# 建立“动态”管理流程 保证智能网联汽车安全

中国软件评测中心 邹博松 朱科屹 王卉捷

随着汽车智能化、网联化和电动化程度的不断提高，智能网联汽车信息安全问题日益严峻，产业链的各个环节对信息安全的重视程度还远没有达到要求，甚至存在多个环节并没有考虑信息安全需求的情况。因此全面推进智能网联汽车信息安全发展，定期进行安全渗透测试，积极探索信息安全关键技术和产品创新，进一步建立健全智能网联汽车信息安全防护体系至关重要。

智能网联汽车测评工程技术中心（赛迪汽车）组织撰写了《智能网联汽车安全渗透白皮书（2020年）》，从产业发展、安全态势、攻击场景、渗透指标、渗透实践等切入点对智能网联汽车安全总体形势进行分析，提出安全渗透测试指标并基于此进行渗透实践，针对性剖析安全漏洞，提出安全保障建议。

## 智能网联汽车信息安全问题日益严峻

随着汽车信息通信、人工智能、互联网等行业深度融合，智能网联汽车已经进入技术快速演进、产业加速布局的新阶段。IHS Markit数据显示，目前全球市场搭载车联网功能的新车渗透率约为45%，预计至2025年可达到接近60%的市场规模。长期预测，中国智能网联汽车市场将不断增长，至2025年将接近2000万辆，市场渗透率将超过75%以上。

一方面，2019年上市的传统燃油车联网率超过40%，预计2020年后将超过70%，网络技术的普及和不断提升推动了智能网联汽车发展，汽车的联网率增加使得其逐步成为网络攻击重点目标，安全问题风险突出，安全防护基础薄弱。另一方面，工信部车联网动态监测情况显示，2020年以来发现整车企业车联网信息服务提供商等相关企业和平台受到的恶意攻击达到280余万次，平台漏洞、通信劫持、隐私泄露等风险十分严重。威胁由车外进入车内、影响程度加大、网络安全与功能安全要求矛盾等问题层出不穷。

智能网联汽车产业链长、防护界面众多，安全问题复杂，各主体探索建立车联网产业链信息安全分级分类管理模式，明确各自安全的要求也迫在眉睫。

整车企业、互联网企业和安全解决方案提供商纷纷布局汽车安全领域，推出特有的解决方案。整车企业携手网络安全公司，共建智能网联汽车安全实验室，合力推进汽车网络安全检测技术和防护技术的研发。互联网企业依托在传统IT领域的技术沉淀和积累，推出了安全芯片、安全操作系统、安全网关等产品。安全解决方案提供商则在汽车信息安全领域中投入大量测试类产品，通过对车辆自身特性以及网络传输协议的分析，实现对车辆信息安全测试的标准化、工具化、流程化，保障车辆不受外界攻击，提高车辆的安全防护能力。

2020年信息安全十大风险分析了包括不安全的云端接口、未经授权的访问、系统存在的后门、不安全的车载通信等在内的最常见、最危险的汽车信息安全漏洞。近期爆出的安全事件也显示，攻击者一旦利用安全漏洞，便可实现非法访问、敏感数据窃取、远程控制等操作，严重影响驾驶员的行车安全，甚至生命财产安全。为了避免更大的损失，各主体都开始强化在汽车信息安全方面的能力，例如针对现有车型可以开展渗透测试、漏洞挖掘等，依据分析结果和影响危害，设计防护方案以及创新安全技术等。

## 呈融合性、整体性特点

（一）网络安全技术领域扩展，智能网联汽车成为新目标

随着云计算、大数据、车联网等创新技术的逐步应用，新形式网络安全威胁和风险正不断滋生、扩散和叠加。其中，汽车行业的产品、产业的智能化升级是典型代表。智能网联汽车作为搭载先进传感器等装置，融合云、网、路、端、人各要素，涉及信息通信、电子汽车交通等多行业、多领域、多主体，运用人工智能、自动驾驶等新技术的新一代产品，其网络安全问题呈现融合性、整体性特点。

智能化、网联化发展使得汽车面临的网络安全风险不断增大，相较传统互联网，因其应用环境更加特殊、组网更加复杂、管理更加困难，智能网联汽车面临的安全威胁也更加突出。首先，车端威胁复杂。智能网联汽车车端威胁主要涉及车载信息交互系统、车载诊断（OBD）接口、车载网关、车内网络等。车内多个存在攻击风险的脆弱点，引入了众多威胁场景。其次，软件大规模应用。软件重新定义汽车的趋势导致智能网联汽车车内代码量和复杂度激增，漏洞数量也随之增加，给了攻击者更多的可乘之机。最后，与外部连通性增强。车车通信、车路通信、车云通信和短距通信等车内外通信场景为攻击者提供了更多的攻击面，通信安全防护水平参差不齐也极大降低了攻击成本与难度。智能网联汽车功能的大幅增加，导致信息安全接入点和风险点不断暴露，逐渐成为攻击者目标。

（二）产业价值体系正在构建，外部环境安全隐患突出

智能网联汽车产业已进入技术快速演进、产业加速布局的新阶段。2020世界智能网联汽车大会上发布的《智能网联汽车技术路线图2.0》提出的目标是：到2035年智能网联汽车技术和产业体系全面建成，产业生态健全完善，整车智能化水平显著提升，网联式高度自动驾驶汽车大规模应用。新产品、新业态、新模式不断涌现，以智能网联汽车为载体的产业多样化服务伴随着大量信息资产的产生。

随着汽车与外部的互联互通程度不断增强，一旦攻击者利用高危漏洞，除了对本车及车主造成安全威胁，甚至还有可能蔓延至其他车辆，从中获取大量利益，甚至可能威胁公共安全乃至国家安全。近年来智能网联汽车信息安全事件频发，外部环境安全隐患日益突出。根据工信部数据统计，在2019年的专项调研、检测中发现，85%的关键部件存在着安全的漏洞，80%以上的车联网平台和APP存在缺乏身份鉴别、数据明文存储等隐患，近六成企业缺乏自动化的网络安全监测响应能力。Upstream Security的《2020年汽车网络安全汇报》指出，汽车制造行业的互联网攻击快速提升，全行业遭遇的威胁愈来愈广泛。数据显示自2016年到2020年1月，汽车网络安全事件的年安全事故总数提升了605%，仅在2019年就提升了1倍左右。按照目前的发展趋势，随着汽车联网率不断提升，安全问题会更加突出。

（三）数据信息泄露风险加剧，个人信息保护不断加强

智能网联汽车的信息安全危机不仅能够造成个人隐私泄露、企业经济损失、车毁人亡等严重后果，甚至上升成为国家公共安全问题。据统计，有56%的消费者表示，信息安全和隐私保护将成为他们未来购买车辆时主要考虑的因素。由此可见，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。当前，正处于智能网联汽车发展关键时期，强化智能网联汽车的数据及个人信息安全保障已成为当务之急。

## 建立信息安全防护体系 提高产品安全质量

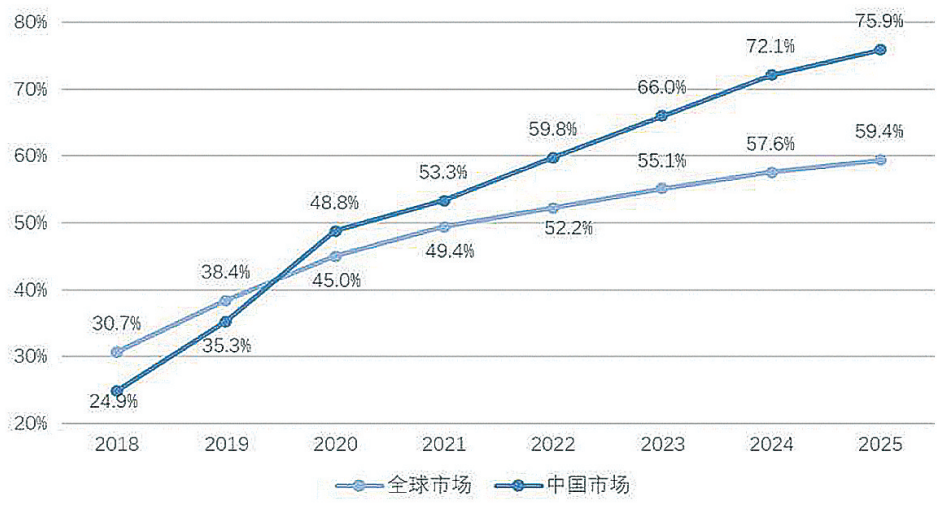
现如今，在互联网时代下的任何行业对于信息安全的基本要求，无论是在团队建设层面、流程管理层面还是技术要求层面，永远都不会过时，智能网联汽车行业也不例外。

组建信息安全团队，明确各主体细分职责。目前很多车联网企业，包括产品服务供应商还没有实现建立专职的技术团队负责设计、实施、运维智能网联汽车信息安全。做到信息安全专业化是任何企业都需要解决的第一步，之后则是细化内部团队工作职责。同时受限于自身成本、技术能力等因素，可以考虑请专业团队开展相关安全解决方案咨询、代码安全加固、整车渗透测试等服务，发挥产业链各主体技术优势，实现资源互补。

“安全左移”，建立“动态”安全管理流程。“安全左移”，即在设计阶段考虑更多安全因素，是降低安全风险、实现低成本高回报的解决办法。随着软件定义汽车的普及，智能网联汽车信息安全逐渐向DevSecOps转变。微软提出的安全开发生命周期（SDL）流程在设计阶段提出安全需求，在验证阶段测试需求是否满足，软件发布后进行应急响应，给出了组建一个从安全需求、防护措施与检测到应急响应的动态安全管理流程的有效思路，构建标准化安全开发全生命周期管理，提高产品安全质量。

“自上而下，由内向外”，加强技术防护。随着智能网联汽车软件化程度逐步上升，加强数据、应用到底层物理硬件“自上而下”的纵向防护愈加重要。同时网联化也伴随着“由内向外”的车辆自身外部接口安全防护及车辆对外通信安全保障需求提升。建议遵循最小权限设计原则，保证应用及服务的用户都只能访问必需的信息或资源；加强操作系统原生安全，选项默认处于开启状态并合理配置；实现纵深防御，将不同安全防护手段应用于智能网联汽车的每个技术层面，提高攻击门槛；减少暴露非必要的接口，裁剪非必要组件，从而减少攻击面。

2018—2025年智能网联汽车渗透率趋势




图片来源：IHS Markit车联市场分析，2020年

# 2021年5G B/G端融合应用规模增长将超200%

赛迪智库无线电管理研究所 彭健 孙美玉

近日，赛迪智库发布了《5G发展2021展望白皮书》。白皮书显示，2021年，我国5G网络建设和产业规模将进一步增长，且增幅将超过2020年度；四大运营商仍将继续布局5G规模组网，并联合企业广泛探索5G融合应用；5G融合应用将使C/B/G多端用户和市场受益，其中工业互联网领域的5G专网建设将率先发力。

## 5G网络建设规模进一步增长

2020年我国5G网络基础建设加快部署，在推动5G在各行业转型升级和融合发展过程中发挥了提质增效的积极作用。虽然新冠肺炎疫情导致5G网络基础设施建设面临一定阻力，但整体建设进度保持了相对稳定的水平。截至2020年9月底，全国已累计建设开通5G基站69万个，超过全球总数的75%，提前完成全年50万个的目标。北京、上海、广州、杭州等城市实现5G网络城区连片覆盖，提前完成了全年的既定目标，保持适度超前的建设态势。与此同时，运营商积极加大5G建设投资。中国移动5G相关投资约1000亿元，是2019年5G建设投资的4倍，截至9月底已提前完成全年30万个建设目标，开通5G基站35万个。中国电信、中国联通分别规划5G相关投资453亿元、350亿元，截至9月底共同建设5G共享基站超过30万个，超前完成前三季度新增共建共享5G基站25万个的目标。中国广电正通过“全国一网”的整合、推动700MHz频段频率迁移等措施，加快5G网络的建设步伐。

2021年5G建设将保持适度超前的态势。业界普遍认为适度超前建设符合公共基础设施的普遍特点，尤其是结合移动通信2G、3G、4G的技术发展规律来看，都实现了支持产业快速成型的目的。2021年四大电信运营商将持续加大5G网络投资力度，预计将是2020年的1.5到2倍。此外，国家和地方对5G基础设施建设都大力支持，部分省市对2020—2022年5G建设计划进行了明确，2022年5G基站建设将会达到一个高潮，2021年保持稳步推进的趋势。

## 5G C/B/G端融合应用市场前景巨大

在前期的5G融合应用试点示范过程中，超高清视频传输和虚拟现实等方面的案例较多，例如近年来的5G春晚、5G国庆等直播，有助于加速该类型5G融合应用场景的进一步落地。随着4K/8K视频的不断推广与普及，以及VR/AR技术的不断升级，5G+超高清视频、5G+VR等网络直播方式将成为最新的主流。预计2021年，5G将在超高清视频直播、VR/AR等领域给C端用户带来更加极致的体验，从而刺激用户增加消费，相关企业进而获利，相关融合应用渗透规模再翻一番。此外，5G手机等终端设备在全新的5G网络架构下也将迎来全面升级，带动5G换机热潮。预计2021年，5G手机渗透率将超过8%。同时，各电信运营商也将通过向用户提供更加流畅的5G网络服务而进一步获利。

以物联网智能感知为代表的工业互联网、车联网等B端5G融合应用场景，以及智慧城市、智慧水务、智慧电网等G端5G融合应用场景具备企业和政府两个巨大量级的客户群。工业互联网以感知技术为基底，应用5G网络的高速率传播以及超低时延，能够大大降低工业过程中的成本，提高工业生产效率，促进工业数字化发展。依靠5G可靠传输的智能网联汽车5G-V2X技术也正在加紧进行研发和试验。同时，在智慧城市、智慧物流、智慧电力、智慧水利、政府数据管理、安防监控、政府大数据等方面，B和G端融合应用利用5G网络的特性可大幅提高工作效率，将为5G新基建释放更多需求。预计2021年，B端和G端融合应用规模平均增长将超过200%，在工业互联网、车联网、政府数字治理等方面最为显著。

## 5G将对工业互联网领域显著赋能

近两年的5G行业级应用主要面向eMBB应用场景。目前，面向uRLLC和mMTC工业物联网方向的R16版本已经冻结。R16围绕基本功能增强、垂直行业能力扩展、运维自动化及网络智能化增强三方面，进一步增强5G更好服务行业应用的能力。R17版本目前正在准备中，将继续对基础能力进行增强，同时在工业物联网IIoT、网联无人机、定位、网络控制的交互服务等能力上继续增强。随着2021年全国5G新基建的进一步大规模铺开，5G业务逐步向各垂直行业延伸拓展，5G+各行业融合应用场景也将全面打开，垂直行业的融合应用将呈现百花齐放的壮观景象，相应的商业模式也将更加完善。

工业互联网将成为“十四五”期间5G商用的重点领域。根据相关数据统计，目前5G在工业互联网、智慧医疗、超高清视频、智慧城市、车联网等行业领域应用占比已经高达70%，尤其是工业互联网，截至2020年10月，国家层面在建“5G+工业互联网”项目超1100个，占据全部项目的近1/3，是5G先进成果的最佳应用场景之一。2020年7月，工信部印发《工业互联网专项工作组2020年工作计划》，同时提出将研究制定《工业互联网创新发展行动计划（2021—2025年）》。此外根据《关于推动工业互联网加快发展的通知》《关于推动5G加快发展的通知》等文件要求，“要探索基于5G行业专用频谱的专网建设，以推动工业互联网在更广范围、更深程度、更高水平上融合创新”，开展面向工业互联网领域的5G专网建设成为我国工业数字化转型的必经之路。可以预测，2021年工业互联网领域的5G专网相关建设工作将会进一步提速。