附件 1

智能网联汽车产品准入、召回及软件在线升级管理与技术指南

为加强智能网联汽车产品准入、召回及软件在线升级（以下称 OTA 升级）管理，制定本指南。本指南中智能网联汽车产品搭载的组合驾驶辅助系统是指国家标准《汽车驾驶自动化分级》（GB/T 40429-2021）定义的 2 级驾驶自动化系统（以下简称系统）。

一、加强企业能力建设

（一）健全安全保障能力。企业生产搭载组合驾驶辅助系统的智能网联汽车产品的，制定相应的安全管理制度，健全企业质量安全体系和产品技术标准，明确安全责任部门和负责人，健全流程、方法、工具等设计验证能力，完善网络安全、数据安全、功能安全、预期功能安全、个人信息保护、OTA 升级管理等保障能力，确保对开发、生产、运行等阶段进行有效的安全管理，持续保障智能网联汽车产品质量安全。

（二）加强安全监测与报告管理。企业生产搭载组合驾驶辅助系统的智能网联汽车产品的，建立事件监测和分析评估机制，健全系统相关安全事件监测、事件事故报告流程，强化事件调查、分析、处置、改进，以及事故深度调查分析

与技术改进等能力，健全事件事故数据记录和存储管理，确保监测数据的真实性、安全性和完整性。

（三）规范营销宣传行为。企业向消费者提供有关智能网联汽车驾驶自动化等级、系统能力、系统边界等信息时，应当真实、全面，不得作虚假、夸大系统能力或引人误解的宣传，确保消费者正确理解和使用智能网联汽车产品。企业在组合驾驶辅助系统或功能命名及营销宣传中，不得使用暗示消费者该系统可以作为自动驾驶系统使用，具备实际上并不具备的功能等用语，防止驾驶员滥用风险。

（四）严格履行告知义务。企业生产搭载组合驾驶辅助系统的智能网联汽车产品的，建立面向用户的告知机制，告知范围至少包含驾驶员责任、系统基本信息和正确使用方式、系统能力、系统边界、状态转换、人机交互、发生安全事件的应急处置方法等内容，确保用户以易理解的方式掌握相关信息。企业编制的智能网联汽车产品使用说明书、用户培训材料，内容表达科学合理、图文并茂、简洁易懂、完整准确，易于一般用户阅读、理解和操作，并通过随车配发的说明书、车载显示终端、企业官方网站等有效方式告知用户，避免驾驶员将组合驾驶辅助功能作为自动驾驶功能使用。

（五）健全产品售后服务管理体系。企业要履行质量担保义务，明示智能网联汽车产品售后服务承诺及应急措施等内容，提供售后服务，并保证在设计使用寿命期和企业承诺

的质量担保期内向用户提供质量合格的备件、维修和咨询服务。企业对用户就其提供的智能网联汽车产品或者服务的质量和使用方法等问题提出的询问，应当作出真实、明确的答复，加强售后争议处理能力建设。

（六）加强产品安全与召回能力建设。企业健全搭载组合驾驶辅助系统的智能网联汽车产品安全与召回管理体系，建立缺陷信息收集、调查分析、召回决策与实施管理机制；建立应急管理机制，具备及时处置安全突发事件的能力；提高召回专业人员技术水平，提升缺陷技术分析与评估能力；建立智能网联汽车产品追溯体系，提高召回实施效率和完成率。

二、强化产品安全管理

（七）加强产品安全设计。企业对生产的搭载组合驾驶辅助系统的智能网联汽车产品，明确安全概念，确保安全目标实现，并将其设计为：

1. 具备与组合驾驶辅助系统功能相匹配的硬件和软件。

2. 确保智能网联汽车产品性能不低于机动车强制性国家标准对应的安全技术要求，装备的电子控制系统不影响有关机动车强制性国家技术标准规定的制动、转向、照明和信号装置等安全要求。

3. 具备检测系统失效的能力，在失效时执行合理降低风险的策略。采取有效措施防止可合理预见的驾驶员误用风

险，包括检测驾驶员脱离驾驶任务的必要技术措施、设置合理的防误用阈值等。

4. 汽车通信链路、OTA 升级活动等采用合规且有效的网络安全防护技术。采取有效措施防御未经授权的系统硬件和软件变更、数据提取或操作等网络安全和数据安全威胁，确保车辆及其功能、车辆数据和个人信息持续处于被保护的状态。

5. 对于行车辅助功能，系统具备评估驾驶员持续执行驾驶任务的技术措施，检测驾驶员是否脱离驾驶任务，确保驾驶员始终执行相应的动态驾驶任务。对于系统发起的车辆运动控制，还需确保系统行为合规合理。

6. 智能网联汽车产品在系统激活期间向驾驶员提供安全干预或退出系统的方式。针对系统失效、达到系统边界等情况，应当给予合理的时间让驾驶员做出适当的反应，采取必要措施，降低碰撞风险，保持驾驶员对系统的可控性。

（八）明确系统边界和安全响应措施。企业明确系统边界，包括道路类型、道路基础设施、天气条件、对其他道路使用者行为的响应能力等，验证智能网联汽车产品具有探测和响应系统边界的能力。当系统在激活状态下探测到已超出、正在超出或即将超出系统边界时，采取合理策略告知驾驶员。

（九）确保控制策略合理。企业确保系统具备明确的激

活、动态驾驶任务执行和退出策略。对于行车辅助，当系统检测到驾驶员脱离动态驾驶任务、未响应警告且没有采取必要的控制措施时，系统适时启动风险减缓功能以使车辆安全停车；驾驶员未规范使用组合驾驶辅助功能的，系统应当具备禁止激活相应功能等限制策略。对于泊车辅助，系统具备检测运行区域内其他道路使用者、障碍物，以及为避免碰撞而安全停车或减缓车速的能力。

（十）合理设计人机交互方式。企业确保系统向驾驶员提供及时、可区分、易于理解的提示信息，包括系统状态、系统边界、驾驶员需要执行的操作、驾驶员脱离动态驾驶任务等，确保驾驶员对系统能力认知清晰准确，避免驾驶员过度依赖；确保系统和功能开启或激活的人机交互过程，与装备在车辆上的其他系统不会产生混淆。当功能状态发生变化或转换为其他驾驶自动化功能时，系统及时向驾驶员提供提示信息。当执行动态驾驶任务期间发生系统失效时，系统发出失效警告信号。

（十一）开展充分的测试验证。企业确保在设计和开发过程中对组合驾驶辅助系统及其功能进行全面安全评估，针对系统边界和安全响应、控制策略、人机交互等，采用模拟仿真、封闭场地、实际道路、网络安全等必要测试方法开展充分测试，确保智能网联汽车产品满足安全要求。实际道路测试符合国家有关保密、测绘等法律法规及管理规定。

三、强化沙盒监管深度测试

（十二）强化沙盒监管深度测试。企业主动履行质量安全主体责任，在搭载组合驾驶辅助系统车辆量产销售初期，要通过沙盒监管深度测试开展新技术潜在风险验证，不断提升组合驾驶辅助系统安全水平，并具备必要的深度测试和应急处置资源。深度测试要聚焦于事故场景和缺陷场景等的识别与应对，以及高危场景下的预期功能安全和功能安全问题。企业对组合驾驶辅助系统未知风险加强研究和评估，鼓励联合构建可应用于深度测试的危险场景库，包括事故场景、失效场景、缺陷场景、特定复杂场景等。

四、强化汽车软件在线升级管理

（十三）加强 OTA 升级企业保障能力。企业生产具备软件 OTA 升级功能的智能网联汽车产品的，应当健全完善与产品及升级活动相适应的管理制度和保障能力，强化安全保障和防护、影响评估、测试验证、执行过程保障、日志记录、历次升级信息保存、OTA 召回实施等技术能力，建立 OTA 升级活动的唯一标识（如能够唯一标识具体 OTA 升级活动的软件版本），完善电子控制器（ECU）软件版本编制规则、OTA 升级服务平台 IP 地址和域名信息等备案信息。企业应对升级软件的功能和代码进行验证，保护升级包的真实性和完整性，防范安全风险，确保车辆进行 OTA 升级时处于安全状态。企业应建立 OTA 升级用户告知机制，在执

行 OTA 升级前，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，并应得到车辆用户确认；在执行 OTA 升级后，应告知车辆用户车辆升级的结果。企业应当识别升级活动所影响的系统及电子控制器，并保存软件初始和升级版本（集），保护车辆上的软件版本免受篡改，并能通过标准化的电子通信接口读取软件版本，确保升级目的、影响评估、升级涉及的系统与变更参数、升级的功能与变更参数、升级任务信息等升级活动备案信息真实、准确和完整，支持实施升级追溯管理。

（十四）规范 OTA 升级活动备案。企业应当具有规范化实施智能网联汽车软件 OTA 升级活动备案能力，加强备案统筹管理。企业应当根据《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网网络安全和数据安全工作的通知》等规定，按照汽车软件在线升级备案关于企业能力、车型功能和升级活动等有关要求，通过汽车软件在线升级备案系统向工业和信息化部备案；应当根据《关于进一步加强汽车远程升级（OTA）技术召回监管的通知》规定，按照《关于汽车远程升级（OTA）技术召回备案的补充通知》要求，通过智能网联汽车安全大数据云平台向市场监管总局备案。