CSTC中国评测 见证质量 技术白皮书

# 智能网联汽车安全渗透白皮书 2.0（2021 年）

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

北京航空航天大学

国汽（北京）智能网联汽车研究院有限公司

智能网联驾驶测试与评价工业和信息化部重点实验室

赛迪（浙江）汽车检测服务有限公司

2021 年 12 月

# 序 言

智能化、网联化发展使得汽车领域应用环境更加特殊、管理更加困难，智能网联汽车所面临的网络安全威胁也更加突出。在此背景下，中国软件评测中心智能网联汽车测评工程技术中心自 2020 年起，聚焦整车安全威胁分析、网络安全渗透指标体系建设、测评实践结果分析等方面组织撰写《智能网联汽车安全渗透白皮书》系列，旨在为行业提供一手测试数据，围绕关键安全漏洞进行剖析，针对智能网联汽车企业提出安全防护建议。

2021 年，《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》先后开始实施，工业和信息化部于 8 月发布《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见》，为智能网联汽车领域安全发展指明方向。“网络安全”在智能网联汽车领域持续升温，并逐步纳入监管范围。

为此，我们深入研究、组织撰写《智能网联汽车安全渗透白皮书 2.0》。与 1.0 版本相比，本白皮书持续跟踪分析行业内法规、政策、标准动态，继续为行业提供渗透结果数据及安全建议；对标最新政策法规、技术标准，更新完善渗透测试指标体系；新增智能网联汽车网络安全威胁分析内容。

本白皮书由智能网联汽车测评工程技术中心（赛迪汽车）牵头，在中国智能网联汽车产业创新联盟指导下，联合

国家信息技术安全研究中心、北京航空航天大学、国汽（北京）智能网联汽车研究院有限公司等多家单位撰写，参与人员包括邹博松、朱科屹、路鹏飞等，在此特别感谢中国电子信息产业发展研究院副总工程师安晖、中国软件评测中心总工程师陈渌萍、北京航空航天大学交通科学与工程学院院长杨世春教授对本白皮书的撰写指导。

本白皮书中主要观点和结论仅代表编写组的思考，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。

中国软件评测中心 巩潇

2021 年 12 月

# 版权声明

指导组：安　晖　　陈渌萍　　杨世春　刘鸿运

编写组：邹博松　　朱科屹　　路鹏飞　黄　浦

曹耀光　　麻　斌　　罗承刚

# 目 录

# 前 言

近年来随着人工智能、和网络技术在汽车行业的加速渗透，智能网联汽车已经成为行业公认的发展方向。车辆功能更加多样，数据信息更加开放，而与之伴随的是网络安全风险点明显增加，并由此导致了针对汽车产品的网络安全事件大量爆发，引起了国内外公众的普遍关注。

在此背景下，国内外政府、网络安全技术公司和汽车企业都在积极开展相关研究，从政策引导、标准规范到安全风险分析和防护技术研发等各个层面展开工作，努力建立健全智能网联汽车网络安全保障体系，并取得了初步成果。

本白皮书涵盖行业内网络安全态势解析、智能网联汽车网络安全威胁分析、车辆资产识别、关键安全问题解析、测试指标体系等内容，为针对性地开展网络安全防护技术研究提供参考。

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）是工业和信息化部的直属单位。长期服务和支撑国家部委、地方政府以及电信和互联网、汽车、教育、卫生、广电、交通、能源、银行、证券、保险、航空等各大行业，业务范围覆盖全国 31 个省、自治区、直辖市，业务网络覆盖全国 500 多个城市,构建了基于第三方服务的科技产业链。

智能网联汽车测评工程技术中心（赛迪汽车）是中国软件评测中心核心业务板块，依托于智能网联驾驶测试与评价

工业和信息化部重点实验室及智能网联汽车软件检测中心，开展整车信息安全、V2X 安全、车载终端信息安全、电动汽车通信协议及数据格式一致性及安全、源代码安全等测评服务，以及标准政策解读、共性技术研究、产业发展规划等专业咨询服务。具备整车及零部件的功能、性能、可靠性、信息安全的综合测试与评价能力，致力于为政府部门、企业、科研院所等提供专业、安全、可靠的第三方咨询、测试、评估服务。

# 一、智能网联汽车网络安全背景

## (一) 智能网联汽车网络安全现状

### 1. 网络安全问题持续引起高度关注

随着汽车产业在智能化网联化方向深入发展，新型汽车产品已逐步成为车轮上的数据中心，车载软硬件配备也变得更加复杂。据统计，今天的汽车有多达 150 个车载控制器和大约 1 亿行代码，支撑自动驾驶、网联通信、人机交互等新兴功能的实现。与此同时，高度复杂的汽车电子电气系统、通信网络和软件配备也为针对车辆和道路基础设施的网络攻击创造了大量的机会。

据 AV-TEST Institute 数据显示，过去十年中恶意软件的数量从 2011 年的约 6500 万增加到 2020 年底的约 11 亿；根据工信部车联网动态监测情况显示，2020 年以来发现的针对整车企业、车联网信息服务提供商等相关企业的恶意攻击达到 280 余万次。近年来，各国网络安全研究人员和汽车企业披露的网络安全事件和安全风险漏洞也在持续增加。截至 2020 年底，有 110 个 CVE 漏洞与汽车产品有关，其中 2020 年披露 33 个，2019 年披露 24 个，涉及车内网络、网关、传感器、车载信息娱乐系统、蓝牙、OBD 端口、移动 APP 等车辆各个方面。这些网络安全漏洞不仅可能影响到车辆的信息娱乐服务质量，欺诈车辆用户，甚至可能直接导致车辆控

制失效。2010 年至 2020 年间的信息安全事件影响到的车辆功能层面如下图 1-1 所示。

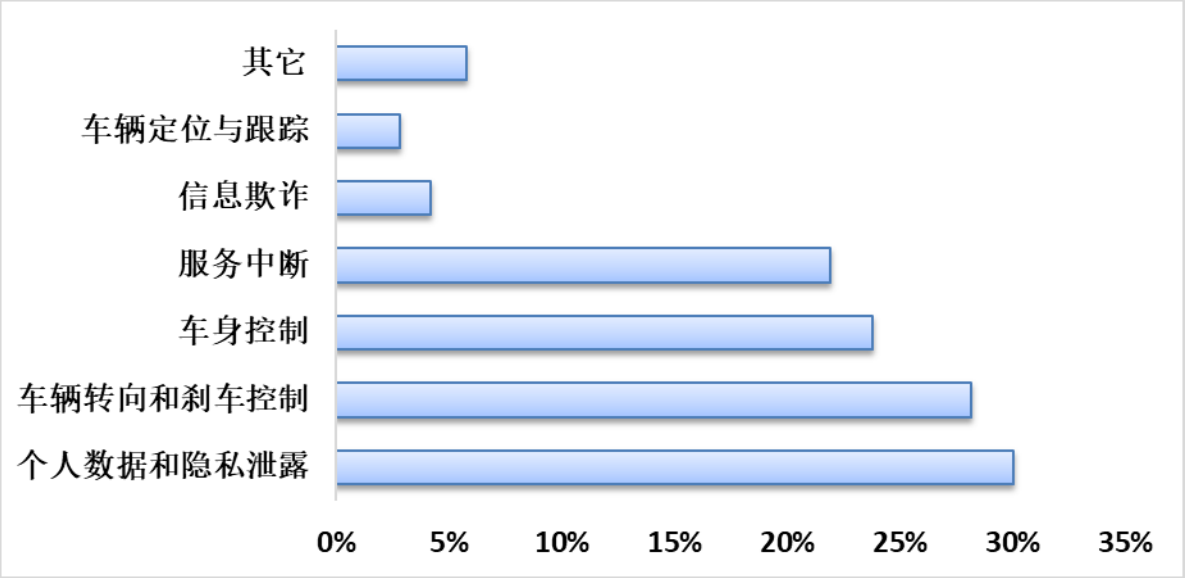



**图1-1 网络安全漏洞影响车辆功能**

## 2. 网络安全保障成为产业发展重点

事实上，国内外汽车企业在研发智能网联汽车伊始，并未充分考虑到为之配备充分的网络安全保障功能。直至 2016 年前后，频繁出现的车辆网络安全攻击事件引起了较大的社会反响，并威胁到车辆用户和汽车企业的人身和财产安全，大部分车企开始意识到建设网络安全保障能力的重要性。2018 年前后，汽车企业和网络安全技术企业纷纷采取行动，布局汽车网络安全技术和安全保障体系研发，从网络安全管理组织架构建设、汽车产品网络安全研发流程制定，到网络安全威胁分析以及网络安全风险应对策略研究等各方面提升智能网联汽车产品的网络安全水平，避免因网络攻击导致的非法控制，隐私泄露、财产损失甚至人员伤亡，保障智能

网联汽车产业健康发展。

目前，国内外汽车企业正在积极建立专业网络安全部门或者子公司，加强网络安全管理。例如以奔驰为代表的欧美汽车企业通过建设网络安全云平台，使车主能够自主掌控车辆数据的开放程度，提升对个人数据的安全防护。同时在工厂端与第三方网络安全企业合作，挖掘并修复智能网联汽车产品安全漏洞，提升风险防护水平。以日产为代表的日韩企业则在公司内部建立研发管理系统和信息安全平台，提升网络安全管理能力，从产品研发流程层面保障网络安全，同时对外与专业网络安全技术公司合作，提升网络安全防护技术。

国内企业在网络安全防护方面同样在加紧部署，造车新势力开始组建网络安全团队，并与专业网络安全科技公司开展合作，建立以主动防御为核心的网络安全防护体系，从云端、车端、移动端全面保障网络安全。同时传统车企也正在网络安全领域积极跟进，例如上汽集团组织下属企业加入集团网络安全保护与管理体系，统一部署数据加密软件，保证集团整体的数据安全，并通过自建云平台和云计算中心，为车辆产品提供全品类的云安全服务。

**3. 网络安全实践取得初步成果**

在实践层面，各国企业在智能网联汽车网络安全保障方面逐步形成了统一思路，并在相关政策法规和标准的指导下

逐步建立并落实安全设计、制造、测试实践；开展安全风险识别，威胁分析和漏洞挖掘。通过诊断服务、OTA 更新等方式修复安全问题，并持续提升车辆的网络安全防护水平。

国际上，行业巨头已经在智能网联汽车网络安全技术研究和产品合规方面取得了初步成果。2021 年 9 月，恩智浦公司宣布，其研发的 S32G 网关处理器已获得第三方实验室认证，符合最新发布的 ISO/SAE 21434 标准。同期，韩国汽车电子供应商 LG 公司也宣布将收购以色列汽车网络安全专家 Cybellum，通过“数字孪生”方法检测和评估网联汽车服务和硬件中的漏洞，并部署下一代汽车硬件和服务。

我国网络安全技术研究虽然起步较晚，但是经过近年来的快速发展，已经赶上了全球网络安全技术发展进度，成为全球重要的网络安全保障力量。其中我国在相关领域的专利申请量紧随美国之后，高达 38.36%，如下图 1-2 所示。网络安全技术能力的快速提升为我国保障智能网联汽车产品安全运营提供了坚实基础。

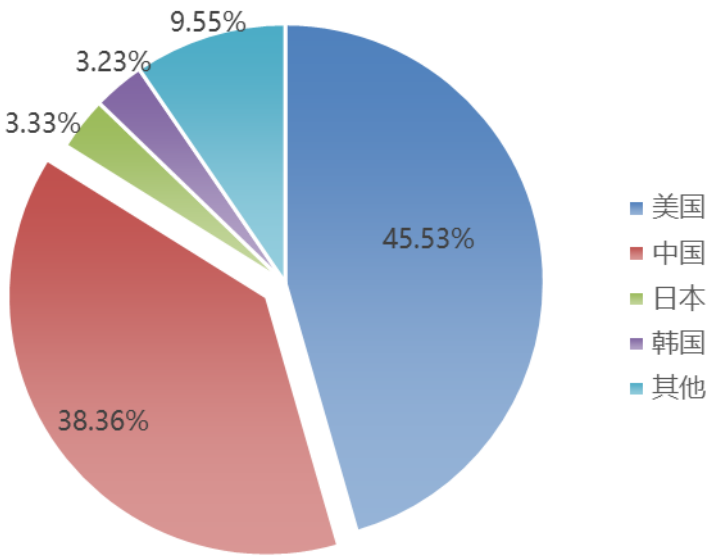



**图 1-2 全球网络安全专利技术来源国分布**

在技术实践方面，早在 2017 年，互联网科技企业 360 就发布了《智能网联汽车信息安全建设最佳实践》，旨在阐述智能网联汽车全生命周期的网络安全保障方法，指导企业有效开展信息安全生态建设。2021 年 6 月，传统整车企业上汽集团发布了网络安全管控标准 2.0，提出了车云协同信息安全和个人信息保护安全模块的建设方案。2021 年 9 月，通信科技企业华为研发的智能汽车解决方案 BU 正式获得汽车网络安全 ISO/SAE21434:2021 符合性证书，成为全球首个通过 DEKRA 德凯 ISO/SAE21434 认证的智能汽车解决方案供应商，标志着我国科技企业已具备为汽车行业客户提供符合业界网络标准的产品方案的能力。

### (二) 政策及法规

#### 1. 国外政策法规发展现状

2018 年 9 月 UNECE WP.29 TFCS 工作组发布了

《UN_ECE-WP.29_recommendations on Cyber Security》等三份指导性文件，成为后续网络安全、数据保护和软件升级标准研制的重要参考依据，其中网络安全指导文件中的ANNEX A “Draft new Regulation on uniform provisions concerning the approval of cyber security” 在 2020 年作为 CSMS 认证与车型审批的正式法规正式颁布，并于 2021 年 1 月正式生效，成为 1958 年协定书（包含了德国、法国等欧盟国家，以及英国、澳大利亚、日本、韩国等国家）缔约国之间通行互认的网络安全认证。

WP.29 在 2020 年 7 月 24 日的工作会议中讨论将 CSMS 认证法规推广至 1998 年协定书缔约国范围。需要指出的是，中国并不在 1958 年协定书缔约国中，但已在 2000 年 10 月 10 日正式加入了 1998 年协定书缔约国，因此我国也将持续关注该领域国际法规的变化，并积极应对相关政策法规的落地对中国车企及中国市场上的国际品牌车企带来的影响。

《WP29-R155-2020 网络安全与网络安全管理系统》法规从网络安全角度提出了对新车辆及其制造组织的要求，规定了 OEM 需要满足的网络安全要求，并计划将该要求作为整车厂获得特定国家范围内，特定车型认证的前提条件。内容框架如下:

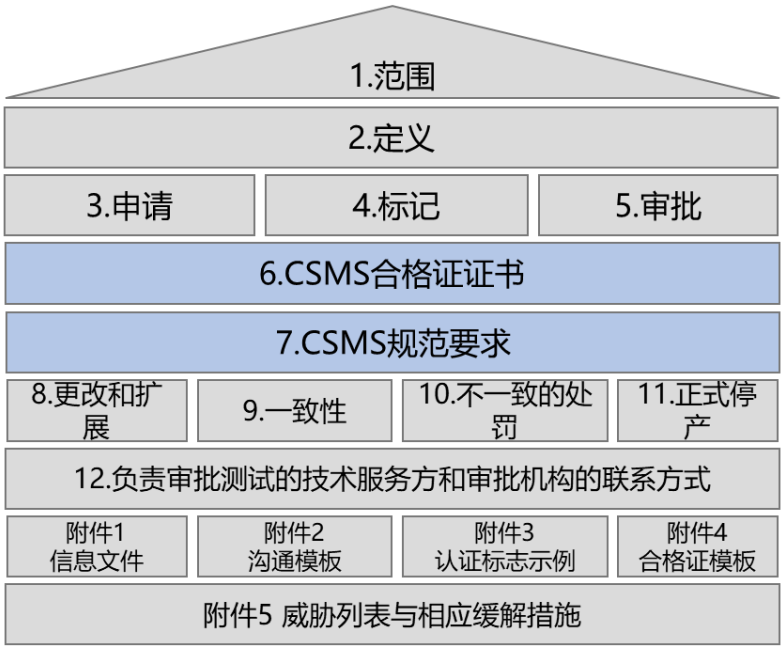



**图 1-3R155 法规内容框架**

R155 法规的适用范围涵盖了 M 类、N 类、至少装有 1 个电控单元的 O 类以及具备 L3 以上自动驾驶功能的车辆。其内容主要包含:

- CSMS (Cyber Security Management System 网络安全管理体系认证)

审查 OEM 是否在汽车的完整生命周期内制定了网络安全相关的保障流程，以确保汽车全生命周期中都有对应的流程措施用以控制相关风险。

- VTA (Vehicle Type Approval 车辆型式审批认证)

针对 OEM 在网络安全开发中的具体工作执行情况进行审查，从而为确保车辆的网络安全防护技术能覆盖全生命周期的安全需求，并保证所实施的网络安全防护方案能够有效应对车辆面对的网络安全风险。

根据法规要求，OEM 必须获得 CSMS 认证证书，并且在特定车型研发及量产项目上充分证明其认证体系中涵盖的流程能够充分且有效运行之后，才具备申请特定车型型式认证的资格。同时法规还供应商管理提出了要求，OEM 需要证明其有能力应对其供应链中来自 Tier1 服务提供商或集团子公司中可能存在的信息安全风险。

除此之外，以美国为代表世界汽车大国，也在国内积极制定政策法规，提升网络安全保障水平。今年 7 月，美国众议院能源与商业委员会投票通过，决定将八项网络安全法案提交到众议院全体会议决议，并均以口头表决的形式获得通过。包括与智能网联汽车网络安全密切相关的 HR 2685《了解移动网络的网络安全情况法案》，旨在敦促美国国家电信与信息管理局( NTIA )检查并报告移动服务网络的网安态势; HR 3919《2021 年安全设备法》，要求禁止各方授权或使用通信委员会在“违禁清单”中列明的企业所提供的网络设备; HR 4028《信息与通信技术战略法案》，旨在分析信息及通信技术供应链中的供应商，确定供应链中的薄弱环节等。

这些法案的通过反映出各国正在高度关注网络安全问题，一方面试图通过政策法规建设保障相关产业的健康发展，另一方面也试图以此作为竞争手段建立自身在网络安全领域的发展主动权。

## 2. 国内政策法规发展现状

由于网络安全属于国家安全战略，而智能网联汽车又在2015年被列为我国国家战略发展的重要内容，因此我国也在政策法规和标准体系建设层面开展了各项工作，保障智能网联汽车网络安全。

2020年2月，国家发改委等11部委联合发布《智能汽车创新发展战略》，明确提出了发展智能汽车的六大具体任务，其中包括构建全面高效的智能汽车网络安全体系，要求完善安全管理联动机制，提升网络安全防护能力，加强汽车数据安全监督管理。并提出到2025年，围绕智能汽车网络安全，建设形成相对完善的政策标准体系。

2020年7月，《数据安全法（草案）》发布，提出了支持促进数据安全与发展的措施、数据安全制度、数据安全保护义务、政务数据安全与开放规则、数据安全工作职责等方面内容。并提出有效应对境内外数据安全风险，建立健全国家数据安全管理制度，完善国家数据安全治理体系。

2020年8月，交通运输部发布《推动交通运输领域新型基础设施建设的指导意见》，要求建设集态势感知、风险预警、应急处置和联动指挥为一体的网络安全支撑平台，加强信息共享、协同联动，形成多层级的纵深防御、主动防护、综合防范体系。

2020年10月21日，《个人信息保护法（草案）》发布，

草案确立了以“告知-同意”为核心的个人信息处理规则，明确了个人信息处理者义务，其中也包含了对人脸识别、隐私曝光数据跨境传输、自动化决策、信息脱敏等热点问题的应对策略。

2021 年 6 月和 8 月，《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》先后开始实施，加上 2017 年开始实施的《中华人民共和国网络安全法》，我国已在网络安全保障领域初步形成了法律体系框架。

2021 年 8 月，工业和信息化部发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》，内容整体框架如下图 1-4 所示。旨在明确原则要求，逐步探索开展准入管理，并基于三部上位法要求，加强数据和网络安全管理，规范软件在线升级、加强产品管理，加快智能网联汽车产品推广应用，推动汽车产业创新发展。

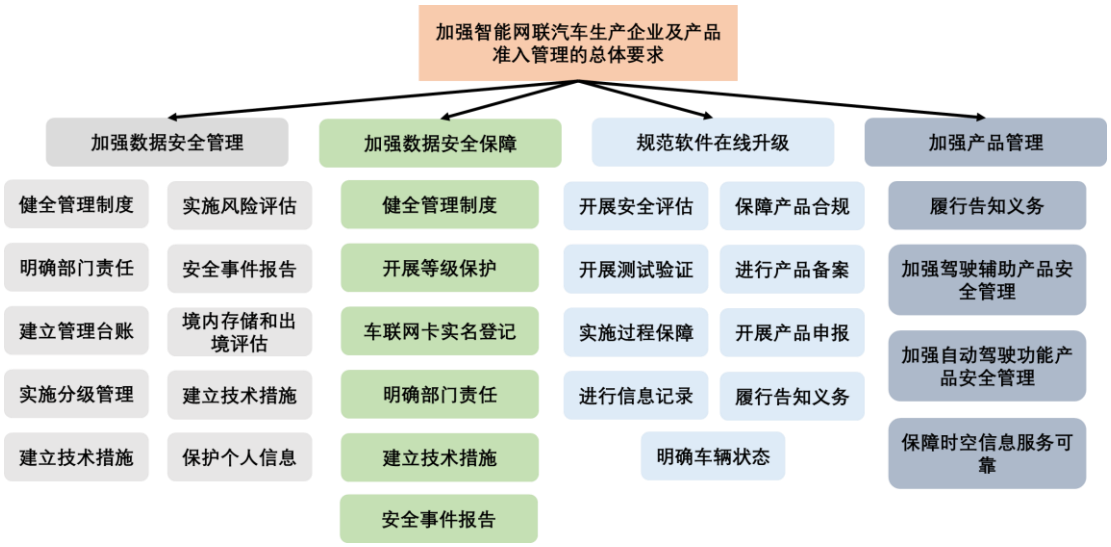



**图 1-4 智能网联汽车准入管理办法内容框架**

相比于 2018 年 12 月发布的《道路机动车辆生产企业及

产品准入管理办法》，新的准入办法中明确提到了《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法规要求，体现出智能网联汽车产品准入管理的特点，也体现出对网络安全和数据安全的重视。同时在总体上，新的准入管理办法要求压实企业主体责任，参考企业安全生产主体责任的制定形式，进一步明确智能网联汽车产品技术研发相关的第一责任人、全员岗位、安全防控、基础管理、应急处置等项具体责任。

### (三) 标准及规范

#### 1. 国外标准规范建设现状

2016 年，SAE 发布《J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems》指导文件，结合威胁分析和风险评估的方法对汽车网络系统的全生命周期安全保障给出了建议，并定义了安全测试方法的框架，给出了市场上主流的安全相关工具及其制造商的列表。

2016 年，ISO 道路车辆技术委员会与 SAE 联合成立 SC32/WG11 Cybersecurity 网络安全工作组，基于 J3061 参考 V 字模型开发流程，制定汽车网络安全标准 ISO/SAE AWI FDIS 21434-2021，提出从风险评估管理、产品开发、运行/维护、流程审核等四方面来保障汽车网络安全工作开展。

ISO/SAE 21434 标准的重点内容包括建立合理的安全保障管理制度，在车辆全生命周期(研发、量产、运行和维护阶

段)建立流程管理体系，如需求管理、追溯性管理、变更管理、配置管理、信息安全/网络安全管理监控和信息安全管理/网络安全事件管理，以及相关的应急响应机制，保障产品免受网络安全攻击。其内容框架如下:

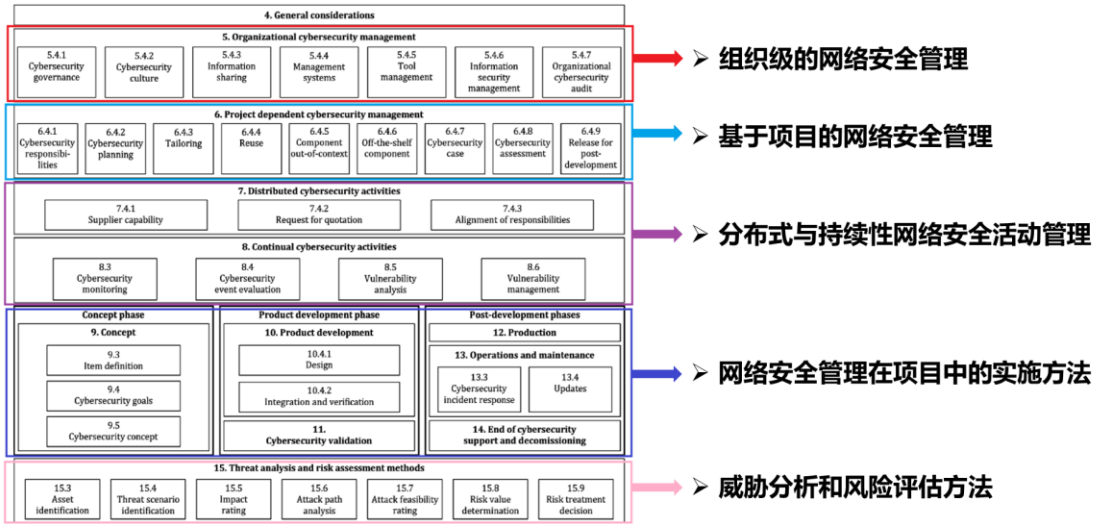



**图 1-5 ISO/SAE 21434 标准内容框架**

## 2. 国内标准规范建设现状

国内为落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律要求，加强车联网（智能网联汽车）网络安全标准化工作顶层设计，也在积极开展标准化建设工作，并取得了初步成果。

2021 年 6 月 21 日，工信部组织编制了《车联网（智能网联汽车）网络安全标准体系建设指南》并面向社会公开征求意见。《指南》针对车载联网设备、基础设施、网络通信、数据信息、平台应用、车联网服务等关键环节，提出覆盖终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等方面的技术架构，见下图 1-6 所示。

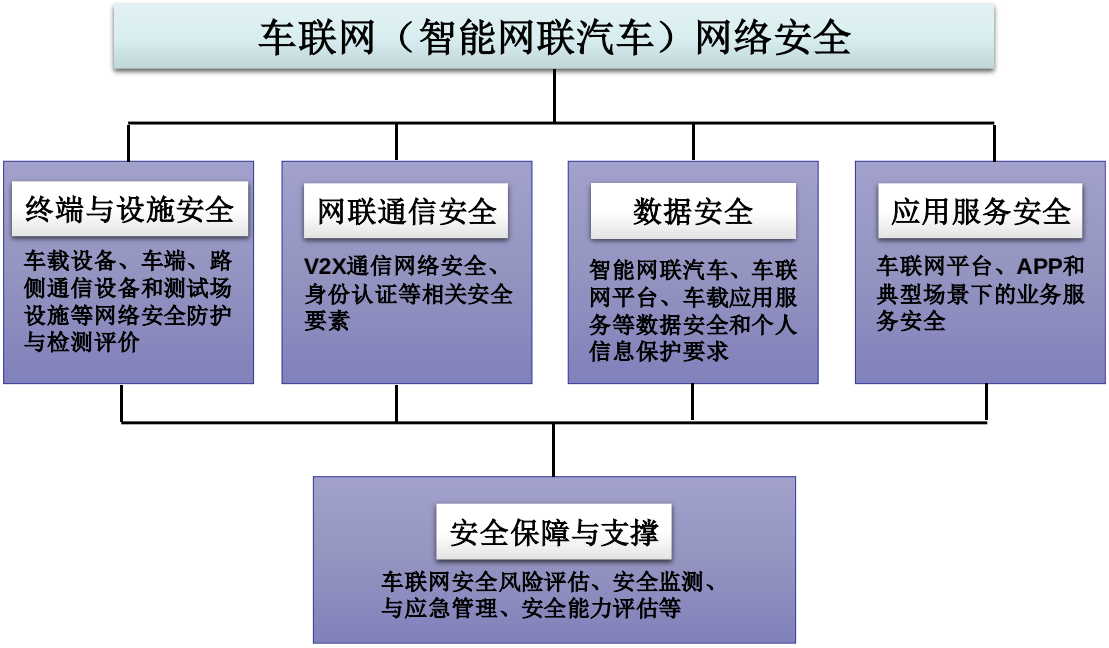



**图 1-6 车联网（智能网联汽车）网络安全技术架构图**

车联网（智能网联汽车）网络安全标准体系框架共六部分内容，其中，总体与基础共性标准包括术语和定义、总体架构、密码应用等三类；终端与设施安全标准包括车载设备安全、车端安全、路侧通信设备安全和测试场设施安全等四类；网联通信安全包括通信安全、身份认证等两类；数据安全包括通用要求、分类分级、出境安全、个人信息保护、应用数据安全等五类；应用服务安全包括平台安全、应用程序安全、服务安全等三类；安全保障与支撑类标准包括风险评估、安全监测与应急管理、安全能力评估等三类，如下图 1-7 所示。

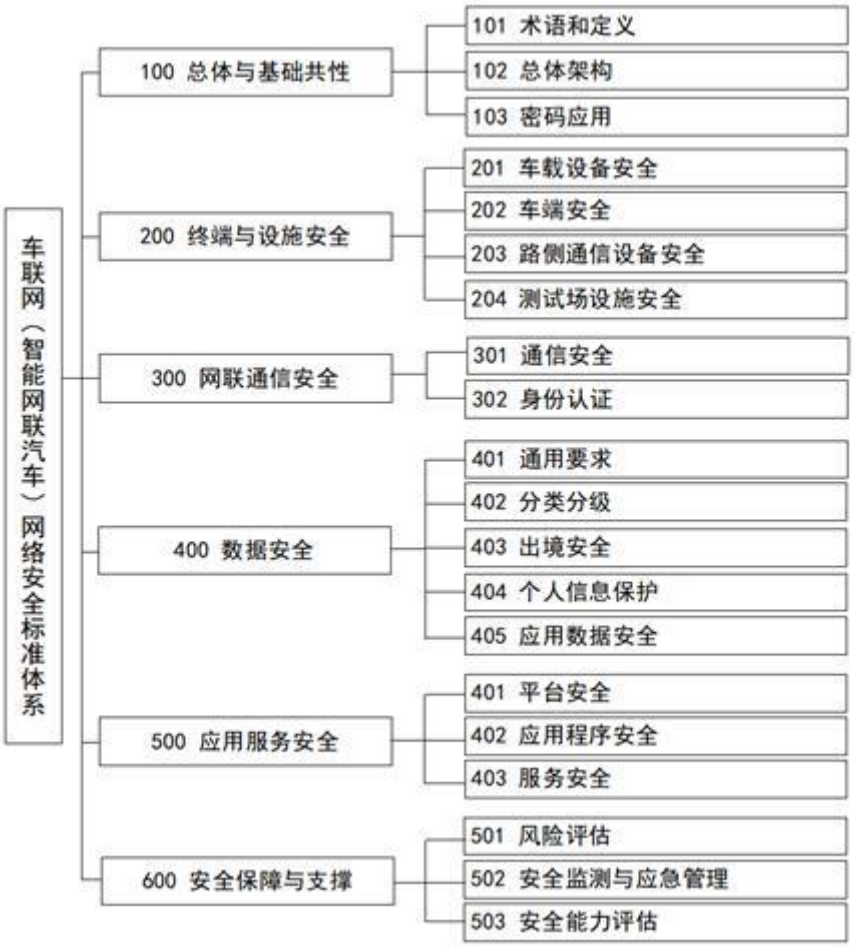



**图 1-7 车联网（智能网联汽车）网络安全标准体系框架**

围绕上述建设规划，目前我国汽标委（SAC/TC 114/SC 34）下设的“汽车信息安全标准工作组”已分 4 批次累计开展了 15 项标准制定及研究项目，其中《车载信息交互系统信息安全技术要求及试验方法》《汽车网关信息安全技术要求及试验方法》等 4 项推荐性国家标准已正式发布；强制性国家标准《汽车软件升级通用技术要求》《汽车整车信息安全技术要求及试验方法》已立项，预计今年年底项目组内征求意见。推荐性国家标准《电动汽车充电系统信息安全技术要求》项目已进入报批阶段；《汽车诊断接口信息安全技术要求》等四项标准已提交立项。除标准制定项目外，陆续开

展了《汽车信息安全风险评估规范》等 5 项标准需求研究项目，为标准制定提供预研成果。

在数据安全标准建设方面，信安标委（TC260）也正在开展标准研究与制定工作，现已发布了 GB/T 35274-2017《信息安全技术 大数据服务安全能力要求》、GB/T 37932-2019《信息安全技术 数据交易服务安全要求》及 GB/T 39477-2020《信息安全技术 政务信息共享 数据安全技术要求》等国家标准，分别针对大数据服务、数据交易及政务信息共享的数据应用场景提出了安全要求。而在检测评估类标准方面，GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》提出了数据安全能力成熟度框架，明确了成熟度各等级的数据安全要求及相关评估方法。上述标准都可以为智能网联汽车领域数据安全标准的制定提供参考。

## 二、智能网联汽车网络安全威胁分析

### (一) 威胁分析方法论

对于智能网联汽车网络安全来说，无论是企业进行风险管理还是渗透测试实施，威胁分析都是最基础的一步。在智能网联汽车网络安全领域，无论是国际上联合国欧洲经济委员会（United Nations Economic Commission for Europe，UNECE）法规、美国高速公路安全管理局（National Highway Traffic Safety Administration，NHTSA）政策、还是国内主管

单位所出台的相关要求均把风险管理和评估放到重要位置。汽车行业网络安全的技术标准 ISO/SAE 21434 给出了技术要求，在该标准中明确了威胁分析和风险评估的分析流程可概括为下图 2-1 所示。

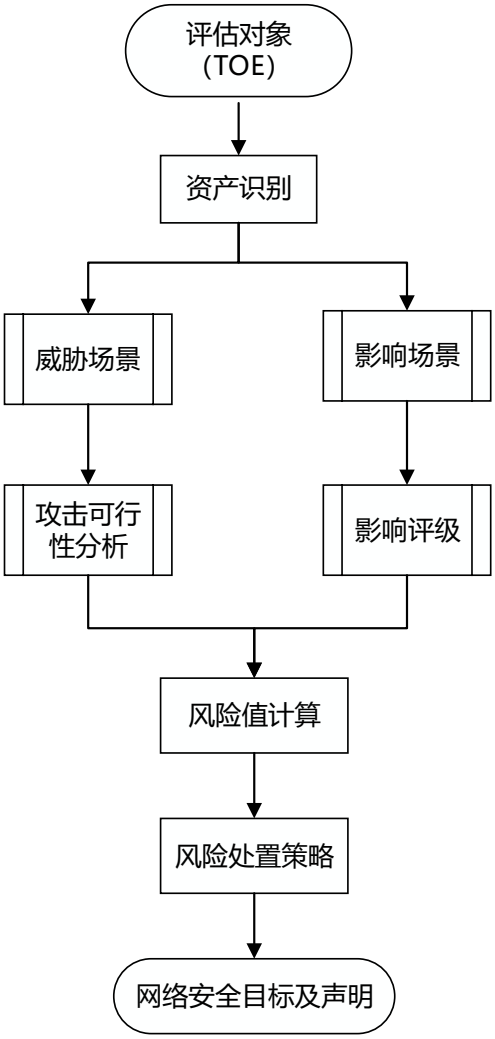



**图 2-1 威胁分析和风险评估的流程**

威胁分析和风险评估完整的流程可理解为攻击者和防护者视角相融合的分析过程。如图 2-1，资产分析之后，左侧的路径“威胁场景->攻击可行性分析”概括的是从攻击者的角度分析目标对象可能存在的漏洞和攻击路径，并对攻击可行性进行分析评级；右侧“影响场景->影响评级”的路径

是从防护者或利益相关方的角度分析破坏资产的安全属性可能带来的危害影响，并对影响等级进行分析；然后根据攻击可行性和危害影响的评级结果来计算风险值，并对应给出不同风险处置策略。以网关 FOTA 升级的威胁分析和风险评估举例，网关作为评估对象，分析破坏网关的可用属性导致控制器固件升级失败的这一威胁场景的攻击可行性，如从 T-Box 发起针对网关发起拒绝服务攻击，破坏网关的可用属性，输出结果为该攻击路径的攻击可行性的值。然后分析网关 FOTA 功能无法使用所带来人身安全、财产损失、车辆运行和隐私法规等方面的影响等级。经过上述两大方面的分析，输出网关执行升级的风险清单。作为防护者，受制于项目开发周期和资源的投入，做出风险处置决议。具体各阶段的流程及内容如下:

**明确评估对象：**明确评估对象环节处于整个威胁分析和风险评估的起点，是分析工作的基础。这一阶段，需要根据业务场景，确定项目对象，明确评估对象的系统构成、功能、边界、接口、数据流等内容。

**资产识别**：所谓资产，是指具有一个或多个网络安全属性的有价值的数据、组件等对象，其网络安全属性的破坏会给利益相关方造成危害及影响。识别评估对象定义范围内的相关资产及其安全属性。通过资产清单列出相关资产，各资产需包括功能属性、安全属性、现有安全措施及所对应的影

响场景。

**影响场景及影响评级：**基于对资产识别的结果，识别项目对象的功能和相关利益者，描述业务场景中核心资产的安全属性受到破坏时，可能造成哪方面的危害。可以从人身安全（S）、财产损失（F）、车辆运行（O）和隐私法规（P）等角度来分类危害的影响，企业也可以定义新的类别，并同步到整个供应链，达成共识。对利益相关方的潜在不利影响进行评级，得出影响等级。

**威胁场景识别：**依据资产识别和影响场景的分析，具体分析通过采取什么行为破坏某资产对应的哪个安全属性，最终导致什么样的后果。在描述威胁场景时，应具体描述资产、影响场景、攻击方法、攻击面之间的关联关系。按照这种方法，罗列所有项目对象的核心资产涉及到的威胁场景。实际中可能会有多个威胁场景导致同一个影响场景的情况，或者同一个威胁场景导致多个影响场景的情况。威胁场景识别可以通过小组讨论、头脑风暴或威胁建模的方法（例如STRIDE、EVITA、TVRA、PASTA 等）开展。

**攻击可行性分析及其等级：**首先，分析威胁场景中涉及的所有攻击路径，可以根据“自顶向下”的方法，将威胁场景逐层分解，尽可能识别所有攻击方案，罗列出具体的攻击方法和实现手段，推断具体哪些路径可以实现攻击，如通过攻击树、攻击图等分析；也可以根据资产网络安全脆弱性识

别的结果构建“自底向上”的攻击路径。在分析攻击路径时应有逻辑地列出相关资产、威胁场景、攻击者、攻击方法、攻击工具和攻击步骤。其次，针对每一条攻击路径，选择基于攻击潜力、CVSS、攻击向量的方法进行攻击可行性等级分析。最后，从专业知识、对目标对象的了解程度、攻陷时间、攻击所需要的设备、机会窗口等方面计算出攻击潜力值，对应得出攻击可行性的等级（高、中、低、极低）。在分析过程中，若发现某个攻击路径不足以完整地导致威胁场景，则此条攻击路径可以被丢弃。

**风险值计算：**针对每个威胁场景的安全等级可以有两种方法得出，第一种是根据已经分析得出的攻击可行性等级和影响等级对照风险值计算矩阵表，得出风险值，对应相应的安全等级。第二种是通过风险计算公式，得到该威胁场景的风险值，对应计算出安全等级。安全等级越高，越需要重视，重点部署相应的保护措施。

**风险处置决策：**针对不同风险值的风险，可以采取规避风险、降低风险、转移风险、保留风险等处置决策。规避风险可以通过移除风险源来实现；降低风险，要定义网络安全目标，并制定防护措施；转移风险和保留风险均要出具网络安全声明，以表明转移风险或保留风险的前提条件及约束条件。在这个过程中企业要根据实际情况和功能安全相结合，综合考虑给出处理方案。

本白皮书中涉及威胁分析的内容包括资产识别、影响场景、威胁场景识别、基于威胁场景的攻击路径分析、攻击可行性分析及其等级，在此分析的基础上可以制定渗透测试指标及方案，为渗透测试做好前期准备工作。风险值的计算及风险处置属于后续产品开发中需进一步执行的操作，本文不作具体展开。

### (二) 整车网络安全资产分析

随着智能网联汽车技术的发展，整车所处的车联网环境越来越复杂，需要保护的资产越来越多，涉及到的威胁点也越来越多。整车网络安全问题的来源是信息的交互，通过梳理通信边界、整车拓扑结构、信息交互场景以及车辆相关功能列表可以识别出核心资产。在此过程中，核心资产的分析可以根据需要从不同维度进行划分。

一是从整车拓扑结构的角度出发。核心资产可以定义到零部件级别，将中央网关、T-Box、IVI 等内、外通信节点列为核心资产；涉及自动驾驶功能，如车载计算平台，其网络安全属性的破坏可以带来功能安全问题的也列为核心资产。

二是从关键应用场景出发。整车在车联网环境下接受云平台的指令和服务，使用的通信协议或涉及到 V2V、V2I 通信的外联设备等都应列为核心资产。

三是从数据安全角度出发。网络安全伴随着数据的流转而产生，可以将某些关键数据，如车辆状态信息、车辆行驶

轨迹及用户信息等重要信息作为核心资产，从攻击向量、攻击路径、攻击面等多个维度构造攻击树，分析其攻击可行性及安全危害程度。

基于威胁分析的基本方法，本文梳理了车联网环境下智能网联汽车的关键核心资产，如下图 2-2。本部分工作为整车渗透分析可能的攻击路径提供基础，为渗透测试实践提供基本思路。

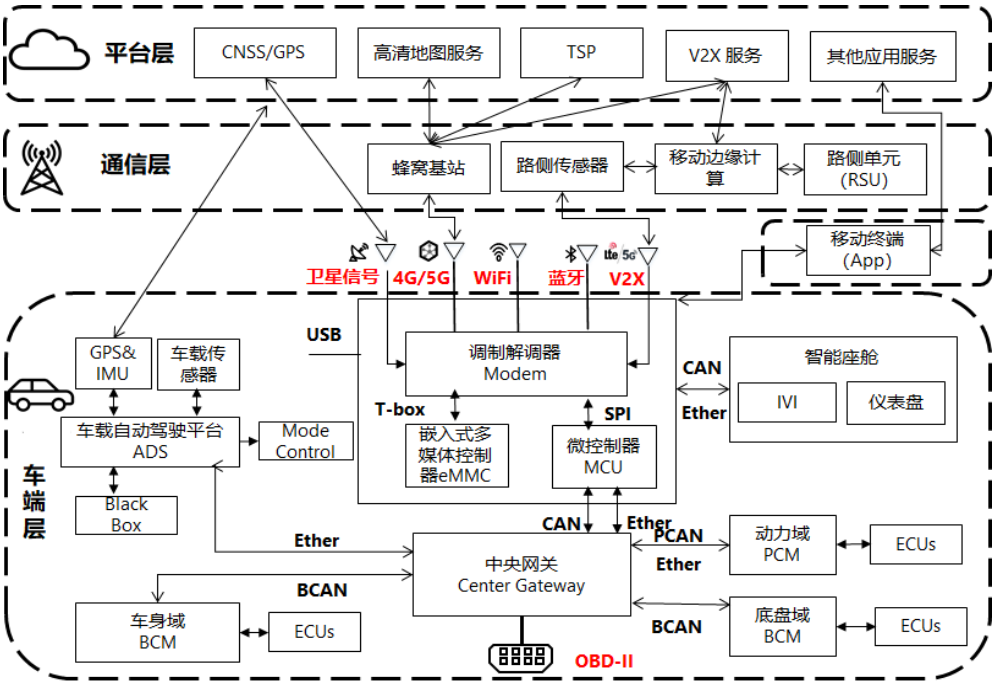



**图 2-2 车联网环境下智能网联汽车的关键核心资产**

### 1. 平台层

平台层包括整车企业对汽车提供远程服务的平台（TSP 平台）、远程升级服务平台（OTA 平台）以及第三方服务平台等。攻击者可以篡改平台给车辆下发的指令，远程控制车辆，对车辆使用者的人身安全造成影响；此外，平台会存储大量用户信息、车辆状态信息以及车辆行驶轨迹，通过平台

漏洞获取平台权限，可以窃取用户信息，造成个人隐私泄露的风险。对于平台的攻击，会波及到所有与平台相连接的车辆、应用及与其相关的所有数据。

随着车辆与平台的交互越来越多，而且远程的控制对于攻击者来说没有物理空间和设备的限制，更容易实现。在2019年所有公开的安全事件中，有25%是来自于对平台的攻击，而2020年在此基础上又增长了70%，攻击平台成为数量排名第一的攻击向量。

**2. 通信层**

通信层包括用于实现车-车、车-路、车-云信息交互的OBU/RSU等设备，以及实现智能交通控制的移动边缘计算。攻击者可以劫持通信会话，篡改通信内容、篡改移动计算结果。车辆收到错误的信息会导致车辆使用者的人身和财产安全受到影响，甚至带来交通安全问题，存在侵害个人或组织的利益、影响社会秩序的风险。

目前车辆和后台通信一般会采用4G/5G的方式，车辆和车辆之间、车辆和道路之间则可能会用到LTE-V。攻击者可以设置伪基站，欺骗通信单元，发送伪造的信息。但是这种方式对攻击设备、攻击环境和攻击人员的专业要求较高，实现的成本比较大。如果发现通信方式采用比较安全的4G/5G的方式，攻击者大概率会选择其他的攻击路径。

**3. 车端**

车辆本身涉及到的核心资产比较多，比如 T-Box、IVI、智能座舱、汽车网关、车载计算平台等。基于以上任一核心资产，都有多种方法破坏其安全属性，造成不同程度的影响。比如，通过系统或软件漏洞获取 IVI root 权限，破解 IVI 与 T-Box 或网关的通信，进一步实现控制 ECU。也可以监听车辆与云平台的通信，实现远程控车。

**4. 移动终端**

移动终端 App 可以让车辆用户更方便快捷地控制车辆，用户可以通过控车 App 实现获得车辆的位置、跟踪车辆轨迹、打开车窗和车门、启动引擎等操作。控车 App 几乎成为新一代车辆的标配，但也成为引入汽车行业中的一个风险因素。控车 App 涉及到第三方提供服务，应用本身代码的漏洞、与平台通信过程中的漏洞、App 的接口调用漏洞等均可以成为攻击向量。

**(三) OTA 升级威胁分析实例**

在软件定义汽车的时代，汽车软件在线升级已成为必然趋势。2021 年 7 月发布的《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见》将软件在线升级纳入准入管理，要求企业生产具有在线升级功能的汽车产品的，应当建立与汽车产品及升级活动相适应的管理能力，具有在线升级安全影响评估、测试验证、实施过程保障、信息

记录等能力。

各主机厂的软件 OTA 方案存在差异化，经过本次渗透测试的摸底调研，可以大体将车辆 OTA 升级方式分为两种类型。主动升级是由车端向云端发起升级请求或影响车辆功能一致性的其他请求。被动升级是云端平台主动推送升级任务到车端，由车辆判定自身升级条件后，进行升级包下载、并将升级包在车内进行转发，找到目标节点。

以 T-Box 为升级主节点的软件在线升级为例，实践 ISO/SAE 21434 给出的威胁分析方法。

### 1. 评估对象及资产识别

以 T-Box 为升级主节点时，识别软件升级的系统构成、功能、边界，接口，数据流，识别资产的安全属性，从机密性（C）、完整性（I）、可用性（A）分析出关键资产。汽车软件 OTA 升级范围及数据流分析见下图 2-3:

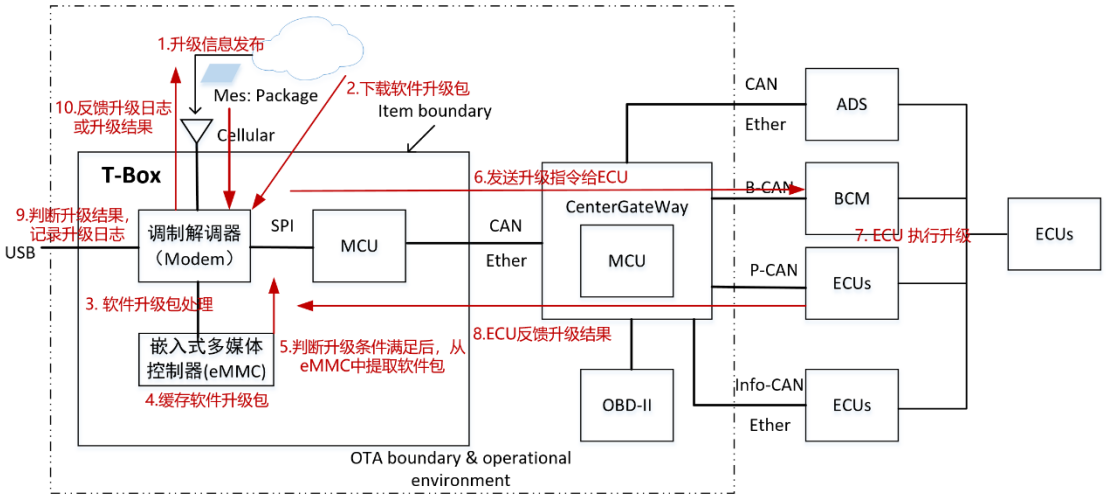



**图 2-3 软件 OTA 升级范围及数据流分析**

车辆软件升级的具体流程总结如下:

（1） 云平台推送升级信息到 T-Box;

（2） 收到升级消息后，车辆根据信息下载升级包;

（3） 升级包下载完成后，T-Box 对升级包进行验签、解包、存储等操作;

（4） 车辆判断车辆的状态及车内总线状态;

（5） 车辆状态符合升级要求后，T-Box 会将升级包发送给 Gateway，Gateway 将升级包发给升级目标 ECU，目标 ECU 执行升级;

（6） 升级后目标 ECU 反馈升级结果到 T-Box，打印升级日志，由 T-Box 将升级日志反馈到云平台。

经以上分析，OTA 过程中所涉及核心资产可概括为数据资产：软件升级包、升级日志信息；零部件资产：T-Box、Gateway、总线及目标 ECU；软件资产：零部件上所运行的系统、程序。

## 2. 影响场景及影响评级

基于对资产的分析，依据 ISO/SAE 21434 中 15.5.2 对影响场景及评级的划分，给出影响场景严重等级分析，如下表 2-1 所示:

**表 2-1 影响场景严重等级分析**

| 影响场景 Damage Scenario | 影响等级 Impact Level | | | | | |
|---|---|---|---|---|---|---|
| | 人身安全 Safety | 财产损失 Financial | 车辆运行 Operational | 隐私和法规 Privacy and legislation | 影响值 Estimating impact level | 影响等级 Value |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 无法正常执行软件升级 | 无伤害 | 0 | 无影响 | 0 | 影响程度低 | 1 | 无影响 | 0 | 1 | 轻微影响 |
| 软件包泄露，导致核心知识产权泄露 | 无伤害 | 0 | 影响程度中 | 100 | 无影响 | 0 | 无影响 | 0 | 100 | 重大影响 |
| 车辆运行状态下，非预期地进入升级模式 | 危及生命伤害 | 1000 | 无影响 | 0 | 影响程度高 | 100 | 无影响 | 0 | 1100 | 重大影响 |
| 写入恶意软件，篡改车辆工作逻辑 | 危及生命伤害 | 1000 | 无影响 | 0 | 影响程度高 | 100 | 无影响 | 0 | 1100 | 重大影响 |
| 升级过程违反国家相关法律法规 | 无伤害 | 0 | 无影响 | 0 | 无影响 | 0 | 影响程度高 | 100 | 100 | 重大影响 |

## 3. 威胁场景及攻击可行性分析

基于对资产和影响场景的分析，依据 ISO/SAE 21434 中 15.4 对威胁场景识别的方法，给出威胁场景分析，以软件升级包的完整性、机密性、可用性被破坏为例，进行威胁场景分析，见表 2-2:

**表 2-2 威胁场景分析**

| | 安全属性识别 | | | 威胁场景 |
|---|---|---|---|---|
| | 机密性 | 完整性 | 可用性 | |
| 关键资产名称 | | √ | | 通过篡改待升级软件包的内容，破坏其完整性，构造出恶意软件写入车载 ECU，引起车端功能逻辑错误 |
| | √ | | | 通过破解升级软件包，导致机密性破坏，窃取其中的核心算法 |
| | | | √ | 通过干扰软件包的下载和升级进程，导致软件包不可用，使得升级过程无法正常开展 |

基于威胁场景结合实际渗透经验，用攻击树的方式总结破坏软件升级包的安全属性可能存在的攻击路径，如图 2-4 所示。

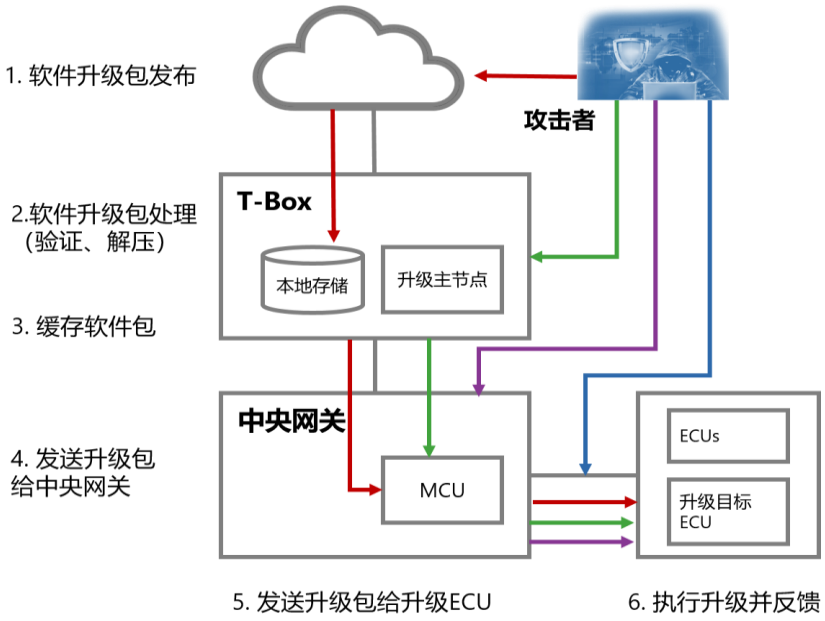



**图 2-4 攻击路径分析**

针对每个威胁场景下的每个攻击路径进行威胁等级评估，即进行可行性分析，从专业知识、对目标对象的了解程度、攻陷时间、攻击所需的设备、机会窗口等进行评估，计算出攻击潜力值，对应得出攻击可行性等级。以实现“通过篡改/伪造升级包内容，使升级失败/ECU 失效功能失效”这一威胁场景的四条攻击路径为例，攻击可行性的评估结果如下表 2-3 所示:

**表 2-3 攻击可行性的评估结果**

| 威胁场景 | 攻击路径 | 威胁等级 Threat Level | | | | | | | | | | | | 攻击可行性等级 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 专业知识 | | 对目标对象的了解程度 | | 攻陷时间 | | 攻击所需要的设备 | | 机会窗口 | | 攻击潜力值 | | |
| 通过篡改/伪造升级包内 | OTA 平台网页漏洞扫描-网页扫描/系统漏洞-发现下载升级包链接-获 | 外行 | 0 | 公开 | 0 | <一周 | 0 | 标准 | 0 | 困难 | 10 | 10 | | 高 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 容，使升级失败/ECU失效功能失效 | 取升级包-篡改升级包内容 | | | | | | | | | | | | |
| | CAN 总线监听数据流，依据 UDS 协议要求，找到与网关的通信，获取升级包-篡改升级包内容 | 能手 | 3 | 保密 | 3 | <一个月 | 1 | 专用 | 4 | 中等 | 4 | 15 | 中 |
| | 寻找 T-Box 的业务逻辑漏洞，获取升级包-篡改升级包内容 | 能手 | 3 | 保密 | 3 | <一个月 | 1 | 专用 | 4 | 中等 | 4 | 15 | 中 |
| | 物理拆解 T-Box，从车端存储升级包的芯片中提取固件-获取升级包-篡改升级包内容 | 能手 | 3 | 保密 | 3 | <一个月 | 1 | 专用 | 4 | 困难 | 10 | 21 | 低 |

综上，对软件 OTA 升级的资产进行识别，分析影响场景并给出评级，分析威胁场景，并基于此分析攻击路径和攻击可行性，为整车渗透测试实践提供理论基础，指导测试指标的梳理。

## 三、智能网联汽车网络安全渗透测试指标

### (一) 测试依据

中国软件评测中心参考《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》《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见》中提出的网络安全具体要求，以及依据 ISO/SAE-21434《道路车辆 信息安全工程》、GB/T

40861-2021《汽车信息安全通用技术要求》、GB/T 40857-2021《汽车网关信息安全技术要求及试验方法》、GB/T40856-2021《车载信息交互系统信息安全技术要求及试验方法》等国内外标准，结合威胁分析的结果，总结渗透测试指标。

### (二) 测试指标

智能网联汽车整车网络安全威胁分析及渗透测试指标主要从信息传输安全、外部连接安全、数据安全、物理非法操作等方面展开，测试指标如下图 3-1。

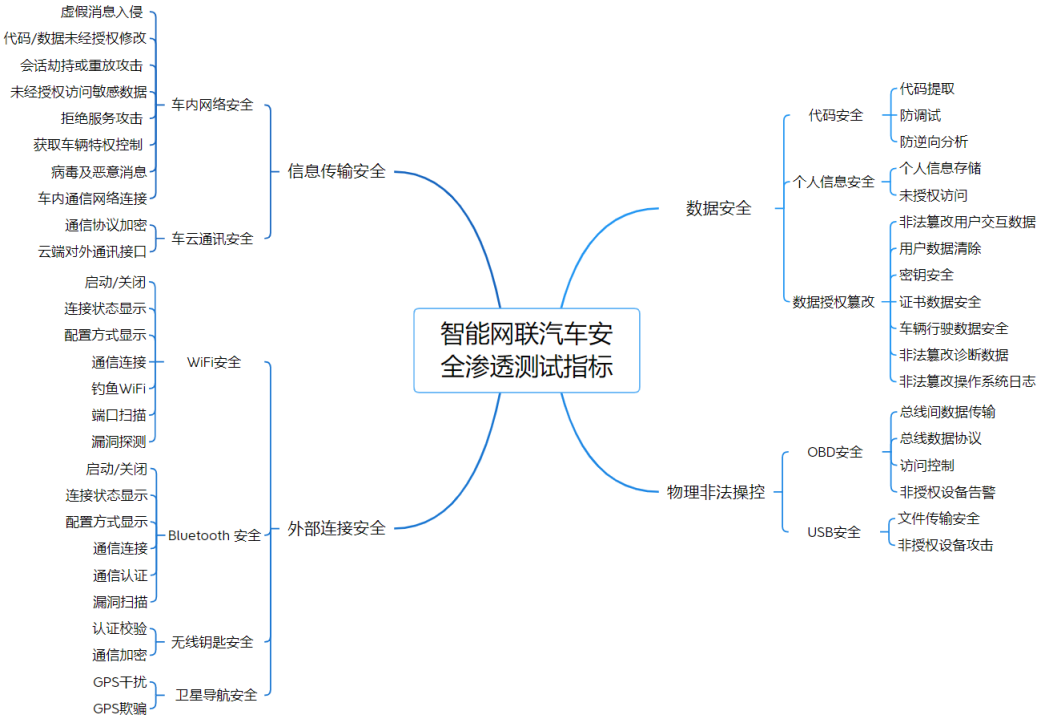



**图 3-1 渗透测试指标**

### (三) 测试内容

#### 1. 信息传输安全

信息传输安全测试从车内网络安全和车云通信安全两

个方面开展。车内网络安全主要针对车内网络设备（T-Box、IVI 等）系统的安全性进行测试，测试内容包括虚假消息入侵、代码/数据未经授权修改、会话劫持或重放攻击、未经授权访问敏感数据、拒绝服务攻击、获取车辆特权控制、病毒及恶意消息。车云通信安全主要针对汽车和云平台通信的安全性进行测试，测试内容包括车内通信网络连接、云端对外通信接口、通信协议。

**2. 外部连接安全**

外部连接安全测试从 Wi-Fi、蓝牙、无线钥匙和卫星导航四个方面开展。Wi-Fi 安全主要针对车机通过 Wi-Fi 与外部设备连接的安全性进行测试，测试内容包括启动/关闭、连接状态显示、配置方式显示、通信连接、钓鱼 Wi-Fi、端口扫描、漏洞探测。蓝牙安全主要针对车机通过蓝牙与外部设备连接的安全性进行测试，测试内容包括启动/关闭、连接状态显示、通信认证、漏洞扫描等。无线钥匙安全主要监听无线钥匙通信内容查看是否存在漏洞，测试内容包括认证校验、通信加密。卫星导航安全主要针对汽车导航定位模块的安全性进行测试，测试内容包括 GPS 干扰、GPS 欺骗。

**3. 数据安全**

数据安全测试从代码安全、个人信息安全和数据非授权篡改三个方面开展。代码安全主要针对车机应用和手机应用的代码安全性进行测试，测试内容包括代码提取、防调试、

防逆向分析。个人信息安全主要针对车机和手机应用的个人信息安全性进行测试，测试内容包括个人信息存储、未授权访问。数据非授权篡改主要针对车机和手机应用敏感数据的安全性进行测试，测试内容包括非法篡改用户交互数据、用户数据清除、密钥安全、证书数据安全、车辆行驶数据安全、非法篡改诊断数据、非法篡改操作系统日志。

**4. 物理非法操控**

物理非法操控从 OBD 安全和 USB 安全两个方面开展。OBD 安全主要测试内容包括总线间数据包传输、总线数据协议、访问控制、非授权设备告警。USB 安全主要测试内容包括文件传输安全、非授权设备攻击。

## 四、智能网联汽车网络安全渗透实践

### (一) 背景介绍

为了贯彻落实《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理意见》，测试验证目前智能网联汽车网络安全防护情况，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）在中国智能网联汽车产业创新联盟指导下，联合国家信息技术安全研究中心、北京航空航天大学、国汽（北京）智能网联汽车研究院有限公司，在全国范围内启动了智能网联汽车渗透测试工作。本次测试实践的前提要求是不损坏车辆、不拆解车辆、黑盒测试，开展用户

侧渗透测试。本次测试共 15 辆车，被测车辆覆盖传统车企和造车新势力产品，其中新能源车 9 辆，燃油车 6 辆。具体信息如下表 4-1 所示。

**表 4-1 被测车型列表**

| 车型 | |
|---|---|
| 北汽极狐 | 理想 ONE |
| 红旗 E-QM5 | 蔚来 ES6 |
| 比亚迪元 | 广汽 GS8 |
| 吉利 GSe | 沃尔沃 XC40 |
| 比亚迪唐 | 奥迪 A4L |
| 奔驰 GLE450 | 沃尔沃 S90 |
| MINICooperS countryman | 吉利领克 01 |
| | 轩逸 日产 |

## (二) 渗透测试结果概要

通过本次渗透实践共发现 15 种典型问题。具体问题类型及检出率如下图 4-1 所示。其中高频问题集中在 Wi-Fi 安全、GPS 欺骗、未授权访问敏感数据、安装包逆向风险等。

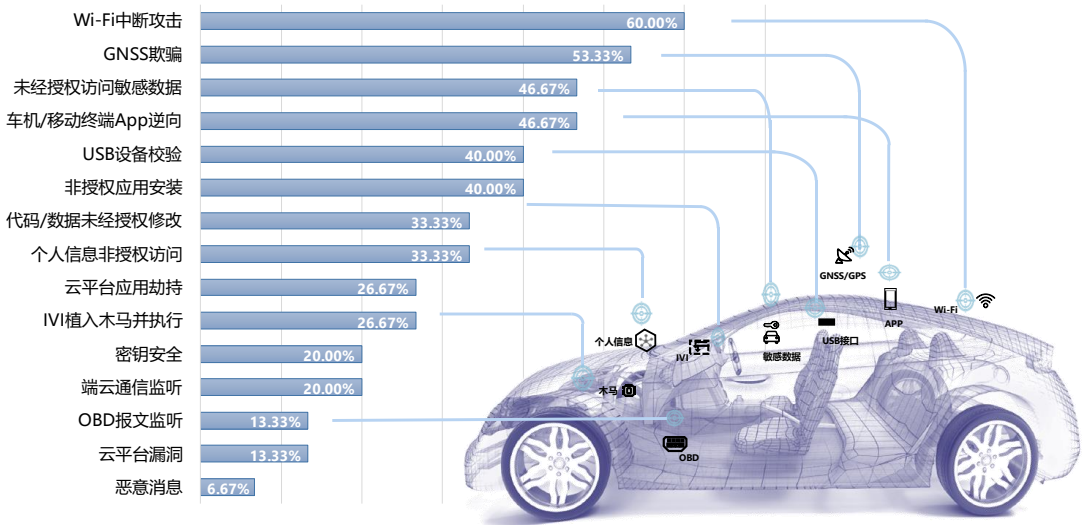



**图 4-1 问题检出率**

依据威胁分析方法论，本文对上述安全问题的攻击可行性和安全影响分别进行了分析。

如表 4-2 所示，本文从对专业知识的依赖程度、对目标对象的了解程度、攻击时间、设备需求、难易程度 5 个方面分析了以上问题的攻击可行性。其中，Wi-Fi 中断攻击、GPS 欺骗、云平台应用劫持以及扫描云平台漏洞 4 种安全问题所需付出的攻击成本较低，因而也更容易成为攻击者的目标。相比之下，密钥安全和恶意消息攻击因为需要攻击者具备较高的网络安全技术水平和对攻击目标的深入了解，并辅助以专业设备，所需付出的攻击成本较高，从而降低了攻击可行性。

在表 4-3 中，从网络安全问题对人身安全、财产安全、车辆运行安全、个人隐私安全四个方面的影响程度对影响等级进行分析。发现 GPS 欺骗、未经授权访问敏感数据、非授权应用安装、代码/数据未经授权修改、个人信息非授权访问、

IVI 植入木马并执行、密钥安全、OBD 报文监听 8 项网络安全问题均能造成严重影响。其中 GPS 欺骗可能对车辆的正常运行产生严重干扰；未经授权访问敏感数据和个人信息则会给个人隐私带来威胁；非授权应用安装和代码修改、密钥安全、端云通信监听问题和 OBD 监听可能造成用户财产和隐私数据的流失，并影响车辆运行安全。

**表 4-2 网络安全问题攻击可行性等级分析**

| 攻击路径 | 专业知识 | 目标对象了解程度 | 攻陷时间 | 攻击所需要的设备 | 机会窗口 | 攻击可行性等级 |
|---|---|---|---|---|---|---|
| Wi-Fi 中断攻击:尝试中断 WiFi 连接 | 外行 | 公开 | <一周 | 标准 | 容易 | 高 |
| GPS 欺骗:使用工具对 GPS 的地址位置进行欺骗，检测汽车定位和导航是否可以正常使用 | 能手 | 公开 | <一周 | 专用 | 容易 | 高 |
| 未经授权访问敏感数据:检测未授权用户是否能访问敏感数据 | 能手 | 保密 | <一个月 | 专用 | 中等 | 中 |
| 非授权应用安装 | 能手 | 保密 | <一个月 | 专用 | 中等 | 中 |
| 代码/数据未经授权修改:尝试进入 T-Box 或 IVI 工程模式，进入系统修改代码或数据，是否能成功修改 | 能手 | 保密 | <一个月 | 专用 | 中等 | 中 |
| 个人信息非授权访问 | 专家 | 保密 | <一个月 | 专用 | 中等 | 中 |
| 云平台应用劫持 | 能手 | 公开 | <一个月 | 标准 | 中等 | 高 |
| IVI 植入木马并执行:检查被测样件是否能被植入病毒并执行，向被测样件发送恶意消息是否被响应 | 专家 | 保密 | <一个月 | 专用 | 中等 | 中 |
| 密钥安全 | 专家 | 机密 | <=6 个月 | 专用 | 中等 | 非常低 |
| 端云通信监听:监听车端和云端通信，查看是否采用安全通信协议 | 能手 | 公开 | <一个月 | 标准 | 中等 | 高 |
| OBD 报文监听:检查安全区域间是否采用边 | 能手 | 保密 | <一个月 | 定制 | 中等 | 中 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 界访问控制机制对来访的报文进行控制 | | | | | | |
| 云平台漏洞:获取车辆服务平台 URL，通过测试工具进行漏洞扫描 | 外行 | 公开 | <一周 | 标准 | 困难 | 高 |
| 恶意消息:检查被测样件是否能被植入病毒并执行，向被测样件发送恶意消息是否被响应 | 专家 | 机密 | <一个月 | 定制 | 中等 | 非常低 |

**表 4-3 网络安全问题影响等级分析**

| 攻击路径 | 人身安全 | 财产损失 | 车辆运行 | 隐私和法规 | 影响等级 |
|---|---|---|---|---|---|
| Wi-Fi 中断攻击:尝试中断 WiFi 连接 | 无伤害 | 无影响 | 影响程度低 | 影响程度低 | 轻微影响 |
| GPS 欺骗:使用工具对 GPS 的地址位置进行欺骗，检测汽车定位和导航是否可以正常使用 | 轻度伤害 | 影响程度低 | 影响程度中 | 无影响 | 中等影响 |
| 未经授权访问敏感数据:检测未授权用户是否能访问敏感数据 | 无伤害 | 影响程度低 | 无影响 | 影响程度高 | 重大影响 |
| 非授权应用安装 | 无伤害 | 影响程度中 | 影响程度低 | 影响程度中 | 重大影响 |
| 代码/数据未经授权修改:尝试进入 T-Box 或 IVI 工程模式，进入系统修改代码或数据，是否能成功修改 | 无伤害 | 影响程度中 | 影响程度高 | 影响程度高 | 重大影响 |
| 个人信息非授权访问 | 无伤害 | 影响程度 | 无影响 | 影响程度 | 重大影响 |

| | | | | | |
|---|---|---|---|---|---|
| | | 低 | | 高 | |
| 云平台应用劫持 | 无伤害 | 影响程度低 | 影响程度低 | 影响程度中 | 轻微影响 |
| IVI 植入木马并执行:检查被测样件是否能被植入病毒并执行，向被测样件发送恶意消息是否被响应 | 无伤害 | 影响程度中 | 影响程度高 | 影响程度高 | 重大影响 |
| 密钥安全 | 无伤害 | 影响程度中 | 影响程度中 | 影响程度高 | 重大影响 |
| 端云通信监听:监听车端和云端通信，查看是否采用安全通信协议 | 无伤害 | 无影响 | 无影响 | 影响程度中 | 轻微影响 |
| OBD 报文监听:检查安全区域间是否采用边界访问控制机制对来访的报文进行控制 | 无伤害 | 无影响 | 影响程度高 | 影响程度中 | 重大影响 |
| 云平台漏洞:获取车辆服务平台 URL，通过测试工具进行漏洞扫描 | 无伤害 | 无影响 | 影响程度低 | 影响程度中 | 轻微影响 |
| 恶意消息:检查被测样件是否能被植入病毒并执行，向被测样件发送恶意消息是否被响应 | 无伤害 | 无影响 | 影响程度低 | 影响程度中 | 轻微影响 |

基于对上述网络安全问题的分析结果，从攻击可行性和影响程度两个方向综合考虑，得出对各网络安全问题进行安全防护的重要性，如下图 4-2 所示。

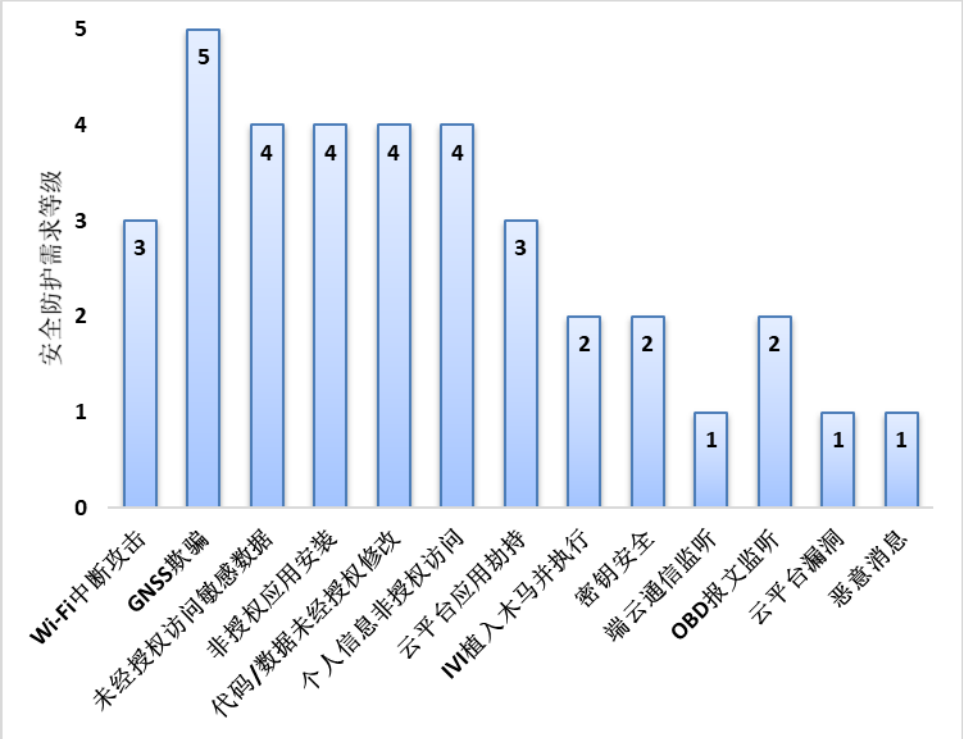



**图 4-2 安全防护需求分析**

其中，均迫切需针对 GPS 欺骗、未经授权访问敏感数据、非授权应用安装、代码/数据未经授权修改、个人信息非授权访问 5 项网络安全问题开展防护工作，提升车辆网络安全水平。其中，GPS 欺骗因为攻击成本低，安全影响后果严重，成为安全防护需求等级最高的项目。

### (三) 关键问题分析

#### 1. 车端个人敏感信息泄露

**（1） 为什么要保护个人敏感信息？**

隐藏自己，不让自己暴露。暴露个人敏感信息本身就是

一种风险，用户在使用车辆的过程中往往会将个人明感信息与车辆绑定，如系统账号、电话号码、通讯录等。个人敏感信息保护是对人的基本尊重。人们有时满足自身好奇心的方式就是窥探他人敏感信息，甚至是隐私信息，这是一种违法行为。车辆应注意保护用户的个人隐私，避免因车辆的网络安全问题泄露个人隐私，使其成为攻击目标。

影响信任关系。比如，我们在开车出行时需要使用语音助手告诉汽车我们将要前往的目的地，这本身就是一种信任关系。个人敏感信息保护是我们对车辆本身信任的基本条件。如果企业不重视个人信息安全防护，违反与用户达成的信息保护协议，不仅违背道德、触犯法律，而且也破坏了用户与车辆生产企业或运营企业之间的信任关系。没有信任，其他的商业行为也就不可能继续并且生存下去。

**（2） 智能网联汽车涉及哪些个人信息？**

2021 年 8 月签发第 91（号）主席令，颁布《中华人民共和国个人信息保护法》。该法案中第二十八条中定义，敏感个人信息指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

随着汽车智能化的快速发展，车辆在使用过程中必然会采集、处理、传输、存储个人敏感信息，甚至隐私数据，如

个人声纹信息、身份信息、位置信息、及行驶轨迹信息等等。其目的是为了识别用户身份，方便用户使用车辆更加丰富的功能，例如车载娱乐功能、自动泊车功能及部分自动驾驶功能等等。因此如何安全合理的使用个人敏感信息成为智能网联汽车行业所要面临的关键问题之一。

**（3） 测试内容**

通过安全威胁分析的前期工作，确定可能涉及个人信息安全的关键零部件包括 IVI、车载网关、TCU、VCU 及部分关键 ECU 等等。尝试通过渗透手段，进入这些车辆关键部件系统，搜索、查看、篡改系统运行信息、系统配置文件、日志文件。尝试在非授权条件下获取用户敏感数据、读写用户个人信息、导出与用户相关的个人敏感数据等。

**（4） 测评结果分析**

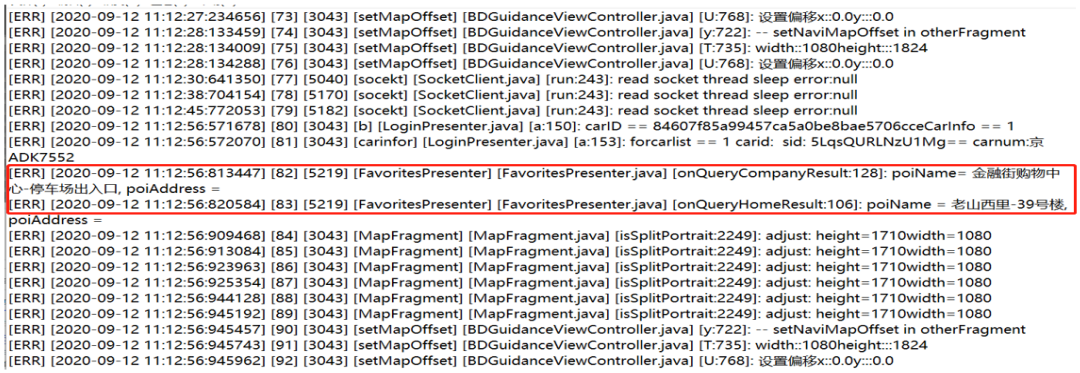
通过本次渗透测试，发现被测车辆中有 56%的车型存在个人敏感信息泄露的问题，可以在非授权访问的情况下访问用户个人敏感信息及隐私数据，如车辆位置信息、车辆软件升级信息（如下图 4-3 所示）及个人身份信息等。

其中 60%的被测车辆可以通过入侵系统、激活工程模式，提取和拷贝车辆行驶日志（如下图 4-4 所示），地图位置日志，T-Box 运行日志（如下图 4-5 所示，为 T-Box 中获得的某条控车指令）等；40%的被测车辆可在非授权条件下访问用户的通讯录（如下图 4-6 所示）、图片、视频等个人

信息；个别被测车辆可以实现通过非法安装木马的方式，打开车内麦克风，在车辆行驶过程中录制车内对话内容，窃取用户信息。

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="hellow">helloworld</string>
    <string name="update">Tbox固件升级</string>
    <string name="back">返回</string>
    <string name="startFtpServer">开启FTp服务</string>
    <string name="no_tbox_update_file">没检测到TBox升级文件</string>
    <string name="tbox_update_file_too_much">检测到多份TBox升级文件,请确保只有一份升级文件</string>
    <string name="eth1_state_error">网卡状态异常，请打开网络开关</string>
    <string name="updateing">正在升级中...</string>
    <string name="ftp_users">ftpserver.user  min.userpassword=A  \10 ftpserver.user.admin.l
    <string name="update_fail">升级失败</string>
    <string name="update_fail_timeout">12 minutes overtime</string>
    <string name="update_fail_TBOX">TBOX回复升级失败，请导出TBOXLOG</string>
    <string name="update_success">升级成功</string>
    <string name="udisk_notfind">U盘未挂载</string>
    <string name="udisk_path">/mnt/udisk2</string>
</resources>
```

**图 4-3 OTA 软件升级信息**



```
[ERR] [2020-09-12 11:12:27:234656] [73] [3043] [setMapOffset] [BDGuidanceViewController.java] [U:768]: 设置偏移x::0.0y:::0.0
[ERR] [2020-09-12 11:12:28:133459] [74] [3043] [setMapOffset] [BDGuidanceViewController.java] [y:722]: -- setNaviMapOffset in otherFragment
[ERR] [2020-09-12 11:12:28:134009] [75] [3043] [setMapOffset] [BDGuidanceViewController.java] [T:735]: width::1080height:::1824
[ERR] [2020-09-12 11:12:28:134288] [76] [3043] [setMapOffset] [BDGuidanceViewController.java] [U:768]: 设置偏移x::0.0y:::0.0
[ERR] [2020-09-12 11:12:30:641350] [77] [5040] [socekt] [SocketClient.java] [run:243]: read socket thread sleep error:null
[ERR] [2020-09-12 11:12:38:704154] [78] [5170] [socekt] [SocketClient.java] [run:243]: read socket thread sleep error:null
[ERR] [2020-09-12 11:12:45:772053] [79] [5182] [socekt] [SocketClient.java] [run:243]: read socket thread sleep error:null
[ERR] [2020-09-12 11:12:56:571678] [80] [3043] [b] [LoginPresenter.java] [a:150]: carID == 84607f85a99457ca5a0be8bae5706cceCarInfo == 1
[ERR] [2020-09-12 11:12:56:572070] [81] [3043] [carinfor] [LoginPresenter.java] [a:153]: forcarlist == 1 carid:  sid: 5LqsQURLNzU1Mg== carnum:京
ADK7552
[ERR] [2020-09-12 11:12:56:813447] [82] [5219] [FavoritesPresenter] [FavoritesPresenter.java] [onQueryCompanyResult:128]: poiName= 金融街购物中
心-停车场出入口, poiAddress =
[ERR] [2020-09-12 11:12:56:820584] [83] [5219] [FavoritesPresenter] [FavoritesPresenter.java] [onQueryHomeResult:106]: poiName = 老山西里-39号楼,
poiAddress =
[ERR] [2020-09-12 11:12:56:909468] [84] [3043] [MapFragment] [MapFragment.java] [isSplitPortrait:2249]: adjust: height=1710width=1080
[ERR] [2020-09-12 11:12:56:913084] [85] [3043] [MapFragment] [MapFragment.java] [isSplitPortrait:2249]: adjust: height=1710width=1080
[ERR] [2020-09-12 11:12:56:923963] [86] [3043] [MapFragment] [MapFragment.java] [isSplitPortrait:2249]: adjust: height=1710width=1080
[ERR] [2020-09-12 11:12:56:925354] [87] [3043] [MapFragment] [MapFragment.java] [isSplitPortrait:2249]: adjust: height=1710width=1080
[ERR] [2020-09-12 11:12:56:944128] [88] [3043] [MapFragment] [MapFragment.java] [isSplitPortrait:2249]: adjust: height=1710width=1080
[ERR] [2020-09-12 11:12:56:945192] [89] [3043] [MapFragment] [MapFragment.java] [isSplitPortrait:2249]: adjust: height=1710width=1080
[ERR] [2020-09-12 11:12:56:945457] [90] [3043] [setMapOffset] [BDGuidanceViewController.java] [y:722]: -- setNaviMapOffset in otherFragment
[ERR] [2020-09-12 11:12:56:945743] [91] [3043] [setMapOffset] [BDGuidanceViewController.java] [T:735]: width::1080height:::1824
[ERR] [2020-09-12 11:12:56:945962] [92] [3043] [setMapOffset] [BDGuidanceViewController.java] [U:768]: 设置偏移x::0.0y:::0.0
```

**图 4-4 车辆行驶记录**

```
D/TCU 4G  (  835): send SignalQulity request.
D/TCU Native(  835): business data(0 bytes): protocol version 0x0601, business ID 0x0601
D/TCU Native(  835): pro    data(13 bytes):
D/TCU Native(  835): 6C 79 0D 00 01 06 01 06 00 C1 40 BB 66
I/TCU Native(  835): send 44, data : 0x01,0x06, len:13
D/TCU DataDispatcher(  835):    data(13 bytes): Business ID = 601
D/TCU TimeOutHandler(  835): receive message: onMessageRequest >>> 1537 Request.
D/TCU DataDispatcher(  835): R    ved Protocol Package from native: 08 05
D/TCU ProtocolAnalyzer(  835): Business ID: 8601 is handled by module "4G" (com.lanyou.tcu.protocol.b.c@2cfe9880)
D/TCU TimeOutHandler(  835): receive message: onMessageResponse <<<<<< 1537 response.
D/TCU 4G  (  835): [ Module4GHandler @Override  handleBusinessData] get Signal level: 5
D/TCU DeviceManager(  835):    Manager @Override onSignalLevelUpdate] get Signal level: 5
D/TCU Native(  835): receive 46 bytes via socket: write to circle buffer 46 bytes.
D/TCU Native(  835): 6C 79 2E 00 01 06 05 86 00 0A 0A 43 48 4E 2D 55 4E 49 43 4F 4D 12 0F 34 36 30 30 39 38 30 34 34 37 30 37 33 38 38 18 01 20 01 81 22 BB
66
D/TCU Native(  835): post business data ID = 0x8605 (33 bytes)
D/TCU Module4GStatusListener(  753): signal quality report: 5
D/TCU DataDispatcher(  835): receive package: [B@2d03c020 from native, handle data by Thread[Thread-54,5,main]
D/TCU serviceLibrary DeviceManager( 1424): ++++++++++++++++++++++++++++++++++++++++++++++ return mDeviceManager.getMobileSignalQuality
D/TCU DataDispatcher(  835): handle native post data success.
D/TCU DataDispatcher(  835): Received Protocol Package from native: 0a 0a 43 48 4e 2d 55 4e 49 43 4f 4d 12 0f 34 36 30 30 39 38 30 34 34 37 30 37 33 38 38 1
8 01 20 01
D/TCU ProtocolAnalyzer(  835): Business ID: 8605 is handled by module "4G" (com.lanyou.tcu.protocol.b.c@2cfe9880)
D/TCU TimeOutHandler(  835): receive message: onMessageResponse <<<<<< 1541 response.
D/TCU DeviceManager(  835): ----------> datalink state report: true, usb state report: true
I/wanghuan(  553): current signal level is5
D/TCU Module4GStatusListener(  553): signal quality report: 5
D/TCU DeviceManager(  835): [ DeviceManager getMobileSignalQuality ] get Signal level: 5
D/TCU 4G  (  835): send SignalQulity request.
D/TCU Native(  835): business data(0 bytes): protocol version 0x0601, business ID 0x0601
D/TCU Native(  835): protocol data(13 bytes):
D/TCU Native(  835): 6C 7    00 01 06 01 06 00 C1 40 BB 66
I/TCU Native(  835): send 44, data : 0x01,0x06, len:13
D/TCU DataDispatcher(  835): send data(13 bytes): Business ID = 601
D/TCU TimeOutHandler(  835): receive mess    ageRequest >>> 1537 Request.
D/TCU Module4GStatusListener(  753): datalink available state: true
D/TCU 4G  (  835): ~~~~~~~~~~~~~~~~~~ Message Network State Report: networkName = CHN-UNICOM  IMEI = 460098044707388, datalink available = true, usblink ava
ilable = true
D/TCU Native(  835): receive 15 bytes via socket: write to circle buffer 15 bytes.
D/TCU Native(  835): 6C     00 01 06 01 8(    5 C0 16 BB 66
```

**图 4-5 控车指令**

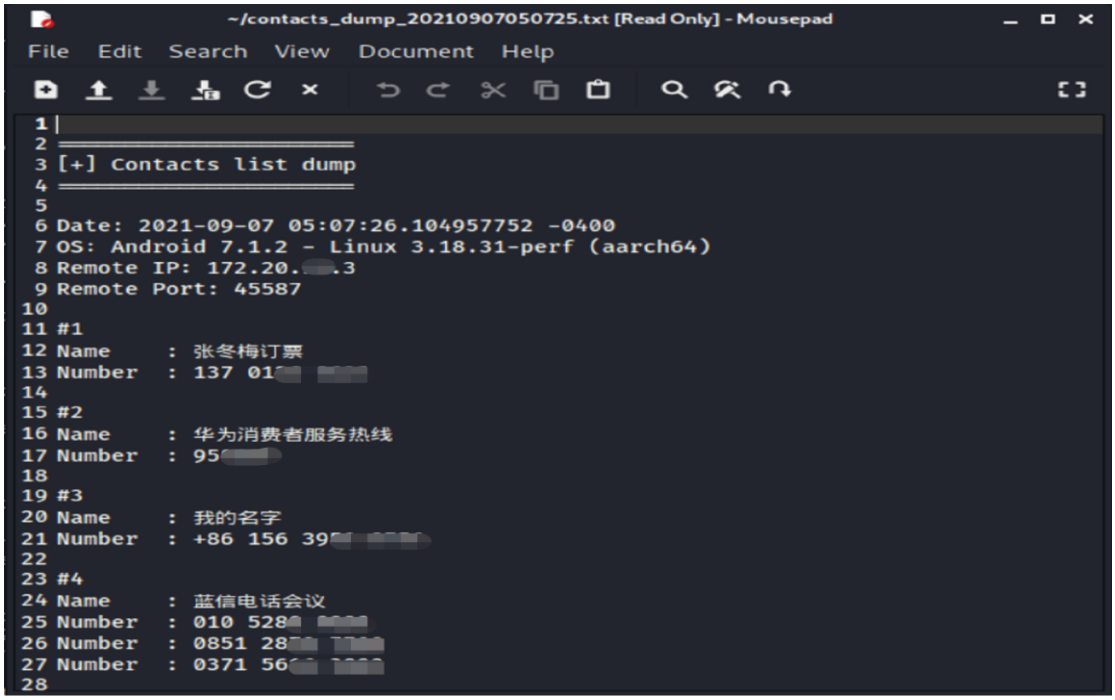



**图 4-6 明文存储用户通讯记录**

### （5） 安全防护建议

针对车端个人敏感信息安全防护，应采取“规范管理+技术防护”相结合的方式来保证个人信息的保密性、完整性及可用性。

管理层面，企业应遵守《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》及《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见》、《汽车数据安全管理若干规定（试行）》等相关政策要求，同时参考国家标准，建立数据分类分级规范及数据管理台账。在数据管理台账或企业其它相关管理办法中需涵盖针对个人信息的管理内容。

技术层面，车辆在采集、传输、处理、存储、销毁个人

信息时需得到用户授权。车辆对必须采集、存储的个人信息应采取去标识化处理等措施，关键敏感信息需进行加密处理。针对用户个人敏感数据资产严格进行访问权限控制。

## 2. GPS 攻击

### （1） 测试内容

使用射频开发板，例如: LimeSDR、BladeRF 和 HackerRF 等工具，模拟卫星发射的信号，通过覆盖真实卫星信号，实现欺骗。基本原理是将虚假的欺骗信号进行广播，目的是使接收端将其误解为真实信号，诱导被攻击端计算出错误位置、错误时钟偏移，从而诱发危险行为。基本原理如下图 4-7 所示。

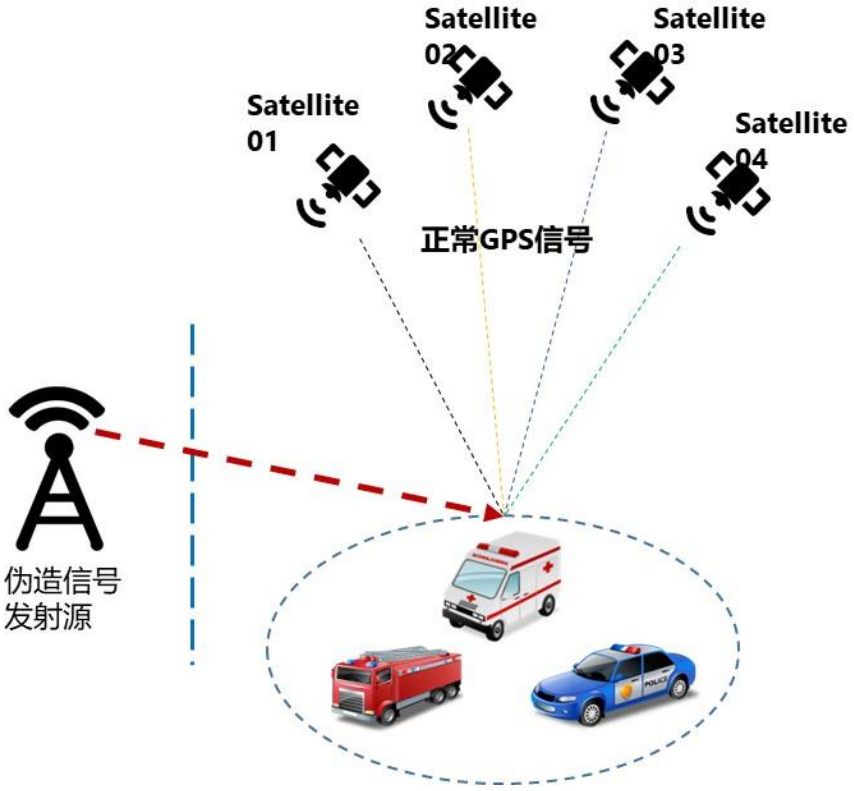


图 4-7GPS 欺骗基本原理

GPS 攻击检测分为两个步骤，首先使用 GPS 干扰工具模拟 GPS 信号，干扰汽车 GPS 定位系统，测试车辆定位是否准确，导航是否可以正常使用。其次，编辑虚假 GPS 信号数据，使用 GPS 模拟工具发射，对被测车辆进行位置欺骗（如下图 4-8 所示），检测汽车定位是否准确，导航是否可以正常使用。

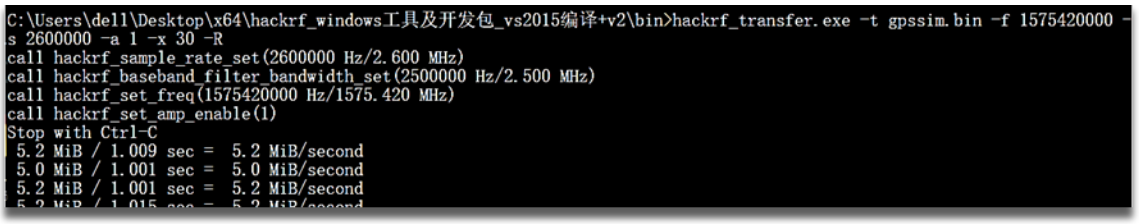



图 4-8 使用模拟工具发射虚假 GPS 信号

### （2） 测试结果分析

在本次渗透测试中，64%的被测车辆在 GPS 攻击测试过程中欺骗成功，将车辆定位到非真实坐标区域。例如：将一辆正在北京行驶的车辆欺骗定位到拉萨河中。

GPS 攻击的原理简单，攻击成本低，使用某些开源工具就可以完成攻击的全部过程。但是，GPS 攻击的危害却极大，在医疗、消防、公安等特种车辆在执行任务或抗震救灾的场景下，一旦遭到攻击，那么所带来的危害则是不可预计的。比如：救护车在运送危重病人过程中由于 GPS 信号错误，导致车辆行驶到错误路线，那么将造成病人的生命安全无法得到保障。

### （3） 安全防护建议

基于信号处理的欺骗检测。寻找在信号欺骗期间发生的失真或干扰，从载波幅度，编码相位和载波相位中检测不合理的跳跃。

基于漂移的欺骗检测。感知车辆位置或时钟的异常变化。如欺骗导致车辆时钟误差变化过快，则车辆可以检测到时钟漂移率大于其合理值。车辆已知速度，加速度和转弯率最大值都可以用来检查是否存在过度漂移。与时钟漂移类似，如果检测到不真实的运动轨迹，车辆将发出报警。

### 3. OTA 平台信息泄露

#### （1） 测试结果分析

在测试过程中发现，部分主机厂 OTA 软件升级云服务在未登录的状态下，通过访问 OTA 平台 URL 子页面可直接下载软件升级包的 apk 文件。存放升级包的目录暴露，且未做模糊化处理。通过目录名可联想判断出该目录是为了方便内部开发人员测试临时创建，并未对访问该目录的 session 信息做判断。同时，该目录未使用过滤器或拦截器等防护措施。

通过该漏洞，攻击者可在互联网环境下非法获取目录中的所有资源。测试实践中发现，目录中包含 IVI 的完整升级包。若攻击者获取升级包，可分析 IVI 的业务逻辑和存在的潜在威胁，为下一步攻击做好准备。若内部测试人员在该目录放置其他重要文件，均可被攻击者轻易获取。

### （2） 安全防护建议

首选建议是删除该目录，如必须保留该路径，建议在 WEB-INF 下存储资源，因为浏览器无法直接访问 WEB-INF 下资源，需通过重定向后才可以访问。另外，也可以在代码中使用 filter 并通过检查 session 对象的属性，来限制直接通过 url 访问子目录的问题。

## 五、智能网联汽车网络安全建议

### (一) 行业应完善政策标准，企业抓紧政策标准落地

今年以来，国家在智能网联汽车网络安全、数据安全领域、个人信息保护等方向相继出台了法律法规，《关于加强智能网联汽车生产企业及产品准入管理的意见》中也对网络安全保障提出了明确要求，引起了相关企业的高度关注。但与此同时，由于相关配套标准的建设工作仍在推进中，部分关键技术和产品要求尚未明确，企业大多尚未对标准法规的落地做好准备工作。

事实上，企业现阶段应该认真学习相关法律法规、准入管理意见关于网络安全保障的要求，对照企业自身网络安全保障能力，及时查找不足，并参考 R155、ISO/SAE 21434 等标准内容，从组织架构建设、管理体系建设、专业人员配置、项目管理优化、测试验证环境建设、体系文件制定等方面研究确定标准法规响应方案，在积极跟进国家政策法规体系建

设动向的同时做好基础工作，尽量缩短开展合规性工作的准备时间，保障产品的顺利研发和上市。

### (二) 企业应提高安全意识，产品需全生命周期防护

无论是标准法规要求，还是从企业产品自身安全技术需求方面考虑，都要对智能网联汽车的全生命周期进行网络安全保护。首先，依据标准和法规的要求，整个行业需达成网络安全的共识，提高供应链上所有相关企业的安全意识。其次，企业应将网络安全防护措施融入到产品中，随着技术的发展，智能网联汽车运行的环境越来越复杂，存在的威胁和风险越来越多，企业为保证自身产品在行业中的影响力，应具备抵御攻击的能力，做好网络安全防护措施。

在产品全生命周期方面，首先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有效解决办法。从安全需求、防护措施、应急响应多角度出发，设计动态安全管理流程，构建标准化安全开发全生命周期管理体系。概念阶段的设计就要将网络安全纳入其中，制定出网络安全目标，指导开发过程；在产品发布前要进行相关的验证测试和渗透测试，以保证发布产品的网络安全性；在产品运行维护阶段，不断检测监测车辆的网络安全性，做到及时响应。安全设计是开发、需求分析阶段的必要环节，不该是在产品下线后“修修补补”的工作。

无论是硬件定义汽车的时代，还是软件定义汽车，甚至

是信息数据定义汽车，终将离不开一个基本立足点，那就是安全定义汽车。因此，为了实现更有效地的提高车辆产品安全防护效果，同时合理控制成本，对于智能网联汽车产品的网络安全应做到“早打算、早布局”。