NTCAS 汽标委

汽车信息安全仿真测试标准领航研究报告

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

汽车信息安全仿真测试标准领航研究由中国汽车技术研究中心有限公司牵头，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。本项目立足智能网联汽车的网络安全需求，以仿真测试场景分类为基础，以安全仿真攻击构建方法为核心突破点，旨在构建一套汽车全生命周期的仿真测试标准体系，解决行业痛点问题。

传统的网络安全测试主要有三大痛点，一是依赖实车，测试成本高；二是风险大，网络攻击一旦生效可能导致车辆 ECU 永久性损坏，若此时车辆处于行驶状态则会酿成重大安全事故，三是受限于物理环境，某些网络攻击的执行依赖于车上的电子电气架构。本项目创新性地引入了汽车信息安全仿真测试方法，通过模拟总线协议、无线协议及 V2X 环境等，可以实现“低成本、低风险”的高效测试，且能覆盖传统方法难以复现的极端和复杂攻击场景。本项目通过仿真场景构建、测试对象分层选择、安全要素分析，建立了合规性、功能性等维度的安全评估方法。基于 ATT&CK 模型，完成框架适配、攻击路径建模与组合，并落地为信息收集、路径模拟、测试优化及自动化集成的全流程方案。面向整车和零部件层级，形成了虚拟化仿真的可靠性、准确性等六项指标以及仿真攻击的攻击覆盖率等四项指标的量化评估方法，革新了汽车信息安全研究模式。

衷心感谢参与研究报告编写的各单位和组织：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、安徽江淮汽车集团股份有限公司、比亚迪汽车工业有限公司、泛亚汽车技术中心有限公司、深圳引望智能技术有限公司、腾讯云计算（北京）有限责任公司、重庆长安汽车股份有限公司、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）、北京天融信网络安全技术有限公司、中国汽车工程研究院股份有限公司、北京航迹科技有限公司、上海汽车集团股份有限公司乘用车分公司、东风商用车有限公司、广州小鹏汽车科技有限公司、鹏城实验室、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、国家工业信息安全发展研究中心、中机博也（宁波）汽车技术有限公司、长城汽车股份有限公司、北京信长城科技发展有限公司、北京赛目科技

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：赵雄、方熙宇、刘雪淼、吴犇寅、李雨冉、束照坤、纪梦雪、马鑫、孟雪、方锦祥、肖湘楠、潘凯、张文凯、巩星辰、冯河清、王璐、何强、何凯、朱科屹、张慧妍、范雪俭、胡雨翠、贺鹏、戚琪、王彦伟、王艳华、尹相晨、高岩、杨晶、贾世准、张添、张翔新、张金池、刘阳、杨智博、郭振、任世轩、张小东、刘鹏、刘祎、雷宇的、郑奕文、柯正锐。

目　录

1. 汽车网络安全仿真测试研究背景

1.1. 汽车网络安全仿真测试的意义和目的

1.1.1. 汽车网络安全背景

为顺应新一轮科技革命和产品变革趋势,把握智能汽车的创新发展机遇，国家发改委、中央网信办、科技部、工信部等 11 个部委联合印发了《智能汽车创新发展战略》,该文件提出了 2025 年时间节点的战略愿景，明确指出“到 2025 年，中国标准智能汽车的技术创新、产业生态、基础设施、法规标准、产品监管和网络安全体系全面形成，并将构建协同开放的智能汽车技术创新体系作为发展的主要任务，其中包括完善测试评价技术，重点研发虚拟仿真、软硬件结合仿真、实车道路测试等技术和验证工具等内容”。

另一方面，现行汽车、交通管理法规以人为主体，作为以自动驾驶系统为驾驶主体的智能汽车，其诸多创新设计导致了现行的法律法规与智能汽车应用存在诸多不适用性，相关的技术标准尚存在诸多空白，跨行业标准协同不足等问题日益显著。因此，汽车网络安全仿真测试的研究不仅完善了汽车网络安全体系，也填补了跨行业标准协同的空白。

伴随着汽车智能化、网联化的融合发展，汽车已经从单纯的交通工具转变为智能化移动终端设备，车辆运行安全、网络安全和数据安全风险交织，使得安全形势日趋复杂。近年来，汽车网络安全事件呈逐年上升趋势，技术漏洞、安全意识缺失已经成为黑客组织对车辆发起恶意攻击的主要原因，暴露出车辆被盗、勒索赎金、数据泄露、行驶车辆失控等严重问题。

为有效应对汽车领域不断涌现、快速演化的新型攻击手段，降低车辆运行安全、网络安全和数据安全风险，解决由此带来的数据泄露、行车安全等问题，急需提出一套高效可行的网络安全测试方案。汽车网络安全仿真测试方案，具有低成本、高效率的特点，技术上互联性强、集成度高，与汽车发展相适应。因此，相关研究的开展具有重要意义，仿真测试方法有助于汽车提高汽车网络安全测试效率。

而智能汽车作为一个集环境感知、规划决策、多等级辅助驾驶等功能于一体的综合系统，它集中运用了计算机、现代传感、信息融合、通讯、人工智能及自动控制等技术。其面临的网络安全方面的威胁也是复杂多样。仿真测试能够模拟出真实或潜在的攻击场景，揭示网络安全系统中的潜在问题和安全漏洞。因此，汽车网络安全仿真测试的研究有助于探究汽车网络安全漏洞。

1.1.2. 现阶段测试工作难点

全国汽车标准化技术委员会
智能网联汽车分技术委员会

随着汽车智能化、网联化技术的飞速发展、用户需求的急剧增长，汽车的开发模式逐步转为敏捷模式，模式的转变显著加快了汽车功能的迭代速度，为用户带来了更为频繁的产品更新和体验升级。汽车功能快速迭代的同时，相应的测试工作量也迎来了显著提升。在更敏捷的开发模式中，测试是贯穿于整个开发过程的持续活动，每一次版本更新都需要经过严格的测试，以确保产品的稳定性和安全性。因此，不断提升测试效率和质量是智能汽车在快速迭代中保持高性能和可靠性的重要保障。

车辆智能化网联化程度不断提高，内部的电子控制单元的数量、复杂性逐渐增加，在电子电器架构上逐渐形成了以网关为枢纽、以 T-Box 为车云通信接口的网联化趋势。这也给车辆网络安全带来更多的威胁，给测试工作带来了越来越多的挑战。越来越多的零部件具有了连接车外网络的通信渠道，越来越多的零部件需要进行网络安全测试，这也对测试环境、测试工具、测试方法提出了更高的要求。

网络安全测试需要在零部件、台架或实车环境中进行，不同种类的测试需要大量的硬件资源支持，零部件层级的测试需要各类型域控制器、网关、车机、T-box、定位模块、V2X 模块等，整车层级测试也往往涉及多个阶段不同状态的整车，导致对硬件的依赖和消耗越来越高，物料成本直线上升。

基于真实环境的网络安全测试，需要完备的软硬件环境支持，并需要搭建完整的台架运行环境，在环境调试的过程中可能出现各种各样的问题，需要投入大量的资源解决环境问题。通常，不同的零部件开发由不同的部门分别负责，环境搭建需要沟通、协调各个部门协同支持来解决版本适配、通信接口等一系列问题，沟通成本较高。

在车辆整车开发生命周期，需要进行不同类型的不同目标的多次网络安全测试，涉及 Tier1 供应商、OEM、检测机构等，测试任务繁重，在没有统一的测试用例、测试方法和测试工具链的情况下需要投入大量的时间进行测试工作，也会造成同一测试内容重复进行、重复审核的问题。此外，测试环境的差异性会导致测试结果存在一定差异，也会导致问题查找定位难、问题修复难等一系列问题。

1.1.3. 仿真测试的目的及意义

汽车制造商和供应商潜在的安全隐患，实际生产过程中的软硬件安全问题，测试阶段的潜在的敏感信息泄露等一系列网络安全问题都可能导致产品召回和维修，造成企业巨大损失。汽车仿真网络安全测试在加速汽车测试周期、简化环境搭建、节省硬件成本、统一测试工具和方法、降低沟通成本等方面具有重要意义，可以显著实现降本增效。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

缩短汽车测试周期：传统的汽车测试通常需要在实际车辆上进行，这会花费大量时间和资源。汽车测试过程中涉及研发节点较多，而通过仿真测试可以在虚拟环境中快速模拟各种场景，尤其在漏洞发现——版本更新——验证测试的周期内，仿真测试可实现多人同步异地测试，大大缩短测试工作时间；在版本更新过程中，仿真测试的软件更新流程也较为简单，只要在虚拟化平台上重新关联系统镜像文件即可实现更新，减少了更新过程中的刷写、OTA升级等过程；在验证测试过程中，测试工作也可通过仿真平台上调用脚本进行迅速复验，从而缩短了产品研发过程中的迭代周期，加速了汽车的研发和上市。

节省硬件成本：真实车辆和零部件的硬件成本较高，而仿真测试则可以在虚拟环境中进行，无需多种类实体汽车零部件设备，仅需提供硬件虚拟化服务的计算机，从而节省了大量的硬件成本。

仿真环境搭建便利：仿真测试可以在虚拟环境中进行，无需真实车辆和硬件设备，只需建立合适的仿真环境即可。仿真环境搭建可通过虚拟化服务提供底层硬件支持，建立虚拟化硬件层厚，每次仅需要刷写不同版本的系统，不仅搭建成本相对较低，且可以随时随地进行测试，突破了传统测试方法对于车辆和测试人员的地域限制。对于测试人员来讲，仿真测试提高了测试的灵活性和便利性；对于 OEM 来讲，既节省了实体车辆及零部件的成本，又拓展了测试渠道，使其不局限于传统的测试组织和机构。主机厂可以将测试工作发布到互联网中，网罗全球白帽测试资源，大大提高了产品在研发周期中漏洞发现的可能性，间接提高了产品的网络安全性。

测试工具和方法统一：通常情况下，不同的测试人员使用的工具并不完全相同，而通过仿真测试可以通过仿真平台实现测试工具和方法的统一，可以更好地管理和执行测试流程，确保测试结果的一致性和可靠性。这有助于提高测试效率，降低测试误差，且方便团队间的协作与沟通。

节省沟通成本：传统的汽车测试通常需要涉及多个团队和部门，涉及 OEM 自身研发团队、测试部门、供应商技术团队、第三方检测机构，测试过程中经常需要专门的负责人进行技术细节沟通和任务安排，常常跨部门、跨公司协调资源。研发团队需要经过负责人才可以获知当前车辆所存在的问题，且往往都在技术需求下达后。当漏洞出现时，往往需要重新修改工程源码，特别是出现系统内核的相关漏洞后，需要修改底层代码，解决上层应用的依赖关系。而通过仿真测试，可以将测试团队集中在一个虚拟环境中进行测试，研发团队可通过仿真平台更直观的获取漏洞或问题的相关信息，减少了沟通的时间和成本，此外通过仿真平台，前置研发环节可以更好地获取漏洞信息，有助于汽车网络安全测试活动的左移，提高开

全国汽车标准化技术委员会
智能网联汽车分技术委员会

发效率。

仿真测试通过模拟各种可能的攻击场景，包括网络入侵、恶意软件注入、数据窃取等，全面评估汽车系统的安全性能和抗攻击能力。这种测试不仅能够验证安全策略和措施的有效性，还能够有效减少开发人员与测试人员间的信息差，提前发现并解决潜在的安全问题，有效降低了安全风险。通过有效的仿真测试，汽车制造商能够在产品投入实际使用之前，提前做好安全保障工作，保障车辆的运行安全、网络安全和数据安全。相较于传统的测试方法，仿真测试成本更低、效率更高，节约了时间和资源，提高了测试的灵活性和便利性。

综上所述，仿真测试在汽车安全性方面的作用不可忽视，是确保汽车安全性的重要手段，一定程度上预防了恶意攻击和敏感数据窃取行为，保障了人民生命财产安全；防范了汽车领域的潜在威胁，维护了国家安全，保障了国际经济和社会的稳定发展。

1.2. 网络安全仿真相关标准和法律法规现状

1.2.1. 国内标准规范

近年来，我国为了填补仿真测试相关标准的空白，已经在自动驾驶、网络空间安全等领域开展标准研究及标准制定工作，发布了《智能网联汽车在环仿真测试标准体系研究报告》和《自动驾驶功能仿真测试标准化需求研究报告》两项研究报告。此外，还发布了一系列网络空间安全仿真相关标准，如《YD/T 4590-2023 网络空间安全仿真 攻击行为检测技术要求》《YD/T 4597-2023 网络空间安全仿真 无人机系统网络安全仿真平台接入技术要求》《YD/T 4707-2024 网络空间安全仿真 智能汽车安全仿真平台接入要求》等。

1.2.1.1. 自动驾驶领域仿真标准现状

2024 年 4 月发布《智能网联汽车在环仿真测试标准体系研究报告》，分析了智能联网汽车在环仿真平台架构、在环仿真子系统模型及集成系统模型技术现状，提出了对应标准化需求，包括在环仿真软件、硬件的基本功能要求及试验方法、仿真平台接口协议、跨平台接口协议、仿真模型（术语、定义、分类、功能范围、接口、分级、测试方法和相关性要求）、集成系统模型与实车相关性（评估要求、试验方法及流程、试验场景、关键指标及其阈值）等。目前中国汽车工程学会正组织制定《智能网联汽车 车辆在环仿真测试平台》系列团体标准，可为智能网联汽车车辆在环测试平台的搭建方法和测试方法提供标准支撑。

2020 年 11 月发布《自动驾驶功能仿真测试标准化需求研究报告》，对自动驾驶功能仿真测试的通用要求、测试工具、测试场景、测试流程和评价方法等方面开展标准化需求研究，确定“优先启动：仿真测试的术语和定义、仿真测试对象及其要求、仿真测试的可重复性和

全国汽车标准化技术委员会
智能网联汽车分技术委员会

真实性要求、自动驾驶功能基础仿真测试场景及其通过评价指标的标准化工作”、“推迟启动：仿真模型精度要求、仿真测试工具之间及仿真工具内部的数据传输接口、仿真测试工具性能要求、仿真测试场景设计方法、仿真测试场景管理方法、仿真测试场景数据格式、仿真测试流程的标准化工作”的研究结论，目前正在研制《智能网联汽车自动驾驶功能仿真试验方法及要求》（国标），包含了优先启动的自动驾驶仿真测试标准内容。

1.2.1.2. 网络空间安全领域仿真标准现状

2023 年 12 月以来，由中国通信标准化协会组织制定，工信部发布了一系列网络空间安全领域仿真测试标准，这些标准从恶意软件危害性测评、知识获取、攻击行为检测、产品安全测评管理、试验环境隔离、其他领域仿真平台接入、网络安全检测等网络安全相关角度进行建立，并于 2024 年 4 月开始实施。除此之外，中国网络空间安全协会也在 2023 年 6 月发布了部分网络靶场相关标准，对传统网络安全领域仿真标准进行补充。

1.2.1.3. 汽车网络安全领域仿真标准现状

对于汽车网络安全领域而言，目前缺少相应标准用于支撑汽车网络安全仿真测试工作，参考前期已开展的汽车自动驾驶、网络空间安全等领域的仿真测试标准研究成果，可重点对仿真平台架构、仿真软/硬件基本要求及试验方法、仿真测试对象及其要求、仿真平台接口协议、跨平台接口协议、仿真模型、集成系统模型与实车相关性、可重复性和真实性等方面开展需求研究。

表 1 已发布仿真相关标准汇总表

NO.	领域	标准名称	状态	发布/研制机构
1	汽车自动驾驶	智能网联汽车 在环仿真测试标准体系研究报告	已发布	全国汽车标准化技术委员会智能网联汽车分技术委员会（以下简称TC114/SC34）
2	汽车自动驾驶	智能网联汽车 车辆在环仿真测试平台 第 1 部分：试验台架式平台搭建要求及方法	正在制定	中国汽车工程学会
3	汽车自动驾驶	智能网联汽车 车辆在环仿真测试平台 第 2 部分：试验场地式平台搭建要求及方法	正在制定	中国汽车工程学会
4	汽车自动驾驶	智能网联汽车 车辆在环仿真测试平台 第 3 部分：试验台架式平台测试要求及方法	正在制定	中国汽车工程学会
5	汽车自动驾驶	智能网联汽车 车辆在环仿真测试平台 第 4 部分：试验场地式平台测试要求及方法	正在制定	中国汽车工程学会

全国汽车标准化技术委员会
智能网联汽车分技术委员会

6	汽车自动驾驶	自动驾驶功能仿真测试标准化需求研究报告	已发布	TC114/SC34
7	汽车自动驾驶	GB/T 智能网联汽车 自动驾驶功能仿真试验方法及要求（报批稿）	正在制定	TC114/SC34
8	汽车自动驾驶	T/CMAX 121—2019 自动驾驶车辆模拟仿真测试平台技术要求	已发布	中关村智通智能交通产业联盟
9	网络空间安全	YD/T 4577-2023 网络安全仿真 恶意软件危害性测评方法	已发布	中国通信标准化协会（以下简称CCSA）
10	网络空间安全	YD/T 4589-2023 网络空间安全仿真 网络安全知识获取系统的功能要求	已发布	CCSA
11	网络空间安全	YD/T 4590-2023 网络空间安全仿真 攻击行为检测技术要求	已发布	CCSA
12	网络空间安全	YD/T 4591-2023 网络空间安全仿真 产品安全测评管理系统技术要求	已发布	CCSA
13	网络空间安全	YD/T 4594-2023 网络空间安全仿真 试验环境隔离要求	已发布	CCSA
14	网络空间安全	YD/T 4597-2023 网络空间安全仿真 无人机系统网络安全仿真平台接入技术要求	已发布	CCSA
15	网络空间安全	YD/T 4704-2024 网络空间安全仿真 网络安全检测指南	已发布	CCSA
16	网络空间安全	YD/T 4707-2024 网络空间安全仿真 智能汽车安全仿真平台接入要求	已发布	CCSA
17	网络空间安全	YD/T 4587-2023 网络空间安全仿真 术语	已发布	CCSA
18	网络空间安全	YD/T 4588-2023 网络空间安全仿真 参考架构	已发布	CCSA
19	网络空间安全	YD/T 4592-2023 网络空间安全仿真 角色定义及功能	已发布	CCSA
20	网络空间安全	YD/T 4593-2023 网络空间安全仿真 平台试验操作要求	已发布	CCSA
21	网络空间安全	YD/T 4595-2023 网络空间安全仿真 网络安全试验知识的统一表示与接口要求	已发布	CCSA
22	网络空间安全	YD/T 4596-2023 网络空间安全仿真 网络数据采集指南	已发布	CCSA
23	网络空间安全	YD/T 4661-2024 网络空间安全仿真 互联网域名系统根服务风险仿真技术要求	已发布	CCSA
24	网络空间安全	YD/T 4700-2024 网络空间安全仿真 安全技术效能评估方法	已发布	CCSA
25	网络空间安全	YD/T 4701-2024 网络空间安全仿真 运行控制接口要求	已发布	CCSA
27	网络空间安全	YD/T 4702-2024 网络空间安全仿真 轨道交通综合监控系统仿真平台接入技术要求	已发布	CCSA

全国智能网联汽车标准化技术委员会

28	网络空间安全	YD/T 4703-2024 网络空间安全仿真 目标网络构建与管理总体技术要求	已发布	CCSA
29	网络空间安全	YD/T 4705-2024 网络空间安全仿真 网络采集探针实施技术要求	已发布	CCSA
30	网络空间安全	YD/T 4706-2024 网络空间安全仿真 运行控制技术要求	已发布	CCSA
31	网络空间安全	YD/T 4708-2024 网络空间安全仿真 资源管理库技术架构	已发布	CCSA
33	网络靶场	T/CSAC 001-2023 网络靶场 基于技战术模型的安全测评方法	已发布	中国网络空间安全协会
34	网络靶场	T/CSAC 002-2023 网络靶场 能力分级指南	已发布	中国网络空间安全协会
35	网络靶场	T/CSAC 003-2023 网络靶场 资源描述要求	已发布	中国网络空间安全协会
36	网络靶场	T/CSAC 004-2023 网络靶场 试验任务导调总体要求	已发布	中国网络空间安全协会
37	网络靶场	T/CDEIIEA 001-2022 网络战靶场功能技术要求	已发布	成都电子信息产业生态圈联盟
38	网络靶场	网络逻辑靶场攻防技术深化分析	已发布	期刊：网络安全和信息化
39	网络靶场	网络安全靶场构建中的数据安全保障技术研究	已发布	期刊：信息与电脑
40	互联网	YD/T 4268-2023 IP 网络路由仿真系统的信息接口技术要求	已发布	CCSA
41	互联网	卫星互联网安全仿真测试技术研究	已发布	期刊：天地一体化信息网络
42	核工业	核工业网络安全仿真测试床的建设研究	已发布	期刊：自动化仪表
43	电力系统	电力系统安全仿真技术：工程安全、网络安全与信息物理综合安全	已发布	期刊：中国科学

全国汽车标准化技术委员会
智能网联汽车分技术委员会

1.2.2. 国外标准规范

目前国际上在网络安全仿真方面暂未开展针对性标准建设，相关标准及研究成果如下：

2021 年 8 月发布的 ISO/SAE 21434 是 UN/WP.29 R155 的关键支撑标准，规定了汽车电子电气系统在概念、产品开发、生产、运营、维护和报废阶段的网络安全风险管理（框架性 V&V）的工程要求，搭建了网络安全测试相关管理流程。

2017 年 SimVentions 公司发表《Future Look – Effective Cybersecurity Using Modeling & Simulation》，主要阐述如何用网络安全仿真技术提高网络安全工程的效率以及效果。

2021 年 Hamdi Kavak 等人研究的《Simulation for cybersecurity: state of the art and future directions》表明模拟在网络安全研究中的应用具有巨大潜力。

2017 年欧盟委员会公布标准《Security standards applying to all European Commission information systems》，标准规定由欧盟委员会或代表欧盟委员会拥有、采购、管理或运营的通信和信息系统安全的基本原则和目标。

1.2.3. 国内外法律法规及监管要求

1.2.3.1. 国内监管要求

目前国内已出台《网络安全法》《数据安全法》《个人信息保护法》《汽车数据安全管理若干规定（试行）》《关于加强车联网网络安全和数据安全工作的通知》《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于开展智能网联汽车准入和上路通行试点工作的通知》等汽车网络安全相关法律法规及监管要求，同时计划 2025 年发布的强制性国家标准《汽车整车网络安全技术要求》明确指出“车辆制造商应通过测试来验证所实施的网络安全措施的有效性”，并提出具体技术要求和测试要求。

1.2.3.2. 海外法规要求

2018 年 5 月，欧盟出台《通用数据保护条例》（GDPR）用于保护个人数据隐私安全，同时美国、日本、韩国、新加坡、泰国、俄罗斯等国家也出台了相应个人信息保护法规，因此，汽车对个人信息数据的处理应满足当地合规要求。

2020 年 6 月，联合国世界车辆法规协调论坛（UN/WP.29）发布 R155（强制汽车网络安全）法规，定义了 CSMS（Cyber Security Management System/网络安全管理体系认证和 VTA（Vehicle Type Approval/车辆型式认证）的相关规范要求，明确要求对汽车开展 TARA 分析和风险识别并通过测试来验证有效性和充分性。

综上所述，对于国内车企的出海车型而言，一是需要满足出口所在地的个人信息数据合规要求，二是需要满足 WP29 58 协议国关于汽车网络安全的 R155 法规要求。

从汽车网络安全仿真相关标准和法律法规现状方面来看，主要是以国家推荐性标准为主，领域主要是汽车自动驾驶与网络空间安全领域，尚无针对智能网联汽车的网络安全领域的仿真标准。

1.3. 汽车仿真测试发展和研究现状

1.3.1. 汽车仿真测试发展

全国汽车标准化技术委员会 智能网联汽车分技术委员会

汽车仿真测试是一种利用计算机模拟技术对汽车的各项性能进行测试和评估的方法。使用仿真测试技术提供一个安全、可控且成本效益高的测试环境，减少实车测试的需求，它使工程师在产品开发的早期阶段发现潜在的设计问题，优化汽车性能，提升产品开发效率，降低开发成本、缩短开发周期，并满足日益严格的法律法规要求。

汽车仿真测试技术在汽车领域应用广泛，可针对零部件或者整车进行仿真，用于驱动控制、车辆动力学、空气动力学、热管理、可靠性、燃油经济性、排放和噪声等方面。随着汽车智能化程度的不断提高，软件在定义汽车，车辆功能日趋复杂、软件数量也越来越多，通过环境传感器与周边行驶环境的信息交互与互联更为密切，针对智能驾驶的仿真测试技术已成为当前汽车智能化世界性的研究热点。

国际汽车制造商协会（Organisation Internationale des Constructeurs d'Automobiles，OICA）在 2019 年正式提出了由审核/评估（包含模拟仿真测试）、封闭场地测试和实际道路测试的“三支柱”方法对智能驾驶汽车进行测试认证。联合国经济委员会世界车辆法规协调论坛（UNECE/WP.29）自动驾驶与网联车辆 (GRVA，Working Party on Automated/Autonomous and Connected Vehicles）自动驾驶验证方法的非正式工作组（IWG on VMAD, Informal Working Group on Validation Method for Automated Driving）提出包含场景目录以及模拟仿真测试、封闭场地测试、实际道路测试、审核评估和使用中检测报告等多支柱的测试方法。

仿真测试可以帮助研发人员和汽车认证检测机构完善优化对自动驾驶系统产品的验证测试流程和认证检测方法。通过海量高覆盖度、复杂度的场景库，不但可以增加测试工况范围和复杂程度，更可以对其零部件、子系统与整车集成进行不同层级的全链条测试。仿真测试相比于封闭场地测试、公共道路测试具有场景配置灵活、测试效率高、测试重复性强、测试过程安全、测试成本低等众多优势，可实现自动测试和加速测试，且不依赖于特定的技术实现，允许评估不同技术方案的安全性。通过仿真覆盖实车检测不能实现的危险场景和边角场景，在仿真测试环境下及早发现实车测试不易甄别的软件故障。

根据测试对象和仿真测试形式的不同，测试方法包含软件在环(SIL)、模型在环(MIL)、硬件在环(HIL)、驾驶员在环(DIL)、车辆在环(VIL)，云仿真测试等，覆盖产品开发的不同阶段。建立测试场景数据库，通过 VTD、PreScan、CarMaker 等测试平台工具链进行传感器和 V2X 等动态场景仿真，覆盖感知层、决策层和执行层，形成闭环控制，持续迭代和优化。同时与实车测试相结合，利用仿真测试来指导实车测试的设计，并用实车测试结果来验证仿真模型的准确性。当前国内外大量企业和机构均搭建了不同形式的在环仿真测试平台，加速车辆相关产品的开发。Waymo、Tesla、百度、腾讯、华为等也建立了高并发、集群管理的

全国汽车标准化技术委员会
智能网联汽车分技术委员会

虚拟云仿真平台用于自动驾驶测试和验证，全都具备日仿真百万公里以上的能力。

1.3.2. 汽车仿真测试在自动驾驶领域的研究

一、基于场景的虚拟测试方法：随着自动驾驶等级的提高，传统的测试工具和方法已不能满足需求。基于场景的虚拟测试方法因其在测试效率和成本方面的优势，成为未来自动驾驶汽车测试验证的重要手段。这包括了对测试场景的不同定义方式、测试场景的数据来源及处理方法的研究，以及软件在环、硬件在环和车辆在环测试方案及其关键技术的梳理。

二、高等级自动驾驶汽车（HAV）的安全性测试：安全性测试是规模化应用的基本保障。场景化虚拟测试正成为验证 HAV 安全性的核心方法。这涉及到测试场景自主划分、自动化仿真生成和未知高风险场景搜寻等理论方法的研究，以及支撑测试场景生成、驾驶行为双向交互和多传感器物理模型融合的高可信仿真技术的研究。

三、虚拟现实（VR）技术的应用：为了减少实际路测的风险、降低成本并加速开发，建立了基于 VR 的自动驾驶车辆测试平台，结合 AirSim 系统和 UE4 引擎，实现了控制器-in-the-loop 模拟方法，以完成不同驾驶条件下的模拟测试，并优化自动驾驶控制系统。

四、CARLA 开源模拟器：CARLA 是一个为自动驾驶研究开发的开源模拟器，支持开发、训练和验证自动驾驶城市驾驶系统。它提供了灵活的传感器套件和环境条件配置，以及用于评估自动驾驶性能的指标。

五、面向自动驾驶的虚拟仿真测试平台架构设计：提出了一种面向自动驾驶的虚拟仿真测试平台架构，研究了虚实一体动态交通流仿真、车辆动力学与传感器仿真、高置信度仿真场景库构建和仿真结果评估体系等模块的实现方法。

六、人工智能技术的应用：利用人工智能技术中的 VR 技术建立无人驾驶车辆仿真模型，通过仿真驱动模块内的执行驱动装置和驾驶模拟器仿真无人驾驶车辆在场景中行驶，有效对无人驾驶车辆进行虚拟仿真测试。

七、虚拟场景快速建模与测试案例生成方法：研究了基于概率统计分布的多维度测试案例自动生成算法，可以有效地提高测试效率。此外，还研究了利用高清渲染管线技术的环境特性模拟方法，使构建的虚拟环境更逼近于真实环境。

1.3.3. 汽车仿真测试在网络安全领域的研究

汽车仿真测试在网络安全领域的研究目前处于初期阶段，主要集中在面向网络安全的汽车整车虚拟化仿真技术、面向网络安全的汽车零部件虚拟化仿真技术、汽车网络安全威胁评估仿真技术。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

1.4. 仿真技术在汽车网络安全领域应用现状

当前在汽车网络安全领域，仿真测试及相关技术的研究仍处于发展初期，尚未广泛应用。受制于车联网业务场景类型繁杂、各厂商间汽车与零部件高度差异化等客观因素，高度覆盖、广泛兼容的通用型汽车网络安全仿真测试体系技术成熟度不足。少数汽车生产厂商、研究机构、监管机构、安全厂商以及高校在智能网联汽车网络安全测评验证实践中，依托相对成熟的汽车功能测试和技术验证仿真平台进行部分网络与数据安全测评，但测试环境缺少和车联网网络安全业务场景深度融合，相关技术能力暂未形成行业化、规模化及产业化应用。

仿真测试在汽车网络安全领域应用前景广阔，目前主要广泛应用于车联网及智能网联汽车网络与数据安全合规验证、渗透测试、攻防演练、安全试验、业务功能验证、漏洞挖掘与影响评级等各类场景。合规验证方面，可以依托仿真体系实现在环状态下对智能网联汽车整车、车辆零部件、车端异构网络、车端应用与业务、车联网数据等元素按照国内外相关标准法规进行合规验证，有效解决车联网产业高速发展下网络安全多元化测评需求和测试流程规范化问题；渗透测试方面，仿真测试可以通过接入技术为汽车软硬件、通信和云端等模块提供统一接口，配置流量事件重放、场景编排和态势呈现等功能，在避免攻击测试对车辆的物理性破坏前提下开展漏洞挖掘；攻防演练方面，仿真测试可以通过模拟云端、路侧端、车端以及车内网络、车载应用、车辆组件、数据等各类车联网关键元素，生成业务流拓扑构建典型业务场景，为攻防演练提供贴合实际运营场景的靶标体系；安全试验方面，可通过仿真环境模拟车辆实际运行环境，在模拟基础上对车载入侵检测、车载防火墙、车联网认证加密、车联网数据安全防护、车联网安全运营平台等车联网安全技术开展试验，测试能否有效进行安全赋能，实现安全防护预期；业务功能验证方面，仿真测试体系主要针对蓝牙钥匙、辅助驾驶、V2X、OTA 等业务场景进行仿真模拟，在仿真环境下验证相关业务是否存在网络安全与数据安全隐患；漏洞挖掘与影响评级方面，一方面通过仿真测试系统与被测资产建立在环测试环境，实现被测资产动态检测，挖掘潜在安全漏洞，另一方面可将安全漏洞在仿真环境中进行相应威胁场景与攻击路径绘制，实现漏洞风险等级评估。

目前，汽车网络安全仿真测试主要包括车联网业务类仿真、总线协议仿真、无线协议仿真等方面内容。

1.4.1. 车联网业务类仿真

当前车联网业务类仿真主要包括 ADAS、V2X、OTA 等典型业务场景，各机构依托相较成熟的汽车功能仿真（系统）平台结合车联网网络安全要素，搭建具备车联网业务网络与

全国汽车标准化技术委员会
智能网联汽车分技术委员会

数据安全测试环境，开展一定程度的网络安全类测试。由于传统汽车功能仿真（系统）平台主要为 Prescan、Carmaker、Carsim 等国外系统平台，缺少和国内相关业务与场景深度融合。因此国内在车联网业务类型网络安全仿真测试技术发展仍处于发展初期，目前鹏城实验室、北京质检院、天融信、大鲲智联等机构与企业在该领域初步掌握一定技术积累。

1.4.2. 总线协议仿真

总线协议仿真目前主要采用上位机模拟车端 ECU 间信息通信环境，可针对车端异构总线网络如 CAN/CANFD/CANXL 总线、车载以太网、LIN 总线等进行仿真与模拟，在此基础上进行车端总线安全测试。可面向总线网络开展泛洪攻击测试、模糊测试、注入测试、逆向测试等各类网络安全测试。总线协议仿真测试当前处于相对较为成熟阶段，部分企业具备较为成熟的技术实力。

1.4.3. 无线协议仿真

无线协议仿真目前主要依托无线综测仪与汽车搭建无线通信业务场景，可针对车载蓝牙、车载 Wi-Fi、车辆 GNSS、车端无线射频网络、车载蜂窝网络、V2X 等协议进行网络安全测试。可开展认证测试、干扰测试、加密检测、中间人攻击测试、篡改攻击测试、重放攻击测试等多种类型网络安全测试。无线协议仿真测试当前处于高速发展阶段，主要以通用无线测试技术与车联网业务场景进行结合的形式进行开展，天融信、泽鹿、鹏城实验室、为辰信安、腾讯科恩实验室等机构与企业在该领域具备一定技术实力。

此外，还有一些机构与企业尝试采用搭建车辆电子电器架构黄板车的形式将被测资产以硬件形态与仿真模组搭建仿真环境，并开展网络与数据安全测试。但由于各厂商、各型号、各 Tier1 供应商所提供硬件组件存在较大差异性，纯硬件形态仿真测试体系通常只能针对少数车型或零部件类型开展测试，不具备通用性。因此，该类型测仿真体系当前主要为各汽车生产厂商与零部件供应厂商进行内部产品网络安全检测测试使用，部分研究机构与安全厂商出于技术研究有少量技术积累。一汽集团、东风集团、比亚迪、经纬恒润、鹏城实验室、天融信等机构与企业在该领域有一定技术积累与应用。

从技术层面来看，目前建模仿真技术已广泛地应用于多种领域，但是在网络安全领域中的应用还处于探索阶段。当前主要集中在以下几个方面：

（1）网络安全仿真：

模拟网络攻击：通过仿真技术模拟各种类型的网络攻击，如 DDoS 攻击、SQL 注入、跨站脚本等，以评估网络系统的抗攻击能力和安全性。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

评估防御策略：利用仿真技术模拟网络安全防御策略的应对效果，包括入侵检测系统、防火墙、安全路由器等，以验证其有效性和可靠性。

（2）密码学仿真：

密码系统分析：通过仿真技术模拟密码系统的加密和解密过程，评估其安全性和抵抗攻击的能力，包括对称加密、非对称加密和哈希算法等。

密码分析工具：开发用于密码破解和分析的仿真工具，用于评估密码系统的强度和寻找潜在的漏洞。

（3）人工智能安全仿真：

对抗性学习仿真：模拟对抗性学习环境，研究如何提高机器学习模型对抗攻击的能力，包括对抗样本的生成和检测。

恶意软件仿真：利用仿真技术模拟恶意软件的行为，研究如何利用机器学习和深度学习技术来检测和防御恶意软件。

（4）物联网安全仿真：

模拟物联网攻击：使用仿真技术模拟物联网系统中的各种攻击场景，包括设备入侵、信息窃取等，以评估物联网系统的安全性。

安全通信仿真：模拟物联网设备之间的通信过程，研究安全通信协议和机制的有效性和可靠性。

（5）信息隐藏仿真：

隐写术仿真：开发用于模拟隐写术的工具，研究不同类型的隐写术对信息隐藏的效果和安全性。

数字水印仿真：通过仿真技术模拟数字水印的嵌入和提取过程，评估数字水印技术在版权保护和身份认证中的应用效果。

目前国内外针对汽车仿真测试方法和评价指标等方面开展了大量的研究工作，但仍存在以下两个方面的问题：

（1）智能网联汽车网络安全仿真测试场景尚需完善。当前测试库以经典的车辆测试场景为主，如 Wi-Fi、蓝牙、IVI、第三方车载应用等，但这些简单场景不能满足智能网联汽车在网络安全方面所有功能测试的需求。如何建立接近实际智能网联汽车真实环境的复杂网络安全测试场景，能在统计学上覆盖现实网络安全攻击中的典型现象，是当前一个亟待解决的问题。

（2）缺少智能网联汽车网络安全仿真测试标准评价体系。目前，针对智能网联汽车网

全国汽车标准化技术委员会
智能网联汽车分技术委员会

络安全测试的仿真测试处于起步阶段，尚未形成明确的评价体系。网络安全测试所用的指标不够全面，大量研究利用传统网络安全测试指标进行测试评价，如是否系统漏洞、数据泄露等。而与智能网联汽车车辆密切相关的汽车网关、OTA、CAN 等具有实际工程意义网络安全测试指标的仿真研究较少。

1.5. 小结

综上，汽车网络安全行业对汽车网络安全仿真测试有强烈的需求，且国内外法规对汽车网络安全提出了较高要求，因此开展汽车网络安全仿真领域标准化研究具有重要的意义。尽管国内外在汽车仿真标准研究报告和网络空间安全仿真方面发布了一系列标准，但在汽车网络安全领域缺乏相关标准支撑。从汽车仿真测试发展与研究现状来看，仿真技术在传统汽车业务应用中相对成熟，具备可借鉴的基础。同时，其在汽车网络安全领域也已有初步研究及探索性应用，能够提炼出基本研究方向。此外，仿真技术在车联网业务、总线协议、无线协议等汽车网络安全相关领域的应用实践，也为研究提供了参考。因此，本项目将聚焦汽车网络安全仿真场景库构建方法、汽车网络安全仿真技术及评价指标、汽车网络安全仿真测试示范应用等方面开展研究。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

2. 汽车网络安全仿真测试

2.1. 汽车仿真测试场景分类基础

随着汽车“电动化、网联化、智能化、共享化”的全面推进，几乎任何一项新技术的诞生都离不开汽车电子的身影。电子技术在动力总成控制、底盘控制、车身控制以及车载信息娱乐系统等各个部分所占的比重越来越大，所占的整车成本也越来越高。电子技术已悄然成为汽车各方面功能拓展和性能提升的重要技术支撑。由于汽车电子硬件系统的多样性，ECU 软件的开发受到硬件系统的制约，每当需要更新硬件时，都会导致 ECU 软件重新编写或大规模修改，之后还要进行一系列测试，从而导致了高昂的研发费用与漫长的研发周期。

2.1.1. AUTOSAR 规范

2.1.1.1. AUTOSAR 概述

在 2003 年，由全球汽车制造商、零部件供应商及其他电子、半导体和软件系统公司联合建立了汽车开放系统架构联盟（AUTomotive Open System Architecture，AUTOSAR），并联合推出了一个开放化的、标准化的汽车嵌入式系统软件架构——AUTOSAR 规范。与传统 ECU 软件架构相比，AUTOSAR 分层架构的高度抽象使得汽车嵌入式系统软、硬件耦合度大大降低。

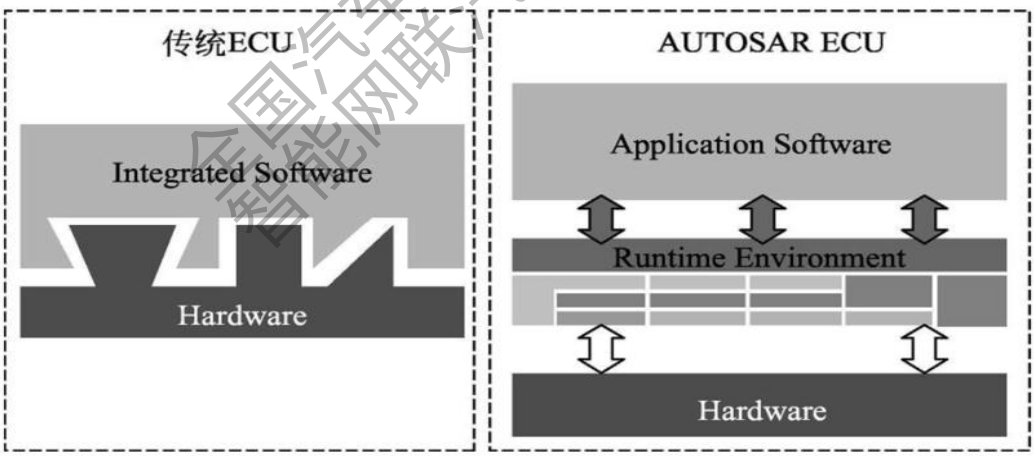


图 1 传统 ECU 与 AUTOSAR 架构

2.1.1.2. AUTOSAR 分层架构

AUTOSAR 规范主要包括分层架构、方法论和应用接口三部分内容。其中，分层架构是实现软硬件分离的关键，它使汽车嵌入式系统控制软件开发者摆脱了以往 ECU 软件开发与验证时对硬件系统的依赖。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

在 AUTOSAR 分层架构中，汽车嵌入式系统软件自上而下分别为应用软件层（Application Software Layer，ASW）、运行时环境（Runtime Environment，RTE）、基础软件层（Basic Software Layer，BSW）和微控制器（Microcontroller），如图所示。为保证上层与下层的无关性，在通常情况下，每一层只能使用下一层所提供的接口，并向上一层提供相应的接口。

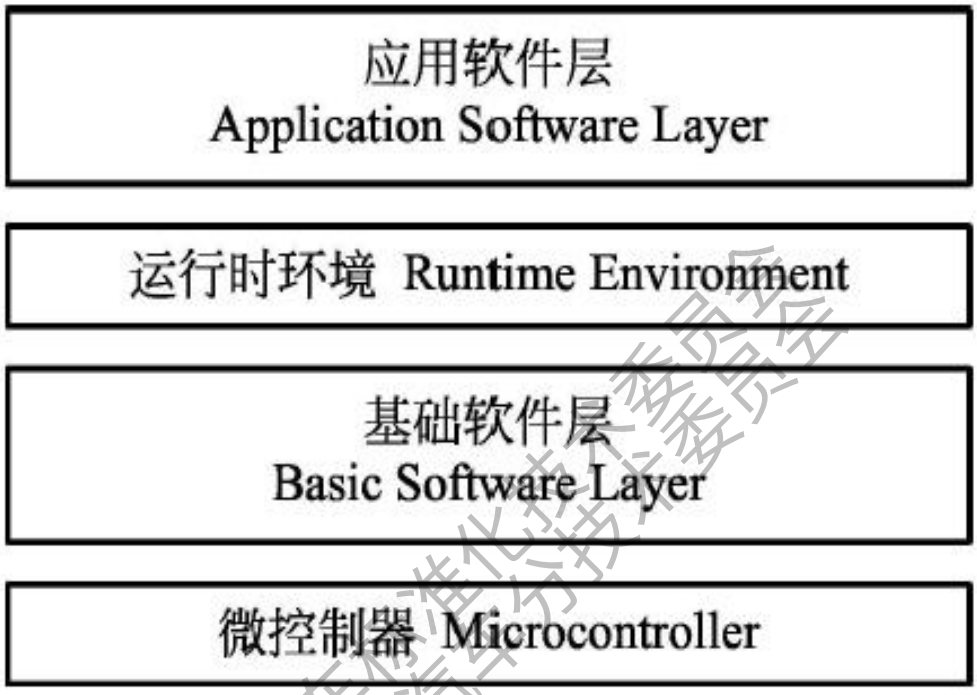


图 2 AUTOSAR 分层架构

2.1.1.2.1. 应用软件层

应用软件层包含若干软件组件（Software Component，SWC），软件组件间通过端口（Port）进行交互。每个软件组件可包含一个或多个运行实体（Runnable Entity，RE），运行实体中封装了相关控制算法，可由 RTE 事件触发。

2.1.1.2.2. 运行时环境

运行时环境（Runtime Environment，RTE）作为应用软件层与基础软件层交互的桥梁，为软硬件分离提供了可能。

RTE 可以实现：软件组件间、基础软件间、软件组件与基础软件之间的通信。RTE 封装了基础软件层的通信和服务，为应用层软件组件提供了标准化的基础软件和通信接口，使得应用层可以通过 RTE 接口函数调用基础软件的服务。

RTE 抽象类 ECU 之间的通信，即 RTE 通过使用标准化的接口将其统一为软件组件之间的通信。由于 RTE 实现与具体 ECU 相关，所以需要为每个 ECU 分别实现。

全国汽车标准化技术委员会 智能网联汽车分技术委员会

2.1.1.2.3. 基础软件层

基础软件层（Basic Software Layer，BSW）可分为 4 层：服务层（Services Layer）、ECU 抽象层（ECU Abstraction Layer）、微控制器抽象层（Microcontroller Abstraction Layer，MCAL）、复杂驱动（Complex Drivers），如下图 3 所示。

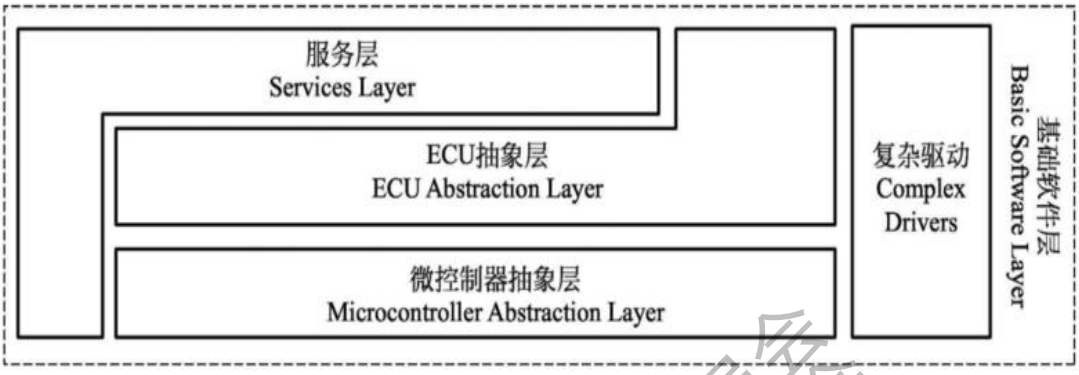


图 3 AUTOSAR 基层软件层

（1）服务层

服务层（Services Layer）提供一些常用服务：系统服务（System Services）、存储器服务（Memory Services）、通信服务（Communication Services）。

提供网络通信管理、存储管理、ECU 模式管理、实时操作系统（Real Time Operating System，RTOS）等服务。除操作系统外，服务层的软件模块都与 ECU 平台无关。

（2）ECU 抽象层

ECU 抽象层（ECU Abstraction Layer）包括板载设备抽象（Onboard Devices Abstraction）、存储器硬件抽象（Memory Hardware Abstraction）、通信硬件抽象（Communication Hardware Abstraction）和 I/O 硬件抽象（Input/Output Hardware Abstraction）。

该层将 ECU 结构进行了抽象，负责提供统一的访问接口，实现对通信、存储器或 I/O 的访问，从而不需要考虑这些资源是由 MCU 提供，还是片外设备提供。该层与 ECU 平台相关，但与 MCU 无关，

（3）MCU 抽象层

微控制器抽象层（Microcontroller Abstraction Layer，MCAL）是实现不同硬件接口统一化的特殊层。通过微控制器抽象层可将硬件封装起来，避免上层软件直接对 MCU 寄存器进行操作。

MCAL 包括微控制器驱动（Microcontroller Drivers）、存储器驱动（Memory Drivers）、通信驱动（Communication Drivers）以及 I/O 驱动（I/O Drivers），如下图 4 所示。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

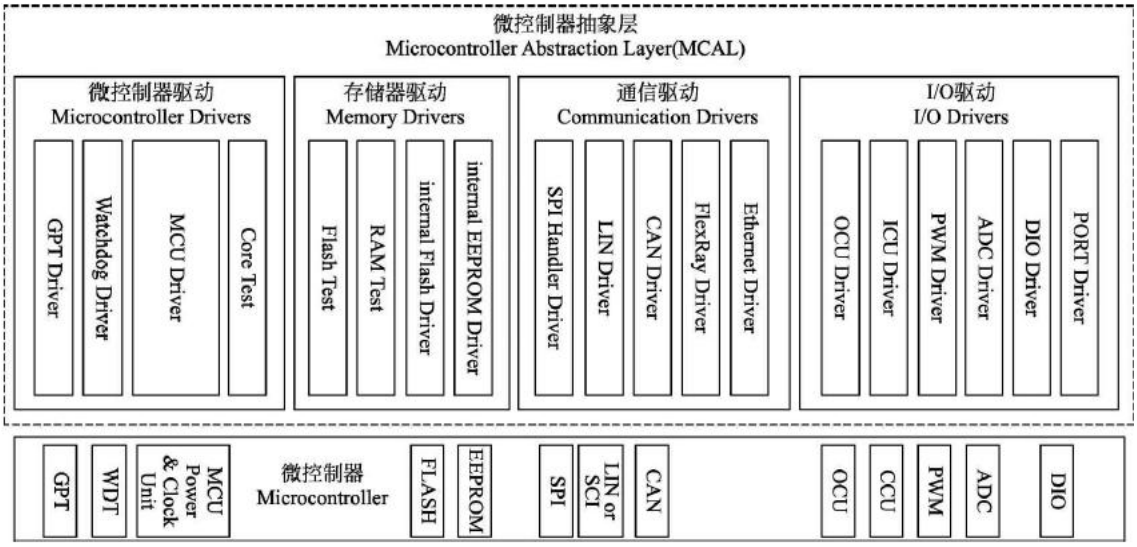


图 4 微控制器抽象层

上述各层又由一些列基础软件组件构成，如下图 5 所示。

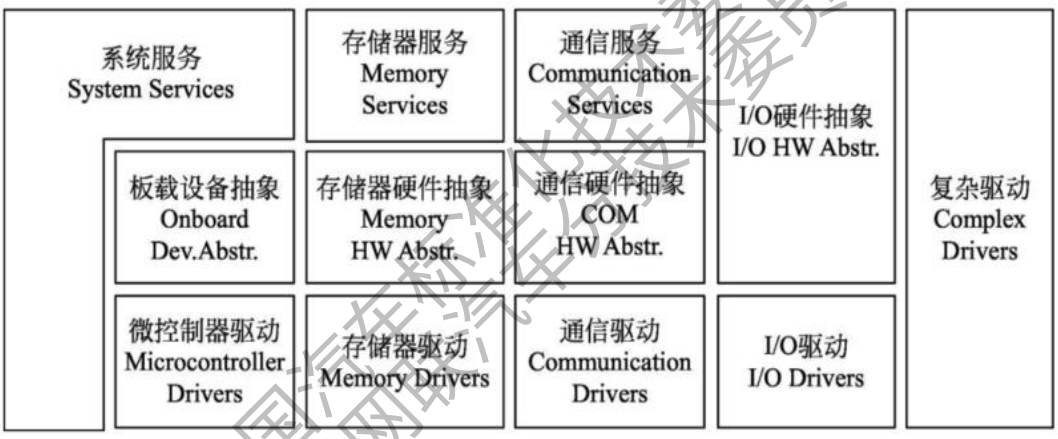


图 5 AUTOSAR 基础软件层结构

2.1.1.2.4. 复杂驱动层

由于对复杂传感器和执行器进行操作的模块涉及严格的时序问题，难以抽象，所以在 AUTOSAR 规范中这部分没有被标准化，统称为复杂驱动（Complex Drivers）。

2.1.1.3. AUTOSAR 国内应用现状

近年来，随着国内新能源汽车相关控制器正向开发需求的增长，AUTOSAR 规范在国内越来越受到大家的关注，AUTOSAR 已广泛应用于众多领域控制器中，其在汽车电子领域与其他领域技术发生了许多交叉，并且应用需求也越来越大。目前国内主流整车厂以及一些零部件供应商都开始致力于符合 AUTOSAR 规范的车用控制器软件开发。

截至目前，AUTOSAR 组织已发布 Classic 和 Adaptive 两个平台规范，分别对应安全控制类和自动驾驶的高性能类。Classic 平台基于 OSEK/VDX 标准，定义了安全车控操作系统

全国汽车标准化技术委员会
智能网联汽车分技术委员会

的技术规范。Classic AUTOSAR 的软件架构如图 6 所示，其主要特点是面向功能的架构（FOA），采用分层设计，实现应用层、基础软件层和硬件层的解耦。

图 6 Classic AUTOSAR 软件架构

AUTOSAR 组织为应对自动驾驶技术的发展推出了 Adaptive AUTOSAR（AP）架构，如图 7 所示，其主要特点是采用面向服务的架构（SOA），服务可根据应用需求动态加载，可通过配置文件动态加载配置，并可进行单独更新，相对于 Classic AUTOSAR（CP），可以满足更强大的算力需求，更安全，兼容性好，可进行敏捷开发。

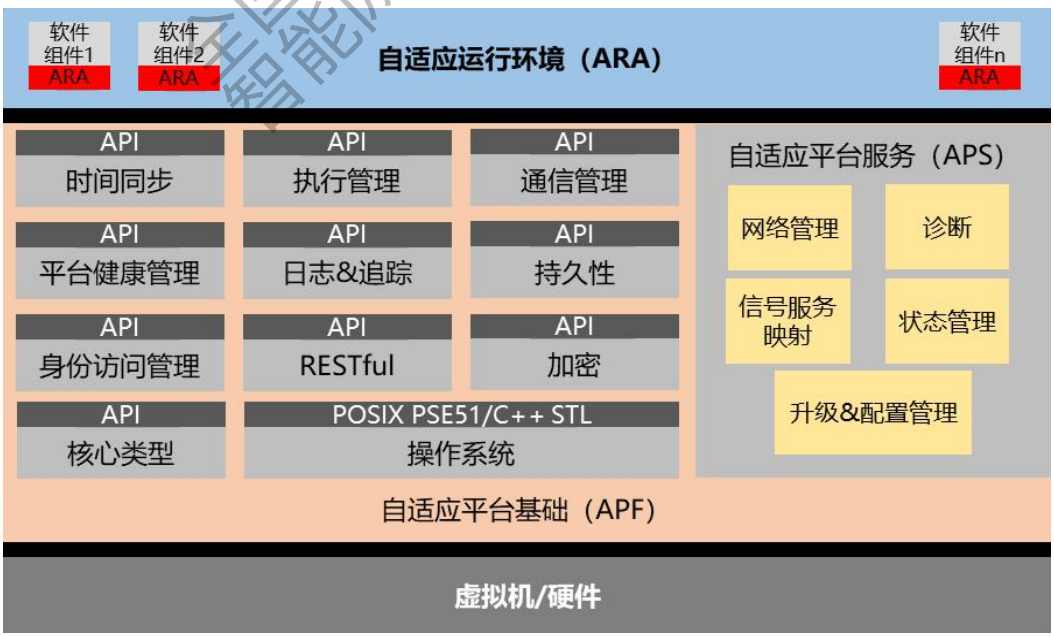


图 7 Adaptive AUTOSAR 架构

全国汽车标准化技术委员会 智能网联汽车分技术委员会

2.1.2. 电子电气系统

2.1.2.1. 概述

电子电气架构（EEA，Electronic/Electrical Architecture）是集合整车电子电气系统功能需求分析、系统方案设计、网络架构设计、子系统功能开发、整车电气原理及线束拓扑设计等内容为一体的顶层规划工作，是一种将整车动力驱动、底盘转向、娱乐信息、车身电气等用户功能转化为系统策略、网络数据、容错诊断、能量管理、电源分配、物理布局等具体实现的电子电气系统解决方案。

根据新阶段智能网联汽车的发展需求，在关键技术的组成划分上，新型电子电气架构横跨功能架构、软件架构、物理架构，同时纵贯数据架构、网络架构、安全架构。相对于研究对象的横向视角观之，功能架构包括整车动力、底盘、智驾、智舱等各功能域的应用接口与应用功能方案，是实现用户功能的系统工程化与数据化的实现载体。软件架构由应用软件平台与底层基础软件平台组成，向上为功能架构提供可复用的应用软件实现支撑，向下建立统一的面向不同硬件的基础软件组件，实现软硬件解耦。物理架构主要由部件级硬件平台与元素级芯片平台组成，是电子电气架构的真实物理反映。系统实现的纵向视角观之，数据架构包括数据采集、数据处理以及数据应用，为整车数据价值挖掘和释放提供基础保障。网络架构包含多种车载网络通信技术，为其他架构部分提供信息传输基础保障。安全架构主要由功能安全、预期功能安全以及网络安全的系统范畴组成，为其他架构部分提供整车全方位系统级安全保障基础。各个子架构之间相互依赖，协同配合，共同构成整车宏观电子电气架构。

2.1.2.2. 技术现状

2.1.2.2.1. 分布式架构

分布式 E/E 架构根据汽车功能的不同进行划分，每个电子控制单元（Electronic Control Unit，ECU）的设计都基于特定的功能需求展开。在该架构中，各个 ECU 通过 CAN 总线进行信息传递，以实现整车的功能。在这种架构中，每个 ECU 只负责单一功能的实现，一辆车通常分布着上百个 ECU，它们不仅直接驱动执行器和传感器，还承担着复杂的业务功能控制逻辑。这种架构的软硬件紧密耦合，每次扩展一个功能，都需要增加相应的 ECU 和通信信号。然而，由于 ECU 的计算能力有限，通信带宽受限，功能升级困难等问题，这种架构存在制约架构升级和影响汽车安全性能的瓶颈效应。此外，随着 ECU 的增加，车内的线束也会变得更长，增加了整车的质量和成本，同时也给整车的布置和装配带来了很大的困扰。

2.1.2.2.2. 域集中式架构

全国汽车标准化技术委员会
智能网联汽车分技术委员会

随着车载以太网的广泛应用和高算力芯片的低成本大带宽，域集中架构逐渐摆脱了分布式架构在安全性、可扩展性等方面的困境。域集中架构的基本思路是根据功能将多个电控单元（ECU）的功能进行聚类，整车只部署几个域控制器（DCU）作为主控。典型的基于中央网关的域集中架构，各 DCU 负责完成各个域的数据处理与功能决策，并对该域下属的传感器与执行器进行控制管理。域之间通过中央网关交换所需数据，这种架构不仅保证了域间的通信和互操作性，同时也实现了网络安全和功能安全。

2.1.2.2.3. 中央集中式架构

为了降低车内结构连接的复杂度、提高算力利用率、降低成本、提高安全性，中央集中式架构进一步将域集中架构中的多个 DCU 融合为一个或多个拥有更强算力的多核异构 SoC 芯片和多种操作系统组合的中央计算平台（CCP）。车载传感器和执行器不再按照功能部署，而是按照物理位置划分就近接入区域控制器（ZCU）。在这种架构中，各采集和执行节点通过 ZCU 将原始数据传输到一个或多个 CCP 中进行处理，所有数据处理和决策都在 CCP 中完成。ZCU 主要负责数据采集、通信协议转化和数据传输等功能。多个 ZCU 之间通过以太网构成环形网络，进一步提高通信冗余和可靠性。按照区域进行传感器和执行器的就近接入简化了构型布置，缩短了线束长度。该架构将整车控制计算功能全部集中到一个 CCP 中。然而，从目前的技术能力来看，多 CCP 架构在硬件设计、软件开发和安全冗余等方面都要求更高，因此单 CCP 架构是当前主流方案。

图 8 汽车电子 E/E 架构

2.1.2.3. 系统分解

因为系统的分解主要是针对组件进行的，任何一个复杂系统都可以有多个视图，从每个视图看到的组件可能完全不同。对于电子电气系统来说，从逻辑视图看到的是逻辑功能，从物理视图看到的是各种部件，从过程视图看到的是开发过程中的各种阶段性工作和输出物。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

智能网联汽车组件也完全取决于观察者的位置和角度：一个控制器既可以被继续分解为外壳、印刷电路板总成（Printed Circuit Board Assembly，PCBA）和插件等更小的部件，也可以与周边的传感器和执行器等组成一个较大的组件。

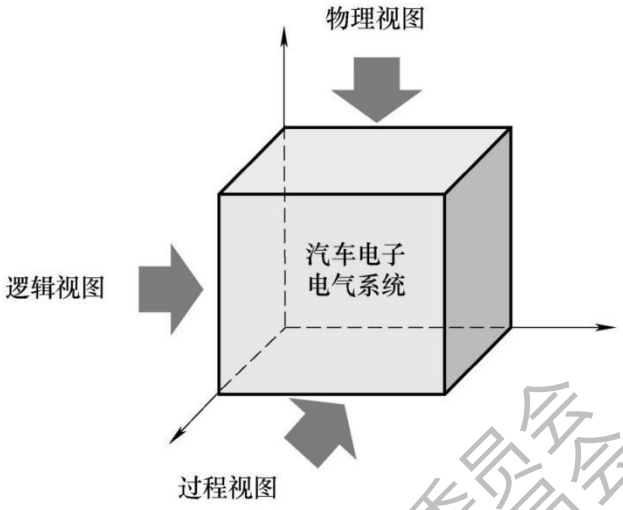


图 9 汽车电子电气系统视图

2.1.3. OSI 七层网络模型规范

2.1.3.1. 概述

OSI（Open System Interconnection）模型是国际标准化组织（ISO）提出的一个框架，用于实现不同计算机系统之间的通信。这个模型将通信任务分解为七个层次，每一层都承担着特定的功能，每次数据传递时都会从上层到下层逐级传输，直到物理层对传输介质进行信号传递，然后在接收端逐级向上直到应用层。

2.1.3.1.1. 物理层（Physical Layer）

物理层是 OSI 模型的最底层，负责传输比特流（即 0 和 1 的序列）。它定义了数据传输的物理媒介（如电缆、光纤等）、传输方式（如电信号、光信号等）以及物理接口（如插头、插座等）。物理层不关心数据的内容，只负责数据的物理传输。

2.1.3.1.2. 数据链路层（Data Link Layer）

数据链路层在物理层之上，负责在相邻节点间可靠地传输数据帧。它通过引入帧的概念（即一段包含地址、数据和控制信息的比特流），实现了数据的封装和传输控制。数据链路层还负责处理物理层的错误，如比特错误，并提供流量控制和访问控制等机制。

2.1.3.1.3. 网络层（Network Layer）

网络层负责将数据包从源节点传输到目标节点，可能跨越多个网络。它通过引入 IP 地

全国汽车标准化技术委员会
智能网联汽车分技术委员会

址等概念，实现了数据的路由和转发功能。网络层还负责处理网络拥塞和错误等问题，并提供网络服务的接口。

2.1.3.1.4. 传输层（Transport Layer）

传输层位于网络层之上，负责在源主机和目标主机之间提供端到端的可靠或不可靠的数据传输服务。它通过引入端口号等概念，实现了应用程序之间的通信。传输层协议如 TCP（传输控制协议）和 UDP（用户数据报协议）分别提供了面向连接的可靠传输和无连接的不可靠传输服务。

2.1.3.1.5. 会话层（Session Layer）

会话层负责在两个应用进程之间建立、管理和终止会话。它通过提供同步点和会话控制等机制，实现了应用程序之间的会话管理。会话层还可以提供身份验证和加密等安全服务。

2.1.3.1.6. 表示层（Presentation Layer）

表示层负责数据的表示和编码，以确保数据在传输过程中能够被正确理解和解释。它通过数据压缩、加密、格式转换等机制，实现了数据的透明传输。表示层还负责处理不同系统之间的数据表示差异。

2.1.3.1.7. 应用层（Application Layer）

应用层是 OSI 模型的最顶层，直接面向用户和应用程序。它为用户提供了各种网络应用服务，如电子邮件、文件传输、Web 浏览等。应用层协议如 HTTP、FTP、SMTP 等定义了应用程序之间的通信规则和接口。

2.1.3.2. 与 AUTOSAR 映射关系

- 物理层和数据链路层在 AUTOSAR 中主要由 BSW 中的通信堆栈（ComStack）内的相应模块来实现。其中包括 ECU 硬件抽象层、网络管理模块等，以确保物理信号的传输和帧的正确交换。
- 网络层在 AUTOSAR 中主要涉及 BSW 的通讯服务模块，该模块负责决定数据如何在不同节点间路由和传输。
- 传输层在 AUTOSAR 中可以理解为 BSW 的 PDU 路由和 PDU 传输模块，负责端到端的数据包传递。
- 会话层和表示层在 AUTOSAR 中对应的是运行时环境（RTE）部分，包括标准接口和数据转换机制，以支持软件组件间的高级通信。
- 应用层在 AUTOSAR 模型中主要对应于软件组件（SW-Cs），它们实现具体的汽车功能，如发动机管理、车门控制等。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

2.2. 仿真测试场景分类

2.2.1. 场景分类原则

2.2.1.1. 完备性

对系统分解工作的基本要求是完备性，即不遗漏、不重叠，此原则也被称为 MECE（Mutually Exclusive, Collectively Exhaustive，相互独立，完全穷尽）法则。无论哪一个视图，都需要充分识别系统中的所有组件，并让每一个组件都归属于某一个子系统，且唯一归属于这个子系统。

2.2.1.2. 可管理

分解后得到的对象的颗粒度既不能太小也不能太大，要维持在一个可被管理的程度。如果太小，则管理成本会很高，需要大量的人力来对应。如果太大，则分解的作用就不明显了。

2.2.1.3. 高内聚低耦合

由于被分解的系统中各个组件之间存在着各种连接关系，因此当被分解为多个子系统之后，这些子系统之间就会继承内部组件之间的连接关系，从而形成子系统之间的连接关系。这种子系统之间的连接关系导致了子系统之间的相关性。

内聚指的是一个系统或模块内部的组件之间的相关性，相关性越高，内聚程度越高，系统的独立性越好，可靠性越高。耦合指的是不同系统或模块之间的相关性，相关性越高，耦合程度越高，系统的独立性越差，对其他系统的依赖程度就越高。

2.2.2. 仿真测试场景分层

在本次仿真测试研究中，从汽车研发与通信协议的角度出发，综合电子电气系统、AUTOSAR 架构、OSI 网络模型不同场景要素研究，提出了场景要素具体情况，对智能网联汽车仿真测试项目中所涉及到的测试场景进行分类，测试场景要素主要包括物理层、硬件抽象层、服务层、应用层四个层级。其中：

物理层包括外部有线接口、内部有线接口、芯片、硬件 4 类；

硬件抽象层包括协议栈、驱动、安全 3 类；

服务层包括运行时环境、通讯、存储、其他 4 类；

应用层包括系统、其他 2 类。

2.2.2.1. 硬件层

所有智能网联汽车的设计最终总是要落到各种实体零部件上才能发挥作用，而且物理实体是智能网联汽车电子电气系统中最容易被人感知的组件形式，也是对系统成本影响最大的

全国汽车标准化技术委员会 智能网联汽车分技术委员会

部分，所以对于仿真测试系统而言，与实际物理硬件层的仿真测试工作是重要的工作之一。

硬件层主要实现智能网联汽车整体逻辑架构中的车载智能终端，包括无线通信设备、外部有线接口、内部有线接口、芯片、硬件等内容。

在这一环节，需要测试车内设备安全以及车内设备的关联安全问题，确保攻击者不能控制汽车关键功能或潜在风险模块。

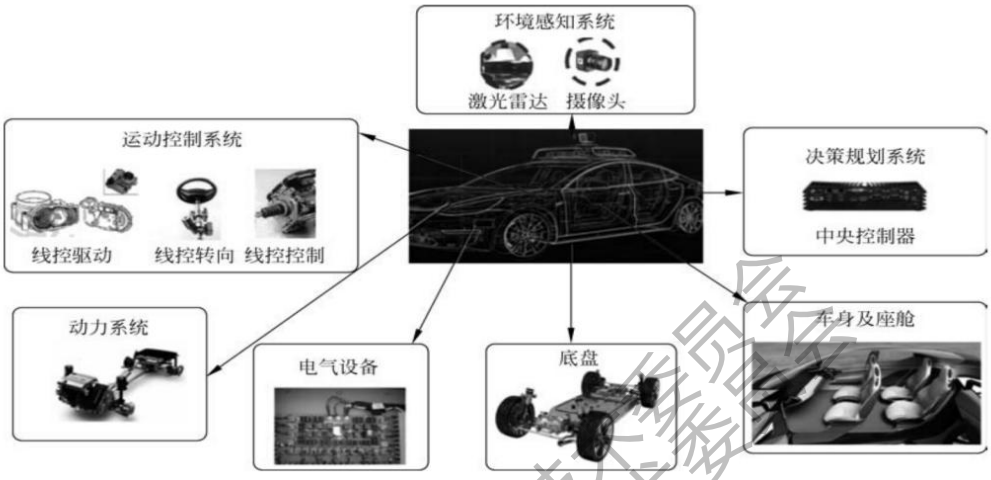


图 10 智能网联汽车组成部分

2.2.2.2. 硬件抽象层

硬件抽象层主要实现上层软件和硬件之间的接口，是一个交互层次，为其它各层提供通用的技术基础服务，包括协议栈、驱动、安全等内容，通过硬件抽象层可将硬件封装起来，负责提供统一的访问接口，实现对通信、存储器等对象的访问。

2.2.2.3. 服务层

服务层的目的在于提供给应用层可用的服务内容，主要包括：诊断、操作系统、通信、内存管理等。

服务层是智能网联汽车的服务提供部分，对于此部分的测试内容包括智能网联汽车信息服务智能终端数据传输、身份认证和云端服务安全，确保测试涵盖智能网联汽车应用运行全流程。云端服务安全即智能网联汽车远程服务提供商安全，该项测试的主要内容是远程服务器高危漏洞检测、服务器操作系统安全评估、服务器系统服务安全评估和其他服务器相关安全评估。智能网联汽车智能终端是与远程服务器直接通信的设备，对其的测试包括服务接口渗透、终端应用非法注入及检测等。

2.2.2.4. 应用层

主要包含线程调度，应用服务，与模型进行与实体无关的业务逻辑。

- 应用层位于服务层之上，它可协调多个聚合服务和领域对象完成服务编排和组合，

全国汽车标准化技术委员会
智能网联汽车分技术委员会

协作完成业务。

- 应用服务是在应用层，负责服务的组合、编排、转发、转换和传递，处理业务用例的执行顺序以及结果的拼装，以粗粒度服务通过 API 网关发布到前端。还可进行安全认证、权限校验、事务控制、发送或订阅领域事件等。

2.2.3. 仿真测试对象安全要素

2.2.3.1. 硬件安全威胁

- 印刷电路板(Printed Circuit Board，PCB)安全威胁：可能泄露集成电路芯片型号、接口电路、总线协议等信息。
- 处理器芯片安全威胁：在运行程序会泄露电磁信息、时间信息、功耗信息等侧信道信息。基于不同侧信道信息可以发起时序攻击、功耗攻击、电磁攻击。故障注入技术同样给处理器芯片带来严重的安全风险，电压故障注入、电磁故障注入、激光故障注入等攻击可以改变处理器运行逻辑。
- 存储芯片安全威胁：数据存储芯片面临数据残留威胁，Flash 存储数据可通过编程器读取。
- 硬件调试接口安全威胁：JTAG、SWD、USB 等硬件调试接口也为攻击者获取片上系统内部存储数据提供了可行性。
- 板载总线安全威胁：SPI 总线与 I2C 总线面临数据监听、数据篡改等网络安全威胁。
- 通信 PHY 和 MAC 干扰：模拟故障如短路/开路/互短、数字干扰如篡改信号电平、Bits 序列。

2.2.3.2. 固件安全威胁

汽车电子设备固件分为三类：

- 全操作系统固件：包含成熟的操作系统，应用在具有高性能与多功能需求的场景中;
- 部分操作系统固件：为满足特殊需求的实时操作系统，或者供应商定制的操作系统，完成基本的资源、任务管理等;
- 无操作系统固件：编译好的二进制指令，没有进程管理、中断响应等操作系统功能。

口令、密钥、重要的网络资源地址、用户名、邮件地址等隐私信息可能明文编码在固件中。恶意攻击者可通过逆向工程技术获取目标系统的运行逻辑。攻击者也可以访问固件中的文件系统获取具有价值的关键数据，甚至可以通过动态分析的方式分析目标固件在真实物理运行环境下是否存在网络安全漏洞。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

2.2.3.3. 总线安全威胁

智能网联汽车网络安全威胁框架中的总线安全威胁包括 CAN 总线安全威胁、FlexRay 总线安全威胁、LIN 总线安全威胁、MOST 总线安全威胁、车载以太网安全威胁。

一方面，部分车内总线为了满足车内通信对于低延时的特殊需求，在设计时缺乏基本的安全防护机制，如传输数据加密、通信认证、数据完整性校验等。

另一方面，部分车内总线应用层协议具备较强的车辆访问与控制功能，如 UDS 协议、SOME/IP 协议等。

2.2.3.4. 无线电安全威胁

无线电安全威胁，侧重于以无线传输介质为基础的物理层与链路层安全。依据不同的传输距离，智能网联汽车中使用的无线通信技术分为：

- Bluetooth 技术：面临中间人攻击等威胁；
- Zigbee 技术：用于胎压监测领域，面临传输层泛洪攻击、网络层“虫洞”攻击和选择性转发攻击、链路层拒绝服务攻击、无线电监听、篡改、阻塞攻击等威胁；
- UWB 技术：用于测算车辆位置，面临大范围数据监听等威胁；
- NFC 技术： 应用于汽车钥匙领域，面临拒绝服务、通信数据中继等威胁；
- DSRC：应用于车载通信单元，其信道的开放性面临无线通信监听威胁；
- Wi-Fi：Client 和 AP 两种模式，固件和协议均可能受到威胁；
- PC5：CV2X 应用于车载通信单元，其信道的开放性面临无线通信监听和重放威胁；
- 蜂窝网络：以 5G、C-V2X 等为代表的蜂窝网络通信技术，用于车联网通信中的“车-车”通信与“车-云”通信，面临中间人攻击、拒绝服务攻击、重放攻击等威胁。

2.2.3.5. 网络安全威胁

网络安全威胁更侧重于基于 TCP/IP 协议栈的上层网络通信安全。攻击者可能窃听网络中传输的敏感信息而获取传输内容。

2.2.3.6. 云端安全威胁

智能网联汽车与云端服务平台进行网络通信，同样面临来自云端的网络安全威胁。攻击者如果攻陷云端服务平台，不仅可以获取用户资料等隐私数据，也可以利用云端服务平台通过远程无线网络入侵目标车辆。

2.2.3.7. 应用安全威胁

在远程车辆控制场景中，应用程序也可能作为攻击跳板为智能网联汽车带来重大网络安全隐患。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

2.2.3.8. 隐私安全威胁

路线规划、智能调度等车联网服务中，车辆需要周期性广播自身状态信息，包括车辆实时位置、速度、行驶状态等关键数据。

2.2.3.9. 传感器安全威胁

智能网联汽车高度依赖传感器数据实现自动驾驶的特性为车辆引入了更广泛的攻击面与潜在的网络安全风险。

2.2.4. 仿真测试方法

2.2.4.1. 环境控制

环境控制类测试方法旨在通过外部干扰或伪造通信环境破坏车辆系统的正常运行，如表2所示。

表2 环境控制类测试方法汇总表

测试方法	描述
传感器模拟攻击	通过模拟传感器数据（如海豚音攻击、激光干扰激光雷达、投影欺骗摄像头）破坏传感器可用性。
协议降级	干扰蜂窝通信，强制降级至安全性较低的协议（如GSM）。
信号干扰	干扰汽车无线电通信，阻止正常数据传输。
中间人攻击	利用有缺陷的通信协议劫持并篡改流量。
伪基站&Wi-Fi 热点	伪造基站或Wi-Fi 热点，窃听或操纵车端与云端的蜂窝通信数据。
中继攻击	中继通信信号，使车辆误判信任设备的物理距离。

2.2.4.2. 初始访问

初始访问测试方法聚焦于攻击者如何首次侵入车辆系统，如表3所示。

表3 初始访问测试方法汇总表

测试方法	描述

全国汽车标准化技术委员会
智能网联汽车分技术委员会

售后市场/客户/经销商设备	通过非原厂设备（如第三方硬件）作为初始入侵点。
浏览器漏洞利用	利用车载浏览器漏洞，在用户访问恶意网站时获取系统访问权限。
无线电接口漏洞利用	通过无线接口（如蓝牙、Wi-Fi、GPS）发送恶意消息进行攻击。
存储介质植入恶意程序	通过 USB 等可移动介质自动运行恶意程序。
安装恶意 APP	诱导用户安装非授权 APP 以获取车辆控制权。
物理操纵	通过物理接触（如 OBD 接口、改线）直接访问或修改 ECU 数据。

2.2.4.3. 执行

执行类测试方法描述攻击者如何在系统内运行恶意代码或指令，如表 4 所示。

表 4 执行类测试方法汇总表

测试方法	描述
命令和脚本解释器	利用系统内置的解释器（如 Shell）执行任意命令。
Native API	直接调用操作系统原生 API 执行恶意操作。

2.2.4.4. 持久化

持久化测试方法旨在保持攻击者在系统内的长期存在，如表 5 所示。

表 5 持久化测试方法汇总表

测试方法	描述
利用 UDS 实现持久化	通过 UDS 服务（如固件更新、内存写入）维持恶意代码驻留。
禁用软件更新	阻止系统更新以延长恶意程序存活时间。
修改操作系统	篡改系统分区或内核，使恶意代码在重启后仍存在。
修改 TEE	将恶意代码植入可信执行环境（TEE），逃避检测。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

2.2.4.5. 权限提升

权限提升测试方法关注如何获取更高系统权限，如表 6 所示。

表 6 权限提升测试汇总表

测试方法	描述
存在漏洞的命令/服务	利用 ECU 漏洞执行恶意代码提权。
错误的系统配置	利用配置错误（如普通用户可编辑系统文件）提权。
系统内核漏洞	通过内核漏洞获取系统级权限。
SUID 提权	利用具有 SUID 属性的可执行文件提权。
Sudo 提权	利用配置不当的 sudo 权限工具提权。

2.2.4.6. 防御绕过

防御绕过测试方法针对如何规避安全防护机制，如表 7 所示。

表 7 防御绕过测试方法汇总表

测试方法	描述
绕过签名保护	安装未签名软件绕过代码验证机制。
绕过完整性保护	篡改软件完整性校验机制。
禁用防火墙	修改 ECU 防火墙配置降低防御能力。
绕过 UDS 27/29 服务	通过弱加密或暴力破解绕过 UDS 安全访问服务。
绕过强制访问控制	利用漏洞突破 SELinux 等访问控制机制。
故障注入	通过注入故障（如电源干扰）绕过安全验证。

2.2.4.7. 凭证获取

凭证获取测试方法旨在通过多种手段窃取或破解车辆系统的身份验证信息，如表 8 所示。

表 8 凭证获取测试方法汇总表

全国汽车标准化技术委员会
智能网联汽车分技术委员会

测试方法	描述
网络嗅探	监听车辆网络流量，捕获明文传输的认证凭据（如用户名、密码或会话令牌）。
文件获取	从系统文件中提取未加密或弱加密的敏感信息（如配置文件、日志中的密码）。
OS 凭证 Dump	利用工具（如 Mimikatz）从操作系统内存或注册表中转储明文或哈希形式的凭证。
输入捕获	通过伪造输入界面（如恶意键盘程序）记录用户输入的账号密码。
暴力破解	尝试枚举可能的密码组合（如字典攻击）破解账户凭证。
弱口令	利用默认密码或常见弱口令（如“admin/123456”）直接登录系统。

2.2.4.8. 发现

发现类测试方法用于探测车辆系统的漏洞、配置或敏感信息，为后续攻击提供情报，如表 9 所示。

表 9 发现类测试方法汇总表

测试方法	描述
漏洞扫描	使用自动化工具扫描 ECU 的已知漏洞（如未修补的 CVE 漏洞）。
漏洞发现	通过逆向工程或模糊测试挖掘未知漏洞（如协议解析逻辑缺陷）。
UDS 信息收集	未授权读取 UDS 诊断服务接口的配置、固件版本等敏感信息。
定位发现	通过 GPS 或蜂窝网络定位接口追踪车辆的地理位置。
服务端口扫描	扫描 ECU 开放端口（如 TCP/UDP），识别可被利用的服务（如 SSH、Telnet）。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

文件发现	遍历文件系统（如 ls、find 命令）寻找敏感文件（如密钥、日志）。
应用软件发现	枚举当前运行的进程和服务，识别潜在攻击目标（如老旧版本的中间件）。
系统信息发现	获取操作系统版本、硬件型号、补丁状态等详细信息。
网络配置发现	分析网络接口配置（如 IP 地址、路由表），定位内部网络结构。
网络连接发现	监控当前网络连接，识别与外部服务器的通信行为（如数据外传）。

2.2.4.9. 横向移动

横向移动测试方法描述攻击者在车辆网络内部扩散控制的策略，如表 10 所示。

表 10 横向移动测试方法汇总表

测试方法	描述
远程服务	通过 Telnet、SSH 等远程服务登录其他 ECU，执行跨系统操作。
利用 ECU 漏洞横向移动	利用已入侵的 ECU 作为跳板，攻击相邻设备（如通过 CAN 网关渗透动力系统）。
ECU 重新编程横向移动	通过 OTA 更新或诊断接口上传恶意固件，控制其他 ECU。
UDS 横向移动	滥用诊断服务（如 UDS 的远程执行功能）向其他 ECU 发送指令。
ECU 网络接口横向移动	利用多网卡 ECU 桥接不同网络（如车内娱乐网络与安全关键网络），突破网络隔离。

2.2.4.10. 功能影响

功能影响测试方法描述如何破坏车辆核心功能，如表 11 所示。

表 11 功能影响测试方法汇总表

测试方法	描述

全国汽车标准化技术委员会
智能网联汽车分技术委员会

滥用 UDS 影响车辆功能	通过 UDS 服务非法触发车辆功能（如紧急制动）。
拒绝服务	通过资源耗尽或逻辑漏洞瘫痪系统。
非预期的消息	发送异常消息导致 ECU 行为异常。
篡改 CAN 消息	修改 CAN 总线消息内容干扰其他 ECU。
重放攻击	重复发送历史消息触发重复操作（如重复解锁）。

2.3. 汽车仿真测试场景库构建

2.3.1. 概述

结合安全威胁模型，对不同层级的仿真测试对象（涵盖硬件、协议、服务、应用等维度）进行安全要素分析，同时对相关法律法规所带来的合规要求进行分析，根据分析结果匹配评估类型与测试方法，形成的从“仿真测试对象→安全合规要素→测试方法”的完整链路称为仿真测试场景。所有场景的有机集合构成仿真测试场景库。

本章节提出的汽车仿真测试场景构建模型以仿真测试场景分类原则、仿真测试场景分层为基础，以仿真测试对象、安全要素分析、合规分析、评估类型与测试方法为构建步骤实现仿真测试场景的系统性构建。

模型包含三层结构：仿真测试对象层、安全合规基线层、评估方法与测试方法选择层。

2.3.2. 仿真测试场景库构建模型详解

2.3.2.1. 仿真测试对象层

2.3.2.1.1. 仿真测试对象

下图 11 分类枚举了仿真测试对象：

硬件层					硬件抽象层			服务层				应用层	
无线通信设备	外部有线接口	内部有线接口	芯片	硬件	协议栈	驱动	安全	运行时	通讯	存储	其他	系统	其他
Bluetooth	有线以太网	JTAG	存储	PCB	USB	微控制器	安全启动	复杂操作系统	Bluetooth配置	日志存储	GPU访问	调试服务	浏览器
BLE	CAN	SPI	计算	雷达	Bluetooth	存储器	安全存储	实时操作系统	WLAN配置	数据存储		应用安装服务	语音服务
Wi-Fi	LIN	UART	通信	摄像头	Wi-Fi	通信	安全加解密		以太网通讯	文件访问		SSH服务	远程更新
蜂窝网络	FlexRay	SWD	能源	显示屏	BLE	I/O			CAN通讯			FTP服务	车辆控制
GNSS	USB		接口	麦克风	蜂窝网络				系统内通讯			诊断服务	胎压监测
UWB	充电接口			扬声器	GNSS				Bluetooth通讯			OTA服务	工程模式
NFC	SD卡				NearLink								车辆启动鉴权
RF（钥匙）	HDMI				NFC								投屏
DSRC	Type-C				UWB								远程控车
					CAN								车辆控制鉴权
					以太网								多媒体服务

图 11 仿真测试对象

基于分层架构原则，将测试场景划分为以下四类层级：

- 硬件层

全国汽车标准化技术委员会
智能网联汽车分技术委员会

- 通信接口：内部有线接口（CAN 总线、SPI、UART 等）、外部有线接口（以太网、USB 等）、无线协议（蓝牙、Wi-Fi、蜂窝等）
- 物理组件：芯片（存储/计算/通信芯片）、PCB、传感器（雷达、摄像头）、其他硬件设备（充电枪、显示屏）

- 硬件抽象层
  - 协议栈实现：CAN 协议栈、TCP/IP 协议栈、蓝牙协议栈等
  - 驱动模块：微控制器驱动、存储器驱动、通信驱动等
  - 安全：安全启动、安全存储、加解密模块
- 服务层
  - 基础服务：实时操作系统、复杂操作系统、运行时环境、通信服务
  - 功能服务：诊断服务（UDS）、存储服务（日志/数据存储）、安全服务（安全启动、加解密模块）
- 应用层
  - 用户功能：ADAS（AEB、ACC）、信息娱乐（IVI、语音服务）、车辆控制（远程控车、OTA 更新）、智能充电、V2X

2.3.2.1.2. 对象选择逻辑

- 根据场景选择对象：根据被测功能所属层级定位核心对象（如以太网测试需覆盖硬件层芯片、硬件抽象层协议栈）。

- 根据对象扩展测试链：以硬件层（车载以太网）为例，攻击链可纵向延伸至对应的硬件抽象层车载以太网协议栈、服务层诊断服务、应用层车载诊断软件。

2.3.2.1.3. 对象选择示例

- CAN 总线测试场景：
  - 硬件层（内部有线接口）
  - 硬件抽象层 CAN 协议栈
  - 服务层 CAN 诊断服务
- 车载以太网测试场景：
  - 硬件层
  - 硬件抽象层（TCP/IP 协议栈）
  - 服务层车载以太网诊断服务

2.3.2.1.4. 对象数据库选择示例

支持各应用层协议、中间件协议的动态通信数据库，如 vCDL、ARXML、DBC。

2.3.2.2. 安全合规基线层

全国汽车标准化技术委员会 智能网联汽车分技术委员会

在明确仿真测试对象后，需进一步确立测试活动所依据的准则与规范，即安全合规基线层的主要职能。该层次为测试评估提供了判断标准：其一为基于技术视角的安全要素，其二为基于政策法规遵循要求的合规要素。

2.3.2.2.1. 安全要素

基于安全维度模型，针对测试对象提取关键安全属性：

- 机密性

  数据传输加密强度、密钥存储隔离性、敏感信息暴露面

- 完整性

  校验算法鲁棒性、防篡改机制

- 可用性

  故障恢复能力、资源分配策略（总线仲裁、优先级抢占）

- 真实性

  身份认证机制（预共享密钥、证书链）、防伪装攻击能力

- 可追溯性

  日志审计完整性、时间戳同步机制、事件关联分析能力

2.3.2.2.2. 合规要素

- 合规性
  - 国外标准规范，例如 UN/WP.29 R155、ISO/SAE 21434
  - 国内法律法规，例如《网络安全法》《数据安全法》《汽车整车网络安全技术要求》
  - 国外法律法规，例如《通用数据保护条例》

2.3.2.2.3. 要素举例

如表 12 所示，对于车载以太网安全进行安全要素和合规要素进行分析：

表 12 车载以太网安全合规维度

安全合规维度	关键要素描述
机密性	数据泄露防护
完整性	校验码机制、防篡改设计、OTA 签名验证
可用性	故障恢复时间、抗 DoS 能力、冗余设计
真实性	双向认证机制、防重放攻击

全国汽车标准化技术委员会
智能网联汽车分技术委员会

可追溯性	日志完整性保护、可信时间戳、审计轨迹留存周期
合规性	符合 UN R155/R156、ISO/SAE 21434、GDPR 等法规要求。

2.3.2.3. 评估方法与测试方法选择层

本层基于第二层安全合规基线的分析结果，将安全要素与合规要求映射到具体测试方法，结合测试对象层级特性，形成可执行的测试方案。测试方法需覆盖安全属性的验证与合规性评估，并通过技术手段实现闭环验证。

2.3.2.3.1. 安全要素驱动的测试方法构建

- 安全要素分解：

  从第二层提取测试对象的安全属性（如机密性、完整性）及合规要求。

- 评估类型匹配：

  根据安全属性选择渗透测试或合规性评估。

- 技术适配：

  结合测试对象的层级（硬件/协议/服务/应用）选择具体测试方法。

- 场景实例化：

  设计可执行的测试用例，明确输入、预期输出及判定标准。

2.3.2.3.2. 合规要素驱动的测试方法构建

- 合规要素

  从第二层提取法规中与测试对象相关的部分。

- 评估类型

  合规性的评估类型一般就是合规性评估，同时也可能是渗透测试评估、功能安全评估、性能评估。

- 技术适配

  结合测试对象的层级（硬件/协议/服务/应用）选择具体测试方法。

  法律法规中提供的技术方案。

- 场景实例化

  设计可执行的测试用例，明确输入、预期输出及判定标准。

2.3.3. 仿真测试场景库构建流程图

全国汽车标准化技术委员会
智能网联汽车分技术委员会

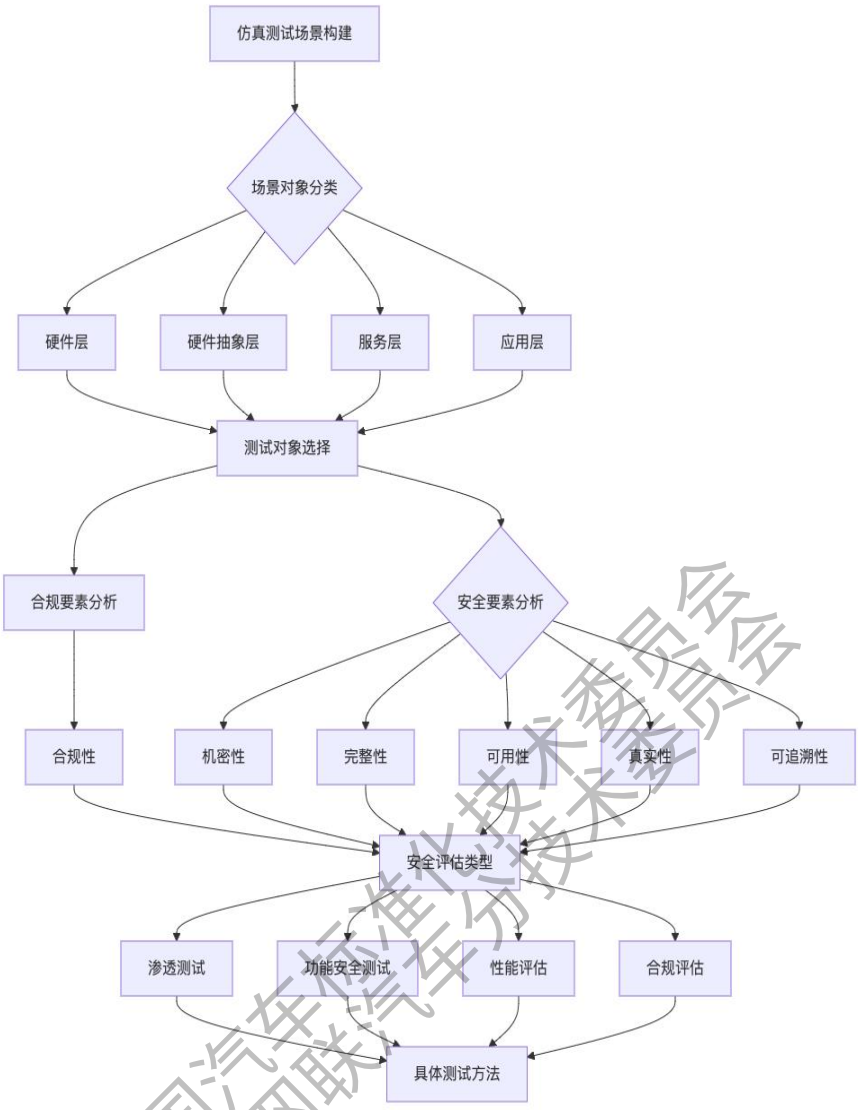


图 12 仿真测试场景库构建流程图

2.3.4. 典型应用案例

2.3.4.1. 案例 1：CAN 总线安全仿真测试场景构建

CAN 总线测试场景对象：

- 硬件层（内部有线接口）
- 硬件抽象层 CAN 协议栈
- 服务层 CAN 诊断服务

根据 CAN 总线测试对象进行安全要素分析，对分析获得的安全要素匹配对应的测试方法，形成测试方法库。CAN 总线仿真测试场景构建流程如下图 13 所示。

全国汽车标准化技术委员会
智能网联汽车分技术委

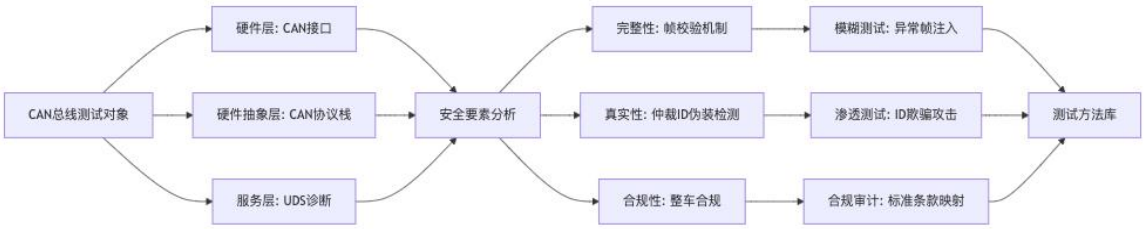


图 13 CAN 总线仿真测试场景构建流程

2.3.4.2. 案例 2：车载以太网安全仿真测试场景构建

车载以太网测试对象：

- 硬件层车载以太网硬件
- 硬件抽象层（TCP/IP 协议栈）
- 服务层车载以太网诊断服务

车载以太网测试对象的安全合规要素的测试方法构建如下表 13 所示。

表 13 车载以太网测试对象安全合规要素的测试方法

安全合规要素	关键要素描述	评估类型	测试方法
机密性	数据泄露防护	渗透测试	使用 Tcpdump 软件对车载以太网进行抓包，判断是否采用了 TLS1.2 以上的安全协议
完整性	防篡改设计	渗透测试	使用抓包软件对流量进行抓取和篡改，判断目标设备是否可以识别篡改后的请求
完整性	OTA 签名验证	渗透测试	篡改 TBOX 固件签名后刷机，判断签名验证是否生效
可用性	故障恢复时间、抗 DoS 能力、冗余设计	功能安全 性能评估	使用 DoS 测试软件通过车载以太网对 ECU 发起测试，检测测试期间设备是否运行正常，是否在结束测试后可以恢复正常运行
合规性测试	双向认证机制、防重放攻击	渗透测试	使用 Tcpdump 软件对车载以太网进行抓包，判断是否对真实性进行认证
可追溯性	日志完整性保护、可信时间戳、审计轨迹	合规性 功能安全	通过车载以太网诊断服务向目标设备发送恶意诊断消息，查看相关安全事件

全国汽车标准化技术委员会
智能网联汽车分技术委员会

	留存周期		是否被完整记录、安全保护、留存足够时间
合规性	符合 UN R155/R156、ISO/SAE 21434、GDPR 等法规要求。	合规性	通过车载以太网诊断接口向车辆发送未授权请求，查看相关请求是否被拒绝执行
合规性	《汽车整车信息安全技术要求》——7.1.1.2 要求：车辆应关闭非业务必要的网络端口。	合规性	测试人员应依据车辆生产企业提供的车辆业务端口列表，通过 Wi-Fi、车载以太网、蜂窝网络等通信通道将测试车辆与扫描测试设备组网，使用扫描测试设备测试车辆所开放的端口，并将测试得到的车辆开放端口列表与车辆业务端口列表进行比对
合规性	《汽车整车信息安全技术要求》：7.3.1.2 车载软件升级系统不应存在由汽车行业权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。	合规性 渗透测试	对车载以太网固件进行漏洞扫描，检查是否存在由汽车行业漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞

全国汽车标准化技术委员会
智能网联汽车分技术委员会

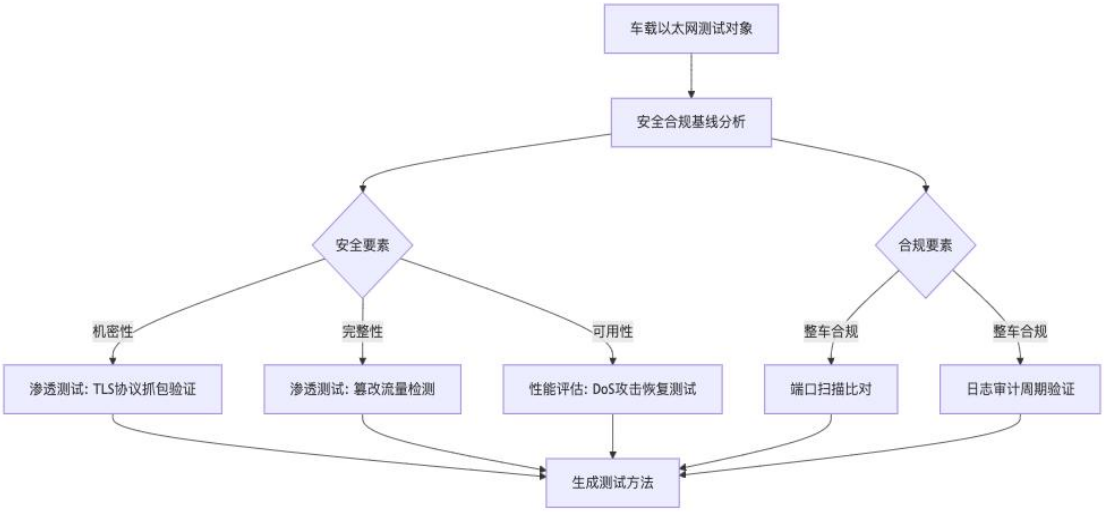


图 14 车载以太网测试场景构建流程图

全国汽车标准化技术委员会
智能网联汽车分技术委员会

3. 汽车网络安全仿真技术及评价指标

3.1. 面向网络安全的汽车整车虚拟化仿真技术

3.1.1. 整车网络安全仿真目标

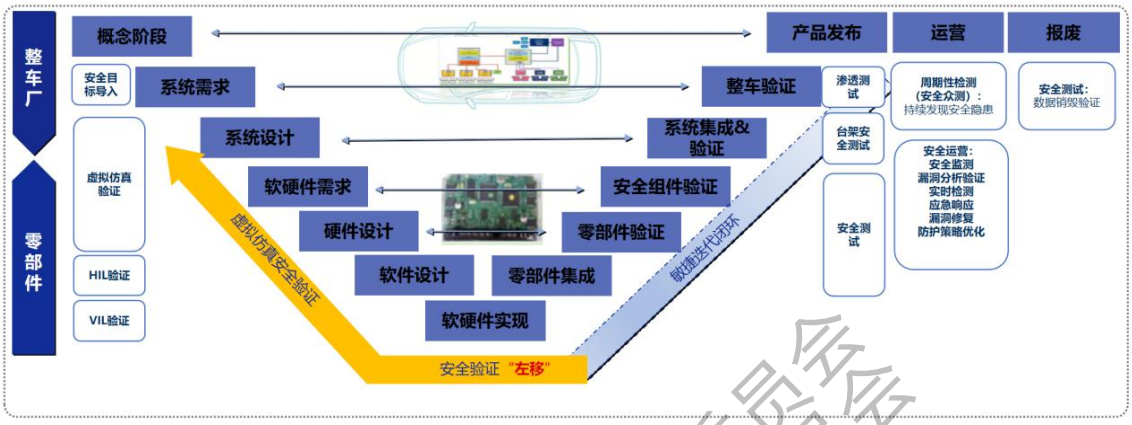


图 15 整车网络安全设计生命周期图

汽车仿真技术的应用可以通过仿真测试可以弥补实车测试的不足，实现设计缺陷的早期发现，提高测试效率，降低测试成本。另一方面，仿真测试可以覆盖更多的测试场景，特别是在一些难以在实车中实现的极端条件下，仿真测试具有无可替代的优势。同时，在网络安全领域应用仿真技术是对智能网络汽车“三支柱法”的拓展和响应。

3.1.2. 整车网络安全仿真技术架构

3.1.2.1. 汽车信息全仿真技术概述

仿真技术是一种通过计算机模型来模拟现实世界事件或系统行为的技术。在汽车网络安全领域，仿真技术被用来创建虚拟环境，以模拟和分析汽车信息系统在各种潜在威胁下的表现。这种技术允许研究人员在不影响真实车辆操作的前提下，测试和评估安全措施的有效性，从而在早期阶段发现和修复潜在的安全漏洞。

一个典型的汽车网络安全仿真平台包含多个关键组成部分。首先是仿真引擎，它是平台的核心，负责运行和管理仿真过程。其次是模型库，其中包含了各种车辆系统和网络环境的模型。用户界面提供了一个直观的操作平台，使研究人员能够轻松设置仿真参数和观察结果。此外，数据分析模块用于处理仿真产生的大量数据，提取有价值的信息。最后，安全测试和验证工具用于评估仿真结果的准确性和可靠性。

有效的仿真过程管理对于确保仿真活动的顺利进行至关重要。这包括仿真场景的设计、仿真参数的配置、仿真执行的监控以及结果的分析。在整个过程中，需要考虑到仿真的可重

全国汽车标准化技术委员会 智能网联汽车分技术委员会

复性、可扩展性和灵活性。同时，为了确保仿真结果的有效性，必须对所使用的模型和假设进行验证和校准。通过严格的管理流程，仿真可以为汽车信息系统的安全性提供有力的支持。

3.1.2.2. 系统组成

本报告提出的整车网络安全仿真技术架构如图 16 所示。按照系统功能，仿真技术架构由整车威胁场景库、汽车业务场景库、网络安全目标仿真系统、汽车网络安全模拟仿真测试分系统、基础设施资源库、汽车整车网络安全仿真综合管理平台，总计六部分组成。

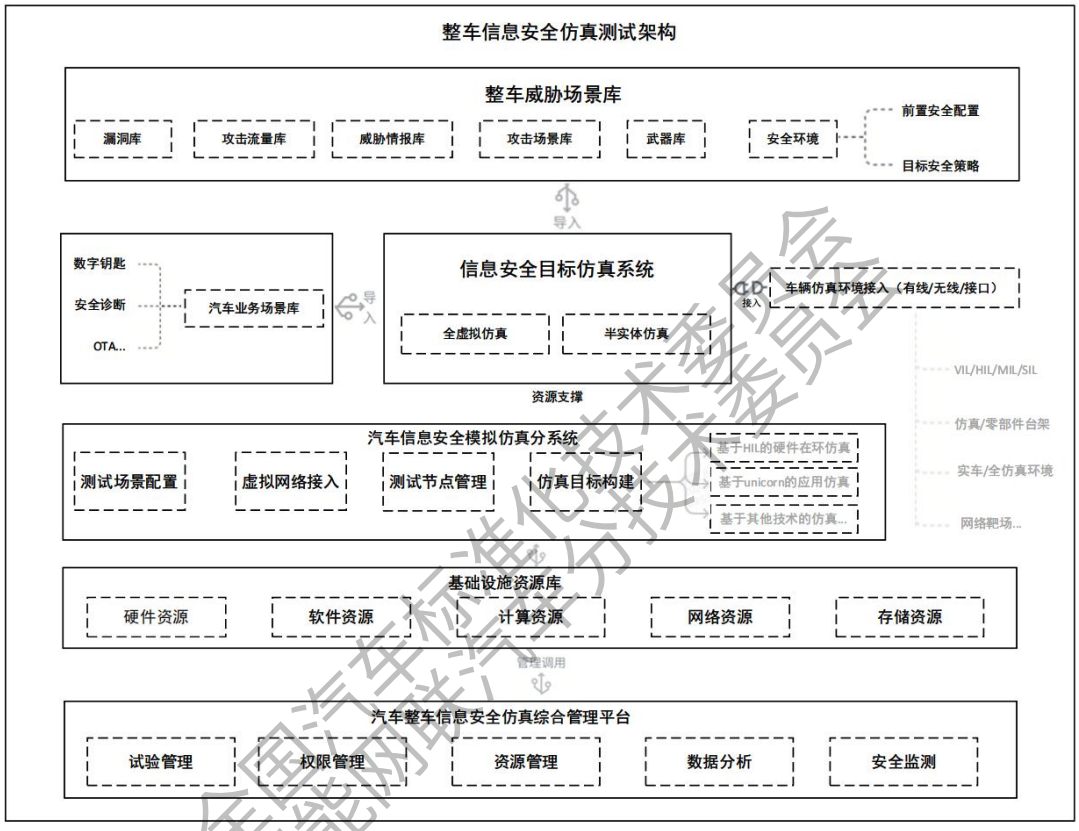


图 16 整车网络安全仿真技术架构

——整车业务场景库可依据实际应用车型的功能进行选择性加载，研究人员可自定义不同整车业务的拓扑和逻辑。

——整车威胁场景库包含漏洞库、攻击流量库、威胁情报库、攻击场景库、武器库以及安全环境，其含括了用于网络安全仿真模拟和测试的所有资源。其“安全环境”按照在仿真测试中的角色分为前置安全环境和目标安全策略两种，前置安全环境为验证安全目标提供设定的安全前提，目标安全策略与整车 E/E 架构功能逻辑仿真系统共同组成仿真测试目标。

——网络安全目标仿真系统可提供全虚拟仿真及半实体仿真两种模式。全虚拟仿真常在汽车概念阶段导入，此时不存在任何硬件实体，仅仅是针对概念阶段的整车网络架构的逻辑进行安全验证。半实体仿真则采用虚实结合的方式，在模拟仿真中引入部分真实的部件实体，如基于 T-Box、网关、IVI 等关键零部件搭建的系统台架。以真实的部件实体和低版本

全国汽车标准化技术委员会 智能网联汽车分技术委员会

的软件系统为基础构建仿真环境，对目标部件/系统的网络安全进行针对性验证和仿真。相比于全虚拟仿真可有效解决仿真周期长、成本高、难拓展、一致性差等问题。同时仿真目标可接入 VIL 等在环仿真台架。

——汽车网络安全模拟仿真测试分系统应根据试验想定方案构建试验需要的目标网络环境，通过试验场景配置、虚拟网络支撑、互联接入、试验节点管理，构建一个逼真的目标网络。同时可实现网络环境和用户行为的模拟，能够按照配置，生成网络流量和真实用户的操作行为，实现真实网络环境的模拟。

——基础设施资源库由硬件资源、软件资源、计算资源、网络资源、存储资源等部分组成。为汽车仿真系统运行提供计算性能、存储空间、网络连接基础资源。

——汽车整车网络安全仿真综合管理平台统筹管理各个系统模块，实现对仿真环境的加载和资源的灵活调配以及将功能场景按照一定时序逻辑动态地导入到整车场景中，并给予研究人员必要交互策略和功能以实现技术架构的管理。

3.1.2.3. 分系统基本功能

3.1.2.3.1. 汽车整车网络安全仿真综合管理平台

汽车整车网络安全仿真综合管理平台，能够实现各类网络节点的虚拟仿真，运行于计算集群之上，实现虚拟网络拓扑结构与计算集群底层物理网络拓扑结构的逻辑分离，能够按照目标网络的统一配置要求实现与实物网络的一体互联。分系统支持虚拟机、轻量级虚拟化等方式实现虚拟网络节点的模拟，结合虚拟网络调度管理与链路虚拟仿真技术，实现网络拓扑可灵活重构的大规模虚拟网络。

3.1.2.3.2. 网络安全目标仿真系统

网络安全目标仿真系统旨在构建用于网络安全方案验证及测试的对象，按照承载实体划分为全虚拟及半实体两种目标构建方式：

全虚拟仿真旨在汽车研发的概念阶段，在完全不借助实体部件的前提下，依据车辆的整车功能场景、逻辑架构进行网络拓扑仿真，此类仿真较为抽象，仿真难度大、真实性较差，仅仅作为初期的功能逻辑验证。

随着面向服务架构和虚拟计算基础设施的出现和应用，汽车信息系统网络环境、应用环境和安全环境变得相当复杂，构建一个同目标网络完全一致的真实网络环境周期长、成本高、难拓展、难调整；而采用全部由仿真方法来评估现有网络时，仿真网络与目标网络的差异性会对评估结果准确性产生影响。因此，采用虚实结合的半实物仿真方式，在模拟仿真中引入真实设备并导入部分真实流量，可以更快捷、更真实地对网络环境进行模拟。

全国汽车标准化技术委员会 智能网联汽车分技术委员会

搭建由仿真模型和实物组成的安全虚拟仿真环境，通过仿真网络基础平台、部分安全防护功能仿真模块以及实物中的安全功能样机构建完整的安全防护体系，为仿真业务数据及导入的真实的业务数据流提供运行环境。同时，该仿真网络环境可以作为相关的网络渗透、综合测试及系统级评估的对象。

基于半实体仿真模式，可提供针对零部件、VIL 台架和实车与仿真基础平台进行连接，提供多种访问接口，实现虚实互联。

3.1.2.3.3. 整车业务场景库

整车业务场景库收录了整车业务相关的逻辑和功能场景，诸如 OTA、数字钥匙、远程诊断等整车业务，可以以场景库导入的形式加载到仿真目标中去，进行补充和完善。

3.1.2.3.4. 整车威胁场景库

整车威胁场景库可实现数据库存储与管理、知识库存储与管理、攻防武器库存储与管理等功能。

数据库存储与管理应负责加载、清洗、存储、管理整个系统的多模态数据，并提供高性能数据查询和数据分析工具。知识库存储与管理应为网络安全知识和试验场景知识提供统一的知识表达。攻防武器库存储与管理负责管理攻击方、防御方所需要的攻防工具。

3.1.2.4. 整车数据安全仿真系统数据交互关系

1）数据采集与整合

✓ 漏洞库的构建：通过安全研究、行业报告和漏洞数据库，收集针对汽车电子系统的已知漏洞信息。

✓ 攻击流量库的建立：使用网络流量生成工具模拟各种攻击流量，如 DDoS 攻击、恶意软件传播等。

✓ 威胁情报库的更新：订阅多个安全组织的威胁情报源，自动更新最新安全威胁信息。

✓ 攻击场景库的设计：基于真实的攻击案例和假设的攻击情境，设计一系列详细的攻击场景。

✓ 武器库的整理：收集和分类常见的黑客工具和攻击方法，形成标准化的武器库。

2）数据传输

✓ 有线连接：使用以太网线缆将车辆/台架的诊断接口（如 OBD-II 接口）与仿真系统相连，确保高速且稳定的数据传输。

✓ 无线连接：利用 Wi-Fi 或蜂窝网络技术，实现车辆与仿真系统之间的远程通信。

✓ 接口标准化：制定统一的 API 接口标准，使得不同设备和系统能够无缝对接。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

3）仿真目标数据构建：

✓ 全虚拟仿真：在高性能计算平台上，利用虚拟化技术完全模拟车辆的运行环境，进行无风险的测试。

✓ 半实体仿真：结合实车的部分硬件（如传感器、控制器）与虚拟环境，进行更为逼真的测试。

✓ 仿真环境构建：根据不同的测试需求，动态配置网络拓扑、系统参数等，创建多样化的仿真环境。

4）虚拟仿真测试数据流转：

①测试准备阶段：

✓ 环境搭建：根据测试需求配置仿真环境和实际测试环境，确保所有设备和系统正常运行。

✓ 测试工具部署：安装必要的测试软件和工具，包括网络分析工具、安全扫描器等。

✓ 测试数据准备：从漏洞库、攻击流量库等中选择适当的数据，为测试提供基础。

②测试场景配置：

✓ 场景设计：基于预设的攻击场景库，设计具体的测试案例，包括攻击类型、攻击路径、预期结果等。

✓ 参数设定：根据不同的测试目标，设定相应的参数，如攻击强度、持续时间等。

✓ 环境校验：在开始测试前，对仿真环境和测试设备进行最后的检查，确保一切就绪。

③虚拟网络接入：

✓ 网络拓扑构建：根据测试需求构建虚拟网络环境，模拟真实的网络条件。

✓ 网络参数调整：调整网络的信号强度、延迟、丢包率等参数，以符合测试场景的要求。

✓ 连接验证：确保车辆与仿真系统之间的连接稳定可靠，无通信障碍。

④测试节点管理：

✓ 节点配置：配置和管理多个测试节点，确保它们能够协同工作。

✓ 任务分配：将不同的测试任务分配给各个节点，实现并行测试，提高效率。

✓ 状态监控：实时监控各测试节点的状态，及时发现并处理异常情况。

⑤仿真目标构建：

✓ 目标明确：为每个测试定义清晰的目标，如检测特定漏洞、评估防御策略的效果等。

✓ 指标设定：设定可量化的测试指标，如响应时间、成功率、资源消耗等。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

✓ 预期结果：预测测试的可能结果，并与实际结果进行对比分析。

⑥测试执行：

✓ 启动测试：按照预定计划启动测试，记录测试开始的时间和初始条件。

✓ 过程监控：实时监控测试过程中的关键指标，如网络流量、系统性能等。

✓ 数据采集：收集测试过程中产生的数据，包括日志文件、网络流量记录等。

⑦测试结束与恢复：

✓ 结束确认：在测试完成后，确认所有测试任务均已结束，并记录结束时间。

✓ 环境恢复：将仿真环境和测试设备恢复到初始状态，以便进行下一轮测试。

✓ 数据备份：对收集到的数据进行备份，以防数据丢失或损坏。

5）数据分析与闭环：

✓ 数据整理：收集所有测试相关的数据，包括原始数据、日志文件、网络流量记录等，并进行分类和归档。

✓ 深度分析：利用数据分析工具和技术，对收集的数据进行深入分析，识别出任何异常或不符合预期的行为。

✓ 问题定位：基于数据分析的结果，准确定位问题的根源，如特定的漏洞、配置错误或性能瓶颈。

✓ 报告编制：编写详细的测试报告，包括测试过程、发现问题、分析结果和改进建议。

✓ 反馈循环：将测试结果和分析报告反馈给相关的开发团队和管理层，以便进行必要的修复和优化。

✓ 闭环验证：在问题修复后，重新进行测试以验证修复效果，确保问题得到彻底解决。

✓ 知识库更新：将测试过程中发现的新漏洞、攻击手段和防御策略更新到知识库中，为后续的测试提供参考。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

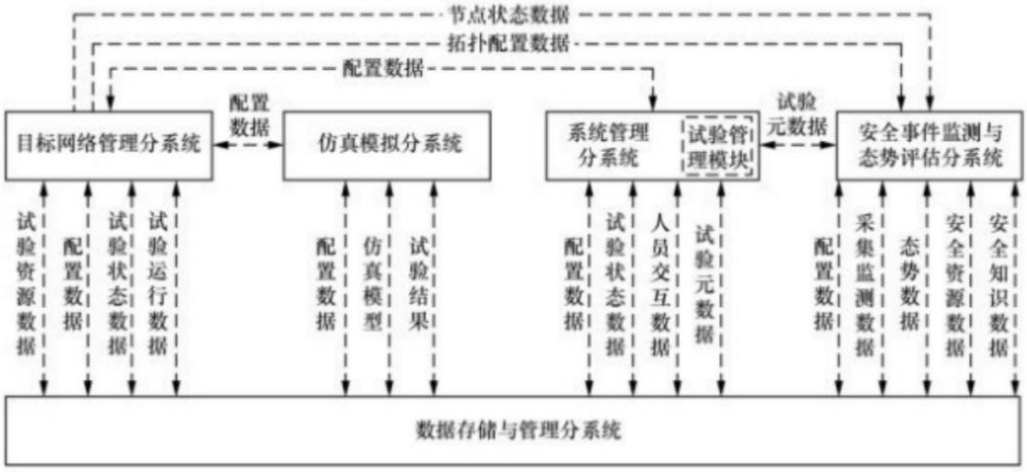


图 17 整车数据安全仿真系统数据交互关系图

3.1.2.5. 仿真技术路线现状

汽车进入智能化、网联化新阶段后，面临日益严重的网络安全风险，零部件自身的网络安全问题可能会在装配到整车后被进一步放大。因此，有必要在零部件开发过程中同步进行网络安全测试，最大程度确保其安全性，而零部件网络安全仿真有望作为网络安全测试的补充手段，以提高测试效率，降低测试成本。

3.1.2.5.1. 基于 QEMU 的仿真技术

QEMU 是一款基于 GNU（GNU's Not Unix，一款类 Unix 操作系统）通用公共许可证（GPL）协议开源的虚拟机软件，它是一个可以在任何平台上运行汇编指令级别的仿真软件，目前支持包括 X86、ARM、MIPS、RISC-V 等多种架构的 CPU 及单板的仿真。借助 QEMU，软件开发人员相当于快速得到了一块虚拟的单板，从而进行 gdb 调试、开发测试等活动（如在 X86 电脑上通过 QEMU 仿真出来的 ARM、RISC-V 单板运行 ARM、RISC-V 架构的程序），QEMU 能让程序以为自己运行在一块真实的单板上，因为 QEMU 上运行的 OS、APP 与单板二进制完全一致，无需单独构建镜像。目前，在 QEMU 上已经支持了一些商用的 SoC，并且软件开发人员也可以开发私有 SoC，为后续零部件（网络安全）仿真提供运行基础。

嵌入式程序能在单板上运行有两个前提条件，一是单板上的处理器可以识别该程序的汇编指令，二是程序中所访问的设备（如串口）在单板上必须真实存在，且与程序所期待的设备完全相符。而 QEMU 的优势是，众多开源贡献者已将世界上通用的处理器指令集以及不太常见的处理器指令集均完成了仿真开发，这在很大程度上解决了第一个前提条件，除非单板上的处理器调用了自定义的指令集，那么需要参考其他处理器的实现完成上述指令集的仿真开发。同时，QEMU 的众多开源贡献者也已经完成了常见设备的仿真开发，这些常见设备的代码可以作为范例为开发定制设备的仿真代码提供参考基础，如通过修改代码逻辑等手

全国汽车标准化技术委员会
智能网联汽车分技术委员会

段完成定制设备的开发，用来解决第二个前提条件。当完成在 QEMU 上的单板仿真开发，就可以在这块虚拟单板上进行软件开发进而开展零部件（网络安全）仿真工作了。但是，任何仿真都不可能百分百替代真实的单板，有时是为了在缺乏开发环境的情况下，提前为软件开发人员提供相应开发平台的一种补充手段。

3.1.2.5.2. 基于 Unicorn 的仿真技术

Unicorn 框架是一个轻量级、多平台、多架构的 CPU 模拟器框架，基于 QEMU 开发。它的设计目的是提供一个简洁易用的 API，使用户能够专注于 CPU 操作，而忽略底层机器设备的差异。Unicorn 支持多种架构系统，包括 ARM、ARM64(Armv8)、M68K、MIPS、SPARC 和 x86（包括 x86_64），其中 ARM、mips 平台是汽车 ECU 常见架构，并且 Unicorn 支持 Windows、Linux、BSD 和 Solaris 等操作系统部署，并且提供平台独立且简洁易用的 API，方便开发者进行仿真操作，对于仿真平台搭建、开发也具有优势。

Unicorn 支持根据汽车 ECU 固件进行仿真，并且已经有案例，如针对 Renesas RH850 架构的支持，这是一种常用于汽车 ECU 的系统芯片，已经有网络安全人员成功模拟过该 ECU 并进行测试，而且市面也有针对 Unicorn 仿真的网络安全测试工具；如 FUZZWARE，这是一个基于 Unicorn 的模糊测试系统，旨在对嵌入式固件（包括单片机固件）进行高效模糊测试。在评估中，FUZZWARE 成功发现了 Zephyr 和 Contiki-NG 等嵌入式固件框架网络栈中的多个未知漏洞，并获得了 CVE 编号，这证明了 Unicorn 在嵌入式系统固件模糊测试中的有效性。

总的来说，Unicorn 引擎作为一种通用的 CPU 模拟器框架，结合其对嵌入式系统 CPU 架构的支持，使其非常适合应用于汽车 ECU 固件的仿真和安全测试，尤其是模糊测试等自动化测试方法，相关研究工作已经证明了 Unicorn 在这一领域的实用价值。

3.1.2.5.3. 基于 Simics 的仿真技术

基于 Simics 的零部件网络安全仿真技术是一种通过虚拟环境模拟和测试汽车零部件网络安全的先进方法。Simics 作为一个高度可扩展的全系统仿真平台，能够在多个硬件架构和操作系统上运行，使得开发人员可以在虚拟环境中对汽车零部件进行全面的网络安全测试，从而提高测试效率，降低测试成本。该技术包括配置虚拟机和网络环境、安装和运行各种安全测试工具、记录和分析测试结果等步骤。通过这种方式，开发人员可以在虚拟环境中发现和修复潜在的安全问题，确保零部件的安全性和可靠性。

Simics 支持多种架构，包括 x86、ARM、MIPS 和 PowerPC 等，能够模拟从单个处理器到复杂多处理器系统的运行。其全系统仿真能力使得 Simics 不仅可以仿真处理器，还可以

全国汽车标准化技术委员会
智能网联汽车分技术委员会

仿真整个系统，包括内存、I/O 设备等，从而进行全面的系统级测试。通过快照和回放功能，开发人员可以记录仿真运行状态，并在需要时回到特定状态，方便调试和测试。此外，Simics 支持多种调试工具，如 gdb，使得开发人员可以在仿真环境中进行详细的代码调试。

总的来说，基于 Simics 的零部件网络安全仿真技术，通过创建精确的虚拟环境，能够有效地提高汽车零部件网络安全测试的效率和可靠性，如精确模拟硬件和软件的交互，支持多种处理器架构和硬件配置，提供强大的调试和监控工具等。在零部件开发早期阶段，可以使用 Simics 进行全面的网络安全测试，通过仿真复杂的系统环境发现潜在的安全漏洞，并进行应急响应和安全事件的重现和分析。

3.1.2.5.4. 基于 dSPACE 的仿真技术

基于 dSPACE 的零部件网络安全仿真技术是一种通过在真实硬件环境中进行高精度、实时仿真测试的先进方法，可以提供用于汽车电子和控制系统的硬件在环仿真解决方案。该技术利用 dSPACE 平台的强大处理能力和丰富的接口，能够在硬件在环环境中对汽车零部件进行全面的网络安全测试。通过系统搭建、模型开发、网络安全测试以及数据采集与分析等步骤，开发人员可以在 dSPACE 平台上精确模拟和测试零部件的安全性能。使用各种安全测试工具，如漏洞扫描、渗透测试和恶意软件分析，能够有效发现和修复潜在的安全问题，确保零部件在实际应用中的安全性和可靠性。dSPACE 平台支持多种接口和实时仿真，提供高精度的测试结果，能够模拟真实的运行环境和攻击场景。其强大的数据采集和分析能力，能够实时记录仿真数据，并提供详细的测试报告。该仿真技术适用于漏洞扫描、渗透测试、安全补丁测试和恶意软件分析等多种应用场景。

3.1.2.5.5. 基于硬件在环（HIL）的仿真技术

基于 NI（National Instruments）HIL 系统的零部件网络安全仿真技术，通过在仿真环境中结合实际硬件设备，实现对 ECU 的功能和安全测试。将硬件与仿真软件结合，用于测试和验证零部件在网络安全方面的性能和可靠性。这种技术通过在受控的实验环境中引入实际的硬件组件（如 ECU），并将其与虚拟仿真系统（如由 NI 提供的仿真和测试平台）连接起来，模拟真实的操作条件和环境，特别关注于测试系统在面对网络攻击、信息篡改和数据泄露等网络安全威胁时的表现。主要组件包括硬件组件（如传感器、控制器）和 NI 提供的硬件接口设备（如 PXI、CompactRIO 等），以及基于 LabVIEW 或 VeriStand 等仿真软件创建的仿真平台。整个工作流程包括系统建模、硬件接入、仿真环境设置、测试运行和结果分析，旨在验证零部件在各种安全威胁下的响应和行为。

该技术在汽车行业用于测试 ECU 在面对车载网络攻击（如 CAN 总线攻击）时的响应

全国汽车标准化技术委员会
智能网联汽车分技术委员会

能力。该技术的主要优势在于其高效性、可重复性和灵活性，能够在实验室条件下快速测试和验证系统的安全性，减少实际操作中的风险和成本，并且可以重复进行多次测试，确保结果的可靠性和一致性。然而，这种技术也面临一些挑战，如需要高度专业的知识来设置和管理复杂的仿真环境和测试脚本，高质量的 HIL 系统和仿真工具可能会有较高的成本投入，且某些实时操作和攻击模拟可能对硬件和软件的性能要求较高。

3.1.2.5.6. 基于软件在环（SIL）的仿真技术

SIL 在整个开发过程中测试软件 ECU，不依赖于硬件，采用标准验证 PC，并支持并行测试、计算机集群和云端部署，具有柔性和可扩展性。构建高精度的软件在环仿真环境需要支持不同种类的控制器，包括 AUTOSAR CP、AP 和非 AUTOSAR 控制器。通过仿真平台 PC VEOS，可以支持虚拟化控制器和被控对象模型仿真，模型基于 Simulink 和 FMI FMU 标准，具有开放性，能够与其他平台联合仿真，并支持汽车相关协议标准如 ASAP 和 XIL-API。VEOS 仿真平台还具备完全自动化操作能力，提供完全自动化脚本操作，便于系统部署和测试。控制器的虚拟化支持不同种类的控制器，包括传统嵌入式控制器、经典控制器和自适应控制器，确保高度还原的虚拟化和硬件无关代码复用。

此外，基于 MATLAB/Simulink 和 CarMaker 也可以开展 SIL 仿真，前者主要用于控制算法的设计和验证，后者主要用于虚拟测试驾驶和交通场景的仿真。

3.1.2.5.7. 基于 VEOS 平台的混合技术的仿真技术

在仿真过程中，通过共同的工具链实现 SIL 和 HIL 的无缝复用，早期集成测试和持续集成提高了集成效率和质量，避免大爆炸式集成，加速软件测试和上市时间。仿真平台 PC VEOS 支持不同种类的控制器虚拟化，从代码生成虚拟控制器（包括 AUTOSAR 和非 AUTOSAR 控制器），并在 SIL 环境中进行测试。工具链软件如 ControlDesk、MotionDesk 和 AutomationDesk 支持实验管理、动画显示和自动化测试，确保在早期 PC 上对 ECU 软件和功能进行验证。通过这种方式，VEOS 可以实现 80%的 ECU 软件测试，早期集成测试和持续集成可以提高集成效率和质量。

3.1.2.5.8. 基于 CANoe 的安全仿真技术

安全仿真技术以“总线通信-系统互联-XIL Tesing-CICT”的多层架构为核心，通过虚拟化与实时仿真技术的融合，实现智能网联与车载电子系统的全生命周期信息安全验证。

CANoe 作为汽车电子系统仿真测试的核心平台，基于数据库驱动的通信模型，通过导入 DBC/ARXML/vCDL 等数据库文件自动构建包含网络拓扑和通信矩阵的虚拟环境，满足 CAN/CANFD/CANXL、Ethernet、FlexRay、DDS、V2X、HTTPs 等多总线协议，通过 CAPL、

全国汽车标准化技术委员会
智能网联汽车分技术委员会

Python 或 C#编写的仿真节点模拟真实 ECU 的通信行为与逻辑交互，并借助 Interaction Layer 实现节点与总线的精确同步，并可依据内嵌模糊测试生成器实现安全鲁棒性验证。

通过 ECU 虚拟化与安全模型仿真，实现对安全机制、密钥生命周期与算法逻辑的早期验证；结合信号仿真与故障注入功能，重现电气层与总线层攻击场景，评估系统防护能力与安全冗余设计。CANoe 中 SIL Kit 实现跨平台的虚拟化互联与时间同步，支持分布式安全协同测试，基于 vVIRTUALtarget SE 生成 AUTOSAR 软件虚拟化，为安全功能软件验系统实现闭环验证。

同时，结合 CI/CT 持续集成与测试理念，将安全测试驱动开发，可通过 CANoe Server Edition 云端平台支持跨平台 CLI 自动化构建、回归与安全验证，配合 VT/VIO System 硬件实现电气层故障注入，形成了从总线通信到系统应用层的完整仿真解决方案，为智能网联汽车的全生命周期开发与验证提供了强大支撑。

3.2. 汽车网络安全威胁评估仿真技术

3.2.1. 威胁分析与风险评估

汽车网络安全威胁分析和风险评估(Threat Analysis and Risk Assessment，TARA）主要通过识别汽车的网络资产，分析其的潜在安全威胁，综合考虑威胁攻击可行性、危害影响等因素，识别出车辆/零部件/业务可能存在的网络安全风险，并确定其风险等级，为网络安全正向开发、安全漏洞修复提供依据。汽车网络安全威胁评估工作可在车辆的全生命周期的各个阶段开展，目前国内外各汽车生产厂商通常选择在概念阶段进行整车/零部件/业务的网络安全风险威胁评估，作为整车网络安全设计的重要参考指标；也可选择在车辆开发后期从整车/业务维度进行网络安全威胁评估，确定网络安全风险等级，为后续安全防护技术应用提供技术支撑。TARA 分析的主要流程如图 18 所示。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

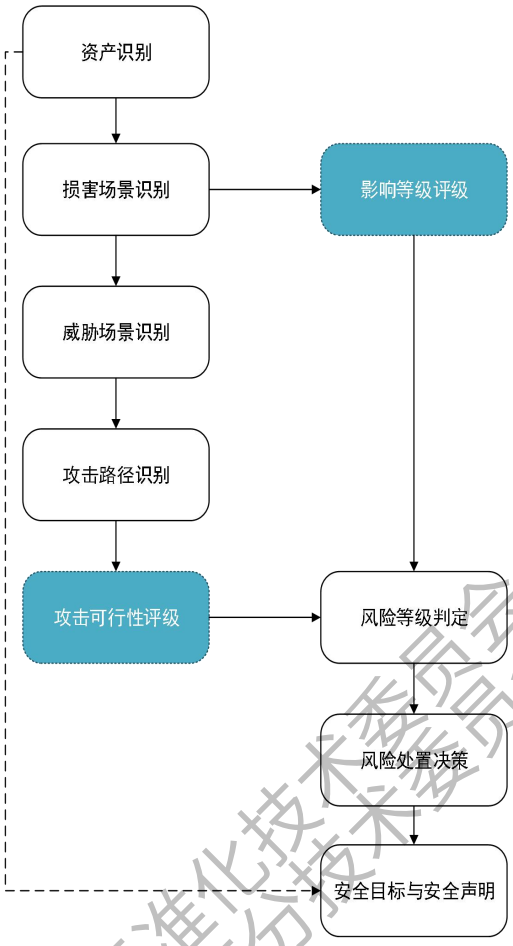


图 18 TARA 分析流程图

资产识别是识别出整车及系统对象中的网络安全资产，并确定资产对应的网络安全属性，在网络安全属性确认方面，可以使用微软的 STRIDE 模型，将威胁（欺骗、篡改、抵赖、信息泄露、拒绝服务、特权提升）映射为真实性、完整性、不可抵赖性、机密性、可用性和权限属性。

损害场景识别需要识别出安全资产的某项安全属性被损害时，会对道路参与者产生怎样的不良后果。

影响评级从安全、财务、操作和隐私（S、F、O、P）四个维度评估损害场景发生时对道路参与者造成不利的影响。如果有这四类以外的影响，也应该记录在文档中。每个维度的评级分为四档：严重的、重大的、中等的、可忽略的。影响等级的计算方式是从四个评分维度（S、F、O、P）中取最大的一个值。下表给出了影响程度评估方法。

全国汽车标准化技术委员会
智能网联汽车分技术委

表 14 评分标准表

评分维度	影响等级	安全影响评估标准
安全 Safety	严重	危及生命的伤害，致命的伤害
	重大	重伤和危及生命的伤害
	中等	轻度和中毒伤害
	可忽略	无伤害
财产 Financial	严重	财务损失会导致受影响的利益相关者无法承受的灾难性后果
	重大	财务损失会导致受影响的利益相关者可以承受的重大后果
	中等	财务损失会导致受影响的利益相关者可使用有限的资源以承受的不便后果
	可忽略	财务损失会导致无影响，可忽略的后果，或与利益相关者无关
操作 Operational	严重	操作损失会导致车辆无法工作，从非预期运行到车辆无法操作
	重大	操作损失会导致车辆功能丢失
	中等	操作损失会导致车辆功能或性能的部分下降
	可忽略	操作损失不对车辆功能或性能产生影响，或明显的影响
隐私 Privacy	严重	隐私损失会对道路参与者造成显著或甚至不可逆的影响。在这种情况下，关于道路参与者的信息是高度敏感的，并且易于关联至个人身份信息主体
	重大	隐私损失会对道路参与者造成重大影响。在这种情况下，关于道路参与者的信息是： a) 高度敏感且难以关联至个人身份信息主体，或 b) 敏感且易于关联至个人身份信息主体。
	中等	隐私损失会对道路参与者造成极大不便。在这种情况下，关于道路参与者的信息是： a) 敏感但难以关联至个人身份信息主体，或 b) 不敏感但易于关联至个人身份信息主体。
	可忽略	隐私损失对道路参与者不会造成影响，或会造成些许不便。在这种情况下，关于道路参与者的信息是不敏感的，并且难以关联至个人身份信息主体。

威胁场景识别是识别出可能导致资产受到损害的场景，威胁场景描述了资产被破坏可能的原因，例如篡改车辆位置信息导致位置信息的完整性丧失，从而导致自动驾驶功能异常。

攻击路径分析针对威胁场景，分析可能实现该威胁场景的路径，分析可基于已知的漏洞，攻击案例，漏洞分析结果等历史经验，一个威胁场景可能对应多个攻击路径。

在 21434 中采纳了 CVSS 3.0 中可利用度的度量标准，评估攻击路径的攻击可行性。CVSS 全称 Common Vulnerability Scoring System（通用漏洞评分系统），是由 NIAC 开发，FIRST 维护的一个评估漏洞严重程度的评价体系。该方法主要从攻击向量、攻击复杂性、权限要求和用户交互四个维度进行评估。每个维度的度量标准见下表：

全国汽车标准化技术委员会
智能网联汽车分技术委员会

- 攻击向量（V）

表 15 攻击向量维度评定标准

分值	0.85	0.62	0.55	0.2
评定标准	远程网络 可远程利用，即此脆弱组件可被一个以上网络跃点的距离进行攻击。	相邻网络 攻击仅限于同一共享物理或逻辑网络，如蓝牙、Wi-Fi 等。	本地 攻击者只能通过本地读/写进行攻击，或攻击者可以在本地登录	物理 攻击者只能通过物理方式接触和操作组件

- 攻击复杂度（C）

表 16 攻击复杂度维度评定标准

分值	0.77	0.44
评定标准	低复杂度 攻击者可以随意攻击，不存在惩罚机制	高复杂度 攻击无法随意完成，攻击者需要对脆弱组件投入大量的准备

- 权限要求（P）

表 17 权限要求维度评定标准

分值	0.85	0.62	0.27
评定标准	无权限要求： 攻击前无需授权	低权限要求： 攻击前需要拥有用户权限	高权限要求 攻击前需拥有管理权限才能进行攻击

- 用户交互（U）

表 18 用户交互维度评定标准

分值	0.85	0.62
评定标准	不需要任何用户交互就可以攻击脆弱组件	需要用户采取一定措施才能攻击脆弱组件

CVSS 可利用性：E=8.22*V*C*P*U

根据表 19，可将计算出来的 CVSS 可利用性隐射到对应攻击可行性值.

表 19 CVSS 可利用性到攻击可行性隐射表

CVSS 可利用性值（E）	攻击可行性评级	攻击可行性
0.12-1.05	很低	1
1.06-1.99	低	2
2.00-2.95	中	3
2.96-3.89	高	4

对于每个威胁场景，应根据相关危害场景的影响和相关攻击路径的可行性，确定一个风险值。如果一个威胁场景对应多个危害场景，可为每个危害等级确定一个风险值。如果一个

全国汽车标准化技术委员会
智能网联汽车分技术委员会

威胁场景对应多条攻击路径，可以取攻击可行性的最大值。

表 20 风险值对应表

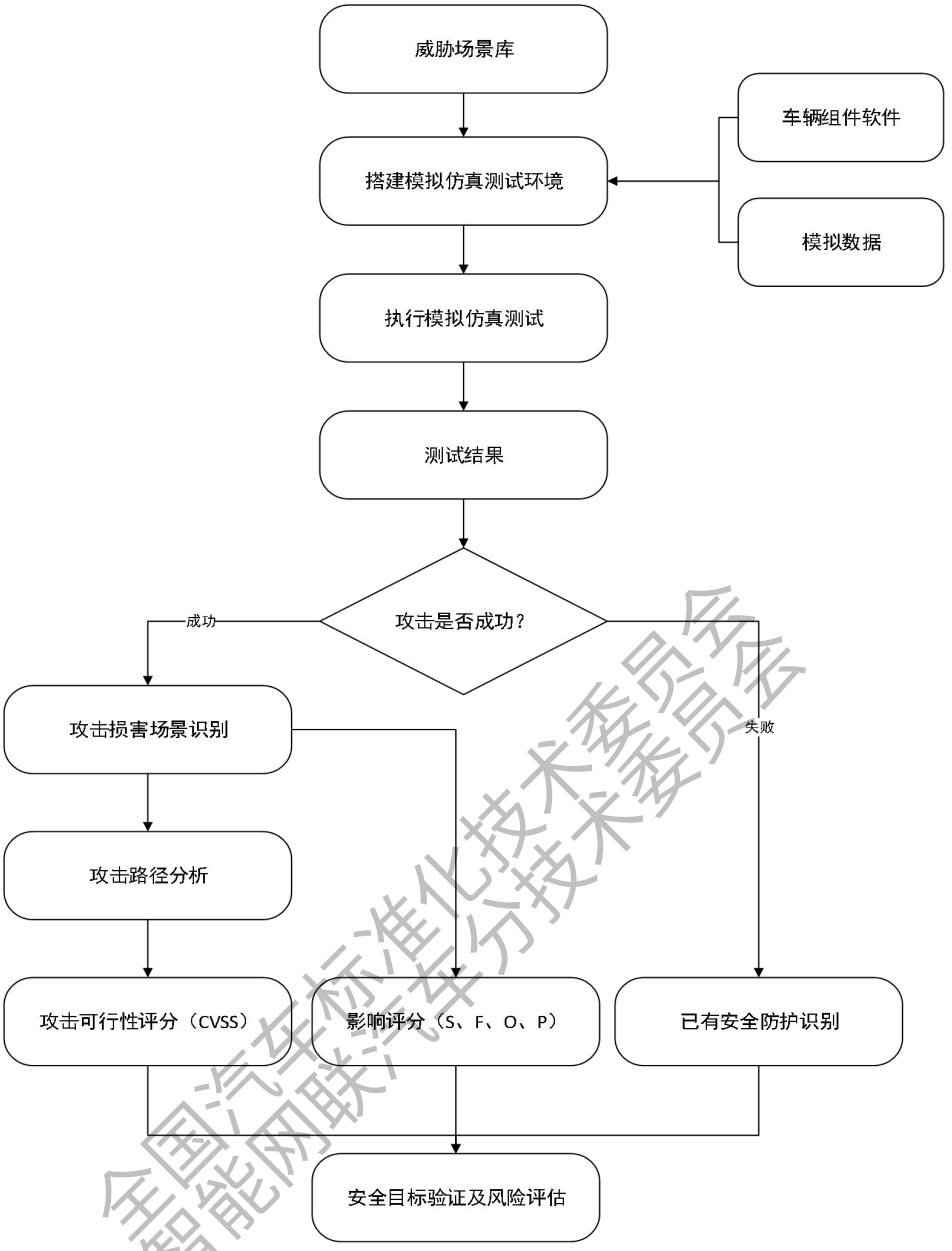
		攻击可行性			
		非常低	低	中	高
影响等级	严重	1	3	4	5
	重要	1	2	3	4
	中等	1	2	2	3
	可忽略的	1	1	1	1

3.2.2. 威胁场景仿真测试评估

在汽车网络安全威胁分析和风险评估中，仿真技术作为一种高效且安全的系统方法，不仅为测试业务闭环搭建提供了创新的解决方案，还为安全攻击路径的模拟开辟了新的思路。该技术的应用使得汽车制造商和安全专家能够在不影响实际车辆的情况下，模拟伪造指令和数据篡改等攻击情景，深入了解系统的脆弱性和潜在的安全风险，从而评估车辆系统的防护能力。

在汽车全生命周期右侧，即车辆测试阶段，可以使用虚拟仿真技术，通过软件进行仿真测试便可达到对车辆网络安全进行测试评估。可以基于第 2 章威胁情报库进行仿真模拟攻击，根据 3.3.1 的 TARA 方法论中从安全、财务、操作和隐私（S、F、O、P）四个维度评估损害场景发生时对道路参与者造成不利的影响，进行影响评级；另外，根据测试结果也可以对攻击可行性进行评估。

全国汽车标准化技术委员会
智能网联汽车分技术委员会



全国汽车标准化技术委员会
智能网联汽车分技术委员会

图 19 威胁仿真测试评价流程

3.2.3. 汽车网络安全威胁评估

3.3.1 章节是基于 ISO/SAE 21434 中 TARA 方法论，在车辆生命周期左侧概念设计阶段，通过识别整车系统的网络安全资产，确定资产对应的网络安全属性，识别出该项资产的某项安全属性被损害时，会对车辆功能、车辆使用者和道路参与者产生怎样的不良后果，例如“车辆位置信息”完整性受到损害，导致车辆无法获得正确的位置信息。影响评级可以从安全、财务、操作和隐私（S、F、O、P）四个维度评估损害场景发生时对道路参与者造成不利的影响。TARA 方法论是在 V 型模型左侧概念阶段，基于逻辑场景进行分析，从而对威胁场景的风险等级进行评估。

3.3.2 章节是通过虚拟仿真的方式测试出威胁场景库中影响等级、攻击可行性等级，在 V 型模型右侧测试验证阶段。而虚拟仿真测试的结果可以进一步验证或评估 TARA 过程中损害场景、攻击可行性等级，使得 TARA 方法论在 V 型模型左侧车辆概念设计阶段，能提高威胁分析评估的准确度。

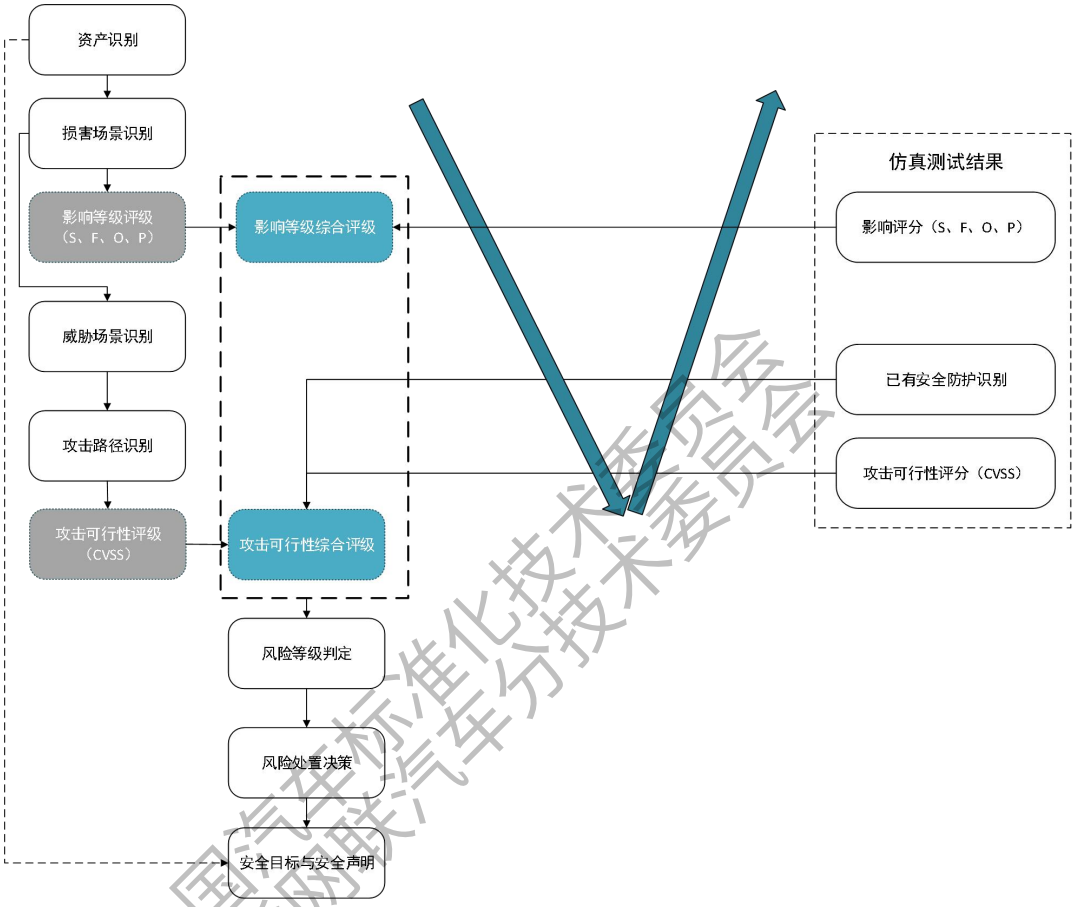


图 20 基于仿真测试的威胁分析风险评估流程

在车辆开发中，V 型模型的迭代过程可能因为需求变更、设计调整或其他因素而需要重复。每次迭代都可能涉及返回到 V 型模型的左侧（开发过程）的某个阶段，进行必要的修改，然后再继续通过测试阶段。这种迭代过程有助于逐步完善系统，确保最终产品的质量。

3.2.4. TARA 在 V 型模型中的应用

TARA（Threat Analysis and Risk Assessment，威胁分析和风险评估）作为功能安全和网络安全的核心活动，在 V 型模型的左侧（设计阶段）和右侧（验证阶段）均有重要应用。在 V 型模型的左侧，TARA 用于驱动安全需求定义和架构设计，确保威胁分析结果直接转化为系统设计约束。在需求分析阶段，基于车型电子电气架构识别关键资产（如 ECU、CAN 总线），可以参考仿真测试对象（2.2.3 章节），结合 STRIDE 模型或攻击树分析威胁场景

全国汽车标准化技术委员会
智能网联汽车分技术委员会

（如数据篡改、未授权访问），并利用仿真测试对象（2.2.3 章节）与仿真测试方法（2.2.4 章节）建立威胁库，输出威胁清单与风险矩阵，定义安全目标（如通信完整性、固件防篡改）。在架构设计阶段，集成硬件安全模块（HSM）、入侵检测系统（IDS）等机制，同时分析跨域接口（如以太网）的协同攻击风险，确保架构设计覆盖多节点攻击链。

在 V 模型右侧，TARA 通过攻击场景复现与残余风险评估实现安全机制闭环验证。基于威胁清单设计测试用例，结合仿真测试场景（2.2.2 章节），利用 HIL 测试、总线攻击模拟（CANoe）及渗透工具（Kali Linux）复现攻击，验证加密算法、安全启动等机制的有效性。测试结果更新 TARA 风险矩阵，完成 UNECE R155/R156 等法规的合规性验证（如 OTA 签名、事件响应），最终证明系统风险可接受且满足车规要求。

TARA 通过 V 模型的对称性实现端到端安全闭环，左侧将威胁转化为设计约束，右侧通过场景验证确保需求落地。将 TARA 工具与合规标准融合推动功能安全与网络安全的深度协同，成为智能汽车规避系统性风险、提升安全韧性的核心方法论。这种从“威胁分析”到“安全验证”的完整链路，不仅满足法规强制要求，更引领行业从“合规驱动”向“韧性驱动”的安全范式升级。

3.3. 汽车网络安全仿真攻击构建方法

基于 ATT&CK 框架，构建面向汽车网络安全仿真攻击。下文基于技术架构和技术实现路径两方面对构建方法过程进行了描述。

3.3.1. 基于 ATT&CK 模型的仿真攻击技术架构

（1）ATT&CK 框架适配

ATT&CK 框架是由 MITRE 公司开发的，提供了一套详尽的攻击技术和策略库。为了将 ATT&CK 框架有效应用于汽车网络安全领域，需要进行适配。首先，定义汽车系统中的攻击面，包括车载网络（如 CAN、LIN、FlexRay）、控制单元（ECU）以及外部接口（如 USB、无线通信）。这些组件和接口是攻击者可能利用的目标。利用攻击面，构建与汽车系统相关的攻击方法库。ATT&CK 框架中的技术（TA）和策略（TTPs）需要根据汽车系统的特性进行调整和扩展。例如，汽车中的远程控制、诊断接口和软件更新机制都是攻击者可能利用的目标。将这些技术映射到汽车系统中，可以生成针对汽车的攻击技术库。

（2）攻击路径建模

攻击路径建模是基于 ATT&CK 框架构建攻击路径组合的核心步骤。首先，定义攻击链模型，将 ATT&CK 中的攻击技术与汽车系统组件映射起来。这些攻击链描述了攻击者从初

全国汽车标准化技术委员会
智能网联汽车分技术委员会

始访问到最终目标的潜在路径。例如，攻击者可能通过物理访问、网络攻击或软件漏洞获得对车辆控制单元的控制。

随后，进行威胁建模。结合汽车的具体威胁模型，识别可能的攻击路径。这可以通过分析汽车系统的设计和功能来完成。例如，远程控制接口可能存在被攻击的风险，或者某些 ECU 可能因未修补的漏洞而暴露于攻击之下。

（3）攻击路径组合

为了模拟不同的攻击场景，需要生成各种攻击路径组合。这可以通过路径组合算法来实现。这些算法通常利用组合数学和图论技术，考虑攻击技术的顺序和组合，从而模拟攻击者的行为模式。攻击路径组合的生成应考虑以下因素：

攻击技术的依赖关系：某些攻击技术可能依赖于其他技术的成功执行。需要根据这些依赖关系生成合理的攻击路径。

系统状态和配置：攻击路径的有效性可能受系统状态和配置的影响。例如，某些攻击路径可能在系统更新后失效。

最终，根据实时威胁情报和系统状态动态调整攻击路径组合。通过集成实时数据流和态势感知技术，可以实现对攻击路径的动态优化和调整。

3.3.2. 技术实现路径

（1）信息收集

在构建攻击路径组合之前，需要收集系统的详细信息。首先，收集汽车系统的硬件配置、通信协议、软件版本等。这些信息有助于精确构建攻击路径模型。例如，了解汽车控制单元的具体型号和通信协议，有助于识别潜在的攻击点。

其次，整合已知的漏洞数据库和安全报告。这些数据库和报告提供了已知的漏洞信息，有助于识别可能的攻击点。例如，某些 ECU 可能存在未修补的漏洞，攻击者可以利用这些漏洞进行攻击。

（2）攻击路径模拟

攻击路径模拟是验证攻击路径组合有效性的关键步骤。首先，使用建模工具（如 UML、SysML）绘制汽车系统架构，并将 ATT&CK 框架中的攻击技术映射到系统组件。这些工具可以帮助可视化攻击路径，识别潜在的攻击点。

其次，创建模拟环境，通过攻击模拟工具（如攻击模拟平台、仿真器）来测试不同攻击路径的有效性。例如，可以使用仿真器模拟攻击者对汽车控制单元的攻击，并验证攻击路径

全国汽车标准化技术委员会
智能网联汽车分技术委员会

的实际效果。

（3）测试与优化

在模拟环境中执行攻击测试，验证攻击路径组合的实际效果。这包括测试不同的攻击策略和技术组合。例如，可以测试通过远程控制接口攻击 ECU 的效果，以及通过物理访问攻击车辆控制系统的效果。

根据测试结果优化攻击路径组合，改进攻击模型。优化过程包括调整攻击路径的顺序、修改攻击技术的配置，以及根据测试结果更新攻击模型。可以提高攻击检测和防御能力。

（4）自动化和集成

开发自动化工具来生成和测试攻击路径组合。自动化工具可以提高效率，减少人工干预。例如，开发自动化脚本来生成攻击路径，并自动执行攻击模拟测试。

3.4. 汽车网络安全仿真更新策略评估方法

随着智能网联汽车技术的发展，网络安全问题倍受关注。为保障汽车网络安全仿真系统性能，制定合理的仿真更新策略变得尤为重要。本章节旨在提供一套汽车网络安全仿真系统更新策略评估方法，考量其更新内容、时机等方面，评估汽车网络安全仿真系统的环境、参数等信息动态更新方式及规则，以指导汽车网络安全仿真的实施和优化，确保在软件及硬件等更新后，能够有效评估其载体的准确性、稳定性、系统性能、可追溯性、可恢复性、指定版本仿真、兼容性等关键指标，以及样品（数据库、攻击方法等）的及时性、攻击效果验证、覆盖率、有效性及法规适配性等关键指标，为仿真模型能力提供有力支撑。

仿真更新策略是仿真环境、参数等信息动态更新的方式和规则。目的是提高方针的准确性、效率等参数。仿真更新策略包括更新的内容、更新的时机、更新的方法。仿真更新策略的评估方法即是对上述仿真更新策略效果的评估方法。

3.4.1. 载体

3.4.1.1. 准确性

准确性是对仿真模型精度和可信度的评估。汽车仿真模型的准确性评估包括仿真与真实车辆的通用数据、通信安全、软硬件升级、数据安全及其他关键参数*数量。仿真模型须能够真实反映在不同工况条件下的表现，确保仿真结果与实际情况相符，策略更新后的软件和硬件要求能够正常执行预期功能，确保更新后仿真模型性能、场景覆盖度、问题修复等方面不受影响，准确性与更新前保持一致或有所优化。具体内容包括但不限于以下方面：

身份认证：评估更新前后身份认证机制的变化，包括认证强度、认证流程的简化或复杂

全国汽车标准化技术委员会
智能网联汽车分技术委员会

化等。

密钥管理：检查密钥的生成、分发、存储和销毁过程是否安全，是否有优化。

数字证书：评估数字证书的更新、撤销和管理流程是否符合安全标准，是否有改进。

*注：具体关键参数需参考不同的场景进行判定。

3.4.1.2. 稳定性

稳定性评估应聚焦于仿真系统在不同网络环境和硬件配置下的表现，包括数据传输的稳定性、系统在高负载条件下的运行可靠性、协议层面的抗干扰能力等。此外，还应重点测试在通信协议更新、系统迭代过程中，仿真系统的适应性及稳定性，确保仿真测试不会因系统不稳定而影响测试结果的准确性。具体内容包括但不限于以下方面：

网络延迟和数据包丢失：评估更新后的仿真模型在网络通信方面的表现，重点关注网络延迟和数据包丢失率。通过模拟不同网络条件，如高负载和低带宽情况，来测试仿真模型的响应时间和数据完整性；

系统崩溃和死锁问题：检查更新后的仿真模型是否在任何情况下都避免了崩溃和死锁现象。通过 MTBF 评估系统崩溃和锁死的频率，确保在各种条件下系统的稳定性。

无线通信协议的稳定性：评估仿真模型是否遵循了正确的通信协议初始化步骤和要求，评估无线通信协议在不同条件下的性能表现，关注重点包括但不限于抗干扰能力、丢包率、时延等综合考量以全面评估无线通信协议的稳定性。

有线通信协议的稳定性：在多 ECU 的环境中，评估有线通信协议在传输中是否稳定，关注重点包括但不限于吞吐量、延迟、数据传输抖动、错误率、多节点不产生环路、总线仲裁、传输优先级和地址分配等综合考量以全面评估有线通信协议的稳定性。

3.4.1.3. 性能评定

性能评定是对仿真系统中的关键性能指标做出评定，主要关注但不限于仿真系统在动态环境中对输入变化的响应速度，以及仿真结果与实际系统行为之间的时间同步，综合考虑响应时间、数据处理能力、仿真与现实的同步性、及时反馈机制及性能验证等因素。通过对更新前后系统的各项关键性能指标进行监测与对比，确保更新保持性能不变或更新后的系统性能有所提升。

3.4.1.4. 可追溯性

可追溯性是对汽车网络安全仿真系统在测试过程中的记录和追踪能力的评估。有效的可追溯性不仅有助于确保测试过程的透明性，还能在出现问题时提供必要的信息以进行分析和排查。评估可追溯性时，应根据实际情况考虑关键参数记录、操作步骤跟踪、过程记录颗粒

全国汽车标准化技术委员会
智能网联汽车分技术委员会

度、关键内容等，确保可追溯性在更新后性能不变或更新后的可追溯性性能有所提升。

3.4.1.5. 可恢复性

可恢复性是对汽车网络安全仿真系统在遭遇意外事件或安全威胁后恢复能力的评估。有效的可恢复性能够确保在系统出现故障或受到攻击后，快速且有效地恢复至升级前可用版本或初始版本。评估可恢复性时，应关注故障检测能力、恢复策略、备份机制、恢复时间目标（RTO）、恢复点目标（RPO）等。确保每次更新经过充分验证能在出现问题时迅速恢复到安全状态。

3.4.1.6. 指定版本仿真

指定版本仿真是对系统具有切换特定的旧版软件系统来适配旧版本车型执行测试的能力。例如，为了验证旧车型的功能和安全性，需要在旧版本的系统环境中进行攻击测试仿真，系统能够迅速切换到先前的版本，以适配不同车型的测试场景需求，提升系统的灵活性，确保测试过程的高效和可靠。更新后需保证系统版本切换的可用性和有效性。

3.4.1.7. 兼容性

兼容性是对汽车网络安全仿真系统、仿真系统与测试对象之间的兼容能力，确保更新后的系统能够在不同的操作系统或计算环境中运行，保证其功能的一致性。同时，确保针对不同车型、软件版本和硬件组件的交互和协作。满足仿真系统对各种车型和配置的条件，包括对不同通信协议、数据格式和功能特性的适配，以满足不同测试需求。

3.4.2. 信息资源

3.4.2.1. 及时性

及时性是确保漏洞库能够实时更新，以反映最新的安全威胁和漏洞信息。利用自动化工具定期检查漏洞库，从安全研究机构、漏洞披露平台等来源获取信息，确保其与最新的安全威胁数据库（如 CVE、NVD、NVDB-CAVD、CNVD、CNNVD 等）保持同步。为实现漏洞库实施版本控制，应记录每次更新的内容和日期，以便追踪历史变更，及时更新其相关的安全问题和攻击方法。

3.4.2.2. 攻击效果验证

确保仿真环境更新后进行针对漏洞库中记录的漏洞进行验证测试。通过针对特定更新后漏洞的模拟攻击，观察仿真系统在受到攻击时的效果及反应，并记录相关数据进行分析，可用于现实中不同车型漏洞的攻击效果验证对比。

3.4.2.3. 覆盖率

全国汽车标准化技术委员会
智能网联汽车分技术委员会

覆盖率是评估仿真测试有效性的重要指标，旨在确保仿真环境在更新后能够全面反映潜在的安全威胁。通过比对汽车行业权威漏洞平台如车联网产品专用漏洞库、NVDB-CAVD、CNVD、CNNVD 等政府主管部门认可的其他漏洞平台中的攻击方法、漏洞类型的系统评估，以确保仿真环境的全面性。

3.4.2.4. 有效性

有效性是指针对漏洞库和攻击方法更新所采取措施的实际效果。通过比对更新前后的漏洞库中列出的漏洞数量、类别及严重性，对新引入的攻击方法与现有安全标准进行符合性检查，确保其在真实场景中的有效性。对于检测出来的漏洞，需有明确的修复措施与验证流程，以确保漏洞被及时、有效地修复。

3.4.2.5. 法规适配性

确保更新后的仿真系统在使用过程中遵循当前现有的法律法规和行业标准。

3.5. 虚拟化仿真技术评价关键指标

为了确保网络安全虚拟化仿真技术的有效性和可靠性，需要建立一套全面的评价体系来进行系统化评估。本章节通过识别关键评价指标，对虚拟化仿真技术进行深入分析。具体而言，这些评价关键指标可以分为两大类：一是面向整车和零部件的网络安全虚拟化仿真评价关键指标，包括模型的准确性、计算效率、可扩展性、可靠性和安全性；二是面向汽车网络安全仿真攻击的评价关键指标，包括攻击检测率、反应时间、防护效果、误报率和系统兼容性。通过这种分类和细化，能够更全面地评估虚拟化仿真技术的性能和应用效果，从而为技术的进一步优化和改进提供科学依据。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

3.5.1. 面向整车、零部件的网络安全虚拟化仿真评价关键指标

以下列出了一些关键的评价指标。这些指标不仅涵盖了技术的基本性能，还考虑了实际应用中的需求和约束：

3.5.1.1. 可靠性

指仿真技术在使用时应能保持正常运行，在遇到外部干扰、异常输入时，仍能够正常运行；运行过程中，不会对用户、环境或其他外部系统造成危害的能力。

3.5.1.2. 准确性

指基于仿真过程中使用的参数应贴近真实环境，逻辑参数设置合理，输出结果应与实际系统的行为高度一致，具有较强的参考价值。

3.5.1.3. 可扩展性

指仿真技术具备灵活性、可配置性，能根据不同需求和场景调整和适配。

3.5.1.4. 兼容性

用于衡量仿真技术对于软件、硬件的适配性。在软件层面，如对于多种操作系统的支持、对于多种工程文件的支持等。硬件方便，例如对多种处理器的支持、对多种设备的支持等。

3.5.1.5. 可追溯性

用于衡量仿真技术能否对测试过程和结果进行记录、用于问题回放和排查分析。

3.5.1.6. 法规适配性

用于衡量仿真技术、模型对目前关键法规审核、测试内容的支持程度。包括技术层面和管理层面。

3.5.2. 面向汽车网络安全仿真攻击的评价指标

这一部分重点讨论仿真攻击的关键评价指标，这些指标不仅补充了技术的基本性能评估，还进一步细化了对攻击技术及其效果的衡量标准。通过这些指标，可以更全面地评估仿真攻击的有效性和实际应用价值。

3.5.2.1. 攻击覆盖率

用于衡量涉及的攻击技术在 ATT&CK 等攻击模型整体库的覆盖程度。

3.5.2.2. 兼容性

用于衡量仿真攻击所使用的技术对攻击目标的适配程度。

3.5.2.3. 攻击目标达成率

用于衡量仿真攻击效果的参数。

3.5.2.4. 实时性

衡量针对外界攻击技术的演进和漏洞更新情况。

3.5.3. 网络安全虚拟化仿真技术评价关键指标量化评估方法

为了系统性地评价网络安全仿真技术的适用性与成熟度，有必要建立科学、统一的量化评估方法。

本节围绕两大应用场景展开：一是针对整车、零部件的网络安全虚拟化技术的评估；二是面向网络安全场景的攻击仿真评估。针对两类技术路径，分别构建了涵盖可靠性、准确性、可扩展性、可追溯性等性能指标及攻击覆盖率、兼容性、达成率、实时性等安全指标的多维度评估体系，并引入“木桶原理”（木桶原理即系统性能的上限由最短板决定）与加权计算模

全国汽车标准化技术委员会
智能网联汽车分技术委员会

型，实现客观、可比的综合评价。通过选择最低得分项代表整体表现，强调薄弱环节在网络安全仿真应用中的关键影响，促使系统性优化。

3.5.3.1. 针对整车虚拟化、零部件虚拟化技术的评估量化方法

整车及零部件的网络安全虚拟化仿真技术，是支撑智能汽车网络安全开发周期缩短与测试覆盖提升的重要工具，本节设定了六项关键性能指标：可靠性、准确性、可扩展性、可追溯性、兼容性和法规适配性，并为每项指标划分五级评估等级。通过“木桶原理”，以最低得分项作为整体能力表现的代表，体现网络安全虚拟仿真系统的薄弱环节及优化方向，从而为工程应用提供定量依据和改进参考。

表 21 整车及零部件网络安全虚拟化仿真技术关键性能指标

序号	关键指标	评估方法（其中打√的为基线指标）		
		等级	描述	基线
1	可靠性	A	无影响：仿真系统在所有情况下均能持续稳定运行，无故障或干扰。	
		B	轻微影响：仿真系统偶尔会出现轻微故障或性能下降，但不影响关键功能。	
		C	中等影响：仿真系统在遇到外部干扰或高负载时，出现短暂或间歇性故障，影响部分功能。	√
		D	高影响：仿真系统频繁故障，影响大部分功能，需频繁修复或维护。	
		E	完全不可靠：仿真系统无法维持稳定运行，频繁崩溃或不可用。	
2	准确性	A	无偏差：仿真与实际情况完全一致，结果高度可靠。	
		B	轻微偏差：仿真结果与实际有轻微偏差，但在允许的误差范围内。	
		C	中等偏差：仿真结果与实际有明显偏差，需要进一步校准和调整。	√
		D	高偏差：仿真结果严重偏离实际，无法提供有意义的参考。	
		E	完全不准确：仿真结果与实际严重不符，无参考价值。	
3	可扩展性	A	无限制扩展：系统可以无缝扩展，适应所有新需求和场景。	
		B	轻微限制：系统大部分情况下可扩展，但有部分场景需要额外调整。	
		C	中等限制：系统在部分场景下难以扩展，需要大量定制或修改。	√
		D	高限制：系统在许多场景下无法扩展，扩展难度较大。	
		E	无法扩展：系统完全不具备扩展能力，只能适应特定场景。	
4	可追溯性	A	完全可追溯：系统可以完整地记录并回放测试的全部过程和结果。	
		B	部分可追溯：系统只能记录部分过程或结果，但无法做到全面回放。	
		C	基本可追溯：系统只能对结果进行简单记录，缺乏过程追踪能力。	√
		D	低可追溯性：系统只能记录部分结果，且记录不完整或不可靠。	
		E	无法追溯：系统没有任何记录和回放功能。	
5	兼容性	A	完全兼容：系统能适配所有常见的软件、硬件和操作环境。	
		B	大部分兼容：系统能适配大部分常见的软件和硬件环境，但有轻微不兼容。	
		C	中等兼容：系统仅适配部分常见的软件或硬件环境，其他场景需要额外定制。	

全国汽车标准化技术委员会

		D	低兼容性：系统与大部分环境不兼容，需要重大修改或补丁才能适配。	
		E	不兼容：系统无法适配任何其他环境，仅能在特定环境中运行。	
6	**法规适配性**	**A**	完全适配：完全支持（100%）相关法规内容	
		B	高度适配：75%≤法规适配率<100%	
		C	中等适配：50%≤法规适配率<75%	
		D	低等适配：0<法规适配率<50%	
		E	不支持：无法适配任何法规内容	

将上表中的关键指标进行汇总，基于“木桶原则”对仿真技术进评估。（注：兼容性和法规适配性不参与最终评估）。

如针对某仿真技术 x，量化评估为：可靠性：A、准确性：B、可扩展性：B、可追溯性：C，则该仿真技术 x 的最终评分为 C。

表 22 评估等级划分表

等级	对应描述
A	优秀
B	良好
C	合格
D	较差
E	极差

全国汽车标准化技术委员会
智能网联汽车分技术委员会

3.5.3.2. 针对汽车网络安全仿真攻击的评估量化方法

为系统评价不同仿真攻击技术的有效性与适应性，本节从攻击覆盖率、兼容性、攻击目标达成率、实时性四个关键指标维度构建多维量化评估模型，采用独立开放式评分计算各关键指标能力值。该方法能够有效刻画仿真攻击技术的广度、深度与实战能力，为其在攻防演练、漏洞验证和防护评估等网络安全场景中的工程应用提供量化参考。各关键指标与汽车网络安全仿真攻击的技术价值和应用场景需求相契合，能多维度、科学地衡量仿真攻击技术的综合能力。

表 23 仿真攻击技术有效性与适应性关键评估指标及方法

序号	**关键指标**	**评估方法**		
		等级	**描述**	**量化**
1	**攻击覆盖率**	**A**	高覆盖率：覆盖了大部分或全部 ATT&CK 模型的技术和策略（>60%）	9~10
		B	中等覆盖率：覆盖了 ATT&CK 模型中的部分技术和策略（20-60%）。	5~8
		C	低覆盖率：仅覆盖少数 ATT&CK 技术或策略（<20%）。	0~4
2	**兼容性**	**A**	高兼容性：仿真攻击技术完美匹配攻击目标的漏洞或架构，攻击容易执行，仿真环境能够高度还原目标车辆在实际运行中的各类场景。	9~10

		B	中等兼容性：仿真攻击技术部分兼容目标系统，可能需要调整或利用边界条件，仿真环境能够模拟出目标系统的大部分关键特征，但在某些细节或者特定场景下，与实际情况存在一定偏差。	5~8
		C	低兼容性：仿真攻击技术与目标系统不兼容或无法实现预期效果，仿真环境与目标系统实际运行环境相差甚远，无法为攻击测试提供有效的支撑。	0~4
3	**攻击目标达成率**	**A**	高达成率：仿真攻击几乎总是成功达成攻击目标。	9~10
		B	中等达成率：仿真攻击有时能够达成攻击目标，但成功率取决于特定条件。	5~8
		C	低达成率：仿真攻击通常难以达成攻击目标，成功率很低。	0~4
4	**实时性**	**A**	高度实时性：仿真攻击能迅速跟踪和应对最新的攻击技术和漏洞，实时更新。	9~10
		B	中等实时性：仿真攻击能够在合理时间内跟踪并适应新型威胁，通常需要一些更新时间。	5~8
		C	低实时性：仿真攻击无法及时应对新型威胁，更新滞后。	0~4

各关键指标能力值评分及对应描述可参考表 24。

表 24 各关键指标能力值评分表

分数	对应描述
8.5＜综合评分≤10	优秀
7.0＜综合评分≤8.5	良好
5.5＜综合评分≤7.0	合格
4.0＜综合评分≤5.5	较差
综合评分≤4.0	极差

全国汽车标准化技术委员会 智能网联汽车分技术委员会

4. 汽车网络安全仿真测试技术应用及标准化发展建议

随着汽车智能化、网联化进程的深度推进，汽车网络安全仿真测试作为提前识别风险、验证防护方案有效性的关键手段，其技术应用及标准化发展将为保障汽车全生命周期安全筑牢防护屏障。本章节基于当前技术发展现状与产业实践需求，从技术应用发展与标准化建设两个维度提出建议，为行业明确后续推进规划提供可参考的实施路径。

4.1 汽车网络安全仿真测试技术应用发展建议

4.1.1 汽车网络安全仿真测试试点验证

4.1.1.1 试点验证目标

本阶段试点验证的核心目标是在真实业务场景与实际操作环境中，检验汽车网络安全仿真测试相关评价指标、量化方法及执行流程的适用性与可行性，通过收集来自产业端（整车企业）与检测端（检测机构）的反馈意见，发现存在的问题与优化空间，为后续标准的正式落地与广泛应用奠定基础。

4.1.1.2 试点场景选择

为确保试点验证的代表性与针对性，优先选取汽车网络安全领域的典型核心场景开展验证工作，例如：安全隔离、安全启动等。

4.1.1.3 试点参与主体确定

综合考虑企业技术能力、业务覆盖范围及行业代表性，筛选 2-3 家整车企业与对应的 2-3 家汽车网络安全检测机构组成试点合作团队。其中，整车企业需具备成熟的车型研发体系与仿真测试能力，能够提供实际车型的软硬件环境；检测机构需具备汽车网络安全测试资质，熟悉国内外相关标准与测试方法，能够协助开展验证过程中的指标量化与流程合规性评估。

4.1.1.4 试点实施内容

试点工作围绕标准领航项目研究的实际应用展开，检验评价指标、量化方法、流程等在真实业务环境下的适用性，收集合理性可操作性的反馈。

4.1.2 汽车网络安全仿真测试技术共享平台

4.1.2.1 研究基础与核心目标

数据资源的碎片化、协作主体的分散化成为制约仿真测试效率提升的关键。基于现有数据共享平台的研究成果，通过对行业内主流平台数据的系统化整合，融合汽车网络安全仿真测试数据，补充汽车行业特有的漏洞信息、攻击方法与仿真测试案例，形成覆盖“漏洞发现-攻击验证-测试落地”全流程的动态数据共享平台。该共享平台将实现实时更新与共享，为汽车网络安全仿真应用提供精准、全面的数据支撑。

4.1.2.2 跨主体协作平台搭建与资源共享体系

为实现资源的高效整合与复用，平台将搭建跨主体协作架构，吸引车企、检测机构、漏洞平台（如 CNVD、CNNVD 等）、仿真工具厂商等核心主体加入，形成产学研用协同联动的生态。重点构建指标案例库、漏洞数据池、问题解决方案库。

4.1.3 构建汽车网络安全准入管理与仿真测试互认体系

从准入源头筑牢汽车网络安全防线，可考虑将虚拟仿真测试正式纳入技术审查范畴，提交材料可包含场景库建设方案与仿真测试体系实施方案，确保测试过程可追溯、测试结果可验证。分阶段推动仿真测试从试点探索向国家及行业标准技术升级，配套建立指标库、测试用例库、自动化工具链等支撑体系。通过建立指标与法规条款（GB 44495—2024、GB/T 44464—2024、R155 等）的对应关系，使仿真测试结果既能用于研发验证，也能直接支撑合规性审查和市场准入。

全国汽车标准化技术委员会
智能网联汽车分技术委员会

旨在确立仿真测试审查要求与差异化框架、推进仿真测试标准化落地与跨主体互认机制、实现仿真测试与汽车全生命周期的深度融合、搭建协同生态平台与认证体系，强化行业公信力、建立标准动态更新机制，适配行业发展需求。

4.1.4 网络安全仿真测试国际化交流与合作

4.1.4.1 促进标准对接与融合

积极联动国内车企、科研机构及检测认证机构，组建专业化团队参与国际汽车网络安全标准的提案、制定与修订工作，重点聚焦网络安全仿真测试的技术指标、流程规范及评价方法，将我国在智能网联汽车网络安全领域的实践经验与技术成果转化为国际标准提案，提升在国际标准体系中的话语权。同时，加强与国际标准化组织（如 ISO、IEC）、区域标准化机构（如欧洲 CEN/CENELEC）及主要汽车产业国（如德国、美国、日本）的同行交流，建立常态化沟通机制。通过参与国际标准研讨会、联合开展仿真测试技术验证项目等方式，推动汽车网络安全仿真测试标准的国际对接与融合，减少因标准差异导致的技术壁垒，为我国汽车企业“走出去”营造更便利的国际环境。

4.1.4.2 平衡区域化标准差异

在国际化推进过程中，需重点关注不同区域的标准特性与法规要求，其中欧盟市场的标准体系具有典型代表性。欧盟尚未将中国网络安全相关建设纳入 GDPR（《通用数据保护条例》）框架，其标准制定过程高度谨慎，需综合考量技术安全性、数据隐私保护、区域产业利益等多重因素，且欧盟内部各国（如德国、法国、意大利）的具体标准要求存在差异，给我国汽车企业进入欧洲市场带来挑战。

对此，应采取“双向适配”策略：一方面，针对欧洲市场的准入需求，推动我国汽车网络安全仿真测试标准与欧盟核心标准（如 UN R155 网络安全法规、WP.29 工作组相关要求）的兼容性验证，明确欧洲车型进入中国市场时需满足的网络安全仿真测试要求，保障我国市场的技术安全与标准独立性；另一方面，通过技术交流与案例分享，向欧盟及成员国传递我国标准的科学性与合理性，推动其在标准制定中参考我国实践经验，减少非技术因素对标准对接的干扰，避免将标准作为区域保护或限制他国产业的工具。

4.1.4.3 互助共进，赋能市场发展

针对俄罗斯、东南亚、拉美等新兴汽车市场，其网络安全仿真测试标准体系尚处于建设阶段，存在标准缺失、技术能力不足、合规成本高等问题。以技术分享结合标准注入为核心，推动中国汽车网络安全仿真测试标准在这些地区的融合与应用。

我国智能网联汽车领域的部分标准（如 L2 级智能驾驶网络安全强标）已具备先发优势，

全国汽车标准化技术委员会
智能网联汽车分技术委员会

而欧盟等地区尚未形成对应的完善标准体系，可将此类标准作为国际标准的补充提案，通过国际标准化组织提交，既填补全球标准空白，也实现中国标准“走出去”的突破性进展。

可通过以下路径实施：一是联合国内龙头企业与行业协会，在新兴市场开展网络安全仿真测试技术培训、标准解读会及案例研讨会，分享我国在 L2 级及以上智能网联汽车网络安全强标（如 GB/T 35273-2020《网络安全技术 个人网络安全规范》在汽车领域的延伸应用）的制定与实施经验，为当地标准建设提供参考；二是在新兴市场的本地化合作项目中，将我国网络安全仿真测试标准纳入合作协议，推动当地企业采用我国标准开展测试验证，降低其标准建设成本与合规成本；三是支持国内检测机构在新兴市场设立分支机构，提供符合中国标准的仿真测试服务，形成服务式输出模式，提升中国标准在全球范围内的认可度与影响力。

4.1.4.4 聚焦技术协同，夯实国际化合作基础

汽车网络安全仿真测试的国际化合作本质上是技术层面的协同与共享，需规避非技术因素的干扰，以技术实力为核心构建合作信任。一方面，加强与全球领先企业、科研机构的技术交流，围绕仿真测试工具开发（如漏洞挖掘平台、攻防仿真系统）、测试场景库建设（如车联网攻击场景、数据安全泄露场景）、测试结果互认等关键技术领域开展联合研发，共同攻克技术难题，提升全球网络安全仿真测试的整体技术水平；另一方面，建立国际技术协作平台，推动各国检测机构之间的仿真测试数据共享、技术验证结果互认，减少重复测试，降低产业链整体成本。

同时，针对不同国家的法规要求，开展标准协调工作：对于已引入国际标准的国家，推动我国标准与国际标准的协调适配，确保我国企业符合当地法规要求；对于尚未建立明确标准的国家，以技术提案的形式发声，推动其参考国际通用标准与中国实践，形成科学合理的法规体系，最终实现以技术交流促进标准协同、以标准协同推动产业共赢的国际化合作目标。

4.2 汽车网络安全仿真测试标准化发展建议

随着智能网联汽车技术的飞速发展，仿真测试作为保障网络安全的重要手段，已在行业中得到广泛应用。通过仿真测试，能够有效模拟真实世界中的复杂场景，提前发现潜在的安全风险。然而，在跨机构、跨平台的测试结果对比与共享中，仍然存在一致性、可比性与可重复性等方面的问题。因此，推进仿真测试的标准化工作变得尤为迫切。标准化不仅有助于提升测试过程的透明度和公正性，还能通过统一规范确保测试结果的可靠性与有效性，进而推动整个行业网络安全水平的提升。

4.2.1 标准化建议

全国汽车标准化技术委员会
智能网联汽车分技术委员会

制定基本标准可以确保仿真测试活动的有效性与一致性。在标准化工作中，测试环境与平台的标准化至关重要。当前，各类仿真测试平台在硬件配置、操作系统、虚拟环境搭建等方面存在差异，这导致了不同平台上进行同一测试时，结果的可比性受限。为此，建议基本的硬件配置标准，包括服务器、存储和网络架构的要求，以确保不同测试平台具有充足的计算能力和环境支持。在软件方面，应当约束测试平台所依赖的操作系统、依赖库及仿真工具的版本，以避免因平台差异导致测试结果不一致。此外，虚拟环境的搭建标准化也应当被纳入考虑，特别是涉及到网络拓扑结构和设备间交互的仿真环境，标准化的虚拟环境有助于确保不同测试场景下的测试一致性和可重现性。

在测试用例库的标准化方面，建议建立统一的测试用例库规范，以保证测试场景的完整性与覆盖面。该用例库应当包括各类攻击场景的模拟、漏洞路径的测试、以及系统性能的考察等内容。标准化测试用例的描述语言、执行步骤和参数设定等，能够使不同测试机构或平台在执行时不产生偏差，并增强测试用例的可共享性。此外，漏洞库的标准化同样至关重要，应当根据攻击方式、攻击路径等要素建立统一的漏洞库，为仿真测试提供可复用的基础数据。

仿真测试流程与方法论的标准化有助于提高测试过程的统一性与透明性。统一的测试流程涵盖了测试准备、执行、数据记录与缺陷追踪等环节，能够规范测试活动的执行，减少人为因素的干扰，提高测试的公正性与可控性。方法论的标准化同样重要，它有助于制定合适的测试维度、结果评估标准和数据收集方式，从而使得每次仿真测试都能够严格按照统一的标准进行，确保测试结果的科学性和准确性。

统一的评估方法与指标体系能够帮助各方对测试结果进行准确对比与评估，避免因标准不一致而产生的误解或误判。评估的指标应包括但不限于攻击成功率、误报率、系统稳定性、响应时间等关键因素。测试报告的标准化能够确保报告内容的完整性与一致性，应当明确报告中必须包括的内容，如测试目标、环境设置、测试过程、评估结果与改进建议等，从而为后续的安全整改与验证提供详实依据。

4.2.2 可探索标准化方向

在已制定基础标准的基础上，接下来应重点探索测试过程中更细化的标准化措施，以进一步提升仿真测试的综合性与深度。首先，仿真模型“保真度等级”的标准化至关重要，建议明确 L1 协议级（聚焦通信协议正确性）、L2 行为级（复现 ECU/子系统功能逻辑）、L3 物理级（融合动力学与环境交互）的等级划分，规定各等级测试目标与适用场景，此举可统一行业度量衡，解决“低保真测试、高安全性声明”问题，支撑研发各阶段精准测试，为“仿真

全国汽车标准化技术委员会
智能网联汽车分技术委员会

测试结果互认”奠定基础。测试数据格式的标准化是提升数据兼容性的重要一环，目前多平台数据格式、存储方式差异大，导致共享复用困难，建议制定统一标准，明确数据项结构、类型、单位等，确保不同平台数据高效对接，标准化格式不仅利于数据交换，还能减少后期分析的格式误差。而数据交互与报告输出的标准化同样关键，为支撑“跨主体协作平台”建设，建议定义含功能模型接口（FMI）、日志格式及结构化报告标准的交互规范，此举可打破数据孤岛，实现不同厂商工具无缝集成，降低协作成本，形成全行业协同预警与响应能力。

攻击注入接口的标准化是提高测试一致性的核心手段，现有平台攻击注入接口、方式差异大，导致相同场景表现不一致，建议制定统一标准，确保攻击注入方式、数据传递机制、触发条件一致，提升测试结果可靠性与可比性，标准化需聚焦核心接口与触发机制，允许上层应用按需调整，兼顾一致性与技术创新。在此基础上，未知威胁测试能力的标准化需同步推进，建议增设章节规范，将对抗性测试（如 GAN 传感器欺骗）、智能模糊测试（覆盖率引导 Fuzzing）纳入流程，推动测试从“验证已知”转向“探索未知”，评估车辆应对 0-day 漏洞的鲁棒性，引导产业构建主动防御体系。当前依赖定性描述的评估方式也应全面转向可量化体系，建议引入“威胁检测成功率（TDR）”“攻击链中断点覆盖率（KCPC）”“平均响应时间（MTTR）”等指标，设定分级通过阈值，此举可消除评估主观模糊性，为监管提供执法依据、车企提供优化目标，还可作为汽车网络安全险精算数据。

问题披露与共享机制的标准化是提升行业整体安全水平的重要环节，建议建立统一漏洞披露平台，规定披露时限、内容、流程，确保测试发现的漏洞及时共享，便于各方采取补救措施，此举有助于跨平台漏洞信息共享，推动修复协同，提升行业漏洞响应与修复速度。而构建动态“基线威胁场景库”可作为漏洞信息转化与共享的重要载体，建议标准附录联动国家级漏洞平台、行业信息共享中心，建立动态更新库，融合 ATT&CK 框架将零散漏洞转化为结构化测试故事线，作为行业测试“最小集合”，通过动态更新实现测试从“测已知漏洞”转向“预测潜在威胁”，帮助车企同步真实世界风险，升级为持续动态的安全验证。同时，测试环境的“数字存证与可追溯性”需得到保障，建议每次测试生成含完整环境参数的“数字快照”，用区块链/数字签名确保不可篡改，记录软件版本、网络拓扑、测试脚本等关键信息，该机制可一键还原测试场景，为安全事件归因、认证争议提供证据，支撑跨主体安全责任界定。

云计算技术的普及使云仿真平台的应用逐渐成为未来仿真测试的重要发展方向，为了确保云仿真平台的高效性与安全性，建议制定云平台的接口标准、性能标准及安全要求等，通过统一的云平台标准，可以确保不同平台之间在资源调度、数据传输和攻击模拟等方面的兼

全国汽车标准化技术委员会
智能网联汽车分技术委员会

容性，并为多租户环境下的仿真测试提供必要的保障，云平台标准化有助于提升跨组织合作的效率，结合数字存证、数据接口统一等措施，为未来的大规模仿真测试提供全面的技术支持和安全保障。

全国汽车标准化技术委员会
智能网联汽车分技术委员会