WAIC | WORLD ARTIFICIAL INTELLIGENCE CONFERENCE
2019世界人工智能大会

智能网联汽车产业趋势与安全挑战

SIGSI
赛博研究院

版权声明

出品方：

上海赛博网络安全产业创新研究院

咨询专家：

孟海华，上海科学学所副研究员

范昌琪，上海市移动互联网产业促进中心主任

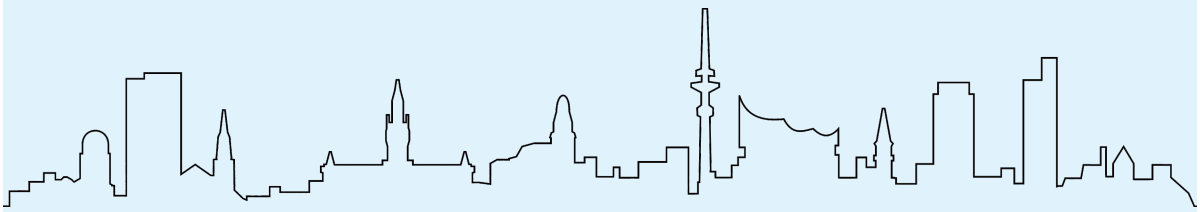
目录

引言

当前，全球汽车产业向着联网化、智能化、绿色化、共享化、无人（驾驶）化等方向全速迈进，智能网联汽车融合汽车制造、IT/通讯、出行服务等诸多产业，经济价值巨大，产业生态丰富，带动效应明显，是全球各国科技与经济竞争的主战场。根据麦肯锡研究报告预测，智能网联汽车产业生态链在2025年的经济规模可达到1.9万亿美元，我国将是全球智能网联汽车产业发展的重要推动者和受益者。

2018年12月25日，工业和信息化部印发《车联网(智能网联汽车)产业发展行动计划》，提出到2020年，实现车联网（智能网联汽车）产业跨行业融合取得突破，具备高级别自动驾驶功能的智能网联汽车实现特定场景规模应用，车联网综合应用体系基本构建，适应产业发展的政策法规、标准规范和安全保障体系初步建立。这为我国智能网联汽车产业发展确定了清晰目标，也将进一步加快推动产业发展。

然而，在当前自动驾驶等技术仍不成熟的阶段，智能网联汽车仍面临功能安全、网络安全、数据安全、隐私安全等众多安全挑战，亟待产业界各方全力协助，共同致力于为公众提供安全、可靠、便捷的产品和服务。本报告对全球智能网联汽车产业发展趋势、安全挑战、安全应对进行了全面梳理和分析，并提出了促进产业安全发展的建议，以期为政策制定者、产业界以及监管部门提供参考。



1、智能网联汽车内涵与系统组成

智能网联汽车是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与X（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、舒适、节能”行驶，并最终可实现替代人来操作的新一代汽车。

智能网联汽车由环境感知系统、智能决策系统和控制执行系统组成。其中环境感知系统通过激光雷达、毫米波雷达、摄像头等车载环境感知技术，高精度定位技术，以及V2X通信技术，实现对车辆位置信息、车辆行驶数据、车辆周边道路环境的全方位感知与信息收集，为智能决策系统提供所需的各类数据。智能决策系统基于由智能汽车芯片、操作系统、算法等组成的计算平台，对环境感知系统输入的各类信息进行处理和分析，判断和决策车辆的驾驶模式和下一步要执行的操作，并将操作指令发送给控制执行系统。控制执行系统包括两个方面，一方面线控制动系统基于智能决策系统的指令完成对车辆的转向、制动、加速等控制，实现车辆安全行驶，另一方面人机交互系统向乘客提供车辆信息、道路交通信息、安全信息以及娱乐、办公、消费等信息服务，实现出行与生活服务的打通。

智能网联汽车功能的实现需要汽车制造商、零部件供应商、车载计算平台开发商、出行服务供应商等多方主体参与，因此，智能网联汽车的产业链较长，具体而言，上游包括感知系统、通信系统、决策系统、控制系统等，中游包括智能驾驶舱、自动驾驶解决方案等，下游包括出行服务、物流服务等，其中感知系统又包括摄像头、激光雷达、高精度地图、高精度定位等，决策系统又包括计算平台、芯片、操作系统、算法等。

2、智能网联汽车产业发展趋势

2.1 ICT产业与汽车产业竞合态势加剧

纵观全球智能网联汽车产业链形态，呈现出整车厂、主机厂、关键零部件厂商、互联网/IT巨头、通信业巨头、网约车服务商、新车企等“多轮驱动”的态势，持续塑造着全球智能网联汽车产业发展格局。

一方面，传统车企和关键零部件厂商从现有汽车技术体系出发，通过掌控传感器、控制器和执行器研发设计的核心价值环节，配合感知和机器决策技术以高级驾驶辅助系统（ADAS）为关键路径过渡到自动驾驶和无人驾驶，目前国内外主流车企均已推出智能汽车产品和规划，博世、大陆、德尔福、电装等汽车零部件供应商加强技术创新，为用户提供自动驾驶、汽车互联、人机交互等系统性解决方案。另一方面，谷歌、苹果、特斯拉、百度、阿里等网络科技企业，依托云计算、人工智能、高精度地图、激光雷达、协同式环境感知系统等技术，试图颠覆传统汽车产业形态，重新定义汽车商业价值。由于智能网联汽车高度依赖通信网络设施，华为、爱立信和诺基亚等通信设备商以及运营商积极加入产业布局。

由于传统车企、关键零部件厂商、网络科技企业、通信设备商、网络运营商等在智能网联汽车产业化发展中各自具有不可替代的优势，传统汽车产业与网络科技产业的竞争与合作也在不断深化，智能网联汽车产业呈现出“合纵连横”态势，例如在2019上海车展期间，华为与沃尔沃汽车、上汽荣威、ARCFOX、宁德时代等多家主机厂和零部件配套企业开启战略合作，提供ICT基础设施建设和智能化服务，呈现出通信企业与汽车厂商之间不断增强的紧密合作。此外，宝马集团在2019年7月宣布与中国联通、腾讯和四维图新3家国内科技公司签约合作，与中国联通和四维图新将分别就5G移动通讯以及高精度地图开展合作，与腾讯将合作建立宝马集团在中国的“高性能数据驱动开发平台”。表明全新的产业生态正在快速形成。

2.2 “软件定义汽车”时代全面来临

“软件定义汽车”（Software Defined Vehicle，SDV）成为汽车产业的共识和趋势，软件将成为未来汽车中至关重要的部分。根据美国电气和电子工程师协会报告，上世纪80年代初一辆轿车的电子系统只有5万行代码，而现在高端豪华汽车的电子系统就有6500万行程序代码，提升了1300倍；根据摩根斯坦利估算，未来自动驾驶汽车60%的价值将源于软件，车控软件、嵌入式操作系统、自动驾驶软件、娱乐系统、办公系统等软件生态将不断丰富成熟，极大地提升智能网联汽车性能和用户体验。例如，特斯拉通过采用与传统汽车不同的集中式电子电气架构，即通过自主研发底层操作系统，并使用中央处理器对不同的域处理器和ECU进行统一管理，可实现汽车像智能手机一样采用在线方式进行软件升级（Over The Air，OTA），持续改进车辆功能和用户体验，赋予汽车更多生命力。2018年6月，特斯拉就曾通过OTA空中升级将Model 3的刹车距离缩短接近20英尺。

此外，大众集团是“软件定义汽车”概念的积极拥护者，大众集团CEO赫伯特·迪斯在2018年上任后进行“大刀阔斧”改革，指出软件将占未来汽车创新的90%，汽车将转变为软件产品，大众必须成为一家软件驱动型的汽车公司，并宣布成立“Digital Car&Service”部门，使大众汽车集团成为全球范围内第一家将汽车硬件开发和软件开发彻底分离的车企。2018年11月，大众集团还宣布对位于德国斯图加特的软件公司Diconium进行战略投资，并收购该公司49%的股份，以帮助其开发OTA、流媒体平台、停车应用等数据增值服务。2019年6月，大众又宣布2025年前其所有新车型都将使用vw.OS汽车操作系统，并搭载大众与微软合作的汽车云服务。

2.3 汽车智能芯片门槛高市场竞争激烈

智能网联汽车芯片可以高效实现感应、控制、执行、决策、通信、导航等功能，是智能网联汽车的关键核心部件。根据IC Insights测算，2018年全球车载芯片市场规模达到323亿美元，同比增长18.5%，到2021年，汽车芯片市场规模约436亿美元，复合增速位居芯片六大主要终端应用市场之首。目前，全球智能车载芯片技术壁垒较高，主要供应商均在国外，包括恩智浦NXP、英飞凌、意法半导体、瑞萨等传统的汽车芯片供应商，也有纷纷布局车载芯片领域的老牌芯片企业如高通、英特尔、三星、英伟达等，部分整车厂如特斯拉、现代汽车等也在加紧布局汽车智能芯片。国内汽车智能芯片起步较晚，但近年发展迅猛，包括华为、百度、四维图新、地平线、寒武纪、阿里平头哥等开始全面布局汽车智能芯片，例如华为于2019年初推出全球首个支持V2X的多模芯片巴龙5000，7月底阿里平头哥推出玄铁910，可用于设计制造高性能端上芯片，应用于5G、人工智能以及自动驾驶等领域。

表1 汽车智能芯片发展态势

时间	企业名称	事件	相关信息
2019.7	阿里平头哥	推出玄铁 910	可用于设计制造高性能端上芯片，应用于 5G、人工智能以及自动驾驶等领域。
2019.7	英特尔	发布“Pohoiki Beach”芯片系统	该系统主要由 Loihi 神经拟态芯片构成，可处理深度学习任务，速度比 CPU 快 1000 倍，效率高 10000 倍，耗电量小 100 倍，可应用于自动驾驶汽车。
2019.7	丰田、电装	两家公司同意成立一家合资企业，专注于开发下一代汽车半导体芯片	新公司将于 2020 年 4 月成立，投资额约为 5000 万日元(约合 45.90 万美元)。电装将持有合资企业 51% 的股份，剩余股份将由丰田持有。
2019.4	特斯拉	发布完全自动驾驶计算机芯片	首席执行官埃隆·马斯克称这款计算机 “客观来说是全球最好的芯片”。
2019.1	华为	推出全球首个支持 V2X 的多模芯片巴龙 5000	巴龙 5000 不同于之前发布的 “巴龙系列芯片”，这款芯片体积小、集成度高，能够同时实现 2G、3G、4G 和 5G 多种网络模式，具备能耗更低、延迟更短等特性。
2019.1	三星	联合奥迪正式推出旗下首款自动驾驶汽车芯片 Exynos Auto V9	Exynos Auto V9 专为高级信息娱乐系统而设计。芯片本身基于三星自家的 8nm 工艺制造，内置8个 ARM 最新的 Cortex-A76 CPU 内核，最高主频可达到 2.1GHz。除此之外还集成了ARM Mali G76 GPU、高级 HiFi 4 数字音频处理芯片以及独立的 NPU 处理单元。
2019.1	高通	宣布推出第三代高通骁龙汽车驾驶座平台芯片	以骁龙 820A 为基础，支持沉浸式图像、多媒体、机器视觉，以及 AI 等功能，并且将产品分成 Performance、Premier 与 Paramount 三种等级，分别针对入门、中阶，以及超级运算平台使用。此外，该平台设计是以模组化架构为基础，让汽车制造商可向消费者提供多种定制化选择。
2018.9	ARM	ARM 面向汽车自动驾驶领域推出 Cortex-A76AE 芯片	该芯片增强了自动驾驶汽车在安全方面的性能，如自动躲避功能，根据 ARM 方面表示，首批使用该芯片的自动驾驶汽车将于 2020 年上市。

2.4 汽车大数据/云计算市场需求空前巨大

智能网联汽车从研发、生产、运营、服务等全生命周期均需要采集、存储和处理海量实时的数据资源。按照行业的初略估算，一辆新车每天能产生20GB的数据，未来拥有更强自动驾驶能力的汽车，预计每秒就能产生10GB的数据，除了车载本身需要强大的存储设施来共享处理工作负载，云端数据中心也将提供进一步的存储、处理和分析，除了汽车制造商，还有保险公司、高精地图厂商、运营服务商等多元化的客户需求。智能网联汽车产业的云计算/大数据服务需求被全面打开，例如2018年9月，大众汽车宣布与微软Azure合作为联网汽车打造全新的“大众汽车自动化云”，阿里、百度、华为等针对智能网联汽车推出专业化汽车云服务。

2.5 5G+C-V2X赋能汽车通信迈入新台阶

全球范围内V2X车联网通信技术进入加速研发和测试阶段，高通、华为、三星、沃达丰、爱立信等各大通信商联合车企、汽车零部件厂商不断深化合作，加紧C-V2X等技术快速落地和商业化应用。同时随着2019年5G加速进入预商用阶段，将赋能C-V2X技术实现突破性进展，C-V2X也将成为5G的先导性应用。5G是实现车联网的重要条件，其高速率、低时延、高可靠、低功耗、大连接等特点将带来更智能的车路协同、更安全的自动驾驶和更丰富的乘车服务。2018年12月工信部印发的《车联网（智能网联汽车）产业发展行动计划》提出，2020年后，5G-V2X逐步实现规模化商业应用。目前，国内已经启用多条5G自动驾驶测试道路，加速推动5G在智能网联汽车领域率先落地。

- 2018年9月，中国移动发布国内第一条5G自动驾驶车辆测试道路，与目前国内封闭的自动驾驶道路不同，位于北京市房山区高端制造业基地的5G自动驾驶车辆测试道路完全开放，道路可提供5G自动驾驶所需的5G网络、5G边缘计算平台、5G-V2X能力、5G高精度定位能力。
- 2019年1月，重庆市自动驾驶测试道路（九龙坡区）启用，可测试车辆在5G环境下对于“危险场景预警”“连续信号灯下的绿波通行”“路测智能融合感知”“高精度地图下载”“5G视频直播”和“基于5G的车辆远程控制”等场景的应对能力。
- 2019年7月，柳州市政府宣布正式启用全球首条集成5G、V2X、无人驾驶、远程驾控四项前沿技术的公开测试道路。

2019年7月，华为的5G+C-V2X车载通信技术被评为全球新能源汽车创新技术，基于该技术，华为研发出全球首款5G车载模组MH5000。该模组不仅让车载终端具备高速率、低延时的5G移动通信能力，还可以同时具备车路协同的C-V2X通信能力，加快汽车行业进入5G时代。

2.6 新业态加速塑造全新汽车服务生态圈

随着汽车继智能手机之后成为下一个需求旺盛的移动智能设备，以汽车为中心的智能互联全域生态正在快速形成。各大互联网科技公司加紧围绕数字感知、智能交互、个性服务、新零售等新业态、新模式打造全新汽车互联生态圈。例如斑马智行基于AliOS汽车专属操作系统，通过超级账号打通互联网世界，致力于为用户提供便捷的一体化系统服务，斑马智行目前已连接停车、加油、车品、维保、救援、支付、车险等10大类出行生态，并已和10个汽车品牌合作，涉及30+车型。2019年6月新推出的斑马智行系统MARS（V3.0），除去2.0版本已有的情景式智能语音控制、加油站智能推荐及自动支付、美食智能推荐与订位、停车场无感支付、智慧车险服务等功能以外，又新增基于“AI场景引擎、地图智慧引擎、语音融合引擎”的28项新功能，真正将出行生态服务串联起来。

2.7 高级别自动驾驶在部分场景加速落地

自动驾驶是智能联网汽车的关键技术，高级别自动驾驶（L4及以上）将彻底变革出行服务模式，推动汽车行业真正实现智能化、自动化、共享化，为人类提供完全不同的出行体验。但目前L4级自动驾驶技术在全球范围内都处于测试阶段，由于法规的不完善，以及安全性能仍待大幅度提高，L4级自动驾驶汽车真正在环境复杂的城市道路上实现落地仍需较长时间。然而，在某些行驶环境相对简单、行驶速度较慢并且容错率高的特定场景中，高级别自动驾驶车辆正快速落地商用，例如封闭园区、物流仓储、机场摆渡等场景。这不仅能解决此类场景中的各种需求，还能推动高级别自动驾驶技术的快速成熟。例如2019年7月，新加坡国立大学的无人驾驶小型电动巴士开始在校园内试行免费载客；2019年5月17日，宇通客车打造的具备智能交互、自主巡航、车路协同等功能的L4级宇通自动驾驶公交车开始落地试运行；2018年7月百度宣布其研制的全球首款L4级别自动驾驶汽车阿波龙小巴车已量产下线。

2.8 国内外智能网联汽车法规相继落地

当前各国为促进智能网联汽车技术发展，在充分考虑安全因素的基础上，都纷纷制定了智能网联汽车相关法规，并加速推动有利于产业发展的法律法规的制定。

目前，全球范围内智能网联道路测试规范已经趋于成熟。美、日、欧、韩、中等国家和地区都已制定自动驾驶车辆道路测试管理规范，其中美国内达华州早在2011年就率先制定相关法规、发放测试牌照，随后，美国加利福尼亚州、佛罗里达州、密歇根州、纽约州等多个州先后允许自动驾驶汽车进行道路测试。法国于2016年通过了允许自动驾驶汽车道路测试的法令，英国于2015年发布自动驾驶道路测试指南，允许在封闭道路测试后使用公共道路进行测试。德国2017年也通过其国内首个自动驾驶相关法律，允许企业和科研机构在公共道路上进行自动驾驶汽车测试。此外，日本2016年颁布《自动驾驶汽车道路测试指南》,开始允许自动驾驶汽车道路测试试验。在我国，2018年4月工信部、公安部、交通运输部联合制定《智能网联汽车道路测试管理规范（试行）》，对智能网联汽车道路测试申请、审核、管理以及测试主体、测试驾驶人和测试车辆要求等进行全面规范。截至目前，我国已有约20个城市出台了智能网联汽车道路测试管理规范，并且各地方省市正逐步加大高速公路测试开放力度。

目前，出于安全考虑，国内外大部分自动驾驶道路测试法规都要求自动驾驶汽车测试时必须配备经过严格培训的测试人员，强制要求测试主体在测试前购买相关保险，必须通过封闭道路测试验证后方可在公共和开放道路上进行测试。但也不乏有部分国家和地区尝试放宽智能网联汽车上路条件，为产业发展创造更为宽松的法规环境。例如美国加州和佛罗里达州都已出台自动驾驶测试法规，允许未配备安全驾驶员的自动驾驶汽车在公共道路上进行测试。

3、智能网联汽车产业安全挑战

智能网联汽车产业链长、行业跨度大、防护界面众多，安全问题复杂敏感，涉及功能安全、软件质量、网络安全、数据安全、隐私保护等诸多方面。近年来，宝马、奔驰、大众、特斯拉等国际大牌智能汽车厂商接连被爆漏洞威胁，远程攻击、恶意控制甚至入网车辆被操控等安全隐患日益突出，Uber、谷歌等自动驾驶测试车辆频频发生安全事故，这都为智能网联汽车产业发展蒙上了阴影。

3.1 智能化导致的功能安全挑战

“智能”是智能网联汽车最核心的功能之一，其中自动驾驶是实现“智能”的关键技术，能够解放驾驶员的手脚，提高驾驶的安全性，减少安全事故发生。然而，在当前阶段，由于技术仍不成熟，加载自动驾驶功能的智能网联汽车在功能安全方面仍存在重大隐患。

智能网联汽车是由感知系统、决策系统、执行系统等软硬件组成的计算机系统代替人类来完成驾驶任务，其安全性依赖于各个组件的可靠性以及协同性。在当前机器学习、计算机视觉等人工智能技术发展仍不成熟的阶段，智能网联汽车的感知准确性、决策可靠性以及控制系统的执行力都仍达不到安全上路的要求，可能出现感知和判断失误，导致安全事故发生。其次，智能网联汽车的设计、研发、测试必须考虑到众多复杂路况、恶劣环境、夜间行车等因素，只有考虑到所有可能发生的情况，才能在真实城市道路场景中运行时保障自身和其他车辆、行人的安全。然而，目前所有厂商都达不到上述安全要求。

截至目前，特斯拉、谷歌Waymo、Uber等公司研制的智能网联汽车在上路测试过程中都曾因自动驾驶系统识别或决策失误导致交通事故的发生。例如2017年8月Waymo公司的自动驾驶测试车辆在加州发生交通事故，事故原因为Waymo自动驾驶汽车前方的另一辆车辆因紧急避让物体进行转向，导致Waymo车辆对这一意外情况未能及时做出反应，紧急情况下测试驾驶员接管了车辆并向右转弯。但在这一过程中，Waymo自动驾驶汽车与另一辆汽车发生了碰撞。再如，Uber公司的自动驾驶汽车曾在2018年3月造成一名推着自行车穿过街道的行人死亡，车辆的自动驾驶系统虽然在事故发生前探测到了受害行人，但并没有立刻做出反应，因此导致了事故的发生。

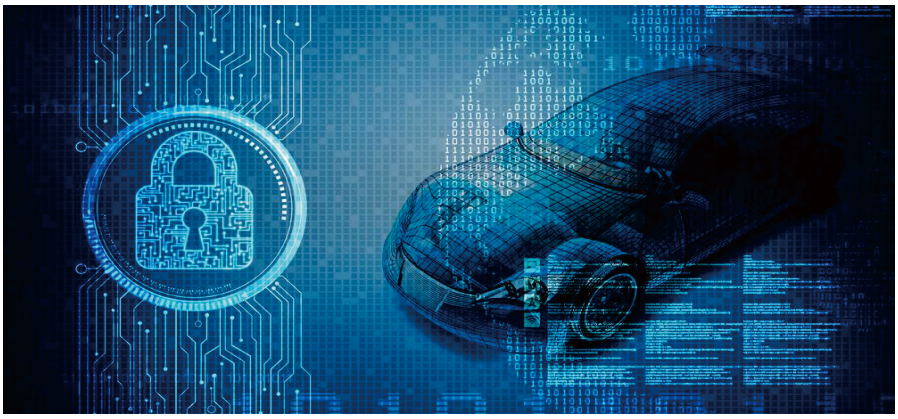
3.2 网联化导致的网络安全挑战

随着汽车产业向着网联化的方向不断发展，车辆本身已从封闭的系统变成了开放的系统，智能网联汽车将逐渐成为像手机一样的智能终端设备。当汽车成为网络空间的一个组成部分，也像其他任何联网的电子设备和计算机系统一样，成为黑客攻击的目标，面临严峻的网络安全挑战。近几年针对汽车的众多攻击事例表明，黑客攻击不仅会造成数据和隐私泄露，还能通过接管和控制车辆驾驶系统，给驾乘人员带来重大的人身和财产安全隐患。

例如早在2015年，两名白帽黑客就通过远程入侵一辆正在路上行驶的切诺基，对其做出减速、关闭引擎、突然制动或者制动失灵等操控，这次事件造成克莱斯勒公司在全球召回了140万辆车并安装了相应补丁。2016年，腾讯科恩实验室的安全专家也利用安全漏洞以“远程无物理接触”的方式成功入侵了特斯拉汽车，实现了对特斯拉驻车状态和行驶状态下的远程控制，可以做到在行驶中突然打开后备箱、关闭后视镜及突然刹车等远程控制。2019年4月，腾讯科恩实验室发布报告显示，利用特斯拉Autopilot自动辅助驾驶系统存在的缺陷，通过欺骗Autopilot系统，可以实现让车辆驶入反向车道；即使Autopilot系统没有被车主主动开启，黑客利用已知漏洞获取Autopilot控制权之后，也可以利用Autopilot功能实现通过游戏手柄对车辆行驶方向进行操控。

此外，汽车安全漏洞不仅会对用户的人身和财产安全构成威胁，还有可能造成城市交通瘫痪，给社会公共安全管理带来治理挑战。例如，佐治亚理工学院的研究人员通过数学模型分析发现，在交通高峰期，只要20%的汽车被黑客入侵导致熄火，就能有效地让城市交通瘫痪，并导致交通事故、人员伤亡等城市混乱，而救护车和消防车也因交通停滞而无法赶到。虽然让数百万辆汽车同时遭到协同攻击具有一定的技术难度，但这项研究成果显示了汽车网络安全风险可能导致的严重后果。

随着车联网的发展，智能网联汽车受到的攻击面越来越广泛。例如，黑客可通过车联网云平台、移动APP、OTA空中软件升级、车载T-BOX、车载信息娱乐系统、车载诊断系统接口、V2X车路通信等环节和节点存在的漏洞实现对车辆的盗窃或控制车辆驾驶系统。



3.3 服务化导致的数据隐私安全挑战

与传统汽车相比，智能网联汽车不断增强的智能化程度以及不断延展的服务模式将导致其采集和处理的数据数量和种类都急剧增长。首先，智能网联汽车的安全运行建立在收集大量数据的基础上，此外，智能网联汽车的行驶过程也因网联化会附带产生各种类型的数据。

具体而言，智能网联汽车采集和处理的数据包括两大类：一类数据不具有个体属性，属于车辆智能行驶所依赖的数据，包括感知、决策、执行所需的周边环境数据、道路路况数据、车辆操作数据、车辆行驶数据等；另一类是与用户相关的数据，包括车辆位置数据、车辆行驶轨迹、用户驾驶习惯数据、车内摄像头采集的车内乘客数据、语音交互系统采集的乘客语音数据、车载系统记录的加油等支付数据、餐厅预定信息，以及用户的上班地点和家庭住址等等，涉及用户大量隐私信息。

第一类数据虽不涉及用户隐私，但往往对于汽车制造商而言也是极具价值的一类数据，可以用于持续改进感知、决策、执行等自动驾驶系统性能，并可提供宝贵的高精地图数据，因此这类数据普遍会回传给汽车制造商。但目前针对这类数据的权属问题仍存在较大争议。第二类数据包含大量用户隐私信息，并且除共享给汽车厂商外，还涉及其他第三方服务商等用于个性化推送、精准营销、汽车保险等数据增值服务，这些数据的采集和使用将涉及用户隐私安全问题，智能网联汽车产业链中诸多主体环节都面临严峻的合规挑战。例如，蔚来汽车研发的智能网联电动汽车就曾在隐私防护方面饱受用户质疑。

此外，涉及外资汽车制造商或第三方服务商的情况还存在数据跨境传输的安全评估问题，包括涉国家安全的地图信息、地理位置信息、用户群体信息等，都面临数据跨境传输的合规性挑战。

4、智能网联汽车安全挑战应对

4.1 政策措施

4.1.1 国外政策措施

当前，全球多个国家针对智能网联汽车安全出台了相关指南等政策性文件，旨在规范智能网联汽车安全评估、安全测试，保障智能网联汽车的安全性。

1. 联合国

在国际层面，联合国世界车辆法规协调论坛（WP29）在加紧制定智能网联汽车安全性相关的法规，并成立了专门的智能网联汽车法规工作组（GRVA），主要聚焦智能网联汽车的安全评估办法、网络安全、以及数据存储系统等方面。2019年6月，在日内瓦举行的联合国WP.29第178次全体会议审议通过了中国、欧盟、日本和美国共同提出的《自动驾驶汽车框架文件》[1]，该框架文件明确了L3及更高级别的自动驾驶汽车的安全性和安全防护的关键原则，包括系统安全、失效保护响应、人机操作界面、目标事件探测与响应、设计适用范围、系统安全验证、网络安全、软件更新、事件数据记录仪、防撞性、碰撞后自动驾驶汽车行为等方面。

2.美国

美国交通运输部和美国国家公路交通安全管理局（NHTSA）2016年9月颁布《联邦自动驾驶汽车政策指南》[2]，要求汽车制造厂商对自动驾驶汽车上路进行全面的安全评估，并针对自动驾驶汽车的设计和研发提出多项安全规范，包括自动驾驶系统如何探测道路环境、如何将道路信息展示给驾驶人、如何应对技术失灵等紧急情况、如何保证联网系统的网络安全以及隐私安全等方面。在此基础上，2017年9月，美国交通部联合NHTSA发布更新版的自动驾驶汽车指南《自动驾驶系统：安全愿景2.0》[3]，确定了十余项安全性能自评标准，包括系统安全、设计适用范围、退出机制、人机交互界面、汽车网络安全、耐撞性等。这些标准是非强制的，企业可以据此提交安全评估报告。2018年10月，美国交通部又发布新版联邦自动驾驶汽车指导文件《自动驾驶汽车3.0：为未来交通做准备》[4]，再次明确强调自动驾驶测试必须在安全第一的原则下展开，并在原有指南的基础上对自动驾驶范围进行了延伸，涵盖客车、大众交通运输工具、卡车等所有地面道路交通系统。

---

1 Proposal for amendments to ECE/TRANS/WP.29/2019/34
Framework document on automated/autonomous vehicles (levels 3 and higher)
www.unece.org › DAM › trans › doc › WP.29-178-10r2e.docx
2 Federal Automated Vehicles Policy - September 2016
https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016
3 Automated Driving Systems2.0: A Vision for Safety
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
4 Preparing for the Future of Transportation: Automated Vehicle 3.0
https://www.transportation.gov/av/3

此外，2017年9月美国众议院表决通过《自动驾驶法案（Self Drive Act）》[5]，要求自动驾驶汽车生产商或者系统提供商向监管部门提交安全评估证明，以证明其自动驾驶汽车在数据、产品、功能等各个方面采取了足够的安全措施，并要求自动驾驶车辆厂商必须制定网络安全计划，包括如何应对网络攻击、未授权入侵以及虚假或者恶意控制指令等安全策略，且必须制定隐私保护计划，包括对车主以及乘客信息的搜集、保存、使用等方面的保护措施。法案还要求NHTSA逐步完善包括自动驾驶汽车在内的汽车安全标准或者安全范围，包括自动驾驶汽车的基本元素如人机交互界面、传感器、促动器、相关软件和网络安全要求等。随后，美国参议院议员也提出《自动驾驶汽车法案（AV START Act）》[6]，要求汽车制造商在测试、销售前提交自动驾驶汽车安全评估报告，并对网络安全、隐私保护提出了明确要求。

3.欧盟

欧洲网络与信息安全局（ENISA）在2016年12月发布了《智能汽车的网络安全与弹性：最佳实践和建议》报告，在系统分析智能汽车面临的风险和威胁的基础上，为企业建立网络安全防御能力提供了指引。此外，欧盟也正积极在成员国之间建立自动驾驶安全法规方面的共识。2019年2月，欧盟成员国达成共识，共同签定自动驾驶指导文件，确定了8项原则，其核心是如何定义自动驾驶车辆的安全，包括系统性能、驾驶任务的转换、行驶数据记录、网络安全及安全评估测试等。

4.英国

针对智能网联汽车网络安全，英国政府2017年8月发布《网联汽车和自动驾驶汽车的网络安全关键原则》[7]，提出包括加强企业内部网络安全管理、安全风险评估与管理、产品售后服务与应急响应机制、整体安全性要求、系统设计、软件安全管理、数据安全、弹性设计在内的 8 项关键原则。随后，在英国交通部和英国国家网络安全中心以及众多汽车企业的支持下，英国标准协会于2018年12月发布《汽车网络安全基本原则》[8]，英国由此成为首个发布此类标准的国家。

5.日本

2018年9月日本国土交通省正式对外发布了《自动驾驶汽车安全技术指南》，明确规定了L3、L4级自动驾驶汽车所必须满足的一系列安全条件，包括设计运行范围(ODD)的设定、自动驾驶系统安全性、人机界面、搭载数据记录装置、网络安全、用于无人驾驶移动服务的车辆安全性、安全性评估等，目标是打造一个自动驾驶系统引发的人身事故为零的社会。

---

5 H.R.3388 - SELF DRIVE Act
https://www.congress.gov/bill/115th-congress/house-bill/3388
6 S.1885 - AV START Act
https://www.congress.gov/bill/115th-congress/senate-bill/1885
7 The key principles of vehicle cyber security for connected and automated vehicles
https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles
8 The fundamental principles of automotive cyber security. Specification
https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

表2 国外智能网联汽车安全相关法规指南列表

国别	发布时间	发布机构	法规指南名称
联合国	2019 年 6 月	联合国世界车辆法规协调论坛（WP29）	《自动驾驶汽车框架文件》
美国	2016 年 9 月	美国交通运输部、美国国家公路交通安全管理局（NHTSA）	《联邦自动驾驶汽车政策指南》
	2017 年 3 月	美国参议院	《汽车安全与隐私法案》[9]
	2017 年 9 月	美国交通运输部、美国国家公路交通安全管理局（NHTSA）	《自动驾驶系统：安全愿景 2.0》
	2017 年 9 月	美国众议院	《自动驾驶法案（Self Drive Act）》
	2017 年 9 月	美国参议院	《自动驾驶汽车法案（ AV START Act）》
	2018 年 10 月	美国交通部	《自动驾驶汽车 3.0：为未来交通做准备》
欧盟	2016 年 4 月	欧洲交通安全委员会	《将自动驾驶安全作为优先事项》[10]
	2016 年 12 月	欧洲网络与信息安全局（ENISA）	《智能汽车的网络安全与弹性：最佳实践和建议》[11]
	2019 年 2 月	欧盟成员国	签署自动驾驶指导文件
英国	2017 年 8 月	英国国家基础设施保护中心、英国交通部、英国智能网联汽车中心	《网联汽车和自动驾驶汽车的网络安全关键原则》
	2018 年 12 月	英国标准协会	《汽车网络安全基本原则》
德国	2017 年 9 月	德国交通和数字基础设施部伦理委员会	《自动驾驶系统编程指导原则》[12]
日本	2018 年 9 月	日本国土交通省	《自动驾驶汽车安全技术指南》

9 https://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf
10 https://etsc.eu/wp-content/uploads/2016_automated_driving_briefing_final.pdf
11 Cyber Security and Resilience of smart cars
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
12 Germany Drafts World's First Ethical Guidelines for Self-Driving Cars
https://futurism.com/germany-drafts-worlds-first-ethical-guidelines-for-self-driving-cars

4.1.2 我国政策措施

我国已于2018年4月正式成立全国汽车标准化技术委员会智能网联汽车分技术委员会，主要负责汽车驾驶环境感知与预警、驾驶辅助、自动驾驶以及与汽车驾驶直接相关的车载信息服务领域国家标准制修订工作，目前智能网联汽车分标委下已设立先进驾驶辅助系统（ADAS）标准工作组、自动驾驶(AD)工作组、汽车信息安全标准工作组、汽车功能安全标准工作组和网联功能及应用工作组，开展各细分领域标准的研究制定工作。在功能安全方面，《智能网联汽车人机交互系统失效保护要求及评价方法》、《汽车交互接口功能安全要求》、《汽车信息感知系统功能安全要求》、《汽车决策预警系统功能安全要求》、《汽车辅助控制系统功能安全要求》等标准正在加紧研制中。在网络安全方面，《汽车信息安全通用技术要求》、《汽车信息安全风险评估要求》、《汽车数据保护安全和隐私保护通用要求》等标准已在制定过程中。此外，全国信息安全标准化技术委员会等标准制定机构也在加紧研制智能网联汽车信息安全标准，目前已发布《信息安全技术 汽车电子系统网络安全指南》（征求意见稿）。

2019年5月工信部发布《2019年智能网联汽车标准化工作要点》，要求组织开展特定条件下自动驾驶功能测试方法及要求等标准的立项，启动自动驾驶数据记录、驾驶员接管能力识别及驾驶任务接管等行业急需标准的预研。此外，要求有序推进汽车信息安全标准制定，完成汽车信息安全通用技术、车载网关、信息交互系统、电动汽车远程管理与服务、电动汽车充电等基础通用及行业急需标准的制定，研究提出汽车软件升级、信息安全风险评估等应用类标准的立项，系统开展汽车整车及零部件信息安全测试评价体系研究。

表3 目前我国在研的智能网联汽车安全标准列表

分类	标准名称
功能安全	智能网联汽车人机交互系统失效保护要求及评价方法
	汽车交互接口功能安全要求
	汽车信息感知系统功能安全要求
	汽车决策预警系统功能安全要求
	汽车辅助控制系统功能安全要求
网络安全	汽车信息安全通用技术要求
	汽车信息安全风险评估指南
	汽车数据保护安全和隐私保护通用要求
	车载操作系统及应用软件安全防护要求
	汽车信息安全通用测试与评价方法
	汽车信息感知设备安全技术要求
	车载 ECU 信息安全技术要求
	车载总线系统信息安全技术要求
	汽车网关信息安全技术要求
	车载信息交互系统（TBOX）信息安全技术要求
	车载诊断接口（OBD）信息安全技术要求
	驾驶员身份认证系统技术要求
	汽车软件升级信息安全防护规范
	电动汽车远程信息服务与管理系统信息安全技术要求
	电动汽车充电系统信息安全技术要求
	汽车信息安全漏洞应急响应指南

4.2 产业实践

4.2.1 产业界将安全融入设计和开发环节

产业界各方积极应对智能网联汽车安全挑战，在产品设计、研发环节充分考虑功能安全、网络安全、隐私保护等方面，力求为客户和用户提供安全可靠的智能网联汽车整车和汽车零部件。

例如，英伟达作为智能网联汽车智能芯片和计算平台等软硬件供应商，通过将在系统中引入冗余和多样性作为安全基本原则，致力于使智能网联汽车的可靠性和安全性达到尽可能高的水平。英伟达在设计自动驾驶处理器和计算平台的架构，以及设计用于自动驾驶和高精度定位的算法时，都应用了这一安全原则，例如英伟达提供了高性能计算所需的冗余传感器、多样的算法以及附加的诊断功能，以支持更安全的运行。具体而言，英伟达为汽车配备了多种类型的冗余传感器，并在集成GPU、CPU、深度学习加速器(DLAs)和可编程视觉加速器(PVAs)的硬件上运行了多种不同的人工智能深度神经网络和算法，用于感知、定位和路径规划，以实现尽可能安全的驾驶。2019年3月，英伟达还为其自动驾驶计算平台推出一个可避免车辆碰撞的新组件“安全力场”（Safety Force Field），该功能可以作为一种独立的手段监督车辆的路径规划和控制策略，如果发现行车安全威胁将会否决并纠正主系统的决策。此外，针对网络安全，英伟达专门建立了网络安全团队，在其系统设计中采用了严格的安全开发生命周期，以及覆盖整个自主驾驶系统（包括硬件、软件、制造和IT基础设施）的威胁模型，为NVIDIA DRIVE自动驾驶计算平台建立了多层防御。英伟达还成立了专门的产品安全事件响应团队，负责管理、调查和协调企业内部和合作伙伴的安全漏洞信息。

通用汽车也在智能驾驶汽车设计、开发、制造、测试和验证的各个环节都将安全内嵌其中。与英伟达类似，通用汽车也将多样性和冗余视为安全的重要保障，例如通用汽车的Cruise AV智能网联汽车装配了两套同时运行的计算系统，配备了激光雷达和惯性跟踪系统等多种定位方法，还为所有重要系统装配了冗余电源和配电，计算机、传感器和执行器之间的通信也配备了冗余路径。针对网络安全，通用汽车也组建了内部的网络安全团队，负责分析和解决所有车内控制系统、移动应用程序和车内应用程序的网络安全问题，并与其他开发团队一起将“设计即安全”原则运用到产品开发环节，在产品中嵌入设备注册、消息验证、安全编程和诊断，以及入侵检测和防御系统等安全功能。2018年4月，通用汽车推出安全漏洞悬赏计划，对能够发现其车辆产品和服务中的网络安全漏洞的研究人员进行奖励。

此外，Waymo、福特汽车、Nuro、Uber等公司也都积极应对各类安全挑战，并已经按照《自动驾驶系统：安全愿景2.0》指南要求向美国国家公路交通安全管理局（NHTSA）提交了自动驾驶安全报告。

国内汽车企业的网络安全意识也明显提升，百度2018年4月启动网络安全实验室，负责为自动驾驶汽车开发安全解决方案，2018年11月发布一站式汽车信息安全解决方案，可解决黑客攻击和隐私泄露等安全问题。长安汽车、比亚迪、蔚来汽车也纷纷建立信息安全部门，或通过与网络安全厂商加强合作，提升产品网络安全防御能力。

4.2.2 积极组建安全联盟共同应对安全挑战

为应对网络安全威胁，2015年美国汽车制造商联盟（Auto Alliance）、美国汽车贸易协会（Global Automakers）和14家汽车制造商共同发起成立了汽车信息共享和分析中心（Auto-ISAC），致力于打造一个共享和分析智能汽车网络安全风险和威胁情报的社区。2016年1月，其建立的网络威胁情报共享平台正式启用，为其组织成员提供全面的网络安全情报，以帮助成员企业高效应对网络威胁。截至目前，全球已有111家企业加入该中心，包括恩智浦、英特尔、Waymo、大众、丰田、本田、沃尔沃、福特、奔驰、大陆、哈曼、博世、大陆等全球众多知名智能网联汽车制造商、汽车零部件厂商以及汽车芯片厂商。

我国也于2017年5月成立了中国汽车信息共享与分析中心（C-Auto-ISAC），由中国汽车技术研究中心有限公司发起成立，目前已完成70余辆汽车的信息安全能力测试，测试发现存在数据漏洞高达2000个以上，测试涵盖整车信息安全七大攻击入口：网络构架、车载娱乐系统、T-Box、云平台、App、ECU及无线电。

此外，2019年4月全球三大汽车巨头福特、丰田和通用公司宣布组建“自动驾驶汽车安全联盟”，该组织将与美国汽车工程师学会SAE合作，帮助起草自动驾驶汽车的安全标准。三家公司成立该联盟组织的目标是推动自动驾驶汽车企业和政府合作，加快制定安全标准，并最终促进相关法规的出台。

4.2.3 网络安全厂商助力汽车安全挑战应对

国内外网络安全厂商都看到了汽车产业的数字化转型趋势和网联化带来的网络安全风险，纷纷开拓汽车网络安全业务。例如腾讯旗下科恩实验室依靠自身多年的漏洞挖掘经验长期致力于车联网系统的漏洞挖掘与研究；360推出“汽车安全大脑”解决方案，通过监控、分析、响应的动态防御手段，为智能网联汽车的安全运营提供保障。此外，Arxan Technologies、Mocana、Intertrust Technologies等国外安全厂商，亚信安全、梆梆安全、绿盟科技等国内安全厂商都将汽车安全作为新增业务。同时，国外也涌现多家专注于汽车网络安全的初创企业，如GuardKnox、CyMotive等。

表4 国内外开展汽车安全业务的网络安全厂商

企业名称	国别	相关产品和解决方案
Arxan Technologies	美国	推出解决方案保护汽车 App 安全。
Mocana	美国	推出端到端网络安全系统，支持安全的、基于加密签名的空中软件升级(OTA)和固件更新。
Intertrust Technologies	美国	推出汽车数据和隐私安全解决方案。
大陆集团（2017 年收购以色列汽车网络安全公司 Argus）	德国	发布端到端安全解决方案，涵盖电子部件安全、部件间通信安全、车辆与外界接口安全、云端安全等。
哈曼国际（2016 年收购汽车网络安全公司 TowerSec）	美国	推出 HARMAN SHIELD 网络安全解决方案，用于检测、管理、减轻和响应针对联网和自动驾驶车辆的网络攻击。
GuardKnox	以色列	推出 Secure Network Orchestrator™（SNO)网络安全解决方案，利用三层 Communication Lockdown ™ Methodology 技术，该解决方案不需要任何外部联接或更新。
CyMotive	以色列	产品包括：汽车端到端安全通信包、入侵检测系统、网络安全控制平台等。
腾讯科恩实验室	中国	依靠自身多年的漏洞挖掘经验长期致力于车联网系统的漏洞挖掘与研究。
360	中国	推出“汽车安全大脑”解决方案，通过监控、分析、响应的动态防御手段，为智能网联汽车的安全运营提供保障。
亚信安全	中国	车联网安全解决方案
梆梆安全	中国	车载管理信息系统保护、传输数据加密
绿盟科技	中国	已建立面向新能源汽车充电基础设施网络安全检测与防护体系，为电动汽车制造商、充电桩设备厂商、充电运营商等提供新能源汽车充电设施网络安全风险评估与安全检测服务，并对应输出充电基础设施产品级安全防护解决方案。
四维创智	中国	已具备汽车 CAN 总线安全测试、TBOX 安全测试能力。

5、总结与展望

当前，全球范围内进入智能网联汽车快速发展阶段，企业之间跨界融合、产业重构的趋势已经非常明显，产业生态正在快速形成与发展。未来，人工智能、5G、物联网、云计算等新一代信息技术的飞速发展，将在智能网联汽车技术发展中产生巨大协同效应，重塑汽车产业业态和商业模式，为人类出行方式带来根本性变革。

但在当前发展阶段，国内外智能网联汽车厂商尚没有完全构建面向中高级无人驾驶阶段的可信安全体系，无论在功能安全、网络安全，还是数据隐私安全方面，智能网联汽车的安全可靠性都亟待加强。倘若没有安全性的保障，将极大地限制智能网联汽车的普及应用。

为促进我国智能网联汽车产业快速以及安全发展，本报告提出几下建议：

1. 聚焦核心技术打造汽车软件生态体系

瞄准全球智能网联汽车发展的核心技术，加强智能网联汽车关键软件技术研发和产业化。一方面吸引国际重点车企/关键零部件厂商的软件研发部门/项目落地我国智能网联汽车示范区，另一方面重点扶持一批瞄准关键技术的软件企业，加大对汽车相关的感知识别系统、车载操作系统、高精度地图、自动驾驶、人机交互等软件方向的政策支持力度，积极推动优质的软件产品与车企的对接，加强软件适配和应用场景的提供，打造高质量的智能网联汽车软件生态体系。

2. 加快提升智能汽车芯片自主研发能力

智能汽车芯片是汽车实现智能化的关键支撑技术，能为智能网联汽车提供强大的计算能力。在全球各大芯片厂商激烈角逐汽车芯片技术领先地位的背景下，我国应加快推动传感器芯片、自动驾驶芯片、V2X通信芯片、智能驾驶舱芯片等智能网联汽车核心硬件技术发展，依托国内重点智能汽车芯片研发企业及科研院所，实现关键核心技术突破，打造我国智能汽车芯片自主研发能力，为我国智能网联汽车产业快速发展夯实根基。

3. 面向行业打造智能网联汽车云服务平台

智能网联汽车产业为云计算/大数据产业带来重大机遇，云计算/大数据发展也是智能网联汽车产业生态发展的关键枢纽。因此，建议引导华为云、阿里云等龙头企业建设行业级的汽车云服务平台，面向国内外汽车产业各方提供云服务，推动智能网联汽车产业链整体上云，基于云平台/大数据促进大产业链相关方的项目合作和精准对接，做大做强汽车云产业生态，全面支撑我国智能网联汽车产业创新发展。

4. 协同各方构建智能网联汽车产业安全能力

安全是智能网联汽车产业化发展的关键痛点，我国须以安全为核心打造智能网联汽车品牌。建议组建智能网联汽车安全联合攻关平台，加快汽车整车厂商、配件厂商、安全厂商的有序对接，推动智能网联汽车安全技术研发和行业标准建立，构建智能网联汽车安全先进检测能力，并建立覆盖智能网联汽车售前、售后等环节的持续测评机制，保障在产品全生命周期中持续更新安全性能，全面提升我国车企的安全能力和市场竞争力。

SIBEI

赛博研究院