车路云供应链安全研究报告

上海观安信息技术股份有限公司

开源网安物联网技术（武汉）有限公司

联合发布

版权声明

上海观安信息技术股份有限公司、开源网安物联网技术（武汉）有限公司共同拥有本报告的版权，并依法享有版权保护。任何个人或机构在转载、摘录或以其他形式使用本报告的文字内容及观点时，必须明确标注资料来源。对于任何未经授权的转载或使用行为，我们将依法追究其法律责任。

目 录

1. 车路云供应链安全挑战 1

1.1 车路云一体化面临网络安全挑战 2

1.2 车路云供应链的复杂性加剧了网络安全威胁 3

1.3 车路云安全相关法律法规与标准体系 3

2. 车路云供应链 5

2.1 智能网联汽车 6

2.2 道路交通基础设施 8

2.3 云端服务平台 8

3. 车路云供应链安全风险 10

3.1 硬件安全 12

3.2 固件安全 12

3.3 系统安全 13

3.4 总线安全 13

3.5 无线电安全 14

3.6 网络安全 15

3.7 云端安全 15

3.8 应用安全 16

3.9 数据安全 17

3.10 传感器安全 18

4. 车路云供应链安全解决方案 21

4.1 建立网络安全管理体系 22

4.2 设计阶段开展威胁分析与风险评估 27

4.3 开发阶段建立软件供应链安全管控体系 33

4.4 测试阶段开展体系化网络安全测试 36

4.5 运营阶段建立供应链漏洞管理体系 47

5. 车路云供应链网络安全案例 51
5.1 电子不停车收费系统 OBU 风险评估案例 52
5.2 软件供应链安全管控案例 60
5.3 整车体系化网络安全测试案例 64
5.4 供应链漏洞管理体系案例 69
6. 趋势与展望 71
6.1 自动驾驶带来的潜在网络安全风险 72
6.2 大模型的普及与应用带来严峻的网络安全挑战 73
6.3 车路云数据融合过程中的安全风险 74

1. 车路云供应链安全挑战

随着智慧交通系统的快速发展，车路云供应链体系作为其核心基础设施，承担了实现车辆、道路和云平台协同运行的重要职责。智能网联汽车通过车载通信系统与道路交通设施和云端平台进行交互，以实现自动驾驶、智能调度、实时监控等功能。然而，这一系统的构建并非易事，它涉及多领域技术融合、多方协作以及复杂的供应链管理。

1.1 车路云一体化面临网络安全挑战

汽车智能化、网联化提升了出行效率与体验，也使车辆架构变得复杂增加了网络安全风险。以汽车为核心，车对车（V2V）、车对基础设施（V2I）、车对行人（V2P）、车对电网（V2G）等通信技术的不断应用将人、车、路、云连接到一起，形成巨大的信息网络。在车路云一体化进程中，为实现诸如自动驾驶、智能座舱等先进功能，智能网联汽车中集成了大量软硬件的车载系统暴露了众多的网络安全攻击面；智能网联汽车与外部互联网连接的无线通信接口使众多远程攻击成为可能；缺乏安全机制的总线传输协议为攻击者控制车辆提供了便利条件；缺乏安全防护的车载传感器让自动驾驶面临着严峻的网络安全考验。

网络安全攻击面的扩展提高了成功恶意攻击的概率，越来越多地引发针对智能网联汽车及其供应链的网络安全攻击事件，危及车辆与人员安全。2013 年，研究人员从第二代车载自动诊断系统（On Board Diagnostics-II，OBD-II）入侵车载控制器局域网（Controller Area Network，CAN）总线，控制了福特翼虎、丰田普锐斯方向盘转向、刹车制动、油门加速、仪表盘显示等重要汽车组件。2015 年，安全研究人员查理•米勒和克里斯•瓦拉塞克利用软件漏洞无线入侵 Jeep 切诺基系统，其后克莱斯勒公司大规模召回应用该系统的汽车。2016 年，科恩实验室通过远程方式成功入侵特斯拉汽车，进行了远程解锁车辆、调节座椅并打开天窗、转向灯等动作。据统计，自 2019 年以来至 2023 年，汽车行业共报告了 725 起 CVE，2023 年 378 起，2022 年 151 起。2023 年，严重和高危漏洞占 CVE 总数的近 80%，而 2022 年这一比例为 71%。严重漏洞占比的增加凸显了及时发现车路云安全风险并优先快速解决风险的重要性。

相比于传统信息设备，以智能网联汽车为核心的车路云供应链更加复杂、产品生命周期更长、对安全更为敏感，网络安全失败的代价也更令人难以承受。在其的生命周期中，智能网联汽车及其他车路云供应链设备一旦发生网络安全事故，将造成隐私泄露、经济损失、导致车毁人亡的惨烈局面，甚至可能被不法分子利用，危及公共安全与国家安全。关注以智能网联汽车为核心的车路云供应链网络安全理论、方法与技术，确保车路云供应链网络安全对于保护人民生命财产安全、促进行业健康发展具有重要意义。

1.2 车路云供应链的复杂性加剧了网络安全威胁

在全球化的浪潮下，汽车工业的发展广泛依赖全球分布的第三方供应商。在车路云架构中，智能网联汽车功能的实现涉及来源于世界各地的供应商提供的众多复杂软硬件系统。这种广泛的依赖关系使得车路云供应链管理变得极为复杂，众多供应商之间的协调与整合难度增大。各供应商采用不同的开发标准和技术架构，容易产生兼容性问题，而这些问题可能隐藏着潜在的安全漏洞。汽车制造商难以全面掌控供应链链条上每个供应商的产品质量和安全性，从而为网络攻击者提供了可乘之机，增加了供应链遭受攻击的风险。

从车路云角度看，随着车路云技术的不断发展和市场竞争的加剧，车路云设备厂商为了创新和降本，常常引入新的供应商。新供应商可能带来前沿的技术和解决方案，但同时也伴随着诸多未知风险。新供应商在进入供应链体系时，其技术水平、安全管理能力和数据保护措施可能尚未经过充分验证。因为缺乏应对汽车行业特定网络安全挑战的经验，其产品或服务中可能存在未被发现的安全漏洞，例如新供应商提供的车联网应用程序可能在数据加密、用户认证等方面存在薄弱环节，容易被恶意攻击者利用，导致车辆信息泄露、被远程控制等严重的网络安全危害，对车路云生态系统的稳定性和安全性构成潜在威胁。

据统计，供应链中的漏洞和恶意程序已成为车路云体系面临的主要网络安全问题。在复杂的车路云供应链体系中，各个系统与模块都可能存在安全风险。硬件层面，芯片、传感器等零部件可能被植入恶意程序或存在设计缺陷。软件层面，无论是操作系统还是应用程序，都可能存在安全风险，恶意攻击者可以利用供应链中的安全漏洞获取车辆控制权或窃取用户数据。供应链的复杂性进一步增加了车路云体系安全建设的难度，也让车路云供应链安全变得愈加重要，解决其安全风险问题迫在眉睫。

1.3 车路云安全相关法律法规与标准体系

为了解决车路云供应链安全问题，世界主要国家和地区相继出台了法律法规和标准体系以保障智能网联汽车及其供应链产品的网络安全。2021 年 6 月，联合国世界车辆法规协调论坛（简称为 UN/WP.29）发布了 3 项关于智能网联汽车的重要法规 R155/R156/R157，即网络安全（Cybersecurity）/软件升级（Software updates）/自动车道保持系统（ALKS）。该系列法规适用于 1958 协议下成员国（UNECE 1958 年协议的缔约方已增加到 54 个，其中包括所有欧盟国家和其他 OECD 国家）。虽然中国不在 1958 协议国中，但是生产的汽车只要销售到上述国家必须通过网络安全认证。

R155 是全球第一个汽车网络安全强制性法规，意味着车辆网络安全已经从符合标准进入到遵从法规的时代。

法规规定了车辆制造商需要满足的网络安全强制要求，给有计划出口至欧盟或其他 OECD 国家的车辆制造商带来了严峻的准入挑战。国内汽车网络安全标准方面，对标 R155 的“GB 44495-2024 汽车整车信息安全技术要求”是国内的强制性国家标准，已于 2024 年发布。该标准规定了汽车信息安全管理体系要求、外部连接安全、通信安全、软件升级安全、数据安全等方面的技术要求和试验方法，适用于 M 类、N 类及至少装有 1 个电子控制单元的 O 类车辆，其将法规给出的“风险点”转化为“技术要求”，细化了车辆同一型式判定技术条件，与联合国 R155 汽车信息安全法规整体协调。

法规中明确规定，汽车及其供应链制造商需要建设 CSMS（Cybersecurity Management System），申请 VTA（Vehicle Type Approval）证书，但是法规并未详细规定如何建设 CSMS。为了解决该问题，ISO/SAE《道路车辆-网络安全工程》作为事实上的行业标准成为各汽车制造商建设 CSMS 的依据。该标准盖了车辆从概念设计到退役的全生命周期网络安全管理。其核心内容是建立网络安全治理框架，通过威胁分析与风险评估（TARA）识别和降低风险，明确安全需求并贯穿产品开发、生产、运营和退役阶段，同时加强供应链的网络安全管理。标准强调持续监控、事件响应及验证确认，以确保安全措施的有效性，并要求通过全面的文档记录支持追溯与合规，旨在帮助汽车制造商和供应链应对网络威胁，保护车辆及乘员安全，同时满足全球法规要求。

2. 车路云供应链

车路云供应链体系高度复杂，涵盖了智能网联汽车、道路交通设施和云端平台三大核心领域。智能网联汽车部分涉及整车制造商、零部件供应商和软件开发商，负责车辆硬件、嵌入式系统以及车载网络的研发与集成；道路交通设施则包括智能交通灯、监控设备、路侧通信单元（RSU）等，需多方协作以实现车路协同功能；云端平台涉及数据存储、实时计算和服务部署，由云服务提供商、数据分析企业及网络安全供应商共同支持。各环节紧密交互，既要求技术和标准的高度统一，又需应对供应商多样化和全球化带来的网络安全管理挑战。

2.1 智能网联汽车

智能网联汽车的发展催生了全新的产业生态，传统的汽车制造供应链被重新定义，从过去的硬件生产为核心，演变为集硬件、软件、通信和数据服务为一体的综合体系。与此同时，智慧交通系统的兴起推动了道路基础设施的数字化转型，以及云计算、大数据和人工智能技术的广泛应用。汽车是车路云供应链的核心组成部分，其复杂性体现在硬件、软件和通信技术的高度融合上。传统汽车供应链以机械和电子元件为主，而智能网联汽车的兴起极大地扩展了供应链的范围，包括传感器、执行器、电子控制单元（ECU）等硬件设备，以及车载操作系统、通信协议栈、人工智能算法等软件组件。

智能网联汽车软硬件供应链涉及感知层、决策层、执行层、通信与网络层、智能座舱系统和车载软件。感知层通过车载传感器（如摄像头、激光雷达、毫米波雷达等）采集环境信息，并结合高精度地图和定位技术，实时构建车辆周围的动态环境模型。决策层通过中央计算单元和人工智能算法对环境信息进行分析，规划路径、制定行驶策略并预测潜在风险。执行层根据决策层的指令，精准控制车辆的动力、转向和制动，实现安全、高效、舒适的自动驾驶。通信模块通过 V2X 等通信技术与其他车辆、道路基础设施和云平台交互，拓展感知范围并优化协同驾驶性能。同时，智能座舱系统提供用户舒适体验，车载软件则为各个层面提供功能支撑。

（1）感知层

传感器已经成为智能网联汽车的关键零部件，是保障车路云安全的关键。为了获取汽车自身状态信息，智能网联汽车装备了胎压监测系统、全球定位系统、全球导航卫星系统(Global Navigation Satellite System, GNSS)、惯性测量单元（Inertial Measurement Unit，IMU）等用于胎压监测、汽车导航、确定位置与方向。除此之外，为了感知周围环境，智能网联汽车搭载了激光雷达（LiDaR）实现光探测与测距，利用毫米波雷达（Radar）感知距离，基于摄像头实现驾驶环境的语义分割、目标探测与追踪、测距、驾驶员疲劳检测，采用超声传感器探测障碍物。

感知层是智能网联汽车的基础构成部分，负责收集和处理车辆周围环境的信息，提供给决策层进行分析和决策。感知层的核心任务是实时获取车辆周边的动态与静态信息，以确保安全驾驶和优化驾驶体验。感知层作用主要体现为三个方面，安全性，通过准确识别周围环境，提供实时风险警告，确保行车安全；决策支持，为决策层提供必要的环境数据，支撑智能驾驶决策的生成；和驾驶体验，增强驾驶员的信心与安全感，提高乘车体验。

（2）决策层

决策层依据感知信息将感知层获取的环境信息（如道路状况、障碍物位置、行人和车辆行为等）与高精地图、交通规则和驾驶任务相结合，制定合理的驾驶策略和路径规划。通过人工智能算法（如深度学习和强化学习）、优化模型和规则引擎，分析和预测车辆周围动态环境的变化，并根据驾驶场景（如城市道路、高速公路、停车场等）确定车辆的动态行为，例如加速、减速、转向、变道、超车或紧急避障。在车路云体系中决策层还与通信模块协作，通过 V2X 技术（Vehicle-to-Everything），与其他车辆、道路基础设施和云端实时交换信息，从而扩展感知范围，优化决策的准确性和协同性。例如，在车队协同驾驶中，决策层能够分配任务并确保车辆之间的高效配合。

（3）通信与网络层

通信与网络层是以智能网联汽车为核心的车路云体系的重要组成部分，负责实现车内与车外信息的高效交互，为感知、决策和执行提供关键支持。该层的核心功能是通过车载通信单元（OBU）和网络协议，实现车辆与外界的互联互通，包括车辆与车辆（V2V）、车辆与基础设施（V2I）、车辆与云平台（V2C）以及车辆与行人（V2P）的信息交互。

通信与网络层主要依托 5G、LTE-V、C-V2X 等先进通信技术，确保数据传输的低延时、高带宽和高可靠性。通过与感知系统协作，该层可以接收来自外部环境的实时信息（如交通信号、路况和其他车辆位置），并向决策层提供更广泛的环境数据支持。同时，它还负责与云端交互，进行高精地图更新、路径优化和大规模协同控制。在车内，该层通过 CAN 总线、以太网等通信网络实现传感器、控制器和执行单元之间的高效数据交换，保证各模块的协同工作。此外，通信与网络层还具有信息安全功能，防止外部网络攻击和数据泄露，确保系统的稳定性和安全性。作为智能网联汽车实现协同感知、智能决策和智慧交通的重要支撑，通信与网络层在构建车联网生态中发挥着至关重要的作用。

（4）智能座舱

智能座舱是智能网联汽车中面向用户体验的核心模块，融合了先进的人机交互（HMI）技术、车载娱乐系统、

驾驶辅助功能和信息显示系统，为驾驶员和乘客提供智能化、便捷化的车内环境。它通过多种传感器和信息技术，感知用户状态，提供个性化服务，并实现人与车之间的自然交互。

（5）车载软件

车载软件是智能网联汽车的核心支撑系统，负责整合硬件资源、执行功能逻辑，并实现车辆的智能化控制和信息交互。它贯穿感知、决策、执行和通信等各个层面，为车辆提供智能驾驶、车内体验和网络服务的功能支撑。主要体现为四个方面，高安全性，提供功能安全与网络安全保障，确保驾驶安全。高实时性，确保在高速行驶和复杂环境下及时响应。智能化，融合人工智能与大数据技术，实现自动驾驶和个性化服务。可扩展性，支持软件OTA 升级，满足用户和技术发展的需求。

2.2 道路交通基础设施

单车智能与车路协同是智能驾驶的两个主流演进方向。智能网联汽车凭借感知技术、人工智能技术具备了辅助驾驶功能，大幅提升了驾驶体验，却无法全面感知车辆附近的道路交通状况，未能实现真正意义上的智能驾驶。基于车路协同技术的车联网则在单车智能之外为智能驾驶提供了强有力的保障。〝车路云一体化〞通过集合车端智能、路侧智能与云端智能，打破过去孤立状态，实现人、车、路的连接，实现信息系统解耦和跨域共用，构建统一的基础层来支持各种应用。

道路交通设施是实现〝车路云一体化〞的重要基础，为云控平台采集来自车辆、道路以及其他交通相关系统的动态交通数据，并向车辆及交通参与者提供来自系统的交通相关信息，其供应链涵盖感知设施，通信网络基础设施、交通附属设施和边缘计算系统。路测感知设施用于对道路交通运行状况、交通参与者、交通事件等进行检测识别，包括摄像机、毫米波雷达、激光雷达及其他路侧感知设施。通信网络基础设施包括基于超高速无线通信（EUHT，EnhancedUltraHighThroughput）的路侧通信设备、基于蜂窝车联网（C-V2X，CellularVehicle-to-Everything）的路侧通信单元等。交通附属设施包括包括信号控制机、信号灯、标志标线等。边缘计算设施主要用于对路侧感知设施的原始感知数据或结构化数据进行存储、融合分析处理，得到较高精度的感知结果信息，支持路侧设备接入，对数据进行汇聚和处理分析。

2.3 云端服务平台

云端服务平台是车路云一体化的核心枢纽，主要用于整合车辆、道路和用户数据，为车联网中的众多实体提

供便捷高效的信息服务，包括封闭式服务与开放式服务。封闭式服务是针对特定行业或平台的服务，特别是与车辆和交通本身高度相关的服务。交通领域的车联网服务多为封闭式服务，如为了提高交通安全的碰撞警告服务、较少停车等待时间，提升交通效率的电子不停车收费服务。开放式服务主要是应用服务提供商为用户提供的信息服务，多为在线或离线多媒体服务、人机交互服务，包括天气信息、音乐、影视等信息娱乐服务。

车联网云端服务管理平台作为智能网联的重要支柱，具有以下主要特征：1）数据汇聚与处理能力。云端平台负责收集来自车辆、路测设备和用户终端的大量数据，通过分布式存储和高性能计算，支持对海量数据的处理与分析，为车辆和用户提供个性化服务与实时决策支持。2）云端平台为智能网联汽车和车联网相关设备提供了丰富的应用服务，例如车辆解锁、启动、空调设置等远程车辆控制，车辆操作系统和软件的远程升级，基于实时交通信息进行路径规划和动态调整，为 ADAS（高级驾驶辅助系统）和自动驾驶功能提供决策支持。3）实时性与高可用性。车联网云端平台需要实时处理来自多个来源的数据，并在毫秒级时间内响应指令。高可用性设计确保系统在任何时候都能正常运行，避免因单点故障导致服务中断。4）高并发性与可扩展性。车联网中的云端平台需要支持数百万辆智能网联汽车的同时连接和操作。通过采用分布式架构和弹性扩展机制，平台能够动态应对流量高峰和资源需求变化。5）跨域互联与协同。车联网生态系统中，云端平台需要与车辆终端、路测设备、第三方服务系统进行跨域通信。例如，与支付平台对接实现自动扣费，与智能交通管理系统协同优化交通流量。

随着车联网技术的快速发展，云端平台的功能和应用日益复杂，其在支持大规模并发连接、实时处理和多系统协作方面展现出巨大的潜力。然而，这种复杂性以及其开放性也使得云端平台成为网络攻击的高风险目标。云端平台存储了大量车辆运行数据、用户个人信息和敏感数据。一旦平台被攻破，这些数据可能被窃取或滥用，造成严重的隐私侵害和经济损失。例如：攻击者可能利用车辆的地理位置数据监控用户行踪；未授权的第三方可能通过平台漏洞访问用户的支付信息。攻击者也可以通过发送大量伪造请求，使云端平台的计算和通信资源耗尽，从而导致系统瘫痪，影响车辆和用户服务的正常运行。这种攻击对高并发要求的车联网云端平台尤为致命。攻击者还可能通过漏洞利用、社会工程学或供应链攻击将恶意代码植入云端平台，窃取敏感信息或对数据进行加密勒索。后门植入页可能为攻击者提供长期的访问权限，威胁系统安全。云端平台与车辆及路侧设备之间的通信需要依赖于可信的数字证书和加密机制。如果信任链被破坏（如证书伪造或被盗用），攻击者可以冒充合法设备与云端平台通信，发起欺诈性操作。攻击者还可能在数据传输过程中篡改或伪造信息，例如：伪造 OTA 更新包，导致车辆加载恶意软件；篡改实时交通信息，造成交通混乱或安全隐患。

3. 车路云供应链安全风险

在汽车制造领域，供应商往往遍布全球，从零部件制造到整车组装，每一环节都需要精准衔接。道路基础设施领域则涉及地方政府、施工企业和设备制造商，各区域标准的不一致性增加了整合难度。而云端平台作为数据中心，依赖通信运营商和硬件供应商，需确保多方资源在性能、安全性和兼容性上的一致性。复杂的供应链体系牵涉大量零部件，漫长的供应链中不同零部件在软硬件与功能上存在重复，理论上也会面临类似的风险。本章基于车路云供应链涉及的软硬件抽象出十个层次的网络安全威胁进行威胁建模。车路云供应链网络安全框架是将车路云体系进行建模的抽象框架，依据由车内到车外、底层到上层、硬件到软件的原则，该框架将车路云供应链涉及到的软硬件抽象为如下十个层次：硬件板卡、关键模块固件、操作系统、车内总线、无线电系统、网络通信、云端服务器、移动设备、隐私数据、传感器。

在车内，硬件板卡与运行在硬件板卡中的固件或者操作系统构成车内 ECU。车内总线承载了智能网联汽车内众多 ECU 之间的数据通信，将所有的 ECU 与传感器连接起来形成复杂的车内通信网络。在车外，传感器感知汽车周围环境与自身状态，感知结果借由总线系统传输到相应 ECU 进行解析并响应。无线电通信技术是车内网络与车外网络的连接点，也因此成为车外网络远程进入车内网络的入口。不同的无线电技术承载的通信协议不尽相同，Bluetooth、RFID 等无线电技术并不涉及传统互联网网络的 TCP/IP 协议，传统互联网网络安全技术并不完全适用于智能网联汽车。网络通信技术除了连接汽车与云端服务平台，也连接了手机等移动终端设备，为智能网联汽车引入了更多的网络安全风险。除此之外，基于通信技术构建的车联网在提供服务的同时也导致了严重的数据泄露问题。

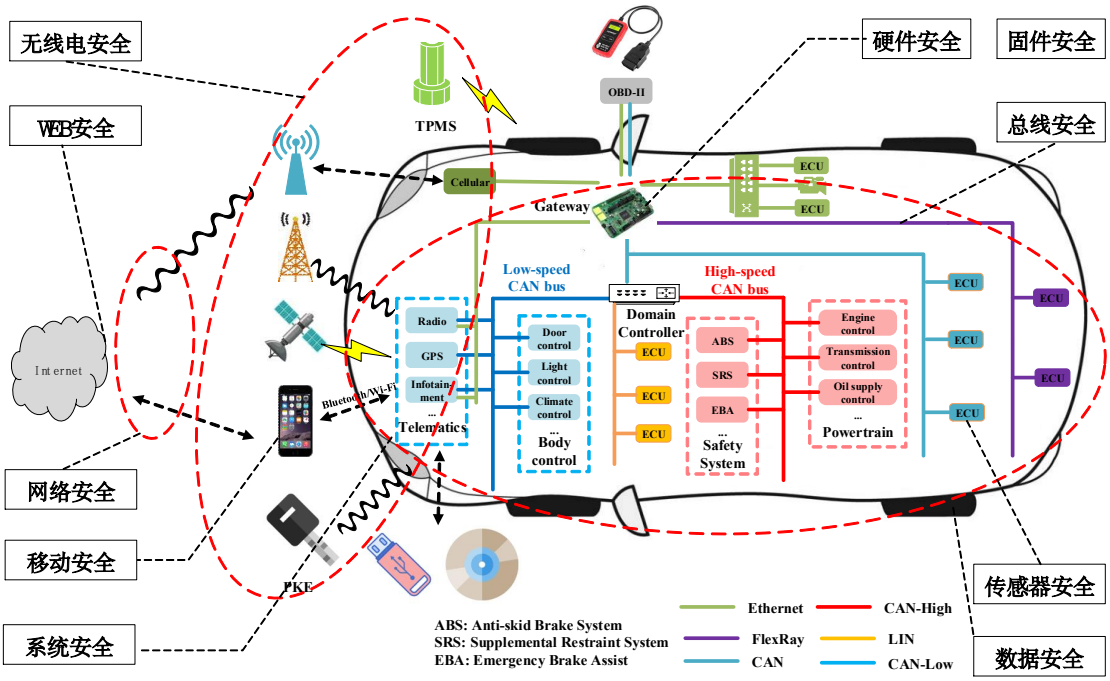


图 1 车路云供应链网络安全框架

车路云供应链网络安全框架并非仅仅针对车路云体系中具体的模块及系统，例如信息娱乐系统、自动驾驶控制系统等，而是将车路云供应链中各个系统涉及到的软硬件抽象为十个层次，可供研究人员对车路云体系进行建模。各个层次中需要关注的网络安全风险如下：

3.1 硬件安全

汽车中大量的 ECU、传感器等汽车电子设备基于硬件板卡运行相应的固件及操作系统实现特定的功能。典型的汽车电子单元硬件系统包含计算单元、存储单元、总线单元、外设接口。基于汽车电子的硬件架构，车路云供应链网络安全框架硬件安全包含印刷电路板安全、处理器芯片安全、存储芯片安全、硬件调试接口安全、板载传输总线安全五个方面。

PCB 是电子设备的承载基础，会泄露集成电路芯片型号、接口电路、总线协议等信息。处理器芯片在运行程序执行特定任务时会泄露电磁信息、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。故障注入技术是测量电路可靠性的重要技术，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改变处理器运行逻辑。

数据存储芯片面临数据残留的安全风险。片外 Flash 存储芯片，攻击者可通过满足特定通信协议的编程器读取存储器中的固件等数据。对于片上系统内部的存储器，JTAG、SWD、USB 等硬件调试接口也为攻击者获取内部存储数据提供了潜在的可行性。SPI 总线与 I^2C 总线是电子设计领域使用的常见总线协议，用于不同芯片之间的数据传输，面临数据监听、数据篡改等网络安全威胁。

3.2 固件安全

架构决定了控制单元的功能复杂程度。基于使用场景与功能复杂程度，车路云供应链网络安全框架将汽车电子设备固件分为三大类：全操作系统固件、部分操作系统固件、无操作系统固件。全操作系统固件包含一个成熟的操作系统，应用在具有高性能与多功能需求的场景中。部分操作系统固件所采用的操作系统常为满足特殊需求的实时操作系统，例如 VxWorks，或者供应商定制的操作系统，具备操作系统的部分特性，可以完成基本的资源管理、任务管理等通用功能。无操作系统固件本质上是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。该类固件具备较好的性能与稳定性，但是大大增加了开发难度与开发周期。

尽管电子控制单元固件形态各异，均面临一定的安全风险。开发人员可能因为疏忽将密钥等敏感信息硬编码在固件中造成密钥泄露，威胁系统安全。除了口令、密钥等敏感数据，重要的网络资源地址、用户名、邮件地址等隐私信息也可能明文编码在固件中。除此之外，恶意攻击者可通过逆向工程技术分析固件的逻辑功能，获取目标系统的运行逻辑以挖掘潜在的逻辑漏洞。恶意攻击者也可以访问固件中的文件系统搜寻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具有网络安全漏洞。

3.3 系统安全

当固件为全操作系统固件，其固件分析便成为一项非常复杂的任务。静态分析采用网络安全框架中的固件安全分析策略，仅仅可以满足一部分安全分析需求。基于真实硬件环境的实时动态分析可以更详细地了解目标系统安全态势，已经脱离单纯的固件安全进入到系统安全范畴。

Linux 等成熟操作系统功能复杂，体系庞大，也面临着更为复杂地的网络安全形势。安全的操作系统需要控制外部实体对系统内资源的访问。操作系统安全既要求操作系统在设计时通过权限访问控制、信息加密性保护、完整性校验等机制保护系统内数据安全，又要通过一系列的配置，保证操作系统避免由于设计与实现缺陷或是应用环境因素引入安全隐患。

3.4 总线安全

车内总线连接不同的 ECU 控制单元，协调汽车各个功能模块之间的数据传输。车路云供应链网络安全框架中的总线安全包括 CAN 总线安全、FlexRay 总线安全、LIN 总线安全、MOST 总线安全、车载以太网总线安全五个方面。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，一旦总线因为缺乏安全机制被攻击者控制，后果不堪设想。

车内总线面临的潜在安全风险包括数据传输风险、拒绝服务威胁、协议实现威胁。如果车内总线在数据传输过程中未对传输节点进行有效的身份认证，恶意攻击者可以伪造传输节点接入车内总线网络。一旦攻击者介入总线网络，在总线协议未对传输数据进行有效加密的情况下，攻击者可以获取监听总线上传输的全部数据，获取传输内容。更进一步，如果总线传输未采取完整性校验机制，攻击者可以伪造总线传输数据对正常的总线通信造成干扰，甚至拒绝服务。对于总线承载的应用层协议，攻击者亦可利用其车辆访问与控制功能对车内网络实施攻击。

3.5 无线电安全

无线电通信技术广泛应用于车联网领域，分布于传感器、车载通信单元、无钥匙进入系统、信息娱乐系统等多个应用场景之中。基于传感器的特点，车路云供应链网络安全框架将 GPS、GNSS、TPMS 等传感器涉及到的无线通信技术划分进入传感器层级进行讨论。依据不同的传输距离，如图 2 所示，车联网中使用的无线通信技术分为短距离无线通信技术、中距离无线通信技术、长距离无线通信技术。其中，长距离无线通信技术允许汽车将数据传输数公里距离，如 LTE-V2X 技术与 5G-NR 技术。中距离无线通信技术传输距离仅有数百米，如无线局域网技术（Wireless Local Area Network，WLAN）、DSRC 技术。短距离无线通信技术覆盖的传输范围仅仅在数米之内，如 BLE、NFC 等技术。

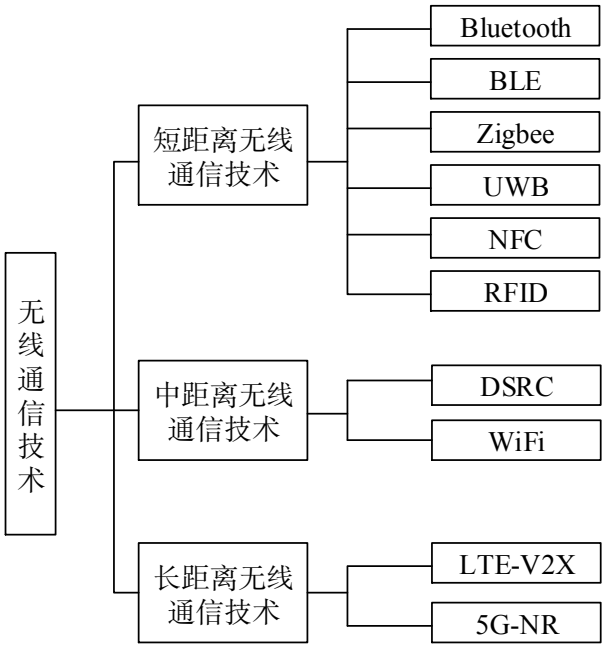


图 2 基于距离的车联网无线通信技术

短距离无线通信技术包含适用于汽车领域的低功耗 Bluetooth 技术、Zigbee 技术、UWB 技术、NFC 技术。攻击者可以在通信双方均无意识的情况下作为中间人介入两台 Bluetooth 通信设备之间的通信，发起中间人攻击。ZigBee 技术用于胎压监测领域，传输层可能遭遇潜在的泛洪攻击。网络层负责数据报文的路由与处理，可能遭遇“虫洞”攻击和选择性转发攻击。链路层干扰通过中断发送节点和接收节点之间的消息交换来造成拒绝服务。攻击者也可以通过无线电工具监听、篡改、阻塞 ZigBee 无线信道中传输的数据。UWB 技术用于测算车辆位置，可达厘米级精度。UWB 高频信号穿透力强，覆盖范围广，便于攻击者再视野范围之外悄无声息地发动攻击。传输速度快则会在短时间内泄露大量传输数据，为密文破解提供足够的数据样本。NFC 技术应用于汽车钥匙领域，

将空 NFC 标签靠近 NFC 设备会诱导设备对标签产生响应，占用 NFC 设备资源，造成拒绝服务。恶意攻击者亦可中继 NFC 标签与设备之间通信数据，绕过身份认证机制，开启车门。

中距离无线通信技术包括 DSRC、Wi-Fi 等技术。DSRC 应用于车载通信单元帮助汽车建立了覆盖范围广大局部通信网络。基于 DSRC 信道的开开放性，任意攻击者可获取相关传输信息。此外，用于密码学运算的随机数在传输中也需要进行有效的安全防护。攻击者也可以通过恶意手段干扰正常的 DSRC 通信，造成设备拒绝服务。中继攻击则可以延长通信距离，造成远距离恶意扣除费用等潜在安全隐患。Wi-Fi 技术在车联网信息娱乐系统中发挥着重要作用，实现车辆与乘员之间的信息共享。同时，Wi-Fi 技术也为车联网带来了一定网络安全隐患，WEP 等不当的加密协议可被轻易破解，泄露传输数据内容。弱口令则为攻击者入侵无线局域网络提供了可能性，一旦攻击者攻陷汽车无线局域网络，则可以进一步搜集信息以寻找高价值资产，为后续攻击奠定基础。

长距离无线通信技术是以 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。5G-NR 标准提供了更高的数据速率，更低的通信延迟，可以实现异构设备之间的良好通信。为了支持 5G 通信快速稳定、低延迟、边缘计算的特点，5G 网络对外暴露更多的设备接口与服务接口，引入了更多的网络安全隐患。除了 5G 网络架构中大量设备引入的传统网络威胁之外，信道威胁也为 5G 通信带来潜在的网络安全风险。攻击者通过操纵被攻陷设备的无线信号或网络流量，达到拒绝服务、协议降级等恶意目的，影响信道资源分配与传输，营造对攻击者有利的网络环境，如恶意利用无线电频段、无线电干扰等。

3.6 网络安全

不同于无线电安全，本框架中的网络安全更侧重于基于 TCP/IP 协议栈的上层网络通信安全，而前者则侧重于以无线传输介质为基础的物理层与链路层安全。网络通信安全方向的威胁则主要表现为网络通信中的敏感数据有可能遭到泄露或修改，从而导致重大损失。攻击者可能窃听网络中传输的敏感信息而获取传输内容。更进一步，攻击者可以将获得的部分或全部合法数据重放给接收者，以达到欺骗接收者的目的。攻击者甚至可以介入合法用户之间的数据通信过程，实施中间人攻击。一旦成功劫持通信过程，攻击者可窃听、篡改合法用户之间的通信信息，同时向通信双方伪装为合法通信实体。

3.7 云端安全

车路云应用生态中，智能网联汽车需要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。

Web 应用是云端服平台的关键应用，Web 站点为客户端-服务器架构，其网络安全威胁分为客户端威胁与服务器威胁。客户端威胁主要包括浏览器威胁、跨站脚本威胁、跨站点请求伪造威胁、点击劫持威胁等。服务器威胁主要包括注入攻击、文件上传威胁、认证与会话管理威胁、访问控制威胁、Web 框架威胁、拒绝服务威胁、PHP 漏洞、不当的服务器配置。

Web 网络安全研究发展已近十余年，有着成熟的研究成果。网络上有海量的 Web 网络安全资料，无论是攻击技术还是防御技术，OWSAP 组织也会定期发布 Web 领域的主要网络安全威胁，关于 Web 网络安全的分析，此处便不再赘述。

3.8 应用安全

智能网联汽车常常通过手机应用程序与车辆交互，例如远程开启空调、远程车辆诊断等应用场景。除了车辆本身的网络安全威胁之外，手机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。

本框架将手机应用程序中需要保护的资产归类为客户端文件、本地存储数据、应用进程、运行时数据、交互界面与接口、网络通信。不同格式的客户端文件面临泄露系统逻辑、敏感信息、被恶意篡改等网络安全威胁。运行时数据包括聊天记录、文本文件、收藏夹、访问记录等，部分手机应用程序可能将银行卡、身份证、联系人以及账号密码等敏感信息存放在本地存储空间。如果没有有效的防护机制，手机应用程序数据极有可能遭到泄露。手机应用程序启动后会向系统申请资源，创建进程，进而运行主逻辑，其进程会一直存在，攻击者可能恶意关闭、劫持进程，也可能注入恶意数据到应用程序的进程之中，妨碍程序的正常运行。

手机应用程序运行时会将程序代码和业务数据加载到程序内存中，基于内存地址可以访问手机应用程序运行时在系统内的存储区域，读取手机应用程序运行时的业务逻辑和业务数据，获取重要信息。在未采取安全措施的情况下，手机应用程序运行时在内存中的逻辑代码和业务数据多为明文存储，容易导致信息泄露安全威胁。当操作系统基于内存共享方式进行进程间通信时， 手机应用程序运行时产生的敏感数据在内存中可能会被其他手机应用程序进程读取，发生数据泄露。

手机应用程序通常提供交互界面用于人机交互，获取用户输入信息、浏览记录等。如果缺乏有效的安全防护机制，攻击者可能通过截取屏幕与录屏的方式窃取用户信息，也可能伪造虚假界面，诱导用户输入用户名及口令

等敏感信息，导致信息泄露。手机应用程序在运行时还会开放网络端口、程序接口等交互服务接口，对外提供数据读写、接口调用、进程间通信等服务。交互接口是数据和程序出入手机应用程序的重要通道，一旦遭到攻击，后果极为严重。基于应用需求，手机应用程序需要与云端服务器等网络资源服务器建立通信链路用于数据通信，如建立 HTTP 会话以传输数据，建立 TCP 长连接同步状态，建立 UDP 连接开展延时敏感服务等。攻击者可能介入通信过程，劫持、篡改通信流量，仿冒通信实体，对手机应用程序及车辆造成安全威胁。

3.9 数据安全

智能网联汽车与道路交通基础设施、云端服务器、移动设备等组成车联网，供路线规划、智能调度、交通管理等服务。然而，便利与安全始终是对立的，为了满足智能调度、危险预警等基本的车联网服务需求，车辆需要不断向周围周期性广播自身状态信息，其中包括车辆实时位置、速度、行驶状态等表明己方状态的关键数据。另一方面，危险预警、个性化推荐等服务需要车联网服务提供商获取车辆身份信息、用户习惯与网络记录等重要隐私数据。

位置数据安全威胁源于明文传输广播数据，攻击者利用 DSRC、C-V2X 等技术无线传输信道的开放性监听无线信号，经过解调与解编码可以获取传输数据比特流。如果攻击者进一步了解协议规范可以基于协议规范解析数据内容。攻击者甚至可以利用商用或开源工具抓取并解析无线信道中传输的数据。一旦车辆状态数据明文传输，攻击者可以获取目标车辆实时状态。除此之外，静态道路拓扑结构与交通规则为攻击者预测车辆轨迹提供了可能性。攻击者基于当前车辆速度、位置、加速度等状态数据，配合线路约束、交通规则约束等约束条件极易推测其未来一段时间内的行驶轨迹。

身份数据安全威胁源于精准的个性化服务与安全关键服务。个性化服务需要用户牺牲个人隐私以便于服务提供商基于用户习惯提供更为精准的个性化推荐服务。而危险预警等则需要在紧急时刻确保预警信息准确抵达目标车辆。攻击者如果获取身份隐私与其他个性化隐私数据即可了解攻击对象的生活习惯等，配合轨迹预测即可能实施盗窃、追踪等违法犯罪活动，对人身及财产安全造成威胁。

3.10 传感器安全

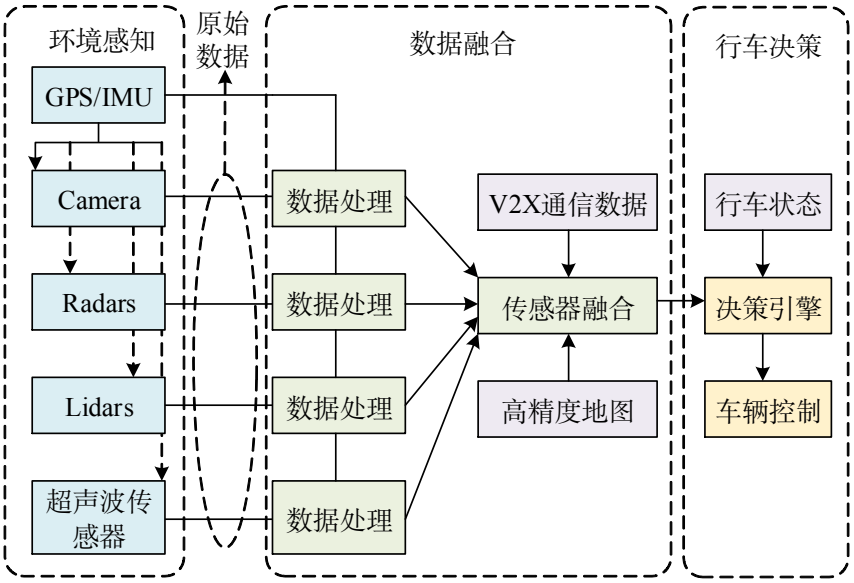


图 3 传感器数据融合

为了感知车辆行驶环境，智能网联汽车搭载了 GPS、光学摄像头、激光雷达、超声波雷达、毫米波雷达、TPMS 等丰富多样的传感器。如图 3 所示，传感器将采集到的数据输入到智能网联汽车的计算系统，进行处理和计算，实现车辆的自主控制。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。

表 1 智能网联汽车传感器

传感器	信号	范围	场景
GPS	微波	全球	定位
GNSS	微波	全球	定位
TPMS	微波	短距离	胎压监测
LiDaR	激光	中距离	碰撞避免、行人探测
Radar	毫米波	长距离	碰撞避免、自动巡航

传感器	信号	范围	场景
超声波雷达	超声波	短距离	停车辅助
摄像头	可见光	短距离	交通信号探测、车道探测、障碍探测
防盗系统	射频	短距离	无钥匙进入系统、防盗系统

表 1 为不同传感器的使用场景。GPS 信号来自卫星，经过长距离的传输抵达地面接收设备时，信号衰减至微弱状态。由于 GPS 信号接收设备倾向于接收强度更强的信号，模拟的 GPS 信号可对正常的信号接收造成干扰，达到定位欺骗的目的。相比于光学摄像头的被动感知，激光雷达是主动环境感知设备，用来识别车道、交通标志等。雷达通过高速旋转的激光收发器来探测并识别障碍物，可能遭受来自攻击者的恶意攻击。通过控制发送假信号的延迟时间和频率，该攻击可以实现在固定位置注入虚拟障碍物以欺骗智能网联汽车。攻击者可以预先接收激光脉冲，立即将激光脉冲转发给激光雷达随后旋转过来的另一个收发器，制造更近距离的虚假障碍物。

同激光雷达相似，毫米波雷达发射特定频率的电磁波并接受障碍物的反射波来测量距离。毫米波雷达发射的微波波长长于激光雷达发射的激光，在风暴、大雾、尘埃等恶劣天气下具有更好的鲁棒性。在针对特斯拉搭载的毫米波雷达的攻击中，攻击者通过向毫米波雷达发送相同的波形信号以降低信噪比来干扰其工作。更进一步，攻击者可以通过精心调制类似毫米波雷达的信号成功欺骗车辆，对于仅仅依靠毫米波雷达实现障碍物识别和碰撞规避的自动驾驶汽车威胁巨大。

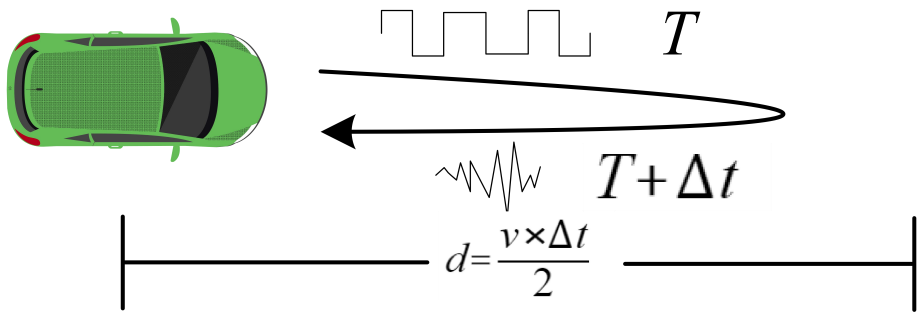


图 4 传感器测距原理：利用信号往返时间来计算距离。v是信号在空中的速度(如声音:340 m/s；电磁波和光: $3 \times 10^8\ m/s$)。

超声波传感器发送和接收超声波，利用反射超声波脉冲的传播时间来计算障碍物的距离，如图 4-4 所示。欺骗攻击与干扰攻击是车载超声波传感器面临的主要网络安全威胁。欺骗攻击试图利用精心制作的超声波来制造伪造障碍物，在超声波传感器检测范围内没有真实障碍物时欺骗智能网联汽车让其误以为存在真实的障碍物。干扰攻击的目的是通过不断发射超声波来降低超声波传感器的信噪比，诱导车辆无法探测障碍物。在智能网联汽车中，摄像头应用于交通标志识别、车道检测、障碍物检测等多种场景。用 LED 光或者激光直接照射摄像头可以致盲摄像头，致其无法发挥作用，可能导致严重事故。

表 2 汽车防盗系统网络安全威胁

防盗系统	安全机制	安全威胁	攻击类型
数字签名系统	挑战应答	短密钥	欺骗攻击
PKES	RFID 标签	虚假钥匙	中继攻击
Hitag2	48bit LFSR 及非线性过滤器	密钥空间，缺乏伪随机数发生器	密钥恢复
Megamous	96bit 安全密钥及 PIN 码	密钥空间，缺乏伪随机数发生器	密钥恢复
硬件加密	AES	密钥存储	故障注入

电子车辆防盗器作为一种常见的防盗装置，实现了电子防盗，在没有电子钥匙等可信认证实体的情况下禁止车辆发动机启动。为了追求便利性，汽车防盗系统多采用无线通信机制，具备一定的网络安全隐患。表 2 展示了不同汽车防盗机制的特性与网络安全威胁。其中，Hitag2 和 Megamos 都因密码设计的缺陷而面临相应的网络安全威胁，包括缺乏伪随机数生成器(PRGs)和比私钥更小的密钥空间。被动无钥匙进入系统（Passive Keyless Entry Systems，PKES）保证了车内物品的安全，也面临着信号中继的安全威胁。攻击者通过中继钥匙与汽车之间的通信信号可以成功开启车门。硬件加密的车载防盗系统面临侧信道攻击与故障注入攻击的威胁。

4. 车路云供应链安全解决方案

车路云供应链复杂的特性使其面临着严重的网络安全风险。为应对这些挑战，需要从汽车生命周期的多个阶段入手，构建一个全面的安全防护与检测体系。在设计阶段，必须在硬件和软件开发中融入安全设计原则，确保系统架构具备防御网络攻击的能力。在生产和供应链管理阶段，需要加强对供应商的网络安全审查，确保供应链中的每个环节都符合安全标准。在运行和维护阶段，必须实时监控和检测网络安全威胁，快速响应潜在的攻击。此外，系统退役时需对敏感数据进行安全销毁，以防止数据泄露。通过贯穿整个生命周期的网络安全管理，可以最大限度地降低车路云供应链中的安全风险，保障智能网联汽车的运行安全。V 型生命周期是汽车开发中广泛采用的一种系统工程方法，如图 5 所示，强调需求与验证的双向对应关系。网络安全作为车路云一体化的重要组成部分，必须在 V 型生命周期的各个阶段得到充分关注和解决。

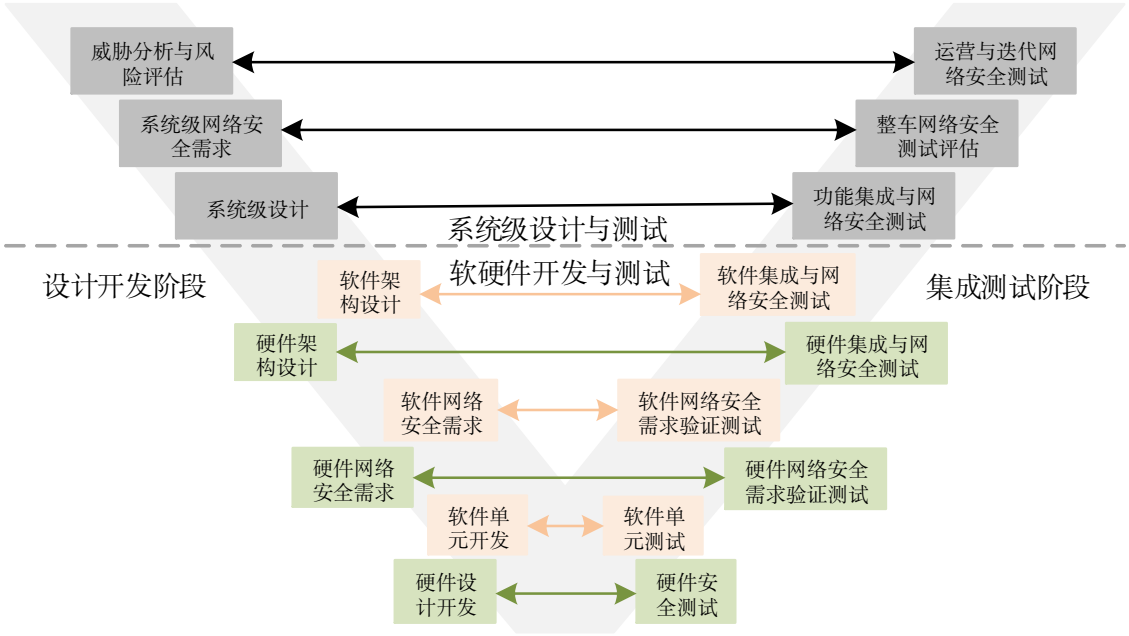


图 5 汽车开发 V 型生命周期

4.1 建立网络安全管理体系

汽车行业事实上的标准 ISO/SAE 21434:2021《道路车辆 网络安全工程》明确要求汽车制造商及其供应商需要建立覆盖车辆全生命周期的网络安全管理体系（Cyber Security Management System, CSMS）。CSMS 的建立不仅是行业法规的必要合规手段，更是保障智车联网网络安全的关键。

4.1.1 组织相关的网络安全管理

ISO/SAE 21434《道路车辆 网络安全工程》标准针对智能网联汽车的网络安全管理提出了全面的指导框架，其中与组织相关的网络安全活动被详细描述，明确了组织在网络安全管理中的角色和责任，为汽车制造商及其供应链合作伙伴建立和实施网络安全管理体系（CSMS）提供了依据。

网络安全治理。组织需要制定网络安全相关规章制度，建立明确的网络安全方针，阐明组织在网络安全方面的承诺、目标和原则。提供顶层设计，确保网络安全活动与组织战略目标保持一致。明确网络安全相关活动的部门、角色和职责，并保证相关能力的人员、技术和工具等资源支持。

（1）网络安全文化。提升全员的网络安全意识，确保员工能够识别和应对网络安全威胁。通过内部培训、工作坊和宣传活动，培养员工对网络安全的责任感和敏感性。将网络安全嵌入组织的日常运作中，形成〝人人关心网络安全〞的文化氛围。减少人为因素引发的安全事件风险，提高员工对潜在安全问题的主动发现和反馈能力。

（2）管理体系。建立覆盖整个产品开发和运营生命周期的网络安全管理体系，包括风险管理流程，确保网络安全风险被识别、评估和处理；网络安全信息管理，覆盖漏洞管理、威胁情报共享和事件响应；汽车及其产品生命周期覆盖，从概念设计到退役阶段均需实施网络安全活动。提供系统化的框架，用于管理网络安全风险。确保网络安全活动的一致性和持续改进。

（3）网络安全资源管理。确保组织具备足够的人力、技术和财务资源来执行网络安全活动。招聘具备专业技能的网络安全人员，定期培训员工，使其掌握最新的安全知识和技术；投资先进的网络安全工具（如漏洞扫描工具、渗透测试工具），建立实验室环境用于安全测试和验证；为网络安全活动分配专门预算，避免因资金不足影响安全目标的实现。通过资源的合理配置，保障网络安全活动高效开展。

（4）网络安全管理与组织网络安全审核。按照网络安全管理体系的要求来实施活动管理，以保护工作产物的保密性、完整性和可用性。组织进行网络安全体系审核，可与质量管理体系或信息安全管理体系审核结合进行，以判断组织的流程体系是否符合标准要求。

4.1.2 项目相关的网络安全管理

ISO/SAE 21434 标准规定了在项目层面进行网络安全管理的要求和活动，确保网络安全贯穿于汽车产品开

发的整个生命周期，从概念阶段到退役阶段。项目网络安全管理的核心目标是明确项目层面网络安全相关活动的角色和职责，识别网络安全开发范围，通过分析识别网络安全相关的组件，区分新开发组件和复用组件，并分析判断是否需要对安全活动进行裁剪。根据产品开发项目计划和裁剪原则，制定网络安全计划，确定网络安全活动，将网络安全要求融入到项目的每个阶段，确保产品的安全性能够满足预期的设计目标和法规要求。其重点在于系统化地规划、实施、验证和维护网络安全活动。主要活动包括：制定项目级的网络安全计划，确保网络安全与项目开发流程无缝集成，追踪网络安全活动的实施情况。

（1）网络安全计划。制定项目网络安全计划，明确项目中各阶段的安全目标、活动和责任。网络安全计划的内容包括项目范围内的网络安全需求，活动时间表和关键里程碑，网络安全活动所需资源（工具、人员、预算），风险管理策略与验证流程。通过制定网络安全计划统一协调项目中的所有网络安全相关工作，确保网络安全活动与项目开发同步进行。

（2）项目风险管理。在项目范围内执行网络安全风险管理，包括威胁分析与风险评估（TARA），风险优先级划分，制定风险减缓措施，确保每个阶段的设计与实现决策能够降低项目相关风险。通过风险管理将网络安全风险降到可接受的范围，确保风险管理覆盖项目中的每个子系统和组件，预防因风险管理缺失导致的项目延迟或安全问题。

（3）网络安全需求管理。从概念阶段开始，根据产品功能和威胁模型定义网络安全需求。需求管理活动包括收集与分解网络安全需求，确保需求在系统、子系统和组件之间的一致性，追踪需求的实现与验证状态。需求管理确保网络安全需求在项目中得到全面实现，减少因需求不明确导致的后期修改成本，提高设计的明确性和开发效率。

4.1.3 供应商分布式网络安全管理

由于现代汽车系统的复杂性和供应链的多样性，网络安全工作往往需要多个实体（包括原始设备制造商(OEM)、供应商、服务提供商）共同完成。这些分布式活动的重点在于确保在协作过程中网络安全责任的明确分配和执行。

（1）网络安全责任分配。在分布式环境下，将网络安全活动的责任清晰分配给各个相关方（如 OEM、一级供应商、二级供应商等）。每个实体明确其网络安全职责，包括需求、设计、实施、测试和运营阶段。在合同或协议中明确网络安全要求（如供应商需遵循的标准、所需的测试结果）。

（2）网络安全需求流转。从 OEM 到供应商再到次级供应商，网络安全需求需要在供应链中向下流转。确保上级设计的网络安全需求能够在下级实现中得到完整落实。向供应链合作伙伴传递明确的安全目标、风险模型和验证标准。需求流转保证了从系统级到组件级网络安全要求的一致性。

（3）信息共享与沟通。在分布式环境下，各方需要定期共享网络安全信息，包括漏洞、威胁情报和修复措施。使用行业共享平台进行安全情报协作。建立高效的沟通机制，确保问题能够快速得到反馈和解决。

（4）分布式风险管理。网络安全风险管理需要跨多个组织共同完成。各方需要协调进行威胁分析与风险评估（TARA），并在整个供应链中实施风险减缓措施。通过定期审查确保风险管理的持续性和一致性。

（5）分布式验证与测试。不同组织需分工完成各自负责部分的网络安全测试活动，OEM 负责系统级测试和集成测试。供应商负责组件级测试和接口测试。在分布式环境下，需统一测试标准和流程，以确保测试结果的可比较性和一致性。

（6）供应链网络安全管理。供应链中的每个环节都可能引入安全风险，必须进行有效的管理。供应商能力评估，确保其具备必要的网络安全技术能力。审核与监督，定期检查供应商的网络安全活动进展。引入独立评估机构验证供应商的网络安全能力。通过上述措施降低供应链网络安全风险。

4.1.4 持续的网络安全活动

持续性网络安全活动（Continuous Cybersecurity Activities） 通过持续的监测、分析、更新和改进，保持系统的网络安全性。这些活动贯穿于车辆的开发、生产、运营和退役阶段，确保系统能够有效应对动态的网络威胁环境。

（1）威胁监控与情报共享。持续监测与分析新兴威胁和攻击技术，包括零日漏洞、攻击工具和策略的变化。与行业联盟和第三方情报平台共享威胁情报，获取最新的攻击信息和防护建议。提高对潜在威胁的预见性和反应速度，减少企业单独应对复杂威胁的负担。

（2）漏洞管理与修复。持续发现系统中的潜在漏洞，包括开发阶段遗留漏洞和运营阶段新发现的漏洞。建立漏洞管理流程，包括漏洞检测、分类、评估、修复和验证。通过 OTA（空中下载）技术快速推送补丁和更新。确保系统漏洞能够被快速修复，减少暴露窗口期，保持车辆与相关产品软件和硬件的最新安全状态。防止漏洞被攻击者利用，造成安全事件。

（3）网络安全事件管理。建立事件响应流程，包括事件检测、分类、分析、处置和恢复。对发生的网络安全事件进行记录和分析，总结经验教训。定期开展应急演练，验证事件管理流程的有效性。减少网络安全事件对系统运行的影响，提升企业应对突发安全事件的能力。

（4）数据收集与分析。持续收集车辆运行过程中的网络安全相关数据，包括日志、流量信息和异常行为记录。利用大数据分析技术，识别潜在的攻击行为和安全隐患，提前发现潜在威胁，避免攻击造成实际损害。为后续的安全改进提供数据支持。

4.1.5 概念、开发、验证阶段网络安全活动

概念阶段网络安全活动目标是识别和定义系统的网络安全需求，评估潜在的安全威胁和风险，确定高层次的网络安全目标和策略。主要活动包括：威胁分析与风险评估（TARA），用于识别系统可能面临的威胁源和攻击路径，评估各类威胁的潜在影响和利用可能性，确定风险等级并优先处理高风险；定义网络安全目标，根据 TARA 结果确定需要保护的关键资产（如通信数据、硬件模块、用户隐私），明确系统在机密性、完整性和可用性方面的安全目标；初步系统范围划定，确定网络安全活动的范围，包括系统的边界、接口和关键子系统，描述各子系统的安全相关功能和依赖关系；建立网络安全需求，从网络安全目标出发，转化为高层次的网络安全需求，定义需求的优先级，并为后续开发阶段提供输入；制定网络安全计划，明确概念阶段的安全活动时间表，确保资源（如预算、人力和工具）满足网络安全要求。

开发阶段网络安全活动目标是将高层次的网络安全需求细化为可实现的技术要求。在设计和实现中嵌入网络安全功能，确保系统具备必要的防护能力。主要活动包括：网络安全需求分解，根据概念阶段的需求，将网络安全目标分解为子系统级和组件级的具体技术要求，明确每个模块需要实现的安全功能（如加密、认证、访问控制）；安全架构设计，设计整体系统的安全架构，定义各子系统和接口的安全措施，确定关键技术（如加密算法、密钥管理机制）和安全机制的位置；详细设计与实现，在代码层面实现网络安全功能：网络安全设计验证，确保设计满足安全需求，使用仿真工具或模型验证工具检查安全机制的正确性；供应链网络安全管理，与供应商协作，明确其需满足的安全要求，验证供应链提供的组件或服务是否符合安全规范。

验证阶段网络安全活动目标是确保系统在实现和集成后满足定义的网络安全需求。通过测试和分析验证系统在实际运行环境中的抗攻击能力。主要活动包括：功能验证，检查各模块的网络安全功能是否正确实现，数据加密是否正常工作；安全测试，执行静态测试、渗透测试、模糊测试等测试技术评估系统的抗攻击能力；系统集成测试，测试各子系统在集成后的协作安全性；验证合规性，确保系统符合 ISO/SAE 21434、UNECE WP.29 等

法规和行业标准的要求；漏洞修复与验证，针对测试中发现的漏洞进行修复，重新测试修复的功能，确保漏洞已被有效解决。

4.1.6 生产、运行、维护阶段网络安全活动

根据提出的生产阶段的网络安全要求，制定生产控制计划，包括生产工具和设备、网络安全控制措施以及核查网络安全规范的方法，并根据不同性质的网络安全事故，组织需制定网络安全事故响应计划。另外，组织需对相关项或组件进行更新。组织需建立沟通机制或流程，对于终止某个相关项或组件的网络安全支持，终止网络安全支持需向客户通报。另外，报废时组织需提供网络安全要求。

4.2 设计阶段开展威胁分析与风险评估

在设计阶段开展威胁分析与风险评估（TARA）是解决车路云供应链安全问题的重要方法。通过系统性识别潜在威胁和漏洞，评估其对供应链安全的影响，汽车制造商和供应链企业可以共同制定相应的防护措施。从源头进行 TARA 不仅能够优化系统架构设计，还能帮助上下游企业在产品开发初期协作应对安全挑战，显著降低供应链的整体安全风险。这一方法为构建安全可靠的车路云供应链提供了坚实的基础。

车路云供应链网络安全风险评估体系，包括资产识别、威胁分析、风险评估三个主要内容。资产识别确定评估范围以及系统中攻击者可能感兴趣的高价值资产，威胁分析系统地揭示了资产可能面临的潜在网络安全威胁及其对资产属性的影响程度。风险评估根据安全威胁的潜在危害对网络安全风险进行评级并基于风险制定网络安全目标。

4.2.1 网络安全资产识别

ISO/SAE 21434《道路车辆-网络安全工程》给出了实施 TARA 的指导性框架。如图 6 所示，风险评估体系应当包含三个阶段：资产识别阶段、威胁分析阶段、风险评估阶段。资产识别阶段定义目标系统、确认评估边界与假设，识别高价值资产；威胁分析阶段识别威胁场景，分析攻击路径，对网络安全威胁进行评级；风险评估阶段确定攻击概率，分析网络安全危害并对网络安全风险进行评级。在网络安全风险评估体系中，TARA 流程基于实际使用场景多次循环迭代，直至在可承受的成本下消除已知的重大网络安全风险。

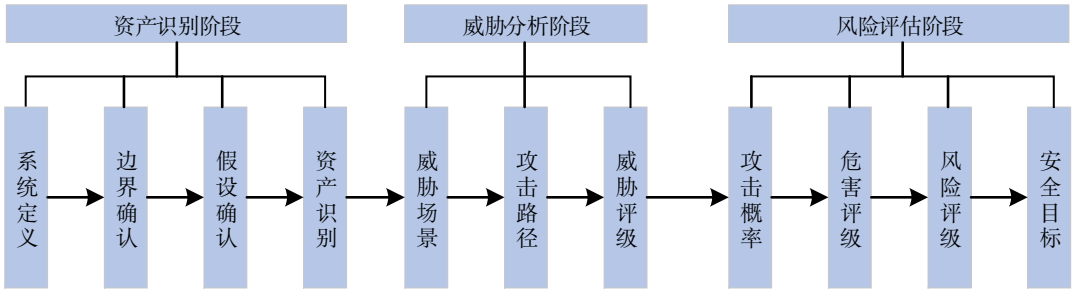


图 6 风险评估体系架构

（1） 系统定义

网络安全风险评估需要基于先验知识，在进行网络安全风险评估之前，有必要详细定义待评估的目标系统。系统定义需要包含系统功能设计、运行原理、软硬件组成等信息。通过系统定义，网络安全风险评估人员可以获取系统的高层功能与低层设计等基本信息，并基于这些信息制定后续网络安全评估计划。

（2） 边界确认

边界确认有助于限定网络安全风险评估范围，避免超出必要范围的扩大式评估，增加风险评估的复杂度，造成资源浪费。目标系统经过确切的定义之后便存在明确的物理与逻辑边界。物理边界限定了目标系统硬件范围内的组件，超出系统组件范围内的物理实体及组件均不在目标系统的物理边界之内，不属于需要评估的范围。同理，对于数据、功能等非硬件资产，逻辑边界限定了其范围。与目标系统无关的数据、功能等均不属于此系统的评估范围。

（3） 假设确认

〝假设〞解释了风险评估需要对环境做出的设定，以便被评估对象能够在假定条件下能够正确地提供功能。如果被评估对象被置于不满足假设条件的运行环境中，被评估对象可能无法成功运行或者无法正确提供相应的功能。〝假设〞可以限定运行环境的物理属性、人员交互、运行时条件等。

关于运行环境的物理假设指的是对环境的物理要求，例如假定被评估对象放置在最小化电磁辐射的房间内，或者假定被评估对象的访问控制台放置在限制访问区域等。人员交互假设指的是对与被评估对象交互的人员进行假设，例如假设用户经过足够的培训来操作被评估的对象，用户具备足够一定的网络安全意识，不会泄露账号密码。实时运行环境假设则是对运行需要的资源进行假设，例如假设工作站至少有 10GB 的可用磁盘空间来运行评估对象的软件等。

需要注意的是，假设在评估过程中被认为是正确的， 即假设中的内容不会在后续网络安全风险评估活动中被评估，默认情况下不会对目标系统造成安全威胁。基于此，评估人员只能对运行环境进行假设，决不能对评估对象的行为进行假设。

（4） 资产识别

“资产”在网络安全风险评估中表示需要保护的内容。站在攻击者的角度，资产是系统中值得关注的内容，有助于帮助其实施下一步攻击以破坏目标系统或者获得进一步的经济利益。智能网联汽车中的设备丰富多样、形态各异，具备大量对恶意攻击者具备吸引力的内容。这些内容具有多种表现形式，从文件、日志、数据库，到网络带宽、系统提供的服务、关键数据或设备的访问权限等。

尽管需要保护的信息内容形态各异，其本质上都会在信息系统设备中经历存储、传输、处理三个关键步骤，以满足信息所有者的需求。对于信息系统设备而言，众多的信息内容主要通过数据与服务的方式对展示给信息所有者。数据可能存在于非易失性存储设备、传输信道以及正在进行运算的处理器中。服务是信息系统设备与信息所有者或其他信息系统实体之间交互的方式，也是数据在不同实体之间传递的接口。一旦设备无法提供相应的服务，相关实体之间也失去了信息交互的渠道。权限则是服务与数据的访问控制机制，只有具备权限的实体才可以访问相应的资源，使用对应的服务。因此，本文提出的网络安全风险评估体系将资产分为三类：数据、服务、权限，TARA 均基于此三类资产开展。

1）数据：数据是在评估对象中存储、处理和传输的资产。攻击者可以获取和篡改数据资产，也可以通过冒充目标数据的授权用户或通信实体来访问并操纵数据资产。基于 CIA（Confidentiality，Integrity，Availability）[116]模型，数据资产的属性包括机密性、完整性和可用性。机密性保证只有特定权限的使用者才可以读写或更改数据。完整性保证数据在生命周期中无法被恶意篡改。可用性保证数据的合法使用者可以在需要的时候能够访问所需要的数据。

2）权限：被评估对象通常会基于不同的角色对系统资源设置不同级别的访问权限，不同级别的访问权限可以访问不同的资源。恶意攻击者往往希望获得更高级别的权限来访问更重要的资源。权限资产的属性是可用性，可用性保证具备权限的实体可访问及操作权限允许范围内的资源。

3）服务：服务是被评估对象外部提供的功能与接口，是被评估对象与外部实体进行交互的窗口。攻击者可以采取相应的行动，迫使目标失去对外提供服务的能力，从而影响目标服务的可用性。服务资产的属性是可用性，可用性保证了被评估对象具备正常提供服务的能力。

在开展网络安全风险评估的第一阶段，网络安全风险评估人员可通过头脑风暴方式识别目标系统中需要保护的高价值资产，包括存储、传输或者处理过程中的数据资产，系统提供的重要服务以及访问重要资源的权限，为后续威胁分析与风险评估奠定基础。

4.2.2 网络安全威胁分析

（1） 威胁场景与攻击路径

威胁是恶意攻击者针对目标资产的敌对行为，可以影响资产的一个或多个属性，例如密钥泄露威胁会影响目标资产的机密性。对目标资产造成安全威胁的实体可以是攻击者、用户、计算机进程、意外事件等。威胁场景分析基于系统中的高价值资产。如何全面准确的描述威胁场景成为威胁分析需要解决的重要内容。在本文提出的网络安全风险评估体系中，威胁场景通过攻击入口、威胁类型、攻击性质、攻击路径、攻击意图等信息描述，再现攻击者为了获取目标资产发动的攻击行为。威胁场景详细信息如下：

· 威胁名称：用于标识网络安全威胁场景。

· 威胁类型：本文提出的风险评估体系基于 STRIDE 威胁模型对智能网联汽车网络安全威胁进行分类，共有六种类型：仿冒 (Spoofing) 、篡改 (Tampering) 、抵赖 (Repudiation) 、信息泄露 (Information Disclosure) 、拒绝服务 (Denial of Service) 、特权提升（Elevation of Privilege）。

· 攻击性质：基于是否需要物理连接被攻击目标，攻击性质被分为三类：物理攻击、近场攻击、远程攻击。其中物理攻击需要物理接触目标设备，实施攻击的难度较大。近场攻击通过 Wi-Fi、NFC 等近场通信技术发起，无需物理接触攻击目标，成功实施的可能性相对较高。远程攻击通过蜂窝等远程通信技术发起，具备极大的便利性与覆盖范围。

· 攻击入口：清晰明了地表明网络安全攻击从何处发起。

· 攻击路径：描述安全威胁所对应的攻击路径，涉及的攻击入口及关键节点。

· 目标资产：表明安全威胁针对的系统资产。

攻击路径分析基于攻击入口与目标资产，分析人员基于攻击入口出发，分析攻击者获取目标资产所需要经历的关键节点，绘制出包含多条攻击路径的攻击树。攻击路径详细描述了攻击者成功发动攻击所经历的关键节点，

攻陷不同节点所需要的专业知识、攻击工具、付出的时间与经济成本等，为威胁等级评估奠定基础。

（2） 威胁等级评估

相较于传统信息设备，智能网联汽车有更为严格的网络安全要求，传统计算机网络安全事故造成的危害可能只是经济损失或隐私泄露，但智能网联汽车网络安全事故可能会造成生命财产损失。为了更精确地评估智能汽车网络安全风险，本文提出的网络安全风险评估体系将通用漏洞评分系统引入威胁分析，并在此基础上进行优化，增加适用于汽车领域的评分指标，使其更适用于智能网联汽车。

威胁等级评估需要考虑网络安全威胁的复杂度、先验知识、影响性。复杂度表征造成网络安全威胁的攻击具备的复杂程度，复杂度得分越高，该网络安全威胁越难以在现实中实现。先验知识表示发起具备网络安全威胁的攻击需要具备的先验知识，需要具备的先验知识越多，发起相应攻击的难度越大。影响性表示该网络安全威胁对目标资产的影响程度，影响性得分越高，该网络安全威胁对目标资产的影响越大。

4.2.3 网络安全风险评估

风险描述了网络安全威胁对智能网联汽车及其环境造成的危害。本文提出的风险等级分析综合考虑网络安全威胁转化为实际网络安全攻击的概率以及实际攻击事件对智能网联汽车及其环境造成的潜在危害。在评估网络安全攻击危害时着重考虑人身伤害、财产损失、功能失效、隐私泄露四个指标。

威胁分析暴露目标系统面临的网络安全威胁，风险评估揭露潜在的网络安全威胁风险。为了削减目标系统的网络安全风险，需要采取相应的安全措施，此安全措施即为安全目标。安全目标的制定基于 TARA 结果，旨在保护目标系统免于相应的网络安全威胁，规避相应的网络安全风险。

在概念设计阶段循环迭代资产识别、威胁分析与风险评估活动可不断完善设计方案，衍生出安全目标用于持续削减设计方案中存在的网络安全风险。为了削减部分网络安全风险而提出的安全目标也可能引入额外的网络安全风险，循环迭代上述活动则可以在下一轮 TARA 中削减被额外引入的网络安全风险。

（1） 不同网络安全风险评估方法比较

CVSS 是网络安全漏洞评分机制，解决网络安全漏洞的评级问题。网络安全风险评估体系将 CVSS 的评分机制引入智能网联汽车网络安全威胁的评级方法，并对评分参数进行了深度优化，使其更适用于汽车网络安全威胁评级。该机制一定程度上反映了不同参数对网络安全威胁等级的影响程度，弥补了 EVITA、HEAVENS 等 TARA

方法无法定量评估网络安全威胁的不足。

尽管攻击树模型也可以单独用于 TARA，且在分析攻击路径的可以同时附带攻击概率与攻击危害等参数以便于威胁与风险评估。但攻击树模型在网络安全风险评估体系中主要基于目标资产与攻击入口识别攻击路径，用于确定威胁场景。威胁评级、攻击概率、危害评级与风险评级则有相应的量化机制完成。

EVITA 模型虽然提供了资产识别、威胁分析与风险评估的相应方法，却缺乏详细的威胁与风险评价指标，无法精细量化智能网联汽车面临的网络安全威胁与风险。EVITA 中对于安全危害的评估仅仅基于安全、隐私、经济、功能粗略的划分为五个等级，未采用精确的评分机制。在安全威胁的复杂程度与攻击概率的评估中，EVITA 考虑的因素也仅限于攻击能力、专业知识水平等有限的几个因素，并未涉及对资产的影响程度、攻击范围、时间窗口等其他影响威胁复杂度与攻击概率评估的因素。

HEAVENS 相较于 EVITA 则具备更多的威胁分析与风险评估细节。HEAVENS 将威胁与资产及其属性之间建立映射关系，在威胁分析方面会对威胁进行分类与评级，但是在评级时依据的指标较少，仅有专业度、对评估对象的了解程度、时间窗口、攻击设备复杂度四个指标。

如表 3 所示，本文提出的智能网联汽车网络安全风险评估体系吸取了现有 TARA 模型的优点，综合了多种模型的可取之处并有所创新。相比于现存 TARA 方法，网络安全风险评估体系创新型地在资产识别阶段通过边界确认与假设确认明确评估边界，避免扩大评估范围。在威胁场景识别与攻击路径分析时采取了具备优势地攻击树模型，保证了基于目标资产与攻击入口两个条件可以全面识别系统面临地网络安全威胁。在对进行威胁评级时将 CVSS 机制引入并修改优化，在 HEAVENS 原有地四个指标基础上增加到 12 个指标，从威胁复杂度、先验知识、对资产地影响性三个方面对安全威胁进行评级。在风险评级时，除了考虑安全威胁导致的人身伤害、财产损失、隐私泄露、功能失效等安全危害，也考虑了威胁转化为实际攻击的可能性。

表 3 不同 TARA 方法比较

TARA 方法	资产识别				威胁分析			风险评估			
	系统定义	边界确认	假设确认	资产识别	威胁场景	攻击路径	威胁评级	攻击概率	危害评级	风险评级	安全目标
EVITA	✓			✓	✓	✓		✓		✓	

TARA 方法	资产识别			威胁分析			风险评估			
	系统定义	边界确认	假设确认	资产识别	威胁场景	攻击路径	威胁评级	攻击概率	危害评级	风险评级	安全目标
HEAVENS	✓			✓	✓		✓	✓	✓	✓	✓
攻击树	✓			✓	✓	✓		✓	✓	✓	✓
CVSS					✓			✓	✓		✓

4.3 开发阶段建立软件供应链安全管控体系

4.3.1 车路云软件供应链网络安全风险

〝软件定义汽车〞（SDV，Software Define Vehicle）逐步成为汽车行业对智能汽车演进方向的共识。以汽车为主体的车路云软件供应链具有技术体系复杂、供应链长、产业融合深的特点，网络安全形势严峻。其网络安全风险主要体现在如下方面：

（1）供应链企业在软件开发过程中的典型安全风险

目前，智能汽车行业软件供方数量庞大，已形成了由操作系统供方、自动驾驶供方、智能座舱供方、数据高精度地图供方、销售服务软件供方等共同组成的供应链生态。复杂多样的供应链在带来技术与服务的同时也存在着不可忽视的安全风险。1）软件开发环节：错误编码形成代码级安全缺陷、测试不充分形成功能级或逻辑级安全缺陷、开发工具污染引入后门；2）软件发布环节：主要存在因发布或交付渠道被恶意劫持而导致的恶意篡改风险；3）软件上线环节：主要存在运行环境污染、应急响应不及时、软件升级更新引发新漏洞等风险。以充电桩管理平台供方和客户代理商管理系统供方为例，通常这些系统不会直接与车辆进行交互以控制车辆，但这类软件系统在运营过程中会产生大量汽车行驶数据、存储用户个人信息，一旦所提供服务或工具存在软件漏洞，都有可能导致用户隐私和商业数据被盗取，甚至对人身财产、社会安全造成威胁。

（2）需方在软件采购与运维过程中的典型安全风险

从实践中可以看出，软件需方（如：整车厂）在软件采购交付环节与软件上线运维环节也存在典型的安全风险。1）采购交付环节：缺乏对供方软件供应链安全能力的识别，往往将重点放在供方资质审查，而忽视了对于组织战略、团队人员、资源配置等方面的综合研判；缺乏对供方软件产品的安全测试评估，往往将重点放在软件功能适配，而忽视了对于软件安全漏洞的检测与分析；2）上线运维环节：该环节的安全风险主要是软件运行环境污染、软件升级更新风险以及对汽车软件安全事件缺乏快速、完善、合理的安全运营和应急响应。

（3）开源软件使用造成的安全风险

软件的开源化趋势已成为主流，开源软件成为软件开发者开发代码的重要来源，大量使用开源软件在提升研发效率的同时也将开源软件的安全问题引入了智能汽车行业软件供应链。开源软件面临主要的风险包括以下 3 个方面。1）开源漏洞风险：根据新思科技《2022 年开源安全和风险分析》报告显示在航空航天、汽车、运输和物流行业被扫描的代码库中使用开源的比例高达 97%、包含开源漏洞的代码库占比为 60%。2）开源后门植入风险：攻击者会对暴露在外网的开源软件进行攻击，通过公开的已知漏洞获得服务权限，然后作为跳板开展安全攻击。3）开源数据泄漏风险：汽车软件供方的对外开源项目、贡献代码时无意或有意将未经信息清洗的代码公开到托管平台上去，导致涉及企业敏感数据或个人隐私信息公开，严重威胁企业与个人的财产和隐私安全。

4.3.2 车路云软件供应链安全管控体系

软件供应链是车路云供应链的重要组成部分，在开发阶段建立软件供应链安全管控体系是解决车路云网络安全风险的重要方法。通过对软件组件的来源、质量和安全性进行严格管理，汽车制造商和开发企业能够有效防范供应链中潜在的安全威胁。此外，采用自动化工具对代码进行审查和漏洞检测，结合版本控制和供应商认证机制，可进一步提高软件供应链的透明度和安全性，为车路云系统的长期稳定运行提供保障。针对供方在软件开发过程中的典型安全风险、需方在软件采购与运维过程中的典型安全风险、开源软件使用造成的安全风险，构建适用于车联网供应链安全治理体系，以控制软件供应链安全风险。

（1）软件供方的安全治理策略

对于车路云软件供方，应围绕软件生命周期开展安全治理工作。1）在组织机构方面，设置明确的软件供应链安全管理机构，为软件供方自身的软件供应链安全保障拟定战略、配置资源。2）在制度建设方面，建立有关软件产品的安全管理制度，包括但不限于涉及软件产品开发过程和软件产品运营过程的安全开发制度、应急响应制度、检测认证制度。3）在人员配备方面，配备具有相应能力、资质的安全管理与技术人员，并提供必要的软

件供应链安全培训。4）在工具配置方面，配备自身安全可靠、能够为汽车软件的安全质量提供支撑与保障的软硬件设备。汽车软件供方还需做好软件研发涉及的开源技术治理工作。通过建立专属的开源治理团队，与研发、基础设施管理、网络安全保障等团队联动，明确分工，共同维护开源安全。在研发管理规范中包含开源技术治理的相关条项，对开源组件使用安全意识、开源组件安全检测、开源组件使用具体操作、开源组件技术支持等具体实践进行指导和规范，确保开源组件及相关开源技术的合规使用与风险可控。配置开源组件管理工具，实现对开源组件有关引入审核、无效退出的安全管理，配置开源组件安全检测工具，实现对开源组件安全漏洞和许可证风险的安全管理。

（2）软件需方的安全治理策略

对于车路云软件需方，在软件采购和上线运维过程中从以下四个方面入手：建立软件供方管理体系、供方资质评估、供方产品安全风险评估、供方退出管理。1）建立软件供方管理体系：企业应根据自身业务情况，建立相应的软件供方管理制度、软件供方评价标准及安全框架；2）供方资质评估：根据制定的软件供方评估模型和相关标准，对符合要求的软件供方进行尽职调查，从企业资质、行业影响力、技术创新能力、软件交付质量、应急响应能力等多个维度进行综合资格评估；3）供方产品安全风险评估：对供方软件产品进行安全基线分析和安全风险评估，针对软件潜在的安全漏洞、风险以及可能造成的影响进行评估，确保产品安全；4）供方退出管理：供方合同结束时，应对合同进行复核，确保所有义务都已得到履行，随后进入退出程序，仔细考虑数据保存和处置，最后通过复盘不断优化迭代软件供方风险管理系统及供方准入机制。

（3）供需双方需配置的软件安全检测技术能力

软件供应链供需双方还需加强软件安全检测技术能力，有助于软件供方在软件开发过程中主动识别自研软件产品可能存在的安全缺陷和安全问题，也有助于软件需方在软件采购过程中检测评估拟购软件产品可能存在的安全缺陷和安全问题。典型的软件安全检测技术如下。

1）静态检测技术

静态检测技术对软件源程序和代码进行扫描，从语法、语义等方面分析并识别源程序和代码中存在的代码级缺陷。此检测技术不需要运行软件程序，而是通过语法分析、数据流分析等对程序源代码进行扫描并与其规则库比对，检测不符合安全规范的函数调用，即可识别源程序和代码中潜在的漏洞并定位所在位置。

2）软件成分分析技术

软件成分分析技术针对软件包含开源组件的安全问题进行识别。该技术主要包括两方面：1）开源代码片段分析，主要利用代码克隆分析技术以及机器学习分析引擎实现对代码片段成分的准确分析；2）开源软件安全检测，主要利用恶意代码识别技术、二进制特征匹配以及代码片段分析的结果。

3）模糊检测技术

模糊测试技术对软件质量缺陷进行检测。该技术以随机、意外或畸形的模糊数据作为输入，反复运行软件程序，在不了解测试对象内部操作机制的情况下对目标软件执行自动安全测试。模糊测试技术通过具备细粒度异常监控能力，能够将轻微异常信息进行捕获和分析，

从而识别对象软件的缺陷。

4）其他软件安全检测技术

针对汽车软件自身安全功能的有效性和可靠性，可通过典型软件测试方法进行验证。针对汽车软件中可能存在的后门，可通过异常流量检测技术发现后门被利用而引起的网络流量异常变化。针对汽车软件中可能存在的恶意操作，可通过应用软件动态分析技术对汽车软件运行时行为进行监测，发现对软硬件系统进行恶意操控和破坏。

4.4 测试阶段开展体系化网络安全测试

建立标准、规范的安全测试框架对于系统性开展智能网联汽车网络安全测试具有重要意义。车路云系统复杂，涉及供应链软硬件设备众多，安全测试是解决供应链威胁的重要方法之一。通过在开发和部署的各个阶段开展全面的安全测试，供应链中的潜在漏洞和风险可以被及时发现和修复。例如，在硬件和软件组件中进行渗透测试，可以显著提高系统的安全性。同时，自动化测试工具与人工审查相结合能够覆盖更多的潜在威胁场景，为供应链提供更强的抵御能力。安全测试作为供应链防护的重要环节，有助于构建更为稳固的车路云安全生态。

4.4.1 基于威胁的安全测试流程

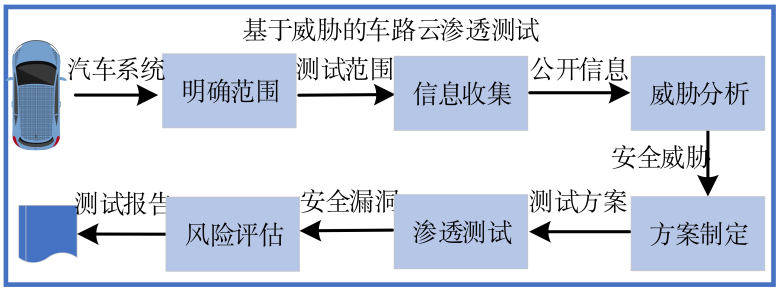


图 7 基于威胁的车路云安全测试流程

如图 7 所示，基于威胁的车路云安全测试将安全测试流程规范化为明确范围、信息收集、威胁分析、方案制定、安全测试、风险评估六个步骤。由于智能网联汽车是包含数十个 ECU、传感器的复杂网络，甚至与其他车辆、移动设备、车联网平台存在数据交互，在没有明确测试范围的情况下，安全测试人员无法把握测试边界，可能对正常的车辆功能与平台服务造成影响。明确测试范围解决了测试过程中测试边界不清晰，测试人员难以把握测试边界的问题。

在信息收集阶段，安全测试人员在授权测试权限内尽可能搜集与被测目标相关的信息，如网络地址、芯片型号、通信协议与接口等。官方网站、宣传页面、新闻报道等提供了大量有价值的公开信息。在授权情况下，测试人员亦可通过拆解测试目标获取硬件接口、芯片型号等关键信息。信息收集在安全测试过程中不断迭代，随着测试不断深入，可收集利用的信息也趋向丰富。

安全测试的目的是站在攻击者的角度对目标进行全面攻击性测试以发现潜在的网络安全漏洞。如何确定测试内容成为需要解决的首要挑战。威胁分析则为制定安全测试计划提供了参考。基于威胁的车路云安全测试流程以威胁分析为前提，测试人员利用攻击树等方法对被测目标进行威胁建模，识别其面临的网络安全威胁。安全测试方案则严格覆盖被测目标网络安全威胁，逐条测试安全威胁是否可演化为网络安全漏洞，导致严重的网络安全风险。

风险评估基于攻击成功发起的概率与造成的危害网络安全漏洞的严重性进行评级。网络安全威胁转化为漏洞的概率取决于攻击成功的复杂程度。攻击对人员的技术水平、攻击设备复杂度、攻击时间与经济成本等的要求越高，攻击越复杂，攻击成功的概率越小。攻击导致的危害则反应为不同程度的车辆功能失效、人身伤害、财产损失、隐私泄露。

4.4.2 车路云供应链安全测试框架

车路云供应链安全测试框架包含如图 8 所示的十个测试子框架：硬件安全测试框架、固件安全测试框架、系统安全测试框架、总线安全测试框架、无线电安全测试框架、网络安全测试框架、云端安全测试框架、应用安全测试框架、隐私安全测试框架、传感器安全测试框架。测试框架包含该层次的网络安全测试内容，不同测试子框架相互补充，可覆盖车路云不同供应商软硬件设备络安全测试。

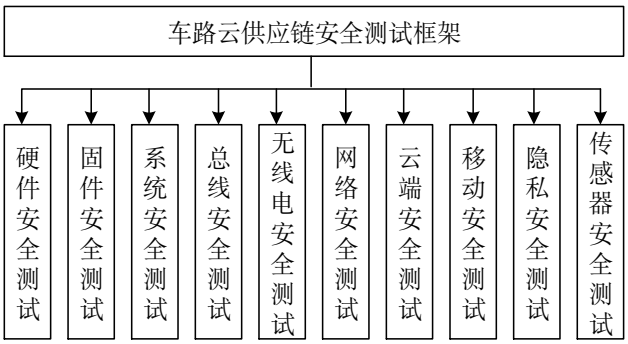


图 8 车路云供应链安全测试框架

传统的以信息娱乐系统等车辆模块为中心的安全测试方案需要为每一个待测试的车辆模块进行威胁建模、定制安全测试方案。基于安全测试人员的专业水平与不同厂商同类产品差异性，同类别车辆模块在不同测试场景下的安全测试方案显著不同，难以重复利用。该方案与待测试模块高度耦合，无法标准化，极大增加了安全测试难度。

相比于以车辆模块为中心的安全测试方案，车路云供应链安全测试框架将整车网络安全测试内容抽象为十个层次。测试内容绑定 JTAG 接口、Wi-Fi 模组等高细粒度的功能与软硬件模块，与待测试模块高度解耦。测试人员无需为每一个需要测试的模块定制安全测试方案，仅需要基于模块软硬件架构复用测试框架中相应的测试用例。层次化安全测试框架显然在一定程度上标准化安全测试内容，降低了安全测试难度，提高了安全测试效率。

（1）硬件安全测试框架

硬件安全测试框架评估车路云电子设备硬件板卡的网络安全性。如图 9 所示，硬件安全测试框架包括 PCB 安全测试、硬件接口安全测试、板载总线安全测试、芯片安全测试。PCB 安全测试评估电子设备 PCB 是否会泄露硬件接口、总线协议、芯片型号等重要信息。硬件接口测试包括 UART、JTAG、SWD、USB 等接口测试，一方面测试人员需要评估硬件接口是否会泄露诸如系统启动日志、系统硬件信息、存储映射信息、系统固件等敏

感信息及数据。另一方面，测试人员需要评估硬件接口是否会暴露系统命令行窗口，允许攻击者对被测系统进行调试以获取重要数据或执行恶意命令及程序。

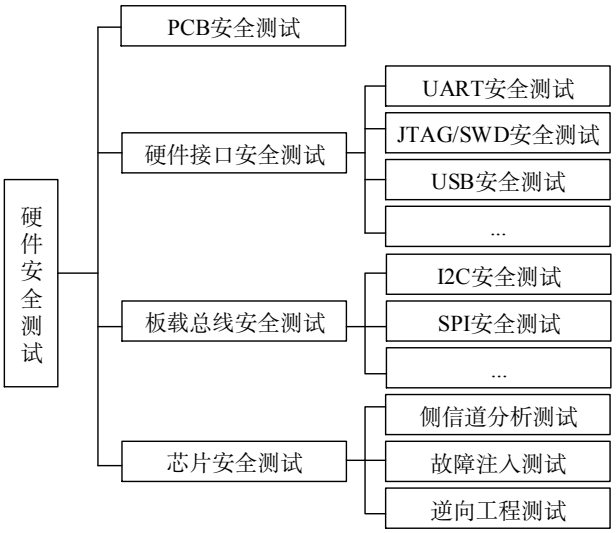


图 9 智能网联汽车硬件安全测试子框架

板载总线安全测试包括 I2C、SPI 等通信协议的安全测试。测试人员应评估总线上传输数据的机密性、完整性。芯片安全测试包括侧信道分析测试、故障注入测试、逆向工程测试。攻击者通过上述测试评估被测系统的关键芯片是否可以抵御功耗分析、电磁分析、时间分析等侧信道攻击；是否具备防止电压故障注入、电磁故障注入、光学故障注入等故障注入攻击的安全机制；是否具备防护逆向拆解的物理防护机制。

（2）固件安全测试框架

固件安全测试框架评估智能网联汽车 ECU 固件的网络安全风险。如图 10 所示，固件安全测试框架包含固件获取测试、固件加扰测试、信息获取测试、文件系统测试、静态安全测试、动态安全测试。固件获取测试要求测试人员从公共网络、空中下载机制、固件更新应应用程序、JTAG、SWD、UART、I2C 和 SPI 等方式尝试获取系统固件。如果测试人员可通过上述方式提取出固件，则固件存在信息泄露的安全风险。固件加扰测试需要安全测试人员评估被测系统的固件是否具备加密、压缩、加壳等安全防护机制。通过分析固件的熵值分布可判断固件是否具有加密或者压缩的保护机制。通过逆向分析工具简要分析固件的反汇编代码可判断固件是否存在保护壳。

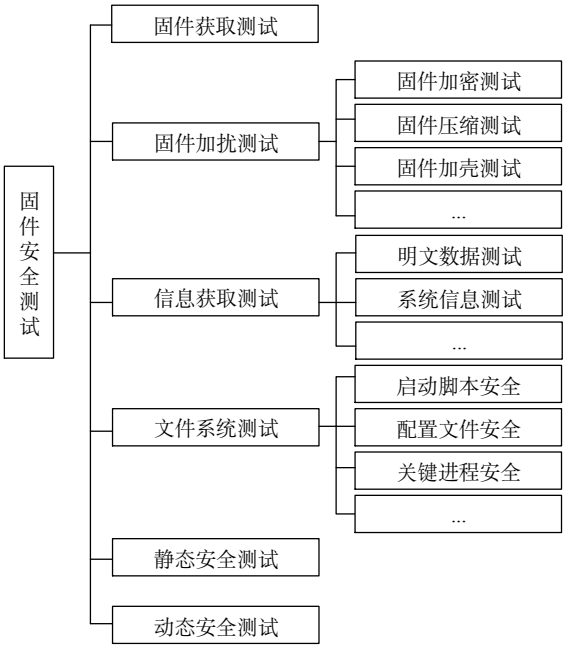


图 10 智能网联汽车固件安全测试框架

明文数据测试评估固件是否泄露认证口令、服务器 IP 地址、用户名等敏感数据。系统信息测试评估固件中是否存在特定格式的文件头以及符号表等泄露 CPU 架构、固件存储空间分布等关键信息的数据。文件系统测试需要测试人员对被测系统固件中的文件系统进行分析，查看其中是否存在关键的启动脚本、配置文件等。静态测试中，测试人员将目标固件导入到 IDA Pro 等固件逆向分析工具对固件进行逆向分析。借助工具，测试人员可获得固件中函数的调用逻辑，进而定位到加解密、安全认证等关键函数或者攻击者感兴趣的目标函数。动态分析则需要测试人员利用 QEMU[180]等仿真工具在仿真环境中运行目标固件，对目标固件进行包括模糊测试在内的动态测试。

（3）系统安全测试框架

系统安全测试框架评估被测系统操作系统面临的网络安全风险。基于传统互联网领域的网络安全测试经验，本项目提出的系统测试框架包括如图 11 所示的启动安全测试、运行安全测试、服务安全测试、应用安全测试、数据安全测试、配置安全测试以及访问控制测试。启动安全测试评估系统的启动过程，测试其 Bootloader、内核镜像、文件系统镜像在启动过程中是否存在被替换或恶意篡改的安全风险。运行安全测试用于评估运行过程中是否对关键文件及代码进行了有效的安全度量，防止系统加载了被恶意篡改或替换过的文件及代码，造成信息泄露或权限提升风险。应用安全测试则从数据、网络、服务交互等维度对系统内的应用程序进行安全评估。数据安全测试评估数据在生命周期中是否被安全存储与备份，攻击者是否可以篡改与解析数据内容。配置安全测试评估

安全人员是对系统进行了有基本的安全配置，如是否关闭了不必要的服务与端口等。访问控制测试从系统登陆、身份认证、防火墙等维度对关键服务及通信的访问控制机制进行评估。

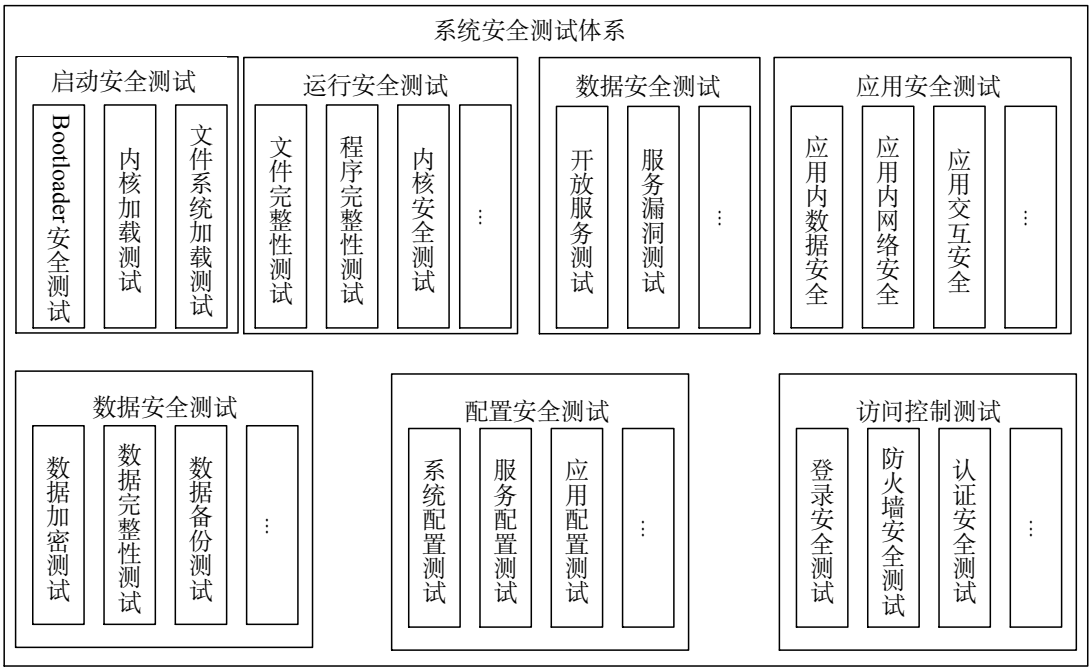


图 11 智能网联汽车系统安全测试框架

（4）总线安全测试框架

总线安全测试框架评估智能网联汽车车载总线网络的安全性。如图 12 所示，尽管车载总线网络包含多种总线协议，本项目基于车载总线通信的特点提出了覆盖当前车载总线协议的安全测试框架，包含加密测试、完整性校验测试、通信认证测试、拒绝服务测试、重放测试、通信矩阵测试、诊断服务测试、网络隔离测试、ECU 访问测试与模糊测试。

加密测试、完整性校验测试、认证测试、重放测试与拒绝服务测试是总线协议的基本测试项目，用于评估总线协议是否具备保护数据机密性、完整性、可用性、新鲜性、防欺骗性等机制，保证所传输数据的基本安全。此外，汽车制造商在总线数据帧的数据段会采用通信矩阵作为厂商私有协议描述车辆控制指令。通信矩阵测试评估攻击者是否可以轻易获取控制指令内容。网络隔离测试评估安全设计人员是否有效隔离车载网络中的不同总线网络。诊断服务测试评估攻击者获取并利用诊断指令查看、篡改车辆诊断数据的难易程度。ECU 访问测试评估攻击者通过总线网络访问并控制 ECU 节点的难以程度。模糊测试评估总线通信是否存在未知的可利用漏洞。

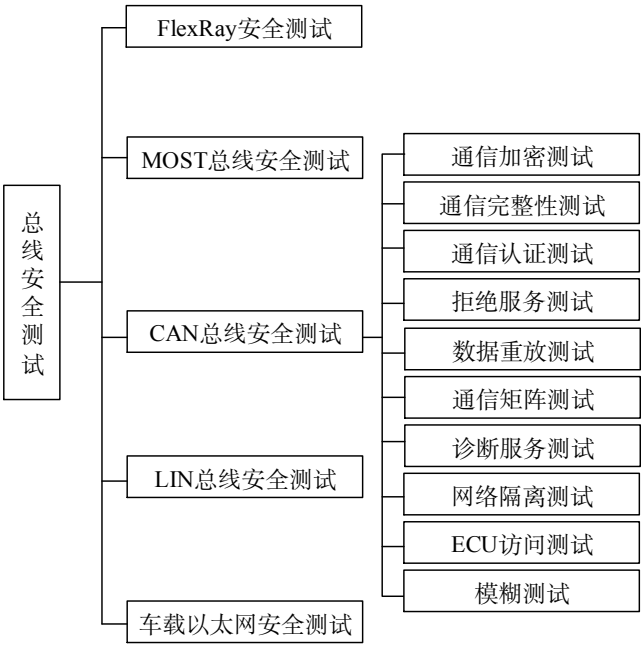


图 12 智能网联汽车总线安全测试框架

（5）无线电安全测试框架

无线电测试框架评估智能网联汽车无线通信系统安全风险。智能网联汽车无线通信协议主要包含 Bluetooth、Wi-Fi、NFC/RFID、蜂窝通信协议以及 DSRC，不同的通信协议采用不同的无线频段传输数据。无线通信协议安全评估遵循如图 13 所示的测试框架，包括漏洞利用测试、加密测试、完整性测试、认证测试、数据重放测试、数据中继测试、拒绝服务测试、中间人攻击测试、广播测试与模糊测试。

漏洞利用测试旨在评估被测试系统相关无线通信协议是否存在已知的可利用漏洞，测试人员需要关注相关协议的漏洞披露情况，研究已知的网络安全漏洞并开发漏洞验证测试程序。加密测试、完整性测试、认证测试、重放测试与拒绝服务测试评估被测系统无线电通信协议是否具备保护传输数据机密性、完整性、可用性、防止欺骗性、新鲜性的安全机制。中继测试评估被测系统是否可以抵御无线电通信中继攻击。中间人攻击评估被测系统是否采取了严格的双向认证机制，防止攻击者介入无线通信流程，窃取及篡改通信数据。广播测试评估相关协议的广播机制是否可被用于设备发现等，造成信息泄露。模糊测试用于发现无线电协议的未知恶意漏洞。

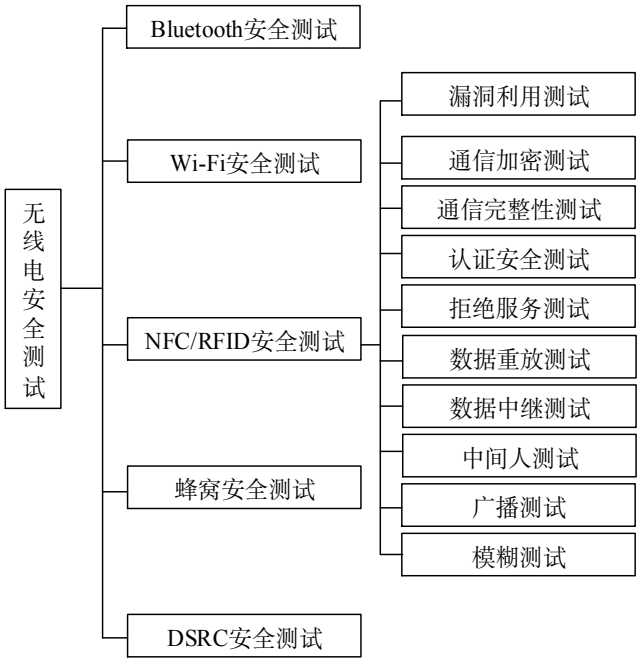


图 13 智能网联汽车无线电安全测试框架

（6）网络安全测试框架

网络安全测试框架与无线电通信测试框架有所不同，无线电通信测试框架关注于无线通信协议及其实现的网络安全风险测试，偏重于物理层及链路层，网络安全测试框架则关注在不同物理链路上数据传输安全，偏重于网络层、传输层及应用层。基于传统的网络安全测试经验，如图 14 所示的网络安全测试框架包含加密测试、完整性测试、通信认证测试、重放测试、拒绝服务测试、中间人 测试、模糊测试、漏洞利用测试、网络隔离测试。网络安全测试框架的测试方法与无线电测试框架相近，只是侧重的通信数据在开放系统互连（Open System Interconnect，OSI）模型中所处的层次不同，在此不再赘述。

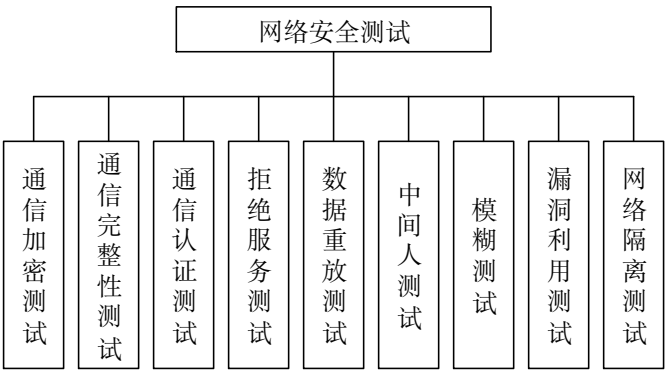


图 14 智能网联汽车网络安全测试框架

（7）云端安全测试框架

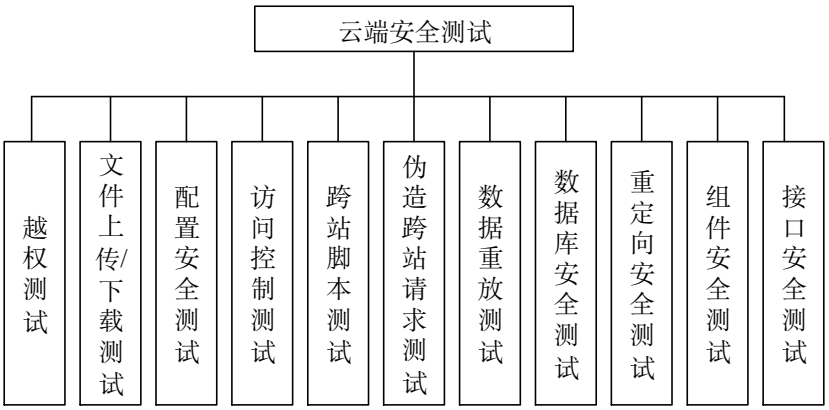


图 15 智能网联汽车云端安全测试框架

云端测试框架评估智能网联汽车云端服务平台网络安全风险。如图 15 所示，基于传统互联网领域 Web 安全测试经验，云端测试框架包含越权测试、配置测试等诸多测试项目。越权测试评估评估 Web 应用程序的权限管理是否正确合理，符合真实的业务需求。文件上传与下载测试评估 Web 应用程序是否正确处理文件格式、大小等，防止恶意代码通过文件上传到云端。配置安全测试评估安全人员是否安全配置 Web 服务器。访问控制测试评估 Web 服务器是否具备合理的访问控制策略。跨站脚本攻击测试、跨站请求伪造攻击测试、重定向安全测试等测试项评估目标 Web 服务器是否存在相应类型的网络安全漏洞。数据库安全测试评估数据库是否存在数据注入等网络安全风险。数据重放测试评估 Web 应用程序是否可以抵御重放攻击。组件安全与接口安全评估 Web 应用程序采用的接口与组件是否存在网络安全风险。

（8）应用安全测试框架

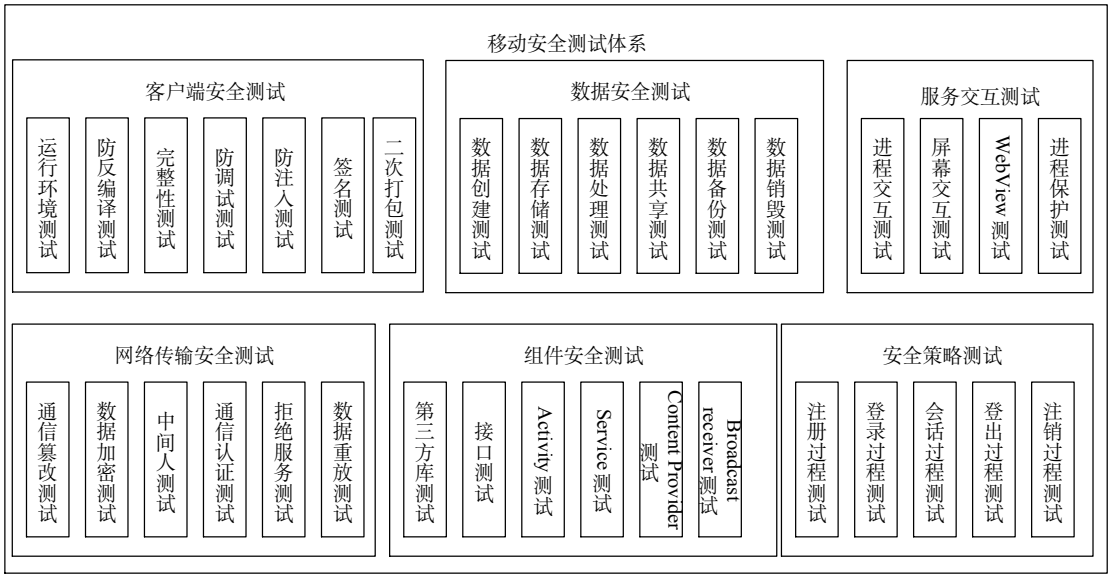


图 16 智能网联汽车应用安全测试框架

如图 16 所示，应用安全测试框架评估移动应用程序网络安全风险。客户端安全测试评估应用程序代码文件的安全性。攻击者可以通过 Apktool、dex2jar 等工具反编译应用程序文件，定位并解析应用程序中的关键代码，测试应用程序是否存在潜在的网络安全漏洞。在客户端运行过程中，测试人员可利用关键代码进行动态调试，验证静态反编译的分析结果，确认漏洞是否可以被有效利用。运行环境测试评估应用程序是否检测对环境进行最高权限检测。反编译防护测试评估安全人员是否对客户端代码进行加加密、混淆、加固等安全防护。完整性校验测试评估是否可以篡改客户端代码。调试防护测试评估客户端代码是否具备防止动态调试的安全机制。注入防护测试评估客户端代码是否存在进程保护和内存保护机制，防止被外部程序动态代码注入。签名、二次打包测试评估应用程序客户端是否可以被正确签名以及可以被二次打包。

进程交互测试评估跨进程通信是否可以保证通信数据的安全，避免隐私数据被不具备权限的进程访问造成信息泄露。屏幕交互测试评估应用程序使用期间是否可以防止屏幕被劫持、截屏、录屏。WebView 测试评估应用程序是否存在相关已知漏洞。进程保护测试评估应用程序是否存在保护进程交互数据的机制。

数据安全测试从数据创建、数据存储、数据处理、数据共享、数据备份、数据销毁全生命周期评估数据是否够得到安全管理。另一方面，部分数据会在移动应用程序与云端平台之间进行传输，网络安全测试则从加密、完整性校验、数据重放、拒绝服务、安全认证、中间人攻击等维度评估数据传输安全性。组件安全测试评估移动应用程序使用的组件及接口的安全性。安全策略测试评估用户创建及销毁过程中的安全处置策略是否合理。

（9）隐私安全测试框架

车联网服务中，用户车辆需要不断向周围车辆广播位置、速度、方向、身份等状态及身份信息。车辆状态及身份数据设计用户个人隐私，如遭不当利用，可危及用户人身及财产安全。隐私安全测试框架从身份隐私保护、位置隐私保护等维度评估被测试车辆是否保护用户的身份及位置等隐私数据。

（10）传感器安全测试框架

传感器安全测试框架评估智能网联汽车传感器的网络安全风险。如图 17 所示，基于现有攻击方式，本项目将传感器分为两类：携带基带数据的传感器；未携带基带数据的传感器。前者包括胎压监测系统、汽车防盗系统、导航定位系统等传感器系统，攻击者通常利用软件定义无线电工具监听并精确篡改此类系统中传输的数据。后者包括超声传感器、摄像头、激光雷达、毫米波雷达等传感器系统，一般用于测距、环境扫描等场景，攻击者并未精确篡改传感器数据，仅仅产生传感器信号以欺骗或者干扰传感器信号接收系统。

携带基带数据的传感器面临数据明文传输、无完整性校验机制、缺乏认证机制、缺乏消息新鲜性管理机制等基本数据传输风险。此外，本项目传感器测试框架还从拒绝服务、信号干扰两个维度评估目标传感器系统的健壮性。未携带基带数据的传感器则可从信号干扰、信号伪造、传感器失效、拒绝服务、信号处理算法安全性等维度进行网络安全评估。

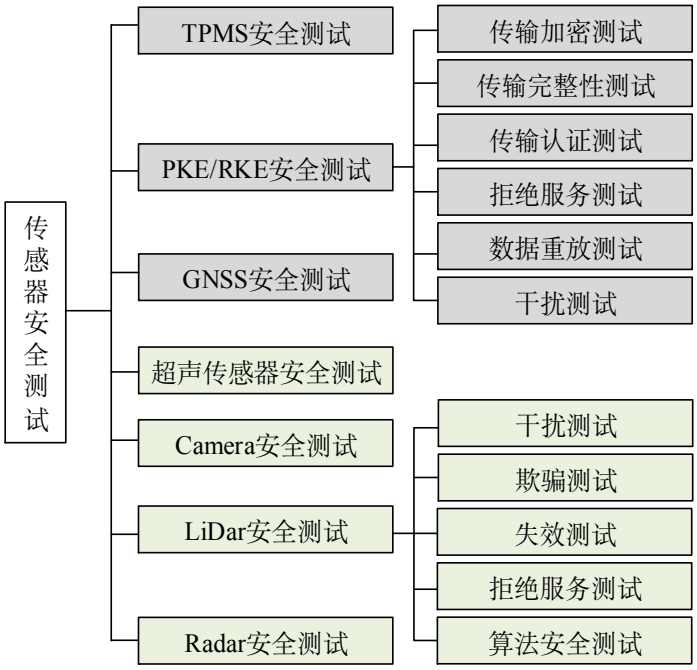


图 17 智能网联汽车传感器安全测试框架

4.5 运营阶段建立供应链漏洞管理体系

随着车路云技术的快速发展，供应链中的网络安全问题日益凸显。车路云供应链由零部件供应商、整车制造商、软件开发商和服务提供商等多方参与组成，涉及软硬件的复杂交互，面临复杂的供应链安全形势。潜在网络安全漏洞的可能导致数据泄露、系统瘫痪甚至车辆失控，对用户安全和行业信誉造成重大影响。建立车联网供应链网络安全漏洞管理平台是一种有效缓解漏洞危害的方法，通过实时监测和漏洞管理，降低攻击面，提升整体安全性。帮助车联网供应链企业满足如 ISO/SAE 21434、UNECE WP.29 等信息安全标准的要求。另一方面，供应链漏洞管理平台实现了从漏洞发现到修复的快速闭环，提高响应效率，降低潜在损失。同时为供应链各方提供协同平台，强化信息共享与合作。通过有效管理漏洞，降低安全事件发生概率，增强市场竞争力。

4.5.1 漏洞发现

在供应链安全管理中，漏洞发现作为整个漏洞管理生命周期的起点，是保障车联网网络安全的关键步骤，其全面性和准确性直接影响漏洞评估与修复的效果。随着企业网络安全建设的不断深入，漏洞发现的渠道变得越来越多，很多企业除了内部加强安全检测，渗透测试外，都有自己的 SRC 平台，这极大的促进了企业信息系统的完善跟优化。常见的漏洞来源渠道主要如下：

（1）技术性渠道。通过代码扫描工具、网络扫描工具、模糊测试工具等自动化扫描工具，实时监测系统、日志审计等安全监测系统以及手工代码审计等人工分析方式在技术层面发现潜在网络安全漏洞。

（2）组织性渠道。通过供应链厂商自测、企业内部安全测试等内部测试与评估，漏洞赏金计划、行业漏洞披露等漏洞披露计划，行业监管部门、情报平台等行业信息共享在组织层面尽力搜集相关漏洞信息。

（3）外部渠道。通过 CVE、CNNVD 等行业公开漏洞数据库，学术论文与技术报告等学术研究成果，开源项目、论坛等开源社区利用好外部数据资源建立漏洞数据库，为后续漏洞管理打下坚实基础。

漏洞发现过程应避免触碰法律界限，否则在漏洞发现过程中无意的违法违规行为会对发现者和漏洞处理的相关人员带来无法挽回的损失。漏洞发现者可能会违反与漏洞有关的保密协议（NDA）。当发现疑似没有修补的漏洞时，都应将漏洞报告给供应商。除非供应商已经公开报告过该漏洞，否则不应假定该厂商已意识到该漏洞。

4.5.2 漏洞评估

漏洞类型是漏洞管理的基础，一般都会分为一级大类，二级大类，一级大类主要根据技术层面划分，如主机安全、网络安全、应用安全、移动安全、终端安全等，当然还可以根据业务性质划分，如数据安全，业务安全等。一般来说，漏洞产生的原因，以及漏洞造成的结果，都可以成为二级分类的细分方向，有时候会考虑两者结合。

漏洞等级常见的区分方式有两种，一种是三级分类，一种是五级分类。三级分类就是高危、中危、低危；五级分类是严重、高危、中危、低危和告警。

三级分类，无论对于安全从业者，还是安全以外的管理者而言，都简单易懂。但是对具体场景如已经产生了或极易产生安全事件的漏洞（一般 5 级时是“严重”），仅作高危不能体现其程度和对时效性的要求，对于风险极低也难以被利用的漏洞，在人力资源紧张的情况下要求尽快修复也不合适（一般 5 级时定为“告警”）。

五级分类，由于可以选择的等级太多，对于模糊的时候，容易出现不同工程师对同一漏洞定级不一致的情况，这个出现差异的比例比三级分类时候大的多。对于后续漏洞分析、向管理者汇报时也多少有一定困扰。

等级评定标准依据为 CVSS v3(Common Vulnerability Scoring System，即“通用漏洞评分系统”)，根据漏洞对系统机密性（C）、完整性(I)、可用性(A)影响，将漏洞等级分为【严重】、【高危】、【中危】、【低危】四个等级。

CVSS 的好处在于提供了标准化的漏洞评分方法，涵盖了软件，硬件和固件漏洞的主要技术特征。其输出一些分数，这些分数表明了漏洞的严重性。CVSS 由三个度量标准组成：基本，时间和环境。基本评分根据漏洞的固有特征反映漏洞的严重性，漏洞的固有特征在一段时间内保持不变，并假设是在不同环境中最坏情况下的影响。时间指标基于随时间变化的因素（例如，漏洞代码的可用性）。环境度量标准是在特定环境下的基本评分和时间评分的组合，环境评分考虑了在该环境中存在缓解措施的影响。

基本分数通常由产品的相关组织或第三方来给出。通常仅发布基本度量标准，这些基本度量标准不会随时间变化，并且对于所有环境都是通用的。使用 CVSS 进行度量需要在基本度量标准的基础上添加时间评分和环境评分，以确定在特定环境中的严重程度。相关人员可以使用 CVSS 信息作为漏洞管理过程的一部分，漏洞管理还考

虑了不属于 CVSS 的因素，以便对威胁进行排名并做出补救。这些因素可能包括：客户数量，由于违约，生命或财产受到威胁而造成的金钱损失，或公众可信度。这些不在 CVSS 的范围内。

4.5.3 漏洞处理与修复

当以上的流程与标准都规范化后，就可以进入漏洞的处置流程了，这是漏洞管理中必不可少且非常重要的环节，发现的所有漏洞，都需要人员进行处理，跟进，直至漏洞修复，已到达规避、减少及降低风险的作用，更好的为业务服务。漏洞修复大致流程如下：

（1）漏洞录入

在漏洞验证完成后，安全工程师需要根据企业内部的漏洞等级划分标准，将存在的漏洞录入漏洞管理系统或工单系统中，我们是将漏洞管理系统与工单系统相结合的方式。

当漏洞创建成功后，会自动邮件通知漏洞修复人员，当漏洞的状态或内容有变动时，会实时邮件通知漏洞创建者及漏洞修复人员，当然对改漏洞关注的人员也可收到漏洞变更邮件，这样极大的提高了漏洞修复进度的实时性，能极大的提高漏洞修复率。

（2）漏洞分发

采用漏洞管理系统与工单系统相结合的方式，可以参考以下几点，这有助于减少安全工程师的工作量，提高工作效率以及漏洞修复率，也可为以后漏洞管理自动化做好准备。可以根据 URL/app 名称/ip/应用系统名称自动匹配部门和修复人；已有漏洞知识库，在选定某一类安全漏洞的时候，可以自动弹出该类漏洞的的修复方案和风险。

（3）漏洞跟进

漏洞录入漏洞管理系统后，就需要有人员进行跟进、处理，不然漏洞迟迟不修复，也无法达到规避、减少或降低风险的目的，采用的是下面的方法：录入时，自动邮件告知系统负责人；根据漏洞等级设定的时效性，设置修复计划时间，修复计划时间到期，自动发送邮件至系统负责人邮箱提醒；每周一，梳理修复计划已过期且未修改修复计划的漏洞，会在漏洞周报中重点标明；超过两个修复周期的漏洞，邮件抄送部门领导。

（4）漏洞修复周期

漏洞修复周期，包括漏洞的验证、评估、分发、复验、修复和关闭的各个环节。漏洞的修复周期，会根据漏洞等级确定。当然，以上各种修复修复周期要求都是参考，实际执行的时候，需要给安全工程师和业务同事，拥有“延期”的权限，不同等级延期要求不同，但不能超过修复时间的 2 个周期，当然特殊情况按特殊处理，

（5）漏洞数据分析

对于漏洞管理整个流程来说，漏洞缓解或已解决后，关闭工单不是最终的目的，需要对漏洞数据进行分析，持续运营。例如，统计一段时间内，外网系统出现的次数最多的 Top10 漏洞排名，分析漏洞出现的原因；自主开发系统中漏洞数量最多的 Top10 系统排名，分析造成的原因；哪些供应商的开发的系统漏洞数量最多？分析存在的原因；是否需要约谈供应商沟通，是安全开发能力的问题，还是研发安全意识不够？

4.5.4 协同漏洞披露

当供应商或漏洞处理人员收到漏洞报告时，需要将其与正在处理的其他漏洞，正在进行的新功能开发以及其他非安全错误修复的工作进行优先级排序。验证漏洞报告真实性以及准确性。在真实准确基础上，对于那些供应商认为合法且有价值的漏洞报告，对每个漏洞的严重程度进行度量与分级。可以通过提供补丁来修复漏洞。或者利用其他缓解手段作为临时解决方案。

在大多数情况下，供应商通过对漏洞的充分分析，会创建并发布修补程序来对漏洞进行修复。但有时无法及时解决问题，供应商或第三方会采取一些缓解漏洞影响的措施作为临时解决方案。

在公开发布漏洞之前，提出草案描述漏洞有利于帮助 CVD 参与者进行讨论和评论。至少报告者和供应商应该共享一份建议草案，以使双方对漏洞披露的进度都完全了解。理想情况下，双方都有机会更正错误的信息，并明确过程中每个人的职责。如果多个供应商收到影响，也应让他们参与草案，以此来获得更多的反馈，同时还确保了用去发布补丁和披露漏洞的渠道。一旦草案完成，下一步就是将漏洞文档发布到先前确定的渠道中。

漏洞一经披露，供应商和报告者都应积极寻求有关文档或补丁任何问题的反馈。某些情况下，者可以采取技术监视的形式（例如，监视来自供应商的更新服务下载日志，检查已部署系统版本的清单，甚至进行扫描）以确定防御程序的部署进度。即使不可能，不允许，有风险，昂贵或其他不切实际的技术监视，通常也可以通过支持请求，在线讨论等监视用户的反馈。

5. 车路云供应链网络安全案例

5.1 电子不停车收费系统 OBU 风险评估案例

（1） OBU 资产识别

1) OBU 系统定义与评估边界确认

电子不停车收费系统（Electronic Toll Collection，ETC）是解决高速公路及城市停车场收费效率低下的关键技术。ETC 系统在车载单元（On board Unit，OBU）与路侧单元（Road Side Unit，RSU）之间利用 DSRC 技术进行无线通信，实现在不停车通过收费站的情况下缴纳路桥费用。OBU 在 ETC 系统中同时兼具通信与信息存储的作用。一方面，OBU 存储车辆信息、道路信息、车主信息等用于路桥费用结算。另一方面，OBU 与 RSU 之间进行 DSRC 通信。依据供电方式，OBU 分为主动式与被动式，主动式为有源 OBU，唤醒之后主动发送 OBU 中存储的车辆信息。被动式为无源 OBU，通过感应电流传递相关信息。

案例所选取的分析对象为一款主动双片式前装 OBU。该 OBU 使用 BLE 芯片，具备 BLE 通信能力；使用 SE 安全芯片，具备安全存储与数据加解密能力；使用 CAN 控制器，具备与车载 CAN 总线通信能力；使用 MCU 协调控制 OBU 各个模块之间的协同运行；使用 ETC 射频芯片处理 DSRC 通信数据，可与 RSU 无线通信；提供 UART、SWD、CAN、BLE、ISO7816 等外部接口；使用 I^2C、SPI 总线用于各个模块之间的数据传输。

2) 评估假设确认及 OBU 资产识别

假设描述了目标 OBU 可以稳定正常运行的前置条件，排除 OBU 因为制造、操作不当、管理不当等导致的网络安全威胁。OBU 风险评估假设如表 4 所示。

表 4 OBU 假设

假设名称	假设描述
安全制造	在 OBU 生命周期的制造集成阶段，假设采取了合适的技术以及措施保证了 OBU 资产的安全，包括初始密钥等材料的产生、安装和导入。
安全操作	在 OBU 生命周期各个阶段，假设对目标 OBU 的操作均按照标准流程执行，不会因为操作不当对 OBU 资产造成损害。

假设名称	假设描述
安全管理	假设与目标 OBU 相关的材料，如文件、数据、密钥等都在管理方的控制之下，不会发生材料泄露事件。
可信人员	假设在 OBU 投放到市场之前所有接触到 OBU 的技术人员、管理人员均是可信的，不会对 OBU 资产造成安全威胁。
物理保护	假设 OBU 产品拥有相应的物理保护机制。
运行正常	假设 OBU 在生命周期的运行阶段正常运行。

基于 OBU 设备信息，本文提出的威胁模型从硬件安全、固件安全、通信安全、数据安全四个维度识别 OBU 中具有利用价值的资产。

1）硬件安全。硬件安全囊括了设备硬件可能导致的网络安全问题，具体包括印刷电路板（Printed Circuit Board，PCB）安全、总线安全、硬件接口安全、芯片安全。恶意攻击者通过 PCB 板可以获取目标设备采用的芯片型号、硬件接口引脚、总线通信类型，通过硬件接口可以获取目标设备的启动信息、调试权限、交互数据、设备固件、内部存储数据等信息，通过总线可以获取模块通信数据、内部存储数据等信息，通过芯片分析可以获取芯片功耗、运行时间、电磁信息等信息，进而推断出密钥、随机数等关键敏感数据。

2）固件安全。获取设备固件对于恶意攻击者而言具有重要意义，不仅因为通过逆向分析可以揭露目标设备的运行逻辑，也因为开发人员的疏忽可能导致密钥、网址、账号、邮箱等敏感信息被硬编码在固件中而遭到泄露。

3）通信安全。通信安全涉及目标设备所有通信类型的全部流程，包括通信数据机密性、完整性、可用性、防重放性、防中继机制以及通信实体之间的身份认证。恶意攻击可以监听通信信道获取并操作通信数据，如果通信数据未加密，攻击者可以了解通信内容，如果通信数据无完整性校验，攻击者可以篡改通信内容，如果通信实体之间无身份认证机制，攻击者可以仿冒通信实体以及发动中间人攻击，如果通信数据无防重放机制，攻击者可以重放通信数据，如果通信协议无防中继机制，攻击者可以中继通信数据。

4）数据安全。数据安全指的是经过目标设备严格保护的数据存在的安全问题，例如安全芯片中存储的数据同样可能存在数据安全威胁。恶意攻击者可能通过芯片安全分析获取安全芯片中存储的敏感数据，导致数据泄露、数据篡改等数据安全威胁。硬件安全、固件安全、通信安全同样可以导致数据安全威胁，已在前述维度进行讨论，

故此维度并不重复讨论。

基于上述四个维度，本次分析的目标 OBU 具有价值的安全资产如表 5 所示。其中机密性标注该资产是否需要机密性保护以避免攻击者可以直接获取，完整性标注该资产是否需要完整性保护以避免攻击者可以随意篡改，可用性标注该资产是否需要可用性保护以免攻击者可以随意使用或者使其拒绝服务。

表 5 OBU 资产

资产	机密性	完整性	可用性	资产类型
PCB 芯片印字	✓			数据
PCB 引脚印字	✓			数据
UART 交互数据	✓			数据
UART 调试权限			✓	权限
SWD 交互数据	✓			数据
SWD 调试权限			✓	权限
OBU 固件逻辑	✓			数据
OBU 固件敏感数据	✓			数据
I^2C 总线数据	✓			数据
SPI 总线数据	✓			数据
DSRC 通信数据	✓	✓	✓	数据
BLE 通信数据	✓	✓	✓	数据
BLE 通信服务			✓	服务

CAN 通信数据	✓	✓	✓	数据
CAN 总线服务			✓	服务
ISO7816 通信数据	✓	✓	✓	数据
安全芯片数据	✓	✓	✓	数据

（2） OBU 威胁分析

基于资产与假设，OBU 威胁分析结果如表 6 所示。依据攻击者的攻击路径，可将安全威胁分为两类：1）本地威胁，攻击者物理接触 OBU 及其各个模块向目标 OBU 发起攻击造成的威胁，UART 接口、SWD 接口等威胁均属于本地威胁。2）远程威胁，攻击者通过无线方式远程发起攻击造成的威胁，DSRC 通信、BLE 通信等威胁均属于远程威胁。安全威胁中，攻击者均以获取、篡改 OBU 存储与传输的数据，或者获取、拒绝 OBU 权限与服务为最终目的。

表 6 OBU 安全威胁

威胁名称	威胁描述	威胁类型	攻击入口	攻击性质
PCB 数据泄露	PCB 印字可泄露芯片型号、总线协议、接口引脚等信息。	信息泄露	PCB	物理接触
UART 数据泄露	UART 接口可泄露启动信息、系统运行数据等数据。	信息泄露	UART	物理接触
UART 调试权限	UART 获取系统调试权限。	权限提升	UART	物理接触
SWD 数据泄露	SWD 接口可泄露启动信息、系统运行数据等数据。	信息泄露	SWD	物理接触
SWD 调试权限	SWD 获取系统调试权限。	权限提升	SWD	物理接触

固件逻辑泄露	固件泄露系统运行逻辑。	信息泄露	SWD/UART	物理接触
固件数据泄露	固件泄露关键敏感数据。	信息泄露	SWD/UART	物理接触
固件篡改	篡改固件运行逻辑。	篡改	SWD/UART	物理接触
I^2C 总线监听	攻击者监听 I^2C 总线数据。	信息泄露	I^2C	物理接触
I^2C 总线篡改	攻击者篡改 I^2C 总线数。	篡改	I^2C	物理接触
SPI 总线监听	攻击者监听 SPI 总线数据。	信息泄露	SPI	物理接触
SPI 总线篡改	攻击者篡改 SPI 总线数据。	篡改	SPI	物理接触
BLE 通信监听	攻击者监听 BLE 通信数据。	信息泄露	BLE	近场无线
BLE 通信篡改	攻击者篡改 BLE 通信数据。	篡改	BLE	近场无线
BLE 通信仿冒	攻击者伪造 BLE 通信实体。	仿冒	BLE	近场无线
BLE 拒绝服务	攻击者干扰 BLE 通信服务。	拒绝服务	BLE	近场无线
DSRC 通信监听	攻击者监听 DSRC 通信数据。	信息泄露	DSRC	近场无线
DSRC 通信篡改	攻击者篡改 DSRC 通信数据。	篡改	DSRC	近场无线
DSRC 通信仿冒	攻击者仿冒 DSRC 通信实体。	仿冒	DSRC	近场无线
ISO7816 监听	攻击者监听通信数据。	信息泄露	ISO7816	物理接触
ISO7816 篡改	攻击者篡改通信数据。	篡改	ISO7816	物理接触
CAN 总线监听	攻击者监听 CAN 总线数据。	信息泄露	CAN	物理接触
CAN 总线篡改	攻击者篡改 CAN 总线数据。	篡改	CAN	物理接触
CAN 总线仿冒	攻击者仿冒 CAN 总线实体。	仿冒	CAN	物理接触

CAN 拒绝服务	攻击者干扰 CAN 总线通信。	拒绝服务	CAN	物理接触
SE 数据泄露	攻击者获取 SE 存储数据。	信息泄露	SE	物理接触
SE 数据篡改	攻击者篡改 SE 存储数据。	篡改	SE	物理接触

（3） OBU 风险评估

基于网络安全风险评估体系中的威胁评级与危害评级机制可计算出安全威胁等级与安全危害等级。基于安全风险等级矩阵可得到如表 7 所示的安全风险等级。等级越高，安全风险越大。

表 7 OBU 安全风险等级

威胁名称	安全威胁等级	安全危害等级	安全风险等级
PCB 数据泄露	中	低	低
UART 数据泄露	中	低	低
UART 调试权限	低	高	中
SWD 数据泄露	中	低	低
SWD 调试权限	低	高	中
固件逻辑泄露	中	高	中
固件数据泄露	中	高	中
固件篡改	中	高危	高
I^2C 总线监听	低	中	低
I^2C 总线篡改	低	中	低
SPI 总线监听	低	中	低

SPI 总线篡改	低	中	低
BLE 通信监听	中	中	中
BLE 通信篡改	低	高	低
BLE 通信仿冒	低	高	低
BLE 拒绝服务	低	高	低
DSRC 通信监听	中	中	中
DSRC 通信篡改	低	高	低
DSRC 通信仿冒	低	高	低
ISO7816 监听	低	中	低
ISO7816 篡改	低	中	低
CAN 总线监听	中	中	中
CAN 总线篡改	中	高	中
CAN 总线仿冒	中	高	中
CAN 拒绝服务	中	高	中
SE 数据泄露	低	中	低
SE 数据篡改	低	高	低

（4） OBU 安全目标

基于 TARA 结果，OBU 面临的网络安全威胁及其潜在网络安全风险均已清晰。网络安全风险评估体系意在用于智能网联汽车生命周期的概念设计阶段减少产品设计方案中存在的网络安全风险。但其作用不仅仅如此，该风险评估体系亦可用于产品开发完成之后的风险评估，指导安全测试。OBU 风险评估结果在理论上会衍生出安

全目标，安全目标便是安全测试通过与否的依据。如果安全测试表明 OBU 达到了安全目标，则 OBU 不存在相关的网络安全威胁，否则 OBU 面临相应的网络安全风险。

表 8 OBU 安全目标

威胁名称	安全目标
PCB 数据泄露	无 PCB 数据泄露
UART 数据泄露	无 UART 数据泄露
UART 调试权限	无 UART 调试权限
SWD 数据泄露	无 SWD 数据泄露
SWD 调试权限	无 SWD 调试权限
固件逻辑泄露	无固件逻辑泄露
固件数据泄露	无固件数据泄露
固件篡改	固件不可篡改
I^2C 总线监听	防 I^2C 总线监听
I^2C 总线篡改	防 I^2C 总线篡改
SPI 总线监听	防 SPI 总线监听
SPI 总线篡改	防 SPI 总线篡改
BLE 通信监听	防 BLE 通信监听
BLE 通信篡改	防 BLE 通信篡改
BLE 通信仿冒	防 BLE 通信仿冒

BLE 拒绝服务	防 BLE 拒绝服务
DSRC 通信监听	防 DSRC 通信监听
DSRC 通信篡改	防 DSRC 通信篡改
DSRC 通信仿冒	防 DSRC 通信仿冒
ISO7816 监听	防 ISO7816 监听
ISO7816 篡改	防 ISO7816 篡改
CAN 总线监听	防 CAN 总线监听
CAN 总线篡改	防 CAN 总线篡改
CAN 总线仿冒	防 CAN 总线仿冒
CAN 拒绝服务	防 CAN 拒绝服务
SE 数据泄露	防 SE 数据泄露
SE 数据篡改	防 SE 数据篡改

5.2 软件供应链安全管控案例

面对越来越严苛的网络安全要求，主机厂与其供应链企业逐步将网络安全建设左移，在研发阶段尽量解决网络安全风险问题。为应对软件开发中的安全风险问题，某主机厂在内部建立软件供应链安全管控平台，集中解决软件开发过程中的安全风险问题。

（1）软件供应链安全管控平台需求

1）平台具备项目管理角色功能，例如：项目经理+PMO+安全人员，实现不同角色的管理，不同管理角色有不同视角和管理权限。

2）平台支持在开发过程中能根据业务形态场景定义不同的安全需求。

3）平台支持安全需求产生，能自动基于安全需求关联产生测试用例。

4）平台能够对接各种安全检测工具，可对软件供应链产品进行体系化安全测试。

5）平台能对接企业内部账号管理平台、邮件系统、OA 系统、培训系统

6）平台能集成车联网威胁建模功能，把车联网的安全需求，在台统一管理

7）软件开发整个项目生命周期安全管理也加入平台

8）支持安全知识库，可标注知识库来源

9）平台支持汽车相关网络安全漏洞管理

（2）平台架构设计

软件供应链安全管控平台目前设计理念是重点关注安全因素的软件开发项目管理平台，通过安全赋能对接其他业务需求、研发管理、功能测试管理、企业各种管理。包含的安全实践活动覆盖软件安全开发全生命周期。

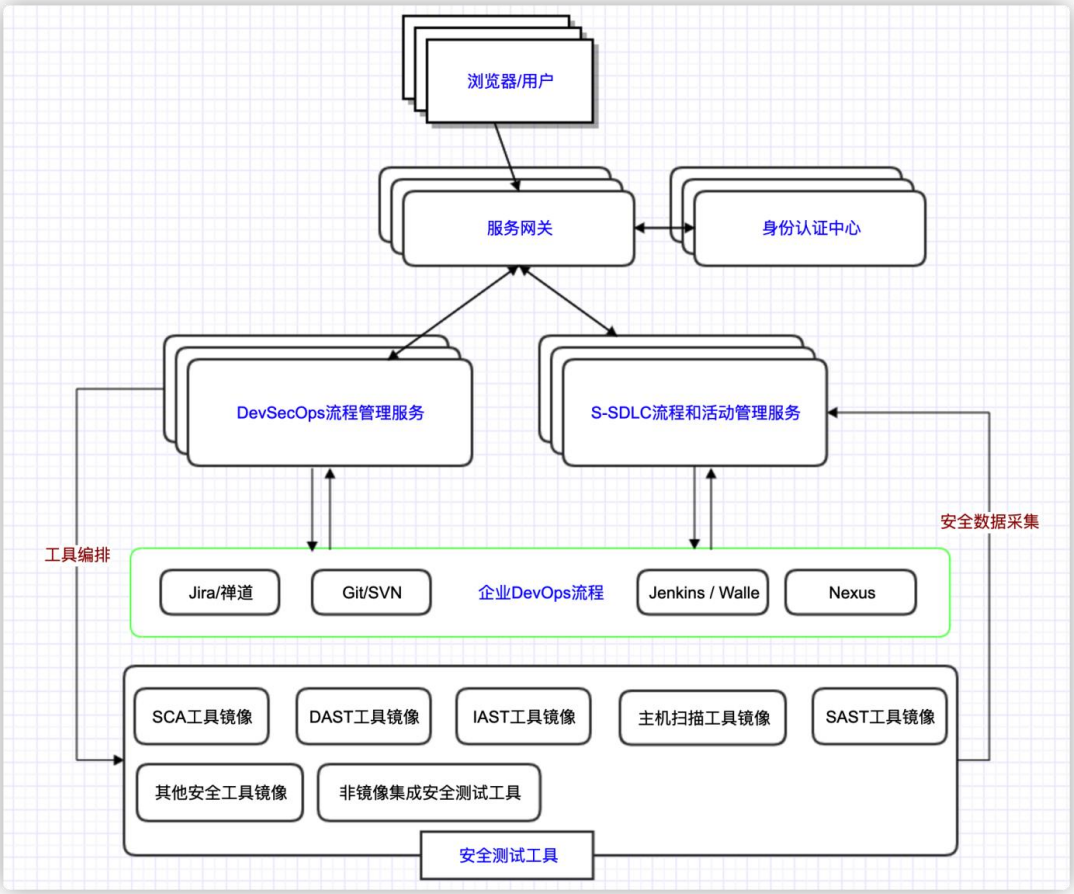


图 18 软件供应链安全管控平台架构

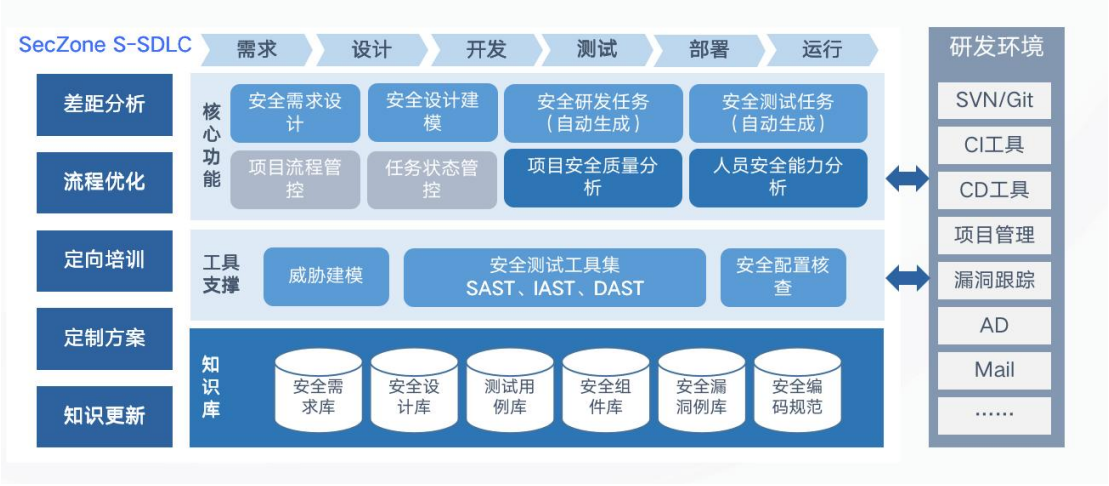


图 19 软件供应链安全管控平台应用场景

(3) 项目角色权限管理

平台可以基于角色管理用户和权限，能够为用户(角色)分配系统中所能操作的权限。项目/任务管理(增删改查)角色与项目/任务评审角色分开，基于角色的权限隔离和数据隔离，不同角色用户登录，展示不同页面内容，例如：

项目经理：只可看到自己管理的项目，只对自己的项目在全阶段具备所有操作权限。

PMO（类似监理）：可看到所有项目，但每个项目只能看到控制门阶段的内容，控制门阶段就是用来评审资料。

安全团队：可管控所有项目，具备所有项目的所有权限。

（4）业务场景化安全需求

业务场景关联安全需求：平台可预置各种业务场景模板，针对业务场景可预置各种安全需求。当涉及平台不包含的预置场景，也可通过威胁建模问卷调查，根据企业实际业务场景，填写完后自动分析并快速推导出对应功能场景的安全需求。也可在线自定义业务场景和安全需求，与后面知识库进度联动。

自定义项目需求：企业可自定义添加需求任务，并把任务指定推送给相应设计、开发、测试阶段。

（5）任务关联推送

可根据业务场景确认的安全需求任务，自动化分析出所对应的安全测试用例，安全测试用例与安全需求对应，一条安全需求会对应多条测试用例，能够在测试阶段保证利用安全测试用例内容对需求阶段提出的安全需求是否正确实现进行有效的测试度量。

（6）集成各种安全工具

提供安全工具编排接口，支持多种安全工具编排调度和数据展示，可管理并配置 Vulhunter、SourceCheck、CodeSec 等安全工具编排调度和数据展示，平台统一管理和提供安全测试工具调度接口。

（7）安全漏洞管理

通过人工渗透测试发现的漏洞或者通过安全检测工具发现的漏洞，都可以在平台进行展示和管理，通过确定

渗透测试报告数据结构，可定制开发将渗透测试结果上传到平台中，实现对漏洞形成闭环管理。首页支持展示项目安全漏洞及修复进展情况-项目总数、未完成安全任务、未修复漏洞、CVE 数量、项目风险趋势收敛图、任务需求增长趋势图、安全漏洞数量等。

（8）车联网威胁建模

基于项目的安全管理可以明确安全责任人，通过项目管理实现责任的分配，例如可按车型进行项目管控。提供元素模板，用户可以基于元素库在一个项目中进行多个 TRAR 模型绘制。通过这种方式可以实现 item 的重用，模型中会看到各种系统、模块、组件之前的架构逻辑关系，支持不同的 TARA 模型和不同的车联网安全标准与法规要求。

攻击路径分析功能展示某一项威胁对于目标资产潜在的攻击方式，便于了解针对目标资产可能的攻击方式。利用攻击可用性+严重性+漏洞转化系数综合评估，基于标准或方法论的方式得出风险系数，也可根据企业自身车联威胁理论方式不同，在平台做定制开发调整。通过威胁建模分析出安全需求，通过安全需求对 item 存在的漏洞进行修复，最后可通过相关检测工具或人工方式验证其是否在修复之后依然存在相关漏洞。

（9）软件研发项目管理

源代码编写提交（JAVA、Python 等）→→→ 代码存储管理（Git、SVN）→→→ 代码拉取构建镜像（Jenkins）→→→ 镜像容器管理（Docker）→→→ 业务功能测试 →→→主机部署上线。

5.3 整车体系化网络安全测试案例

（1） 测试范围与信息收集

本案例选用的车辆为国产某型号 2021 款新能源电动汽车。经厂商授权，在不拆卸车辆电子控制单元、不影响云端服务平台正常服务的情况下对目标车辆进行全方位的网络安全测试。该车辆的测试范围如下：

（1）测试人员可物理接触车辆，但无权限拆卸车辆获取电子控制单元。由于无法拆卸车辆暴露关键电子控制单元的硬件板卡，无法全面执行层次化渗透测试框架中的硬件安全测试。同时，测试人员不得对云端服务平台进行渗透测试以免影响云端服务平台正常业务。

（2）测试人员保有实体钥匙及常规用户账号，可正常进入车辆并正常使用车辆功能以获取必要的信息。由

于测试人员无法破坏车辆，所有车辆功能对于测试人员如同黑盒，在有限的信息下，测试人员仅可控制车辆功能的输入并观察其响应。

（3）在上述限制下，测试人员需针对整车进行全面的网络安全测试。

信息收集是不断迭代的过程，随着测试工作的推进，测试人员可不断获取新的信息为后续测试奠定基础。在测试开始之前，经公开渠道查询相关信息可知该型号车辆具备如图 20 所示的硬件。在硬件支持下，该型号车辆具备如下智能功能，所有功能均在车辆得到验证。

（1）信息娱乐。车辆信息娱乐系统配备大尺寸触控屏幕，采用 Android 操作系统，提供诸多应用程序，支持丰富的信息娱乐体验。信息娱乐系统提供蓝牙、4G 网络、Wi-Fi 及热点等网络功能，能够与云端服务平台与移动设备进行通信。

（2）移动终端远程车辆控制。用户可通过移动终端上的应用程序远程控制车辆，在验证用户身份后，用户可远程执行开闭车门、灯光、空调等操作。

（3）移动终端蓝牙虚拟钥匙。用户可激活蓝牙钥匙功能，将手机等移动终端作为虚拟钥匙用于开闭车门，启停车辆发动机。需要注意的是，本实验车辆并未激活蓝牙钥匙功能。

（4）OTA 车辆系统远程升级。车辆可通过 OTA 方式实现部分功能的远程升级。

（5）被动无钥匙进入及一键启动。用户携带汽车实体钥匙靠近车辆时即可自动解锁车辆。车辆检测到实体钥匙位于车内时才会允许启动发动机。

（6）胎压监测及告警。车辆搭载胎压监测系统，可实时监测车辆轮胎压强与温度。当车辆轮胎压强明显偏离正常数值时可向车驾驶员发出告警信息。

（7）倒车雷达及告警。车辆搭载超声波传感器，可用于辅助泊车。当车辆倒车过程中接近障碍物时可向驾驶员发出告警信息。

（8）交通标志识别。车辆搭载高清摄像头，可用于识别道路交通标志，辅助驾驶员做出驾驶决策。

（9）车辆诊断。车辆开放 OBD-II 诊断接口，用户可通过利用诊断设备连接诊断接口定位汽车故障。



图 20　某型号车辆硬件信息

（2） 网络安全威胁分析

在不拆卸车辆、测试前期无额外可利用信息的前提下，基于智能网联汽车网络安全威胁框架对该型号车辆进行威胁建模。如图 21 所示，攻击者在现有约束条件下仅可利用车辆暴露的硬件接口、无线接口、传感器发起攻击。其中，攻击者利用 OBD-II 接口可入侵车内总线网络，利用 Wi-F、蓝牙及 4G 网络通信可入侵车外网络，利用 GNSS、TPMS、超声波传感器、被动无钥匙进入系统、车载摄像头可入侵车载传感器。

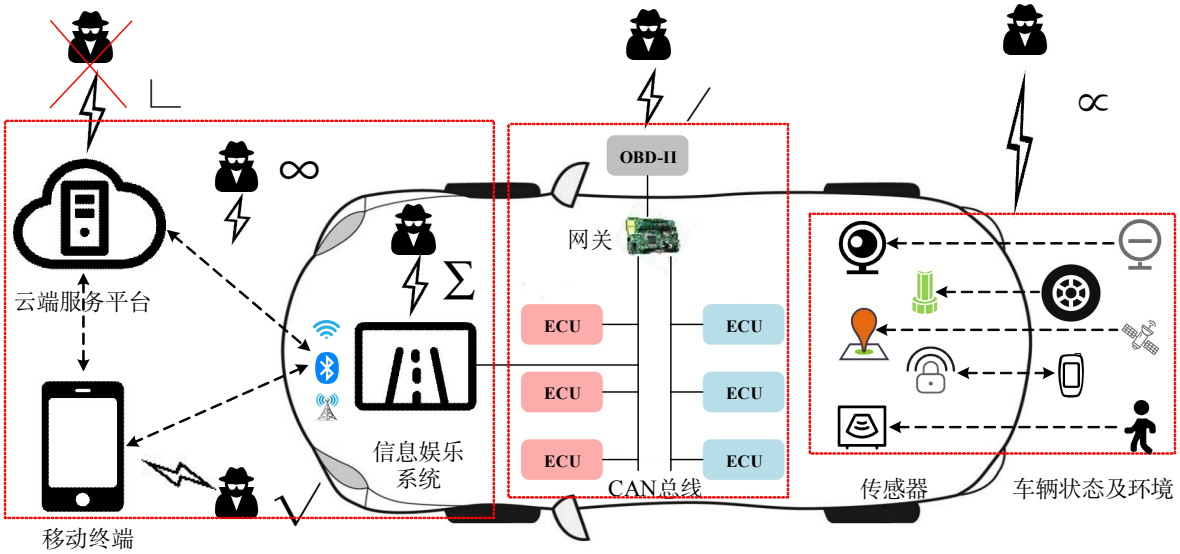


图 21　某型号车辆网络安全威胁模型

在网络安全测试初期，基于现有信息，该型号车辆面临的网络安全威胁表 9 所示。包括信息娱乐系统、云端

服务平台、移动终端、CAN 总线、传感器在内的多个车辆系统面临直接的网络安全威胁。攻击入口丰富，攻击者可从蓝牙、Wi-Fi、4G、网络、应用程序、OBD-II、TPMS、被动无钥匙进入系统、GNSS、车载摄像头、超声波传感器等多个入口发起攻击，包含远程攻击、近场攻击及本地攻击。网络安全威胁涉及无线电安全威胁、网络安全威胁、总线安全威胁、移动安全威胁、云端安全威胁、传感器安全威胁六个威胁框架层次。值得注意的是，为了避免对云端服务平台正常业务造成影响，本次网络安全测试并未获取针对云端平台的渗透测试权限。

表 9　某型号车辆网络安全威胁

威胁标号	汽车系统	攻击入口	威胁框架层次	威胁性质
①	信息娱乐系统	蓝牙	无线电安全威胁	近场威胁
		Wi-Fi	无线电安全威胁	近场威胁
		4G	无线电安全威胁	远程威胁
		⑤网络	网络安全威胁	远程威胁
⑥	云端服务平台	⑤网络	云端安全威胁	远程威胁
③	移动终端	应用程序	移动安全威胁	远程威胁
		应用程序网络	移动安全威胁	远程威胁
②	CAN 总线	OBD-II	总线安全威胁	本地威胁
④	传感器	TPMS	传感器安全威胁	近场威胁
		被动无钥匙进入系统	传感器安全威胁	近场威胁
		GNSS	传感器安全威胁	近场威胁
		车载摄像头	传感器安全威胁	近场威胁
		超声波传感器	传感器安全威胁	近场威胁

（3） 网络安全测试方案

基于网络安全威胁分析结果与授权测试范围，在智能网联汽车层次化渗透测试框架与模糊测试技术指导下，该型号车辆网络安全测试方案如表 10 所示。网络安全测试方案可覆盖该型号车辆直接面临的网络安全威胁。其中，移动终端在该型号车辆中主要用于远程车辆控制与虚拟蓝牙钥匙。本车辆蓝牙钥匙功能尚未激活，无法正常使用，故测试方案中的移动终端安全测试实际为远程车辆控制安全测试。

表 10　某型号车辆网络安全测试方案

测试子系统	一级测试内容	渗透测试框架层次	是否采用模糊测试
信息娱乐系统	蓝牙安全测试	无线电安全测试	是
	Wi-Fi 安全测试	无线电安全测试	是
	4G 安全测试	无线电安全测试	否
	车辆网络安全测试	网络安全测试	是
	车载操作系统安全测试	系统安全测试	否
	应用程序安全测试	移动安全测试	否
远程车辆控制	移动网络安全测试	移动安全测试	是
CAN 总线	CAN 总线安全测试	总线安全测试	是
传感器	TPMS 安全测试	传感器安全测试	是
	被动无钥匙进入系统安全测试	传感器安全测试	否
	GNSS 安全测试	传感器安全测试	否
	车载摄像头安全测试	传感器安全测试	否
	超声波传感器安全测试	传感器安全测试	否

在不拆卸车辆电子控制单元的情况下，无法通过硬件安全测试方法获取电子单元固件，网络安全攻击等方式尚不确定是否可以获取 ECU 固件。因此，在网络安全测试初期，测试人员智能将车辆视为黑盒，仅可以利用模糊测试技术，通过控制车辆功能的输入并观察其响应的方式确定其是否存在潜在的网络安全漏洞。故本次车辆测试中，模糊测试技术主要用于携带基带数据的车辆通信领域，如蓝牙、Wi-Fi、网络通信等，车载摄像头、超声波传感器等视觉与测距传感器则不在模糊测试范围内。

5.4 供应链漏洞管理体系案例

（1）收集安全漏洞

如果发现产品中的漏洞或要报告安全事件，可以访问指定 SRC 平台报告漏洞。收到邮件后，将发送包含跟踪标识符的自动答复。如果有需要，可以使用提供的 PGP 公钥对通信进行加密。

（2） 安全奖励计划

与安全社区有着长期而密切的关系，为安全研究提供现金奖励，该计划帮助团队修复产品中的安全漏洞，也激励广大安全人员主动为产品安全建设提供意见。安全奖励计划主要包括漏洞奖励计划、补丁奖励计划、漏洞研究补助金等。

（3）漏洞政策

供应商和研究人员需尽快对发现的漏洞负责。团队会立即将漏洞通知供应商，并在 90 天后（如果供应商发布修复程序的话）更快地与防御社区公开共享详细信息。如果截止日期在周末或公众假期到期，则截止日期将移至下一个正常工作日。在 90 天的截止日期到期之前，如果供应商告知补丁计划在特定日期（即截止日期后的 14 天内）发布，将延迟公开披露，直到补丁发布为止。当在开发中发现软件以前未知且未修补的漏洞时，在 7 天内有必要采取更紧急的措施。经过 7 天没有补丁或其他消息的情况下，将研提供有关漏洞的详细信息，以便用户可以采取措施保护自己。团队保留在极端情况下将截止日期提前或延后的权利。团队希望缩短相关部门对安全漏洞的响应时间，但也会导致在最后期限时稍微延迟漏洞的披露时间。

（4）漏洞披露信息发布

最开始，对于危害程度严重的“0-day”漏洞，报告查看权限受到限制，只有负责团队成员才能看到漏洞报告内容。当漏洞需要披露时，将“限制”对漏洞修复过程信息的访问。目前基于公开原则，于漏洞的技术描述可以公开访问，所有人都可以了解到漏洞的修复过程。 如果披露错过了最后的截止时间，则会为其添加“截止期限超出”标签。如果该漏洞被允许 14 天的宽限期，则该漏洞将带有特殊标签。

漏洞报告应直接传达给负责开发此修补程序的供应商或开源项目。通常会使用官方联系方式来报告安全漏洞（例如，电子邮件地址或漏洞跟进系统），并且会遵循每个项目的文档化流程来处理安全漏洞，直到漏洞得到修复或披露截止日期过去为止。有时，会与第三方（例如受该漏洞影响的组织）共享漏洞报告。

6. 趋势与展望

车路云的蓬勃发展为汽车行业带来巨大变革，但也带来了严峻的网络安全挑战。在此背景下，多方面的积极举措正不断推动车路云网络安全防护体系走向成熟。但是依然面临潜在挑战。

6.1 自动驾驶带来的潜在网络安全风险

随着自动驾驶技术的飞速发展，基于人工智能的自动驾驶算法已成为车辆自主决策的核心。然而，这些算法的安全性和可靠性正面临越来越多的挑战，人工智能算法的不可解释性和对数据质量的依赖，使其容易受到攻击者的利用。例如，对抗样本攻击已成为影响自动驾驶安全的重要威胁。攻击者可以通过在道路标志上附加微小的扰动，让算法产生错误识别，导致车辆偏离正常轨道或做出危险操作。此外，训练数据集的质量直接决定了自动驾驶算法的性能。一旦攻击者在数据集中注入恶意样本，可能导致算法在某些情况下产生错误判断，这种后门攻击在训练阶段难以察觉，但在实际应用中会造成严重后果。对于实时算法更新和模型部署，版本管理的安全性同样是关键，任何未经授权的修改都可能引入新的漏洞。

算法的复杂性也加剧了安全隐患。自动驾驶算法通常需要处理大量感知数据，包括摄像头、激光雷达和雷达信号，这些数据通过融合后生成决策。一旦攻击者对感知系统进行干扰，例如利用伪造信号欺骗传感器，算法可能生成错误的环境感知结果，从而做出不安全的决策。

为应对这些挑战，未来的自动驾驶算法安全需要在以下几个方面加强：1）提升算法的鲁棒性。研发能够抵抗对抗样本攻击的深度学习模型，同时通过改进算法架构和训练策略，降低对恶意数据的敏感性。2）强化数据集的安全管理。在数据采集、标注和存储阶段引入多层次的验证机制，确保数据集的真实性和完整性。通过数据完整性检查工具，防止恶意样本的注入。3）建立算法审计与验证体系。引入可解释性人工智能技术，对自动驾驶算法的决策过程进行可视化和验证，确保其符合安全要求。同时，建立算法更新的完整性验证机制，防止未经授权的模型替换。4）加强感知系统的协同防护。针对传感器欺骗攻击，开发多传感器交叉验证技术，提升感知数据的可信度。通过动态调整算法权重，应对可能的感知干扰。5）开展安全威胁仿真与测试。定期对算法进行安全测试，包括对抗样本生成、后门攻击模拟和环境干扰测试，评估其在不同场景下的安全性能，并提出改进措施。6）推进行业安全标准化。制定针对自动驾驶算法的安全标准，明确算法开发、测试和部署的安全规范，推动算法安全认证体系的建立。

6.2 大模型的普及与应用带来严峻的网络安全挑战

随着大语言模型（如 ChatGPT）的快速发展和普及，网络安全领域正在经历一场深刻的变革。这些模型因其强大的自然语言处理能力和广泛的应用场景，显著降低了网络攻击的技术门槛，使得网络安全攻击的普及化成为一种新的威胁趋势。在车路云供应链网络的背景下，人工智能模型的双刃剑效应尤为突出。

大模型因其易用性、广泛的知识覆盖和对复杂任务的自动化支持，正在被不法分子利用来设计和实施网络攻击。例如，攻击者可以使用 ChatGPT 编写复杂的恶意代码、生成社会工程攻击邮件、甚至帮助发现零日漏洞。这种趋势表明，网络攻击不再仅是高技术门槛的领域，而是逐渐成为更多不具备专业知识的个体也可以参与的行为。在车路云供应链网络中，网络安全的复杂性进一步提升。车辆与路侧设备、云端服务之间的实时数据交互需要高强度的网络安全防护。然而，攻击者可以利用大模型生成逼真的钓鱼信息或伪造通信数据，以干扰车路云系统的正常运行。例如，攻击者通过生成仿真的远程指令劫持车辆控制系统，或者伪造路侧单元（RSU）的通信内容，诱导车辆做出危险决策。

为了应对因大模型普及带来的网络安全威胁，车路云供应链网络需要加强对大模型的监管，制定针对大模型应用的法律法规，明确其使用边界，防止其被用于非法目的。同时，建立模型开发者和使用者的责任追溯机制。同时，在车路云网络中引入更高级的威胁检测系统，结合机器学习和行为分析技术，实时监控并应对可能的攻击行为。此外，还可以通过行业培训和公众教育，提升对低门槛攻击的防范意识，尤其是在社会工程攻击方面，培养用户的防骗能力。在技术手段方面，利用人工智能技术，开发针对大模型生成内容的检测工具。例如，通过语言模式分析识别由大模型生成的恶意内容，从而及时阻止潜在的威胁。针对供应链厂商，通过端到端的安全加固措施，确保供应链每个节点都具备一定的抗攻击能力。对于数据传输和处理环节，采用更强的加密技术和验证机制，防止数据被篡改或窃取。

随着大模型的进一步发展，在车路云供应链网络中，安全与技术的平衡将成为未来发展的核心。要实现这一目标，需要行业、政府和研究机构的协同努力。在技术层面，通过强化模型的安全设计，避免其被不法分子滥用；在政策层面，推动国际合作，建立针对大模型的使用规范；在实践层面，通过持续的安全测试和评估，确保系统能够应对新型攻击。大模型的出现不仅带来了前所未有的便利，也催生了更多样化的网络安全威胁。唯有在技术与安全之间找到平衡，才能保障车路云供应链网络的长期稳定与发展。

6.3 车路云数据融合过程中的安全风险

随着车路云一体化技术的不断发展，高质量、个性化的车路云服务成为提升用户体验和交通效率的关键。然而，这些服务的实现依赖于海量数据的融合使用，而这一过程中的隐私保护问题已成为亟需解决的重要挑战。车路云服务的核心在于对多源异构数据的深度融合。这些数据包括但不限于车辆运行数据、驾驶员行为数据、道路环境数据以及云端分析数据。虽然数据融合可以为用户提供更智能、更精准的服务，但数据的大规模收集、传输和共享也增加了隐私泄露的风险。

首先，个人隐私数据的暴露是一个显著问题。在车路云网络中，车辆的行驶轨迹、驾驶习惯以及与驾驶员身份相关的信息均属于敏感数据。一旦这些数据被非法访问或利用，可能导致用户隐私泄露，甚至带来财产或人身安全风险。其次，汽车数据的商业化利用也带来潜在隐患。许多车企和服务提供商在数据融合过程中可能对数据进行深度挖掘，以支持商业决策和精准营销。这种数据的广泛使用如果缺乏透明度和用户授权，将进一步加剧隐私风险。此外，数据融合过程中还面临潜在的技术性攻击。例如，攻击者可能通过数据流量监听、数据注入或伪造数据源等方式，对数据的真实性和完整性造成威胁。这不仅危及数据的隐私性，还可能影响车路云服务的可靠性。

为了应对数据融合中的隐私问题，需要从技术、管理和政策多个层面采取综合措施。在数据收集和处理阶段，采用先进的匿名化和脱敏技术，确保个人身份信息无法通过数据融合过程被追溯。例如，通过差分隐私技术限制数据分析过程中可能暴露的敏感信息。利用联邦学习、多方安全计算等隐私计算技术，实现数据在不离开本地的情况下进行协同分析与处理，减少数据共享带来的风险。建立严格的数据访问权限管理体系，确保只有经过授权的用户和应用才能访问敏感数据。同时，引入动态授权机制，根据使用场景动态调整数据访问权限。采用端到端加密技术确保数据在传输过程中的安全性，防止数据被截获或篡改。同时，在数据存储环节采用分布式存储和多重加密技术，进一步提升数据保护能力。通过数据使用记录和审计机制，向用户提供透明的数据使用报告，确保数据使用过程符合用户授权和相关法规要求。在国家和行业层面制定隐私保护相关法律法规，明确数据融合使用的边界和责任。同时，推动行业隐私保护标准的建立，规范数据处理和使用流程。

在车路云一体化的未来，隐私保护与个性化服务的平衡将成为技术创新和产业发展的核心目标。一方面，技术的发展需要更多的数据支持，以实现更高效、更智能的服务。另一方面，用户对隐私保护的需求也在不断提高。实现这一平衡需要多方的共同努力。在技术层面，进一步提升隐私保护技术的普适性和易

用性；在政策层面，推动全球范围内的数据保护合作与法规对接；在用户层面，提高隐私意识，增强用户对数据使用的监督能力。数据融合中的隐私问题不仅是技术挑战，更是社会问题。在未来的车路云供应链网络中，只有在隐私保护得到充分保障的基础上，才能实现技术与服务的可持续发展，为智能交通的未来奠定坚实基础。

致谢

感谢车联网安全集智联盟在研究报告撰写过程中的全面指导。

感谢王文君、包宏宇、阮子禅、张雪松、刘德林、张耀、胡芳、张海春，参与研究报告的研究发起和内容编撰。