附件 1

智能网联汽车准入和上路通行试点实施指南

（试行）

针对智能网联汽车准入和上路通行试点工作，工业和信息化部、公安部、住房和城乡建设部、交通运输部研究制定了《智能网联汽车准入和上路通行试点实施指南（试行）》（以下简称《指南》），指导汽车生产企业和使用主体在车辆运行所在城市限定区域内有序开展试点工作。《指南》包括智能网联汽车准入、使用主体、上路通行、试点暂停与退出四个部分。

第一部分 智能网联汽车准入

第一章 智能网联汽车生产企业

一、设计验证能力

（一）企业应建立专门的智能网联汽车产品设计开发机构，统一负责产品设计和制造过程开发工作，配备与设计开发任务相适应的专业技术人员。专业技术人员至少包括自动驾驶系统的系统功能定义、系统架构设计、系统安全设计、软件开发、仿真分析验证、系统集成与调试、整车测试验证等方面的人员，以及专职的功能安全、预期功能安全、网络安全和数据安全、软件升级保障团队。对于企业集团，设计

开发机构可统一设立。

（二）应建立适用于本企业的自动驾驶系统开发工作流程，应包括参与部门及职责，输入输出物管理、评审、验证、确认等方面的内容。

（三）理解和掌握所生产的智能网联汽车产品开发方面的技术，至少包括:

1. 自动驾驶环境感知系统、智能决策系统、控制执行系统、其他电子电气系统的边界划分和接口定义;

2. 自动驾驶控制系统技术，包括自动驾驶控制策略，系统/部件软硬件的基础原理、结构、功能和性能要求，控制器软硬件设计、测试评价方法、标定、故障诊断和解决措施等。

（四）企业应建立与智能网联汽车产品相适应的产品信息数据库，数据库内容至少包括:

1. 申请车型使用的环境感知系统、智能决策系统、控制执行系统等的生产企业及性能参数信息;

2. 申请车型的自动驾驶系统及关联系统和总成/部件的图样、规格参数、技术要求、设计计算和仿真分析结果、产品安全状态监测数据和分析结果。

（五）企业具备必要的自动驾驶系统开发和验证工具（含软件和设备），支持相应的汽车安全完整性等级的系统开发和验证的仿真测试工具链，以及配置管理工具、问题管理工具、定位定向设备、场景模拟设备等。

（六）企业应具备与自身研发工作相适应的试验验证能力，至少具备针对智能网联汽车产品的模拟仿真、封闭场地、实际道路、网络安全和数据安全、软件升级、数据记录等测试验证能力。

二、安全保障能力

企业安全保障能力要求包括功能安全保障、预期功能安全保障、网络安全保障、数据安全保障、软件升级管理、风险与突发事件管理等能力要求。

（一）功能安全保障能力

1. 企业应建立汽车安全生命周期相关阶段的功能安全管理流程，针对汽车安全完整性等级明确对应流程要求，避免不合理的风险。

2. 企业应建立功能安全管理制度，涵盖整体功能安全管理、产品开发安全管理、安全发布管理等内容。

3. 企业应明确生产、运行阶段的功能安全要求。

4. 企业应明确功能安全支持过程要求，包括分布式开发接口管理、安全要求的定义和管理、配置管理、变更管理、验证、文档管理、软硬件组件鉴定等内容。

（二）预期功能安全保障能力

1. 企业应建立预期功能安全开发流程，具备功能及系统规范、危害识别和评估、功能不足识别和评估、功能改进、验证及确认策略定义、已知危害场景评估、未知危害场景评估、预期功能安全成果评估、运行阶段的监测等能力，保障

产品不存在因自动驾驶系统预期功能的不足所导致的不合理风险。

2. 企业应建立预期功能安全管理制度，明确预期功能安全管理职责和角色定义，开发人员的技能水平、能力等要求。

（三）网络安全保障能力

1. 企业应建立智能网联汽车产品网络安全管理制度，明确网络安全责任部门和负责人，应保障智能网联汽车产品开发流程遵循网络安全管理制度要求，落实网络安全责任，并依法落实备案管理、安全评估、用户真实身份信息核验、日志记录留存等网络安全相关管理要求。

2. 企业应建立智能网联汽车产品网络安全风险管控机制，具备网络安全风险识别、分析、评估、处置（例如，测试验证、跟踪等）等风险管控能力，以及及时消除重大网络安全隐患的能力。

3. 企业应建立智能网联汽车产品网络安全监测机制，具有监测、记录、分析网络运行状态、网络安全事件等技术措施，具备按照规定留存相关网络日志不少于6个月的能力。

4. 企业应建立智能网联汽车产品网络安全漏洞管理和应急响应机制，制定网络安全事件应急预案及应急处置操作规程，具备及时处置安全漏洞、网络攻击等安全风险的能力，具备支持车辆用户和安全员采取相应措施的能力。

5. 企业应建立智能网联汽车产品与供应商相关的风险

识别和管理能力，明确供方产品和服务的网络安全评价标准、验证规范等，具备管理企业与合同供应商、服务提供商、企业内部组织之间安全依赖关系的能力。

6. 企业应建立智能网联汽车产品网络安全管理制度的持续改进机制，在关键流程变更、网络安全事件发生后及时更新完善网络安全管理制度、相关机制等。

7. 企业应建立车联网卡实名登记制度，严格落实车联网卡实名登记有关要求。

（四）数据安全保障能力

1. 企业应当建立健全智能网联汽车产品数据安全管理制度，依法履行数据安全保护义务，明确责任部门和负责人。

2. 企业应建立智能网联汽车产品数据资产管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。

3. 企业应采取智能网联汽车产品数据安全保护技术措施，确保数据持续处于有效保护和合法利用的状态，依法依规落实数据安全风险评估、数据安全事件报告等要求。

4. 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法律法规规定在境内存储。因业务需要，确需向境外提供的，应当依照法律、行政法规的相关规定执行。

（五）软件升级管理能力

1. 企业应建立智能网联汽车产品软件升级管理制度，具备软件开发管理、配置管理、质量管理、变更管理、发布

管理、应急响应管理等能力。

2. 企业应制定智能网联汽车产品软件升级设计、开发、测试、发布、推送等过程的标准规范，并遵照执行。

3. 企业应具备识别、评估和记录软件升级对智能网联汽车产品安全、环保、节能、防盗性能影响的能力，确保符合相关法规、标准和技术要求。

4. 企业应具备识别软件升级的目标车辆、评估目标车辆软硬件配置与软件升级兼容性的能力，确保软件升级与目标车辆配置兼容。

5. 企业应具备识别车辆初始和历次升级的软件版本的能力。

6. 企业应具备记录并安全保存每次软件升级过程相关信息的能力，信息应至少保存至智能网联汽车产品停产后 10 年。

7. 企业应建立软件升级系统必要的网络安全防护管理和技术措施，确保软件升级流程的安全可靠。

8. 企业应建立软件升级用户告知机制，明确告知升级目的、升级前后变化、升级预估时间、升级期间无法使用的功能等信息。

9. 企业实施在线升级活动前，应当确保汽车产品符合国家法律法规、技术标准及技术规范等相关要求并向工业和信息化部备案，确保符合备案要求，保证汽车产品生产一致性。涉及产品安全漏洞修补的，需按有关要求向工业和信息

化部报送。

（六）风险与突发事件管理能力

企业应建立智能网联汽车风险与突发事件管理制度，具备突发事件应急预案及应急措施，具备安全风险排查及处理、事故原因分析等保障能力。

三、安全监测能力

企业应对其开展实际道路测试和上路通行的智能网联汽车安全状态进行监测和报告，确保监测数据和报告的真实性、安全性、完整性。

（一）企业应当建立智能网联汽车产品安全监测服务企业平台（简称企业平台），具有数据接收、数据上报、数据存储、数据补发等功能。

（二）企业应将车辆自动驾驶安全相关的事件监测数据上报省级或市级智能网联汽车产品安全监测平台（简称地方平台）、工业和信息化部试点管理系统（简称试点管理系统）以及企业平台所在地公安机关网安部门（仅涉及车联网网络、数据安全相关），用于支撑智能网联汽车产品安全性能评估、准入许可评估调整等。其中，涉及车联网网络、数据等安全相关数据，同步上报至国家车联网（智能网联汽车）安全监管和公共服务平台。

（三）企业应编写月度和年度应用评估报告，证明产品符合智能网联汽车产品技术要求，并上报地方平台和试点管理系统。与自动驾驶相关的有碰撞风险或发生碰撞的安全事

件，企业应立即上报事件分析报告。

（四）企业平台应保障网络安全和数据安全，具备权限管理功能、防篡改功能，以及高可用机制，防止机器失效带来的任务失效和数据丢失。

（五）企业应妥善保管智能网联汽车产品安全状态监测数据，月度、年度应用评估报告，以及安全事件分析报告，并长期存档备查。企业不得泄露、篡改、毁损、出售或者非法向他人提供，不得监测与产品安全状态无关的数据。

（六）企业应具备智能网联汽车产品质量信息分析能力，可采集和储存与自动驾驶相关的产品缺陷信息、车辆故障信息、道路交通事故信息及消费者投诉信息，进行分析并实施改进。

四、用户告知机制

（一）企业应建立用户告知机制，确保用户充分掌握智能网联汽车与传统汽车在操作、使用等方面的差异。

（二）告知信息包括但不限于智能网联汽车产品功能及性能限制、安全员职责、人机交互设备指示信息、系统操作说明、功能激活及退出条件和方法、最小风险策略、系统潜在风险说明、人工接管预留时间、不可避免碰撞的响应策略等信息。告知信息应明确写入产品使用说明书。

第二章 智能网联汽车产品

一、产品技术要求

智能网联汽车产品应当符合《道路机动车辆生产企业及

产品准入管理办法》《新能源汽车生产企业及产品准入管理规定》等道路机动车辆产品准入要求，应具有明确的自动驾驶功能定义及其设计运行条件，并符合动态驾驶任务执行、接管、最小风险策略、人机交互、产品运行安全、网络安全、数据安全、无线电安全、软件升级、数据记录等技术要求。应说明车辆运行所在城市所具备的必要基础设施条件，包括支持智能网联汽车产品设计运行条件的公共道路、交通基础设施、通信基础设施等。

（一）动态驾驶任务执行要求

1. 自动驾驶系统应能持续识别其设计运行条件，仅能在设计运行条件内激活，并具备明确的功能激活和退出策略。在激活状态下，自动驾驶系统应执行全部动态驾驶任务，当到达设计运行条件边界时，应执行合理的策略。

2. 自动驾驶系统应具备充分的目标和事件探测与响应能力，支持其安全且合理地执行全部动态驾驶任务。

3. 自动驾驶系统应具备安全驾驶决策及控制的能力，至少包括符合合理规划控制车辆行驶路径与行驶速度、合理应对存在的风险等要求，且驾驶行为应符合其他道路使用者的预期。

4. 自动驾驶系统应不存在由系统失效和功能不足引起的危害而导致的不合理风险，且具备自动识别自动驾驶系统失效的能力，确认自动驾驶系统是否能够持续执行动态驾驶任务，并提供必要的信息提示。自动驾驶系统失效或功能不

足时，应执行合理的控制策略，直至车辆进入最小风险状态或动态驾驶任务被接管。

5. 在激活状态下，自动驾驶系统应避免导致交通事故。当碰撞事故不可避免时，自动驾驶系统应采取合理控制策略，降低事故伤害或损失。

（二）接管要求

对于需要安全员执行接管的自动驾驶系统，应具备安全、可靠、有效的接管策略，及时向安全员发出介入请求，并能够检测安全员是否执行接管操作。当安全员未能及时响应介入请求，自动驾驶系统应执行最小风险策略以达到最小风险状态。

（三）最小风险策略要求

1. 自动驾驶系统应具备最小风险策略，用于避免或减缓车辆与其他道路使用者的风险。

2. 自动驾驶系统最小风险策略应在符合道路交通安全法律法规前提下充分考虑安全风险，且应设计合理，包括触发、执行、终止和信息提示等。

3. 在自动驾驶系统执行最小风险策略过程中，不应禁止安全员通过合理的方式干预车辆。

（四）人机交互要求

1. 自动驾驶系统应具备供安全员激活、退出等的专用操纵方式。

2. 自动驾驶系统应具备安全、可靠、有效地响应干预

的策略，并应能检测安全员是否执行干预操作。

3. 自动驾驶系统应持续向用户提示明确、充分的自动驾驶系统状态信息，不应对用户造成干扰。当自动驾驶系统状态发生变化时，自动驾驶系统应及时向用户提供必要的提示信息。

4. 对于需要安全员接管的自动驾驶系统，应具备安全员接管能力监测功能，应对安全员是否具备执行动态驾驶任务接管的能力进行识别，并在安全员能力不满足要求时，发出警告信号。

5. 车辆应依法依规合理使用声音、照明、光信号、无线电信号等方式与其他道路使用者或相关设施进行交互。

（五）产品运行安全要求

1. 自动驾驶系统在激活状态下，不应对车辆驾乘人员和其他交通参与者造成不合理的交通安全风险。

2. 自动驾驶系统在激活状态下，应遵循《中华人民共和国道路交通安全法》《中华人民共和国道路交通安全法实施条例》，以及车辆运行所在地相关道路交通通行规则规定，满足道路交通安全管理相关要求。

3. 产品测试与安全评估方案、实施、结果等涉及产品运行安全要求的，由公安机关道路交通安全相关技术服务机构进行评估。

（六）网络、数据和无线电安全要求

1. 应能够防御车辆外部连接安全威胁。包括利用第三

方应用漏洞进行攻击、外部接口（USB、OBD 等）入侵等。

2. 应能够防御通信通道安全威胁。包括车辆接收消息的欺骗攻击、窃听攻击、劫持或重放攻击，未经授权操作、删除或篡改车辆上的代码，拒绝服务攻击，非法提权攻击，恶意数据注入等。

3. 应能够防御软件升级安全威胁。包括破坏软件升级程序或固件、篡改软件升级包等。

4. 应能够防御对车辆数据安全威胁。包括未经授权提取、操作或删除车辆数据，个人信息泄露、篡改、丢失等。

5. 应能够防御行为安全威胁。包括无意加载恶意软件、无意触发网络安全风险点等。

6. 应能够防御物理操控安全威胁。包括未经授权替换关键的车辆电子控制单元、添加车辆电子控制单元进行中间人攻击等。

7. 应不存在由汽车行业权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。

8. 应保证搭载的、接入公用电信网的车载通信设备依法取得电信设备进网许可，无线电发射设备符合《无线电发射设备管理规定》等国家无线电管理有关要求。

（七）软件升级要求

1. 应保护升级包的真实性和完整性，以合理地防止其受到损害和无效软件升级。

2. 应保护车辆上的软件版本免受篡改。

3. 车辆应具备更新软件版本的能力，并应能通过标准化的电子通信接口读取软件版本。

4. 在执行软件升级前，应确保车辆满足先决条件，如确保车辆有足够电量完成软件升级。

5. 在执行软件升级前，应告知车辆用户有关软件升级的信息，并应得到车辆用户确认。

6. 当执行软件升级可能影响车辆安全时，应在升级执行过程中通过技术手段确保车辆安全。

7. 若执行软件升级影响驾驶安全，车辆应确保升级执行期间无法被驾驶，并确保安全员不能使用任何可能影响车辆安全或成功执行软件升级的车辆功能。

8. 在执行软件升级后，应告知车辆用户车辆升级的结果。

9. 若升级失败或中断，车辆应能够恢复到以前的可用版本，或确保车辆处于安全状态。

（八）数据记录要求

1. 智能网联汽车产品应配备事件数据记录和自动驾驶数据记录功能。

2. 自动驾驶数据记录功能记录的数据元素应至少包括车辆及自动驾驶数据记录系统基本信息、车辆状态及动态信息、自动驾驶系统运行信息、行车环境信息、驾乘人员操作及状态信息等。

3. 在自动驾驶系统激活期间，记录的事件数据应至少

包括自动驾驶系统激活、退出、发出介入请求、开始执行最小风险策略、发生严重失效、有碰撞风险、发生碰撞等。

4. 智能网联汽车产品应具备数据存储能力、断电存储能力，遵循存储覆盖机制，能够持续正常记录和存储数据。

5. 记录的数据应能被提取并正确解析，能通过标准化的方法或途径实现数据提取。

6. 智能网联汽车产品应保证记录数据的完整性和真实性，以防止数据被篡改、伪造或恶意删除。

二、过程保障要求

智能网联汽车产品过程保障要求包括整车尤其是自动驾驶系统的功能安全过程保障、自动驾驶系统预期功能安全过程保障、整车网络安全和数据安全过程保障等要求。

（一）整车尤其是自动驾驶系统的功能安全过程保障要求至少包括:

1. 应在整车层面定义和描述自动驾驶系统，包括但不限于自动驾驶功能和接口，其与安全员、环境和其他系统的依赖性和交互，技术标准要求。

2. 应定义由自动驾驶功能异常表现导致的危害，结合合理的运行场景识别危害事件，针对危害事件按照严重度、暴露概率和可控性进行评估，确认合理的汽车安全完整性等级、危害事件的安全目标。

3. 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、功能冗余等，并将其分配给自动驾驶系统的架构要素或外部措施。

4. 应定义与自动驾驶系统功能安全相关零部件供应商的开发接口协议，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。

5. 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，确保整车和自动驾驶系统的相关要求得到实施和满足。

6. 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）自动驾驶系统预期功能安全过程保障要求至少包括:

1. 应满足自动驾驶系统预期功能安全规范定义和设计的要求，包括但不限于自动驾驶功能及其设计运行条件、动态驾驶任务执行、接管、最小风险策略、人机交互等技术要求。开展危害识别和风险评估工作，制定合理的风险可接受准则。

2. 应识别和评估潜在功能不足和触发条件引起的危害，并应用功能改进等措施避免不合理风险。

3. 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，以确保不存在不合理的预期功能安全风险，并对运行阶段产品的预期功能安全风险进行合理管控。

4. 应定义与自动驾驶系统预期功能安全相关零部件供应商的开发接口协议，确保整车和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和数据安全过程保障要求至少包括:

1. 应开展网络安全和数据安全风险评估，包括资产识别、威胁场景识别、攻击路径分析、风险等级评估、风险处置措施，应考虑所有与供应商等相关方的风险。

2. 在概念设计阶段，应根据网络安全和数据安全风险评估结果，明确网络安全和数据安全的目标和要求，设计安全架构和功能。

3. 在产品开发阶段，应适当地处理或管理已识别的风险，实现网络安全和数据安全风险防范应对处置措施，满足整车网络安全和数据安全的目标和要求等，保护车辆免受风险评估中确定的风险。

4. 在验证确认阶段，应开展整车网络安全和数据安全测试验证，并提供确认情况说明（包括测试指标、测试方法、测试环境、测试结果等），确保有效处置所有已识别的安全风险，以及有效、合理、完整地实现网络安全目标和要求等。

三、测试验证要求

产品应符合模拟仿真、封闭场地、实际道路以及网络安全和数据安全、软件升级、数据记录等测试验证要求。试验过程中不应变更自动驾驶功能相关的软件及硬件。

（一）自动驾驶系统模拟仿真测试的要求至少包括:

1. 应通过定义设计运行条件内不同场景要素的参数组合，验证自动驾驶系统是否符合安全要求。

2. 应证明模拟仿真测试场景至少包括充分、合理的标称场景、危险场景和边缘场景，以有效地验证自动驾驶系统安全。

3. 应证明使用的模拟仿真测试工具链置信度，以及车辆动力学、传感器等模型可信度，并通过与封闭场地和实际道路测试结果对比等手段验证模拟仿真测试的可信度。

4. 应提供模拟仿真测试过程中所涉及的测试场景集、测试手段、测试方法、评估方法以及测试数据管理（记录、处理、存储）等说明，应确保模拟仿真测试结果的可追溯性。

（二）封闭场地测试的要求至少包括:

1. 应采用封闭场地测试方法，验证产品在封闭场地典型场景下的安全性。

2. 封闭场地测试应考虑自动驾驶系统设计运行条件内的关键要素。场景应表征设计运行条件内所要求的行驶工况，并统筹考虑交通环境及附属设施情况。

3. 应对测试开展过程进行记录，对测试过程中所涉及的测试环境、测试人员、测试设备及测试方法的规范性负责，确保测试结果的一致性和准确性。

4. 应对测试数据进行记录，至少包含测试车辆自动驾驶系统软硬件版本信息、车辆控制模式、车辆运动状态参数、

车辆灯光和相关提示信息状态、反映试验人员及人机交互状态的车内视频及语音监控情况、反映测试车辆行驶状态的视频信息、目标物的位置及运动数据等内容，确保测试结果的可追溯性，并对测试结果进行分析与评估。

（三）实际道路测试的要求至少包括:

1. 应在封闭场地测试通过后，进行实际道路测试。

2. 应根据自动驾驶系统所声明设计运行范围对应的道路类型，开展实际道路连续场景测试，以验证产品在实际道路交通运行环境下的安全性。

3. 应对测试开展过程进行记录，对实际道路测试过程中所涉及的测试环境、测试人员、测试设备及测试方法的规范性负责，确保测试结果的一致性和准确性。

4. 应对测试数据进行记录，至少包含测试车辆自动驾驶系统软硬件版本、控制模式、车辆行驶状态、试验人员状态、人机交互状态、测试里程及时长、人工接管、车辆碰撞等信息，确保测试结果的可追溯性。

5. 应对测试车辆进行监测，基于测试里程及时长，自动驾驶功能的响应及试验人员的干预等，验证所声明的自动驾驶功能应对真实交通环境的能力。

6. 实际道路测试申请、审批、机动车登记、道路交通安全违法行为（以下简称交通违法）及交通事故处理的有关要求，本要求未规定的，适用《智能网联汽车道路测试与示范应用管理规范（试行）》（工信部联通装〔2021〕97号）。

（四）整车网络安全和数据安全测试要求至少包括:

1. 应选择适用的方法，对车辆外部连接安全、通信通道安全、软件升级安全、车辆数据安全、行为安全、物理操控安全进行适当和充分的测试，以验证所实施的安全措施的有效性。

2. 应对测试开展过程进行记录，对测试过程中所涉及的测试用例、测试环境、测试人员、测试设备及测试方法的规范性负责，确保测试结果的一致性和准确性。

（五）软件升级测试的主要对象是智能网联汽车产品的软件升级功能，测试要求至少包括:

1. 应开展升级包真实性完整性、软件版本更新及读取、软件版本防篡改、用户告知、用户确认、先决条件、电量保障、车辆安全、驾驶安全、结果告知等测试，确保符合技术要求。

2. 应对测试开展过程进行记录，对测试过程中所涉及的测试用例、测试环境、测试人员、测试设备及测试方法的规范性负责，确保测试结果的一致性和准确性。

（六）数据记录测试要求至少包括:

1. 应满足数据记录测试要求，包括：事件触发试验、连续记录触发试验、数据存储能力试验、存储覆盖机制试验、断电存储试验、网络安全试验、防护性能试验等。

2. 应对测试开展过程进行记录，对测试过程中所涉及的测试用例、测试环境、测试人员、测试设备及测试方法的

规范性负责，确保测试结果的一致性和准确性。

第二部分 使用主体

一、基本条件

试点使用主体应当具备以下基本条件:

（一）在中华人民共和国境内登记注册，具备独立法人资格。

（二）在车辆运行所在城市具备固定经营场所，能够有效支撑智能网联汽车运行安全保障工作的开展。

（三）建立智能网联汽车运行安全保障机构，具备与智能网联汽车运行管理相匹配的负责人、管理人员，细化职责任务。

（四）建立健全运行安全保障制度，对智能网联汽车上路通行进行实时监测、应急处置，保障道路交通安全、数据安全、网络安全。

（五）从事运输经营的试点使用主体还应当具备相应业务类别的运营资质。

二、运行安全保障能力

（一）安全保障机制

试点使用主体应当建立智能网联汽车运行安全保障机制、风险与突发事件管理制度，具备事前、事中、事后全流程保障车辆安全运行的能力:

1. 按规定配备安全员、平台安全监控人员等运行安全保障人员，并建立培训、考核及管理制度。

2. 对车辆运行状态进行实时监测，按规定及时进行隐

患提醒、预警和处置。

3. 建立智能网联汽车突发事件应急预案，具备车辆运行安全风险防控、隐患排查、应急处置等保障能力。

4. 应当建立交通违法和交通事故信息定期上报制度，编写月度报告以存档备查。

5. 车辆仅限于符合条件的试点使用主体使用，对违反规定使用车辆的，取消试点资格。

（二）运行平台

1. 试点使用主体应当具备智能网联汽车运行安全监测平台（简称运行平台），对车辆运行安全状态进行实时监测。

2. 运行平台应当具有数据接收、数据验证、上报、存储等功能，对自动驾驶安全运行事件，按规定将车辆及自动驾驶系统基本信息、车辆状态及动态信息、自动驾驶系统运行信息、安全员操作及状态信息、故障信息等共享至省级或市级智能网联汽车安全监测平台（简称地方平台）、公安部智能网联汽车运行安全管理系统，用于配合相关部门事件调查、责任认定、原因分析等。

3. 运行平台应当保障网络安全和数据安全，具备权限管理功能、防篡改功能及高可用机制。

4. 运行平台应当按规定收集、存储、使用、加工、传输、提供和公开智能网联汽车运行安全信息，不得泄露、篡改、毁损、出售或者非法向他人提供。

（三）运行安全保障人员

1. 运行安全保障人员包括安全员和平台安全监控人员。

2. 安全员应当接受培训并通过考核，熟练掌握道路交通安全法律法规的规定和不同级别自动驾驶系统操作技能，具备紧急状态下应急处置能力。

3. 平台安全监控人员应当接受培训并通过考核，掌握使用主体的安全保障机制及风险与突发事件管理制度，熟练操作运行平台；熟练掌握道路交通安全法律法规；掌握车辆运行时的交通环境；监测过程中发现有规定情形的，及时发出预警、提示接管并采取相应处置措施。

（四）车辆运行保障

1. 试点使用主体应当熟悉自动驾驶功能设计运行条件，能够使用电子围栏等技术手段，确保车辆超出规定运行区域后无法开启自动驾驶功能。

2. 试点使用主体应当具备车辆维护或者保养能力，配合生产企业开展车辆软件升级，及时消除车辆运行安全隐患。

三、责任承担能力

（一）应当对车辆上路通行可能造成的人身和财产损失具备相应的民事责任承担能力，并按要求购买机动车交通事故责任强制保险以及其他交通事故责任商业保险。

（二）当车辆发生交通违法或者交通事故时，能够向相关部门提供足以证明交通违法事实或者交通事故成因的证明材料。

（三）具备配合相关部门开展应急救援、交通事故调查处理及事故调解、损害赔偿的能力。

四、网络安全和数据安全保障能力

应当参照汽车生产企业要求执行。

（一）网络安全保障能力

1. 应当建立智能网联汽车网络安全管理制度，明确网络安全责任部门和负责人，落实网络安全责任，并依法落实网络安全相关管理要求。

2. 应当建立智能网联汽车网络安全风险管控机制，具备网络安全风险识别、分析、评估、处置、跟踪等风险管控能力，及时消除重大网络安全隐患的能力。

3. 应当建立智能网联汽车网络安全监测机制，具有监测、记录、分析网络运行状态、网络安全事件等技术措施，具备按照规定留存相关网络日志不少于6个月的能力。

4. 应当建立智能网联汽车网络安全应急响应机制，制定网络安全事件应急预案，具备及时处置安全漏洞、网络攻击等安全风险的能力。

5. 应当建立智能网联汽车安全漏洞管理机制，具备及时处置安全漏洞、指导和支持车辆用户和安全员采取相应措施的能力。

6. 应当建立智能网联汽车网络安全保障机制，明确产品和服务的网络安全评价标准、验证规范等，确定与产品提供方的安全协议，具备协同管控网络安全风险的能力。

7. 应当建立智能网联汽车网络安全管理制度的持续改进制度，在关键流程变更、网络安全事件发生后及时更新完善网络安全管理制度、相关机制等。

（二）数据安全保障能力

1. 应当建立健全智能网联汽车数据安全管理制度，依法履行数据安全保护义务，明确责任部门和负责人。

2. 应当建立智能网联汽车数据资产管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。

3. 应当采取智能网联汽车数据安全保护技术措施，确保数据持续处于有效保护和合法利用的状态，依法依规落实数据安全风险评估、数据安全事件报告等要求。

4. 车辆上路通行期间，试点使用主体应当遵守以下汽车数据安全管理要求:

（1）车外数据未完成匿名化处理前，不应当向车外提供;

（2）除非安全员自主设定，车辆应当默认设定为不收集车辆数据的状态;

（3）除非取得个人信息主体同意，原则上不应向车外提供车辆数据，符合试点安全监测、交通违法和交通事故处理相关规定要求，法律、行政法规规定等情形除外;

（4）通过车辆处理个人信息应当通过用户手册、车载显示面板、语音、车辆使用相关应用程序等显著方式告知个人信息处理规则;

（5）《汽车数据安全管理若干规定（试行）》等法规、标准规定的其他要求。

五、运营安全保障能力

从事运输经营的试点使用主体和车辆应当符合交通运输部有关运营安全管理要求。

第三部分 上路通行

一、试点使用主体应当在保障道路交通安全的前提下，为车辆上路通行购买机动车交通事故责任强制保险以及每车不低于五百万元人民币的交通事故责任保险。

二、申请上路通行试点的，应当向车辆运行所在城市公安机关交通管理部门车辆管理所申请登记，交验车辆，并提交以下证明、凭证:

（一）试点使用主体的身份证明;

（二）机动车来历证明;

（三）车辆购置税的完税证明或者免税凭证;

（四）机动车交通事故责任强制保险凭证;

（五）机动车整车出厂合格证;

（六）机动车安全技术检验合格证明。

车辆办理注册登记后，试点期间不得办理变更登记、转让登记、抵押登记等业务。

三、车辆不得擅自进行影响车辆功能、性能的软硬件变更。涉及自动驾驶功能软件升级的，试点汽车生产企业应当向工业和信息化部申请批准并备案，由工业和信息化部将备案信息共享至公安部。经批准后，试点汽车生产企业应当及时告知试点使用主体。试点使用主体自愿选择是否升级，选择升级的，应当在车辆停驶的安全状态下进行。

四、车辆运行所在城市应当具备支持智能网联汽车自动驾驶功能设计运行条件和道路交通管理实际相适应的公共

道路、交通基础设施、通信基础设施等必要的基础设施条件。

车辆运行所在城市工业和信息化、公安机关交通管理、交通运输等部门应当按照确保安全、方便管理的原则，确定试点路段、区域，并向社会公布。

试点路段、区域应当设置相应交通标识或者提示信息，保障车辆自动驾驶功能的实现。

试点汽车生产企业及试点使用主体应当运用技术手段，确保车辆自动驾驶功能只能在限定路段、区域范围内激活。不得在公路上开展制动性能试验。

五、试点汽车生产企业、试点使用主体及车辆应当遵守我国道路交通安全法律法规，驾驶行为应当符合道路交通通行规则，保障道路交通安全、有序、畅通。

六、车辆的车身应当以醒目图案、文字或者颜色标示，以提醒周边车辆及其他交通参与者注意。

七、试点使用主体应当在保障道路交通安全的前提下，为车辆上路通行配备相应驾驶资格的安全员，并负责培训，确保其符合以下资格条件:

（一）取得相应准驾车型驾驶证、具有 3 年以上驾驶经历;

（二）最近连续 3 个记分周期内没有被记满 12 分记录;

（三）最近 1 年内无超速 50%以上、超员、超载、违反交通信号灯通行等严重交通违法记录;

（四）无饮酒后驾驶或者醉酒驾驶机动车记录，无服用

国家管制的精神药品或者麻醉药品记录;

（五）无致人死亡或者重伤且负有同等以上责任的交通事故记录;

（六）与试点使用主体签订劳动合同或者劳务合同;

（七）经试点使用主体培训后，熟练掌握自动驾驶相关法律法规、自动驾驶系统专业知识，具备紧急状态下应急处置能力;

（八）法律、行政法规、规章对机动车驾驶人规定的其他条件。

经培训合格的安全员信息应当向车辆运行所在城市公安机关交通管理部门车辆管理所备案。

八、车辆上路通行前，安全员除了按照法律法规对车辆进行安全检查外，还应当对自动驾驶功能相关的车载设备、车辆网络接收和传输设备进行检查调试，确保设备处于良好运行状态。

九、车辆上路通行过程中，安全员应当处于车辆驾驶座位上，在自动驾驶系统激活状态下，监控车辆运行状态及周围环境，当系统提示需要人工操作或者发现车辆处于不适合自动驾驶的状态时，及时接管或者干预车辆并采取相应措施。

十、车辆在自动驾驶系统激活状态下，不得从事校车业务、搭载危险物品。

十一、试点使用主体应当安排安全监控人员对车辆安全

运行状态进行实时监测。发现下列情形时，安全监控人员应当按照应急预案及时发出预警，提示安全员干预车辆并采取相应措施:

（一）发现车辆存在道路交通安全、网络安全、数据安全隐患可能涉及违法犯罪的;

（二）自动驾驶系统故障、失效或者车辆超出运行范围的。

安全员拒不执行、执行不到位或者无法干预的，应当及时分别报告公安机关交通管理部门和网络安全保卫部门。

十二、车辆上路通行过程中发生的交通违法，由交通违法行为发生地的公安机关交通管理部门管辖。

十三、现场发现车辆实施交通违法的，交通警察应当询问安全员，及时固定证据，使用执法记录仪全程摄录，并向安全员开具《道路交通安全违法处理通知书》。通过交通技术监控设备记录车辆实施交通违法的，应当按规定审核录入并通知试点使用主体。

试点使用主体和安全员应当持交通违法自查报告在规定的时间内一并到公安机关交通管理部门接受处理。公安机关交通管理部门应当依照《道路交通安全违法行为处理程序规定》对交通违法事实进行调查，听取当事人陈述、申辩，制作并送达行政处罚决定书。

交通违法涉嫌由自动驾驶系统原因导致的，还应当通知相关主体接受调查处理。

十四、上路通行过程中发生交通违法的，由公安机关交通管理部门按照现行道路交通安全法律规范对安全员进行处理；能够确定交通违法是自动驾驶系统原因导致的，按规定对相关主体进行处理。

十五、公安机关交通管理部门应当定期将交通违法信息抄送至省级或市级智能网联汽车安全监测平台（简称地方平台），由地方平台对车辆及安全员基本信息、自动驾驶系统运行信息进行记录。

十六、车辆上路通行过程中发生道路交通事故时，安全员应当在确保安全的前提下立即停车，抢救受伤人员，保护现场，并迅速报警。安全员现场未报警的，试点使用主体运行平台安全监控人员应当立即报警，远程协助并按照应急预案采取相应措施。

对于仅造成轻微财产损失的事故，当事人对事实及成因无争议的，可以自行协商处理。

十七、试点汽车生产企业和试点使用主体应当积极配合公安机关交通管理部门进行事故调查和处理。车辆发生道路交通事故的，试点汽车生产企业和试点使用主体应当在事故发生后 2 小时内将事故发生前至少 15 秒（或自动驾驶系统激活时刻，两者可取较晚时刻）和事故发生后至少 5 秒（或自动驾驶系统退出时刻，两者可取较早时刻）的视频信息上传至地方平台，并在事故发生之日起 3 个工作日内向公安机关交通管理部门提交事故自查报告和相关信息。相关信息应

当包括车辆及自动驾驶系统基本信息、车辆状态及动态信息、自动驾驶系统运行信息、行车环境信息、安全员操作及状态信息、车内乘客状态信息、故障信息等。公安机关交通管理部门根据事故调查的需要，可以要求试点汽车生产企业、试点使用主体提供其他信息和材料。

未按规定提供或者无正当理由逾期未提供的，由未提供方承担事故责任。

十八、公安机关交通管理部门应当按照现行道路交通安全法律法规、规章和本规定要求进行调查处理，依法确定当事人事故责任。

车辆在自动驾驶系统功能激活状态下发生道路交通事故的，对于涉及财产损失或者当事人伤势轻微，各方当事人一致同意的，可以适用简易程序。

因收集证据的需要，公安机关交通管理部门可以扣留事故车辆，并开具行政强制措施凭证。

公安机关交通管理部门认为需要检验鉴定的，应当委托具备检测能力的鉴定机构进行技术鉴定。

车辆在自动驾驶系统功能激活状态下发生道路交通事故，造成人员重伤、死亡或者严重财产损失，以及产生重大社会影响的，由公安机关交通管理部门会同相关行政主管部门组织开展深度调查，查找安全隐患和管理漏洞，推动问题整改，构成犯罪的，依法追究相关责任人刑事责任。

十九、车辆在自动驾驶系统功能未激活状态下发生道路

交通事故的，按照现行规定承担责任。

车辆在自动驾驶系统功能激活状态下发生道路交通事故造成人身伤亡、财产损失的，由保险公司在保险责任限额范围内予以赔偿；不足的部分，按照《中华人民共和国道路交通安全法》第七十六条规定确定各方当事人的赔偿责任。

由智能网联汽车一方依法承担赔偿责任的，由试点使用主体承担；试点汽车生产企业、自动驾驶系统开发单位、基础设施及设备提供方、安全员等相关主体对交通事故发生有过错的，试点使用主体可以依法追偿。构成犯罪的，依法追究相关责任人刑事责任。

二十、试点使用主体运行平台应当如实记录车辆道路交通违法、交通事故信息，每月将车辆发生的交通违法和交通事故信息基本情况、原因分析、风险对策等上报车辆运行所在城市公安机关交通管理部门以及工业和信息化主管部门。

试点期间发生道路交通事故，造成人员重伤、死亡或者严重财产损失，以及产生重大社会影响的，试点使用主体应当在事故发生后24小时内将事故情况发送至地方平台。省、市级人民政府相关主管部门应当在3个工作日内上报公安部、工业和信息化部。

二十一、试点使用主体应当对车辆上路通行期间收集的数据加强管理，数据处理应当符合汽车数据安全管理等相关法律法规和技术要求。车辆产生的网络安全和数据安全违法违规责任，由安全员、试点汽车生产企业、试点使用主体、

自动驾驶系统开发单位等相关主体依法承担。

二十二、车辆在自动驾驶系统激活状态下，有下列情形之一的，车辆运行所在城市公安机关交通管理部门可以通报车辆运行所在城市主管部门。

（一）自登记之日起，因自动驾驶系统原因发生3次依据《道路交通安全违法行为记分管理办法》应当一次记3分以上的交通违法，或者2起承担同等以上事故责任的交通事故的;

（二）发生交通违法、交通事故后造成较大社会影响的;

（三）公安机关交通管理部门认为车辆存在严重安全隐患，需要通报的。

车辆运行所在城市主管部门接通报后，应当组织调查，存在安全隐患的，通知试点汽车生产企业和试点使用主体暂停使用同一型号、同一版本的自动驾驶系统。

对暂停使用的自动驾驶系统，试点使用主体应当确保与车辆搭载同一型号、同一版本的自动驾驶系统始终处于未激活状态。试点汽车生产企业应当进行整改，并向工业和信息化部、公安部提交整改报告。经评估确认隐患已消除的，方可重新使用。

二十三、试点使用主体在试点期间发生以下情形之一的:

（一）未按规定配备安全员、安全监控人员的;

（二）未按规定将车辆运行数据接入地方平台的;

（三）未按规定提供相关事故过程信息或者事故分析报告；

（四）试点使用主体擅自对已登记的车辆及其自动驾驶系统进行改装的；

（五）车辆在自动驾驶系统激活状态下从事校车业务或者搭载危险货物的；

（六）其他需要中止试点使用主体试点资格的情形。

试点使用主体应当暂停车辆运行，按照有关部门要求进行整改，向车辆运行所在城市公安机关交通管理、工业和信息化等主管部门提交整改报告，并提出恢复车辆运行申请。经车辆运行所在城市公安机关交通管理、工业和信息化等主管部门评估确认后，恢复其试点资格。

第四部分 试点暂停与退出

一、试点暂停

（一）试点汽车生产企业未履行生产一致性和安全保障责任的;

（二）试点汽车生产企业、试点使用主体未履行网络安全和数据安全保护义务的;

（三）工业和信息化部、公安部、住房和城乡建设部、交通运输部及省级主管部门认为试点实施中存在安全风险的其他情形。

涉及前款第（一）项情形的，应当依据道路机动车辆生产企业和产品准入管理有关规定整改。涉及前款第（二）项和第（三）项情形的，应当按规定整改，经省级工业和信息化主管部门、公安机关交通管理和网络安全保卫部门、通信管理部门等评估，报工业和信息化部、公安部等相关部门确认后，方可恢复其试点。

二、试点退出

（一）车辆自动驾驶系统存在安全隐患且安全隐患无法消除的，因自动驾驶系统原因导致死亡 1 人或者重伤 3 人以上承担主要以上责任的交通事故的;

（二）试点汽车生产企业相关条件发生重大变化无法保障试点实施的，隐瞒有关情况或者提供虚假材料等情形的;

（三）试点使用主体相关条件发生重大变化无法保障试点实施的，隐瞒有关情况或者提供虚假材料的，未按规定落

实运行安全管理责任、网络安全和数据安全保护义务，出现违反国家相关法律法规的情况，拒不整改或整改后仍未解决问题的；

（四）工业和信息化部、公安部、住房和城乡建设部、交通运输部及省级主管部门认为试点实施中存在严重问题的其他情形。

退出试点的，试点汽车生产企业应当关闭相应车辆自动驾驶功能，试点使用主体应当及时办理车辆变更或者注销登记，同步办理车联网卡过户、注销等登记信息变更手续，并依法依规对车辆进行处理。