据集的恶意修改，让人工智能算法学习到错误的数据特征，从而歧化人工智能算法的模型参数，造成算法失效或改变其预期执行结果，这种对人工智能算法训练过程进行的攻击被称为数据投毒。人工智能算法往往需要大量的数据进行学习，数据投毒可以在改变少量样本数据的情况下使神经网络失效。相比于数据投毒，通过对抗样本实施攻击是近年来新出现的一种攻击方法。这种方法在不改变模型参数的情况下，对人工智能算法需要识别的数据加以修改，让算法失效，因此它是对人工智能算法识别过程的攻击。

自动驾驶与法律、伦理：自动驾驶是让汽车通过传感器获得对环境的感知数据，集合人工智能系统算法，自主进行路径选择规划，从而达到无人操控的自动

化驾驶目的。由于自动驾驶所依赖的人工智能系统的固有缺陷，有必要通过政策或法律，对那些有可能影响人类伦理的技术进行严格的管控和必要的限制。首先要考虑的是责任伦理问题，是在对责任主体行为的目的、后果、手段等因素进行全面、系统的伦理考量的基础上，对当代社会的责任关系、责任归因、责任原因及责任目标等进行整体的伦理分析和研究。其次，为最小化人工智能所带来的风险，人工智能系统设计应遵循以下原则：①总是以人类的安全为第一原则，永远不要赋予人工智能载体伤害、破坏或欺骗人类的自主能力，并确保人类对载体的控制；②尊重隐私，注重在后续数据处理时的隐私保护；③可解释与追责，当出现事故时，需要能够识别哪里出了问题，系统正在做什么以及为什么要这样做，并确定谁对该事件负责。

（五）隐私计算

隐私计算(Privacy Cornputing)是一种由两个或多个参与方联合计算的技术和系统，参与方在不泄露各自数据的前提下通过协作对其数据进行联合机器学习和联合分析。隐私计算的参与方既可以是同一机构的不同部门，也可以是不同的机构。在隐私计算框架下，参与方的数据不出本地，在保护数据安全的同时实现多源数据跨域合作，可以破解数据保护与融合应用难题。常见的实现隐私计算的技术路径包括联邦学习、安全多方计算、可信计算等，此外区块链也是隐私计算的重要补充。

V 政策法规

导读：系统介绍国内外在智能网联汽车及网络（数字）安全领域的法律、法规建设进程，并对国内外的技术标准体系做了初步的对标，阐述我国多头启标现状及趋势。

一 国外智能网联汽车信息安全政策及管理体系

（一）国外政策现状

美国在通用网络安全方面最为领先，通过加强立法工作，信息安全保障能力得到进一步提高。美国各州政府累计颁布涉及网络空间安全的法律 50 余部，内容复杂、覆盖面广，涉及网络安全的国家战略以及政府的角色、信息安全共享和跨部门合作、盗取或泄露个人隐私信息数据的违法行为、国际网络安全保护合作、网络安全技术研发等方面。

欧洲现行关于网络安全、信息安全和数据保护等的法律在很大程度上也适用于智能网联汽车领域。2016 年 7 月，欧盟正式通过首部网络安全法《网络与信息系统安全指令》(NISD)，致力于在欧盟范围内实现统一、高水平的网络与信息系统安全，明确了欧盟关于网络安全的顶层制度设计。该法案包括确立网络安全国家战略，强调多方合作与参与，确立网络安全事故与信息分享机制等。

日本作为高度重视人工智能应用、汽车产业发达的国家之一，其基于完善的道路基础设施，通过发展智能交通系统，稳步推进自动驾驶技术商业化，分别于 2013 年、2015 年和 2018 年三次发布《网络安全战略》。2013 年 6 月发布《网络安全战略 2.0》，提出构建信息共享平台、对事件的严重性进行分级分类、风险管理、维护和促进安全守则、增强应急响应能力等。2018 年发布《网络安全战略 3.0》，强调针对物联网设备、关键基础设施和供应链的攻击，汽车被明确纳入物联网系统安全领域。

（二）国外政策趋势

1. 明确强制性信息安全义务，汽车厂商承担主要安全责任

随着汽车智能化水平不断提升，技术的融合性和产品的集成性使得汽车信息安全义务内容更加复杂，安全责任边界和归属却比较模糊。明确安全义务的责任

主体是做好车辆信息安全有效管理的前提。

2. 强调安全主体的自我规制，企业内部组织化措施防范风险

对于作为汽车信息安全责任主体的企业，各国的政策法规均强调从公司内部的组织层面采取制度化的措施防范风险扩散，比如，建立网络安全风险事件信息共享制度、隐患报告披露制度、事故响应程序制度、自我审计与风险评估制度。

3. 注重全生命周期的信息安全管理，全链条多环节合作共治

智能网联汽车产业链涉及汽车、电子信息、交通运输等多个行业，包括整车厂商、软硬件技术供应商、电信运营商、安全服务提供商等多个利益相关方。大量的安全防护对象必然拉长安全防护环节，鉴于此，欧美等国要求将信息安全思维贯穿于整个防护链条。

4. 严格规定安全信息把控方式，重视信息溯源和共享

与一般的网络安全威胁相比，智能网联汽车的信息安全问题所侵害的利益主体不仅是被侵害者的财产和人身安全，更有可能涉及社会安全和国家安全。欧美等国在制定相关法律法规和管理实践过程中，倾向于进行更加严格的规定。文件追溯方面，要求信息安全相关工作用文档记录，包括涉及行为事件、设计方案、分析和关联测试数据等内容的保存完整，以便在发生安全事件后提供给执法机构，作为证据进行追查溯源。

5. 支持安全技术研发与应用，鼓励推广有效技术措施

信息安全技术在智能网联汽车领域的应用面临新的需求，在包括抵御网（攻击、漏洞检测、数据防篡改等基本的安全功能需求外，还有针对汽车功能的需求。要求保障车辆终端安全、车辆间数据传输功能完备以及用户信息安全等。

二 国内智能网联汽车信息安全政策及管理体系

（一）法律依据

我国高度重视信息安全领域的发展，从法律、标准及国家战略等多方面入手，开展信息安全治理，保障所有中国公民的信息安全。《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国电子签名法》等一系列已经出台的法律法规已经初步形成了保障我国公民信息安全的法律体系。我国

于 2016 年颁布《网络安全法》，首次在法律层面构建了个人信息保护法，形成了较为完整的法律制度闭环。2018 年，《电子商务法》在《网络安全法》基础上，在个人信息保护方面做了更加细致的要求，要求经营者对于用户查询、更正、删除用户信息以及用户注册的方式和程序进行明示，不得设置不合理的条件使上述权益无法实现等。此外，备受关注的《数据安全法》在 2021 年 6 月 10 日第十三届全国人民代表 大会常务委员会第二十九次会议通过，《个人信息保护法》在 2021 年 8 月 20 日全国人民代表大会常务委员会通过。此外，我国还颁布了针对智能汽车信息安全的相关法规《汽车数据安全管理若干规定（试行）》，与其他多部法律法规中的相关要求互相补充，总体实现了对汽车终端安全、云平台安全、网络安全、信息数据安全等方面的覆盖。

（二）顶层战略和管理体系

最近几年由于世界各地先后曝出信息安全事件，我国政府对信息安全防护的重视度逐渐提升，政策支持力度也不断加大。信息安全成为“十三五”规划重点建设方向之一，我国《网络安全法》《数据安全法》《个人信息保护法》对数据安全、个人信息保护等问题做出了规定，行业数据安全相关法规和指导性文件也逐步落地，《国家网络空间安全战略》《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。负责制定国内智能网联汽车信息安全相关的标准体系、跟进国际标准化工作的汽车信息安全工作组于 2016 年 4 月成立，隶属于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会。2017 年 4 月，工信部发布《汽车产业中长期发展规划》，提出加快网络信息安全和车辆行驶安全保障体系建设，其中重要目标和任务之一是保证智能网联汽车的信息安全，防止智能网联汽车安全威胁。

我国汽车产业信息安全意识处于起步阶段，汽车制造商和用户不了解如何确保信息安全，自身安全防护能力薄弱。随着《汽车数据安全管理若干规定（试行）》的出台，现有的智能网联汽车数据保护立法体系逐步完善，但当前智能网联汽车信息安全测试评价标准体系和技术要求不能促进企业在信息安全方面的进步，也无法有效验证产品和服务的安全性，尚不能够完全满足智能网联汽车产业迅速发展的需要。由于缺乏标准化的安全标准和测试程序，公司根据自己的理解进行规划和实践，无法预测、感知、监控、报告和发布智能车辆的安全风险。

总体来看，我国亟待加强智能网联汽车信息安全管理，预计远期政府将着重加强智能网联汽车信息安全政策体系顶层设计，推进各职能部门统筹协调，开展道路测试示范、推动技术研发、完善标准法规、突破法律障碍等工作，推动智能网联汽车产业可持续健康发展。

VI专题

导读：围绕 V2X 直连通信的通信安全体系这一行业共性技术难题提出解决方案，并就智能网联汽车测试评价体系的基本框架、产品评测方法、人员认证培训展开介绍，并分享典型案例等。

一 V2X 身份认证与安全通信体系

（一）V2X 安全需求

V2X 安全需求主要分为三个部分：直连通信安全防护、通信系统认证管理和通信系统持续监测。

在直连通信安全防护需求方面，要充分平衡信息完整性、真实性的防护和隐私保护。同时，还要结合 V2X 通信的高移动性的特点，以及低时延的要求，系统全面地构建 V2X 安全认证防护体系。

在通信系统认证管理需求方面，在对交通参与者签发证书的时候，要根据参与者的身份进行确权，从证书的类型上对其权限进行区别。执行确权操作、签发证书的功能需要分配给相应的主体并定义相关的流程。此外，还需要通过设定证书的有效期等方式，对参与者所赋予的权限进行时效管理；需要各种匿名化技术对参与者的隐私信息进行保护；需要通过证书撤销的机制限制已经具有 V2X 通信功能的参与者。

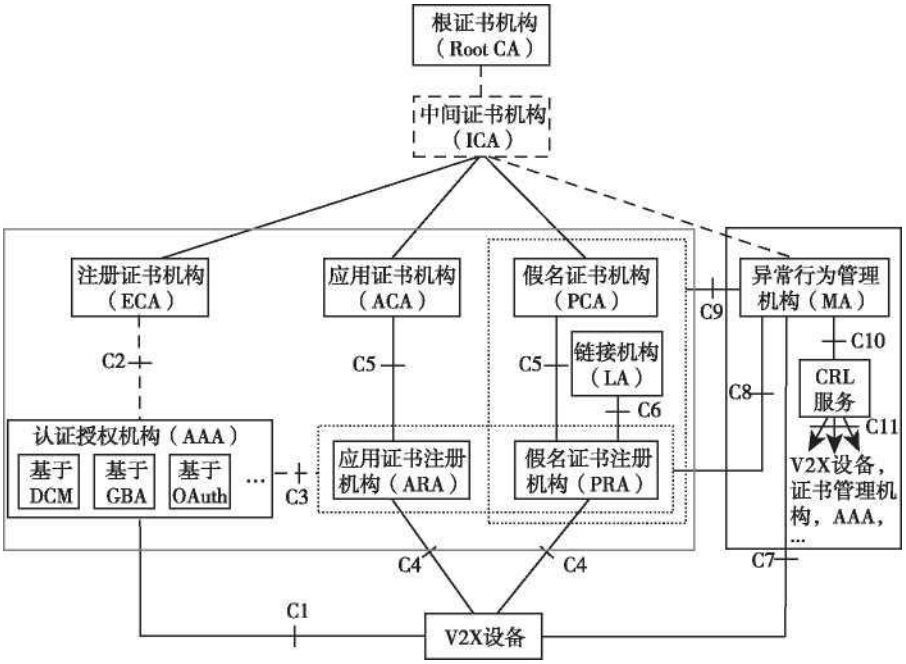
在通信系统持续监测需求方面，V2X 通信系统需要通过技术措施保护消息的安全性。在 V2X 安全系统中需要部署一种能够检测网络中异常行为终端的机制，检测具有异常行为的车辆，阻止其负面影响并确保 V2X 功能的长期可靠。

（二）V2X 安全认证与管理体系

1. V2X 安全认证管理体系

CCSA 的 YD/T 3957 -2021《基于 LTE 的车联网无线通信技术安全证书管理系统技术要求》明确了 V2X 安全管理体系架构，如图 1 所示。图中左侧框内系统组件，实现对 V2X 设备进行数字证书签发的功能，从而该设备能够参与 V2X 通信；而右侧框内的组件，主要实现的是对参与 V2X 通信的设备进行监测，发现判定异

常行为并进行相应处置的组件。这两部分互相配合，形成 V2X 安全管理的闭环，确保 V2X 安全通信系统能够持续安全地正常工作。



V2X 安全管理体系架构

2. 亟待解决的问题

通过总结实践经验发现，目前 V2X 安全认证与管理体系在支撑 V2X 市场化方面还存在一些亟待解决的问题，主要集中在以下三个方面：

一是使用哪一种安全认证系统顶层信任机制才能更有效地实现跨根互认；二是未来对于行驶在路上的具有 V2X 功能的车辆，如何进行监测，以 确保其按照预期的方式正常工作，是否存在异常行为，是否会干扰到其他车辆正常的 V2X 通信；三是具有 V2X 功能的车辆需要通过哪些测试才能进入市场。V2X 测试评判所关注的层面和具体的测试项都可能对技术实现起到引导作用，需要慎重考虑。

（三） V2X 安全认证系统顶层信任机制和异常行为管理

1. 集中式信任体系

在各行业根之上，部署全局根 CA，所有的子 CA 都在同一个根 CA 下管理，形成完整的证书链，建立集中式信任体系。由全局根 CA 签发各行业根 CA 证书，各行业根 CA 再签发各自行业内的子 CA 证书。

2. 分布式信任体系

在分布式 CA 认证架构中，不同 CA 之间通过 CTL 实现交叉认证。CTL 包含全部受信任 CA 的证书，用于传达信任关系，取代基于证书链的交叉认证方式。可

基于选举人机制由多个选举者共同维护 CTL，也可由专门的信任管理机构创建 CTL，建立多 CA 之间的信任关系。信任管理机构在新增、更新和撤销根 CA 证书时对 CTL 进行更新，使用信任管理机构的签名私钥对 CTL 进行签名，并通过专用通道将 CTL 下发至信任域内所有信任体。

3. 异常行为管理

异常行为管理机构主要负责接收上报的异常行为报告，分析、识别系统中的异常行为者，然后形成对异常行为者的处置建议，如吊销证书等。在 V2X 异常管理的初期，异常行为管理机构主要通过接收来自车辆的上报，后续可能进一步拓展为与其他云端的态势感知系统进行联动，全面地对车联网进行监测和响应。识别异常行为需要定义一些特征和检测方法，包括异常行为实例、报告机制和流程，从而进一步规划响应的方式，如定义需要被撤销证书的异常行为。

二 智能网联汽车信息安全技术要求

（一）车身网络安全

通过 CAN 节点、CAN 网络通信、CAN 网关和对外接口通信四个层面的安全防护来加固车辆 CAN 网络信息安全，防止汽车 CAN 网络因受监听、篡改、重放、注入等攻击导致汽车关键信息泄露及影响行车安全。需要从车辆电子电气架构设计阶段就开始考虑，而且必须在车辆的整个生命周期中进行维护。

CAN 节点安全方面，需提高 CAN 节点自身的完整性和可靠性，尽可能降低 CAN 节点被入侵或者破坏的风险，防止因 CAN 节点自身的软硬件设计缺陷而对整个 CAN 网络的信息安全构成威胁。

CAN 网络通信安全方面，需保证 CAN 网络上传输数据的完整性和可用性需求，防止通 信数据被篡改、伪造、重放。

CAN 网关安全方面，需实现外部威胁与车内 CAN 网络的安全隔离，采用网络分段 与隔离技术、路由控制与边界控制等手段提升车内信息交互的安全性。

对外接口通信安全方面，需通过双向身份认证、资源访问控制和完整性检查等技术增强 信息交互的可用性和完整性，实现车内 CAN 网络与外部接入设备或者网络的安全连接。

（二）T-BOX 安全

T-Box 被称为与云端通信的桥梁，主要功能是提供 OBD、MCU/CPU、 FLASH、SENSOR、GPS、3G/4G、Wi-Fi/蓝牙等模块，实现车辆和云平台 之间的通信。它与车辆内部总线相连，通过云平台连接手机/PC。T-Box 提供远程控制、远程访问、安全服务，如远程控制门窗和空调、远程定位车辆、搜索车辆状况、紧急救护等。为保护车载通信终端安全，其目标与安全要求主要体现在硬件、操作系统、应用、数据、通信等五大方面。

（三） 信息平台安全

车联网信息服务平台是面向汽车产业网联化、自动化、智能化需求，利用无线通信网络、互联网等信息通信技术，为车辆驾乘人员以及行业管理等提供的信息服务，支撑汽车和交通服务新模式、新业态的信息服务平台。车联网信息服务平台的体系架构，可以归纳为基础设施、平台和应用服务三个层次。

三 智能网联汽车信息安全测试评价分析

（一）智能网联汽车信息安全评测概述

评测是由评价机构证明产品、管理体系等符合强制性要求或相关技术规范标准的合格评定活动。汽车的信息安全评测应该面向目前行业信息安全威胁，针对汽车上下游企业信息 安全管理体系、产品及人员开展信息安全评测。

信息安全管理体系评测方面，提供了针对组织的信息安全状况的客观证据。通过信息安全管理体系评测，可以向监管机构、客户、合作伙伴等表明组织已经遵守了所使用的标准法规，已充分管理风险，增强相关方信心。

产品评测方面，通过一个统一的、标准化的部件级和整车级的信息安全评测，可以统一各厂商之间对信息安全水平的认知、减少产品间的互操作性问题、增强政府与市场对智能网联汽车相关产品信息安全性的信任度，以促进智能网联汽车行业的发展。

人员认证方面，《网络安全法》明确提出应设立专门的关键信息基础设施安全管理人员并对负责人和关键岗位人员进行安全背景审查、网络安全教育和技术考核等。通过人员信息安全能力认证，可以为组织提供对内部人员能力判别的统一标准，并为不同组织间的人才互认提供基准。

（二）外智能网联汽车信息安全评测现状

国际上针对信息安全管理体系(Cyber Security Management System，CSMS)的认证，目的是从信息安全的流程体系上评估企业的信息安全保障能力，在法规要求中，对信息安全管理体系的要求涉及开发阶段、生产阶段、后生产阶段的组织管理流程、风险管控流程、供应链管理流程、应急响应流程等。

产品评测方面，汽车信息安全产品评测指信息安全型式认证，是针对 OEM 的信息安全 开发中具体的工作项进行审查，即从技术实现上审查汽车信息安全风险是否被识别和有效管控。在实际进行信息安全型式评测工作时，主要包括内容：1. 信息安全对象识别；2. 威胁分析和风险评估；3. 信息安全需求及架构设计；4. 信息安全解决方案设计；5. 信息安全测试验证；6. 信息安全入侵检测及应急响应方案。

（三）智能网联汽车信息安全管理体系和产品测评参考

管理体系方面，国际标准 ISO/IEC 27001：2013 是国际标准化组织

(International Standards Organization, ISO)在 2013 年发布的信息安全管理体系的“要求" 部分,也是整个 ISO/IEC 27000 信息安全管理体系标准族的基础。我国在 2016 年等同采用该标准,并以国标 GB/T 22080 -2016 的形式正式颁布,用于指导国内组织建立、实施、维护和持续改进自身的信息安全管理体系。

产品评测方面,重点是审核汽车主机厂在车辆的全生命周期内是否按照评测标准的要求完成相应的工作。目前国际标准化组织(ISO)和汽车工业协会(SAE)联合全球范围内共 82 家组织/公司共同制定道路车辆信息安全标准 ISO/SAE 21434。该标准的核心在于定义合理的车辆和系统的安全目标,提供以风险为导向的设计分析方法,通过制定适用于车辆全生命周期 的信息安全工程任务及管理活动来保证车辆的信息安全。

(四)智能网联汽车信息安全人员资质认证

目前国内外信息安全人员资格认证类型基本是针对传统互联网及 IT 行业,已有层次化并契合各岗位需求的信息安全人员资格认证,但国内外的信息安全人员资格认证并不能完全符合汽车行业要求,而目前国内外也没有信息安全专业人员资格认证标准/法规能够满足汽车行业需求。

根据国际信息安全人员资格认证类型的调研,人员认证可分为注册信息系统安全师(CISSP)、信息系统审计师(CISA)、国际注册信息安全经理(CISM)、Security +、ISO 27001 Foundation 认证等 5 种类型。

根据国内信息安全人员资格认证类型的调研结果,目前主要由中国信息安全产品测评认证中心(以下简称“国测”)实施国家认证,国测实施认证的主要有国家注册信息安全专业人员(CAP)、国家注册渗透测试工程师(CISP-PTE)、国家注册信息系统审计师(CISP-A)、注册信息安全员(CISM)、信息安全开发人员(CISD)和信息安全保障人员(CISAW)等 6 种类型。

(五)智能网联汽车信息安全评测展望

1.简化评测流程、减轻企业负担

未来在智能网联汽车信息安全评测体系建设过程中,在保证评测充分性的基础上,需考虑汽车产业的复杂性,借鉴国外先进经验,降低评测流程的复杂度,减轻企业负担,提高整体的评测效率。

2.评测标准统一、评测结果互认

当前智能网联汽车信息安全标准还不够完善，而标准是智能网联汽车信息安全评测的依据，因此需要尽快出台智能网联汽车行业公认的信息安全标准，并作为信息安全评测体系建设的基础。检测认证机构作为智能网联汽车信息安全评测的实施机构，需要严格把控对标准解读的准确性，确保信息安全检测评测结果的一致性。

3. 探索自我评测、辅以市场抽查

随着整个评测体系的完善、汽车主机厂能力的提升，在条件成熟后可以效仿美国汽车行业实行“自我认证”，即汽车主机厂按照法规的要求进行自我检查和验证。

（六）智能网联汽车信息安全评测建议

1. 政府主管部门应加强顶层设计，构建国家信息安全评测体系

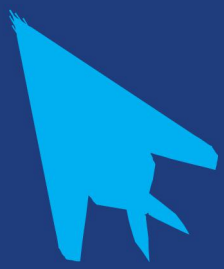
建议政府建设国家级智能网联汽车信息安全评测体系。该体系由政府部门统一监管，采用行业所公认的评测标准，授权具有资质和检测认证能力的评测机构开展认证工作，认证结果在可供全社会查询的平台上发布。国家级智能网联汽车信息安全认证体系的建设，可避免重复认证带来的资源浪费，在全行业内建立统一的信息安全基准。

2. 企业应按照标准要求研发产品，积极获得信息安全评测

汽车主机厂作为汽车通信系统的应用者，担负着为智能网联汽车信息安全产品把关的责任。汽车零部件供应商则需要积极响应整车企业的信息安全需求，制定整体方针，并按照这一方针在各个阶段实施连贯的信息安全对策。

3. 第三方机构应加强能力建设，为行业提供多维度服务

第三方检测认证机构作为智能网联汽车信息安全检测认证的主要实施单位，需要着力于突破安全检测核心技术，充分挖掘创新资源，大力开展智能网联汽车的车端安全、外接终端安全、平台安全、通信安全以及数据安全等前瞻技术研究"同时要加强跨部门、跨领域测试评价机构协同配合，建立权威的车联网安全测试评价体系，重点研发零部件级、系统级、整车级的安全测试评价系统。同时，第三方信息安全服务机构应提升漏洞数据的有效管理能力。国家应推动第三方检测认证机构能力建设，建立智能网联汽车信息安全检测中心。



联系方式

中国汽研·北京分院
地址：北京市通州区兴光三街 3 号
电话：010-81506203/6100
网址：www.caeribeijing.com