智能网联汽车 供应链网络安全研究报告

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

随着信息技术的迅速发展和智能网联汽车产业的日益成熟，汽车行业的智能化与网联化逐渐成为全球汽车产业革新的核心动力。智能网联汽车不仅仅是传统汽车的延伸，更是在智能硬件、人工智能、大数据、云计算等技术的深度融合下，向更高层次进化的智能体。然而，智能网联汽车的快速发展带来了新的挑战，特别是在网络安全领域。智能网联汽车不仅是物理产品，更是信息、数据和服务的集合体，其系统架构高度复杂，涉及的技术层面繁多，涵盖了自动驾驶、车载通信、车联网、数据共享等多方面内容。因此，保障其在复杂网络环境中的安全性，成为产业链上游和下游企业无法回避的重要问题。

智能网联汽车的供应链体系由众多供应商共同协作，供应链中任何一个环节的问题都可能影响到最终产品的网络安全性，这使得整个供应链的网络安全管理显得尤为重要，各供应商的网络安全面临不同的要求和挑战。智能网联汽车的供应链网络安全问题远不止局部环节的技术问题，它涉及供应商管理、第三方服务的依赖、数据交互的安全性等多个层面的协同与防护。由于供应链的复杂性、信息技术的多元性以及来自不同领域的安全威胁，传统的汽车网络安全防护措施难以适应新兴的智能网联汽车产业所面临的挑战。

目前，国内外针对智能网联汽车的网络安全标准研究已有一定的进展。强制性国家标准 GB 44495—2024《汽车整车信息安全技术要求》为整车网络安全提出了基本要求，国际上 ISO/SAE 21434《Road vehicles—Cybersecurity engineering》也为汽车行业提供了指导框架。然而，现有的安全标准和技术规范多聚焦于车辆本身的安全问题，缺少对整个供应链环节中各方协作与网络安全防护的全面要求。在智能网联汽车供应链环节中，如何在多级供应商、跨企业的协作环境中构建可持续的网络安全防护体系，成为了一个亟待解决的问题。

本项目旨在解决现有标准落地实施的问题，完善智能网联汽车供应链网络安全防护能力。通过制定规范化、系统化的技术规范，为车辆制造商、产品供应商、第三方服务供应商等供应链各参与方提供统一、可落地的网络安全指引，从而助力各主体在复杂的供应链协同管理场景中，高效实现合规管控与风险闭环治理，从源头减少供应链各环节的网络安全隐患，保障智能网联汽车在技术迭代加速、多主体协同联动的产业发展阶段实现全生命周期的安全稳定运行。

衷心感谢参与研究报告编写的各单位和组织：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）、中国汽车技术研究中心有限公司、中国第一汽车股份有限公司、比亚迪汽车工业有限公司、吉利汽车研究院（宁波）有限公

司、北京理想汽车有限公司、赛力斯汽车有限公司、东风商用车有限公司、厦门金龙联合汽车工业有限公司、大陆投资（中国）有限公司、泛亚汽车技术中心有限公司、重庆长安汽车股份有限公司、维克多汽车技术（上海）有限公司、浙江零跑科技股份有限公司、北京汽车研究总院有限公司、惠州市德赛西威汽车电子股份有限公司、北京梆梆安全科技有限公司、博世（中国）投资有限公司、中国重型汽车集团有限公司、中车时代电动汽车、知行汽车科技（苏州）股份有限公司、电装（中国）投资有限公司、北京天融信网络安全技术有限公司、长城汽车股份有限公司、中汽智能科技（天津）有限公司、紫光同芯微电子有限公司、襄阳达安汽车检测中心有限公司、上海为旌科技有限公司、郑州信大捷安信息技术股份有限公司。

主要编写人：朱科屹、张慧妍、杨玚、李雨冉、邱昶泓、纪梦雪、马鑫、孟雪、方锦祥、张佳敏、王子维、张军、刘姣、高岩、彭振文、牛方超、杨欣悦、华宇铖、汪向阳、王振、任国栋、陈团圆、蔡佳鹏、卢佐华、殷勇军、徐国强、文健峰、郑志敏、朱书林、蔡精益、范雪俭、付苗、张小东、王海均、贾先锋、刘献伦、种挺、王军、张宇星、刘为华。

目　录

1 智能网联汽车供应链网络安全研究背景

智能网联汽车产业的快速发展，使得智能化与网联化已成为推动汽车产业变革的重要力量。车辆制造商在整车设计、生产、运营等各个环节中日益依赖外部的软硬件资源，逐步形成了一个多层次、跨区域、跨行业协同的供应链体系。该体系中，整车系统广泛集成了来自芯片供应商、零部件供应商、软件供应商、通信模组供应商、云服务商等多个主体的产品与服务，这些不同领域的资源和技术的融合，极大地提升了智能网联汽车的智能化水平和功能复杂性，导致智能网联汽车产业面临的网络安全挑战也日益严峻。

在车辆供应链的各个环节中，涉及的硬件、软件、通信和云服务等各类产品和技术，往往由多个不同的供应商提供，这使得整车系统的安全防护面临前所未有的挑战。供应链的多元化和复杂性导致了大量潜在的安全隐患，攻击者可能通过篡改硬件组件、植入恶意代码、篡改软件升级包等手段，利用供应链中的薄弱环节，实施精准攻击，进而威胁整车系统的安全。这不仅可能导致车辆的远程失控、驾驶员数据泄露、核心功能的瘫痪等安全事故，还可能带来产业链的信任危机，甚至影响公众对智能网联汽车技术的接受度和认可度。

UNECE R155 法规与 ISO/SAE 21434 等国际标准已将供应链网络安全纳入型式批准的重要内容，对企业在网络安全方面的能力提出了更高要求。因此，我国智能网联汽车产业如何在保障国内安全需求的同时，满足国际市场对安全性的严格要求，成为行业发展的关键问题。虽然 GB 44495-2024《汽车整车信息安全技术要求》等国家标准已对智能网联汽车的网络安全进行了总体规范，但在供应链层面，尚存在供应链网络安全责任边界不清晰、网络安全需求传递模糊且供需双方理解存在偏差、缺少有效的供应链网络安全评价机制及供应商管理流程不规范等问题，导致现有的标准和技术要求落地困难。

智能网联汽车供应链网络安全的标准化建设迫在眉睫，亟需通过国家层面的政策推动和技术规范，确保产业链中的每一环节都能够符合安全要求，从而有效防范潜在的安全风险。因此，制定《智能网联汽车 供应链网络安全技术规范》不仅能够为整车制造商与供应商之间的协作提供统一的合规框架和实施路径，还能推动供应链中的各方建立起更加完善的安全保障机制，提升整体安全防护能力。

1.1 智能网联汽车供应链相关定义

1.1.1 智能网联汽车供应链概念

智能网联汽车供应链是由整车制造商、产品供应商、第三方服务供应商等多方主体共同组成的跨领域协作网络，涵盖从产品设计、采购、研发、生产、交付、运维直至废止处理的全生命周期活动。供应链的核心要素包括以下几方面。

（1）硬件：包括车载计算单元、通信模块、控制器、传感器、摄像头、安全芯片及物理接口等，为车辆提供基础硬件支撑；

（2）软件：包括嵌入式固件、操作系统、中间件、应用软件及云端平台服务，用于车辆功能实现与用户交互；

（3）数据：包括个人信息、重要数据及车辆运行数据，用于车辆定位、决策与智能服务，应依据敏感性进行分类分级和保护；

（4）工具与服务：包括开发与验证工具链、测试仿真环境、运维与安全管理平台，以及面向全生命周期的技术与运营支持服务、检测咨询认证服务等。

智能网联汽车供应链通过跨行业、跨领域的协同合作，形成集成化、多层级的生态体系。各参与方围绕全生命周期开展合作，不仅确保信息通信技术产品和服务的高效传递与应用，还需落实网络安全责任与风险防护机制，保障车辆智能化与网联化功能的安全实现。

1.1.2 智能网联汽车供应链组成

智能网联汽车供应链是一个复杂的、多层级的系统，包含多个相互依存且协作的参与者。

1.1.2.1 车辆制造商（OEM）

车辆制造商是智能网联汽车供应链的核心主体，承担着整车的设计、开发、制造与市场

化的全流程责任。作为供应链的主导者，车辆制造商承担着供应链网络安全的总体责任，在供应链中起着关键的协调与引领作用。其主要职责包括：

（1）开展整车集成与制造管理，保障系统和部件的网络安全集成。车辆制造商负责整车的设计、研发、生产及质量管控，整车集成涉及将来自各类供应商的零部件、系统及技术方案的有效融合，需要确保整车的性能、质量与安全符合标准要求。

（2）建立供应商网络安全管理机制，对供应商交付物进行网络安全审查与验证。整车制造商应定期对交付物进行验证，特别是关键零部件，需要严格遵守行业网络安全技术要求。需要定期评估供应商的网络安全管理能力，确保其持续符合网络安全要求。

（3）确保产品符合网络安全相关的标准要求。车辆制造商需要根据标准要求制定相应产品的网络安全技术要求和验收标准，确保所生产的智能网联汽车符合国家、国际及行业的网络安全标准规范。

（4）协调各类资源，实现安全与高效生产。车辆制造商需要协调上游供应商、下游经销商和其他合作伙伴，确保原材料、零部件、技术及服务的及时供应与高效生产，优化生产过程中的资源利用和成本控制。

1.1.2.2 产品供应商

产品供应商是智能网联汽车供应链的重要组成部分，承担着提供关键零部件、技术和系统解决方案的重要职能。供应商根据其在供应链中的位置，可分为不同层级：

（1）一级供应商。一级供应商指直接与 OEM 签署合同、开发协议或其他类似文件并向车辆制造商提供关键系统与核心组件的供应商，负责关键技术的研发、生产及质量保证，并承担较高的技术与合规责任。还包括通过授权代理、分销或系统集成方式向车辆制造商提供关键产品、技术方案的机构。

（2）二级供应商。二级供应商向一级供应商提供服务，提供子系统、组件或关键技术。二级供应商在供应链中起着技术支撑的作用，其产品质量直接影响整车产品的性能和安全。

（3）三级供应商及其他层级供应商。三级供应商主要提供基础原材料、基础组件、基础零部件等。三级供应商是供应链的基础，他们交付物的质量、稳定性和安全性是整个供应链体系的基石。

1.1.2.3 第三方服务供应商

智能网联汽车供应链中的第三方服务供应商为整车制造商及产品供应商提供支持和保障，确保整个供应链高效、安全、合规地运作。第三方服务供应商的具体职责和分类包括以下几个方面：

（1）测试与认证服务。第三方测试与认证机构负责对智能网联汽车进行全面的功能、性能、可靠性与安全性验证，确保汽车在实际使用中能满足相关的标准与法规要求。认证服务不仅涵盖国内标准，还涉及到欧盟、美国等国际市场的认证要求。

（2）咨询与审计服务。随着智能网联汽车技术的不断发展，行业面临的法规、市场需求和技术创新的挑战也日益复杂。第三方咨询机构为整车制造商、供应商及行业监管机构提供战略咨询、技术审计、法规合规性分析等服务，帮助企业评估并降低潜在风险，优化供应链管理，确保技术创新与市场需求的有效对接。

（3）云服务与数据管理。智能网联汽车的数据量庞大且复杂，第三方云服务商为车辆制造商提供大数据存储、云平台建设、数据分析与处理等技术支持，支撑自动驾驶决策、车联网功能及远程诊断等关键应用。

（4）网络安全运营和情报服务。这类服务商旨在通过持续的威胁监测、漏洞预警、应急响应和威胁情报共享，保障供应链内各环节的网络安全。

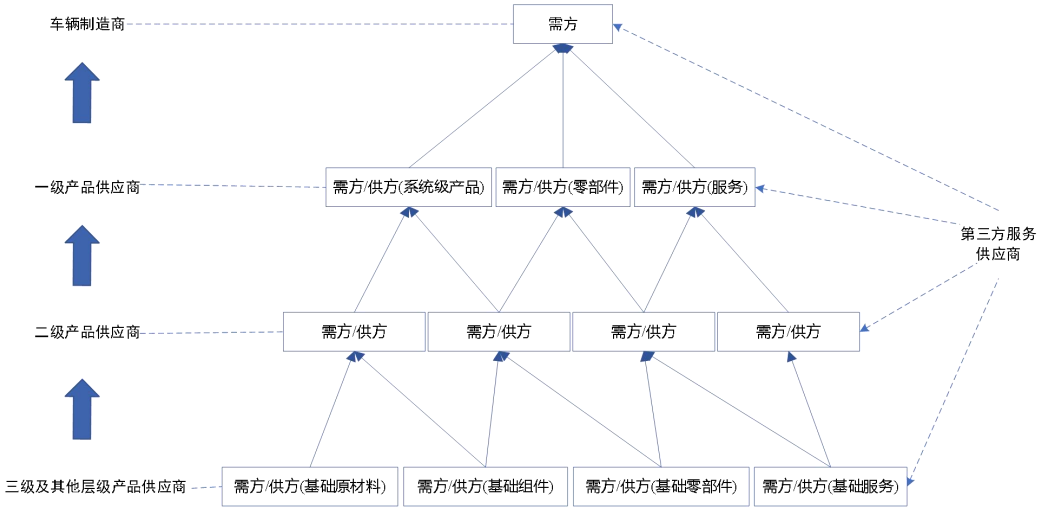


图 1-1 智能网联汽车供应链结构图

1.1.3 智能网联汽车供应链网络安全概念

智能网联汽车供应链网络安全是指在智能网联汽车的全生命周期内，通过系统化的技术手段、管理策略和跨层级协作机制，保障供应链各参与方（包括车辆制造商、产品供应商、第三方服务供应商）之间的网络安全能力，以防范网络攻击、数据泄露及系统故障等对车辆系统运行和用户安全造成的影响。其核心目标是确保智能网联汽车供应链中的各类硬件、软件、数据资产在技术和管理上得到全面网络安全保护，并能够抵御潜在的网络安全威胁。智能网联汽车供应链网络安全的主要内涵包括：

（1）机密性、完整性与可用性保障。通过强化信息安全管理，确保供应链中传输与存储的数据不被未经授权访问或篡改，同时保障数据和系统的持续可用性。

（2）全生命周期网络安全管理。智能网联汽车供应链的网络安全不仅局限于产品的生产及运行阶段，更涵盖了从采购、开发、生产、交付、运维、废止的车辆全生命周期。通过全程管控与技术手段的应用，确保每个环节、每个组件的网络安全，从根本上预防潜在的网络安全风险。

（3）供应链协同防护机制。智能网联汽车供应链的复杂性和多元化，使得网络安全要求在各个环节之间建立紧密的协作机制。整车制造商、产品供应商以及第三方服务商需共同遵守行业相关的网络安全标准和技术要求，从而形成一个安全闭环。通过信息共享、互通有无，协同应对网络攻击和漏洞威胁。

（4）防御体系与应急响应能力。智能网联汽车供应链应具备较强防御性的网络安全体系，包括实时监控、漏洞扫描、入侵检测和加密技术等。同时，在面临网络攻击或数据泄露等突发事件时，应能快速响应和有效应对，通过应急预案和修复机制最小化潜在损失。

智能网联汽车供应链网络安全的目标不仅是保护单一系统的网络安全，更是建立一个协同合作、具有高度防护能力和应对风险能力的网络安全生态系统。通过明确供应链中各参与者的网络安全职责、技术要求与验证方法，全面提升供应链网络安全防护能力。

1.1.4 术语及定义

（1）需方

从其他组织获取产品或服务的组织或个人。

注 1：获取可能涉及或不涉及资金交换。

注 2：重要信息系统或关键信息基础设施的运营者，通常是从智能网联汽车供方获取智能网联汽车产品或服务的需方。

[来源：GB/T 43698-2024，有修改]

（2）供方

开展智能网联汽车生命周期活动的组织。

注 1：供方也可称供应商、供应方。

注 2：供方可以是组织内部的或外部的。

注 3：智能网联汽车供方包括产品供应商、服务提供商、系统集成商、生产商、销售商、代理商等。

[来源：GB/T 43698-2024，有修改]

（3）供应关系

在需方和供方之间的协议，可用于开展业务，提供产品或服务，实现商业收益。

注 1：需方和供方可以是同一个机构。

注 2：在供应链中，上游机构的需方同时也是下游机构的供方。终端客户是可以理解为一种特殊的需方。

[来源：GB/T 36637-2018，有修改]

（4）网络安全

通过技术和管理措施，保障汽车电子电气系统、组件和功能免受网络威胁，确保车辆处于安全运行状态的能力，使其资产不受威胁的状态。

[来源：GB 44495-2024，有修改]

（5）车载计算单元

智能网联汽车中负责异构计算的核心硬件平台，集成 AI 计算单元、通用计算单元、控制单元及安全处理单元，支持高算力需求与实时数据处理，为自动驾驶决策提供算力基础。

[来源：《车载智能计算基础平台参考架构 2.0》，有修改]

（6）通信单元

安装在车辆上实现车与外界信息交互的设备。

（7）控制单元

汽车电子电气系统中接收传感器信号、执行决策指令的电子控制装置。

（8）核心零部件

在智能网联汽车系统中，对车辆功能安全、网络安全或数据安全具有关键影响的电子电气部件。

注：识别核心零部件应综合考虑以下因素：

1）功能安全依赖性—零部件的失效是否可能直接影响车辆的关键功能，如驱动、制动、转向、稳定控制等；

2）智能驾驶关联性—零部件是否参与智能驾驶、环境感知、决策或控制执行等功能；

3）外部通信能力—零部件是否具备外部通信接口或网络连接能力（如蜂窝通信、Wi-Fi、V2X、以太网等，不包括调试接口如 JTAG、UART）；

4）数据敏感性—零部件是否采集、存储或处理个人信息、关键数据或车辆运行数据；

5）远程访问能力—零部件是否具备远程访问、OTA 升级或云端交互能力；

6）安全信任链地位—零部件是否为系统安全信任链的重要环节（含两类：一是核心安全功能模块，如安全芯片、密码模块、密钥管理单元等；二是关键网络硬件设备，如网关）；

7）跨域交互性—零部件是否与多个车辆域（动力域、车身域、智驾域等）存在数据或控制交互关系。

凡满足上述任意一项条件的部件，可判定为核心零部件，应纳入重点网络安全设计、验证与管控范围。

（9）供应链网络安全

在智能网联汽车全生命周期内，针对供应链中涉及的产品、软件、数据及服务，开展的网络安全风险识别、分析、控制与持续改进活动，确保供应链安全责任、过程与结果的可追溯性。

（10）网络安全管理体系

组织为实现网络安全方针和目标而建立的管理体系，包括政策、组织架构、流程、职责及资源配置，用于持续管理网络安全风险。

（11）供应链网络安全管理体系

组织为供应链各环节建立的网络安全管理框架，包括组织管理和供应活动管理两部分，旨在对供应链中涉及的各类网络安全风险进行持续监控、管理和应对。

（12）网络安全档案

供应商提供的证明其网络安全活动满足要求的文件集合，包括风险分析报告、测试报告、漏洞管理记录及安全措施说明等。

（13）网络安全接口协议（Cybersecurity Interface Agreement, CIA）

需方与供方之间签署的网络安全接口文件，用于明确网络安全职责、数据交互方式及安全措施，确保网络安全要求在供应链中的传递。

（14）软件物料清单（Software Bill of Materials, SBOM）

描述软件组成部分及依赖关系的清单，用于跟踪第三方组件及开源库的安全状态。

（15）威胁分析与风险评估（Threat Analysis and Risk Assessment, TARA）

通过识别资产、分析威胁与漏洞、评估风险并制定缓解措施的过程，用于确定网络安全

优先级。

（16）安全基线

在车辆开发与运行中，为保障网络安全而制定的最低配置要求，包括硬件安全、软件安全、数据安全及服务安全等方面的基本规范。

（17）产品安全事件响应团队

组织内部负责发现、评估、通报及处置产品安全事件的专门团队，确保安全问题得到及时响应与闭环处理。

（18）关键数据

智能网联汽车中，影响车辆行驶安全的核心参数数据：包括安全气囊展开控制参数、制动系统压力/响应时间参数、电池包热失控防护阈值、自动驾驶系统紧急避险决策阈值等。

（19）供应链参与方

在车辆开发、生产、运营或服务过程中，参与产品、软件、数据或服务供应的任何主体，包括制造商、零部件供应商、软件提供商、代理商及服务商。

1.2 智能网联汽车供应链网络安全现状

1.2.1 供应链网络安全管理现状

当前智能网联汽车行业供应链网络安全管理的现状可以分为以下方面：

（1）网络安全管理体系的建立

智能网联汽车供应链领域，网络安全管理体系搭建已从“被动合规”向“主动防控”过渡，但整体呈现“头部引领、中小滞后”的不均衡格局。为适配 GB 44495-2024、ISO/SAE 21434

等国内外相关标准要求，整车企业及部分一级供应商已完成全生命周期网络安全管理体系搭建，覆盖供应商准入、零部件研发、生产制造、交付后运维等关键环节，且普遍在体系中融入了供应商安全能力评估模块。然而，部分车企及多级供应商的体系搭建进度滞后，缺乏体系化的安全管控思路与落地能力。

（2）责任与角色分配

当前行业内已形成“整车厂主导、多级供应商协同”的责任分配基本框架，但责任边界界定仍处于完善阶段。整车厂商普遍被认定为供应链网络安全的主体责任人，需主导制定安全管理规范并推动落地，但受供应链链条长、环节多的影响，对下游多级供应商的可控性存在局限。实践中，车企大多通过签署网络安全开发接口协议（CIA）等合同文件，明确与一级供应商的安全协作责任，包括研发阶段的安全需求同步、漏洞响应协同等核心义务。同时，行业正逐步推进责任层级传导机制，要求一级供应商向二级、三级供应商输出安全要求，但中小零部件企业的责任落实力度不足、追溯链条不完整等问题仍较为突出，部分企业尚未建立明确的内部安全岗位职责体系。

（3）供应商网络安全能力评估

供应商网络安全能力评估已成为行业准入核心环节，评估体系日趋标准化但差异化特征明显。当前大多数整车企业已将 ISO/SAE 21434 认证列为一级供应商的准入硬门槛，未通过认证的企业基本无法进入核心供应链。评估流程已形成“文件审核+现场核查+动态复评”的闭环模式，内容涵盖供应商的安全管理体系搭建、风险评估能力（如 TARA 流程落地）、漏洞扫描与修复机制等，对芯片、通信模组等关键部件供应商，还会额外要求提供硬件级防护方案及半年内的漏洞扫描报告，部分高风险零部件供应商需接受驻厂审核。然而，评估资源多集中于一级供应商，对二、三级中小供应商的评估多以书面材料审核为主，现场验证覆盖率较低，存在风险管控盲区。

（4）合规与认证标准的应用

在国内标准方面，GB 44495-2024 作为国家强制性标准，其“全生命周期管控”要求已

推动行业进入合规整改阶段，整车企业正按 2026 年新申报车型合规、2028 年存量车型升级的节点推进体系搭建与产品适配，核心聚焦管理体系标准化与 OTA 升级安全、数据加密等关键场景测试。国际标准方面，ISO/SAE 21434 已成为跨国供应链的“安全信用证”，通过认证的企业可大幅缩短跨国合作审核周期，降低协同成本。此外，TISAX 认证在欧洲车企供应链中应用广泛，成为企业进入欧盟市场的重要资质。

1.2.2 供应链网络安全问题分析

随着智能网联汽车产业的快速发展，供应链网络安全日益成为保障车辆安全和用户隐私的重要组成部分。然而，在智能网联汽车的供应链管理中，仍然存在一些突出的问题，这些问题不仅影响了整个供应链的网络安全，也对车辆的正常运行和行业的可持续发展构成了潜在威胁。当前智能网联汽车供应链网络安全面临的主要问题包括：

（1）模糊的责任边界与供应商产品安全责任缺失

在智能网联汽车供应链全生命周期中，上下游主体间的网络安全责任边界尚未形成清晰统一的界定标准，尤其在多级供应商协同场景下，主机厂、一级供应商、二三级零部件供应商的责任划分存在交叉与空白地带，导致安全事件发生后极易出现责任推诿、归属难定的困境。从实际履约情况看，大量供应商存在安全责任意识薄弱、履行不到位的问题，部分中小供应商未建立符合 ISO/SAE 21434、GB 44495-2024 等相关标准的漏洞管控机制，且在发现零部件或软件漏洞后，未按规范流程及时向主机厂通报，也未开展有效修复工作，存在持续性安全隐患。此外，尽管 GB 44495-2024、UN R155 等法规已逐步落地，但现有标准体系尚未实现供应链全流程的强制性覆盖，不同层级供应商的安全实践缺乏统一约束，导致行业内安全能力水平参差不齐，进一步放大了供应链整体风险。

（2）需求传递模糊且存在偏差

智能网联汽车供应链的网络安全需求传递存在显著的“层级衰减”问题，核心原因在于需求表述缺乏标准化载体、技术指标界定模糊。主机厂向一级供应商传递安全需求时，常存在缺少量化指标的情况，而一级供应商向下游传导时，又易出现需求解读偏差或简化遗漏，

最终导致末端供应商对安全要求的理解与主机厂核心诉求脱节。这种信息断层直接引发多重风险：一是安全标准执行出现偏差，部分零部件因未达到预设安全等级无法适配整车防护体系；二是资源错配与成本浪费，供应商可能因误读需求投入冗余资源，或因需求缺失导致后期返工整改；三是催生供应链安全薄弱节点，如某电子部件因未准确理解加密需求，导致数据传输环节存在被劫持风险，直接影响整车网络安全防护能力。

（3）供应链网络安全能力不均衡

智能网联汽车供应链呈现明显的“头部集中、中小滞后”的安全能力分布格局，网络安全能力不均衡问题突出。主机厂及核心一级供应商凭借充足资源，已构建专业安全团队并落地全生命周期安全管理措施，但大量中小型零部件供应商受资金、技术、人才限制，普遍存在安全能力短板，如未配备专职网络安全人员、缺乏基础的漏洞扫描和风险评估工具、安全投入占比不足等，难以支撑安全技术升级与体系搭建，且技术积累薄弱，对 ECU、车载通信模组等核心部件的安全防护设计能力不足，产品易存在后门漏洞或防护缺陷。这些中小型供应商作为供应链的重要组成部分，其安全能力缺失使其成为整车网络安全体系的薄弱环节，面对日益复杂的网络攻击手段时难以有效应对，大幅提升了供应链整体被渗透的风险。

（4）信息共享与保密之间的矛盾

智能网联汽车供应链的高效协同高度依赖信息共享，如零部件设计参数、测试数据、漏洞信息、OTA 升级方案等关键信息的流转，但信息共享与商业机密、数据安全的保护需求形成尖锐矛盾，成为行业普遍面临的两难困境。在实际协作中，过度开放的信息共享机制已引发多起数据泄露事件，例如某 Tier1 供应商员工违规下载主机厂路测核心数据（含激光雷达测绘数据、电池热管理参数等），相关数据在暗网标价高达数千万元，严重威胁企业技术创新成果与商业利益；然而，若过度收紧信息共享权限，则会导致供应链响应效率下降，如漏洞信息传递延迟可能错过最佳修复窗口期。尤其在涉及自动驾驶核心算法、车载操作系统源代码等敏感信息时，平衡共享效率与保密安全的难度进一步提升，成为供应链网络安全管理的核心挑战之一。

（5）威胁监测与响应能力不足

随着网络攻击技术的迭代演进，智能网联汽车面临的动态威胁日益多元化，而供应链整体的威胁监测与应急响应能力普遍滞后于风险发展态势。在监测层面，多数供应商缺乏实时化、全链路的威胁感知体系，难以精准识别针对车载总线、ECU、云平台等关键环节的攻击行为；在响应层面，应急机制不完善、流程繁琐导致响应延迟，尤其在漏洞管理环节，行业普遍存在漏洞发现与修复周期过长的问题。此外，涉及自动驾驶功能的 OTA 升级需履行严格的合规审批流程，部分企业因审批环节冗余导致升级滞后，无法及时通过 OTA 修复已发现的安全漏洞，进一步延长了车辆的风险暴露时间，加剧了安全隐患。

（6）缺乏有效的网络安全评价机制

当前智能网联汽车供应链尚未建立系统化、全生命周期的网络安全评价机制，核心缺陷集中在准入评估缺失与动态评估不足两大方面。在供应商准入阶段，多数主机厂的评估体系缺乏量化的网络安全能力指标，未将合规性测试结果、网络安全审计报告作为强制准入材料，导致部分安全能力不足的供应商进入供应链体系；在合作存续阶段，现有评估机制普遍缺乏动态性，未建立定期复评制度，无法实时跟踪供应商安全能力的变化，也难以发现合作过程中新增的安全风险。这种重形式、轻实效的评价模式，导致供应链中的安全隐患无法被及时排查，风险在长期运营中持续积累，不仅影响单一环节的安全性，更可能通过供应链传导扩散，威胁整个供应链的稳定性与整车产品安全。

（7）供应商管理流程不规范

部分供应商在与主机厂的协作过程中，网络安全相关管理流程存在明显漏洞，尤其在商业机密与技术文档管理环节，缺乏标准化、全流程的保密管控措施。具体表现为：技术文档流转无严格审批流程，存在随意传输、复制风险；数据访问权限管理松散，未建立“最小权限”原则与操作追溯机制；未落实保密协议的全周期管控，对合作过程中的涉密信息缺乏有效脱敏与防护措施。这些不规范行为易引发严重泄密事件，不仅导致主机厂核心技术成果被窃取，还损害了企业商业信誉。

1.3 供应链网络安全相关法规政策标准

1.3.1 国内法规政策标准

国内与供应链网络安全相关的法规政策标准有：

序号	法规、政策或标准	相关说明	发布时间
1	《网络安全法》	从网络审查、网络产品和服务安全角度对供应链网络安全提出要求	2016 年 11 月
2	《云计算服务安全评估办法》	重点评估云平台技术、产品和服务供应链网络安全情况，申请安全评估的服务商应提交业务连续性和供应链网络安全报告。	2019 年 7 月
3	《网络安全审查办法》	要求对关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应进行网络安全审查。	2020 年 4 月
4	《智能网联汽车生产企业及产品准入管理指南（试行）》	企业应建立供应链网络安全保障机制，明确供方产品和服务网络安全评价标准、验证规范等，确定与供方的安全协议，协同管控供应链网络安全风险。	2021 年 4 月
5	《关于进一步加强新能源汽车辆制造商业安全体系建设的指导意见》	指导新能源汽车辆制造商业建立健全包括网络安全在内的六大方面安全保障体系，提供产品安全保障能力，并在其中提出各零部件供应商、售后服务等相关企业要协同做好安全体系建设工作	2022 年 3 月
6	GB/T 32921-2016《信息安全技术 信息技术产品供应方行为安全准则》	从供应商的角度，信息技术产品供应方在提供信息技术产品过程中，为保护用户相关信息、维护用户信息安全应遵守的基本准则	2016 年 8 月
7	GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》	规定了信息通信技术 ICT 供应链的安全风险管理过程和控制措施。	2018 年 10 月

8	GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》	供应商关系和供应链网络安全作为安全保护的重要项，着重强调供应链网络安全的管理。	2019 年 5 月
9	GB/T 31168-2023《信息安全技术云计算服务安全能力要求》	对云服务商的供应链从采购过程、外部服务提供商、开发商、防篡改、组件真实性、不被支持的系统组件、供应链保护等方面提出了安全要求。	2023 年 5 月
10	GB/T 43698-2024《网络安全技术 软件供应链安全要求》	通过对软件供应链及其面临的安全风险进行分析，制定软件供应链网络安全要求，规定软件产品供应链所涉及的相关要素安全要求，包括软件供应链组织管理要求及开发、交付、使用等环节的安全要求。	2024 年 4 月
11	GB/T 43848-2024《网络安全技术 软件产品开源代码安全评价方法》	规定了软件产品中的开源代码成分安全评价要素和评价流程，适用于软件产品包含的开源代码进行静态安全评价，为软件产品中的开源代码成分进行安全性自评提供依据。	2024 年 4 月
12	RB/T 221-2023《信息技术产品供应链安全评价规范》	认证认可行业标准，对信息技术产品供应链的安全评价方法进行了规范。	2024 年 5 月
13	20192184-T-469 《网络安全技术 关键信息基础设施信息技术产品供应链安全要求》	对关键信息基础设施信息技术产品供应链网络安全提出明确的要求	待发布
14	GB 44495-2024 《汽车整车信息安全技术要求》	规定车辆制造商应建立与供应商之间汽车信息安全依赖关系的过程，以及识别和管理车辆与供应商相关的风险。	2024 年 8 月
15	GB/T 45953-2025《供应链安全管理体系规范》	涵盖供应链各环节的安全管理要求，包括风险评估、信息安全、物理安全、人员管理等核心内容。注：非等效采用 ISO 国际标准：ISO 28000:2022	2025 年 8 月

相关法规政策需要遵照执行，之前的相关标准都可以参考，有些标准适用于软件或 ICT 产品，对于智能网联汽车的供应链网络安全要求可以参考。

1.3.2 国外法规政策标准

通过系统分析国际汽车网络安全相关法规政策标准体系（包括 UNECE R155/156、ISO/SAE 21434 等），发现现有标准主要聚焦整车安全与开发流程，对供应链网络安全的规范不够全面。例如，ISO/SAE 8475 标准提供了零部件 CAL 网络安全保障等级框架，但在实际应用于智能网联汽车复杂供应生态时存在明显不足：一是缺乏针对不同类型供应商（硬件、软件、服务）的差异化要求；二是未充分考虑智能网联场景下数据共享与跨企业协同特性；三是安全责任边界划分与传递机制不够明确。国外与供应链网络安全相关的法规政策标准有：

序号	法规、政策或标准	相关说明	发布时间
1	ISO28000-2022 Security management systems for the supply chain	从供应商角度，规定信息技术产品供应方的行为安全准则	2022 年 3 月
2	ISO/IEC 27036-1 Cybersecurity-Supplier relationships-Part 1： Overview and concepts	概述供应商关系安全的概念与原则	2021 年 9 月
3	ISO/IEC 27036-2 Cybersecurity-Supplier relationships-Part 2： Requirements	规定了定义、实施、操作、监控、维护和改善供应商关系的基本信息安全要求。	2022 年 6 月
4	ISO/IEC 27036-3 Cybersecurity-Supplier relationships-Part 3： Guidelines for hardware, software, and services supply chain security	ICT 供应链信息安全指南，包括硬件、软件和服务等	2023 年 6 月
5	ISO/IEC 27036-4 Cybersecurity-Supplier relationships-Part 4： Guidelilnes for security of cloud services	供应商关系安全云服务安全指南	2016 年 10 月
6	ISO/IEC 20243-1 Information technology. Open Trusted Technology ProviderTM Standard （O-TTPS） - Requirement	是一套减少恶意污染和假冒产品的要求和建议，该标准涵盖了从产品开发到制造和分销的供应链网络安全	2023 年 11 月

	s and recommendations for mitigating maliciously tainted and counterfeit products		
7	美国《国家网络安全计划（CNCI）》	要求在产品、系统和服务的整个生命周期内综合应对国内和全球供应链风险。	2008 年 1 月
8	美国《网络供应链管理和透明度法案》	确保为美国政府开发或购买的使用第三方或开源组件以及用于其他目的的任何固件或产品的完整性。	2014 年 12 月
9	美国《联邦采购供应链安全法案 2018》	创建了联邦采购供应链安全理事会（FASS）为联邦供应链安全制定规则，来保障联邦供应链安全。一是收集与供应链安全风险相关的信息，并与联邦机构和私营部门共享。该信息涉及各种来源的信息，包括各机构用来证明采购禁令正当性的风险评估和其他情报。二是评估特定技术带来的风险并建议采取措施解决这些风险。这些建议可能以排除令（禁止未来从特定制造商处采购特定 ICTS 设备）或清除令（清除特定网络现有 ICTS 设备的指令）的形式出现。	2018 年 12 月
10	美国商务部《保障信息和通信技术及服务供应链安全》（ICTS）临时最终规则	ICTS 规则管辖范围主要覆盖了六种信息通信技术，包括关键基础设施、网络系统、广泛使用的个人数据托管系统、广泛应用的数字应用程序、广泛使用的监控系统，以及新兴技术（例如人工智能、量子计算等）	2021 年 1 月
11	美国第 14028 号行政令《关于改善国家网络安全》	明确要求美国联邦政府加强软件供应链网络安全管控	2021 年 5 月
12	NIST SP800-161《系统和组织的网络安全供应链风险管理实践指南》	为 CII 运营者有效管理供应链网络安全风险	2022 年 5 月
13	欧盟《欧盟网络安全战略》	要求采取措施确保用于关键服务和基础设施的硬件和软件值得信赖和安全可靠	2013 年 2 月
14	ENISA《供应链完整性：ICT 供应链风险和挑战概述和未	建议建立同意的 ICT 供应链网络安全风险评估框架来开展 ICT 供应链网络安全评估工作	2015 年 8 月

	来愿景》		
15	《网络弹性法案》	欧盟委员会发布，要求所有出口欧洲的数字化产品都必须提供安全保障、软件物料清单、漏洞报告机制，以及提供安全补丁和更新。	2024 年 10 月

相关法规政策、标准都可以参考，有些标准适用于软件或 ICT 产品，对于智能网联汽车的供应链网络安全要求也同样可以参考。

1.4 研究目的与意义

1.4.1 研究目的

尽管国际及国内已有如 UNECE R155、ISO/SAE 21434、GB 44495-2024 等法规和标准对汽车全生命周期的网络安全进行规范，但未对智能网联汽车供应链的网络安全要求和实施细则提出具体规定。缺乏统一、系统且可靠的供应链网络安全标准导致整车企业在网络安全管理中面临诸多挑战，不仅增加了维护与合规的复杂性，也加剧了企业间协作的难度。随着智能网联汽车网络攻击的多样化和频繁化，供应链中的安全漏洞逐渐成为攻击者的重点目标，这不仅威胁到车辆的功能和运行安全，更可能对用户的生命与财产安全造成严重威胁。

因此，本报告的核心目标是研究《智能网联汽车 供应链网络安全技术要求》标准化的可行性，旨在研究行业现状，梳理行业统一的安全需求，尽量明晰以规范网络安全实践。这将有助于提升汽车供应链的整体安全性，帮助需方有效识别和应对信息安全隐患，降低因网络攻击所引发的风险，从而确保智能网联汽车在复杂网络环境中的安全可控。

1.4.2 研究意义

本研究聚焦智能网联汽车供应链网络安全这一产业核心领域，对完善智能网联汽车玩过安全标准体系、破解产业实践瓶颈具有重要支撑作用。当前智能网联汽车供应链已呈现“全链路联网化、参与主体多元化、技术架构复杂化”特征，叠加网络攻击从单点渗透向供应链协同攻击演进的趋势，现有安全管理体系暴露出责任边界模糊、安全需求传递衰减、中小供

应商能力短板突出、动态评价机制缺失等结构性缺陷，亟需从体系化层面构建适配产业特性的安全治理方案。

本研究丰富了智能网联汽车供应链安全治理的理论框架。通过明确不同环节、不同层级供应商的安全责任耦合关系，填补现有研究在多级供应商协同安全管控、信息共享与保密平衡机制等细分领域的理论空白，为供应链安全治理的标准化、规范化提供理论支撑。针对当前责任划分模糊、标准碎片化问题，研究将构建覆盖供应链全流程的安全管理规范，明确主机厂与各级供应商的安全责任清单与履约评估标准，推动形成与 ISO/SAE 21434、GB 44495-2024 等标准衔接适配的强制性实施细则，解决安全责任追溯难、中小供应商合规落地难的现实困境。针对安全需求传递偏差、信息孤岛等协同障碍，研究将建立标准化的安全需求传递载体与验证机制，界定不同类型信息的共享边界与加密传输规范，实现安全需求从主机厂到末端供应商的精准落地，规避因需求误读导致的安全防护缺失与资源错配。针对威胁监测响应滞后、漏洞管控周期长等技术痛点，研究将明确供应链各环节的动态监测指标与应急响应技术要求，优化 OTA 升级的安全审批流程与漏洞修复闭环机制，缩短风险暴露窗口，提升供应链对新型网络攻击的快速响应能力。

本研究将推动智能网联汽车供应链安全能力的整体提升。通过构建系统化的供应商安全管理体系、技术要求、测评方法，将网络安全基本要求嵌入供应商准入、存续管理全流程，促使供应商补齐网络安全技术与管理短板，改善供应链安全能力不均衡的格局。同时，标准化的安全管理策略将降低全行业的合规成本与协同管理复杂度，为技术创新提供安全可控的发展环境，为汽车产业数字化转型与交通运输网络安全提供核心保障。

2 智能网联汽车供应链网络安全管理

2.1 供应链网络安全管理目标

智能网联汽车供应链网络安全管理的核心目标是推动车辆制造商、产品供应商及第三方服务商在网络安全管理流程、网络安全技术要求、网络安全测评方法上形成共识，构建覆盖车辆全生命周期的分级责任体系，确保供应链各环节产品、软件、数据及服务的安全可控与全链路可追溯。

具体目标包括三方面：一是建立统一的技术标准与安全基线，衔接 ISO/SAE 21434、GB 44495-2024 等法规要求，实现安全需求向各级供应商的精准穿透，保障全链条防护措施达标并适配新兴技术安全挑战；二是构建全生命周期验证评估与动态监控机制，聚焦硬件零部件、车载软件、数据服务等关键环节，通过定期安全检测、渗透测试及 SBOM 全生命周期管理，防范技术漏洞、软件后门、数据泄露等风险；三是提升供应链协同应急响应能力，建立标准化应急响应流程与协作机制，明确高危漏洞修复时效要求，确保安全事件发生时可快速处置、精准追溯，降低风险扩散影响。

长远目标是打造协同互信的供应链网络安全生态，通过统一安全基线、动态监管体系与协同改进机制，推动各方共建共享安全实践成果，持续优化网络安全标准，最终保障智能网联汽车全生命周期稳定安全运行，赋能行业高质量可持续发展。

2.2 供应链网络安全风险识别

智能网联汽车供应链的网络安全风险贯穿于供应链生命周期各阶段。由于各阶段中涉及的风险评估侧重的方向随着各阶段实施内容、对象、安全需求不同，使得风险评估的对象、目的、要求等各方面也有所不同。以下依据供应链生命周期各阶段，列出应关注的重点风险。

2.2.1 产品采购阶段

（1）供应商准入环节

1）供应链体系能力风险

供应商未建立完善的网络安全管理程序，无法确保全链条的安全性。

供应商缺乏分布式网络安全管理能力，难以监控下游供应商的网络安全情况。

供应商缺乏对产品概念、开发、生产等阶段的网络安全管理能力，可能导致安全漏洞。

2）供应链技术能力风险

外部连接的安全要求未能满足，如远程控制指令未做真实性完整性校验，三方应用缺乏防火墙保护。

车云通信和 V2X 通信的安全要求未落实，通信内容和组件可能受到攻击。

车辆软件升级的安全性不足，可能存在在线或离线升级过程中的漏洞。

车辆数据安全管理不当，导致敏感信息和车辆关键数据泄露。

（2）供应商定点环节

1）信息安全技术能力的定点评估

供应商未具备足够的密钥保护、硬件支持环境能力，或无法有效管理身份验证和访问控制。

供应商缺乏 OTA 开发能力，可能导致远程刷写安全问题。

防火墙、IDS 等安全机制部署不当，可能被绕过或显著影响性能。

供应商在安全日志、漏洞扫描、系统加固等方面的能力不足，可能导致系统被攻破。

供应商未能满足安全启动要求或忽略调试接口的禁用，可能留下后门。

2）数据安全及隐私合规技术能力

供应商未进行 ECU 中数据分类和保护设计，可能导致数据泄露。

数据出车功能中，车端脱敏开发不完善，可能导致隐私泄露。

2.2.2 产品开发阶段

未制定完善的网络安全计划，缺乏有效的风险管理措施。

威胁分析和风险评估不到位，未能识别潜在的安全风险。未制定网络安全规范，可能导致产品存在安全隐患。

产品未进行完整的网络安全验证，缺乏静态/动态分析、渗透测试、模糊测试等安全验证环节。网络安全验证与确认报告未按时出具，无法确保产品在交付前具备必要的安全性。网络安全验证报告缺乏溯源性和可复现性，导致无法支撑安全确认。

2.2.3 产品生产阶段

网络安全生产计划未制定，生产过程中的潜在安全隐患未被有效控制。生产过程中未制定网络安全控制计划，导致生产线存在安全漏洞。

未有效实施网络安全生产控制措施，可能导致安全问题无法及时修复。

2.2.4 产品交付阶段

软件版本交付中缺乏签名验证机制，源代码或二进制包交付中存在信息泄露风险，安全参数（密钥、密码算法等）在交付时保护不当。

2.2.5 产品运维阶段

网络安全监控来源不全，无法及时发现系统中的安全隐患。

网络安全信息未进行有效分类，导致在安全事件发生时缺乏有效的应对策略。

未对安全事件进行评估，漏洞分析及信息共享机制不到位，可能导致漏洞被滥用。

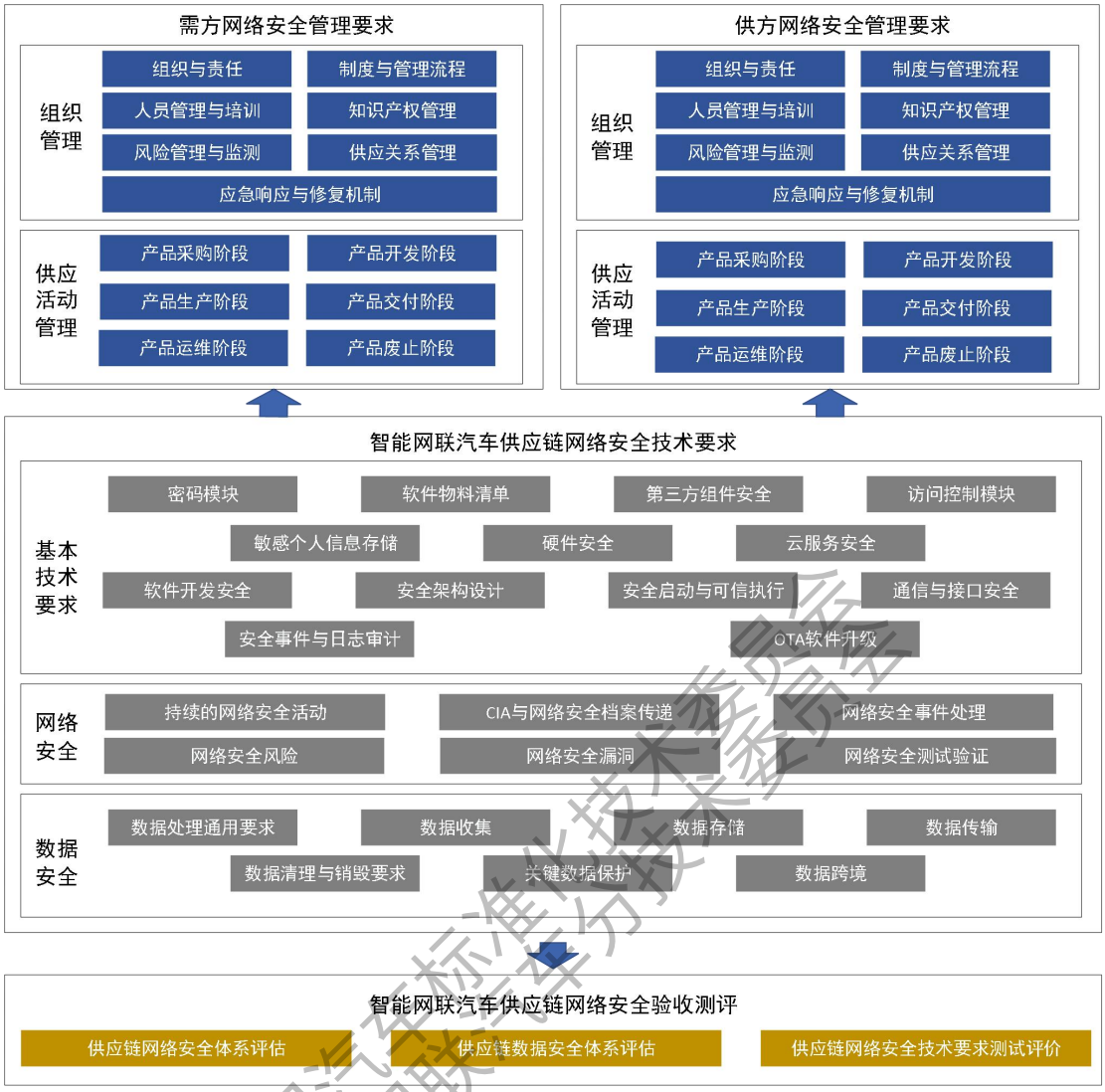
网络安全事件响应不及时或不充分，可能导致事故扩大。

2.2.6 产品废止阶段

产品废止阶段的网络安全管理不规范，可能留下潜在的安全风险

2.3 供应链网络安全防护架构

基于智能网联汽车供应链的相关定义及供应链网络安全风险分析，确立了智能网联汽车供应链网络安全保护框架。该框架规定了智能网联汽车供需双方的网络安全技术要求，进一步从组织管理和供应活动管理两方面规定了需方网络安全管理要求和供方网络安全管理要求，并依据技术要求提出了对应的验证测评方法。



2.4 需方网络安全要求

2.4.1 组织管理

2.4.1.1 组织与责任

（1）组织结构与责任划分

需方应建立完善的网络安全管理体系，覆盖整个产品生命周期，并明确划分相关部门与人员的责任。需方应设立专职网络安全负责人，领导和监督网络安全工作的实施与发展，同

时设立跨部门的网络安全委员会，以确保不同职能部门在网络安全方面的协同与沟通。该委员会应定期评审和调整网络安全政策与战略，以应对不断变化的安全形势。

需方还应设立专职网络安全岗位或小组，负责具体的网络安全工作，如安全设计、渗透测试、风险评估等，确保技术层面的安全措施有效落地。高级管理层应定期审阅网络安全工作进展，并为网络安全相关决策提供支持。

（2）跨部门协作与信息共享

需方应确保各部门（如研发、信息技术、运营、安全、法务等）之间的有效沟通与协作，以便及时发现和解决潜在的网络安全问题。各相关部门应定期参加网络安全管理会议，共享网络安全事件与问题，并共同推动风险控制措施的实施。应建立定期汇报机制，确保高层管理者对网络安全情况的全面了解，以做出及时的决策。

2.4.1.2 制度与管理流程

（1）网络安全管理制度

需方应建立并不断完善覆盖网络安全所有环节的管理制度，制度内容应包括产品设计、开发、生产、运营、数据保护等各个方面。所有网络安全管理制度应遵循国际标准和国家标准，如 ISO/SAE 21434、GB 44495-2024 等，同时结合企业实际需求进行适当调整。

需方应特别关注信息资产管理、网络安全风险识别、供应链网络安全管理、数据加密、隐私保护等重要领域，确保安全管理体系的全面性和系统性。

（2）安全事件应急响应机制

需方应建立完备的安全事件应急响应机制，确保在发生网络安全事件时，能够迅速启动预案并采取有效措施。应急响应机制应包括事件通报流程、漏洞管理、责任划分、处理步骤等内容，以确保在事件发生后，能够高效、有序地响应和处理。

需方应根据安全事件的性质与严重程度设立不同的响应级别，并配备专门的应急处理团

队，保证处理过程不间断、无缝衔接。

（3）审计与改进机制

需方应定期进行网络安全管理体系的内部审计与评估，审查网络安全措施的有效性与适应性。审计内容应涵盖网络安全政策的执行情况、风险防范措施的落实效果、事件响应处理能力等。审计结果应反馈给高层管理团队，及时做出相应调整和改进。

此外，需方应建立持续改进机制，定期评估并更新网络安全管理体系，确保其始终符合行业最新的安全要求与技术标准。

2.4.1.3 人员管理与培训

（1）人员资质与意识培训

需方应确保所有从事网络安全相关工作的人员具备必要的资质与能力。开发、运维及安全岗位的人员应具备较强的网络安全意识，定期进行调查考核，确保其适应岗位要求。

所有员工应接受网络安全意识培训，强化网络安全意识，确保每位员工都能认识到其在保障企业网络安全中的重要角色。针对技术岗位的人员，需定期提供技术性网络安全培训，提升其专业技能，应对日益复杂的网络安全威胁。

（2）权限控制与身份验证

需方应实施严格的权限管理措施，确保员工仅能访问与其职责相关的信息和资源，严格执行最小权限原则。对涉及敏感个人信息和关键资产的系统，应采用多因素身份认证与加密保护机制，以防止未经授权的访问。

需方应定期评审权限分配情况，及时调整与撤销不再适用的权限，防止权限滥用或泄露。

需方应建立有效的身份验证与访问日志记录机制，以便进行安全审计。

2.4.1.4 知识产权管理

需方应对核心技术和知识产权采取严格的保护措施，防止未经授权的访问、泄露或滥用。所有核心技术资料（如源代码、设计图纸、专利等）应加密存储，并设置严格的访问控制。

需方应明确知识产权管理制度，涵盖软件授权、专利管理、技术转让及许可协议等内容，确保所有知识产权的使用合法合规，并避免因知识产权问题产生法律纠纷或商业风险。

对于涉及机密信息的外部合作，需方应在合作开始前与供应商签署保密协议，以明确双方保密义务，确保知识产权安全。

2.4.1.5 风险管理与监测

（1）风险识别与评估

需方应定期进行全面的网络安全风险评估，评估内容应包括信息资产、技术设施、人员管理、流程控制等各个环节。评估应基于当前的威胁情境、漏洞扫描结果及历史安全事件数据，识别出潜在的安全风险和脆弱环节。

需方应确保评估结果及时反馈给高层管理团队。对评估中识别的风险，需方应制定并执行风险应对策略，以降低安全威胁。

（2）安全监控与预警

需方应建立全面的网络安全监控体系，对关键系统与基础设施进行 24 小时全天候监控。监控内容应涵盖流量异常、访问控制、系统漏洞、恶意软件等多方面的安全指标。

需方应实时分析网络安全事件，发现潜在的安全威胁并及时发出预警，确保能够在攻击发生之前或初期就采取有效应对措施。

2.4.1.6 供应链管理与关系

（1）供应链网络安全管理

需方应建立完整的供应链安全管理体系，确保其供应商及第三方合作伙伴符合网络安全要求。需方应对核心零部件供应商进行定期评估，确保其网络安全措施与需方保持一致。

需方应要求供应商提供有效的网络安全管理证明，并对其网络安全能力进行评估与审查，确保供应链中的任何安全漏洞不影响最终产品的安全性。

（2）供应链安全协议与数据共享

需方应与供应商签署网络安全协议（CIA），明确双方在网络安全中的责任与义务，确保供应商在产品生命周期内持续遵守网络安全标准。

需方应确保与供应商之间的数据共享过程安全，避免数据在传输或存储过程中的泄漏。需方应建立数据保护协议，确保所有共享数据加密传输，并加强对敏感个人信息的保护。

2.4.1.7 应急响应与修复机制

需方应在网络安全漏洞被确认后，及时通知相关方，并在协议规定的时间内处理漏洞。需方应与供方共同制定漏洞管理与修复流程，明确修复的时限、漏洞严重程度的评估标准、修复步骤等。

需方应建立漏洞响应团队，专门负责漏洞的快速处理和修复工作。对于高危及以上漏洞，应优先进行处理。

2.4.2 供应活动管理

2.4.2.1 产品采购阶段

（1）供应商评估与分类

需方应将网络安全要求整合至供应商分类及分级评估体系中，特别针对核心零部件，需单独明确供方应满足的网络安全要求。

需方应将供方的网络安全能力应纳入评估机制，核心零部件应要求符合 ISO/SAE 21434、GB 44495-2024 等相关网络安全标准。

需方宜将供方的 ISO 27001、TISAX 等证书作为网络安全环境的评估要求，但不得代替产品级安全责任。

（2）采购流程构建

需方应在采购阶段需建立一套标准化的流程，专门用于识别与网络安全相关的项目，并在招标与采购过程中，安排具备汽车行业网络安全能力的专业人士参与。

需方应明确所需的产品和服务的安全需求，并制定详尽的验收标准，以确保其满足网络安全要求。

（3）合同要求

必须在相关协议与合同中引入汽车网络安全协议文档，该文档应涵盖网络安全活动的执行、漏洞处理机制及明确的安全需求，以确保法律和业务上的必要保障。

2.4.2.2 产品开发阶段

（1）开发监督与评审

需方应对供应商产品的开发过程实施监督与评审，确保参与供方的威胁建模及设计评审，从而共同识别系统级潜在安全缺陷，降低后期修复成本。

需方应要求供方明确源代码审计机制的实施、安全编码规范的遵循，并提供开源组件清单，以防止引入存在已知漏洞或不当开源许可风险的组件。

（2）风险导向开发

供需双方应重视“基于风险的网络安全工程实践”，确保所有安全目标均基于风险分析成果而制定，以提升产品安全性。

2.4.2.3 产品生产阶段

需求应要求供方基于已下发的网络安全要求制定涉及产品生产阶段的网络安全措施和控制计划，以确保产品生产阶段的网络安全实施。

需方应要求供方提供产品产线生产过程的风险评估，依据风险识别结果出具生产阶段的网络安全需求，并提供对应的生产过程安全保障方案，以防止生产过程引入的安全风险。

需方应对供应商产品的生产过程实施监督与评审，确保供方在产品生产过程中安全方案被正确执行。

2.4.2.4 产品交付阶段

需方应实施对交付包及镜像的完整性和真实性验证，确保交付的产品未遭篡改，并在交付产品与开发阶段之间保持一致性。

在 CIA（网络安全接口协议）阶段，需方应制定网络安全评估计划，以评估供应商的网络安全交付物，并进行必要的确认测试，确保交付产品的质量。

2.4.2.5 产品运维阶段

需方应明确运维团队的职责、安全范围及具体内容，确立运维流程。如相关产品需要供方进行运维，需方应明确运维需求，并签署详细的运维协议。

应根据漏洞管理机制组建供需双方的漏洞响应团队，明确供方在补丁响应、事件处置方面的时限责任。

需方应提供统一的漏洞上报和下发途径，并将发现的产品相关的漏洞信息分发给供方，以确保响应的及时有效。

2.4.2.6 产品废止阶段

（1）敏感个人信息清除与处理

需方应要求供应商进行敏感个人信息的识别，并提供完整的敏感个人信息清除方法及操作说明。

对于个人隐私和其他重要敏感个人信息，需方必须确保在产品废止阶段进行全面清除处理。若涉及存储密钥或证书的安全环境，需方应根据供方提供的清除方法及操作说明清除相关数据。

（2）退役处理流程

依据产品生命周期管理标准，需方应制定详尽的产品退役处理流程，以防止核心信息的泄露和仿冒攻击的发生。

2.5 供方网络安全要求

2.5.1 组织管理

2.5.1.1 组织与责任

供方应建立覆盖产品全生命周期的网络安全管理体系，并设立网络安全负责人及网络安全委员会，确保高效沟通与协同。

核心零部件供应商应指定网络安全责任人，负责牵头制定供应链全生命周期网络安全策略、统筹安全体系建设与风险管控工作，并定期向高层管理团队汇报网络安全工作进展、风险态势及重大事项，确保高层及时掌握安全状况并提供资源支持。

2.5.1.2 制度与管理流程

（1）网络安全管理制度

供方应建立并维护涵盖开发、运维和数据保护等方面的网络安全管理制度，该制度应遵循 ISO/SAE 21434、GB 44495-2024 等相关标准。

供方应制定至少包括资产管理、供应链网络安全风险识别、处置与监督检查等内容的总体方针和安全制度。

（2）安全事件应急响应机制

供方应建立网络安全事件的应急响应预案，并与车辆制造商建立协同响应机制，包括漏洞通报流程，以确保安全事件的及时响应与处理。

（3）审计与改进机制

供方应定期审查网络安全管理体系的有效性，监督安全控制措施的落实情况，并针对发现的偏差进行及时纠正，以保障体系的持续改进。

2.5.1.3 人员管理与培训

（1）人员资质与意识培训

核心零部件开发人员需持有网络安全相关认证，并进行背景调查以确保岗位适配性。

所有员工需接受针对汽车网络安全的意识文化培训，相关部门工作人员应根据职责进行网络安全技术培训，确保技术能力与岗位要求相符。

（2）权限控制

采取最小权限原则，禁止无关人员访问核心部件的设计数据或生产系统，以保护关键资产。

2.5.1.4 知识产权管理

供方应对核心资产进行加密存储并设置访问控制，以防止未经授权的访问，并禁止将核心知识产权（如源代码、设计图纸）托管于境外服务器或第三方平台。

建立完善的知识产权管理制度，涵盖软件授权证书、专利、软件著作权及许可协议，防止因知识产权问题导致的法律风险。

2.5.1.5 风险管理与监测

供方应定期进行网络安全风险评估，识别与信息安全相关的资产及管理工具，并及时向需方通报识别的风险和漏洞。

核心零部件供应商应具备年度网络安全审计报告，由内部或第三方机构出具。

2.5.1.6 供应链管理与关系

（1）供应链透明化

供方应提供完整的网络安全相关的供应商层级清单，包括多级供应商的信息（至少详细到下一层级供应商），以确保车辆制造商能够追溯到关键部件的来源。

供方与其供应商需签署网络安全接口协议（CIA），以保证网络安全质量的一致性，并对其供应商开展网络安全能力评估审查。

（2）数据共享与沟通

供方应建立安全的沟通渠道，确保在发现新的安全漏洞时能够迅速通知所有相关方，保持信息的透明性与及时性。

2.5.1.7 应急响应与修复机制

供方必须在确认网络安全漏洞后在《网络安全接口协议》协定的时间内通知需方，并按

照协议要求时限完成漏洞的修复，以确保安全事件的闭环处理。

供方应依照客户要求制定漏洞管理流程，明确修复阈值、漏洞评分标准、漏洞扫描频率及响应时间等，并建立漏洞响应团队。

2.5.2 供应活动管理

2.5.2.1 产品采购阶段

（1）供应商评估与合规性

供方应配合整车厂完成网络安全能力评估。该评估应覆盖网络安全保障能力、开发能力、生产过程能力和运营能力等，并需提供能力证明材料，以便评估其是否符合整车厂提出的安全技术和交付物要求。

供方需具备并提供网络安全保障能力或网络安全管理体系等相关认证文件，证明其在网络安全管理方面的能力。

（2）协议及合约管理

供方须与车辆制造商签署《网络安全开发接口协议（CIA）》，明确双方在数据保护、漏洞披露及连带责任方面的条款，确保各方承担相应的安全责任。

核心零部件供应商必须提供相关的网络安全合规性认证，如 ISO/SAE 21434、GB 44495-2024 等，以证明其产品符合最新的安全要求。除此之外，供应商还应接受定期的安全审查和评估，确保其安全管理措施在整个供应周期中持续有效。

非核心零部件供应商需提供基础安全认证，并禁止使用未经验证的开源代码或第三方组件。

（3）风险管理

供方应对其供应商及合作伙伴进行全面的风险评估、分级与持续监控。通过分析供应链结构，识别潜在的安全风险，如数据篡改、假冒伪劣产品、供应中断和信息泄露等，评估风险的可能性与影响程度，制定相应的应对措施。

2.5.2.2 产品开发阶段

（1）安全开发流程与管理

供方宜遵循安全开发生命周期（Secure Development Lifecycle）的标准进行产品开发，涵盖威胁建模、安全设计、静态代码审计及安全测试，降低产品漏洞的密度，确保产品在设计阶段就具备安全防护能力。

软硬件设计架构时，需确保融入需方提出的网络安全需求，并形成相关的安全开发文档与测试规范，以确保在后续的开发与测试中有据可依。

（2）风险识别与评估

针对核心零部件，供方需建立风险评估制度，开展 TARA（Threat Analysis and Risk Assessment）分析，识别零部件的关键要素及潜在威胁，合理管理已识别的风险，以确保制定出有效的网络安全目标与措施。

（3）文档与确认

供方需输出相应的开发文档，包括网络安全计划、网络安全评估报告和确认测试记录等，确保所有开发活动的透明性，并为后续的审查和追踪提供详实依据。

2.5.2.3 产品生产阶段

供方需对产线生产过程进行风险评估，识别生产过程可能的安全风险，基于风险识别结果出具网络安全需求，采取相应的安全措施以保障生产过程的网络安全。

（1）日志与文档留存

供方需对涉及网络安全的关键生产操作（如固件刷写、密钥注入、接口配置）进行日志记录，并保存日志或文档，确保操作的可追溯性。

（2）事件管理和报告流程

供方应制定生产环境中网络安全事件的应急响应流程，并建立明确的向需方报告安全事件的机制。

（3）密钥与证书的安全注入流程

若存在需要预置加密密钥、数字证书或安全凭证的车辆组件，应在安全环境中通过安全通道注入加密密钥与证书，防止泄露。

（4）生产安全管理要求

保障生产线、编程设备、测试系统的访问控制与防护，防止恶意代码或未经授权的固件注入。

（5）固件与软件完整性

确保编程到 ECU/芯片中的固件及软件包来自可信来源，并经过数字签名或哈希校验验证完整性。

（6）安全标定与测试

对所有对外暴露接口（含通信接口、数据接口等）实施分类分级管控，基于最小权限原则明确访问主体、权限范围及操作流程，配置身份认证、访问审计、加密传输等防护措施，确保接口访问可追溯、可管控。

非必要调试口（含物理调试口、远程调试接口）在产品出厂交付前须完全封闭或禁用；确需保留的调试接口，需单独设计安全访问机制（如加密认证、临时授权、访问时限管控等），并纳入供应链安全测试范围，验证其防护有效性。

（7）生产记录与可追溯性

建立完整的生产安全日志与供应链可追溯体系，确保未来可进行安全事件溯源。

2.5.2.4 产品交付阶段

（1）交付物的安全验证

供方应在交付物中提供真实性和完整性证明材料，确保所有交付的产品完整性未被篡改并符合网络安全标准。

在交付过程中，供方需确保所有交付的文档和资料保持真实性，并支持需方的验收程序，包括渗透测试、漏洞扫描和安全配置检查。

（2）信息共享与支持

供方需在交付过程中进行必要的资源支持，以协助整车厂进行产品信息安全的确认，确保各项数据真实可靠，以便及时处理潜在问题。

2.5.2.5 产品运维阶段

（1）监测与漏洞响应

供方需提供产品网络安全监测与评估计划，确保对网络安全事件进行及时响应，支持产品相关安全漏洞和事件的分析与处置。

建立完善的漏洞响应机制。供方须在高危及以上漏洞发生时，在 CIA 协定的时间内及时通报车辆制造商，并提供相应的修复方案与执行时间表，确保信息安全事件的快速处理。

（2）维护与更新

供方需建立产品的漏洞管理与分析流程，确保高危及以上漏洞在约定时间内得到处置或给予合理解释。供方应持续监控运营阶段的产品，必要时进行软件更新与系统的整体评估。

（3）远程监控与补丁机制

供方应支持车辆制造商对非核心部件的远程监控，并定期提供安全补丁更新。对无法升级的部件，供方需明确风险及替代方案，保障产品在整个生命周期内的安全性。

2.5.2.6 产品废止阶段

（1）网络安全服务终止

供方需在产品退役前完成终止网络安全服务的程序，并提供相关的服务承诺文件，确保整个过程符合相关法律法规的要求。

在产品退役时，供方应实施敏感个人信息的清除措施，包括进行敏感个人信息擦除和恢复出厂设置，确保没有信息泄露的风险，并提交销毁证明与清除报告。

（2）数据与设备管理

对于退役的旧设备，供方需实施符合行业标准的数据销毁策略，防止任何敏感信息的恢复，确保数据的隐私与安全。

供方须建立旧设备报废机制操作指南，对于所有退役产品，需确保相应的记录与审核过程，避免设备流入灰色市场或被用于后续的恶意分析活动。

（3）支持与承接

对于更换的产品，供方应支持数据迁移，并提供必要的后续支持，确保在产品废止阶段的服务不会影响消费者的体验和使用。

3 智能网联汽车供应链网络安全技术要求

3.1 基本技术要求

3.1.1 密码模块

密码算法应采用符合国家或国际的主流算法，如 SM2、SM3、SM4、AES、RSA 等，严禁使用已知存在安全问题的算法，例如 SHA-1 和 MD5。针对不同安全等级的应用场景，应合理配置密钥长度。

应针对不同安全等级的应用场景，应合理配置密钥长度。高安全场景推荐采用高安全等级的硬件密码模块（包括安全芯片）。推荐密码模块通过 GB/T 37092 二级及以上，或 CC EAL4+以上级别的安全认证，以增强数据安全性和系统可靠性。

硬件密码模块应具备物理防篡改能力，支持对温度、电压等环境异常的检测。软件密码模块推荐选用通过 FIPS 认证、通用标准的安全认证（Common Criteria，CC 认证）或国密认证的加密库。

密码模块应具备完善的密钥生命周期管理机制，包括密钥生成、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等的全过程，并支持接口调用权限控制（如基于角色的访问控制），从而增强数据传输与存储过程的安全可靠性。

3.1.2 软件物料清单

企业需维护规范化的 SBOM 清单，详细列出软件生产商、组件版本号或标识符及软件许可证等信息，并采用符合国际或国家标准的格式，如 SPDX 或 CycloneDX。SBOM 的颗粒度应覆盖所有软件组件，包括第三方库、中间件、操作系统，细化至源代码版本和依赖关系层级，确保全面反映系统构成。禁止使用存在高危及以上漏洞未经处置的开源组件，以防引入已知高风险漏洞。

SBOM 应具备与漏洞数据库联动的能力，通过自动分析组件的漏洞对车辆功能潜在影响路径，确保及时识别高风险组件及其调用路径。具体来说，分析要求应包含对依赖组件的漏洞可达性分析，识别攻击路径，并在存在漏洞的组件中明确其运行环境及网络连接情况。此外，SBOM 应支持与供应链管理系统（SCM）的集成，以便进行有效的依赖关系管理和版本控制。

对于每个依赖组件，SBOM 需标明组件名称、版本及供应商信息，并确保定期更新与维护，以与实际版本保持同步。通过这些综合技术要求，智能网联汽车供应链中的软件物料清单将有助于提升软件安全性，确保高效、可靠的系统运行。

3.1.3 第三方组件安全

应对第三方组件实施严格管理与安全控制。除操作系统预留外的第三方组件必须来自可信源或官方仓库。对未经验证的组件，应进行风险评估，并采取隔离、替换或安全配置等措施。应对组件进行漏洞扫描、安全性审查，宜对关键安全接口执行渗透验证。

应建立第三方组件更新管理策略，明确更新频率、验证流程及向后兼容性。当发现高危漏洞时，供方应在 CIA 协定时间内提供处置方案，并支持更新方案的实施；更新组件时，应同步更新 SBOM，并评估依赖链中的潜在风险。对存在高危漏洞且无法及时修复的组件，宜迅速停用或替换，并更新 SBOM 记录，若无法停用和替换的，应进行风险分析，制定和实施缓解措施。

应建立组件弃用管理流程，包括过渡期管理、数据迁移完整性和遗留接口持续监控；不同类型组件应按照更新策略矩阵进行周期性验证和安全检查，确保安全关键组件在规定时间内完成紧急补丁更新。

3.1.4 访问控制模块

应在操作系统层面实施强制访问控制（MAC），并通过 DAC 或操作系统权限管理限制进程和用户对文件、数据库、ECU 接口及其他关键资源的访问。对于重要接口，如诊断

口、OTA 升级接口和关键控制命令，应支持多因素认证（MFA）及车载身份验证机制（如硬件密钥或生物识别），以确保关键操作仅由授权实体执行。

核心零部件的访问控制模块宜结合硬件安全模块（HSM），实现动态令牌刷新及异常行为实时阻断，以防止未授权访问。

网络接口（如 CAN、LIN、以太网、FlexRay）应实施白名单机制，禁止未授权设备接入，并结合身份认证和访问控制策略进行端到端保护。

3.1.5 敏感个人信息存储

所有敏感个人信息，包括密钥、口令和日志数据，需进行安全存储，防止未经授权的访问和篡改。

数据加密密钥宜通过硬件安全模块（HSM）进行托管，密钥的生命周期应受到严格管理，包括自动轮换和定期更新，确保密钥管理过程的安全性和合规性。

敏感个人信息在存储和处理过程中应采用加密技术，未授权的应用不得访问和使用这些数据，尤其是指纹、面容和声纹信息等敏感个人数据，在存储前必须经过技术处理，仅存储特征值。同时，数据删除或销毁应遵循“不可恢复”标准。对于日志数据，宜通过云端存储加密备份，并设定足够的存留期，以防止数据丢失和篡改。

云端系统应建立安全访问控制机制，防止敏感个人信息被未经授权的读取和篡改。对数据存储介质在更换或设备退役前必须执行数据擦除或销毁，这样能够在任何情况下保护敏感个人信息不被泄露。通过这些综合措施，智能网联汽车领域的敏感个人信息存储将有效抵御潜在的安全风险，支持行业可持续发展。

3.1.6 硬件安全

智能网联汽车的硬件安全需构建覆盖从单元级（包括传感单元、控制单元、执行单元、通信单元等）到芯片级（包括芯片和 IP）的多层次防护体系，旨在建立可信计算环境，防

范硬件层面的非授权访问、数据泄露与恶意篡改。硬件安全要求应贯穿产品全生命周期，并与密码算法、访问控制等要求协同实施，形成统一的安全基线。

3.1.6.1 单元级安全要求

单元级安全要求针对整车电子电气架构中的功能单元，涵盖传感、控制、执行及通信等单元的安全防护。

传感单元（如摄像头）在数据采集和传输过程中宜采用加密、完整性保护机制，防止数据被窃取或篡改。传感器固件宜保证其完整性和真实性，可通过签名验证等安全机制实现，以确保固件来源可信及防篡改。在重要数据传输跨越不同总线或外部接口时，宜启用数据加密和完整性校验。

控制单元（如中央网关、域控制器）应严格限制外部接口数量，仅保留业务必需接口（如 USB、SDIO、OBD 等接口）。交付时需向 OEM 提供接口说明并通过安全审核。量产阶段应禁用调试接口（如 JTAG、UART、SWD），或实施严格的访问控制。PCB 单板上的标识调测、端口和管脚的可读丝印应去除，以防范敏感硬件信息泄露。关键控制器（如 T-Box、网关）应支持数据完整性和保密性保护，具备防范指令注入、抗重放攻击等能力，同时宜集成 HSM，支持密钥全生命周期管理、加解密和签名验证等能力。

执行单元（如线控制动、线控转向系统）应验证控制指令完整性和真实性，仅响应授权控制器命令，并支持安全状态监测功能。

通信单元（如 V2X 模块、T-Box）应保障通信链路的保密性和完整性，采用安全版本的传输层协议（如 1.2 及以上 TLS 、TLCP 等）防范数据泄露或篡改。通信模块应支持身份认证和密钥协商机制，确保通信双方的真实性。对外通信模块应支持远程固件签名验证与安全更新机制，防范恶意固件注入。

3.1.6.2 芯片级安全要求

芯片级安全要求聚焦于芯片自身的可信设计和物理防护能力，为单元级安全提供基础支

撑。安全关键电子控制单元（如网关、中央计算、OTA 模块）内置的计算芯片（如 SoC）、控制芯片（如 MCU）、通信芯片等推荐集成 HSM 模块。

此外，关键芯片宜优先选用 BGA（球栅阵列）、LGA（引脚网格阵列）等封装形式，减少管脚暴露，以降低物理攻击风险。

3.1.7 云服务安全

API 与抗 DoS：所有云服务间的 API 调用必须实施认证、授权与限流机制；接入 WAF 防护/DDoS 与异常流量防护，避免潜在的网络攻击；后端服务支持幂等、重试与熔断降级。

零信任：应遵循零信任原则，所有访问应具备身份认证机制，并基于身份最小权限的原则授权，访问过程可审计。运维与第三方访问必须启用 MFA。

服务可用性：供应链所用云服务需满足 SLA（服务等级协议）不低于 99.99%；当云服务中断、网络失联等异常场景发生时，车辆需具备独立安全运行能力，核心控制功能（如行驶控制、制动系统等）不受影响；供方需定期组织云服务中断场景下的降级策略演练。

3.1.8 软件开发安全

软件开发必须贯穿安全生命周期管理，包括需求分析、威胁建模、安全架构设计、代码审计、渗透测试及版本发布等环节。在开发过程中，使用静态应用安全测试和动态应用安全测试工具对代码进行自动化安全检测。对于高危及以上漏洞，要求在 72 小时内给出有效的风险降级处置措施，确保处置率达到 100%。

信息安全核心 ECU 的软件模块应执行安全开发生命周期（SDL），包含需求、设计、实施、验证和发布五个核心阶段，采用威胁建模、静态代码分析、渗透测试等技术手段。

3.1.9 安全架构设计

供应链各方应建立覆盖车辆端、云端及通信链路的安全架构，明确安全边界、信任根及

关键防护节点。

系统设计应依据安全分区原则实现功能隔离，并在体系层面实现纵深防御。

3.1.10 安全启动与可信执行

核心控制单元应具备安全启动机制，确保软件加载及固件更新的完整性与真实性。

应通过可信执行环境或硬件（保护）信任根防止篡改与伪造。

3.1.11 通信与接口安全

具有外部通信能力的部件应采用安全通信协议，并防止重放、劫持及中间人攻击。

物理接口应具备访问控制或防护措施，调试接口（如 JTAG、UART）应受限制管理。

3.1.12 安全事件日志与审计

关键系统与服务应记录安全事件日志，日志内容应可追溯、不可篡改，并定期审计与留存。

3.1.13 OTA 软件升级

OTA 升级包必须采用车辆制造商密钥签名机制，确保升级包的完整性和来源的可信性。必要时可采用双重签名机制，即供应商和车辆制造商双方进行密钥签名。

签名密钥需存储在硬件安全模块（HSM）中，遵循“专人管理、分级授权”原则；密钥销毁需执行不可逆流程，并留存完整的销毁记录。

3.2 汽车产品网络安全技术要求

3.2.1 持续的网络安全活动

在智能网联汽车的网络安全管理中，持续的网络安全活动是保护车辆系统免受网络攻击的基础。开发阶段，企业应实施安全开发生命周期（SDL），内容涵盖从需求分析、设计、开发到测试的各个环节。具体而言，通过执行威胁建模（TARA）能够帮助团队识别潜在威胁并进行影响分析；模糊测试和渗透测试则帮助发现系统的安全漏洞，确保应用程序和网络的安全性。此外，运维阶段应该建立定期的安全活动计划，包括定期开展自动化漏洞扫描并结合人工审核，以确保扫描结果的准确性和覆盖面。同时，定期举行的红蓝对抗演练能够模拟真实攻击场景，检验组织的安全响应能力及防御措施的有效性，确保所有环节都在安全框架下运作。

为了提高安全活动的实效性，企业还应建立网络安全事件模拟平台，定期组织演练，检测防御能力和响应效率。这不仅有助于发现安全机制中的不足，还能促进团队参与者之间的协作，提高整体的安全意识和反应能力。通过这些措施，车厂将能在不断变化的安全环境中，建立起更为稳固的网络安全防线。

3.2.2 CIA 与网络安全档案传递

为确保网络安全责任在供应链各层级间的可传递性与可验证性，需方与供方应签署正式的网络安全接口协议。该协议应明确安全边界、数据交互方式、加密与认证机制、密钥管理策略以及双方在安全事件处置、漏洞修复和信息通报中的职责分工。协议内容应与双方网络安全接口协议要求保持一致，并纳入合同附件进行约束。

供方应根据项目阶段向需方提交网络安全保证文档，以证明其产品或服务满足约定的安全要求。网络安全档案应包括但不限于：风险分析与威胁评估报告（TARA）、安全设计与防护措施说明书、漏洞扫描与渗透测试报告、安全验证与整改记录、合规性声明与签署确认。需方应对供方提交的网络安全档案进行审查与留存，确保内容真实、完整、可追溯。若发现

不符合项或安全隐患，供方应在限定期限内完成整改并重新提交验证材料。所有网络安全接口协议与保证文档应在车辆生命周期内保存，以满足法规审计及后期事件追溯的要求。

3.2.3 网络安全事件处理

网络安全事件处理是保障智能网联汽车安全的重要组成部分。对于网络攻击、数据泄露等安全事件，企业需制定详实的应急响应流程，从监测、发现、应对、分析到补救的每一个阶段都需有针对性的策略。在监测环节，建议部署车载入侵检测系统（IDS），实现对网络流量的实时监控，及时发现异常行为，例如未授权的固件刷写尝试。

一旦安全事件发生，应当立即启动响应措施完成事件隔离，确保受感染模块与正常系统的有效分离。这一过程尤为重要，因为快速的反应可以阻止潜在攻击的进一步扩散。事件发生后，根据事件严重程度进行分类，并在相应的时限内完成事件的溯源分析，生成包括攻击向量和影响范围的详细报告，以帮助相关团队了解事件的全貌及影响。补救措施包括进行根本原因分析，制定修复方案，宜通过第三方审计再确认修复的有效性。建立完善的事件处理机制，企业将能够减少安全事件对运营造成的影响，维护用户的信任和系统的可靠性。

严重程度定义及处置时限示例：

严重度	定义（示例）	初报（首次通知需方/相关方）	初步遏制/隔离决策	溯源/根因分析报告	修复/缓解
严重	影响安全、生命、关键功能或大范围泄露	≤4 小时	≤8 小时内启动首轮遏制措施	≤72 小时提供初步溯源	≤15 天提供修复或替代控制
高	影响关键功能/敏感个人信息但可局部缓解	≤8 小时	≤24 小时	≤7 天	≤30 天
中	功能影响有限或可局部缓解	1 个工作日	3 个工作日	14 天	≤90 天
低	信息性/非直接影响功能	3 个工作日	7 个工作日	30 天	合并到常规发布周期

3.2.4 网络安全风险

在网络安全风险管理方面，建立全面的风险识别和评估机制是至关重要的。企业首先需利用自动化工具进行定期的风险扫描，识别供应链中潜在的风险点，如未授权的第三方组件，这一过程是现代网络安全生态中不可或缺的一部分。针针对识别到的风险,企业应按 CVSS（Common Vulnerability ScoringSystem，通用漏洞评分级分类），高危风险按照双方协定的期限，确保其得到有效处置，并进行后续跟踪。

此外，组织内需建立风险看板，以实时更新风险状态，并定期向车辆制造商提交风险评估报告，确保各方保持信息的透明度和及时性。通过定期开展供应链网络安全风险评估，企业应主动识别现有和潜在的组织管理与供应活动中的安全风险，以便进行相应的风险缓解和应对措施。综上所述，系统化的风险管理能够助力企业在复杂多变的网络安全环境中有效应对各类挑战。

3.2.5 网络安全漏洞

在当前的网络环境中，及时、高效地管理网络安全漏洞显得尤为重要。企业需建立流程化的漏洞管理机制，包括漏洞的收集、分析、报告和处置等环节。通过集成漏洞数据库（如 CVE 和 CNNVD）以及内部红队测试与用户反馈渠道，组织可全面收集有关漏洞的信息。对应收集的漏洞信息，企业需进行深入分析，评估其对车辆功能（如制动系统和自动驾驶）可能产生的影响，并根据潜在风险确定修复的优先级。

对于高危及以上漏洞，企业以一周为限，确保其得到有效处置，并且处置方案需经过车辆制造商安全团队的审核。在漏洞处置后，企业应持续监控漏洞的利用尝试，以防止新的攻击向量出现。加强漏洞管理不仅能够有效降低风险，还能提升企业在应对安全威胁上的整体能力。

3.2.6 网络安全测试

网络安全测试是车载系统安全性验证的重要手段，确保产品在出厂时具备足够的安全性。

所有零部件在设计和开发过程中都应进行符合性测试，核心零部件则应执行更加严格的安全渗透测试，以验证其安全措施的充分性。

定期开展静态代码扫描和动态渗透测试的多类型安全测试，是确保系统安全的一种有效战略。测试范围应全面覆盖系统、接口、通信协议、远程服务等方面，合格的测试结果应被归档作为后续审核的依据。

3.3 汽车产品数据安全技术要求

3.3.1 汽车数据处理通用要求

所有汽车数据处理者在收集和处理数据时，必须确保其目的合理、明确，且与处理目的直接相关。除非得到用户的明确同意，车辆应默认不收集个人信息，并且不向车外提供个人信息。

处理个人信息时，必须采取对个人权益影响最小的方式进行数据采集与处理。

对于涉及生物识别（如指纹、声纹、面部识别、心律等）的敏感个人信息，汽车数据处理者应确保收集该类信息具有充分的目的，并符合隐私保护法律要求。

所有重要数据在处理之前应进行脱敏处理，以避免泄露用户的敏感信息。敏感个人信息的收集应严格控制，并采取适当的安全措施保护数据。

3.3.2 数据收集

汽车数据处理者在收集数据时应根据具体功能的要求，设定合适的数据采集精度，确保摄像头、雷达等设备的覆盖范围与分辨率满足功能需求。

车机系统应设置个人数据授权开关，默认状态为关闭。用户可自主选择是否开启驾驶行为分析数据采集，若未获得用户授权，不能进行相关数据分析。

对于敏感个人信息（如位置、指纹等）的采集，车载系统应明确提示用户，并告知该数据的采集目的和影响。

3.3.3 数据存储

在汽车产品的数据安全管理中，数据存储是基础环节。敏感个人信息（如人脸识别和指纹信息）必须进行强加密存储，建议采用多重认证机制保障访问安全。对于影响行车安全（如车辆配置参数）的非敏感个人信息，可以允许明文存储，但需要实施访问权限控制，以防止未经授权的访问

存储机制应采用经过验证的密码算法，以确保在个人数据传输至非车载系统时，仅授权的流程及个人才能修改或披露数据。同时，对存储数据进行分类管理，包括用户敏感个人信息、诊断数据、运行数据和密钥等。用户敏感个人信息应采用加密技术进行存储，具备有效的访问授权机制；而运行数据与诊断数据则需采取防篡改措施，以实现完整性校验，确保数据在存储过程中的安全性与可靠性。

针对敏感个人信息的存储要求，应按照国家标准执行，采用国密 SM4 或 AES 等强密码算法，并严格按照相关规范进行密钥的全生命周期管理。重要数据需实施数据脱敏处理，并采取分片存储策略，确保安全性。

3.3.4 数据传输

所有车载系统和外部设备的通信，使用密码算法进行加密，确保数据在传输过程中的机密性和完整性。

3.3.5 数据清理与销毁要求

数据的清理与销毁是数据管理的重要内容，确保在不再需要使用数据时，安全地销毁相关信息，防止被滥用。数据删除需遵循国家标准，例如采用符合 GB/T 29186-2012 的物理销毁或逻辑擦除方法，且必须禁止简单的格式化处理。对退役存储设备的销毁，需通过粉碎或

高温熔解等方式，确保数据无法恢复。

在数据清理过程中，必须建立机制以确保个人数据的永久删除，授权用户应负责确保数据按照 OEM 的数据保留政策被安全删除，并应使用最佳可用技术执行安全擦除。此外，远程和本地的数据清除机制应得到支持，包括数据重置、格式化与擦除，从而确保在设备退役或流转之前，敏感个人信息得到彻底销毁，并实施密钥注销以避免恢复。

在数据销毁的技术要求上，应制定详细的程序，确保敏感个人信息、重要数据和一般数据的销毁方法与验证措施，做到层次分明，确保信息安全。

3.3.6 关键数据保护

关键数据的保护对于汽车安全至关重要。应遵循最小化原则，仅采集业务功能所必需的数据，禁止收集不必要的信息。同时，关键数据（如安全气囊展开阈值等）需实施完整性监控，通过添加校验码实现实时检测，避免数据篡改。访问控制策略应确保关键数据仅向功能相关的电子控制单元（ECU）授权，禁止其他模块（如娱乐系统）未经授权的访问。

在处理用户个人信息时，也必须遵循最小必要原则，避免多余的个人数据采集。对打印生成的日志要求与业务情况结合，以确保敏感个人信息仅在用户同意的基础上被处理，并采取数据替换、随机化、去标识化等措施，以防止未授权访问和篡改的风险。对存储关键数据的方案，应采取加密措施，并设立严格的访问控制制度，以防止数据泄露和被篡改。

所有关键数据在传输、处理、存储过程中应实施全链路加密，确保数据在整个生命周期中的安全性和可控性。此外，数据采集系统需具备完整性检测与访问记录留存功能，以便于后续审计与风险评估。

3.3.7 数据跨境

在数据跨境传输方面，必须遵循国家网络安全法规，确保数据的安全与合规。所有数据出境前，需通过主管部门的安全评估，并在加密传输时使用国际通用或国密算法，确保数据

在传输过程中的机密性和完整性。对于跨境存储的数据，务必符合《数据安全法》的相关要求，必要时保留境内的数据备份和访问日志，以应对潜在的法律责任和数据泄露风险。

在进行个人数据跨境传输时，需事先准备全面的日志清单，并对数据进行脱敏处理，确保传输的数据不会对用户隐私造成影响。所有相关的跨境数据处理需在遵循法律法规的框架内进行，并与接收方共同确定数据传输的安全方式，以保障数据的可控性和可追溯性。

4 智能网联汽车供应链网络安全验收测评

4.1 汽车网络安全体系评估

4.1.1 网络安全管理体系

4.1.1.1 供应商网络安全管理体系建设

（1）测评目的

验证供应商建立并实施网络安全管理体系，并验证其符合性。

（2）测评方法

- 审查供应商的网络安全管理文件，包括网络安全管理手册、工作流程和制度等，确认是否建立了完善的管理体系。
- 核实供应商是否已取得相关机构的网络安全管理体系认证证书或评估报告。

（3）评判准则

供应商必须通过认证并拥有符合供应链网络安全相关的网络安全管理体系，且管理体系能够有效执行。

4.1.1.2 供应商网络安全绩效评估机制

（1）测评目的

评估供应商是否建立并有效执行了网络安全绩效评估机制，确保网络安全活动持续改进。

（2）测评方法

- 核查供应商的网络安全绩效评估计划，确认是否有定期评估机制（如月度或年度评估），并检查评估内容是否包括网络安全开发活动的各个环节。

- 审核评估结果，验证其是否采取了有效的改进措施，并已落实到实际操作中。

（3）评判准则

评估机制应覆盖供应商的开发过程及运营阶段，且评估内容要全面，包括安全性、合规性与技术能力等。

注：对于不涉及汽车网络安全的产品或服务供应商，审核验证时应确认其供应范围确实不涉及网络安全要素，此类供应商可免除特定网络安全要求。

4.1.2 网络安全技术能力

4.1.2.1 供应商资质与能力评估

（1）测评目的

确认供应商是否具备满足网络安全开发要求的技术能力和管理能力。

（2）测评方法

- 对零部件供应商，验证其是否在 RFQ（请求报价）文件中列明并传达完整的网络安全要求，且确保该文件只发放给已通过资质验证的合格供应商。

- 审核供应商的网络安全能力评价报告，确保其能力达到行业要求的准入门槛。

- 确认定点供应商是否已依据网络安全开发活动签署相应的网络安全接口协议（CIA），并审核协议内容的完整性与合规性。

（3）评判准则

供应商必须具备相应的资质，并确保网络安全接口协议涵盖了双方的责任、接口要求、里程碑节点等。

4.1.2.2 威胁分析与风险评估（TARA）

（1）测评目的

验证供应商是否已实施威胁分析与风险评估（TARA），识别产品潜在威胁，并制定有效的缓解措施。

（2）测评方法

- 审查供应商提供的 TARA 报告，确认是否进行了完整的威胁场景分析、攻击路径识别、攻击可行性分析等。
- 核实供应商是否已对产品进行系统性的漏洞管理，确保能够及时发现并修复安全漏洞。

（3）评判准则

供应商应能提供基于 TARA 的威胁识别报告，且必须有针对性的漏洞修复计划和实际操作流程。

4.1.2.3 关键资产管理与风险处置

（1）测评目的

验证供应商是否能够有效识别并管理关键资产，并对其潜在风险进行有效处置。

（2）测评方法

- 审查供应商的关键资产清单，确保其覆盖了所有涉及安全的资产，如 ECU 固件、OTA 升级包和用户数据等。

- 审核供应商的风险评估与处置流程，确保其针对不同类型的风险有明确的缓解措施和处理方案。

（3）评判准则

供应商必须建立完整的关键资产清单，并具备多层次的风险处置机制，确保安全事件得到及时有效的处理。

4.2 汽车数据安全体系评估

4.2.1 数据安全管理体系

4.2.1.1 数据安全管理岗位与组织建设

（1）测评目的

确保供应商已建立专职或兼职的数据安全管理岗位，并有足够的人员和团队支持数据安全工作。

（2）测评方法

- 检查供应商是否建立了专职或兼职的数据安全管理岗位、团队或人员，其工作职责是否通过规范要求或其他手段得到确认和保障。
- 审核供应商是否有关键数据安全领域的制度规范和流程，并检查其在组织机构内的落地执行情况。
- 评估执行数据安全工作的人员是否经过专业的技能和安全意识教育培训。
- 检查供应商对合作方主体数据安全相关资质及内部管理制度流程的审核机制，以及对合作项目涉及的数据采集、存储、传输、共享、使用、销毁等维度的相关能力验证机制。

（3）评判准则

供应商必须建立明确的数据安全管理岗位，且岗位职责和人员安排需符合数据安全管理要求。

4.2.2 数据安全技术能力

4.2.2.1 数据安全能力评估与合规性

（1）测评目的

确保供应商已通过数据安全能力评估，具备足够的技术能力和合规性来处理汽车数据。

（2）测评方法

- 审核供应商是否通过数据安全能力评价表评估，验证其管理体系符合性及数据安全能力水平，确保满足准入门槛要求。
- 验证定点供应商是否已依据不同数据处理活动特性签署相应的数据处理协议，审核协议内容是否明确双方数据安全责任与义务。
- 针对具体委外项目，审核验证供应商是否具备相应的数据安全技术能力，并确认技术协议是否完成签署且内容符合数据安全要求。

针对涉及数据跨境的供应商：

- 验证供应商是否依照现行监管要求完成数据出境安全评估申报、合同备案等工作，审核相关文档的完整性与合规性。
- 审核验证供应商是否建立并实施有效的数据出境监测技术机制，包括日志审计、风险事件监测等手段，确保能够对跨境数据流动进行持续安全监控。

- 验证供应商是否建立严格的境外账号管理与数据访问控制机制，审核相关权限设置、访问记录及审计措施是否满足数据安全要求。

（3）评判准则

供应商必须满足数据安全能力评估的准入要求，并对跨境数据处理进行安全评估与合规性审核。

4.2.2.2 数据分类分级与脱敏

（1）测评目的

验证供应商是否能够有效分类分级敏感个人信息，并确保在处理敏感个人信息时采取了有效的脱敏措施。

（2）测评方法

- 审查供应商的数据分类分级清单，确认其对数据进行了合适的分类，并对不同类别的数据采取了相应的保护措施。
- 核查供应商是否定期验证数据脱敏效果，并确保脱敏措施在所有处理场景中有效。

（3）评判准则

供应商必须实施数据分类分级管理，且对敏感个人信息的脱敏措施要经过有效验证。

4.2.2.3 数据防泄露与监控

（1）测评目的

确保供应商能够防止数据泄露，并能对数据传输、存储等环节进行持续监控。

（2）测评方法

- 审查供应商的防泄露机制，确保其能够实时监控数据传输、邮件、USB 等渠道，防止数据泄露。
- 核查供应商是否采用了有效的技术手段，如数据加密、访问控制等，来保障数据安全。
- 检查供应商是否规划建设具有自动化操作审计能力的平台系统，具备数据操作权限配置、异常操作告警与处置等核心功能。
- 检查供应商的系统工具是否符合数据安全成熟度模型特定等级的技术能力要求，可采信第三方的测试报告。

评判准则：供应商必须具备有效的数据防泄漏能力，并对关键数据的传输与存储进行全方位监控。

4.3 技术要求测试评价

4.3.1 基本技术要求验证

4.3.1.1 密码模块

（1）测评目的

验证供应商所使用的密码模块是否符合国际和国内的安全标准。

（2）测评方法

- 使用密码算法验证程序对供应商的密码模块进行严格的测试，验证其是否符合常见的国际和国内安全标准，并确保无已知漏洞或弱密码算法。

- 对硬件密码模块进行物理安全测试，验证其物理防篡改能力，确保能够有效防止物理攻击，包括但不限于物理入侵检测、反侧信道攻击、抗暴力攻击能力等。

- 测试硬件模块是否具备环境异常检测能力，以确保其在温度、电压、电磁干扰等环境异常下的安全性。

- 核查供应商是否使用行业标准的密码算法进行数据保护，确保加密强度符合数据保护的需求。

（3）评判准则

密码模块应通过所有测试用例，且无已知漏洞，采用的密码算法需符合国际及国内标准，并满足相应的安全性要求。

4.3.1.2 软件物料清单（SBOM）

（1）测评目的

确保供应商的软件系统中，所有的第三方组件和开源库均已明确列出，且无未经授权的组件，以防止潜在的安全风险。

（2）测评方法

- 利用软件成分分析工具对供应商的软件系统进行扫描，生成软件成分图谱，清晰列出所有使用的第三方组件和开源库。

- 核查图谱中是否包含未经授权的组件，检查是否使用了过期、存在已知漏洞的第三方组件。

（3）评判准则

软件成分图谱应清晰列出所有第三方组件和开源库，且无未经授权的组件，并确保所有

组件是安全的。

4.3.1.3 第三方组件安全

（1）测评目的

确保供应商所使用的所有第三方组件不包含 6 个月前公布且未经处置的高危及以上漏洞。

（2）测评方法

- 通过漏洞扫描、静态代码分析等方式，对供应商所使用的所有第三方组件进行检查，确认所有第三方组件无 6 个月前公布且未经处置的高危及以上漏洞。
- 对检查到的高危及以上漏洞进行分析，并尝试利用该漏洞。
- 查看检测到的漏洞是否具有相应的漏洞修复措施，并验证其修复的有效性。

（3）评判准则

所有第三方组件必须无 6 个月前公布且未经处置的高危及以上漏洞，且未发现任何未经处置的已知漏洞。

4.3.1.4 访问控制模块

（1）测评目的

验证供应商的访问控制模块是否实施了最小权限原则，防止未经授权的访问。

（2）测评方法

- 使用测试工具对访问控制模块进行权限测试，确保所有权限设置符合最小权限原则。

- 核查是否存在未授权访问路径，验证权限配置是否按需执行。

（3）评判准则

访问控制模块应严格实施最小权限原则，且不应存在任何未授权访问路径。

4.3.1.5 敏感个人信息存储

（1）测评目的

验证供应商是否采取了符合标准的数据存储机制来保护敏感信息，确保敏感个人信息的安全性。

（2）测评方法

- 对汽车供应商提供的产品进行敏感个人信息扫描，检查是否能够发现敏感个人信息。
- 核查敏感个人信息的存储方式，确认是否采用安全的密码算法对敏感个人信息进行加密存储。
- 检查是否在数据存储过程中实施了严格的访问控制措施，确保只有授权人员可以访问敏感个人信息。

（3）评判准则

敏感个人信息必须采用强密码算法存储，且访问控制机制应符合行业安全标准，确保数据存储安全。

4.3.1.6 硬件安全

（1）测评目的

验证供应商的硬件是否具备足够的安全性，确保硬件本身的安全防护措施能够有效抵御

物理攻击和其他潜在的安全风险。

（2）测评方法

- 审查供应商硬件的安全设计，包括硬件加密模块（如 HSM 等）的实施情况、外部接口数量及类型等，确保硬件具备保护关键数据和密钥的能力。
- 检查硬件是否具备防篡改功能，如是否支持安全引导、硬件级加密、物理防护措施等，确保在遭遇物理攻击时数据不被泄露。
- 核查硬件平台是否实现了安全启动机制，确保设备仅启动由授权签名的固件或操作系统。
- 测试硬件是否通过了相关认证，如 FIPS 认证、CC 认证或国密认证的加密库。
- 对专用的硬件安全芯片进行实际的物理攻击测试，如侧信道攻击、逆向工程等，验证硬件在物理攻击下的安全性。

（3）评判准则

硬件平台应具备抗物理攻击的能力，如防篡改、防逆向、支持安全启动等功能。

4.3.1.7 云服务安全

（1）测评目的

验证云服务环境中是否采取了足够的安全控制措施，包括 API 调用频率限制、认证机制以及零信任架构的实施，以确保防止过度请求、DoS 攻击及未经授权的访问。

（2）测评方法

- 对云服务的 API 接口进行压力测试，验证是否实施了频率限制。

- 对 API 调用进行认证机制的验证，确保 API 访问需要有效的身份验证。
- 评估云服务架构是否采用了零信任架构，确保所有网络访问都经过身份验证和权限授权。
- 对服务的 SLA 进行审查，确认云服务的可用性是否符合 99.99%的要求。

（3）评判准则

API 调用必须实施频率限制，并通过认证机制进行身份验证。云服务必须实施零信任架构，确保访问过程中的身份验证和授权。云服务 SLA 应达到 99.99%及以上，确保高可用性。

4.3.1.8 软件开发安全

（1）测评目的

验证软件开发过程中是否贯彻了安全生命周期管理，确保安全需求在开发阶段得到有效识别与管理，且代码在发布前进行严格的安全测试。

（2）测评方法

- 审查软件开发文档，确保包括需求、设计、实施、验证和发布等活动中嵌入了安全要求。
- 使用静态应用安全测试（SAST）和动态应用安全测试（DAST）工具对提供的代码进行自动化安全扫描。
- 对高危及以上漏洞进行验证，确保在 72 小时内进行修复并更新。
- 检查信息安全核心 ECU 的软件模块是否执行了安全开发生命周期（SDL），并进行相关工具的扫描结果验证。

（3）评判准则

软件开发过程中必须严格遵循安全开发生命周期（SDL），并通过自动化工具（如 SAST、DAST）进行代码安全检测。

高危及以上漏洞必须在 72 小时内修复，并确保修复完成后进行再次验证。

4.3.1.9 安全架构设计

（1）测评目的

验证车辆、云端和通信链路的安全架构是否完善，并确保安全边界、信任根和关键防护节点的定义是否清晰。

（2）测评方法

- 审查安全架构设计文档，确认是否涵盖车辆端、云端及通信链路的安全措施。
- 检查系统设计是否遵循了安全分区原则，是否进行了功能隔离。
- 评估架构设计中的纵深防御策略，确保多层安全防护有效实施。

（3）评判准则

安全架构必须覆盖车辆、云端和通信链路的安全防护。

必须遵循安全分区原则，系统设计中必须实现功能隔离和纵深防御。

4.3.1.10 安全启动与可信执行

（1）测评目的

验证核心控制单元是否具备安全启动机制，并确保可信执行环境的实施，以防止篡改和伪造。

（2）测评方法

- 对核心控制单元进行测试，检查是否具有有效的安全启动机制。
- 评估可信执行环境（TEE）或硬件信任根的实现情况，确保固件和软件加载的完整性与真实性。
- 验证固件更新流程，确保在固件加载过程中没有被篡改或伪造。

（3）评判准则

核心控制单元必须具备安全启动机制，确保固件加载的完整性和真实性。

必须实施可信执行环境（TEE）或硬件信任根防止篡改。

4.3.1.11 通信与接口安全

（1）测评目的

验证外部通信能力的部件是否采用了安全通信协议，防止重放、劫持及中间人攻击，确保物理接口的访问控制措施得当。

（2）测评方法

- 对具有外部通信能力的部件进行测试，确保采用了安全的通信协议（如 TLS、SSL 等）。
- 检查是否有防护措施防止重放攻击、劫持和中间人攻击。
- 对物理接口（如 JTAG、UART）进行安全审计，确保它们受到访问控制或限制管理。

（3）评判准则

所有外部通信接口必须采用安全通信协议，防止重放、劫持和中间人攻击。

物理接口必须具备访问控制或防护措施，确保调试接口受到限制管理。

4.3.1.12 安全事件日志与审计

（1）测评目的

验证关键系统与服务是否记录了安全事件日志，确保日志内容可追溯、不可篡改，并定期审计与留存。

（2）测评方法

- 审查系统日志记录策略，确保关键系统和服务生成安全事件日志。
- 检查日志是否具备不可篡改性，并确认是否有有效的审计机制。
- 对日志内容进行抽样审计，确保定期存储并符合安全事件处理的要求。

（3）评判准则

所有关键系统和服务必须生成安全事件日志，且日志内容不可篡改、可追溯。

必须实施定期审计和存储，确保日志符合审计要求。

4.3.1.13 OTA 软件升级

（1）测评目的

验证 OTA 升级包签名机制的有效性与合规性，确保升级包均采用车辆制造商密钥签名，保障升级包的完整性与来源可信性；对需采用双重签名机制的场景，验证供应商与车辆制造商双方密钥签名的完整性及有效性，防范恶意篡改或非法来源升级包的安装风险。

（2）测评方法

- 抽取待测试 OTA 升级包样本，通过专用签名验证工具核查升级包是否携带车辆制造商有效签名，验证签名信息与制造商公钥的匹配性，确认签名未被篡改。

- 对需采用双重签名机制的场景，核查升级包是否同时携带供应商与车辆制造商的双重签名，分别验证两份签名的有效性及签名顺序的合规性。

- 模拟升级包被篡改、签名伪造、签名缺失等异常场景，测试车辆端升级验证模块对异常升级包的识别与拦截能力，验证签名验证机制的实操有效性。

- 审查签名密钥的生成、存储、使用及销毁全流程管理记录，确认密钥管理的安全性，避免因密钥泄露影响签名机制有效性。

（3）评判准则

所有 OTA 升级包必须采用车辆制造商密钥签名，签名信息完整、有效，可通过公钥验证匹配，确保升级包完整性无篡改、来源可信。

需采用双重签名机制的场景，升级包必须同时具备供应商与车辆制造商的有效签名，两份签名均需通过验证，签名实施流程符合既定制度要求。

车辆端需具备完善的升级包签名验证机制，能准确识别并拦截签名缺失、伪造、篡改及不匹配的升级包，禁止异常升级包进入安装流程。

OTA 升级包签名管理策略、实施流程及密钥全生命周期管理记录完整可追溯，符合供应链网络安全相关技术要求。

4.3.2 供应商网络安全验证

4.3.2.1 持续的网络安全活动

（1）测评目的

验证供应商是否定期开展网络安全活动，并保持有效的安全防护能力，确保其产品或系统在生命周期内处于持续的安全防护状态。

（2）测评方法

- 审查供应商的网络安全活动记录，包括安全审计、漏洞扫描、渗透测试、事件响应和修复等。
- 核查供应商是否有定期进行安全审计和漏洞扫描的计划，并确认这些活动是否得到了持续实施。
- 核查供应商是否有针对新兴威胁和攻击的响应机制，并确保其能够迅速更新安全防护措施。
- 通过审查网络安全测评报告，验证供应商是否具备完善的网络安全监测系统，能够实时监控安全事件并及时响应。

（3）评判准则

供应商应有完整的网络安全活动记录，并定期进行安全审计和漏洞扫描。供应商的安全响应机制应及时有效，确保网络安全事件能够在第一时间得到处理。

4.3.2.2 CIA 与网络安全档案传递

（1）测评目的

本测试验证的目的是确保网络安全责任在供应链各层级之间的可传递性与可验证性，验证供方提供的网络安全接口协议和保证文档是否符合双方约定的安全要求。

（2）测评方法

- 对供方提交的网络安全接口协议进行全面审查，验证协议中是否明确规定了安全边界的定义和保护范围、数据交互的方式流程及其安全性、密钥管理策略、双方在安全事件中的责任与流程分工、保协议内容与 CIA 要求一致性等。

- 对网络安全档案进行完整性检查，并验证其中的安全措施是否有效，评估风险分析和防护措施的实际可行性。

- 针对供方提交的漏洞扫描报告与渗透测试报告，选择其中的关键漏洞和风险点进行复测，验证整改效果，并确认整改记录的真实性与完整性。如果存在尚未解决的安全隐患，应核查整改后的结果与确认报告是否真实有效。

- 检查所有网络安全接口协议和网络安全档案是否在规定的周期内被适当存档，并确保其能满足法规审计及后期事件追溯的要求。对文档存档的方式和存储位置进行审查，验证是否能够通过适当的渠道进行访问和追溯。

（3）评判准则

网络安全接口协议必须详细定义安全边界、数据交互方式、加密和认证机制、密钥管理策略以及安全事件处理流程。协议内容应严格遵守双方 CIA 要求，并与法规要求保持一致。若协议中存在模糊或不明确的条款，则不符合评判标准。

网络安全档案必须包含完整的内容，并提供详尽的风险分析、安全设计、漏洞修复记录等信息。文档中的信息应真实、完整、无遗漏，并能清楚证明产品或服务符合约定的网络安全要求。若任何文档存在信息缺失或不真实的情况，则不能通过验证。

供方提交的漏洞修复材料应能够证明已采取有效的技术措施来修复漏洞，整改后不再出

现相同或类似的安全隐患。整改效果应经过重新验证，并且修复过程应有详细记录。未能在规定时间内有效整改的漏洞将被视为不符合要求。

所有文档和协议必须满足法规审计和后期事件追溯的要求。文档应存档并具备良好的可追溯性，能够在需要时通过合法渠道调取。如果文档无法满足这些要求，则视为不合格。

4.3.2.3 网络安全事件处理

（1）测评目的

验证供应商是否具备应急响应机制，能够及时有效地处理网络安全事件，确保系统或产品在面对攻击或威胁时能够迅速恢复。

（2）测评方法

- 审查供应商的网络安全事件响应计划，确认其是否具备明确的事件响应流程和责任分配。
- 检查供应商的历史事件记录，评估其在面对过去安全事件时的响应效果，确认是否及时发现和修复了问题。
- 模拟安全事件，测试供应商的应急响应能力，确保其能够迅速采取措施并有效隔离、缓解威胁。

（3）评判准则

供应商应有明确的网络安全事件响应计划，且历史事件处理及时、有效。应急响应机制应具备快速启动和执行的能力，确保对安全事件的处理及时而有效。

4.3.2.4 网络安全风险

（1）测评目的

验证供应商是否有效识别和管理网络安全风险，确保其能够及时发现潜在威胁并采取措施防范，保障系统的长期安全性。

（2）测评方法

- 审查供应商的网络安全风险管理策略和流程，确保其能够识别、评估和管理来自各方面的网络安全风险。
- 核查供应商是否定期进行网络安全风险评估，包括威胁建模、攻击路径分析等，并验证评估结果是否得到充分应用。
- 核查供应商是否采用了风险分类与优先级管理方法，将不同风险按严重性分级，并根据风险等级制定相应的防护措施。
- 检查供应商是否针对关键资产（如网络设备、服务器、重要数据）进行了定期的风险评估，并确保采取了有效的安全加固措施。
- 核实供应商是否建立了风险缓解策略，确保在风险识别后采取相应的技术措施和管理措施来降低风险。
- 核查供应商是否建立了风险监控和追踪机制，能够在系统运营过程中持续跟踪和处理新出现的安全风险。

（3）评判准则

供应商必须建立有效的网络安全风险管理机制，确保能及时识别、评估和分类网络安全风险。对于高风险，供应商应制定并落实有效的防护和缓解措施，并能够持续监控和更新风险管理策略。

4.3.2.5 网络安全漏洞

（1）测评目的

确保供应商能够及时发现并修复网络安全漏洞，防止漏洞被攻击者利用，威胁系统或产品的安全性。

（2）测评方法

- 审查供应商的漏洞管理流程，验证其是否具备漏洞发现、评估、修复和验证的全流程。
- 使用漏洞扫描工具对供应商的产品或系统进行全面扫描，检查是否存在 6 个月前公布且未经处置的高危及以上漏洞。
- 核查供应商的漏洞修复计划，确认漏洞修复是否在规定的时间内完成，且修复措施得到验证。
- 验证供应商是否有漏洞上报机制，确保发现的漏洞能够及时上报并采取补救措施。

（3）评判准则

供应商应能够及时发现并修复高危及以上漏洞，漏洞修复应在规定的时间内完成，并经过验证。漏洞管理机制应完善，确保所有漏洞都能得到及时处理。

4.3.2.6 网络安全测试

（1）测评目的

验证供应商是否定期进行网络安全测试，确保其系统在面对各种攻击时能够有效防御并保障信息安全。

（2）测评方法

- 审查供应商的网络安全测试计划和执行记录，确认其是否定期进行网络安全测试，

如渗透测试、漏洞扫描、配置审计等。

- 核查供应商使用的安全测试工具和方法，确保测试涵盖了常见的网络安全攻击场景。验证供应商是否使用了自动化工具进行漏洞扫描，并定期对其系统进行全面的渗透测试，发现并修复潜在漏洞。

- 审查供应商的安全测试报告，确认测试中发现的漏洞是否得到了及时修复，且修复措施是否经过验证。

- 核查供应商是否针对不同的网络安全测试结果，采取了针对性的安全加固措施，特别是对于高危及以上漏洞的修复是否迅速有效。

（3）评判准则

供应商应定期进行网络安全测试，并能够提供全面的测试计划和执行记录。测试应覆盖主要攻击场景，且发现的漏洞必须在规定时间内得到有效修复。安全加固措施应针对测试结果采取，确保漏洞修复措施有效执行。

4.3.3 供应商数据安全验证

4.3.3.1 汽车数据存储通用要求

（1）测评目的

通过测试验证，确保车辆数据处理者严格遵守隐私保护法律法规，最大程度降低个人信息泄露风险，并保证用户的隐私权益得到有效保护。

（2）测评方法

- 对汽车数据处理者提供的相关文档进行审核，检查数据收集和处理的目的是否明确且合理，是否与汽车功能及服务直接相关。验证是否在收集个人信息前获得用户的明确同意，确保所有的数据收集行为都符合“知情同意”原则。

- 验证所收集的数据是否仅限于实现特定功能和服务所必需的最低限度，确保不收集无关数据。

- 对涉及生物识别技术（如指纹、声纹、面部识别、心律等）的数据收集行为进行审查，确保这些数据的收集具有充分的目的和合法的依据，并符合隐私保护法律要求。验证生物识别数据在收集、存储、传输过程中的安全性措施，包括加密存储、传输通道的保护等，确保生物识别数据不会被泄露、篡改或非法访问

- 检查在数据处理前是否对所有重要数据（如个人身份信息、车辆位置数据等）进行了有效的脱敏处理。

- 检查敏感个人信息的收集流程，确保对敏感个人信息的收集采取了严格的控制措施，避免不必要的收集和滥用。对数据存储、访问控制和传输安全等方面进行测试，确保敏感个人信息的存储过程符合安全性要求，且采取了适当的防护措施（如加密、访问权限管理等）来防止数据泄漏或被非法访问。

（3）评判准则

数据收集和处理目的必须明确、合法，并直接与汽车功能或服务相关。数据处理者必须遵守隐私保护法律法规，尤其是针对生物识别信息的收集必须符合法律规定并获得用户的明确同意。

个人信息的采集量必须严格控制，并确保所收集的数据仅限于实现车辆功能所必需的最小数据量。

涉及生物识别技术的数据收集必须符合隐私保护法律要求，且收集前必须获得用户明确的同意。

所有重要的敏感个人信息必须进行脱敏处理，以确保即使数据被非法访问，用户的个人信息也无法被识别或恢复。

敏感个人信息的收集、存储和传输过程中必须采取适当的安全措施，包括加密、访问控制等。

4.3.3.2 数据收集

（1）测评目的

确保汽车数据处理者在收集数据时，数据采集的精度、覆盖范围和分辨率符合功能需求，同时确保车机系统在收集个人数据时能够遵守隐私保护原则，提供充分的用户授权机制。

（2）测评方法

- 使用标定工具对摄像头和雷达的精度进行定量验证，确保其数据采集的精度与车载系统的功能要求匹配。
- 验证车机系统中个人数据授权开关的功能，确保其默认状态为关闭，且用户可以自主选择是否开启驾驶行为分析数据采集。验证系统是否记录用户授权选择，并且仅在用户授权的情况下进行数据采集与分析。
- 验对车载系统的界面和提示信息进行测试，确保在采集敏感个人信息（如位置、指纹等）时，系统会明确提示用户并告知数据采集的目的和影响。验证用户在接收到敏感信息采集提示后是否能够清楚理解采集的目的及影响，并根据提示做出相应选择。
- 在未获得用户授权的情况下，测试系统是否会严格阻止相关数据的采集与处理。
- 验证数据存储过程中的脱敏处理应用场景、有效性。
- 验证数据备份方案和有效性，实施备份数据的完整性校验机制。
- 验证数据存储介质的管理机制和安全措施。

（3）评判准则

车载摄像头、雷达等设备的采集精度和覆盖范围应满足车辆设计功能的需求

车机系统中的个人数据授权开关必须默认设置为关闭，且用户应具有明确的选择权来开启或关闭数据采集功能。

在敏感个人信息采集过程中，系统应明确告知用户采集目的、用途及影响，且提示信息应清晰、易懂且具备足够的细节说明。

系统应严格遵守用户授权设置，确保在未获得用户授权的情况下不会收集相关数据。

4.3.3.3 数据存储

（1）测评目的

确保供应商采取了足够的保护措施，确保敏感个人信息在存储过程中得到强加密保护，防止数据泄露或被非法访问。

（2）测评方法

- 验证是否制定数据分类分级管理规范，对数据进行分类分级管理，并对个人信息等特殊类别数据进行识别和分类。
- 验证是否根据数据分类分级结果，对数据分域开展分级差异化存储管控的情况，是否明确不同数据的存储期限、方式和安全措施等情况。
- 验证是否采用安全的密码算法对个人信息和重要数据进行加密存储。
- 验证数据库账号权限管理、访问控制、日志管理、加密管理、版本升级等方面的实施情况。
- 验证数据存储过程中的脱敏处理应用场景、有效性。

- 验证数据备份方案和有效性，实施备份数据的完整性校验机制。
- 验证数据存储介质的管理机制和安全措施。

（3）评判准则

敏感个人信息必须采用强密码算法存储，并且密钥管理流程应符合行业最佳实践。数据存储过程中的访问控制应严格，确保数据的安全性。

4.3.3.4 数据传输

（1）测评目的

验证确保车载系统与外部设备之间的通信过程是否通过密码算法加密，确保数据在传输过程中的机密性与完整性。验证 OTA 升级包的双重签名机制是否得到有效实现，确保升级包在传输过程中未被篡改，且来源可信。

（2）测评方法

- 对车载系统与外部设备间的数据通信协议进行审查，确认是否使用了强加密算法，确保传输过程中数据的机密性和完整性。捕获通信数据并验证是否被加密。
- 使用数据篡改工具进行模拟篡改攻击，测试加密通信是否能够有效检测并阻止数据篡改。
- 验证 OTA 升级包在生成、传输和接收过程中是否采用了双重签名机制，即供应商和车辆制造商双方使用各自的密钥进行签名。通过模拟 OTA 升级过程，提取并验证升级包中的双重签名是否正确、有效。
- 通过对 OTA 升级包进行篡改，测试系统是否能够检测到篡改并阻止升级过程。
- 检查在加密通信或双重签名验证失败时，系统是否能够提供有效的错误处理和

恢复机制，确保不会因数据传输错误或篡改导致系统异常或安全漏洞。

（3）评判准则

车载系统与外部设备的通信必须使用强加密算法，确保数据在传输过程中无法被中间人窃取或篡改。

OTA 升级包必须经过供应商和车辆制造商双方的密钥签名，且升级包在传输和接收过程中能够通过双重签名验证。

OTA 升级包在传输过程中必须能够通过签名验证其完整性和来源可信性。抗篡改能力：系统必须能够检测传输过程中的数据篡改。

错误处理机制：当加密通信或签名验证失败时，系统必须能够提供适当的错误处理和恢复机制，防止系统因安全问题出现故障或被攻击。

4.3.3.5 数据清理与销毁

（1）测评目的

验证供应商是否有严格的数据清理和销毁流程，确保数据在生命周期结束时被彻底销毁，避免数据恢复或泄露。

（2）测评方法

- 验证是否建立数据清理与销毁安全策略和操作规程，是否明确数据销毁对象、原因、销毁方式和销毁要求。
- 验证数据存储期限是否明确，是否于存储期限到期后按期删除数据，如有不可删除的数据是否明确类型及原因。
- 验证数据清理与销毁的有效性、彻底性，是否实现多副本同步删除、缓存数据

删除。

- 验证存储介质销毁机制、销毁策略和操作规程的有效性和适用性。
- 验证被销毁的存储介质是否可能进行数据恢复。

（3）评判准则

数据清理和销毁应符合行业标准，且销毁过程应确保数据不可恢复。供应商应能够提供销毁验证报告，确保销毁过程可追溯且彻底。

4.3.3.6 关键数据保护

（1）测评目的

确保供应商能够有效保护关键数据，防止其在存储、传输过程中受到威胁或被篡改。

（2）测评方法

- 验证是否采用技术手段定期对数据资产进行扫描，是否具备发现识别个人信息、重要数据的能力。
- 验证针对不同类别的个人信息是否设立保存期限，是否针对超期个人信息采取删除或匿名化处理。
- 验证是否建立相关技术或管理措施确保个人生物识别信息与个人身份信息分开存储。
- 验证涉及座舱数据、位置轨迹数据、车外视频和车外图像数据，以及涉及个人信息主体超过 10 万人的个人信息，是否在中华人民共和国境内存储。
- 验证对于人脸车牌等车外个人信息，是否删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等方式脱敏。

- 验证是否在展示、委托处理、提供、公开等环节，对个人信息直接标识符进行去标识化处理。

- 验证在保存、传输等处理敏感个人信息和重要数据时，是否采用了安全措施如加密、安全存储、授权管理、安全审计、数据防泄漏等保护措施。

- 验证是否按照相关重要数据目录或规定，评估重要数据并进行重点保护。

（3）评判准则

关键数据应采用强加密存储，且应有严格的访问控制。数据完整性应通过哈希值、数字签名等方式进行保护。供应商应有完整的数据备份和恢复方案，确保数据操作安全性和合规性。

4.3.3.7 数据跨境

（1）测评目的

确保供应商在跨境数据处理时，符合数据保护法律和法规的要求，避免违反隐私保护相关规定。

（2）测评方法

- 审查供应商是否遵守《数据安全法》和《个人信息保护法》中的数据跨境规定，确保跨境数据的处理符合相关法律法规。

- 核查供应商是否进行数据出境安全评估，并能提供相关的合规文档，如数据跨境合规报告。

- 确认供应商是否在数据跨境过程中采取了合适的安全控制措施，如加密传输、访问控制等，确保数据安全。

- 核查供应商是否有定期的跨境数据监测和审计机制，确保跨境数据流动得到有效监控。

（3）评判准则

数据跨境操作必须符合相关法律法规，且供应商应能够提供完整的合规证明和合规评估报告。跨境数据传输应采取加密等安全措施，并实施持续监控。

5 小结

5.1 智能网联汽车供应链网络安全标准化可行性分析

随着智能网联汽车产业的迅猛发展，供应链的网络安全问题日益突出。智能网联汽车供应链不仅涵盖了大量的硬件和软件系统，还涉及复杂的数据传输与处理环节，这些因素使得供应链的网络安全面临着多层次、多维度的风险。在这种背景下，标准化工作对于提升供应链整体的网络安全性至关重要。通过标准化，可以规范各个环节的安全防护措施，保障信息的安全传输与处理，进而提高系统的整体安全性。

智能网联汽车供应链的网络安全问题并非单一的硬件或软件问题，而是涉及跨系统、跨设备的复杂安全挑战。尤其是车联网技术的广泛应用，使得网络安全防护的范围不再局限于传统的车载网络，而是扩展至整个供应链体系。因此，网络安全防护措施必须覆盖供应链的每个环节，并且根据不同的技术平台和设备需求制定相应的标准。例如，在汽车制造环节，如何保障零部件的网络安全性、如何防止车载设备被恶意软件攻击、如何确保车载系统与云平台之间的数据传输安全等问题，都需要通过标准化的方式进行统一规范。

目前，虽然已有一些针对智能网联汽车网络安全的标准，如 GB44495 和 ISO/SAE 21434 等，这些标准主要集中在整车安全领域，但对智能网联汽车的供应链网络安全缺少可以落地的切实指导。为了应对供应链全生命周期中的安全挑战，未来的标准化工作需要进一步整合跨企业、跨环节的需求，推动形成统一的网络安全框架。这不仅能帮助各参与方在安全防护上实现协同，也能避免因标准分散导致的漏洞和安全防护不均衡的问题。

标准化的实施将为智能网联汽车供应链网络安全提供重要保障。通过统一的标准，能够有效提升各环节之间的安全协同，确保信息的安全传输与存储，减少潜在的网络攻击风险。标准化的推进还能够为供应链中的各方提供明确的安全操作指南，降低各方实施网络安全防护措施的难度，促进技术的广泛应用和推广。

5.2 智能网联汽车供应链网络安全下一步工作计划

随着智能网联汽车的不断发展，车载人工智能技术的广泛应用为驾驶体验和车辆性能带来了显著提升。然而，车载人工智能的普及也带来了新的网络安全风险，尤其是在车辆的实时数据处理、自动驾驶系统、以及车载通信网络等方面，可能成为黑客攻击的潜在目标。为应对这一风险，需要深入研究车载人工智能技术在网络安全领域所带来的潜在威胁，识别车载 AI 系统可能暴露的安全漏洞，并评估这些漏洞可能对车辆和驾驶员安全造成的影响。从供应链网络安全的角度提出相应的防御措施和技术标准，以最大程度减少潜在的安全威胁。

在本研究报告的基础上结合实际应用需求和行业发展趋势，进一步推动智能网联汽车供应链网络安全的标准化进程。通过试点项目的实施和数据积累，完善技术方案与安全策略，为标准制定提供理论依据与实践支持，为行业提供可复制、可扩展的网络安全解决方案，从而推动智能网联汽车产业在供应链安全领域的健康发展。

推动标准的制定和推广，是提升智能网联汽车供应链网络安全整体水平的关键一步。标准不仅能够规范企业的安全操作流程，还能为政府监管提供依据，促进整个行业的合规性建设。该标准将涵盖从覆盖智能网联汽车全生命周期的网络安全管理与技术要求，从而有效减少供应链中的安全漏洞，提升行业整体的网络安全防护能力。