智能网联汽车

安全渗透白皮书（2022）

智能网联驾驶测试与评价工业和信息化部重点实验室
中国软件评测中心·智能网联汽车测评工程技术中心
普华永道商务咨询（上海）有限公司

2022年12月

版权声明

指导单位

中国电子信息产业发展研究院

指导专家

刘文强　　中国电子信息产业发展研究院

安　晖　　中国电子信息产业发展研究院

王　宏　　国家信息技术安全研究中心

编写单位

智能网联驾驶测试与评价工业和信息化部重点实验室

中国软件评测中心·智能网联汽车测评工程技术中心

普华永道商务咨询（上海）有限公司

测试单位

中国软件评测中心·智能网联汽车测评工程技术中心

国家信息技术安全研究中心

赛迪（浙江）汽车检测服务有限公司

前言

“安全是智能网联汽车发展的前提”

在智能网联汽车快速发展的背景下，安全问题不仅为业界人士关注，更逐渐成为社会公众尤其是车主关心的核心问题之一。2022年中国电动汽车百人会论坛上，全国政协经济委员会副主任苗圩在主题演讲中提到，安全是智能网联汽车发展的前提。中国工程院院士、国家智能网联汽车创新中心首席科学家、清华大学教授李克强在2022世界新能源汽车大会发言时称，今年上半年针对车联网平台的网络恶意行为已经超过100万次，汽车信息安全威胁问题日益严重。

为此，编写组在《智能网联汽车安全渗透白皮书（2020年）》、《智能网联汽车安全渗透白皮书2.0（2021年）》系列白皮书的研究基础上，持续跟踪、深度剖析行业内法律法规以及标准动态，探索行业内合规实践，围绕关键安全问题展开分析，提出针对智能网联汽车行业的安全措施与发展建议，形成《智能网联汽车安全渗透白皮书（2022）》。

本白皮书由赛迪汽车联合普华永道撰写，编写组包括邹博松、王卉捷、翁泽鸿、王爽、陈世威，测试组包括朱科屹、王荣、黄浦、张芝军，在此特别感谢巩潇、傅毓敏对本白皮书的撰写指导，刘鸿运对渗透测试的指导。

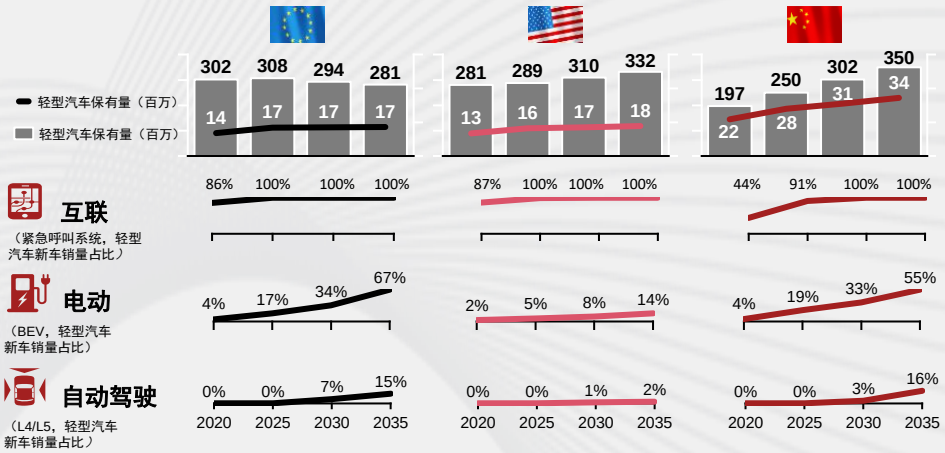
本白皮书的主要观点和内容仅代表编写组的研判和思考，部分内容存在局限性，欢迎业界同仁提出宝贵意见，批评指正。

研究背景 第一章

近年来，汽车产业智能化、网联化、电动化、共享化的“新四化”程度进一步深入，电动汽车作为汽车智能化和网联化的最佳载体，正在加快由人工操作的机械产品转变为基于电子电气架构及信息控制系统的智能终端，不断推动智能网联汽车领域的创新发展。

从新技术广泛落地的层面来看，以网联技术和电动技术为代表的新技术，在全球市场的新车中已经广泛搭载，而L3级以上的自动驾驶技术也将在2025年前后迎来量产的爆发。

- **汽车保有量和新车技术渗透率（万辆，%）**



- 轻型汽车 = < 6t GVW的汽车和轻型商用车；BEV = 纯电动汽车；ICE = 内燃机；TCO=总拥车成本

资料来源：《普华永道思略特2021年数字化汽车报告》

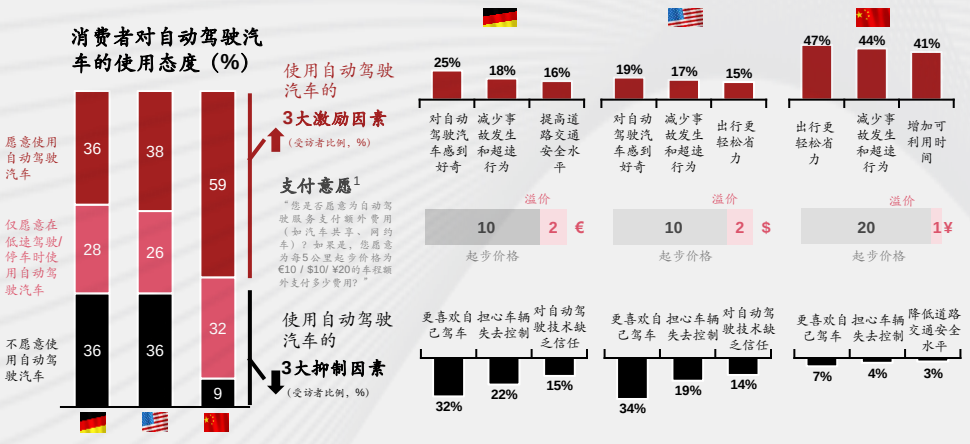
随着智能网联汽车安全的重要性日益凸显，网络安全、数据安全、OTA安全、个人隐私安全引发了越来越多关注，并已成为事关智能网联汽车技术研发和高质量发展的基础性因素，给车企、芯片厂商、零部件供应商等产业链各个环节主体提出了更严苛的安全要求。

（一）智能程度提升，车端安全要求日益提高

2021年，工业和信息化部、国家发改委和科技部联合印发的《汽车产业中长期发展规划》提出，到2025年，汽车L1驾驶辅助（DA）、L2部分自动驾驶（PA）、L3有条件自动驾驶（CA）系统新车装配率达80%，其中PA、CA级新车装配率达25%，L4高度自动驾驶汽车（HA）和L5完全自动驾驶汽车（FA）开始进入市场。可以看出，汽车的智能化已成为明确的发展方向。从车辆智能化程度现状来看，随着技术的不断进步，车载传感器、计算单元、控制单元的搭载总数从一开始的个位数已达到当前的数十上百之计。根据艾瑞咨询数据，2020年中国智能辅助/自动驾驶系统市场规模为335亿元，2025年将达1150亿元，年复合增速达28%。

人工智能与自动驾驶技术的快速发展，在为车辆带来辅助驾驶与自动驾驶体验提升的同时，也对汽车行车安全提出了更多的挑战。自动驾驶系统异常驾驶行为识别能力、系统与各控件间的数据安全能力、传感器和雷达等设备的抗干扰能力、GPS系统的加密通讯与身份识别能力等各方面都需符合更高的安全要求。根据普华永道报告对三国消费者的调查显示，消费者对于自动驾驶的接受程度高，并在自动驾驶过程中尤其关注“安全”因素。

自动驾驶 – 消费者态度、影响因素和支付意愿



1 使用自动驾驶汽车代替司机或自主驾驶的平均溢价支付意愿

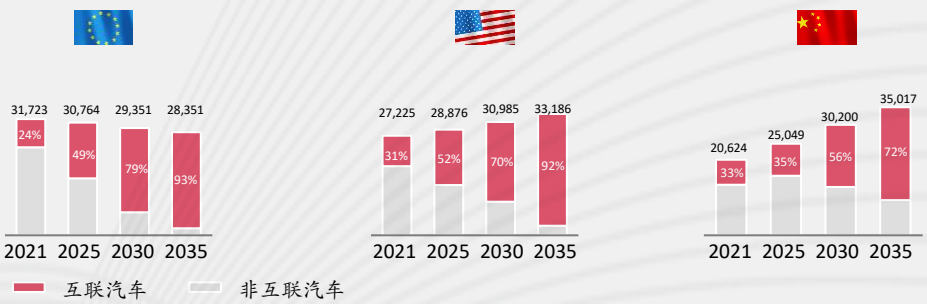
资料来源：《普华永道思略特2021年数字化汽车报告》

（二）网联技术增强，互联互通导致广泛攻击

除了智能化自动驾驶技术的提升之外，车路协同、通信网络等关键技术的快速发展正在使得汽车产品从封闭系统走向开放，汽车网联化程度大幅提升。根据IHS Markit预测，2022年全球网联汽车市场渗透率将达到24%，预计本年度全球车联网市场规模将达到1629亿美元，同比增长约为14%；中国车联网市场增长速度更快，预计增速将达到约24%。

根据《普华永道思略特2021年数字化汽车报告》的统计与预估，到2025年欧洲和美国路面上将有约一半的车辆具有网联功能，在中国这个比例也会超过三分之一。

- **汽车保有量和互联车辆占比（万辆，%）**



资料来源：《普华永道思略特2021年数字化汽车报告》

不同于传统汽车的封闭性，不断融入的新兴网联化技术使汽车面临着更广泛的攻击。网联汽车关联的云端服务器，具有车控功能的手机APP、蓝牙钥匙，车端搭载的车车通信与路侧通信系统、OTA系统等，都是进行网络安全攻击的重要目标与入口。例如，OTA升级场景给了黑客多个攻击路径。一方面可以通过破解升级过程中的加密协议和校验机制，向车机系统植入木马；另一方面可以截获并反编译OTA升级固件包，从源代码层面查找系统未被发现的漏洞与攻击入口；更有甚者，可以直接攻击OTA升级服务器，获取服务器权限，进而篡改升级软件包并下发升级任务给车辆，达到入侵车机系统的目的。

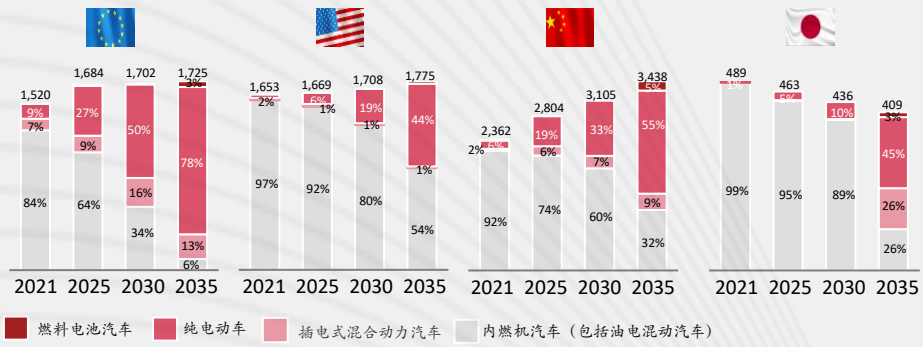
由此可见，在万物互联的大趋势下，如何进一步加强汽车安全防护，保障人车安全，将是行业内各方需要重点关注和解决的问题。

（三）新能源产业发展，充电桩及接口威胁增加

“双碳”目标下，国内新能源汽车产业继续强化顶层设计，不断优化科技创新和产业布局。近几年国内新能源车的保有量正以每年数百万的速度增加，从2020年的492万辆增长到2021年的784万辆，同比增长59.3%。

放眼全球，以欧盟国家为代表发达国家中的纯电动和插电式混合动力汽车产销量也在同步大幅增长。

- **按动力系统划分的新车销量（万辆，%）**



资料来源：《普华永道思略特2021年数字化汽车报告》

充电桩作为新能源汽车产业中一个重要的组成部分，呈现出快速发展的趋势。2020年充电桩建设被纳入国家“新基建”，各种充电服务、充电APP也随之涌现市场。根据中国电动汽车充电基础设施促进联盟（EVCIPA）发布的数据，2017-2021年全国充电桩5年复合增长率达56%，2021年充电桩保有量为261.7万台，较2020年新增94万台，同比增长55.7%。

充电桩在快速推广普及的过程中也暴露出许多安全问题，如充电桩软件安全漏洞、充电桩与APP间授权机制不完善、充电桩间通讯协议明文传输、API鉴权机制缺陷等。

此外，新能源车充电接口中的CAN网络接口很可能在不经意间成为黑客攻击的入口。随着新能源汽车及周边设施的投入进一步加大，如何确保充电过程、三电系统等安全，让广大新能源车主能够安心使用，是目前需要解决的重要问题之一。

安全要求

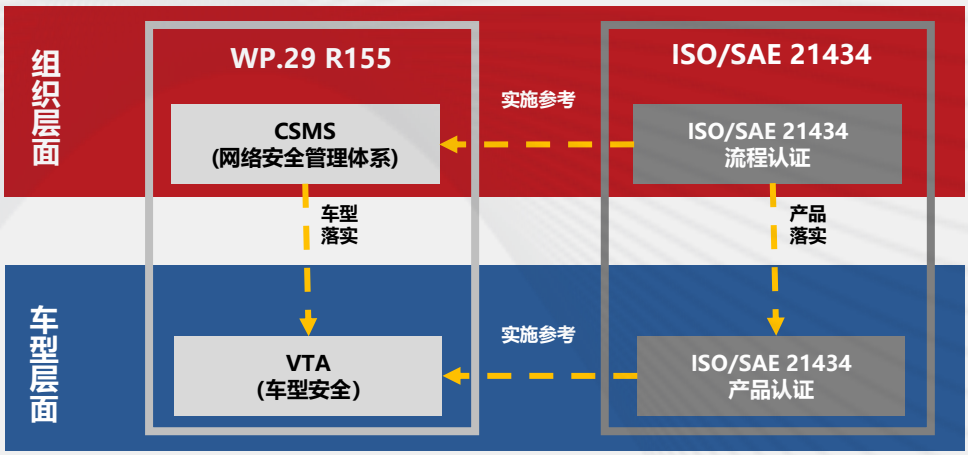
第二章

（一）国外安全法规与标准

UN/WP.29（全称为联合国世界车辆法规协调论坛）于2020年6月发布了一系列汽车关于智能网联汽车的重要法规，其中R155法规对车辆网络安全(Cyber Security)作出了相关规定。

R155作为第一个汽车网络安全强制法规，其主要适用范围包括了欧洲、日本、韩国等“1958 协议”缔约国（以下简称“58 协议国”）。 WP.29所出台的法规被“58 协议国”整车认证法规引用后成为强制要求，即只要在“58 协议国”上市的汽车就必须通过相关认证。

与R155相对应的国际标准ISO/SAE 21434《Road vehicles—Cybersecurity engineering（道路车辆-信息安全工程）》也于2021年8月正式发布。从落地实施角度来看，ISO/SAE 21434可作为法规落地实施时的参考标准。R155法规与ISO/SAE 21434标准之间有很多的关联与交叉，下图可以很好的体现它们的关系：



资料来源：根据SAE International 国际自动机工程师学会官方材料翻译整理

法规R155 车辆网络安全与网络安全管理体系

R155合规认证工作主要分为两个部分，其一是网络安全管理体系认证（CSMS）；其二是车辆网络安全型式认证（VTA）。

在海外，目前各国交通部门已经陆续制定了符合各国情况的法规认证实施细则。截至2022年7月，已经有车企陆续获得了CSMS认证证书，并有少量车型获得了R155认证。特别说明的是，与其他的UN ECE法规类似，在欧盟内部，各国签发的R155证书原则上在欧盟内部各国之间是互认的，因此车企并不一定会选择在车辆的销售目标国家申请认证，而可能会基于种种因素选择在其他的欧盟国家申请认证。据部分公开资料显示，海外各国已经颁发的R155 法规认证证书相关情况统计如下：

国家	认证负责部门	认证证书发放情况
德国	KBA（德国联邦机动车运输管理局）	截至2022年10月，有约八家企业已获得CSMS体系认证证书（其中包括中国自主品牌车企：长城汽车），有至少一款车型已通过型式认证
日本	国土交通省	本田、日产、丰田、雷克萨斯、斯巴鲁、马自达、五十铃、铃木等主流车企已获得CSMS体系认证证书
法国	CNRV	截至2022年7月，尚未有车型通过法国的R155认证，目前有4个车型正在测试中
西班牙	西班牙交通部	截至2022年10月，有至少五家企业已获得CSMS体系认证证书（其中包括中国新势力车企：蔚来汽车）
爱尔兰	NTA （铁路公司与国家交通局）	截至2022年10月，有至少一家企业已获得CSMS体系认证证书（其中包括中国新势力车企：小鹏汽车）

在国内，目前对于R155法规体系层面，有出口需求的自主及部分合资乘用车企业正在积极响应中。现已有自主品牌率先获得了R155 CSMS体系认证，同时其余整车厂也相继进入到CSMS预审核和证书申请的阶段。另外由于车型的研发周期和量产进度的影响，各出口车企的R155 VTA车辆型式认证方面的工作相对耗时更长，尚未有车型获得R155 VTA认证。此外，商用车同样是中国出口车型的热门，在商用车企业中，对于以上两个法规的应对计划普遍较慢，仅有少部分商用车企业的CSMS体系建设工作已经启动，而大部分车企都在法规解读或者咨询认证的立项阶段。

● 标准SAE J3061

国际自动化工程师学会（SAE）编制的SAE J3061推荐规程《信息物理汽车系统的网络安全指南(Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)》是首部针对汽车网络安全而制定的指导,性文件。其第一版于2016年1月发布，前瞻性地确立了网络安全活动在整车生命周期中的重要地位，并定义了一套覆盖车辆全生命周期的流程框架，将汽车网络安全理念贯穿到汽车全生命周期流程中，并为开发具有网络安全要求的汽车电子系统提供了重要的过程依据。

在SAE J3061的初稿发布几个月后，国际标准化组织（ISO）开始与SAE合作，共同牵头制定道路车辆的网络安全国际标准，这便是后来的ISO/SAE 21434。

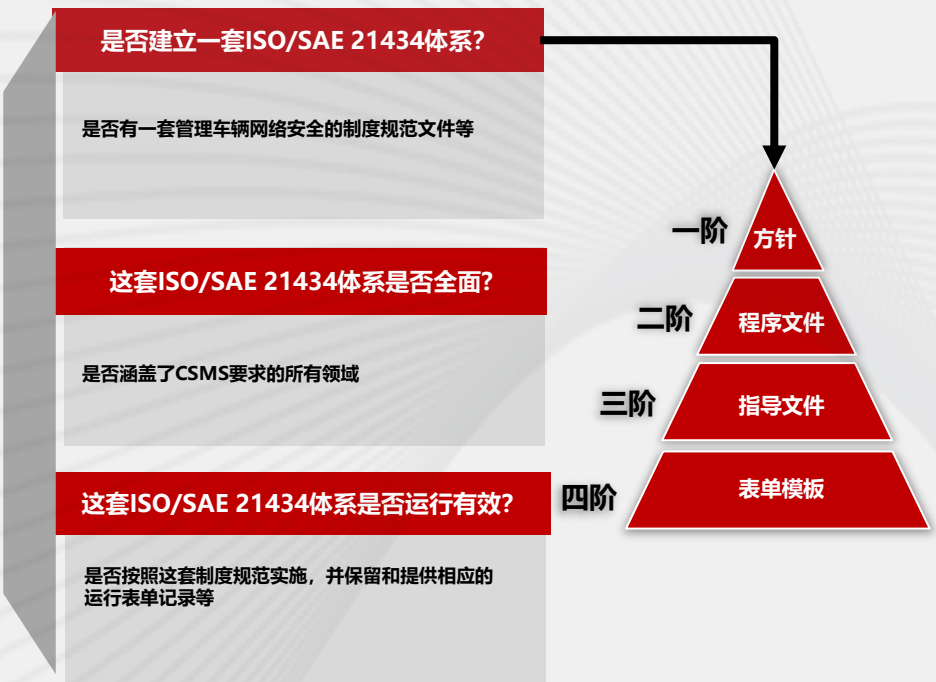
● 标准ISO/SAE 21434

ISO/SAE 21434 《Road vehicles—Cybersecurity engineering（道路车辆-信息安全工程）》标准于2021年8月正式发布。

其针对道路车辆及其部件、接口等，提出了基于车辆生命周期的网络安全风险管理的要求，定义了车辆生命周期包括车辆概念、研发、生产、售后、维护和退役相关等各阶段的要求。通过该标准设计、生产、测试的产品意味着具备了一定网络安全防护能力。该标准不仅适用于道路车辆制造商，也适用于为道路车辆的电子电器系统提供软硬件的各级供应商。

各车辆制造商为了满足R155法规的要求，需要在整车研发过程中，在采购与供应商管理等环节中，加入网络安全相关的活动与流程，而ISO/SAE 21434则是车辆制造商判断与考核零部件供应商网络安全能力的最重要标准。基于此，当前阶段国内外的汽车电子、智能网联、自动驾驶、芯片电子等各个零部件供应商，均在积极推进ISO/SAE 21434的合规落地工作与认证工作。对于ISO/SAE 21434的体系流程认证总体上各企业的工作思路如下：

- **如何获取ISO/SAE 21434认证?**



据公开资料显示，截至2022年10月，国内外已经获得了ISO/SAE 21434流程认证的典型企业统计如下：

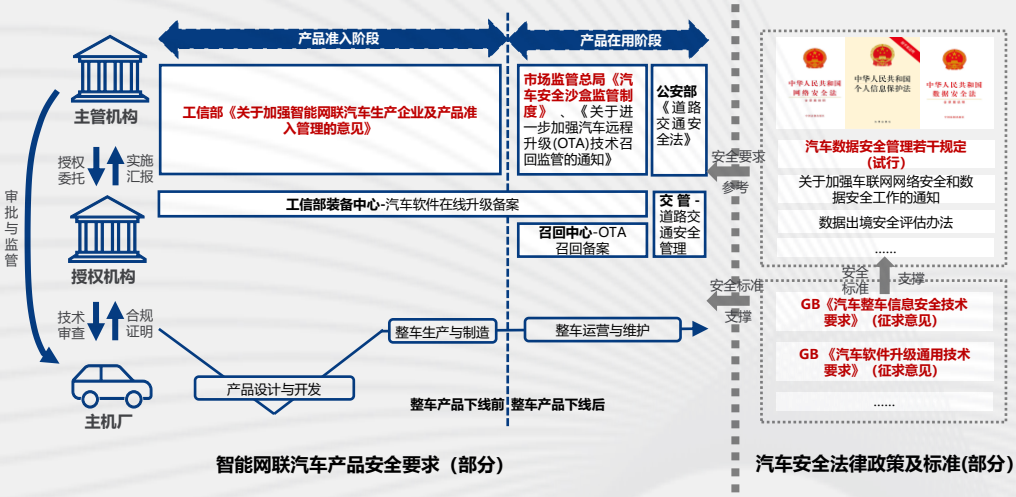
序号	企业类型	公司名称	最新进展	认证机构
1	各级供应商	华为	已获得认证	DEKRA德凯
2		亿咖通科技	已获得认证	BSI 英国标准协会
3		佛吉亚歌乐电子	已获得认证	DEKRA德凯
4		NXP 恩智浦	已获得认证	TÜV南德
5		东软睿驰	已获得认证	SGS
6		德赛西威	已获得认证	TÜV南德
7		地平线	已获得认证	TÜV莱茵
8		华邦电子	已获得认证	TÜV北德
9		赢彻科技	已获得认证	TÜV莱茵
10		汇川联合动力	已获得认证	TÜV莱茵
11	车辆制造商	比亚迪商用车	已获得认证	DNV
12		零束科技	已获得认证	TÜV北德

资料来源：公开信息整理

（二）国内安全政策与标准

车联网是国内汽车产业发展的战略方向之一，我国正在加速法律法规及标准政策制修订工作。以智能网联汽车产品为对象，由于其结构、功能实现等方面与传统汽车存在较大差异，车辆安全相关基本特征、技术参数始终不断变化，工业和信息化部、公安部、市场监督管理总局等主管部门针对车辆产品准入、生产、销售、运营服务及上路等环节提出了监管要求。

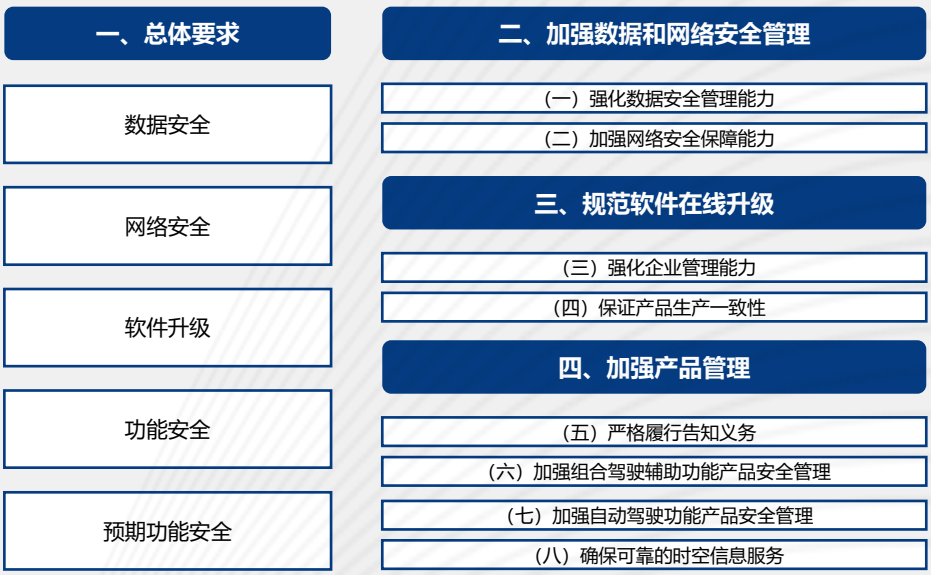
为了切实保障公共及公民安全，产品管理、道路测试等要求中均提及了安全，同时聚焦网络安全、数据安全制定了明确的顶层设计规划。目前智能网联汽车企业及产品需遵循及参考的各方面安全要求及标准（部分）如下图所示：



●关于加强智能网联汽车生产企业及产品准入管理的意见

在《道路机动车辆生产企业及产品准入管理办法》等已有规定的基础上，工业和信息化部于2021年7月发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》，面向有关汽车生产企业提出了加强汽车数据安全、网络安全、软件升级、功能安全和预期功能安全管理，保证产品质量和生产一致性的明确要求。

通过加强数据和网络安全管理、规范软件在线升级等主要要求，明确主机厂等相关汽车企业应具备网络与数据安全保障能力、软件升级管理能力及相应的过程保障能力，并符合安全测试要求。



特别地，由于智能网络汽车产品开发带有典型的软硬解耦特征，软件升级（OTA）技术将伴随整车全生命周期过程，工业和信息化部和国家市场监督管理总局均对其提出了监管要求。工业和信息化部装备工业发展中心、国家市场监督管理总局缺陷产品管理中心对OTA备案的实施细则基本上完全解决了相关企业合规执行上的问题。

2022年9月15日国务院新闻发布会上，工业和信息化部副部长辛国斌表示，工业和信息化部将支持开展智能网联汽车准入试点，推动产业高质量发展。可以预见，随着试点工作的开展，落地性政策以及配套实施细则将陆续出台，进一步指导行业，推动产品管理相关法律法规在地方和部分企业上先行先试。

●汽车数据安全管理若干规定（试行）

2021年7月，国家互联网信息办公室出台《汽车数据安全管理若干规定（试行）》，相较于已有的数据安全要求，该规定是在汽车数据安全管理领域有针对性的规章制度，保护对象呈现明确的汽车行业特征。

规定定义了汽车数据、汽车数据处理、汽车数据处理者的范围以及个人信息、敏感个人信息、重要数据等关键概念含义。提出了汽车数据处理者的责任和义务，规范汽车数据处理活动。释放出政府部门对智能网联汽车数据安全的监管信号，行业内需重视并提高数据安全合规意识。

该规定催生的汽车数据安全年报制度，很大程度上更加规范了汽车数据处理者对汽车数据的合理合法使用及保护，对行业主体提出了安全新要求。同年末，河北省、天津市、上海市、广东省、湖南省等地有关部门陆续发布了关于报送年度汽车数据安全管理情况的通知。

●关于试行汽车安全沙盒监管制度的通告

国家市场监督管理总局、交通运输部等五部门在2022年4月共同发布了《关于试行汽车安全沙盒监管制度的通告》，探索汽车安全沙盒监管制度，监管对象为车辆中使用的环境感知、智能决策、协同控制等前沿技术，或实现各级别自动驾驶、远程升级等新功能新模式。涉及的车辆须通过工信部《道路机动车辆生产企业及产品公告》等市场准入条件，取得强制性认证证书，经营性机动车应当符合营运安全相关标准。

该要求是在后市场阶段针对车辆应用的前沿技术进行深度安全测试的机制，聚焦现有法规没有覆盖的技术风险和质量不确定性问题，通过风险评估的方式，就创新技术安全性进行深度测试和评估，最大限度防范产品应用风险。拟申请进入沙盒需要经过申请、评估、测试、报告、退出等五个阶段，因此对于企业而言，需要关注其中较为重要的流程节点，如入盒申请、盒中监测、出盒评估等，提前准备并完善相应监管保障计划、测试实施方案等，建立自身车辆自动驾驶自评估的安全体系。

●汽车强制性国家标准

在政策的推动下，汽标委、信安标委等标准组织和行业有关单位不断加速汽车数据安全、网络安全、在线升级等标准规范制定进程，用于指导企业加强相关测试验证和检验检测能力建设，不断提升智能网联汽车相关技术和网络安全、数据安全水平。

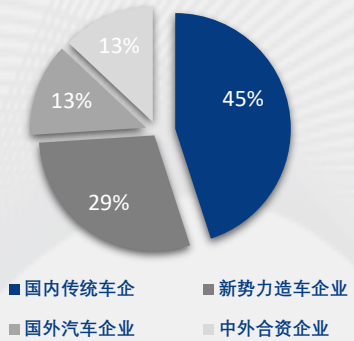
目前，强制性国家标准汽车整车信息安全技术要求、汽车软件升级通用技术要求即将正式发布。《汽车整车信息安全技术要求（草案）》提出了汽车整车信息安全技术要求和企业信息安全管理体系要求，涵盖外部连接安全、车辆通信安全、软件升级安全和数据代码安全，并给出了对应的测试方法，相关的标准验证试验工作已陆续完成。《汽车软件升级通用技术要求》对企业软件升级管理体系和车辆功能均提出了要求，该标准未来的落地实施将助力企业建立相应管理能力，确保车辆进行软件升级时处于安全状态以及指导车端用户进行安全操作，最大程度上规避企业在OTA过程中面临的各种安全风险。

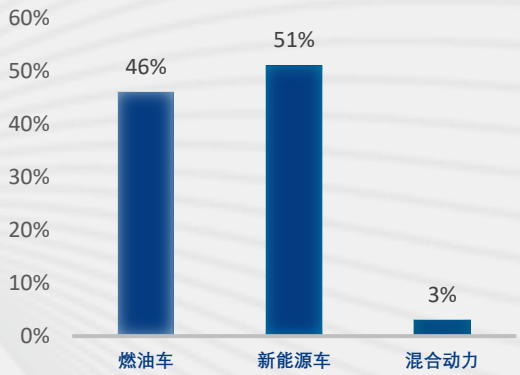
结果分析 第三章

以上述政策法规、技术标准为参考依据，中国软件评测中心（赛迪汽车）在相关主管单位的指导监督下，从2020年开始连续三年牵头组织智能网联汽车安全渗透测试活动，从智能网联汽车产品准入安全要求出发，验证车辆的防护情况，为行业发展提供参考。

●渗透活动3.0

2022年在往届基础上新增了10款车型，全面覆盖了传统车企、造车新势力在售的新能源车辆、燃油车辆以及混合动力车辆，样本更加充分。据统计，三届渗透活动共测试24家主流车企的35个不同车型，包括一汽、比亚迪、东风日产、理想汽车、北汽新能源、合众新能源、威马汽车、上汽大众、零跑汽车、广汽、吉利、长安、奔驰、奇瑞、宝马、蔚来、现代、沃尔沃、小鹏、长城等。

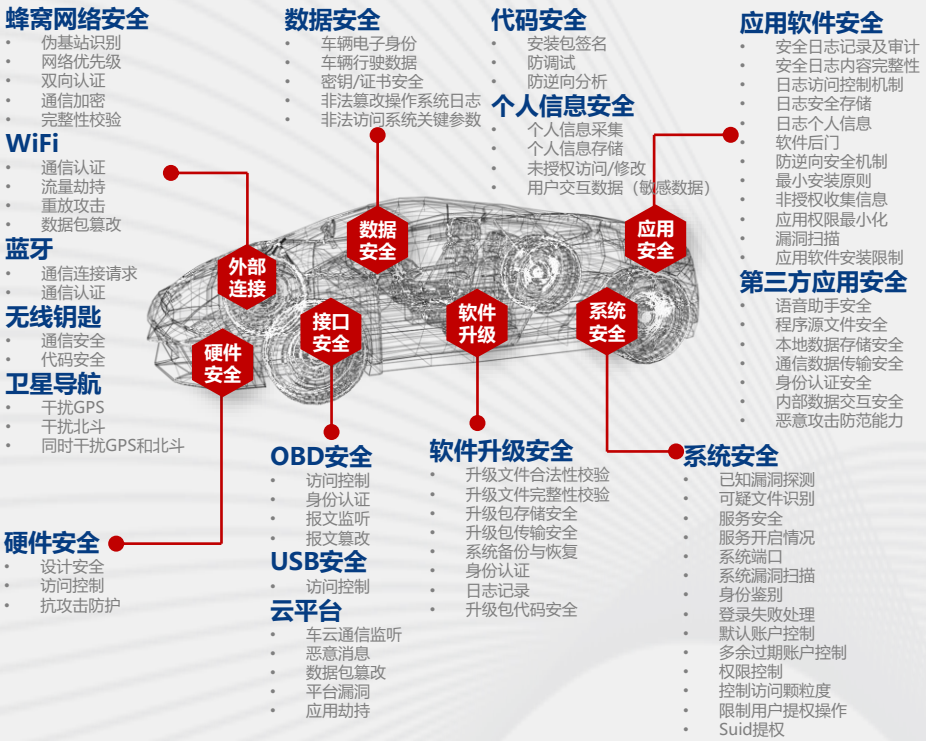




车型主要涉及理想ONE、哪吒U、长安cs75Plus、奥迪A4L、沃尔沃XC40、索纳塔10、斯柯达柯珞克、吉利领克01、蔚来ES6、新瑞虎、广汽GS8、沃尔沃S90、吉利帝豪、红旗E-QM5、吉利GSe、中华V7、极狐αS、比亚迪唐、比亚迪元、长安逸动、MINI Cooper S countryman、奔驰GLE450、长城VV6、奔驰威霆、轩逸日产、传祺GS8、大众Polo、小蚂蚁EQ1、吉利Smart等。

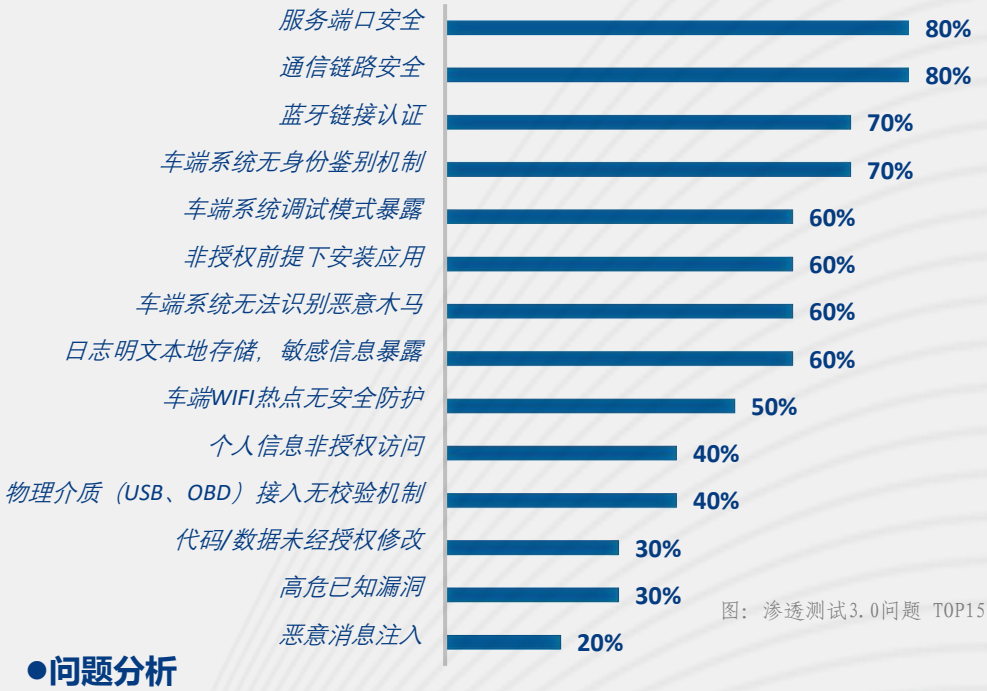
●测试指标3.0

本年度安全渗透测试指标体系细分7类测试指标，共85项测试用例。包括硬件安全、外部连接安全、软件升级安全、接口安全、应用安全、数据安全、系统安全。**基于2020-2021年的研究成果完善了指标体系，在2.0的基础上增加40余项用例，聚焦强标要求新增软件升级安全指标，依据数据安全法和个人信息保护法细化数据安全、个人信息保护指标。**



●测试结果3.0

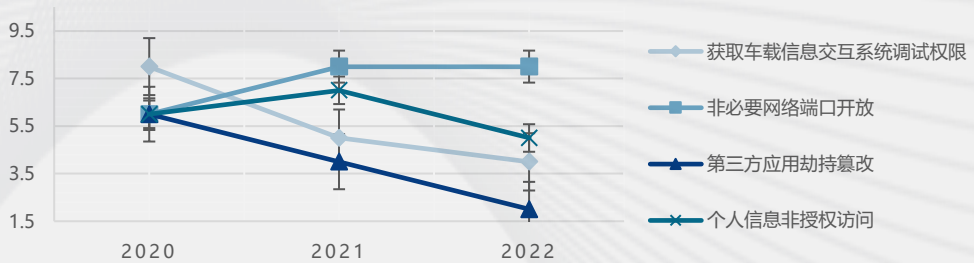
本次测试结果显示，典型问题涉及服务端口安全、通信链路安全、蓝牙链接认证、车端系统无身份鉴别机制、车端系统调试模式暴露、非授权前提下安装应用、车端系统无法识别恶意木马、日志明文本地存储及敏感信息暴露、车端WIFI热点无安全防护、个人信息非授权访问、物理介质（USB、OBD）接入无校验机制、代码/数据未经授权修改、高危已知漏洞等方面，具体检出率如图所示。



图：渗透测试3.0问题 TOP15

●问题分析

据统计，三届渗透测试共计发现汽车安全问题类别超过90项，被测车辆存在的安全问题超过300个。以车内安全、第三方应用安全、个人信息几个典型方面的问题检出率趋势来看，**在相关政策法规和技术标准的引导和逐步规范下，行业内的网络安全意识普遍提升，在车辆上采用了如访问控制、身份鉴别、安全通信协议等方面的防护措施，进入车载信息系统调试模式、获取权限难度逐渐增加。**

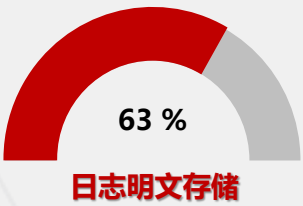


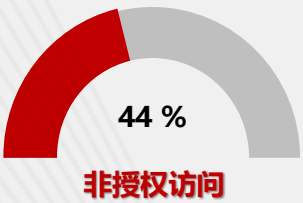
然而，测试过程中也发现，对于新提出的关于数据收集、使用、处理以及相关防护，个人隐私保护，OTA升级等方面的安全要求，部分被测车辆尚未采取防护措施，**数据安全、个人隐私、软件升级等方面的新问题仍是行业需面对并尽快解决的挑战。具体分析及建议如下：**

数据安全问题

数据安全问题主要表现在个人隐私数据泄漏、数据越权访问、数据出境是否合规、敏感数据无安全防护措施等方面。

其中，63%的车型存在安全日志、行为日志明文存储，其日志内容包含车辆行驶轨迹信息，车辆位置经纬度信息，个人身份信息等；44%的车型可以通过车机或其他入口在非授权情况下访问使用敏感数据，对车辆工况数据、密钥数据及证书未做安全防护处理。另外，个别车企存在使用境外服务器部署服务的情况，且使用过程中未进行数据出境的相关评估工作。





●合规分析

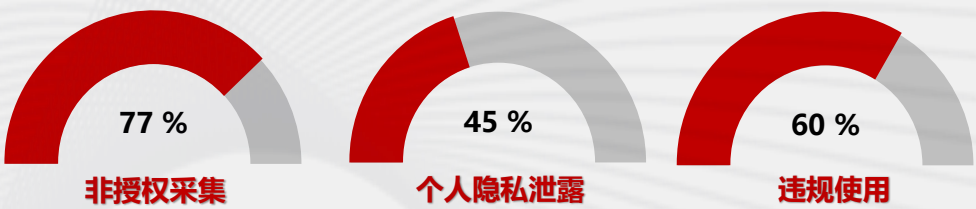
①准确把握安全要求，明确需求对应关系。先后出台的《网络安全法》、《数据安全法》、《密码法》、《个人信息保护法》几部上位法中，均提出数据安全的相关要求。在智能网联汽车行业中，企业将如何正确理解法律法规要求，同时将企业自身在数据安全方面的实际需求与法律法规相结合，是目前所面临的实际问题和难点。建议产业生态中相关企业深入分析自身安全需求，从数据安全体系建设和产品数据安全过程保障出发，提升数据安全保障能力，建立健全相关体系。

②落实安全左移，重视数据生命周期。安全防护意识左移是从源头解决问题的有效办法，同时也可以大大降低安全成本。从概念设计阶段引入数据安全威胁建模和风险评估可以提前发现问题，消除安全隐患。重视数据的采集、生产、传输、使用、存储、销毁的生命周期是现阶段逐步形成的技术路线，也在一定程度上达成了行业共识。例如采用安全的信道链路保障传输层安全，使用授权认证的方式解决合法用户的问题，通过合理的加密方式解决部分数据保密性问题等。

③平衡数据安全、隐私合规与实际使用场景需求的矛盾。实现汽车智能化、网联化离不开对环境数据、工况数据以及个人隐私数据等信息的采集、处理和使用。目前车企在数据授权的方式上大多是采用注册即视为同意的方式，通过《隐私政策》的默认形式让用户同意“一揽子”授权，如果用户拒绝授权则直接影响相应功能的使用。建议企业从用户需求和实际功能角度出发细分数据类型，做好分级管理，避免无差异化授权的形式。通过事前漏洞扫描、安全加固，事中安全策略、加密脱敏，事后安全审计、日志分析来进行动态管理。

个人隐私问题

测试结果显示，77%的车型存在个人隐私数据非授权采集、采集范围未做有效控制等问题；45%的车型存在个人隐私泄露问题，泄露内容包括个人身份信息、车辆位置信息、车内对话内容等；近六成的车型存在违规收集个人信息，违规使用个人信息，个人敏感信息未做安全防护或脱敏处理，车辆使用过程中强制、频繁、过度索取用户权限等问题。当然，汽车隐私合规问题与辅助驾驶功能、座舱娱乐域功能的丰富程度成正比，即车辆与用户的交互功能越多、越频繁，所导致的问题就会越多。



●安全建议

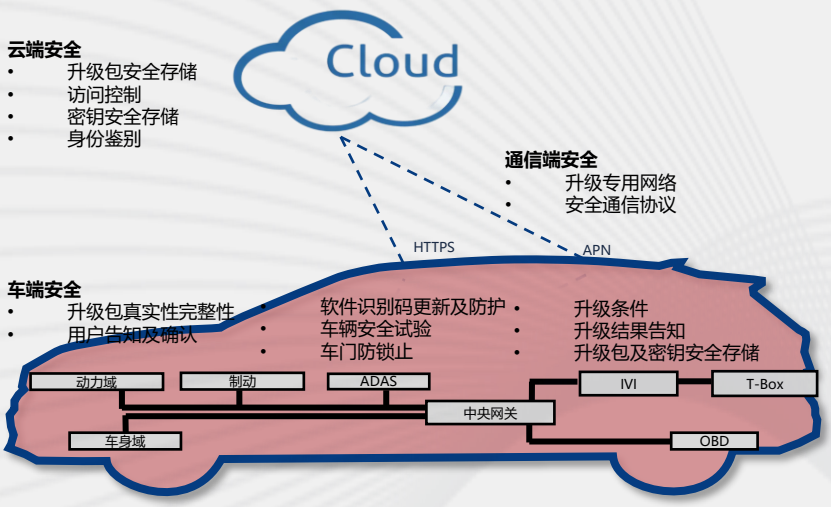
一方面，需重视车辆使用过程中个人信息隐私合规的重要性。应当按要求建立企业级车辆个人隐私数据管理体系，并实现产品级合规，规避企业因处理个人隐私数据所带来的法律风险和处罚。**另一方面**使用加密、脱敏等技术手段，对个人隐私数据的全生命周期进行安全防护。例如，严格加强车端数据的边界管控机制，在车内数据需向车外传输时做好数据分类分级保护、加密脱敏等工作。

OTA安全问题

测试结果统计表明，60%的被测车辆具备OTA功能，其中超九成都存在OTA升级缺陷。其中典型问题主要包括云端服务非授权访问、通信链路明文传输、软件升级包未做签名校验等。

●风险分析

全面覆盖“车、路、云、网”多元交互的汽车OTA作为智能网联汽车领域的新兴技术，其快速发展为智能网联汽车的功能快速升级及用户体验提升带来了强大的动力。在软件定义汽车的智能化转型趋势下，OTA场景应用逐渐广泛，其安全随之也变得至关重要。安全渗透测试通过OTA场景下的威胁分析和风险评估，梳理得出升级流程的高风险环节普遍存在于车端、云端以及两者间的网络通信中，需要对云管端的安全进行全面考虑。



因此，建议从如下方面考虑汽车软件升级过程中的安全。**一是**在云端采用证书、签名、加密机制等安全措施，保障OTA平台的安全服务，保证升级包不会随意被制作和发布，内容不被恶意获取及篡改。**二是**在通信端采用安全可靠的物理链路和安全传输协议来保证升级包传输过程中的安全。**三是**在车端通过功能可靠性设计、安全防御手段等方式实现车内升级的安全加载及启动运行。

结语

网络安全、数据安全、OTA安全、个人隐私安全等已经成为保障智能网联汽车产业健康、有序、高质量发展的重大热点问题，**随着《道路机动车辆生产准入许可管理条例（征求意见稿）》、《关于开展智能网联汽车准入和上路通行试点工作的通知（征求意见稿）》的发布，**标志着智能网联汽车的安全发展已全面进入监管阶段，赛迪汽车将继续携手行业各方力量，以国家法律法规和相关规定为基础，全面提升安全保障及服务能力，共同推动我国智能网联汽车产业的快速发展！

————中国电子信息产业发展研究院 刘文强

联系方式：

中国电子信息产业发展研究院
电话：010-88558772

中国软件评测中心
（工业和信息化部软件与集成电路促进中心）
电话：010-88559439