智能网联汽车生产企业及产品准入管理指南（试行）

（征求意见稿）

第一条 为加强道路机动车辆生产企业及产品准入管理，根据《中国人民共和国道路交通安全法》《中华人民共和国网络安全法》《道路机动车辆生产企业及产品准入管理办法》等规定，针对申请准入的具备有条件自动驾驶、高度自动驾驶功能的智能网联汽车生产企业及其产品，制定本指南。

第二条 智能网联汽车生产企业应满足企业安全保障能力要求（见附件 1），针对车辆的软件升级、网络安全、数据安全等建立管理制度和保障机制，建立健全企业安全监测服务平台，保证产品质量和生产一致性。

第三条 智能网联汽车生产企业应遵守网络安全法律法规规定，建立覆盖车辆全生命周期的网络安全防护体系，采取必要的技术措施和其他必要措施，有效应对网络安全事件，保护车辆及其联网设施免受攻击、侵入、干扰和破坏。

智能网联汽车生产企业应依法收集、使用和保护个人信息，实施数据分类分级管理，制定重要数据目录，不得泄露涉及国家安全的敏感信息。在中华人民共和国境内运营中收集和产生的个

人信息和重要数据应当按照有关规定在境内存储。因业务需要，确需向境外提供的，应向行业主管部门报备。

第四条 智能网联汽车生产企业应明确告知车辆设计运行条件、人机交互设备指示信息、驾驶员职责、驾驶自动化功能激活及退出方法、软件升级维护等信息，解决智能网联汽车与传统汽车在操作、使用等方面可能产生的预期差异问题。

第五条 智能网联汽车产品应明确驾驶自动化功能及其设计运行条件。设计运行条件应包括设计运行范围、车辆状态、驾乘人员状态及其他必要条件；设计运行范围应包括但不限于道路、交通、电磁环境、天气、光照等。

第六条 智能网联汽车产品应能自动探测驾驶自动化系统失效以及是否持续满足设计运行条件，并能采取风险减缓措施以达到最小风险状态。在自动驾驶模式下，智能网联汽车应能按照道路交通安全法律法规及有关部门的相关规定安全行驶。

第七条 智能网联汽车产品应具备人机交互功能，显示驾驶自动化系统运行状态，具备对驾驶员参与行为的监测能力。在动态驾驶任务需要驾驶员参与的情况下，应评估驾驶员执行相应驾驶任务的能力。车辆应能够依法依规合理使用灯光信号、声音等方式与其他道路使用者进行交互。

第八条 智能网联汽车产品应具有事件数据记录和自动驾驶数据存储功能，采集和记录的数据至少应包括驾驶自动化系统运行状态、驾驶员状态、行车环境信息、车辆控制信

息等，并应满足相关性能和安全性要求，保证车辆发生事故时设备记录数据的完整性。

第九条 智能网联汽车产品应满足功能安全、预期功能安全和网络安全等过程保障要求（见附件 2），以及模拟仿真、封闭场地、实际道路、网络安全、软件升级和数据存储等测试要求（见附件 3），避免车辆在设计运行条件内发生可预见且可预防的安全事故。

第十条 智能网联汽车生产企业及产品可参考本指南申请准入。工业和信息化部根据相关规定组织开展准入申请受理、技术审查、应用评估、监督检查等工作。

附件：1. 智能网联汽车生产企业安全保障能力要求

2. 智能网联汽车产品准入过程保障要求

3. 智能网联汽车产品准入测试要求

4. 名词解释

附件 1

智能网联汽车生产企业安全保障能力要求

企业应具备专职的功能安全、预期功能安全和网络安全保障团队，负责产品全生命周期的安全保障工作。具备工业和信息化部规定条件的企业集团可统一设立安全保障团队。企业安全保障能力要求包括功能安全及预期功能安全保障要求、网络安全保障要求和软件升级管理要求。

一、企业功能安全及预期功能安全保障要求至少包括:

（一）企业应满足汽车安全生命周期相关阶段的功能安全活动流程要求，符合汽车安全完整性等级对应流程的规定，避免不合理的风险。

（二）企业应满足功能安全管理要求，符合整体功能安全管理、产品开发安全管理、安全发布管理等规定。

（三）企业应满足生产、运行和服务阶段的功能安全要求，符合生产过程能力评估、控制措施、现场观察说明等规定。

（四）企业应满足支持过程要求，符合开发管理、安全要求的定义和管理、配置管理、变更管理、验证和确认、文档管理、软硬件组件鉴定、在用证明等方面的规定。

（五）企业应满足预期功能安全开发接口管理要求，符合预期功能安全管理职责和角色定义、供应商计划管理等规

定。

（六）企业应满足预期功能安全开发流程要求，符合设计定义、危害识别、功能不足识别、功能改进、验证及确认、安全发布、运行维护等规定，保障车辆不存在因预期功能的不足所导致的不合理风险。

二、企业网络安全保障要求至少包括:

（一）企业应建立健全网络安全责任制度，确定网络安全负责人，落实网络安全保护责任。

（二）在车辆安全生命周期内，企业应当同步规划、同步建设、同步运行网络安全技术措施。

（三）企业应制定网络安全防护制度，定期开展网络安全风险识别、分析和评估，管控生产过程网络安全风险，及时消除车辆及联网设施重大网络安全隐患。

（四）企业应建立网络安全监测预警机制，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于6个月。

（五）企业应建立网络安全应急响应机制，制定网络安全应急预案，及时处置安全威胁、网络攻击、网络侵入等安全风险。

（六）企业应建立产品安全漏洞管理机制，及时修补和合理修复安全漏洞，指导支持车辆用户采取防范措施。

（七）企业应建立完善数据安全管理制度，实施数据分

类分级管理，制定重要数据目录，强化数据访问权限管理和安全审计；采取有效技术措施，强化数据采集、传输、存储、使用等安全保护，及时处置数据泄露、滥用等安全事件。

（八）企业应建立车联网卡实名登记制度，如实登记购车用户身份信息，并会同基础电信企业落实车联网卡实名登记有关要求。

（九）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。

（十）企业应制定网络安全审计规范，并对网络安全管理和技术措施运行、网络安全风险管理和人员安全能力等开展审计。

（十一）企业应建立产品售后网络安全管理机制，包括售后服务、维修、报废阶段的网络安全保障措施。

（十二）企业应在关键流程变更、重特大网络安全事件发生后，及时更新完善网络安全管理规范、安全机制等。

（十三）企业应依法依规为维护国家安全、开展行业监管等提供技术支持和协助。

三、企业软件升级管理要求至少包括:

（一）企业应建立软件升级管理制度，至少包括软件开发管理、配置管理、质量管理、变更管理、发布管理、安全应急响应管理等。

（二）企业应制定软件升级从设计、开发、测试、发布、推送等过程的标准规范，并遵照执行。

（三）企业应能够识别、评估和记录软件升级对产品安全、环保、节能、防盗相关系统的功能和性能的影响。

（四）企业应对软件升级可能影响的功能和性能进行测试和验证，确保符合相关法规、标准和技术要求。

（五）企业应能够识别软件升级的目标车辆，评估软件升级与目标车辆的适应性，确保软件升级与目标车辆软硬件配置兼容。

（六）企业应能够唯一识别车辆初始和升级的软件版本，记录与保存软件升级包完整性验证数据以及相关的硬件配置信息。

（七）企业应记录与安全保存汽车产品初始软件版本和历次软件升级相关信息，应能支持汽车产品全生命周期的追溯需求和监督管理要求。

（八）企业应对 OTA（Over-The-Air，空中下载技术）升级服务平台采取必要的网络安全防护管理和技术措施，对升级的软件进行安全检测，保障 OTA 升级安全。

（九）企业应具备软件升级过程管理能力，履行用户告知义务，记录和保存升级过程相关信息。

附件 2

智能网联汽车产品准入过程保障要求

智能网联汽车产品准入过程保障要求包括整车尤其是驾驶自动化系统的功能安全过程保障要求、驾驶自动化系统预期功能安全过程保障要求和网络安全过程保障要求。

一、针对驾驶自动化功能的安全风险，整车尤其是驾驶自动化系统的功能安全过程保障要求至少包括:

（一）应定义驾驶自动化系统的功能概念，包括范围、要素、运行条件、架构及内外部接口示意图等。

（二）应识别可能造成人身安全伤害的整车功能失效，建立合理的功能安全场景，针对危害事件分析可控性、严重性、暴露率等参数，确认合理的汽车安全完整性等级及危害事件的安全目标。

（三）应按照整车功能安全开发的相关规定进行功能安全分析，明确功能安全要求。功能安全要求应考虑运行模式、故障容错时间间隔、安全状态、紧急运行时间间隔等，并分配给驾驶自动化系统的架构要素或外部措施。

（四）应定义驾驶自动化系统功能安全相关零部件的开发接口要求，明确角色和责任要求，确保在系统、硬件和软件各层级满足整车安全要求。

（五）应进行功能安全集成测试，通过基于需求的测试、

故障注入测试等方法，确保对整车和驾驶自动化系统的相关要求得到实施和满足。

（六）应满足功能安全确认要求，通过检查、测试等方式，确保安全目标在整车层面正确、完整并得到充分实现。

二、驾驶自动化系统预期功能安全过程保障要求至少包括:

（一）应满足预期功能安全规范和设计的要求，识别和评估预期功能可能造成的危害，制定合理的风险可接受准则。

（二）应识别和评估潜在功能不足和触发条件（含可合理预见的人员误用），并应用功能改进等措施减少预期功能安全相关的风险。

（三）应定义验证及确认策略，并进行预期功能安全的验证和确认，评估已知危害场景和未知危害场景下是否符合产品预期功能安全发布要求，并对发布后产品的预期功能安全风险进行合理管控。

（四）应定义驾驶自动化系统预期功能安全相关零部件的接口要求，确保零部件符合对应的预期功能安全设计开发、验证、确认等规定。

三、智能网联汽车产品网络安全过程保障要求至少包括:

（一）应开展网络安全风险评估，包括资产识别、威胁分析、攻击路径分析、潜在影响评估、风险分类应对措施。

（二）在概念设计阶段，应根据网络安全风险评估结果，

明确网络安全目标和要求，设计网络安全架构和功能。

（三）在产品开发阶段，应实现网络安全风险和脆弱性防范应对处置功能，满足整车网络安全目标和要求。

（四）在测试验证阶段，应开展整车网络安全测试验证，并提供测试验证情况说明（包括测试指标、测试方法、测试环境、测试结果等），确保所有已发现的安全风险和脆弱性被有效处置，以及网络安全目标和要求实现有效、合理、完整。

附件 3

智能网联汽车产品准入测试要求

产品准入测试要求是指申请准入的智能网联汽车产品应至少满足模拟仿真测试要求、封闭场地测试要求、实际道路测试要求、车辆网络安全测试要求、软件升级测试要求和数据存储测试要求。

一、驾驶自动化系统模拟仿真测试的要求至少包括:

（一）模拟仿真测试应能验证驾驶自动化系统在典型场景和连续场景下的安全性、道路交通规则符合性，满足相应的道路交通安全要求。典型场景应覆盖封闭场地测试所要求的测试场景及设计运行范围所要求的驾驶自动化功能场景;模拟仿真测试中连续场景应能反应实际道路测试的场景要素组合情况。

（二）应说明驾驶自动化系统的组成及工作原理、驾驶自动化功能及其设计运行条件、风险减缓策略、最小风险状态以及必要的安全风险提醒等。

（三）应说明模拟仿真测试的软硬件环境和工具链、驾驶自动化功能验证的场景库，以及使用的车辆动力学、传感器等模型及其关键参数。

（四）应能在多个相同场景下，通过封闭场地和实际道路测试，并与模拟仿真结果对比，验证模拟仿真测试的有效

范围。

（五）应提供模拟仿真测试过程中所涉及的测试类型、测试方法、评价方法、测试流程以及测试数据存储等说明。应保证模拟仿真测试结果的可追溯性。

（六）应覆盖产品设计运行条件内的道路、基础设施、交通环境等要素，构建典型场景，验证产品所声明的驾驶自动化功能是否符合安全要求。

（七）应定义设计运行条件内不同场景要素的参数组合，针对驾驶自动化功能建立可合理预见的测试场景库；通过连续自动化仿真测试，验证驾驶自动化系统是否符合功能安全和预期功能安全要求。

二、封闭场地测试的要求至少包括:

（一）应能通过封闭场地测试，验证车辆在封闭场地典型场景下的安全性。

（二）封闭场地测试应考虑驾驶自动化功能设计运行条件内的关键要素。场景应覆盖设计运行范围内所要求的行驶范围，并统筹考虑交通环境及附属设施情况。

（三）应对测试过程进行记录，对测试过程中所涉及的测试环境、测试人员、测试方法、测试规范、测试设备及测试流程的规范性负责，能有效保证测试结果的可追溯性、一致性和准确性。

（四）应能提供原始测试数据，应至少包含车辆位置信

息、测试车辆控制模式、车辆运动状态参数、驾驶员及人机交互状态、行车环境信息、车辆执行机构控制信息等内容，并对测试结果进行分析与评价。

三、实际道路测试的要求至少包括:

（一）应能通过实际公共道路连续场景测试，验证车辆在实际公共道路交通环境下的安全性。应通过封闭场地测试后才可进行实际道路测试。

（二）应当根据所声明的产品自动驾驶设计运行范围，选择匹配的公共道路开展车辆实际道路连续测试;基于测试时长、测试里程和自动驾驶功能响应及接管率，验证所声明的自动驾驶功能应对随机场景的能力,且应当满足产品的安全要求，并对测试结果进行分析及评价。

（三）应对测试过程进行记录，对实际道路测试过程中所涉及的测试环境、测试人员、测试方法、测试规范、测试设备以及测试流程的规范性负责，能够有效保证测试结果的可追溯性、一致性和准确性。

（四）应满足车辆测试远程监控与测试数据记录和存储要求。对每一辆测试车辆运行状态进行监控，记录测试车辆行驶轨迹、控制模式、车辆运动状态参数、驾驶员及人机交互状态、行车环境信息、车辆执行机构控制信息、接管信息等数据。数据上传要符合数据传输模式、格式等规定要求。

四、车辆网络安全测试要求至少包括:

（一）应能够防御信息传输安全威胁。包括虚假消息入侵、代码/数据未经授权修改、会话劫持或重放攻击、未经授权访问敏感数据、拒绝服务攻击、获取车辆特权控制、病毒及恶意消息等。

（二）应不存在已公布的网络安全漏洞，预装软件、补丁包/升级包不应存在恶意程序，不应存在未声明的功能和访问接口（含远程调试接口）。

（三）应能够抵御合法用户误操作引发的网络安全风险。

（四）应能够防御车辆外部连接的安全威胁。包括远程非法入侵控制车辆、第三方应用软件恶意代码入侵、外部接口（如 USB 接口、OBD 接口、无线接口等）入侵等。

（五）应能够防御非法盗取、破坏关键数据的威胁。包括提取软件代码、未经授权访问个人信息、提取密钥数据、非法/未经授权修改电子身份、篡改车辆行驶数据、未经授权更改系统诊断数据、未经授权删除/操作系统事件日志、未经授权访问系统关键参数数据等。

（六）应能够防御系统被物理非法操控的威胁。包括非法操作车辆硬件设备，如未经授权的硬件添加到车辆内部进行“中间人”攻击等。

（七）应能够防御数据丢失/车辆数据泄漏的威胁。包括车辆更换使用用户时的个人信息被泄露或破坏等。

五、软件升级测试的主要对象是智能网联汽车的车端软

件升级软件或系统，测试要求至少包括:

（一）车辆应确保在安全状态下进行软件升级，升级执行前应监测车辆状态是否符合软件升级条件，如车辆的运动状态、挡位状态等。

（二）车辆应具备对软件包进行真实性和完整性校验的能力，确保安全下载和执行有效的软件升级包。

（三）车辆应具备升级执行确认功能，升级执行前应提供软件包与待升级零部件的匹配校验功能。

（四）车辆应具备升级执行前提示软件升级的相关信息，包括升级的目的、功能升级描述、升级时车辆工况要求、升级包安装所需时长、升级过程中注意事项等信息。

（五）当升级执行可能影响车辆安全时，应通过技术手段，确保车辆处于可以安全执行升级的状态。

（六）车辆应具备升级完成后提示用户升级成功或失败功能。

（七）车辆应在升级失败或中断后，确保车辆处于安全状态。

六、数据存储测试应至少满足如下要求:

（一）自动驾驶数据记录系统应在驾驶自动化系统激活、驾驶自动化系统退出、驾驶自动化系统发出接管请求情况下进行记录，并可对驾驶自动化系统启动最小风险策略、驾驶自动化系统启动紧急策略、驾驶自动化系统退出紧急策略、

严重驾驶自动化系统故障、严重车辆故障等情况进行记录。记录内容应至少包括车辆和驾驶自动化系统基本信息、触发事件基本信息及事件发生原因并满足数据一致性试验要求；当车辆有碰撞风险和发生碰撞时，需增加记录车辆状态及动态信息、行车环境信息、人员信息及故障信息。

（二）应满足数据存储测试要求，包括：数据存储能力试验、存储覆盖试验、断电存储试验等。

（三）存储的数据应能被正确读取和解析，且不能被篡改。

附件 4

名词解释

一、智能网联汽车：搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与 X（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现安全、高效、舒适、节能行驶，并最终可实现替代人来操作的新一代汽车。通常也被称为自动驾驶汽车。

二、驾驶自动化系统：由实现驾驶自动化的硬件和软件所共同组成的系统。

三、设计运行范围：驾驶自动化系统设计时确定的适用于其功能运行的外部环境条件。

四、设计运行条件：驾驶自动化系统设计时确定的适用于其功能运行的各类条件的总称。

五、最小风险状态：车辆事故风险可接受的状态。

六、有条件自动驾驶：驾驶自动化系统在其设计运行条件下持续地执行全部动态驾驶任务，对于系统发出的介入请求，驾驶员应以适当的方式执行接管。

七、高度自动驾驶：驾驶自动化系统在其设计运行条件下持续地执行全部动态驾驶任务并自动执行最小风险策略，对于系统发出的介入请求，用户可不作响应，系统具备自动

达到最小风险状态的能力。

八、功能安全：不存在由电子电气系统的功能异常表现引起的危害而导致不合理的风险。

九、预期功能安全：没有因预期功能或其实现的不充分性导致的危害而引发的不合理风险。

十、网络安全：汽车的电子电气系统、组件和功能被保护，使其资产不受威胁的状态。

十一、软件升级：根据需要，将某版本的软件程序或配置参数更新到另一个版本并启用的过程。

十二、空中下载技术（Over-The-Air，简称 OTA）：通过无线传输数据的一种方法。