道路车辆 网络安全验证和确认研究报告

全国汽车标准化技术委员会
智能网联汽车分技术委员会

2025 年 12 月

前　言

《道路车辆 网络安全验证和确认》重点研究了汽车网络安全验证和确认的整体策略、用于验证和确认的方法、供应商和主机厂之间的分配原则、网络安全验证和确认的执行时间、边界及其关系、验证和确认活动的质量评估方法，并归纳总结形成标准化建议及后续标准制定路线图。本项目由上海汽车集团股份有限公司乘用车分公司牵头，协同整车企业、供应商企业、汽车行业检测机构等相关方共同完成研究。

调研发现企业对验证和确认存在评估流程不清晰、责任边界模糊、缺乏详细执行指导等问题，通过最佳实践提炼出六类共性测试方法，包括审查、代码分析、功能测试、漏洞扫描、模糊测试、渗透测试，并配套提供了对应的质量评估方法，明确了网络安全相关性判定和相关项定义的质量评估方法，对企业开展 TARA 的过程提出了详细的质量评估建议。既保证了技术可落地，又能更好指导企业展汽车网络安全开发和验证。本项目研究得出的标准化路线由总到分、层层递进，全面覆盖了验证和确认活动的方法论及其质量评估，解决了安全目标模糊、安全声明空泛化、需求验证难等问题。

衷心感谢编写研究报告的单位和组织：上海汽车集团股份有限公司乘用车分公司、中国汽车技术研究中心有限公司、中汽智能科技（天津）有限公司、比亚迪汽车工业有限公司、广州小鹏汽车科技有限公司、上海机动车检测认证技术研究中心有限公司、广州汽车集团股份有限公司、深圳引望智能技术有限公司、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）、吉利汽车研究院（宁波）有限公司、赛力斯汽车有限公司、重庆长安汽车股份有限公司、小米汽车科技有限公司、中国第一汽车股份有限公司、一汽解放汽车有限公司、特斯拉（上海）有限公司、北京航迹科技有限公司、阿波罗智能技术（北京）有限公司、北京地平线信息技术有限公司、北京信长城科技发展有限公司、长城汽车股份有限公司、中国汽车工程研究院股份有限公司、广电计量检测集团股份有限公司。

主要编写人：朱建明、侯件件、张芳芳、杨佳音、赵雄、郭丰源、李雨冉、朱科屹、马鑫、纪梦雪、方锦祥、孟雪、古晓冈、王宏多、时瑞浩、潘凯、赵攀峰、曹国华、陆萍、罗薇、曾涛、刘宇、安然、冯祺、冯鑫磊、刘昊炎、王艳华、刘健皓、赵燕、朱俊、刘鹏、刘祎、孙占朋、尹红、戚琪、郑奕文。

目　录

1 网络安全验证和确认背景及意义

1.1 背景及发展现状

1.1.1 总体介绍

随着汽车驾驶自动化技术的迅猛发展、市场渗透率的快速提高以及网联化的广泛普及，汽车的功能与控制模块日益增多。汽车已从传统交通工具逐渐演变为可移动的智能终端——智能网联汽车。

传统汽车的软硬件架构无外部网络连接，网络安全问题仅存在于车内网层面。而智能网联汽车由于使用计算机系统和网络连接，导致汽车电子电气系统等存在遭受网络攻击的风险，网络安全问题愈发严峻。各国网络安全研究人员和车辆制造商（OEM）所披露的网络安全事件和风险漏洞也在持续增多。

2018年前后，车辆制造商与网络安全技术企业开始在汽车网络安全领域进行布局，从多个维度提升产品的网络安全与风险管理水平。国内外车辆制造商积极组建专业的网络安全部门或子公司，通过多种途径构建网络安全体系并提升网络安全防护技术。

在车辆制造商、零部件供应商、第三方网络安全科技公司、行业机构以及汽车供应链其他参与机构的共同推动下，国际和国内的相关标准化机构纷纷启动了网络安全标准化工作。

在国际层面，国际标准化组织（ISO）、国际汽车工程师学会（SAE）、联合国欧洲经济委员会（UNECE）等机构相继发布了如ISO/SAE 21434（以下简称“ISO/SAE 21434”）、UN R155《关于就网络安全与网络安全管理体系方面批准车辆的统一规定》（以下简称“R155”）、UN R156《关于就软件升级与软件升级管理体系方面批准车辆的统一规定》（以下简称“R156”）等国际标准、指导性法规或强制性法规。

在国内，已经正式发布了GB 44495—2024《汽车整车信息安全技术要求》、GB 44496—2024《汽车软件升级通用技术要求》两项强制性标准，对车辆制造商构建企业管理体系，以及车型产品全生命周期的功能分析、风险评估、需求定

义、系统设计、软件开发、测试验证等环节进行指导并提出要求。

上述标准法规均明确规定，在研发过程中需开展充分且恰当的测试，以验证网络安全措施的有效性。

1.1.2 国际标准研究内容及进展

1.1.2.1 R155

2020年6月，联合国欧洲经济委员会（UNECE）的世界车辆法规协调论坛（UN WP.29）发布了UN R155《关于就网络安全与网络安全管理体系方面批准车辆的统一规定》以及UN R156《关于就软件升级与软件升级管理体系方面批准车辆的统一规定》。其适用范围涵盖了乘用车和商用车，并且已被欧盟、日本以及韩国等60多个国家和地区列为车辆市场准入的强制性要求之一。

R155法规针对汽车网络安全的强制要求分为两部分：其一，是对车辆制造商网络安全管理体系的要求；其二，是对车辆产品网络安全能力的要求。这两部分分别对应网络安全管理体系认证（CSMS）和车辆网络安全型式认证（VTA），旨在确保机动车辆的安全性。

尽管R155为机动车辆的网络安全搭建了基本框架，然而因其侧重于宏观合规要求，在验证和确认（verification and validation，简称V&V）方面存在空白：

其一，对于在R155规范无强制要求的地区销售的车辆，无需按照R155的要求开展验证和确认工作。

其二，测试标准尚未统一：该规范并未明确规定验证和确认的测试标准，致使不同测试机构采用不同标准，进而可能得出不一致的测试结果，难以保障验证和确认的充分性与可靠性。

1.1.2.2 ISO/SAE 21434

2021年8月，国际标准化组织（ISO）和国际汽车工程师学会（SAE）联合发布了全球首个面向汽车行业网络安全管理的国际标准ISO/SAE 21434。该标准旨在为车辆制造商和供应商提供有关汽车网络安全活动的指导，为汽车行业提供网络安全的最佳实践。

此标准构建了一个框架，借助V型架构来识别、评估和管理汽车网络安全风

险。它涵盖了需求定义、系统设计、软件开发、测试和验证等多个阶段，以此确保车辆的安全性与可靠性。

该标准包含对安全风险的评估与管理、安全功能的规划与设计、安全测试与验证等方面的指导内容，同时着重强调了对汽车网络安全采取整体风险管理的方法。

通过实施ISO/SAE 21434标准，车辆制造商和供应商能够更有效地管理车辆的信息安全，保护消费者和车辆免遭网络攻击，并降低潜在的安全风险。

尽管该标准提供了重要的基础框架与指导方针，但其定位和设计决定了以下特点：

1）框架性定位：ISO/SAE 21434 的核心价值在于界定车辆信息安全管理的目标、原则、活动及责任框架（即“做什么”和“为什么做”）。这种定位使得它不涵盖具体的技术实现细节（即“如何做”）。具体的实施办法和技术解决方案需结合组织实际状况、最佳实践以及更底层的技术标准和规范来制定，以此保障该标准在广泛行业应用中的适应性。

2）技术体系的互补性：该标准旨在构建一个稳定且持久的风险管理框架。所以，它并非直接规定或预见所有新兴技术的具体安全要求。对于新技术的安全考量，需依托该标准所建立的流程，结合动态发展的行业最佳实践、专门的技术标准以及最新的安全研究成果来进行补充和细化。

1.1.2.3 ISO/SAE 8477

为解决上述对汽车网络安全验证和确认未详细说明的问题，ISO自2021年7月起开展了ISO/SAE 8477《道路车辆 网络安全验证和确认》（以下简称“ISO/SAE 8477”）的标准预研工作。目前已形成技术草案，并将其列为非规范性技术文件（TR），用以对ISO/SAE 21434进行补充。其主要研究内容包括：网络安全验证和确认的整体策略、可用于验证和确认的方法列表、供应商与OEM之间关于网络安全验证和确认的分配原则、网络安全验证和确认的执行时间、边界及其相互关系。

ISO/SAE 8477在ISO/SAE 21434网络安全工程的框架下，对道路车辆信息安全的验证与确认做出了详细的技术性定义与要求。该技术性规范中关于信息安全

的验证与确认，既考量了计划阶段，也兼顾了执行阶段所需的相关工作，对道路车辆信息安全的技术验证与确认做出了更为详尽的补充要求与说明。验证和确认均可基于ISO/SAE 21434规定的TARA（威胁分析和风险评估）来开展。TARA中明确了网络威胁风险以及实现网络安全目标的缓解措施，分析过程中也产生了网络安全需求。因此，验证和确认为相关风险可接受性提供了证据。

ISO/SAE 8477主要聚焦于目标设定与方法建议，未对具体方法做出限定。该标准包含了验证和确认活动的策略、可供应用的方法列表或参考依据、验证和确认活动的职责分工以及相应的时间安排与执行要求。

ISO/SAE 8477阐述了验证和确认的主要异同点：验证活动主要聚焦于产品是否符合相关要求，而确认活动则着重于确保网络安全目标得以实现。

验证和确认的相似之处在于，二者均为ISO/SAE 21434层级产品开发过程的一部分。每个层级可能存在的漏洞都可能对网络安全的实现产生影响，因此需要进行测试，以验证开发设计中不存在此类漏洞。同时，确认活动也涵盖测试环节，以保障车辆层面的网络安全目标能够达成。

依据ISO/SAE 8477的定义，网络安全的确认在V模型中对应的需求为网络安全目标。整车级别的网络安全验证，涵盖架构设计定义里与功能相关的集成验证，以及对应网络安全需求的验证。零部件级别的网络安全验证，包含零部件层级架构设计定义中与功能相关的集成验证，以及对应网络安全需求的验证。

ISO/SAE 8477中所规定的网络安全验证与确认过程，涵盖了计划制定、具体执行以及结果管理等环节。在验证过程中，需依据子系统的安全需求，并严格按照既定计划来执行。一旦发现风险和漏洞，应依照ISO/SAE 21434的要求进行分析与管控。同时，网络安全的目标、概念、设计阶段以及集成测试阶段均需开展验证工作。网络安全确认过程则要求证明所有风险均已得到妥善处理，或者不存在不合理风险。

基于上述内容，企业应结合自身实际情况，选择适宜的验证与确认方法。所制定的策略需确保将与漏洞相关的风险降至可接受水平，进而实现对网络安全风险的合理管控。该标准为企业的网络安全验证和确认工作提供了较为详尽的指导，对网络安全体系的构建以及相关技术的实施起到了补充作用。

1.1.2.4 德国VDA指导文件——用于网络安全的ASPICE

2021年2月，VDA（德国汽车协会）AK 13发布了《ASPICE网络安全工程过程参考与评估模型》。该模型可与ISO/SAE 21434等标准结合使用，用于对网络安全相关开发过程进行评价，同时对ASPICE标准和V模型进行了重要补充。它引入了网络安全工程过程组 (SEC)，包含4个要素，分别为：SEC.1：网络安全需求启发，SEC.2：网络安全实施，SEC.3：风险处理验证，SEC.4：风险处理确认，详见图1。

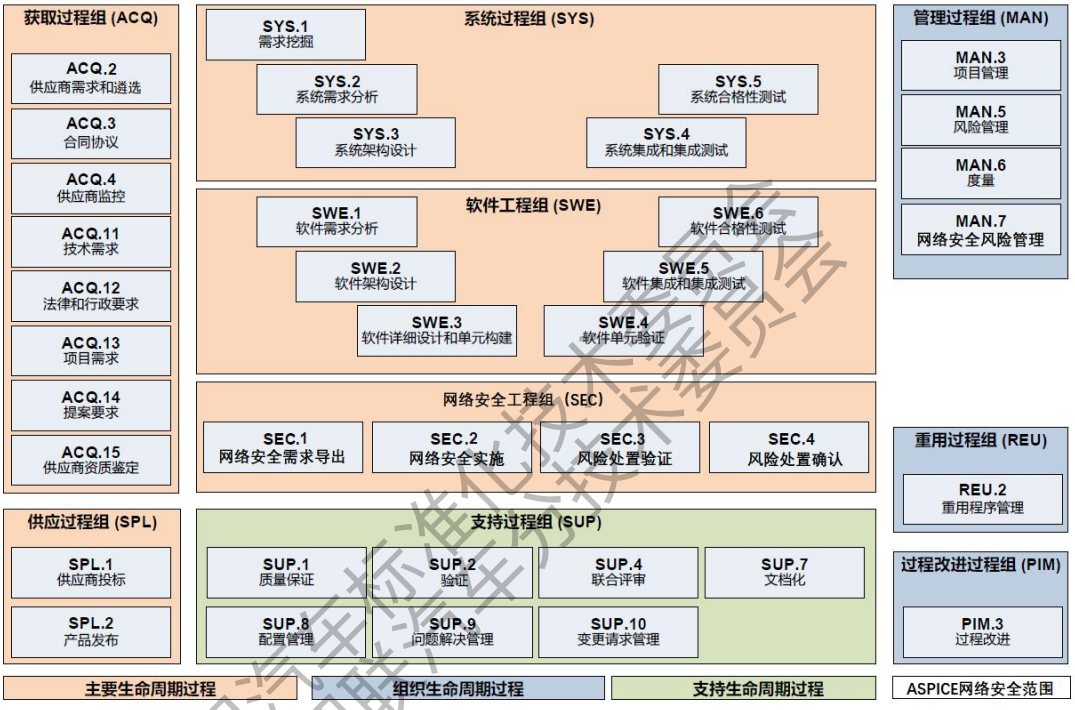

图1 ASPICE和ASPICE网络安全过程参考模型-概述

与网络安全致力于保护重要、敏感数据和软件安全不同，ASPICE更着重于软件开发过程，旨在评估并提升其效率和有效性。ASPICE为包含安全注意事项的开发过程提供框架模型和最佳实践，例如安全测试和安全编码实践，以此指导车辆制造商或其供应商开发安全的软件产品，助力组织在开发过程的早期识别并降低安全风险。这是因为它们分别解决了汽车行业软件开发不同方面的问题。

用于网络安全的汽车SPICE评估，其目的是识别主要生命周期过程、管理过程和支持过程中的系统性弱点，并识别与流程相关的产品风险。和ASPICE一样，网络安全汽车SPICE评估通过提供框架来防范软件开发过程中的风险，但仍需要额外开展针对网络安全的验证和确认实践。

1.1.3 国内标准研究内容及进展

自2021年10月起，国内陆续发布了多个关于智能网联汽车信息安全的强制性国家标准和推荐性国家标准，对汽车整车及其电子电气系统、车载信息交互系统、汽车网关、电动汽车充电系统等部件系统提出了推荐性要求。与此同时，汽标委正在推进相关汽车信息安全配套标准的制定工作，以完善汽车产业链和全生命周期的研发、管理和测试等标准体系。

其中，GB 44495—2024《汽车整车信息安全技术要求》标准规定，需建立涵盖车辆开发阶段、生产阶段以及后生产阶段的车辆全生命周期汽车信息安全管理体系。对于研发过程中的测试和验证，该标准也对其有效性提出了要求，例如“6.6 车辆制造商应通过测试来验证所实施的信息安全措施的有效性”。不过，鉴于标准不宜对技术路线加以限定等因素，不便对研发过程提出强制性要求。

GB/T 46194—2025《道路车辆 信息安全工程》标准等同采用ISO国际标准ISO/SAE 21434:2021，该标准涵盖了安全风险的评估与管理、安全功能的规划与设计、安全测试和验证等方面的指导内容，同时着重强调了针对汽车网络安全的整体风险管理方法。

表1 国内标准进展

序号	标准名称	状态
1	GB 44495—2024 《汽车整车信息安全技术要求》	已发布
2	GB/T 40855—2021 《电动汽车远程服务与管理系统信息安全技术要求及试验方法》	
3	GB/T 40856—2021 《车载信息交互系统信息安全技术要求及试验方法》	
4	GB/T 40857—2021 《汽车网关信息安全技术要求及试验方法》	
5	GB/T 40861—2021 《汽车信息安全通用技术要求》	
6	GB/T 41578—2022 《电动汽车充电系统信息安全技术要求及试验方法》	
7	GB/T XXXX—20XX 《汽车安全漏洞分类分级评价》	制定中
8	GB/T XXXX—20XX 《汽车网络安全入侵检测技术要求及试验方法》	
9	GB XXXX—20XX 《汽车密码应用技术要求》	
10	GB/T 46194—2025 《道路车辆 信息安全工程》	

1.1.4 国内行业现状调研

1.1.4.1 调研结果

本研究报告编写过程中，工作组针对网络安全验证和确认的现状开展了两次调研，第一次早期调研旨在了解行业的基本情况，主要包含以下内容：

1) 企业是否已按照ISO 21434搭建CSMS体系？

2) 开展车型TARA后，企业内部是否有对TARA结果（网络安全目标和声明）的正确性进行质量评估或验收的流程？

3) 企业内部是否有对网络安全概念（需求）进行正确性、合理性的评估过程？

4) 企业内部是否有对网络安全规范或设计方案进行质量评估的过程，例如对设计方案与具体需求对应的合理性和覆盖性进行评估、对设计方案是否引入新的威胁或缺陷有所评估？

5) 网络安全验证活动的开展方式有哪些？

6) 整车层面的集成和测试的工作由哪些角色完成？

7) 零件层面的集成和测试的工作由哪些角色完成？

8) 是否有明确的时间界限划分？

9) 对网络安全验证活动，开展方式有哪些？

10) 对网络安全目标的确认过程，零件层面网络安全的目标确认（例如通过渗透测试等方式）由谁完成？

11) 对整车网络安全目标和声明的确认工作，和零件层面网络安全目标的确认工作是否有明确的时间界限？

12) 网络安全验证和确认活动是否有明确的时间界限？

本次调研问卷的样本涵盖了12家企业，包括百度 Apollo、比亚迪、长安、特斯拉、百度、一汽大众、吉利、一汽红旗、长城、赛力斯、小米和小鹏。

企业类型分布情况为：1家外企、1家合资企业，10家为自主企业，具体情况见图2。车辆类型分布情况为：1家商用车企业，11家为乘用车企业。其中，ISO/SAE 21434 CSMS体系搭建情况为：1家未搭建，其余11家均已完成搭建。

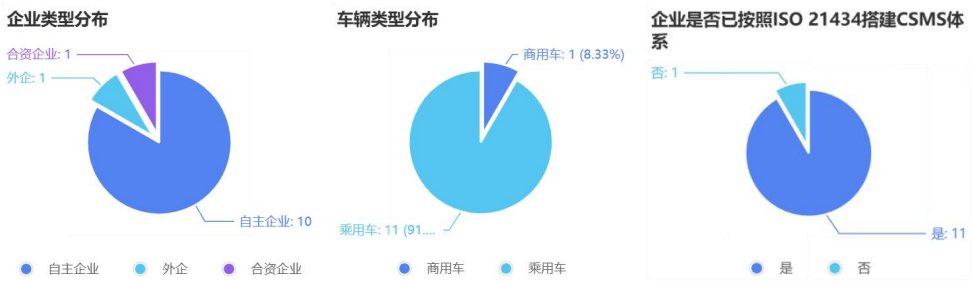

图2 调研企业现状

TARA结果质量评估：所有企业均回复“有开展评估”，不过企业的组织形式存在较大差异。主要形式包括：测试验证（4家）、内部评审（2家）、会议评审与报告结合（2家）。补充说明：部分企业提及“功能开发参与评审”等情况。总结：所有企业均开展了TARA结果评估，但流程的标准化程度参差不齐。

网络安全概念（需求）评估过程：所有企业均回复“有”。主要评估方式如下：测试验证（2家）、内部评审（2家）、会议评审 + 报告（2家）。补充说明：部分企业提及“参考行业最佳实践”“整车信息安全团队验收”。总结：评估过程普遍存在，但缺乏统一标准。

网络安全规范/设计方案质量评估：有评估过程的企业共11家。主要评估方式包括：会议评审（5家）、内部评审（3家）、整车信息安全团队验收（1家）。总结：大部分企业（91.6%）会对设计方案开展质量评估，但评估流程仍有待细化。

网络安全验证活动的开展方式如下：源代码审计（8家）、固件代码扫描（11家）、白盒功能验证（8家）、专家组评审（5家）、灰盒渗透测试（10家）、黑盒渗透测试（9家）、模糊测试（7家）、漏洞扫描（11家）、安全功能测试（1家）。总结：固件代码扫描和漏洞扫描为必选项目，渗透测试的普及率较高，具体情况见图3。

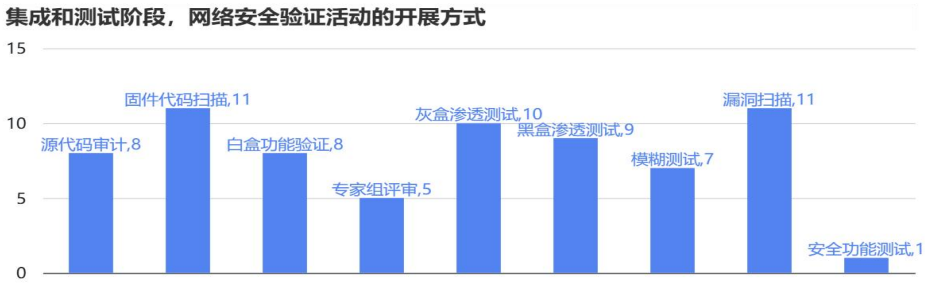

图3 集成和测试阶段，网络安全验证活动的开展方式

测试的角色分工情况如下：在整车层面，有5家由OEM完成，7家由供应商配合完成；在零件层面，有6家由OEM完成，6家由供应商完成。总结：各企业在集成与测试的角色分工上差异较大，在零部件层级的确认活动分工上，2家完全由零部件供应商完成；10家为OEM完成，零部件供应商仅做相关零部件的验证活动。

集成测试阶段的时间界限情况如下：8家企业明确采用“先零件后整车”的模式；4家企业存在“零件与整车同步进行”的情况；在整车和零件层面网络安全目标的确认方面，有7家企业有明确界限，5家企业无明确界限。总结：大部分企业划分了时间界限，但部分自主企业仍存在并行或界限模糊的阶段.

网络安全验证和确认活动时间界限情况见图4：

基于开发阶段或V模型的严格阶段划分25%（3家），如：参考ISO/SAE 21434的V模型执行、变更冻结节点先做验证测试，投产节点再做确认测试、验证是在PT（生产验证）阶段，确认是在SOP（量产）之前；

基于供应商协作的界限划分16.7%（2家），如：零部件供应商完成部件网络安全验证后，OEM再行开展确认活动，以零部件完成所有功能开发，并针对全功能开发完成渗透测试工作为时间界限；

基于模糊的时间管理50%（6家），如：结合需求验证及测试、先开展需求验证，再开展确认测试，中间有并行阶段、通常以样件的时间节点去要求、伴随集成测试节点（未明确验证和确认的具体分界）；无明确时间界限8.33%（1家）。结论：多数企业（58.33%）采用模糊或无时间界限，剩下的企业中仅有1家参考了ISO/SAE 21434的V模型，行业内对于网络安全验证和确认活动时间界限不清晰，且差异较大。

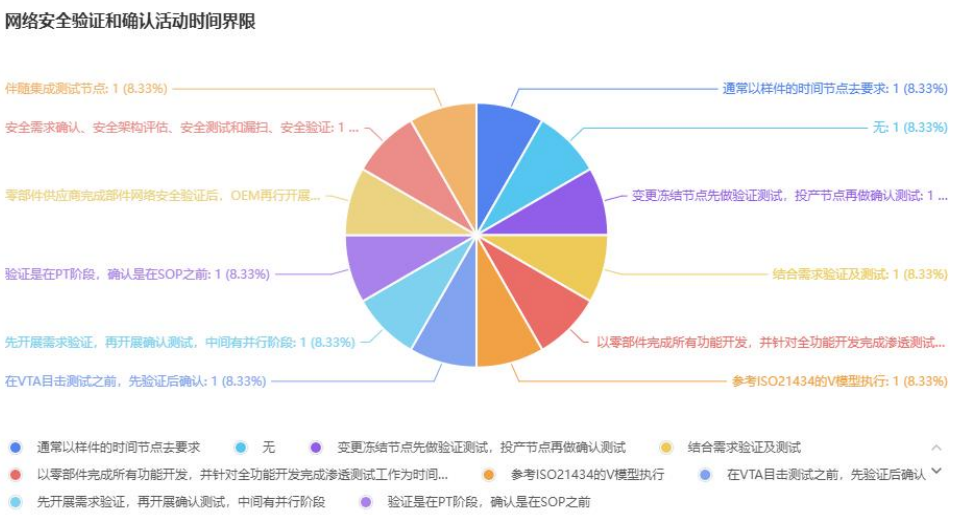

图4 网络安全验证和确认活动的时间界限

考虑到第一次调研中存在些许认知偏差，不能准确的描述验证和确认执行的行业现状，故在在2024年4-5月开展了第二次行业调研，本次调研聚焦在V&V活动分布、V&V最佳实践方法两个板块。共15家单位参与了调研，分别是华为、赛力斯、中国汽研、比亚迪、合众、百度、小米、一汽红旗、信长城、航迹、长城、小鹏、蔚来、地平线、上汽。

V&V活动分布调研目的主要是了解TARA、网络安全声明、网络安全目标、网络安全需求、网络安全控制、网安全规范等过程如何开展质量评估，其结果与第一次调研大致相同，但是更加详实，新增了较多具体的评估办法。如，针对TARA的质量评估，有1家企业是根据TARA结果，开展：

1）核对安全需求方案和安全功能详细设计方案；

2）进行渗透测试

其余企业均是通过专家评审开展TARA质量评估，出具核查报告的方式开展；各家OEM均有针对网络安全声明和假设进行正确性、合理性的评估过程，均已评审记录、会议纪要等形式进行；针对网络安全目标进行正确性、合理性的评估过程基本一致，即根据威胁场景和攻击路径，并结合实际情况综合确定网络安全目标，内部专家会组织会议进行评审，并通过验证和确认测试验证是否达到了网络安全目标；针对网络安全需求进行正确性、合理性的评估过程也同时包含了评审、验证测试等方法；对网络安全控制进行正确性、合理性的评估过程出现了一些分歧，其中5家OEM反馈企业内部暂无相关控措施，其余有控制措施的OEM其

实施方案也各不相同，包括内部评审、功能测试、非正式评估、联合评审等方式；针对网络安全规范或设计方案进行质量评估的过程，中我们重点关注对设计方案与具体需求对应的合理性和覆盖性进行评估、对设计方案是否引入新的威胁或缺陷要有所评估，关于这点，1家OEM采用了Retara的方式，1家OEM要求供应商先对网络安全规范进行评估，出具网络安全规范验证报告，然后再进行网络安全联合评审，出具联合评审报告，1家OEM反馈网络安全需求所对应设计方案由承担该需求的专业组负责，方案与需求对应的合理性和覆盖性同理；其余可归纳为主要靠经验开展评审活动，形成评审会议纪要的方式。

V&V最佳实践方法的调研旨在收集、提炼行业常用的实践方法，并依据这些测试方法，制定相应的质量评估办法，调研的基本情况如下：

序号	单位名称	审查		静态代码分析审查		形式化验证		虚拟仿真		功能测试		模糊测试		漏洞扫描		渗透测试		其他方法请补充	
		验证	确认	验证	确认	验证	确认	验证	确认	验证	确认	验证	确认	验证	确认	验证	确认	验证	确认
1	特斯拉（上海）有限公司																		
2	百度	√	√	√	√	×	×	×	×	√	√	√	√	√	√	√	√	×	×
3	北京航迹	√	√	×	√	×	×	×	×	√	×	×	√	×	√	×	√	×	×
4	小米汽车科技有限公司	√	√	√	√	×	×	×	×	√	√	√	√	√	√	√	√	×	×
5	北京信长城科技发展有限公司	√	√	√	√	×	×	×	×	√	√	√	√	√	√	√	√	×	×
6	一汽红旗	√	×	√	×	×	×	×	×	√	×	×	√	√	×	√	√	×	×
7	中国汽车工程研究院股份有限公司	√	√	√	×	×	×	×	×	√	×	×	√	×	√	×	√	×	×
8	赛力斯汽车集团股份有限公司	√	×	√	×	×	×	×	×	√	√	×	√	×	√	×	√	×	×
9	华为技术有限公司	√	√	√	√	×	×	×	×	√	√	√	√	√	√	√	√	敏感信息扫描	敏感信息扫描
10	比亚迪汽车工业有限公司	√	√	√	×	×	×	×	×	√	√	×	√	×	√	×	√	1.第三方开源组件	
11	吉利新能源汽车股份有限公司	√	√	√	√	×	×	×	×	√	√	√	√	√	√	√	√	×	×
12	长城汽车股份有限公司	√	√	√	×	×	×	×	×	√	√	×	√	√	√	×	√	×	×
13	蔚来汽车	√	√	√	×	√	×	√	√	√	√	√	√	√	×	√	√	√	√
14	小鹏汽车	√	√	×	√	×	×	×	×	√	×	×	√	×	√	×	√	×	×
15	广汽																		
16	地平线	✓	✓	✓	×	×	×	✓	×	✓	×	×	✓	×	✓	×	✓	×	×
17	上汽研发总院	✓	×	✓	×	×	×	×	×	√	×	×	✓	√	√	×	✓	×	×

图5 V&V最佳实践方法调研

根据上图可总结出行业采用的共性测试方法有6种，详见图6，分别是审查、代码析、功能测试、漏洞扫描、模糊测试、渗透测试。每个方法分别有15家采用，另有一些小众的测试方法被采纳，如虚拟仿真、形式化验证、敏感信息测试等。

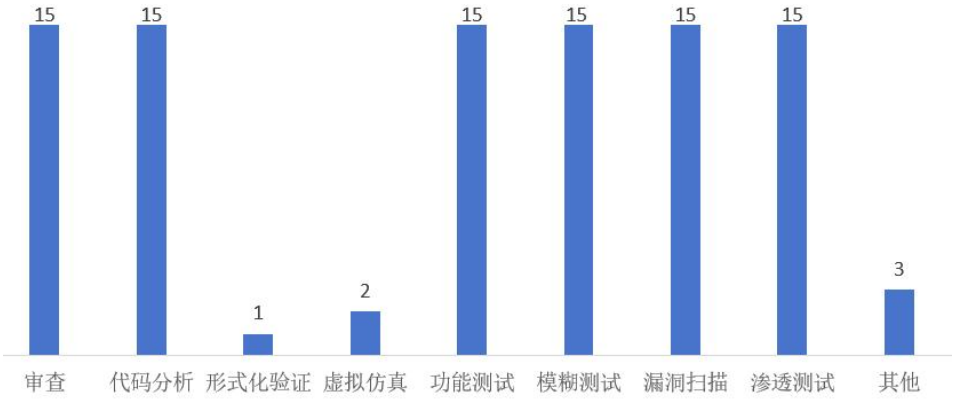

图6 行业采用的共性测试方法

1.1.4.2 行业问题总结

1) 评估流程相对简易或笼统：部分企业仅通过“网络安全测试验证报告”“功能开发参与评审”等方式对TARA结果进行评估，评估流程的规范性和专业性欠佳。

2) 流程标准化程度不足：部分企业并未完整的定义体系流程及活动，不具备连续性。

3) 层次界限模糊：不同企业在零部件与整车开展顺序上存在差异，同时部分企业没有明确的界限，没有统一的测试要求。

4) 时间界限模糊：58%的企业采用模糊或无界限的非结构化时间管理，这不利于对汽车网络安全验证和确认过程进行有效管理。

1.1.4.3 问题分析

1) 对ISO/SAE 21434框架的理解存在差异，从而导致执行出现偏差。

2) 缺乏详细的操作指南，例如TARA量化评估方法、汽车网络安全验证和确认方法等。

3) OEM与供应商的责任边界模糊，网络安全验证和确认的时间界限也不清晰，在并行开发场景中缺乏协同标准。

1.2 意义及重要性

1.2.1 国内外行业意义

国际标准ISO/SAE 21434和R155均涵盖了网络安全验证与确认的要求。对于面向国外市场的企业而言，构建符合国外安全标准的运行体系十分关键，对这部分内容的审查也是审查流程中不可或缺的环节。该指导标准的落实，对企业拓展国外市场具有积极意义。

从国内市场来看，完善企业汽车网络安全体系框架中的网络安全验证和确认部分，无论是新产品进入国内市场，还是现有产品进行迭代更新，标准化的网络安全验证都能提升产品的安全性，更有助于企业在国内市场的发展。

车辆网络安全验证与确认活动的规范，有助于凝聚智能网联汽车行业对于网

络安全验证和确认活动的共识。它能为制造商、供应商、安全服务机构等汽车产业链上的众多企业提供最佳实践参考，引导企业规范开展相关活动。同时，它也为行业监管提供重要支撑，减少国内外市场的技术壁垒，推动汽车网络安全的持续发展。

1.2.2 对企业能力和技术指导的意义

1.2.2.1 确保整车产品的网络安全能力

对于产品研发V模型来说，验证测试环节是证明产品需求得以实现的必要步骤。车辆网络安全作为汽车产业中相对新颖的产品需求，对车辆网络安全需求实现情况进行验证和确认更是不可或缺。从企业合规的角度来看，海外汽车产品准入要求明确规定了对车辆网络安全概念的验证与测试工作，并将验证流程融入车型研发生命周期的各个阶段，以此证明网络安全需求实现的完整性与准确性。从产品网络安全能力建设的角度而言，针对车辆网络安全各层级开展的验证测试工作，有助于OEM更精准地识别产品的网络安全防护能力，强化车企自身的网络安全研发能力，同时在一定程度上更好地识别与管理供应商的网络安全研发能力及其产品的网络安全防护能力。

此外，在整车研发临近尾声时，网络安全确认活动作为对研发全过程中风险识别与管理情况的审查，承担着在整车网络安全能力上线前进行评估的重要作用。网络安全确认从风险管理的视角出发，对研发阶段网络安全活动的流程层面展开再次评估，有助于企业审查当前产品研发流程中网络安全活动的完整性与有效性，进而反馈并推动企业网络安全能力建设。同时，通过开展必要的车型渗透测试活动，从技术层面再次评估产品的网络安全防护能力，有助于企业识别产品的网络安全风险。车辆网络安全确认活动从流程和技术两个维度，在产品上线前进行了全面评估，以确保整车产品具备可靠的网络安全能力。

1.2.2.2 明确供应商与OEM之间的任务分配

R155要求车辆制造商证明其有能力应对供应链中来自Tier1（一级供应商）、服务提供商或集团子公司可能存在的网络安全风险，但对于该风险管理应由哪一方进行管控并不明确。通过规范的车辆网络安全验证和确认活动，可解决诸多供

应商与OEM之间的责任界定和生产成本问题。

责任界定：车辆制造商与供应商需明确各自的责任边界，确保在汽车网络安全问题出现时能够追溯责任。此外，软件供应商和OEM的地位也增加了责任界定的难度，可借助行业公认的具体文件，增进双方的认可。

生产成本：明确的验证与确认时间安排以及任务分配，能够使车辆制造商和供应商达成共识，合理降低成本，在提升汽车市场竞争力的同时，确保其安全可靠。

1.2.2.3 提供合理性、充分性实施细则

如1.1所述，国内外相关重要标准仅对汽车信息安全的合理性与充分性提出要求，却未给出具体细则或实施方法。整车制造商和供应商通常借鉴互联网等跨行业经验来完善自身做法。

在国际方面，ISO已率先采取行动，ISO/SAE 8477以TR的形式对ISO/SAE 21434进行补充支持，明确了汽车网络安全的合理性与充分性。而国内在这方面仍存在空白，制定汽车网络安全的验证和确认活动指导文件将有助于国内车型以及出口车型的开发。

1.3 总结

本章通过对企业在国内外开展验证和确认测试的方式、时间、方法以及测试分配原则进行调研，并结合对V&V测试执行情况的分析，明确了网络安全V&V测试技术与行业标准研究的重要意义。该研究不仅为企业实施V&V测试提供了具体指引，还清晰界定了供应商与车企之间的责任边界，同时为法律法规及标准的落地实施提供了标准化参考，进而有效增进行业共识，推动整体网络安全水平提升。

随着智能网联汽车面临的网络安全问题愈发复杂和严峻，网络安全事件与风险漏洞不断增多。基于汽车企业网络安全体系和供应链安全体系的构建以及网络安全防护技术的提升需求，国际和国内均已发布或正在制定网络安全相关的法律法规及标准。这些法规和标准明确了开展网络安全验证和确认测试的必要性，也明确了行业公认的验证和确认测试技术要求。

然而，在国内现行的标准文件中，尚未有针对汽车网络安全验证和确认提出明确指导的文件。企业在建设汽车网络安全体系的过程中，由于自身能力不够完备，或者对相关标准要求的解读存在差异，导致体系建设出现偏差，无法满足相关标准的要求。

通过实施这一指导性标准，更有助于国内相关标准的落地实践与创新发展。企业在解读相关标准中网络安全验证和确认部分时，能有一个清晰的框架，再结合自身实际情况，企业汽车网络安全体系建设也会更加高效。有了标准文件的指导，有助于企业构建规范化的体系运行机制。

与此同时，网络安全验证和确认作为车辆全生命周期中必不可少的网络安全活动，是确保车辆达到足够且可接受的网络安全水平的关键所在。

因此，规范并明确网络安全验证和确认活动的开展时间、实施方法、范围与深度、职责分配、成果以及质量评估等内容，既填补了我国汽车网络安全领域标准体系框架中 V&V 的空白，也是技术发展与应用落地对标准规范提出的要求，对汽车产业生态网络安全发展具有重要的指导意义。

鉴于以上国内外标准、行业现状及需求背景，有必要在国内开展网络安全验证和确认标准需求研究。通过调研并梳理网络安全验证和确认活动，建立网络安全验证和确认活动的质量评估方法，为网络安全验证和确认标准化工作提供建议。

2 网络安全验证和与确认

2.1 网络安全验证和确认总述

2.1.1 道路车辆 网络安全工程

道路车辆网络安全工程的实施范围覆盖了车辆的全生命周期，包含概念阶段、开发、生产、运维、报废等所有环节。当前可依据ISO/SAE 21434标准来实施，该标准提供了一个标准化的网络安全框架，将网络安全确立为车辆整个生命周期中不可或缺的工程要素。从概念阶段直至车辆报废，它确保在后续开发阶段（如软件更新、服务和维护、事件响应等）充分考量网络安全，并且要求采取有效举措，包括总结经验教训、开展专业培训，以及强化汽车网络安全领域的交流合作，以此全面提升道路车辆网络安全的防护能力。

道路车辆网络安全风险管理的全生命周期管理过程，可用图7的闭环图像来表示。不过，ISO/SAE 21434既未规定具体的网络安全技术或解决方案，也未明确给出补救方法的相关规定。本研究标准《道路车辆 网络安全验证与确认》的核心内容，正是聚焦于产品开发过程中的网络安全的验证活动和确认活动，深入探讨并展开相关的研究与实践。

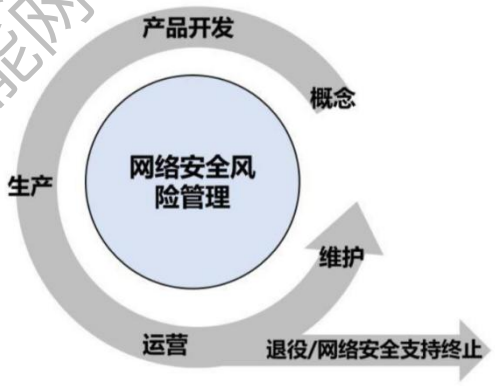

图7 道路车辆网络安全风险管理的全生命周期管理过程

网络安全验证与确认，是车辆全生命周期管理过程中产品开发阶段的两项重要活动。涉及车辆网络安全的整车开发流程，可参考图8所示的 V 字模型来理解。在 V 字模型的左侧，是从整车到子系统再到零部件的逐级分解细化的开发流程，该流程彰显了开发工作的深度与精度。在 V 字模型的右侧，呈现出从零

部件的集成与验证，逐步向上拓展至子系统的集成与验证，最终达成系统及整车层面的网络安全确认活动，保障整车网络安全活动开发验证的完整性与一致性。

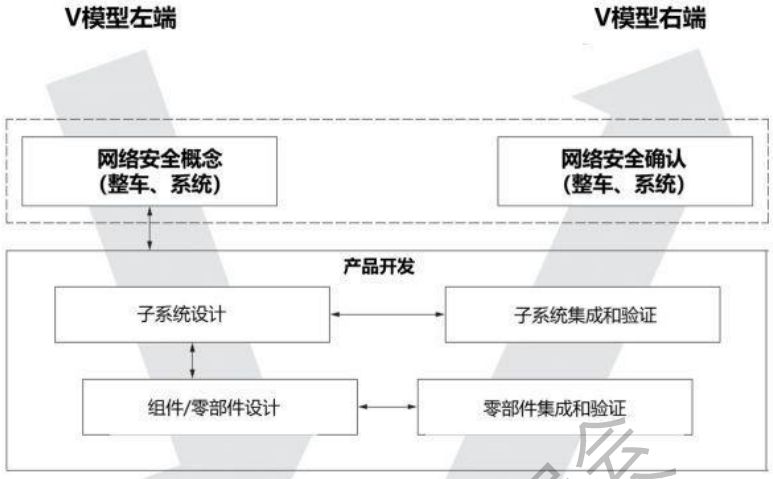

图8 网络安全的开发V字模型

2.1.2 验证与确认(V&V)的关系

验证与确认的概念在功能安全和网络安全领域均有相关定义。网络安全领域的理论基础源于国际标准ISO/SAE 21434。ISO/SAE 21434采用了分层设计理念，这一理念也构成了行业内公认的最佳实践。在这种分层架构中，每个层次的网络安全开发活动既相互独立，又相互嵌套。每个开发阶段都需对其成果的正确性进行验证，以确保一致性。同时，每个层级都可能引入潜在的弱点或漏洞，这些弱点和漏洞可能会对该层级网络安全需求的实现造成影响。因此，为确保各层级网络安全开发活动的准确性和有效性，需要采用评审、测试等多种手段进行深入验证。

网络安全领域的验证和确认活动，其差异主要体现在实现目标和开展内容上。最根本的差异在于验证活动通过审查、测试等手段，以确保零部件、子系统和整车的开发结果契合最初设定的网络安全需求。而确认活动亦可通过审查、测试等方法，检验安全目标是否得以实现。

验证活动的主要目的是验证网络安全开发活动中的风险评估结果、网络安全概念及需求、网络安全方案及实施过程的正确性，这是一项覆盖车型开发V模型全阶段的网络安全活动。对于风险评估结果、网络安全概念及需求、网络安全方

案等阶段（通常称之为左V），验证活动通过评审等方式来验证其结果的正确性。对于网络安全方案的实施阶段（通常称之为右V），验证活动主要通过测试或审查等方法来验证其实施的正确性，保证活动达成目标。确认活动主要目的为确认车型产品网络安全目标及声明的有效性，确认其通过网络安全开发实施过程达到了其网络安全目标，且确认网络安全声明的合理性，最终实现车型产品网络安全风险可控。网络安全确认活动也是一项覆盖车型开发V模型全阶段的网络安全活动。左V的网络安全目标和声明在确认过程中可能会通过审查、渗透测试等方法开展。如果通过测试方法，则与中间的开发方案关联性较弱，然而，若采用审查方法，则需要深入审查开发方案、零件的渗透测试报告等关键内容，需要借助左V和右V的成果物来完成整个确认的过程。（在ISO/SAE 21434第11.4节确认活动的要求及建议中提出，确认活动可以包括：

1) 通过审查第9.5条【网络安全概念】和第10条【产品开发】的工作成果，确认网络安全目标的实现；
2) 渗透测试以证明安全目标的充分性和实现情况；
3) 通过对第9条【概念】和第10条【产品开发】确定所有管理风险进行审查）。

验证活动提供证据证明网络安全需求得到满足，包括：1、符合上一层级的网络安全需求（直至网络安全目标）；2、实施和集成环节符合网络安全需求。考虑到既定的网络安全目标和网络安全声明，确认活动通过提供证据，证明网络安全条目已集成到目标车辆中。尽管验证活动和确认活动的目标有所不同，但它们可采用相同或相似的方法。

如果进行了更改，则应实施变更管理。例如，在产品运行阶段对其进行的变更，如为解决网络安全问题或处理网络安全事件而进行的软件更新，这包括对验证和确认有关的工作成果进行的变更管理，可能涉及对此类活动的补充，如回归测试。

在验证或确认活动过程中识别的异常或发现，例如发现的弱点或漏洞，需进行分析并采取措施予以解决（参见ISO/SAE 21434:2021第8.5和8.6节)。这可能涉及修改项目或组件（如调整运行模式）。问题发现的越晚，解决起来就越困难，这就是为什么验证和确认活动应在依赖的信息输入完成后尽早执行的原因。

根据网络安全接口协议，验证和确认活动可以由车辆制造商和/或供应商共

同执行。该协议涵盖了双方的信息交流，确保各方都能够履行各自的责任。

验证活动确保项目或组件在不同抽象层级上符合分配的网络安全需求，它解答了“我们是否正确构建了项目或组件？”的问题。确认活动侧重于网络安全目标和网络安全声明的充分性和实现情况，可以定义如下：任何能够回答“我们是否构建了一个适当且足够安全的网络安全项目或组件？”这一问题的活动。这是将通用启发式方法“我们是否在构建正确的产品？”在道路车辆网络安全领域的应用。

一个项目包含了多个抽象层级。相应地，网络安全需求及其实施可以用任何层级的细节来指定，包括高层级的概念控制，例如项目级别的网络安全需求，以及详细的控制设计。因此，任何层级都可能存在弱点或漏洞，从而阻碍了分配给该级别的网络安全需求或网络安全目标的实现。

如图9所示，验证活动和确认活动与需求层次有关：

1) 确认与需求层次结构的最高级别相关，即涉及：

(1) 网络安全目标；

(2) 项目级别的网络安全需求；

(3) 与项目级别相关的网络安全假设；

(4) 项目级别的网络安全声明；

从1）可以看出，分配给项目级别的网络安全需求起着特殊作用。如果具体指分配给项目（整体）的网络安全需求，则本文档使用术语“项目级别的网络安全需求”，相反，如果未提及特定的需求层次，则使用术语“网络安全需求”。同时，需要注意网络安全需求及网络安全假设中还需要包含对于环境的需求和假设

2) 验证活动可应用于需求层次结构的任何级别。

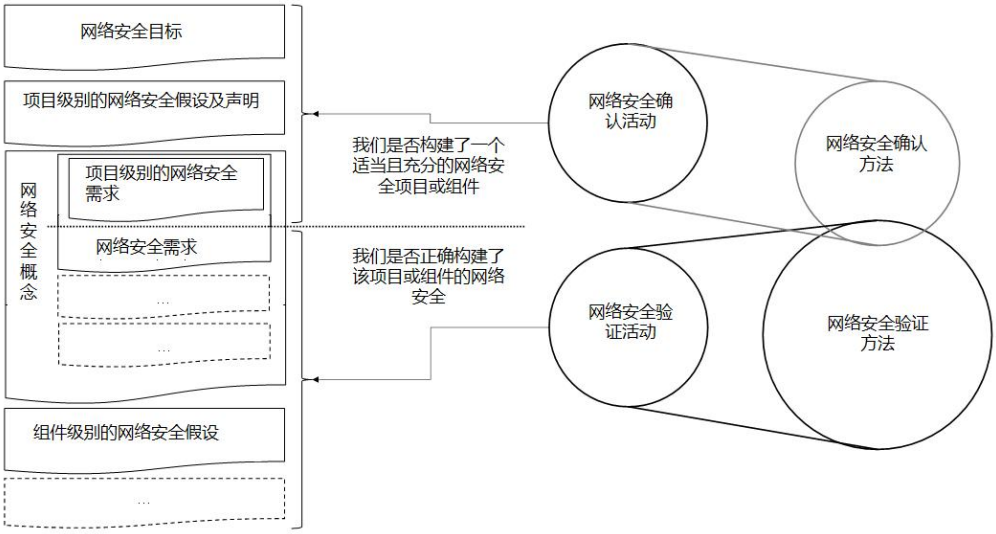

图9 验证和确认之间差异

2.1.3 V&V与其他网络安全活动的关系

验证和确认与其他网络安全活动和ISO/SAE 21434:2021工作成果关系，如图10所示。

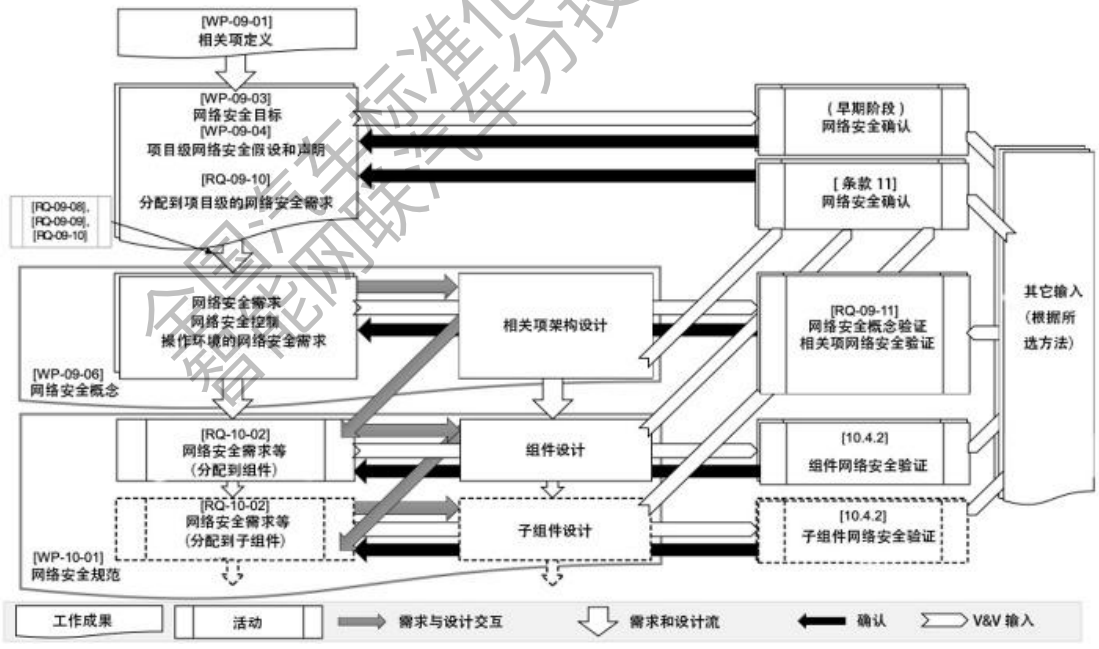

图10 V&V 活动与 ISO/SAE 21434:2021 活动及工作成果之间的关系

验证工作围绕网络安全需求、架构设计或实施等方面展开。网络安全需求以及相应架构设计的细化程度取决于所采用的网络安全控制措施，验证活动也会据此相应确定。因此，图10中的虚线代表子组件的需求、设计和验证。

确认工作适用于抽象和详细层面的网络安全目标。在较高的架构抽象层次上，

确认的重点在于那些尚未细化到可完全实施（“可构建”）程度的假设、网络安全声明或网络安全控制措施。不过，确认也能够延伸至这些目标在实际场景中的有效性，并在架构的任何层面开展技术实施（如渗透测试），涵盖接口（如与其他项目或组件的接口）以及对运行环境的考量。

这是对ISO/SAE 21434:2021第3.1.36节的详细阐释，该节将网络安全确认定义为仅对项目网络安全目标的充分性及其实现情况进行确认。

工作成果“网络安全概念”（参见ISO/SAE 21434:2021第3.1.13节）包括“项目级别的网络安全需求”。

工作成果“网络安全规范”（参见ISO/SAE 21434:2021第3.1.21节）包括“网络安全需求”，以及“架构设计”。

如果早期确认结果没有使网络安全目标失效，则表明项目和组件的网络安全适当和充分。

2.1.4 V&V与开发类型的关系

2.1.4.1 重用

在对现有项目或组件进行重用时，需要对其适用性展开分析，具体如下：

若现有的工作产品未按照 ISO/SAE 21434 标准开发，比如遗留组件，或是并非专门为汽车应用开发的现成组件，就需要判定它们是否适用。

例如，对于验证或确认证据不足且设计无法检查的组件，验证或确认策略（见第2.1.5条）可通过以下方式解决证据缺失问题：

1) 采用黑盒方法指定测试用例和测试方法，以确认威胁场景已得到解决；
2) 用该组件或类似组件的网络安全监控结果，替代通过执行差距分析发现的缺失证据（另见 ISO/SAE 21434:2021，第 8 章）；
3) 检查被重用组件的指定配置，以确认其按照威胁场景的预期运行。

对重用的分析还包括分析对项目、组件或运行环境所做的任何更改的影响，例如对与项目或组件相关的现有验证和确认工作产品的影响。为了解决这个问题，可以计划补充验证和确认活动，例如回归分析或回归测试。

2.1.4.2 独立于环境的开发

独立于环境的开发是基于与供应商期望从潜在OEM处获得的内容有关的假设，包括：

1) OEM打算使用该组件的预期环境，如使用条件；
2) 网络安全目标、概念性网络安全需求或其他网络安全需求，即供应商预期的需求将被指定并分配给潜在OEM在独立于环境开发的组件。

此类假设应在相应的工作产品中予以记录。验证是根据假定的需求进行的，并且可以被视为等同于根据商定的需求进行的验证。

如果OEM计划使用在独立于环境开发的组件，则将其集成到独立环境中。如果分布相应的网络安全活动，则在网络安全接口协议中指定这些活动。验证和确认包括确认相应的假设。如果假设不成立，OEM和供应商共同商定如何解决这一问题。

2.1.4.3 使用现成的组件

使用现成组件的开发是指没有接口协议的开发。即使没有现成组件开发的接口，关于后期开发的网络安全接口协议也可能是相关的，例如关于网络安全监控。现成组件的供应商可以提供与OEM执行的验证或确认活动相关的可用文档。

2.1.5 V&V的策略方法

验证和确认策略为如何规划和开展验证和确认活动提供了框架，包括确认该项目是否符合网络安全需求、已查明的漏洞是否得到妥善处置、是否能抵御现实环境中的各种威胁场景。使用的策略可包括：

1) 范围内的项目或组件的定义；
2) 确定活动目标；
3) 选择方法的理由，例如：网络安全保障级别、进入和退出标准（其中进入标准指能够启动一项活动的条件，退出标准指将一项活动视为已完成的条件）、组织规则和指导原则；
4) 通过/不通过标准；
5) 规划，包括：时间表和责任、与 TARA 等其他活动的协调、活动说明

（包括选定的方法、测试用例和测试范围）、通信渠道和频率、如何管理调查结果或与战略或计划的偏差；

6) 规划分布式活动，包括如何在参与方之间分配活动、就测试范围达成一致、关于互信交流的协议、如何处理车辆制造商或供应商发现的问题。

可以考虑利用现有经验来优化工作，例如，可以利用现有的网络安全控制作为测试用例和测试规范的输入，特别是现有的经验允许将资源集中在项目或组件的网络安全控制方面的新问题或特别关注的问题。

2.2 验证和确认活动

当验证和确认活动的依赖关系满足时，应尽早开展验证和确认活动。这一原则适用于所有网络安全活动，因此可在项目或组件开发的前期和后期执行验证与确认活动。例如，在项目开发前期，就能依据已定义的威胁场景和安全目标，开展对网络安全目标的确认活动。值得一提的是，不仅验证活动，确认活动同样可以在任何阶段进行。

2.2.1 威胁分析和风险评估

TARA（参见 ISO/SAE 21434:2021，[WP-09-02]）依赖于网络安全控制，或者项目或其组件的属性进行风险评估。例如：

示例[1]：风险评估依赖于设计实施的网络安全控制措施，例如依赖于安全启动的攻击可行性评级；

示例[2]：风险评估依赖于通过流程措施实施的网络安全控制，例如根据一套规则或准则进行编码；

示例[3]：由于功能特性或设计特性而涉及滥用的威胁场景。

网络安全工程是一项迭代活动，包括TARA的执行。随着设计和网络安全需求的逐步完善，TARA需同步更新。这一过程可能涉及对风险的调整（例如示例[1]和[2]），也可能涉及威胁场景的新增或修改（例如示例[3]）。这个迭代过程一直持续到可以接受剩余风险为止。如图11所示，虚线表示反馈回路。

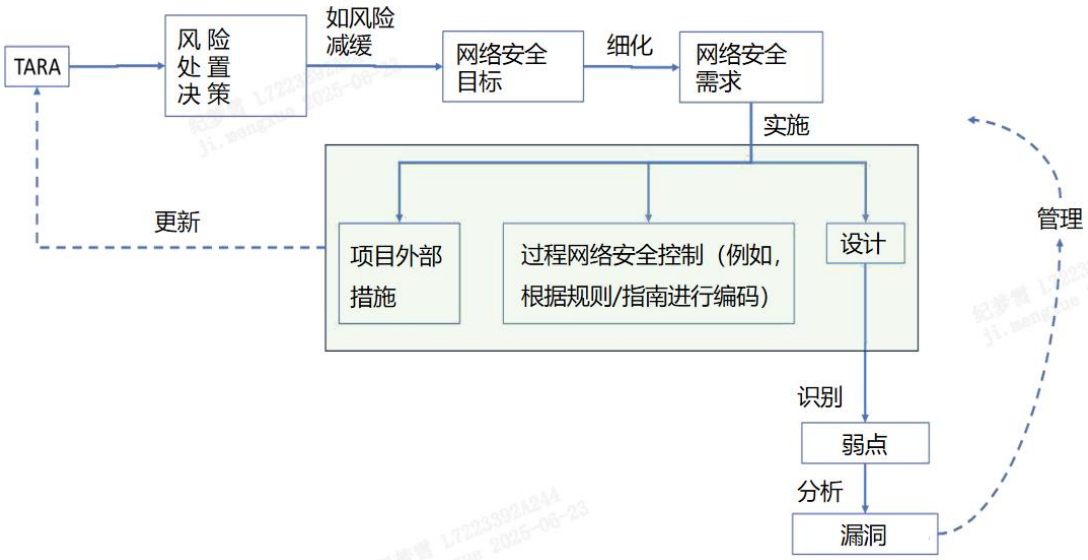

图11 网络安全活动的迭代性质

如上所述，由于TARA可以依赖该设计，因此验证包括提供证据证明TARA中网络安全控制的可信度，包括以下证据：

1) TARA所依赖的网络安全控制措施确实已实施。例：TARA的信用基于指定的网络安全控制，但验证发现该网络安全控制措施未实施（例如缺少监督）或因设计变更未维护（例如缺少变更管理），则需检查确认。
2) TARA所依赖的网络安全控制满足预期效果。例：攻击可行性评级在规范时预测了网络安全控制的效果，但验证需基于现有经验（例如现场数据支持）证明其实际效果与预期一致。

此外，验证还包括提供证据，证明所识别的威胁场景集是正确和完整的。

注1 基于检查表进行检查。这种清单可以包括从以前的发展、其他项目或任何其他来源中已知的威胁场景列表。

注2 结合威胁场景识别。通过检查攻击树分析结果来验证是否识别出使用更复杂的攻击路径的威胁场景。

验证还包括检查 TARA 是否与项目定义一致，即 TARA 确实与所考虑的项目定义有关。

2.2.2 网络安全声明

网络安全声明（见 ISO/SAE 21434:2021，[WP-09-04]）是针对项目外部、关联组件选择共享风险或保留风险定义的。网络安全声明的有效性通过验证或确

认活动来确认，具体取决于网络安全声明内容。以下包含正在验证或确认的对象示例。

1) 基于合理可预见用户行为假设的网络安全声明。

示例：关于信息娱乐系统使用的指定用户行为的隐私敏感信息。

2) 基于项目外部的系统或组件的网络安全声明。

示例：基于车辆中另一个系统、后端、云存储或V2X，此类声明可能涉及对其实施的假设。

注：尽管项目级假设和声明是具体验证的对象，但其他假设，例如在组件级或在脱离上下文的开发过程中做出的假设，可以在验证过程中得到解决。

2.2.3 网络安全目标

网络安全目标（见 ISO/SAE 21434:2021，[WP-09-03]）是针对已识别的威胁场景所定义的。若选择降低风险作为风险处理选项，那么就需要有一个或多个相应的网络安全目标。

需对网络安全目标进行确认，以检查其是否符合以下两点要求：

1) 完整性，即这些目标能够共同应对所有相关的威胁场景；

2) 已实现。

当网络安全目标的依赖关系明确时，应尽早开展网络安全目标的确认工作。

对于依赖于整个项目成果的网络安全目标，确认活动将在项目开发生命周期结束时进行。

网络安全目标和网络安全声明的确认可以同时执行，以确保在开发的早期阶段做出了适当的决策。

网络安全目标的确认可以分步开展，例如：

1) 工作成果的审查：

如果开发是分布式的，那么交付的产品是由不同的组织开发的。因此，交付产品的评审也可以按照网络安全接口协议的规定进行分发。

由于交付产品的审查侧重于技术方面，因此创建工作成果的组织拥有执行相应审查的专有技术。审查结果被合并为车辆级网络安全确认的输入。

2) 渗透测试：

车辆的 E/E（电子电气架构）系统存在攻击面。鉴于整车级确认工作的复杂性，组织可运用零部件级的证据，合理确定整车级确认所涉及的攻击面范围。

示例：若渗透测试能提供确认证据，车辆制造商将向供应商提供攻击面假设、攻击路径等相关信息。

2.2.4 项目级别网络安全概念/要求

验证包括检查指定的网络安全控制是否满足项目级别的网络安全需求。

换句话说，验证包括检查网络安全控制措施是否足够有效地防止或减轻对项目的攻击。

项目中实施的网络安全控制（例如安全启动）在开发后期或生产阶段很难更改。此类网络安全控制措施可优先于其他类型的网络安全控制措施进行验证。

在开发的早期阶段，应对此类网络安全控制进行验证，以确认所选的网络安全控制能够防止攻击，且不会为攻击者提供可乘之机。例如，评估所选网络安全控制是否具备足够的能力来抵御假设的攻击。

这里的策略方法也遵循了概念阶段现有设计的演变：增加新的网络安全控制措施会导致边际分析，进一步确认新的一套网络安全控制手段可以防止攻击，不允许攻击者滥用。这类似于 SAE J2886 DRBFM（Design Review Based on Failure Modes，基于失效模式的设计评审）。

示例[1]：威胁建模（例如 STRIDE、杀伤链、攻击树、故障模式和影响分析、MS meet-in-the-middle 等），创建一个独立的网络安全控制列表（这些控制不来源于网络安全目标：ISO/SAE 21434:2021，[RQ-09-07]）。然后对网络安全概念控制草案进行差距分析，评估其完整性。

示例[2]：研究最先进的攻击项目。然后对网络安全控制草案（概念性，即在项目级别指定）进行差距分析，评估其完整性。即，提供证据来回答问题的分析活动；概念控制是否涵盖了所有最先进的攻击？

示例[3]：对项目设计之前的迭代进行审查，确认网络安全控制草案（概念性，即在项目级别指定）解决了这些迭代中吸取的所有经验教训。

示例[4]：对适用于该项目及其可比/竞争对手的前几次迭代的最普遍的CWEs进行审查，确认网络安全控制草案（概念性，即在项目级别指定）解决了所有最

普遍的CWE。

示例[5]：基于审查的方法可用于验证网络安全概念。例如，可通过将应用于该项目的网络安全控制措施与相关网络安全控制标准目录（即 NIST SP 800-53）进行比较，其中包括对某些类型攻击的控制有效性的考虑。比较结果用作审查的输入依据。

2.2.5 网络安全需求（任何级别的架构细节）

架构设计根据分配的网络安全需求进行验证，因为设计的属性（如后门）可能会引入弱点或漏洞。

ISO/SAE 21434 采用分层方法。然而，并非所有层都重复所有验证活动，而是根据策略方法选择一套适当的方法。

示例：在较低级别的集成中，由于相应子组件（和可利用的交互）的漏洞被认为包含在较高级别的集成测试中，因此在较低级别的集成中不重复进行漏洞测试。

2.3 验证和确认方法

汽车网络安全的验证与确认（V&V）需要采用多种方法组合。方法的选择与组合取决于组织、项目目标、风险等级和具体需求。本条款介绍了一些关键方法，但并非详尽无遗或严格分类。依据确认网络安全的战略方法，未涵盖的方法同样适用。

2.3.1 审查

审查是对工件、文档、流程、样本（或其组合）进行审查，目的是通过审查过程确保存在证据以确认网络安全状态。

安全审查可以是一个过程或会议，旨在让项目人员、经理或其他利益相关方对汽车网络安全相关工作进行检查，从而征求意见或获得批准。在此情境下，“骑车网络安全相关工作”指的是作为开发活动可交付成果而产生的任何技术安全文件或部分安全文件，可能涵盖协议、项目计划和预算、需求文件、规范、设计、概念、源代码、用户文档、支持和维护文档、测试计划、测试规范、标准以及任

何其他类型的安全特定工作产品等文件。

1) 安全设计审查

文档审查旨在评估文件、文档或其他书面材料的内容、准确性、完整性与一致性。文档审查通常由团队成员、专家或相关利益相关者开展，其目的在于确保文档符合预期的标准、要求和规范。

这一项审查的重点在于识别设计缺陷，例如使用不推荐的加密算法，或在错误情况下采用不正确的加密操作模式，或在防范一种攻击时却开启了另一种攻击（如拒绝服务（DoS）攻击）的网络安全控制。

2) 基于检查表的审查

依据列出典型弱点的检查表，对设计是否存在弱点展开调查。此类检查清单可参照例如 ISO/IEC 18045：2021 附录 B 来建立。ISO/IEC 18045：2021 是 IT 信息安全评估方法的一项标准，附录 B 为漏洞评估章节。评估人员利用安全目标的威胁声明中所提供的信息，确定攻击者实施攻击所需的最小攻击潜力，并得出一些有关抵抗攻击的结论。

2.3.2 代码分析审计

代码分析审计是软件开发过程中的关键环节，通过对代码进行系统性的检查与评估，发现其中存在的错误、潜在风险以及不符合规范之处。通过代码审计，可对组件的源代码或二进制文件以及项目中合规义务履行的审计，以识别潜在的安全漏洞和依赖关系，对软件或应用程序中使用的第三方组件（如库、插件、框架等）进行检测和审计，以确保其安全性、稳定性和合规性。

代码审计的常见活动包含安全漏洞检测、代码依赖与供应链分析、安全架构分析与评估、代码接口验证、二进制代码分析。代码分析审计活动应贯穿汽车软件开发生命周期，在需求设计阶段关注架构安全和接口安全，在编码阶段关注实现漏洞和相关依赖库的使用。

安全漏洞检测：利用静态分析工具（SAST）和人工分析，识别缓冲区溢出、SQL注入、跨站脚本（XSS）、命令注入、路径遍历等常见漏洞。

代码依赖与供应链分析：分析项目代码对内部模块和外部第三方库（开源/闭源）的依赖关系，识别存在已知漏洞、许可证风险或过期的组件（使用软件成分分析工具SCA）。

安全架构符合性评估：检查代码实现是否符合既定的安全架构原则（如最小权限、纵深防御、安全隔离）。

接口安全验证：审计代码与外部系统（传感器、总线、通信模块、云端）交互的接口实现，确保输入验证、输出编码、加密、认证和完整性保护的严格实施。

二进制分析：在无法获取源代码时（如对预编译库或逆向工程场景），直接分析二进制文件，评估其结构、行为、引入的潜在漏洞（如编译选项引入的隐患）或进行第三方库的独立安全审计。

2.3.3 功能网络安全测试

汽车功能网络安全测试是一种符合性/一致性测试，用于检查实际实施是否符合网络安全规范中编写和描述的网络安全需求或属性。这类测试侧重于项目或组件中所实施的网络安全控制措施或功能的正确性。

功能网络安全测试的测试依据是基于网络安全需求推导得出的，例如：

1）使用场景，包括要测试的网络安全控制状态和预期行为；

2）网络安全控制的属性或特征，包括重复使用。

功能网络安全测试类型包括正面测试与负面测试：

正面测试(Positive Testing)：验证系统在合法操作和预期输入下的正确响应（如授权访问成功）。

负面测试(Negative Testing)：验证系统对非法操作、意外输入或恶意输入的预期防御行为（如拒绝未授权访问、正确处理畸形输入）。单元测试中的“防御性编码测试”是此类测试的典型例子，关注异常处理、边界值检查。

2.3.4 漏洞扫描

漏洞扫描用于系统性地发现和评估目标系统（软件、配置、网络服务）中已知的安全漏洞、弱点或错误配置，常用于扫描车载信息娱乐系统、T-Box等ECU暴露的网络服务、车载通信协议接口等可能存在的漏洞，快速发现并管理已知风

险。测试环境、测试程序和测试套件取决于假定要控制的漏洞或弱点。例如，测试传输层安全、随机数生成器、私钥管理的已知漏洞。

漏洞扫描程序分为两大类：通常通过网络扫描目标的未经身份验证的扫描程序和从内部审计系统的经过身份验证的扫描仪。

未经身份验证扫描 (Unauthenticated Scanning)：从外部网络视角扫描目标（视为“灰盒”或“黑盒”），典型活动包括：

1) 识别服务版本并与已知漏洞数据库（如CVE）匹配。

2) 收集暴露信息（Banner Grabbing）以发现信息泄露。

3) 运行非破坏性的概念验证（PoC）探测以确认漏洞存在。

经过身份验证扫描 (Authenticated Scanning)：在获得目标设备本地访问权限或有效网络凭据后执行，能进行更深入的内部审计：

1) 全面检查系统配置、补丁级别、用户权限、安全策略设置。

2) 识别仅内部可见的漏洞和弱点。

3) 专注于配置审计的也称为审计扫描 (Audit Scanning)。

2.3.5 模糊测试

模糊测试是一种自动化的测试技术，通过向目标系统注入非预期数据并监控崩溃、内存溢出等异常行为，以智能变异策略（如语法感知、反馈驱动）系统性地发现潜在安全漏洞，广泛应用于汽车 ECU 等安全关键系统、高风险组件及ISO 26262:2018《道路车辆—功能安全》ASIL-D级合规性测试。在车辆安全测试场景中，模糊测试在“云-管-端”三个威胁面的风险发现中均能有效的运用。

根据测试对象的可见性和可控性来划分，模糊测试分为黑盒模糊测试、白盒模糊测试、灰盒模糊测试：

黑盒模糊测试是在不了解测试对象内部结构和实现的情况下执行。只能观察到程序响应（如果有的话），例如崩溃或出现异常行为。

白盒模糊测试是一种具有可用源代码的轻量级程序分析。这也允许测试中的软件和可执行文件具有完全的可观察性，尤其是内部状态。通常结合静态代码分析和动态路径分析。

灰盒模糊测试是黑盒和白盒模糊测试的结合。灰盒模糊方法通常对被测软件

执行轻量级检测。如果对目标软件内部结构和实现有一定的了解但有限，灰盒模糊测试是更高效的选择。

根据测试对象的类型来划分，模糊测试可分为源代码模糊和协议模糊：

源代码模糊测试侧重于检测程序内部的错误，其中程序的状态是次要的。代码覆盖率是衡量进度的一个很好的指标。

协议模糊测试均为黑盒测试，侧重于程序的通信，其中消息被延迟、拦截、重放、随机化、伪造等。模糊器可以在测试期间充当MitM（中间人攻击）。在这里，OWASP（即Open Web Application Security Project，开放网络应用安全项目）使用术语“递归模糊测试”和“替换模糊测试”。

2.3.6 渗透测试

渗透测试是从攻击者的角度进行的一种安全评估，测试人员使用可用信息和工具利用项或组件中的漏洞进行攻击。如果攻击路径已经被识别，采用专用测试方法，则不需要进行渗透测试，如果要探索新的威胁场景，该方法是有益的。渗透测试的有效性取决于时间长短和攻击人员的能力，在进行渗透测试之前，必须确定测试范围并定义攻击者模型。该模型说明了测试中可以假设的攻击者能力。然后，渗透测试将镜像这些功能，以确保攻击场景的真实。

渗透测试分为白盒、灰盒和黑盒测试：

在黑盒测试中，渗透测试人员不会获得任何有关系统的额外信息。

白盒测试会把系统的所有内部信息和源代码都提供给渗透测试人员。白盒测试的思想和优点是加速测试并更深入地评估系统的安全性。如果白盒渗透未识别到任何安全问题，那么以后在现实中就更不可能被没有这类信息的攻击者攻破。

灰盒测试是一种只有部分系统信息可供测试人员使用的渗透测试。顾名思义，灰盒测试介于白盒测试和黑盒测试之间。

渗透测试人员可以在测试范围内通过任意方式来攻击测试对象，这意味着渗透测试可能也包括本报告其他章节中描述的多种工具和方法。例如，渗透测试人员可能会使用模糊器来识别可利用的服务，并使用逆向工程来了解特定服务的逻辑，然后再研究针对该服务的漏洞。尽管与本文中描述的其他安全测试方法有一些重叠，但渗透测试人员会根据需要将这些测试方法与创造性思维结合起来，以

攻击测试对象。与漏洞扫描等方法不同，渗透测试的一个关键目标是证明测试过程中发现的漏洞的可利用性。

一些典型的渗透测试活动如下：

1）服务扫描

服务扫描发现并列出目标网络或总线接口或协议的所有服务。根据网络技术的不同，服务扫描可能不仅仅是扫描某个协议内的可用服务，而是实际扫描网络上各种协议的存在。一个常见的例子是扫描 CAN 总线上 XCP 的存在。

2）DoS 攻击

DoS测试是一种使用大量请求来耗尽系统资源的方法。这些系统资源可以包括：网络带宽、CPU利用率、内存利用率、任何其他类型的系统资源，例如定时器控制块、TCP套接字、TLS连接、到 MySQL 服务器的连接等。

通常，DoS测试是针对网络接口执行的。从测试对象的角度来看，可以对不同类型的DoS攻击进行分类：

(1) 基于网络的攻击：使用到测试对象的大量流量来拥塞测试对象的网络带宽。通常，这些攻击使用无状态网络协议，如IP、ICMP或UDP。在现实世界中，这种大规模攻击是通过使用分布式拒绝服务来执行的，其中来自僵尸网络的多个主机被滥用来产生负载。从测试对象的角度来看，有两个方面需要处理：一方面，DoS测试对象的资源消耗为目标，使测试对象处于过载状态，无法处理新的合法请求或来自现有合法连接的请求。另一方面，网络将开始丢弃数据包，因此合法流量将受到影响，可能导致连接停滞。

(2) 基于协议的攻击：在这里，负载是以一种特定的方式精心制作的，目的是利用测试对象中的实现缺陷。例如，TCP-SYN flood 向目标发送TCP SYN请求，而不通过TCP-ACK确认TCP握手。易受攻击的目标将分配资源，由于没有收到响应，在保护计时器到期之前，这些资源将无法用于合法请求。攻击者发送的TCP SYN太多，以至于所有资源都已耗尽，因此测试对象将无法接受合法请求。缓解这种攻击的一种常见方法是使用TCP SYN cookie。

(3) 基于应用程序的攻击：针对网络协议之上的应用程序和协议。这里并不

总是需要发送大量的数据包。例如，Slowloris攻击通过保持与目标web服务器的许多连接处于打开状态并尽可能长时间地保持打开状态，缓慢但稳定地消耗web服务器资源。

3）压力测试

压力测试是测试超出设计负载时的表现，确定其最大处理能力（如并发用户数、数据吞吐量等），目的是为了发现高负载或资源不足（如CPU、内存、网络带宽耗尽）时可能触发的崩溃、数据丢失或性能骤降等问题，提前发现系统在极端场景下的薄弱环节，避免生产环境中的重大故障。

压力测试会使用大量请求来耗尽系统资源，这些系统资源可以是：

(1) 网络带宽

(2) CPU利用率

(3) 内存利用率

(4) 任何其他类型的系统资源，例如定时器控制块、TCP套接字、TLS连接、MySQL服务器连接压力测试实现与DoS攻击一致，包括针对网络、协议以及应用程序。

3 网络安全验证和确认活动质量评估方法

3.1 TARA活动质量评估方法

1）应对网络安全相关项的相关性判定方法、定义要求的流程，以及开展相应活动的记录进行质量评估。

（1）应明确信息安全相关性判定方法，信息安全相关性判定应至少考虑到影响车辆操作安全、收集或处理用户隐私数据、车内外通信接口及数据安全的相关要求。

（2）企业风险评估中的相关项分析应覆盖全部影响车辆操作安全的功能/组件，且涉及到这些功能/组件的风险评估表单间无前后矛盾。

（3）企业风险评估中的相关项分析应覆盖全部收集或处理用户隐私数据的功能/组件，且涉及到这些功能/组件的风险评估表单间无前后矛盾。

（4）企业风险评估中的相关项分析应覆盖全部车内外通信接口的功能/组件，且涉及到这些功能/组件的风险评估表单间无前后矛盾。

（5）企业风险评估中的相关项分析应覆盖全部涉及数据安全的功能/组件，且涉及到这些功能/组件的风险评估表单间无前后矛盾。

（6）车辆制造商应提供信息安全相关性判定的记录或结果示例。

（7）应对相关项定义进行明确。相关项的定义通常包括：

a.相关项编号及名称

b.相关项可实现的车辆功能描述

c.相关项架构图

d.相关项边界描述

e.相关项数据流图及描述

f.相关项的运行环境

g.安全假设与约束条件

（8）车辆制造商应提供相关性定义的记录或结果示例。

（9）企业的风险评估活动应覆盖车辆产品的所有功能组。

2）应对TARA方法论、分析过程中使用的运行表单，以及开展相应活动的记录进行质量评估。

（1）TARA方法论中应明确资产识别流程，应要求资产清单充分覆盖整车功能清单中的内容。

（2）资产识别流程中应识别其信息安全属性，信息安全属性至少包括可用性、完整性、机密性。

（3）资产识别流程中应对资产详细分类，以便更准确地评估其价值和潜在风险。

（4）资产识别流程中应对已识别的资产，汇总形成资产清单，包括资产编号、资产名称、资产描述、资产的功能或用途。

（5）资产识别流程中应描述资产因信息安全属性被破坏后导致的损害场景。损害场景的描述应至少包括相关项的功能和不利后果之间的关系、对道路使用者是否会造成伤害的描述、涉及的相关资产。

（6）应明确损害场景的影响等级判定流程。

（7）TARA方法论中应明确威胁场景识别流程。

（8）威胁场景识别流程中应识别并描述威胁场景，威胁场景的描述应包括目标资产、资产受损的信息安全属性、信息安全属性受损的原因。

（9）企业风险评估中的威胁场景应覆盖全部资产的全部安全属性。

（10）TARA方法论中应明确攻击路径分析流程。

（11）应要求攻击路径应与该攻击路径可以实现的威胁场景相关联，攻击路径应覆盖全部威胁场景。

（12）TARA方法论中应明确攻击可行性评级流程。应要求攻击可行性评级可采取攻击潜力的方法、基于CVSS的方法或其它已评估有效的方法进行。

（13）TARA方法论中应明确信息安全风险值确定流程。应要求对于每个威胁场景，应根据相关损害场景的影响和相关攻击路径的攻击可行性来确定风险值。

（14）风险处置决策流程中应明确风险处置策略，应与体系文件规定一致，风险处置策略一般包括规避风险、降低风险、分担风险、接受风险，且（参考功能安全D等级或对人身安全、隐私安全相关的）最高等级的风险值不应选择接受风险。对于不可接受的风险，应制定具体的缓解措施或降低风险的策略。

（15）TARA方法论中应明确风险处置决策流程。

（16）车辆制造商应能提供车辆信息安全TARA分析过程中使用的工具表运行及结果示例，证明按照体系流程要求对车型项目的信息安全风险进行了识别、评估、分类、处置，且包含功能概述、资产列表和资产信息安全属性、威胁场景、损害场景和影响评分、攻击路径和攻击可行性评分、信息安全风险等级、信息安全风险处置策略等内容。

3.2 网络安全概念活动质量评估方法

1）应对网络安全目标和网络安全声明的制定和评审流程，以及开展相应活动的记录进行质量评估。

（1）如果选择风险保留和风险转移的处置，应制定网络安全声明。

（2）如果选择风险降低的处置，应制定网络安全目标。

（3）对网络安全目标和网络安全声明进行评审。

（4）应提供网络安全目标和网络安全声明的评审记录。

2）应对网络安全需求的制定和评审流程，以及开展相应活动的记录进行质量评估。

（1）应为实现网络安全目标制定网络安全需求，网络安全需求应覆盖全部网络安全目标。

（2）网络安全需求应下沉到可执行的颗粒度，所有的网络安全需求应有明确的验证方式。

（3）应为每个网络安全需求明确验收标准。

（4）应验证安全需求与相关风险的充分关联，要求需求与风险之间具有可追溯性。

（5）应将网络安全需求分配给所有网络安全相关组件，确保所有网络安全相关的资产均被网络安全需求覆盖。

（6）需要明确网络安全需求适用的全生命周期的阶段，包括设计、生产、售后及运维阶段。

（7）应在落实网络安全需求后对残余风险进行评估，判断残余风险是否达到可接受水平。

（8）应明确验证生产阶段网络安全需求成功落实的方法，制定明确的验证和测试方法，以确认网络安全需求在生产阶段得到了有效实施。(调试接口在生产阶段关闭，或在量产阶段通过版本控制、调试接口强访问控制等方式、在整机产线密钥灌装等等）

3.3 V&V活动质量评估方法

3.3.1 审查活动质量评估方法

3.3.1.1审查对象评估

1）评估集成验证审查所依据的文件、规范和要求的准确性和适用性。核查是否与系统的设计和要求相符，以确保审查的准确性。

2）检查网络安全需求是否与审查活动匹配。

3）检查设计方案是否实现并有相关佐证材料。

4）设计方案是否有签署审批记录保证文档的正确性。

5）安全需求方案更新升版时，审查对象还应包括设计方案版本对应的审批记录。

6）审查对象覆盖了关键的安全领域，例如网络拓扑、访问控制、身份认证等。

3.3.1.2审查过程有效性评估

1) 审查人员应具有一定的资质，参与者应是团队成员、专家或利益相关者。

2) 审查的形式可以为会议、邮件、文档签批，均需有相关记录留存。

3) 审查过程是否有相关方进行评审，并形成记录。

4) 检查审查过程中使用的方法、技术和工具是否能够满足审查需求。

3.3.1.3审查报告评估

1) 审查结果应有形成记录进行保存。

2) 检查审查报告中对系统安全问题的描述和分析是否清晰明确，评估结果是否全面，并提供了合理的改进建议和优化措施。

3.3.2 代码分析审计质量评估方法

3.3.2.1代码分析审计流程评估

1) 代码分析审计中使用的静态分析工具，应是业界成熟并且被广泛接受的工具。该扫描工具应支持对代码编程语言的检测，并且评估工具能否满足项目需求。

2) 代码分析审计人员必须具有代码分析的能力及相关工作经验。

3) 应制定详细的测试计划，包括测试目标、测试范围、测试方法、测试时间表等，测试目标应明确，如验证功能正确性、性能稳定性、安全性等，测试范围应覆盖所有关键功能和模块，确保全面测试。

4) 测试用例应定期更新和维护，确保与需求和代码的变化保持同步。

3.3.2.1代码分析审计报告评估

1) 报告应包含测试对象、测试范围、测试执行者标识、报告版本、测试时间、测试的功能点、测试结果及修复意见等。

2) 报告应包括代码分析的统计以及代码分析存在问题的函数以及地址，并且需要详述具体产生的方法以及修复方案，应详细给出问题存在的位置、具体表现和复现步骤，确保问题的可追踪性和可修复性。

3) 报告应对检查出的问题严重性进行分类，例如致命错误、严重错误、警告等。

4) 应对测试报告进行评审，并形成评审记录，确保报告的准确性和完整性。

3.3.2.1代码分析审计有效性评估

1) 代码分析的代码应覆盖项目涉及到的所有源码，覆盖度达100%。

2) 应定期评估测试工具的性能和功能，确保其满足项目需求。

3) 应通过比较测试工具检测到的问题和实际存在的问题来评估其检出率，检出率应达到85%以上，确保大部分问题能够被及时发现和解决。

4) 测试人员应具备相关经验和技能，或经过必要的专业培训，可查看证明材料，确保测试的专业性和准确性。

5) 应考虑测试工具错误地将正常行为标记为问题的情况，降低误报率。

6) 应考虑测试工具未能检测到实际存在的问题，避免真正的问题被忽视。

7) 确保测试活动的独立性，避免利益相关者的干扰，确保测试的客观性和公正性，测试人员应独立于开发人员，确保测试的客观性和公正性。

3.3.3 功能网络安全测试质量评估方法

功能网络安全测试是基于安全需求规格说明书中定义的安全需求，对相关网络安全功能在车辆各个层级（如整车、系统、模块和子模块等）的实现进行验证的测试活动。对于具体的安全需求，功能网络安全测试可有针对性的设计和执行测试用例，验证安全产品的质量；对于较抽象的安全需求，功能网络安全测试需考虑组合测试、随机测试、边界值/特殊值、等价类划分等测试方法，对产品质量进行评估。

3.3.3.1 功能网络安全测试流程

1) 功能网络安全测试活动应至少包含信息收集、测试方案编写、测试执行、

测试结果确认、测试报告输出五部分。

2) 功能网络安全测试应制定详细的测试方案、测试用例。

3) 测试方案中至少应明确测试对象、测试范围、测试环境及测试设备、测试输入、测试人员及资质、测试计划、测试通过准则、测试交付物。

4) 测试方案中对测试需求的覆盖率需达100%覆盖。

5) 测试用例中至少包括：用例编号、需求编号、用例描述、测试对象、测试方法、预置条件、测试步骤、预期结果。

6) 功能网络安全测试应按照测试方案执行，当测试执行与测试方案有偏离时，应进行测试方案变更并记录变更情况。

7) 功能网络安全测试流程中的输出物（如测试方案、测试用例及测试报告）必须有生成时间、责任人、版本变更的记录，且需经过评审，并输出评审记录。

8) 当涉及到功能需求变更时，必须有对应的文件输入，根据实际情况更新测试方案、测试用例、测试报告等输出物，并记录变更内容。

3.3.3.2 功能网络安全测试报告

1) 功能网络安全测试报告中的内容都应是无错误和无歧义的表达，且表述的信息应是描述清晰且现有技术可以验证的，例如，每一个调试功能接口都应该有明确的连接引脚或访问方式，调试接口划分，具体调试接口用途信息等。

2) 功能网络安全测试报告中的测试步骤应严格按照测试方案与测试用例来执行，不应存在测试报告中的执行方式与审批完成的测试方案和测试用例不一致的情况。

3) 功能网络安全测试报告应至少包含测试编号、测试样品的信息描述（例如版本等信息）、测试方法描述、测试步骤及测试详情描述（必要时需有图片进行佐证）、实际测试结果、所使用的工具及其相关版本描述、测试活动时间描述、测试人员、测试输入以及测试过程中测试样品的状态描述（例如由于测试结果导致其样品状态变更，以致于影响后续测试活动）及报告版本、报告作者和审查者的信息。

4) 功能网络安全测试报告应体现对需求不通过项的一次或多次回归测试过程，并体现最终需求验证通过的测试过程。

5) 功能检测报告应有测试结果汇总的数据，且不能出现测试详情部分的数据与汇总数据不一致的情况。

6) 评估测试报告，并将其与预期结果进行比较。确保问题项被记录追踪，且缺陷的严重性和优先级被正确评估。

7) 功能网络安全测试报告应明确其对于测试结果判定的依据，并体现其根据判定依据对测试结果进行判定的过程。测试结果与预期结果一致时，判定测试结果为“通过”；测试结果与预期结果不一致时，判定测试结果为“失败”，且应通过被测功能失效的影响范围、严重性、发生频率、修复难度等指标，对问题进行定级。

8) 功能网络安全测试活动成果物应能体现测试过程管理，例如跟踪测试过程中发现的问题项，从识别问题、分析问题和定位根因，到最后关闭问题的完整过程。

9) 功能网络安全测试报告应由团队专家或管理层完成审批确认。

3.3.3.3 功能网络安全测试有效性评估

1) 功能网络安全测试实施人员应具备相关经验，或经过必要的专业培训。

2) 功能网络安全测试开展前应对测试工具的运行安全、版本、组成以及来源渠道进行核查并记录，确保测试活动所用工具的有效性。并在测试结果或测试报告中明确标注测试所使用相关工具的版本情况。

3) 功能网络安全测试应随着测试活动的进行，对样品进行检查。

4) 确保样品当前测试版本符合功能设计需求的最新开发版本，避免出现功能未开发，功能状态异常导致测试结果不通过。

5) 确保样品状态可用于继续执行测试活动，保证不会由于前序测试活动的破坏，影响对后序测试活动结果的客观判定。

6) 功能网络安全测试应保证结果在当前环境或者其他相同配置环境，采用相同的测试方法能够实现漏洞或测试结果的稳定复现（对于概率性的失效问题，应能够基于此概率复现）。

7) 功能网络安全测试环境应稳定可用，若涉及到无线通信、网络环境等对测试环境要求的测试活动时，应保证测试环境不受干扰并能够支持测试。

8) 功能网络安全测试实际所使用的工具应与测试报告中的工具清单列表保持一致。

9) 在功能网络安全测试准备阶段，测试相关的环境配置项及测试工具应与测试方案中的定义一致。

10) 对于具体的功能需求，应确保对应测试用例的可执行性和充分性（即可用于验证被测的功能需求）。对于抽象的功能需求，应设计测试策略、方法和用例确保需求被充分验证、以及提供相关测试充分度（覆盖度）的评价指标和结果。

11) 功能网络安全测试应覆盖既定网络安全目标或需求，并在审查方案与计划中明确其与测试项的映射关系。

3.3.4 漏洞扫描质量评估方法

3.3.4.1漏洞扫描实现方式评估

1) 评估漏洞扫描团队成员的资质和经验，包括人员的技能水平和安全意识，以确保测试的有效性和可靠性；同时漏洞扫描活动应保证参与团队及人员的独立性，不应为漏洞扫描对象的利益相关者。

2) 漏洞扫描应制定详细的扫描方案，方案中应至少包括扫描计划、扫描范围（待扫描的项目）、扫描类别（二进制和/或源码）、预期结果、扫描工具（软件成分分析工具与威胁情报查询工具）、扫描结果准确性审核等内容，当扫描执行与扫描方案有偏离时，应进行扫描方案变更并记录变更情况。

3) 漏洞扫描活动应至少包含待扫描项目源代码收集、待扫描项目产品二进制编译、确定软件成分分析工具、确定威胁情报来源、扫描执行、扫描结果确认和扫描报告七部分。

3.3.4.2漏洞扫描对象评估

1) 漏洞扫描的对象应为正式发行环境，不应使用测试环境，以避免对检查结果产生分歧。

2) 定期对新的软件版本执行漏洞扫描，确保软件代码中上报过国家漏洞平台的漏洞都已经得到修复。

3) 漏洞扫描器应与被扫描对象可正常通信。

3.3.4.3漏洞扫描工具评估

1) 漏洞扫描工具的选择应根据扫描对象不同而有所差异。例如，针对系统进行漏洞扫描时，应选择系统漏洞扫描器；针对云平台进行漏洞扫描时，应使用网页漏洞扫描器。

2) 企业应具备对漏洞扫描工具进行评估的过程。

3) 漏洞扫描开展前应对扫描工具的运行安全、版本、组成以及来源渠道进行核查并记录，确保漏洞扫描活动所用工具的有效性。

漏洞扫描器的漏洞库应全面，且漏洞扫描器的漏洞库应按照企业与工具开发商的约定持续更新。

3.3.4.4 漏洞扫描报告评估

1) 漏洞扫描报告应包含检查对象、检查范围、检查执行者标识、检查时间、检查漏洞类型（SLO超期漏洞除外）、检查结果及修复意见。

2) 漏洞扫描报告中的风险点应给出详细的攻击路径。

3) 漏洞扫描报告应对检查出的风险进行定级，至少包含高危、中危、低危或相对应的等级。

4) 漏洞扫描报告应给出具体的漏洞验证方法和提供漏洞的修复方案，或者指明参考资料。

5) 漏洞扫描报告中应有测试结果汇总的数据，且不能出现测试详情部分的数据与汇总数据不一致的情况。

3.3.5 模糊测试质量评估方法

3.3.5.1模糊测试流程评估

1) 模糊测试流程，至少应该包含模糊测试测试范围，测试方案，测试结果确认和测试报告。

2) 模糊测试方案应包括测试计划、测试用例（评估模糊测试用例的设计质量，包括用例的多样性、复杂性和覆盖率、输入数据的生成方式等）、模糊测试工具选择、模糊测试运行时间。

3) 模糊测试应按照测试方案进行，当测试执行与测试方案有偏离时，应进

行测试方案变更并记录变更情况。

3.3.5.2模糊测试报告评估

1) 报告内容方面：应详细记录测试过程、使用的测试工具及其版本、测试数据和发现的问题，报告中描述的内容应该是准确无误且无歧义。

2) 模糊测试报告应至少包含对测试目标的信息描述（例如版本等信息，以及测试过程中测试目标的状态描述（例如测试目标状态变更）。

3) 漏洞可复现性方面：报告应包含测试环境的详细描述，例如软硬件配置、系统版本、测试时间等信息。对于发现的每一个问题，报告应清晰记录当前漏洞的攻击向量数据确保此漏洞可复现。

4) 漏洞生命周期方面：模糊测试报告应体现对漏洞的一次或多次回归测试过程，并体现最终漏洞关闭的测试过程。

5) 模糊测试报告应明确其对于模糊测试结果的判定依据（例如CVSS通用漏洞评分标准或其他依据）。

3.3.5.3 模糊测试有效性评估

1) 评估模糊测试团队成员的资质和经验，包括测试人员的技能水平和安全意识，以确保测试的有效性和可靠性。模糊测试活动应保证参与团队及人员的独立性，不应为模糊测试目标的利益相关者。

2) 模糊测试对象应包括协议栈/软件/系统组件/操作系统，以确保测试数据能够覆盖到所有可能的交互场景（OBD口、WiFi、BT、标准协议接口、文件FUZZ、网络API接口、重要通信协议、重要数据接口、源代码）。

3) 模糊测试使用的工具应为业界主流或被业界广泛认可的模糊测试工具，并对测试工具的版本、组成以及来源渠道进行核查并记录。

4) 模糊测试结果应保证模糊测试任务配置的参数均全部正确，并保证测试环境的稳定性，被测对象在测试过程中正常运行，确保数据包可准确的送达，并保证测试效率。

5) 模糊测试数据集应足够大，执行周期至少满足于测试基本要求的时间。

6) 模糊测试应覆盖既定网络安全目标或需求，并在审查方案与计划中明确其与测试项的映射关系。

3.3.6 渗透测试质量评估方法

3.3.6.1 渗透测试流程评估

1) 渗透测试活动应至少包含信息收集、确定渗透测试范围、方案制定、测试执行、测试结果确认和测试报告六部分。

2) 渗透测试应制定详细的测试方案，方案中应至少包括测试计划、测试用例制定、预期结果、测试工具等内容。

3) 渗透测试应按照测试方案执行，当测试执行与测试方案有偏离时，应进行测试方案变更并记录变更情况。

4) 测试方案、测试用例、测试报告需经过至少一轮评审，并有评审记录。

3.3.6.2 渗透测试报告评估

1) 渗透测试报告中的内容都应是无错误和无歧义的表达，且表述的信息应是描述清晰且现有技术可以验证的，例如，每个漏洞都应描述清楚发现漏洞时的操作步骤、输入信息、具体漏洞信息等。

2) 测试报告结果应证实已按测试计划执行了全部的渗透测试方案，不应存在测试报告内容与测试方案内容不一致等情况。

3) 渗透测试报告应至少包含对测试样品的信息描述（例如版本等信息）、测试方法描述、所使用的工具及其相关版本描述、测试活动时间描述、以及测试过程中测试样品的状态描述（例如由于测试结果导致其样品状态变更，以致于影响后续测试活动）及报告作者和审查者的信息。

4) 渗透测试报告应明确其对于渗透测试结果判定的依据（例如CVSS通用漏洞评分标准或其他依据），并体现其根据判定依据对测试结果进行判定的过程。

5) 渗透测试活动成果物应能体现渗透测试活动过程中测试发现的问题项，并能体现持续跟踪该问题直至关闭的过程。

3.3.6.3 渗透测试有效性评估

1) 渗透测试实施人员应具备至少两年的相关经验，或经过必要的专业培训。

2) 渗透测试活动应保证团队成员的独立性，不应为渗透测试对象的开发成员或其他利益相关者，以确保测试结果客观、公正、可信。

3) 渗透测试开展前应对测试工具的运行安全、版本、组成以及来源渠道进行核查并记录，确保渗透测试活动所用工具的有效性。涉及到数据库、版本库、特征库、漏洞库等测试工具，应保证所用库为最新版本，并在渗透测试结果或渗透测试报告中明确标注测试所使用相关工具库的版本情况。

4) 渗透测试应随着测试活动的进行，对样品进行检查，确保其状态可用于继续执行测试活动，保证不会由于前序渗透测试活动的破坏，影响对后序测试活动结果的客观判定。

5) 渗透测试应保证结果的可复现性，采用相同的测试方法能够实现漏洞或测试结果可复现。

6) 渗透测试环境应稳定可用，若涉及到无线通信、网络环境等对测试环境要求的测试活动时，应保证测试环境不受干扰并能够支持测试。

4 网络安全验证和确认标准化建议

4.1 标准化必要性

自2023年6月《道路车辆 网络安全验证和确认》标准化需求研究项目组成立以来，已在苏州、厦门等地举办七次线下会议，项目组由上海汽车集团股份有限公司创新研究开发院牵头，参与单位近三十家，覆盖国内外OEM、零部件供应商和各检测机构，对道路车辆的验证和确认方法及其质量评估进行了细致且详尽的研究，并形成了本研究报告。

报告第一章详细介绍了网络安全验证和确认的背景以及其重要性，同时对国内外现行和在研标准，以及行业现状展开了深入分析。此外，还对国内车企在网络安全验证和确认方面的实施情况进行了调研，为后续研究奠定了坚实基础。

第二章着重阐述了网络安全验证和确认的概念、适用范围以及具体方法。工作组在借鉴国外优秀案例的基础上，结合国内企业的实际情况，探讨了审查、代码分析、功能网络安全测试、漏洞扫描、模糊测试、渗透测试等多种验证和确认手段，为车企提供了一套完备的网络安全验证和确认方法论。

第三章围绕网络安全验证和确认各阶段的活动与方法，开展了质量评估研究。

旨在提升相关活动的质量，进而更好地指导企业实践，推动行业整体水平的提升。

项目组在研究过程中同样发现，各车企在开展网络安全验证与确认工作时面临着诸多挑战。其一，部分车企合规经验匮乏，缺少具有可操作性的标准化方法来指导相关活动。其二，不同车企所采用的验证和确认方法存在差异，并且缺乏统一的质量评估标准。 为此，项目组建议对网络安全验证和确认的方法论及其质量评估的内容进行标准化，通过对该部分内容的标准化，有助于：

1) 填补行业空白，助力企业合规落地。当前，国内部分OEM已具备UN R155车型认证经验，对网络安全验证与确认流程颇为熟悉。然而，仍有许多企业尚未开展UN R155车型认证，其网络安全验证与确认工作仍停留在理论层面，缺乏可指导操作落地的标准化方法，难以保障验证工作的完整性与有效性，可能直接影响GB 44495—2024《汽车整车信息安全技术要求》的实施执行。因此，建立一套统一的标准体系，对指导企业高质量开展网络安全验证与确认工作至关重要。

2) 规范车辆网络安全验证和确认方法，提升行业整体质量。国家强制性标准GB 44495—2024 《汽车整车信息安全技术要求》已正式发布，并将于2026年1月1日起在新车型上实施。目前，国内车企在开展车辆网络安全验证和确认时所采用的方法各异，实施深度不一，导致验证和确认活动的质量参差不齐，不利于行业的整体安全水平提升。本项目重点研究的质量评估方法可针对验证和确认的各个环节进行质量评估，从而解决行业在进行验证和确认时质量不均衡的问题。通过进一步标准化研究成果，可明确网络安全验证和确认的具体方法和要求，确保相关活动的规范性与一致性，推动行业高质量发展。

3) 对标国际标准，完善国内网络安全验证和确认体系。国际上，ISO/SAE 8477在ISO/SAE 21434《道路车辆 网络安全工程》的框架下，对道路车辆的网络安全验证和确认进行了详细的技术性定义和要求。为更好地适应国内市场需求，本研究成果的标准化可对GB 44495—2024 《汽车整车信息安全技术要求》中验证和确认活动的具体实现细节进行补充和细化。一方面，标准化可为企业提供更具针对性的技术指导，提升网络安全验证和确认工作的可操作性和有效性；另一方面，也能助力中国在国际标准制定过程中贡献自主方案，增强中国汽车产业在全球网络安全标准体系中的影响力。

4.2 建议的标准框架

经项目组成员单位多次研讨并参考汽车信息安全工作组内反馈的意见，建议将本研究报告的第二章“网络安全验证和确认”、第三章“网络安全验证和确认活动质量评估方法”进行标准化，主要包含网络安全验证和确认的概念、网络安全验证和确认的范围和方法，以及对相关活动进行质量评估的方法。

考虑到该部分内容庞杂，若将所有内容体现在单一标准里，会导致标准篇幅过长，增加对标准的理解和执行难度。且由于涉及不同类型的内容，如第二章为方法论、第三章为质量评估等，单一标准的结构不利于使用者高效地查找和应用相关信息。系列标准的结构能很好的解决以上问题，采用系列标准可以确保标准的内容层次清晰，第一部分作为通用基础，定义适用范围、术语和基本原则，各后续部分围绕具体方法展开，形成由总到分、层层递进的逻辑体系，全面覆盖验证和确认活动的方法论以及对应方法的质量评估规范。建议的标准框架如下：