疫情冲击下的中国汽车产业加速制度创新和升级（下篇）

作者：封锐　张云

新冠肺炎疫情席卷全球，我国汽车产能艰难恢复，需求端继续承压。2020 年以来，国家各主管部门相继出台政策法规，促进汽车产业发展。本文旨在梳理近期出台与新能源和智能网联汽车相关的重要产业政策和制度，为汽车行业的从业者和关注此行业的投资人提供参考。

本文分为上下两篇，在上篇中，您已经关注到新能源汽车相关的制度创新：

- 新能源汽车准入政策即将调整
- 新能源汽车补助期延长
- 燃料电池汽车以奖代补
- 新能源汽车标准化工作继续推进
- 汽车产业生产者责任延伸制度继续深化
- 推动公共领域用车电动化

本篇为下篇，重点介绍智能网联汽车的制度升级：

- 智能汽车创新发展战略发布
- 车联网产业标准体系框架趋于完备
- 车联网相关的网络数据安全标准体系建设指南征求意见
- 智能网联汽车制造商的采购活动可能受到网络安全审查
- 汽车驾驶自动化分级标准即将发布

智能汽车创新发展战略发布

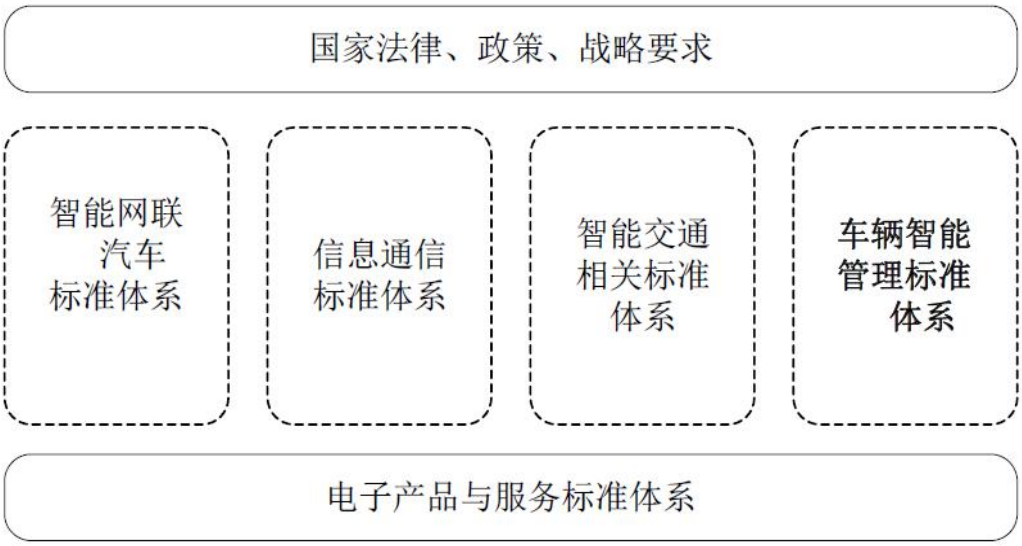
2020 年 2 月 10 日，国家发改委等 11 部委联合发布《智能汽车创新发展战略》，从技术创新体系、产业生态体系、基础设施体系、法规标准体系、产品监管体系和网络安全体系六个方面为中国标准智能汽车产业的发展勾画了发展蓝图。我们认为，其中对于基础设施体系和法规标准体系的顶层设计尤为值得关注。

就中国标准智能汽车的基础设施体系而言，该战略强调：推进道路基础设施的智能化，建设广泛覆盖的车用无线通信网络、覆盖全国的车用高精度时空基准服务能力、覆盖全国路网的道路交通地理信息系统以及国家智能汽车大数据云控基础平台。这些战略目标初步回应了智能汽车发展在 V2X 通信、道路导航、高精地图、交通指挥平台等方面的核心关切。

就中国标准智能汽车的法规标准体系而言，该战略要求：开展智能汽车“机器驾驶人”认定、责任确认、网络安全、数据管理等法律问题及伦理规范研究，明确相关主体的法律权利、义务和责任等。推动出台规范智能汽车测试、准入、使用、监管等方面的法律法规规范，修订完善道路交通安全和地理信息测绘方面的法律法规。这些内容，都是切中要害的研究方向和领域。

车联网产业标准体系框架趋于完备

2020 年 4 月 15 日，工信部、公安部和国家标准化管理委员会联合发布《国家车联网产业标准体系建设指南（车辆智能管理）》。国家车联网产业标准体系整体框架如下图所示：



在上述框架中，智能网联汽车标准体系的建设指南于 2017 年 12 月 27 日发布，与总体要求、信息通信和电子产品与服务相关的国家车联网产业标准体系建设指南已于 2018 年 6 月 8 日发布。目前，仅剩智能交通相关标准体系的建设指南尚未发布。这些建设指南是国家车联网产业标准的施工蓝图，也是理解我国智能网联汽车整体技术架构的重要参照。

车联网相关的网络数据安全标准体系建设指南征求意见

2020 年 4 月 10 日，工信部科技司对《网络数据安全标准体系建设指南（征求意见稿）》公开征求意见并将于 5 月 9 日结束公示。在其网络数据安全标准体系的框架之内，分为基础共性、关键技术、安全管理、重点领域四个大类，而“车联网”正属于数据安全标准体系建设的“重点领域”之一。

根据该征求意见稿，车联网安全覆盖车内、车与车、车与路、车与人、车与服务平台的全方位连接和数据交互过程，数据安全和隐私保护贯穿于车联网的各个环

节。车联网领域的网络数据安全标准主要包括：（1）车联网云平台数据安全，（2）V2X 通信数据安全，（3）智能网联汽车数据安全，以及（4）车联网移动 App 数据安全等。

智能网联汽车制造商的采购活动可能受到网络安全审查

2020 年 4 月 13 日，网信办等 11 部委联合发布《网络安全审查办法》，从 6 月 1 日开始，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，实施网络安全审查。

依据该办法，关键信息基础设施运营者在采购核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务等可能对关键信息基础设施安全有重要影响的网络产品和服务时，应当在与网络产品和服务提供方正式签署合同前申报网络安全审查。如果在签署合同后申报网络安全审查，则应在合同中注明此合同须在产品和服务采购通过网络安全审查后方可生效。审查期限可能长达 45-60 个工作日。如果因监管部门意见不一致进入特别审查程序，整体审查周期可能长达 105 个工作日以上。

公路水路运输领域的重要网络和信息系统运营者，可能被认定为“关键信息基础设施运营者”。对于汽车制造商和售后服务商而言，尽管短期来看可能影响有限，但基于下述因素和趋势，《网络安全审查办法》对其经营活动的影响可能会逐渐增加：

（1） 在智能网联汽车与其制造商以及代表制造商进行数据处理的运营商之间，会发生大量通过传感器、车载芯片和电信网络进行的数据搜集、存储、处理和利用，比如以结构化数据训练和迭代自动驾驶算法，进而通过 OTA 上载不断更新车辆驾驶自动化系统和其它车辆系统。随着品牌内此类车辆上牌量增加，相关的数据安全和信息保护风险也会逐渐放大；
（2） 随着汽车产品的智能化、网联化，每辆汽车均将日益成为一个网络节点，以 V2X 的形式全方位参与网络连接和数据交换，对网联汽车信息系统的未授权侵入及对车辆的恶意控制，将构成对智能网联汽车产业发展和公共交通安全的重大威胁；
（3） 头部汽车制造商正在积极寻求向综合出行服务提供商的角色转变，从而直接进入交通和运输服务行业，运营相关服务网络。

假以时日，每辆智能网联汽车均可能构成公共交通网络和运输服务系统的组成部分，在市场竞争中领先的智能网联汽车制造商和服务提供商，极有可能被认定为关键信息基础设施运营者。汽车产品的智能化和网联化是一个渐进的过程。在这个过程中，汽车生产商需要保持对自身产品技术进步的敏感和关注，在其产品对网络安全和公共交通的影响超过某个临界点时，及时调整工作流程确保合规运营。

汽车驾驶自动化分级标准即将发布

2020 年 3 月 9 日，工信部科技司就推荐性国家标准《汽车驾驶自动化分级》报批稿公开征求意见，并已于 4 月 9 日结束公示。该报批稿基本上采用了与 SAE 标准类似的 0-5 级六级分类，用以界定汽车驾驶的自动化程度。

概而言之：

（1） 0 级自动驾驶大致相当于目前市场上的 ADAS 功能；
（2） 1、2 级自动驾驶仅要求系统持续执行横向、纵向运动控制，并具备相应的目标和事件探测与响应（OEDR）能力。区别在于 1 级仅要求横向*或*纵向运动控制，而 2 级要求二者兼具；
（3） 不同于 1、2 级，3-5 级自动驾驶要求系统可以执行全部动态驾驶任务；
（4） 3、4 级自动驾驶仅要求在在设计运行条件（ODD）内激活和执行全部动态驾驶任务，并均需识别即将不满足 ODD 的车辆状态并基于此提出车辆接管或由系统作出接管；而 5 级则无 ODD 限制；
（5） 3 级与 4、5 级自动驾驶的核心区别在于，3 级系统需配备“动态驾驶任务接管用户”而 4、5 级系统无此角色。基于这种功能限制，3 级系统需要探测动态驾驶任务接管用户的接管能力，并需给其留出反应时间，用户未响应的情况下执行风险减缓策略；而 4、5 级自动驾驶在出现接管需求时（比如驾驶自动化系统失效或车辆其他系统失效），应具备由系统执行动态驾驶任务接管的能力，并自动达到最小风险状态；
（6） 3 级与 4、5 级自动驾驶的次要区别在于，3 级仅需具备识别驾驶自动化系统失效的能力，而 4、5 级除此之外，还需具备识别车辆其他系统失效的能力；
（7） 当用户请求驾驶自动化系统退出时，0-3 级必须立即解除系统控制权，而 4、5 级则可基于存在安全风险暂缓解除系统控制权。

不难看出，上述汽车驾驶自动化分级以及征求意见稿中明确界定的用户和系统之间在自动驾驶过程中的角色分工，是在智能汽车或其自动驾驶系统的设计、制造商与产品使用者之间进行责任分配的基础，对构建相关领域内的归责和举证原则具有重大影响。

结语

2019 年 12 月 3 日，工信部工业装备司就《新能源汽车产业发展规划（2021-2035 年）（征求意见稿）》公开征求意见，其内容既涉及“新能源”，也涉及汽车的“智能化”和“网联化”。其中对“智能网联汽车分级”作出的 5 级划分定义，在短短三个月后就被工信部科技司的《汽车驾驶自动化分级》报批稿所修正，足见此领域内知识更新和技术、政策发展变化之迅速。我们期待这个产业发展规划包含足够的智慧和远见，足以带领新能源和智能网联汽车产业穿越已经到来且可能相当漫长的经济下行周期。