中国汽研 CAERI

HUAWEI

i-IVISTA Intelligent Vehicle Integrated Systems Test Area

智能网联汽车信息安全测试评价白皮书

2021年10月

目　录

编制单位：

主编单位：中国汽车工程研究院股份有限公司

华为技术有限公司

参编单位：北京航空航天大学

北京邮电大学

中国第一汽车集团有限公司

北京汽车研究总院有限公司

北京车和家信息技术有限公司

中汽创智科技有限公司

沙龙智行科技有限公司

奇安信科技集团股份有限公司

杭州安恒信息技术股份有限公司

1. 编制概要

1.1 编制背景

智能化、网联化技术的发展使得汽车信息安全问题愈发突出。相比传统的信息安全事件，智能网联汽车信息安全事件不仅会导致个人隐私数据受到侵犯、企业经济利益受损，还可能对驾乘人员的生命造成严重威胁，甚至危害国家公共安全。

智能网联汽车的信息安全问题已引起各国政府和相关行业的高度重视。从 2015 年开始，国内外便开展了智能网联汽车信息安全的研究工作，研究成果包括法规、标准、报告、测试等。随着智能网联汽车信息安全法规、标准的不断完善，智能网联汽车需要关注信息安全这一理念也逐渐被市场接受并认同。但目前行业内仍缺乏针对整车、零部件的信息安全测试评价方案，使得整车、零部件在信息安全上无法获得公证、定量的评价，影响智能网联汽车行业的健康发展。

1.2 编制目标

本白皮书从政府、企业、消费者角度分别讨论其对于智能网联汽车信息安全测试评价工作的潜在需求，研究分析智能网联汽车信息安全测试评价相关法规、标准和测试评价方案进展，探索提出智能网联汽车信息安全测试评价方法，为智能网联汽车信息安全测试评价工作提供指导和依据，助力我国智能网联汽车行业持续快速发展。

1.3 编制方法

1）研究分析政府、企业、消费者对于智能网联汽车信息安全测试评价工作的潜在需求。

2）调研智能网联汽车信息安全测试评价相关的国内外法规、标准、测试评价方案进展。

3）邀请行业专家咨询评审。

1.4 特别声明

本白皮书的主要观点和内容仅代表编制组目前对智能网联汽车信息安全测试评价工作的研究和思考，欢迎各方专家、学者提出宝贵意见，共同推进白皮书的完善。

2. 智能网联汽车信息安全测试评价需求

据 Upstream Security 发布的 2021 年《汽车网络安全报告》[1]统计，在过去 5 年间，黑客对智能网联汽车攻击的次数增长了 20 倍，而从 2010 年到 2020 年间，远程攻击的数量在所有攻击中占比为 79.6%。远程攻击无需实际接触车辆便可进行，且能在世界任何地方发起，已经成为黑客攻击的主流方式。此外，据相关安全公司研究统计，平均每千行代码可能会引入 4~6 个安全问题，而智能网联汽车动辄上亿行代码，其中的问题数量可想而知。智能网联汽车面临着严重的信息安全风险。

因此，智能网联汽车在智能化、网联化与安全性间的矛盾已成为其发展的制约因素之一，客观上需要提出一套适用于智能网联汽车的信息安全测试评价方法。

- **政府需求**

作为国民经济重要支柱产业和发展制高点，我国正大力发展智能网联汽车产业。但由于智能网联汽车可被远程访问，导致某些攻击者无需实际接触便车辆便可发动攻击，对智能网联汽车信息安全造成了巨大威胁。因此，政府需要有一套能够衡量智能网联汽车信息安全水平的测试评价方法，以支持其掌握相关产品的客观安全水平情况，进而保证国家公共安全，推动智能网联汽车行业健康发展。

- **车厂需求**

智能网联汽车由诸多零部件组装而成，每个零部件的信息安全水平决定了整车的信息安全水平。在整车厂（OEM）采购相关零部件时，可由 OEM 自行对候选名单中的零部件进行逐一测试，并根据测试结果采购相应产品，但这种方法不仅费时费力，还很大程度上取决于测试人员的技术水平。如果零部件携带经权威机构评定的可反映其信息安全水平的测试评价结果，可以给 OEM 带来极大的便利。因此，OEM 需要有一套全面、有公信力、可量化的信息安全测试评价方法来保证测试评价结果可信、可靠、可用。

- **零部件厂商需求**

受成本等因素影响，不同零部件厂商生产的同种产品在信息安全水平上也可能存在很大差异。对于零部件厂商而言，如果可以明确 OEM 对于产品的信息安全水平要求以及相应信息安全水平要求对应的测试评价结果，则可以帮助其更好地明确信息安全目标，避免出现信息安全防护水平不满足要求的情况。

- **消费者需求**

相比传统汽车，智能网联汽车的信息安全问题尤为突出，某些 OEM 已经开始将信息安全防护水平作为卖点之一进行宣传。如同消费者会在潜意识里认定某个品牌的汽车

[1] Upstream Security: Global Automotive Cybersecurity Report

拥有更好的物理安全特性一样，今后智能网联汽车的信息安全防护水平也会成为其区别于其他品牌的一张名片。考虑到将来可能会有越来越多的消费者开始关注汽车的信息安全防护水平，对于这类消费者而言，具有公信力、可量化的智能网联汽车测试评价方法可以为其提供直观的测试评价结果。

3. 智能网联汽车信息安全测试评价现状

3.1 法规进展

3.1.1 国际法规进展

国际上积极开展智能网联汽车信息安全相关的管理法规和技术法规制定工作，目前已完成的法规包括 Regulation (EU) 2019/2144、Regulation (EU) 2018/858、UN-R 155、UN-R 156 等。

- **Regulation (EU) 2019/2144**

欧盟产品准入安全性法规 Regulation (EU) 2019/2144 适用于机动车辆及其挂车，和用于此类车辆的系统、零部件和独立技术单元，定义关于其一般安全及对乘员和弱势道路使用者保护的型式认证要求。Regulation (EU) 2019/2144 于 2019 年 12 月 16 日发布，并已于 2020 年 1 月 5 日实施，其中信息安全部分的要求引用了 UN-R 155 法规，该部分将于 2022 年 7 月起实施。

- **Regulation (EU) 2018/858**

欧盟产品准入基础性法规 Regulation (EU) 2018/858 适用于机动车辆及其挂车，和用于此类车辆的系统、零部件和独立技术单元的型式认证及市场监管，包含 87 项具体技术法规要求，其中 80%采纳了联合国法规。Regulation (EU) 2018/858 于 2018 年 6 月 4 日发布，并已于 2020 年 9 月 1 日实施，其中软件升级部分的要求引用了 UN-R 156 法规，该部分将于 2022 年 7 月实施。

- **UN Regulation No. 155**

联合国 R155 法规“Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”是重要的车辆信息安全技术法规，由联合国欧洲经济委员会（UNECE）世界车辆法规协调论坛（WP29）负责制定。法规规定了 OEM 需要满足的信息安全要求，满足这些要求后，OEM 才能通过网络安全管理体系（CSMS）认证，其生产的车型才能获得型式认证（VTA）。

R155 法规主要包含如下要求：

（a）CSMS 认证： 主要审查 OEM 是否在车辆完整生命周期内制定了信息安全相关的流程，以确保车辆全生命周期中都有对应的流程措施用以控制相关风险，属于管理体系维度。

（b）VTA：主要针对 OEM 网络安全开发中的具体工作执行情况进行审查，确保车辆的网络安全防护技术能覆盖各生命周期的安全需求，且保证实施的网络安全防护能有效应对网络安全风险，属于产品体系维度。

UN Regulation No. 156

联合国 R156 法规“Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system”主要从管理体系和技术需求（产品体系）上对车辆软件更新提出了要求，同样由 UNECE WP29 负责制定。在管理体系上，制造商的软件更新管理系统（SUMS）由软件更新一般流程要求、软件更新信息记录及存储流程要求、软件更新信息安全要求及 OTA 相关流程要求四部分构成；在技术需求（产品体系）上，R156 法规涵盖了软件更新通用需求和 OTA 附加需求，并要求在合规测试中开展对应的测试验证工作。

3.1.2 国内法规进展

近期，我国不断出台相应法规文件，管控智能网联汽车的潜在信息安全风险，促进智能网联汽车产业规范健康发展。

- **市监质[2020]123 号**

市场监管总局于 2020 年 11 月 25 日印发市监质[2020]123 号《市场监管总局办公厅关于进一步加强汽车远程升级（OTA）技术召回监管的通知》，要求生产者获知其生产、销售或进口的车辆或 OTA 实施过程中的车辆，在中国市场上发生被入侵、远程控制等安全事故时，应立即组织调查分析，并向市场监管总局质量发展局报告调查分析结果。

市场监管总局在 2021 年 6 月 4 日印发的《市场监管总局质量发展局关于汽车远程升级（OTA）技术召回备案的补充通知》中，进一步要求生产者在 OTA 备案时，需提交《汽车远程升级（OTA）安全技术评估信息表》。信息表中包含升级流程、升级安全测试和验证报告、安全防护措施等信息。

- **工信部通装[2021]103 号**

工信部装备司于 2021 年 7 月 30 日印发的工信部通装[2021]103 号《关于加强智能网联汽车生产企业及产品准入管理的意见》（以下简称“意见”）从管理体系和产品体系两方面提出了要求：

（a）管理体系：要求企业应当建立健全汽车数据安全管理制度和汽车网络安全管理制度；

（b）产品体系：应加强自动驾驶功能产品的安全管理，自动驾驶功能产品需要满足网络安全过程保障要求和网络安全测试要求。

同时，《意见》中还提到“鼓励第三方服务机构和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”。“测试验证和检验检测能力建设”需要设计一套公认的智能网联汽车信息安全测试评价方法，并在有关部门的监管下开展实施，有效规避因信息安全问题带来的风险。

- **工信部网安[2021]134 号**

工信部网安局于 2021 年 9 月 15 日发布的工信部网安[2021]134 号《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》中指出车联网相关企业要采取管理和技术措施保障车联网安全稳定运行，并要求国内相应标委会加快车联网安全标准建设，包括检测评估和认证标准。

3.1.3 法规进展小结

信息安全对于智能网联汽车至关重要，各国都加快发布信息安全相关法规。

根据当前的法规内容，信息安全主要从管理体系和产品体系两方面进行审查。因此，建设相关测试验证和检验检测能力是支持法规要求落地的重要措施。建设相关测试验证和检验检测能力需要有一套客观、有效的信息安全测试评价方法。

3.2 标准进展

智能网联汽车信息安全相关法规主要包括管理体系和产品体系两方面的要求，本节对相应的标准进展进行分析。

3.2.1 管理体系相关标准

- **VDA“Automotive Cybersecurity Management System Audit”**

UNECE 已经制定了针对 OEM 的 CSMS 要求，需要有进一步的标准明确根据什么准则和打分方法对 OEM 和合作方进行审计，以验证 OEM 和供应商的 CSMS 能力。为此，德国汽车工业协会（VDA）于 2020 年 12 月发布了红皮书“Automotive Cybersecurity Management System Audit”。该标准定义了汽车 CSMS 审核的评价准则和评价方案，以确保 OEM 和合作方的满足 R155 法规的要求。

标准详细介绍了可用于审核 OEM 和合作方（供应商、服务提供商等）的 CSMS 提问表。根据标准描述的评价方案，可以给出 CSMS 的审计结果。此外，标准还为提问表中各问题提供了示例，以便于审核员通过这些示例的协助完成 CSMS 评估。

- **ISO/SAE 21434:2021(E)**

ISO/SAE 21434 Road vehicles — Cybersecurity engineering 是国际上制定的重要汽车行业网络安全标准，于 2021 年 8 月正式发布。标准覆盖车辆整个生命周期的工程管理，参考 V 字模型开发流程，从安全风险管理、产品开发、生产、运营/维护、跨产品或者组织层面的保障流程等方面来保障车辆网络安全工程工作的开展，使得依据该标准设计、生产、测试的产品具备网络安全防护能力，免受车辆电子电气组件及其功能相关威胁场景的危害。

- **ISO PAS 5112**

ISO/SAE 21434 仅提出了车辆电子电气系统工程中的信息安全工程要求，使电子电气系统工程能够跟上不断变化的技术和攻击方法，但标准并没有提供详细的审计条款条款，因此 ISO 启动了 ISO PAS 5112 Road vehicles—Guidelines for auditing cybersecurity engineering，作为 ISO/SAE 21434 的配套审计指南。ISO PAS 5112 参考了 ISO 27001，并在其基础上根据车辆网络安全工程的要求做了扩展，如在建立审核方案目标时考虑了对车辆信息安全需求的识别，在实施审计方案时要求相应成员具备汽车信息安全相关知识，在报告的审核方面增加了对 ISO/SAE 21434 中的工作产品进行审核等。

- **GB/T 道路车辆 信息安全工程**

《道路车辆 信息安全工程》是中国全国汽车标准化技术委员会（以下简称“汽标委”）基于 ISO/SAE 21434 开展的转化国家标准，计划于 2023 年发布。此外，汽标委计划在 ISO PAS 5112 正式发布后开展国家标准转化工作，具体转化形式待定。

3.2.2 产品体系相关标准

- **整车信息安全相关标准**

《汽车整车信息安全技术要求与试验方法》作为汽车信息安全领域国家强制标准，将从管理要求、外部连接、车辆通信、软件升级、外部服务器、无意识行为、潜在漏洞、数据代码等方面定义车辆应当满足的信息安全要求，同时标准将设计对应的试验方法以帮助相关企业检验每条要求的满足程度。

- **零部件信息安全相关标准**

针对智能网联汽车的关键零部件，如远程信息服务终端（T-BOX）和网关，汽标委也分别制定了推荐性国家标准《车载信息交互系统信息安全技术要求及试验方法》和《汽车网关信息安全技术要求及试验方法》。其他零部件的信息安全标准也在研究/制定当中，如车控操作系统标准、智能驾驶计算平台标准等。

3.2.3 标准进展小结

目前国内管理体系和产品体系的标准均已开始制定，可以为智能网联汽车信息安全的测试评价工作提供一定的指导。

然而，国内仍缺乏一套智能网联汽车信息安全测试评价方案，以标准为依据，开展对智能网联汽车的信息安全测试评价工作。

3.3 行业信息安全测试评价方案

- **5Stars 联盟信息安全测试评价方案**

5Stars 联盟是一个由多家汽车行业研究机构组成的组织，合作为智能网联汽车信息安全问题制定全新的框架，以应对智能网联汽车与日俱增的信息安全威胁。5StarS 于 2019 年发布白皮书“A roadmap to resilience”，提出了一套包含管理体系和产品体系的汽车网络安全测试评价框架，以确保智能网联汽车的组件和系统在其整个生命周期中均按照相关网络安全标准进行设计，包括产品开发、生产、运营、维护和退役阶段，并通过漏洞评估证明车辆具有足够的安全性。

此外，考虑到测试会随着时间以及不同车辆而变化，5StarS 委员会还维护了一份指导文件，用于指导第三方服务机构为车辆测试评价制定适当的计划，同时核实服务机构及测试评价人员的能力，以确保不同服务机构间测试评价的一致性。

- **信息技术安全评估通用准则**

信息技术安全评估通用准则（CC）是信息安全测试评价标准以及信息安全技术发展的重要里程碑。CC 标准定义了评价信息技术产品和系统安全性的基本准则，提出了目前国际上公认的表述信息技术安全性的结构，即把安全要求分为：1）规范产品和系统安全行为的功能要求；2）解决如何正确有效地实施这些功能的保证要求。产品的安全性通过 CC 标准定义的七个评估保证级来衡量，级别越高则安全保证级别越高，同时评估项和严格程度也会递增。CC 测试评价的两个重要环节是确定安全目标（ST）和评估，安全目标可基于保护轮廓（PP）撰写或直接撰写，其中 PP 为一类产品或系统的安全要求，ST 为某个特定产品的安全要求。

5StarS 的测试评价方案仍处于初步阶段，缺乏一套具体可操作的方案执行细则。CC 是针对信息技术领域设计的标准，在车用操作系统方面有一些应用，缺乏在汽车行业对整车、零部件进行测试评价的大规模应用案例。

4. 智能网联汽车信息安全测试评价方案

本白皮书基于对法规、标准和当前测试评价方案的研究，提出一种智能网联汽车信息安全测试评价方案。

4.1 测试评价对象

虽然目前的整车与零部件相关标准已经包含相应试验方法，但这些标准只能作为信息安全测试评价方案的输入，仍然需要有一套智能网联汽车信息安全测试评价方案把上述标准组合起来。

一方面，智能网联汽车整车信息安全水平是 OEM 首要关注的；另一方面，智能网联汽车整车信息安全要求又需要分解到各个零部件，这些零部件的信息安全水平反过来又决定了整车信息安全水平。因此，智能网联汽车信息安全测试评价方案不仅需要能对整车的信息安全水平做出真实的评价，还应该能对零部件进行信息安全测试评价。

4.2 测试评价范围

目前，从法规要求来看，智能网联汽车信息安全测试评价应包含管理体系和产品体系两部分，因此本白皮书提出的智能网联汽车信息安全测试评价方案在测试评价范围上包含了管理体系和产品体系两方面，如图 1 所示。

对管理体系和产品体系的测试评价涵盖概念、设计、开发、测试、生产、运行、维护、报废各个阶段，应对产品全生命周期的各种风险。

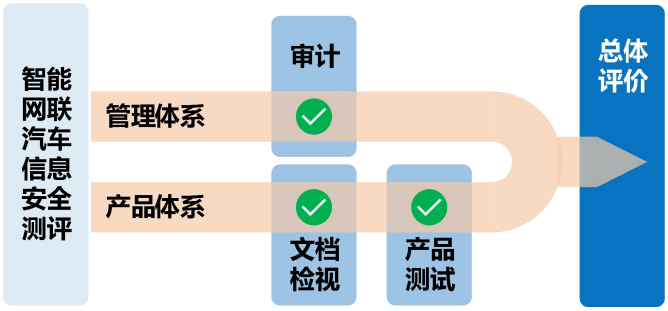

图1 智能网联汽车信息安全测试评价范围

管理体系的测试评价范围主要涉及组织策略和流程相关的审计（如表 1 所示），组织策略方面包括企业的网络安全制度、网络安全文化、人员角色等，流程方面包括企业网络安全流程文件、模板、工具等。

表1 智能网联汽车管理体系信息安全测试评价范围示例

维度	内容	示例	方式
组织策略	网络安全制度	网络安全方针、策略、管理发文等	审计
	网络安全文化	能力管理、意识管理、持续改进等	
	人员角色	负责人及相应权限、支持网络安全的资源等	
流程	网络安全流程	网络安全概念、设计、开发、验证、生产、运维等流程文件	
	模板	TARA分析模板、设计模板、事件响应计划模板等	
	工具	开发工具、验证工具等	

产品体系的测试评价范围主要涉及产品技术要求相关的文档检视和产品测试（如表2所示），技术要求文档包括TARA分析文档、产品设计文档、测试规范等，测试包括基于技术要求开展的符合性测试、漏洞测试、Fuzzing测试、渗透测试等。

表2 智能网联汽车产品体系信息安全测试评价范围示例

维度	内容	示例	审查方式
技术要求	TARA分析文档	资产的确定、影响严重程度的评级、影响类别的考虑、威胁场景的识别、攻击分析的方法、攻击可行性的确定、风险矩阵的建立等	文档检视
	产品设计文档	架构设计文档、系统设计文档、功能设计文档等	
	测试规范	测试工具、测试环境、测试用例等	
产品测试	符合性测试、漏洞测试、Fuzzing测试、渗透测试等		测试

上述测试范围可根据测试对象的不同要求进行裁剪，如对于信息安全要求较高的部件（如智能驾驶计算平台等），管理体系和产品体系的测试评价更为严格，这将体现在需要检视的文档更多、范围更大，执行的测试更为全面、深入等方面。

4.3 测试评价依据

智能网联汽车信息安全测试评价方案应基于标准构建，表3列出了建议参考的部分标准。

在管理体系方面，可依据《道路车辆 信息安全工程》对企业组织、流程进行审计。

在产品体系方面，可依据整车和零部件标准对产品进行测试评价，包括《汽车整车信息安全技术要求及试验方法》、《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》、《电动汽车远程服务服务与管理系统信息安全技术要求及试验方法》、《汽车软件升级通用技术要求》等标准。

表3 智能网联汽车信息安全测试评价依据示例

项目	标准	说明
管理体系	GB/T 道路车辆-信息安全工程	ISO 21434转化国标，定义网络安全管理体系要求，包括组织和流程要求

产品体系	GB 汽车整车信息安全技术要求及试验方法	整车角度的信息安全要求和相应测试方法
	GB/T 车载信息交互系统信息安全技术要求及试验方法	T-Box、IVI的信息安全要求和相应测试方法
	GB/T 汽车网关信息安全技术要求及试验方法	车载网关的信息安全要求和相应测试方法
	GB/T 电动汽车远程服务服务与管理系统信息安全技术要求及试验方法	GB/T 32960配套信息安全标准
	GB 汽车软件升级通用技术要求	OTA标准，内含信息安全要求

4.4 测试评价方法

4.4.1 管理体系测试评价方法

本测评方案基于标准《道路车辆 信息安全工程》中相关要求，从企业治理、项目管理、概念阶段、产品开发阶段、验证阶段、生产阶段、运维阶段、供应商管理等模块开展审计工作（如图 2）。

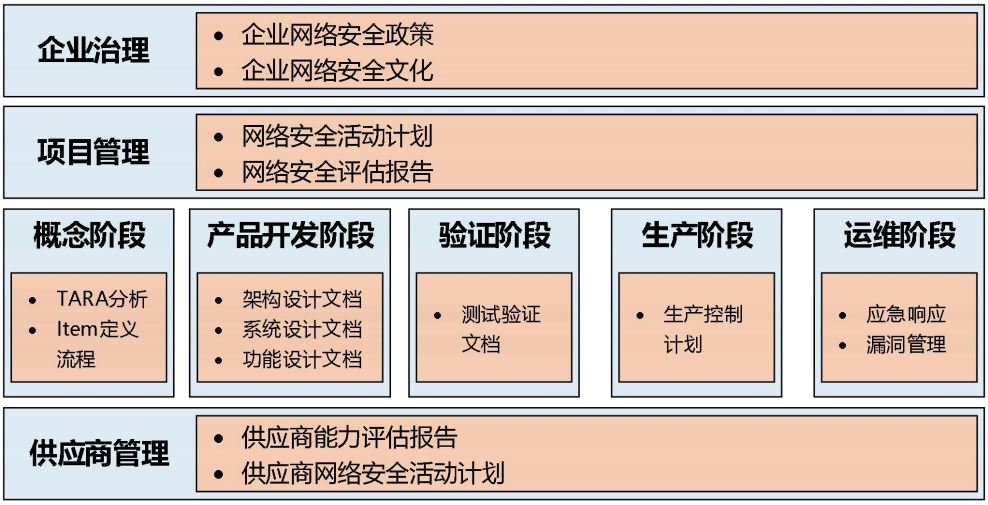

图2 基于《道路车辆 信息安全工程》的管理体系测试评价审计

针对每个模块的检查项进行审计，并完成相应打分，得出模块的得分。然后基于每个模块的得分汇总为管理体系的总体得分，如果总体得分高于事先设定的门限，则表明通过管理体系测试。

4.4.2 产品体系测试评价方法

本测评方案参考 ISO/SAE 21434 标准等相关风险评估方法，首先制定智能网联汽车漏洞风险评估方法，为汽车漏洞评级提供技术支撑。其次在此基础上对汽车存在的攻击面进行分类，对单一攻击面存在的若干漏洞评估结果进行融合，从而得到单一攻击面的风险评估结果。然后对汽车各个攻击面的风险评估结果进行整合，得到汽车部件的风险评估结果。最后汇总汽车各部件的风险评估结果，得到智能网联汽车整车风险评估结果。

汽车部件级风险评估架构图如图 3 所示：

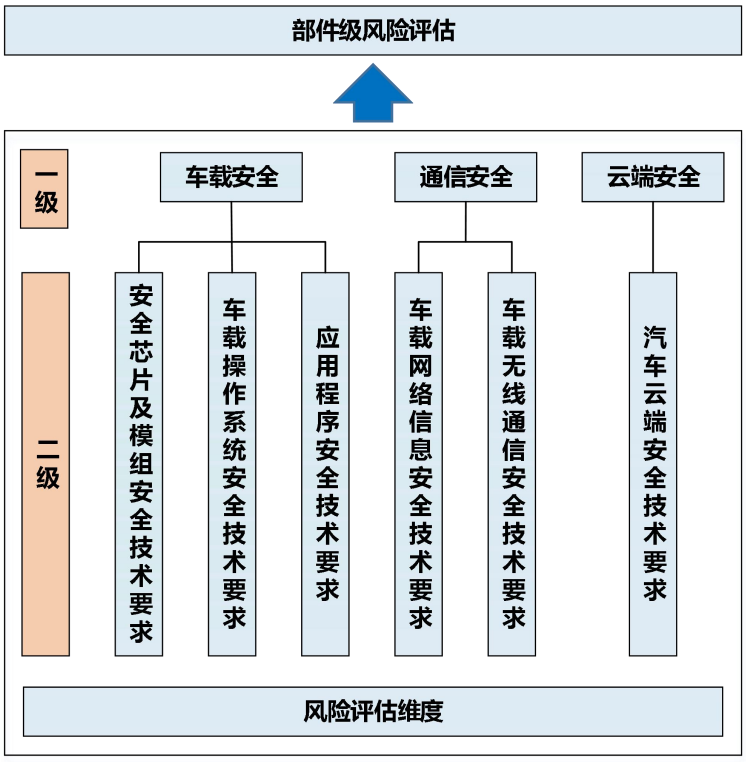

图3 智能网联汽车部件级风险评估方法架构图

从图 3 中可以看到，部件级风险评估方法包括两个部分，第一部分是对汽车漏洞进行风险评估，第二部分是基于汽车漏洞风险评估结果，完成部件级风险评估。

4.4.2.1 风险评估方法流程

本测评方案中的风险评估流程与 ISO/SAE 21434 标准中的风险评估流程保持一致，流程见图 4。在此基础上，本测评方案对攻击可行性评级和攻击影响评级进行了明确说明和解释。

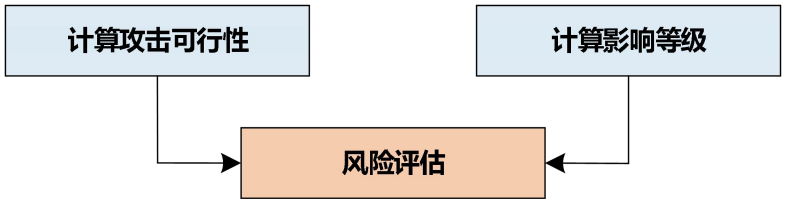

图4 智能网联汽车漏洞风险评估流程

- **攻击可行性**

攻击可行性代表了漏洞可被攻击者利用的程度，越容易被利用的漏洞则对汽车风险越高。下表对攻击可行性的四个级别进行了说明，四个等级分别代表了四种不同程度攻击的威胁。

表4 攻击可行性等级和相应标准

等级	说明
高	容易完成攻击
中	使用适度的方法可实现攻击
低	通过高难度的方法可实现攻击
极低	很难或几乎永远不可能完成攻击

- **攻击影响评级**

由于攻击者使用漏洞会造成汽车资产在安全、财产、运行和隐私方面的损害，因此ISO/SAE 21434 对攻击影响评级包含了安全、财产、运行和隐私四个方面。本规范结合当前相关法规和标准，同时为了扩大风险评估覆盖面，攻击影响增加 CIA 维度。

安全损害影响等级对产品的功能失效所引起人员伤害程度（包括个人车主及行人）进行了定义，详细定义如下：

表5 安全影响等级

影响等级	安全影响等级指标
致命	个人车主及行人角度： S3：危及生命的伤害（生存不确定），致命
严重	个人车主及行人角度： S2：严重危及生命的伤害（可能存活）
一般	个人车主及行人角度： S1：轻中度伤害
无	个人车主及行人角度： S0：无伤害

财产损失影响等级定义了利益相关者的财产损失程度，详细定义如下：

表6 财产损失影响等级

影响等级	财产损失影响等级指标
致命	（1）OEM/供应商角度：漏洞符合产品缺陷定义，将导致 OEM 车型召回，遭到行政处罚，引起公司声誉受损，市场份额受损。公司无法承受引起的相关经济损失（如破产，公司倒闭等） （2）运营商：漏洞会引起运营商经营行为无法进行（受召回影响），引起运营商声誉受损，市场份额受损。运营商无法承受引起的相关经济损失（如破产，公司倒闭等） （3）个人车主角度：漏洞会引起个人车主无法承受的整车价值全部损失，如导致车辆报废、整车被盗、个人电子支付被入侵等
严重	（1）OEM/供应商角度：漏洞符合产品缺陷定义，将导致 OEM 车型召回，引起公司声誉受损。公司可承受引起的相关经济损失 （2）运营商：漏洞会引起运营商业务受到影响（受召回影响），声誉受损。运营商可承受引起的相关经济损失 （3）个人车主角度：漏洞会引起个人车主可承受的财产损失，财产损失范围为车辆价值的 10%-99%。如车辆部件损坏、付费功能激活等
一般	(1) OEM/供应商角度：漏洞被攻击者利用可导致公司产品非预期功能激活，对公司财产造成损失。如付费功能非法使用等。

	(2) 运营商：漏洞会引起运营商车辆产品非预期功能激活。如付费功能非法使用等 (3) 个人车主角度：漏洞会引起个人车主车辆价值 10%以下的财产损失。如车辆付费功能激活、个人电子支付被入侵等
无	财产损失不会产生任何影响，忽略不计

运行异常影响是指汽车功能运行异常对个人车主驾驶车辆产生影响的程度，详细定义如下所示：

表7 运行异常影响等级

影响等级	运行影响等级指标
致命	个人车主角度： 资产被攻击后，导致车辆无法工作。功能出现重大中断，无法被人为控制消除。或者不符合安全或法规要求。涉及与车辆行驶相关的制动系统、动力系统和转向系统功能失效
严重	个人车主角度： 资产被攻击后，导致车辆部分功能丧失。车辆进入跛行模式，仍然可以运行，无法被人为控制消除。如变速箱档位切换异常，新能源电池管理异常、发动机转速异常等
一般	个人车主角度： 资产被攻击后，造成部分功能降级或性能下降。驾驶员可以人为消除。如车辆外观有一定异常，或者驾驶舱出现噪音，引起驾驶员困扰。车载娱乐系统、车身舒适系统、车辆辅助功能（与行驶控制无关）等功能降级
无	个人车主角度： 资产被攻击后，不会导致车辆功能降级或性能下降

隐私泄露影响是车辆受到攻击后个人隐私指泄露影响程度，详细定义如下所示：

表8 隐私泄露影响等级

影响等级	隐私泄露影响等级标准
致命	个人车主角度： >利用漏洞造成的隐私泄露会对用户造成严重或不可逆转的影响 >隐私信息包括对机构的承诺、无法偿还的债务、个人健康生理信息、宗教或哲学信仰、婚史、种族或民族血统、个人生物识别信息、性取向、未公开的违法犯罪记录、残障自然人的特殊需要、刑事调查报告或者由于隐私泄露会形成自然人破产、丧失工作能力以及形成的心理和物理创伤的信息
严重	个人车主角度： >利用漏洞造成的隐私泄露会对用户造成重大影响 >隐私信息包括银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录、虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息、个人身份信息、社保信息、纳税信息、行踪轨迹、住宿信息、精准定位信息、处罚信息、通信记录和内容、通讯录、好友列表、群组列表等，或者由于隐私泄露引起银行黑名单、资产损失、失业、个人声誉受损的信息
一般	个人车主角度： >利用漏洞造成的隐私泄露会对用户造成较大的麻烦 >隐私信息包括个人电话号码 、网络身份识别信息、设备信息、个人偏好、教育状况、兴趣爱好、个人电子邮件地址、姓名、年龄、 自然人可识别的照片或视频等信息，或者导致骚扰电话、骚扰信息、诈骗的信息

无	个人车主角度： 隐私泄露不会带来任何影响或可以忽略不计的后果，例如水电费账单等

CIA 影响性指标组反映漏洞成功利用后所带来的机密性影响、完整性影响和可用性影响。

通过计算安全损害、财产损失、运行异常、隐私泄露和 CIA 五个维度数值，计算得到攻击影响综合评级。

- **风险评估评级**

对攻击可行性和攻击影响结果进行综合性风险评估，风险评估结果分为致命、严重、一般、提示和无五个级别。

4.4.2.2 汽车风险评估方法

基于汽车漏洞风险评估方法，整合部件攻击面，完成部件级风险评估。

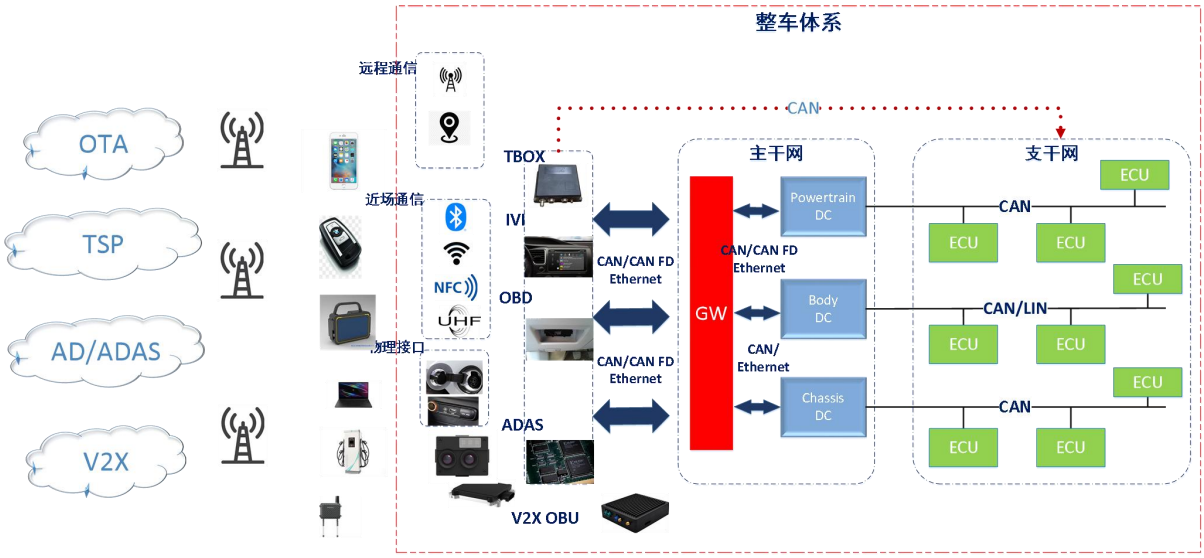

图5 部件攻击面

根据部件所处的位置与整车安全关联关系的不同，部件级风险评估分为关键节点软硬件、车内网络、车外通信以及车联网业务安全四个攻击面。软硬件关注控制器自身功能，车内网络关注 CAN、车载以太网网络通信相关内容，车外通信关注蜂窝网络、蓝牙等内容，车联网关注云端后台内容。

通过汽车漏洞风险评估方法可得到漏洞风险评估结果，基于漏洞与攻击面的对应关系可以得到各攻击面与漏洞风险评估结果的对应表，从而计算各攻击面的风险评估结果。获得部件风险评估结果后，整车风险评估结果可依据各部件在整车的重要程度通过加权计算得出。

4.5 方案小结

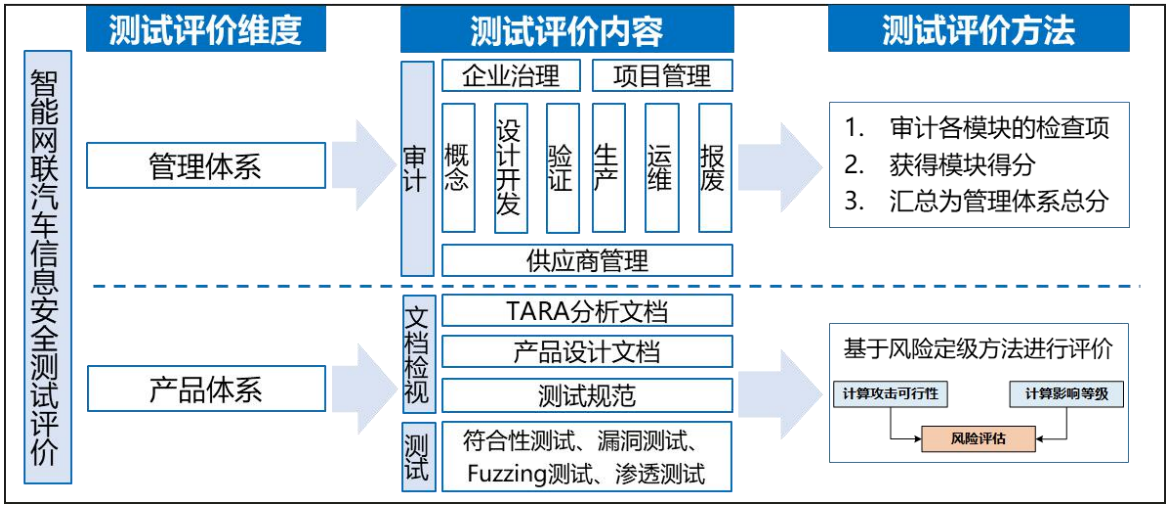

图6 智能网联汽车信息安全测试评价方案小结

本白皮书提出的智能网联汽车信息安全测试评价方案参考了当前业界法规、标准的最新进展，其测试评价范围覆盖管理体系和产品体系两方面，并将管理体系评价结果和产品体系评价结果汇总作为智能网联汽车的完整评价。测试评价方案还存在以下特点：

- 全面：测试评价范围覆盖管理体系和产品体系，适用于 OEM 和零部件供应商对所生产的产品进行信息安全水平的全面评估。
- 可信赖：测试评价方法基于已发布或正在制定的相关标准，保证了测试评价方法的公信力。
- 可操作：测试评价方法按照标准流程开展，可保证测试评价工作可被复制。
- 可比较：测试评价结果支持横向比较，在反映产品真实水平的同时，可以帮助企业了解改进方向，最终牵引行业不断向前发展。

5. 结束语

保障智能网联汽车信息安全需要全社会的共同协作，构建健康的生态环境、适当的防护机制和可信的审核能力。完善的智能网联汽车信息安全测试评价方案能够准确评价智能网联汽车的信息安全水平，保障国家安全，促进智能网联汽车行业健康发展。

本白皮书从政府、企业和消费者角度出发，探讨不同群体对于智能网联汽车信息安全测试评价工作的潜在需求，结合国内外标准、法规要求，提出一套涵盖管理体系和产品体系的智能网联汽车信息安全测试评价方案，该方法符合全面性和可操作性原则，具备可信赖、可比较的特点。

希望本白皮书的提出观点能为智能网联车信息安全测试评价工作的开展创造条件，为行业健康有序发展提供指导和依据，对推动我国智能网联汽车信息安全测试评价持续快速发展起到重要意义。

附录：缩略语

缩略语	英文名称	中文名称
AD	Automated Driving	自动驾驶
ADAS	Advanced Driver Assistant System	高级驾驶辅助系统
CC	Common Criteria	通用准则
CSMS	Cyber Security Management System	网络安全管理体系
ISO	International Organization for Standardization	国际标准化组织
OEM	Original Entrusted Manufacture	原始设备制造商/整车厂
OTA	Over-the-Air	在线升级
PP	Protection Profile	保护轮廓
SAE	Society of Automotive Engineers	美国机动车工程师学会
ST	Security Target	安全目标
SUMS	Software Update Management System	软件更新管理体系
T-BOX	Telematics-Box	远程信息服务终端
TARA	Threat Analysis and Risk Assessment	威胁分析与风险评估
TSP	Telematics Service Provider	车辆远程服务提供商
UNECE	United Nations Economic Commission for Europe	欧洲经济委员会
V2X	Vehicle to Everything	车联网
VCAL	Vehicle Cybersecurity Assurance Level	汽车安全评估级别
VDA	Verband der Automobilindustrie	德国汽车工业协会
VTA	Vehicle Type Approval	车辆型式认证

中国汽研 CAERI

HUAWEI

i-IVISTA
Intelligent Vehicle Integrated Systems Test Area

官网： https://www.caeri.com.cn 官网：http://www.huawei.com 官网：http://www.i-vista.org