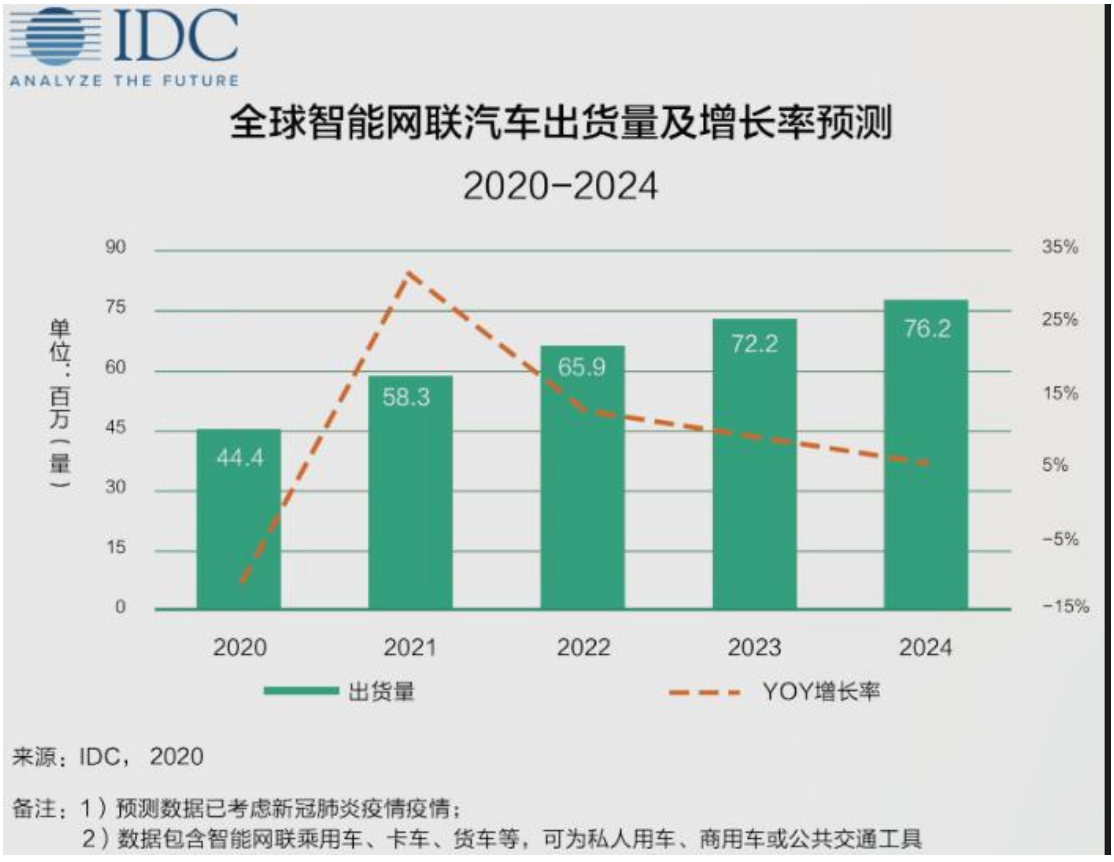
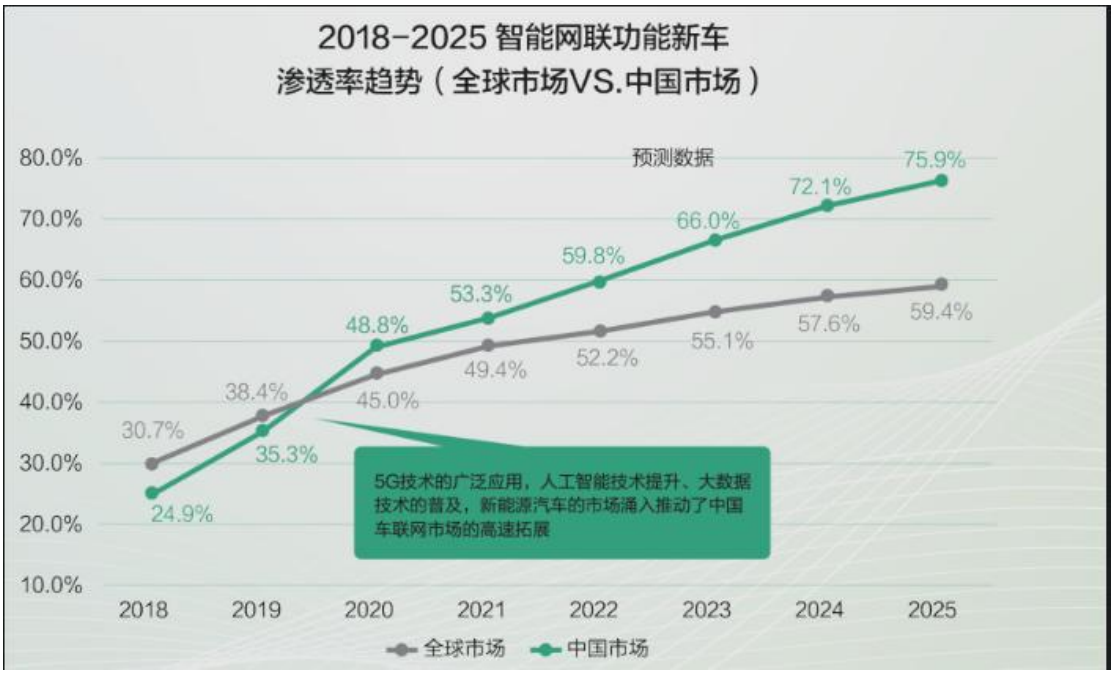
智能网联汽车安全研发体系研究方案

对于智能网联汽车行业来说，2020 年特斯拉市值增长为全球第一的汽车厂商成为汽车互联化、自动化、共享化和电动化发展的标志性事件。尽管受新冠疫情冲击，国内外智能网联汽车依然蓬勃发展。随之而来的不仅有层出不穷的车联网信息系统安全问题，更有各国政府密集公布的各类安全法规和标准。智能网联汽车行业面临的合规要求和安全风险比以往任何时候都更重要、更严峻。我们尝试从法规标准、攻防研究、学术研究发展和建设建议等多个维度总结智能网联汽车信息安全产业的最新发展情况。

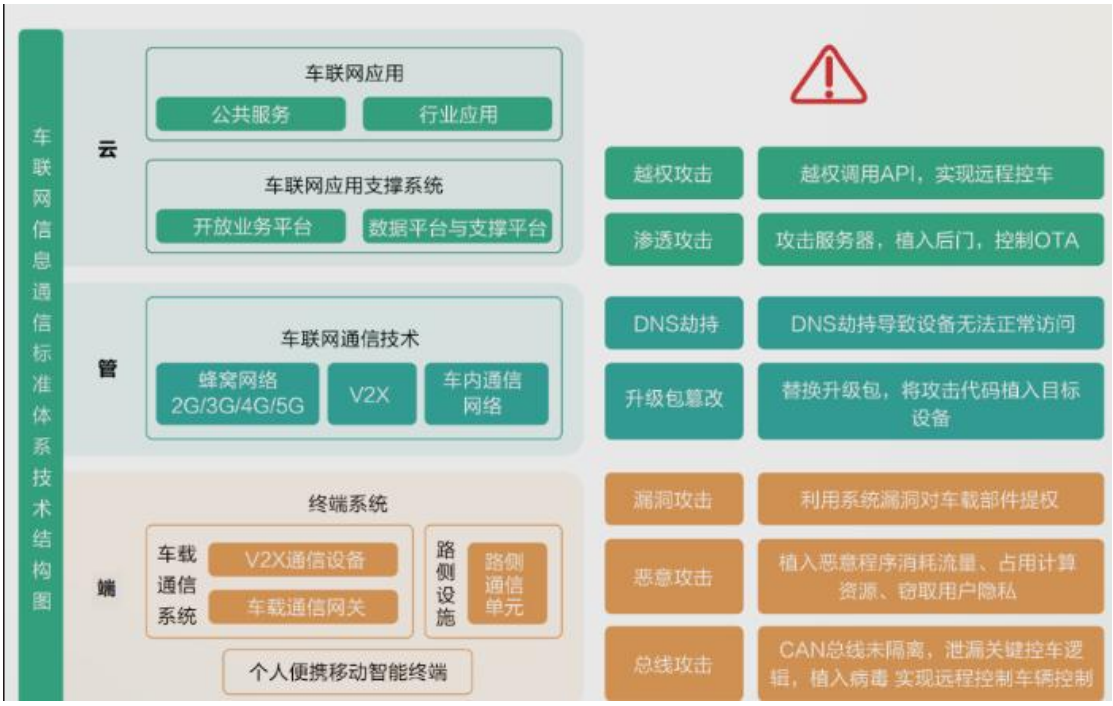


尽管受到新冠疫情的打击，中国智能网联汽车产业依然孕育出新一轮生机。随着汽车"新四化"的进程加速，百年传统汽车产业迎来了大变革，"软件定义汽车"的时代已经悄然来临。智能化、网联化是汽

车行业发展不可逆转的趋势。如智能网联汽车渗透率变化图显示，预计到 2025 年，中国市场 75.9%的新车型将具备自动驾驶和联网功能。

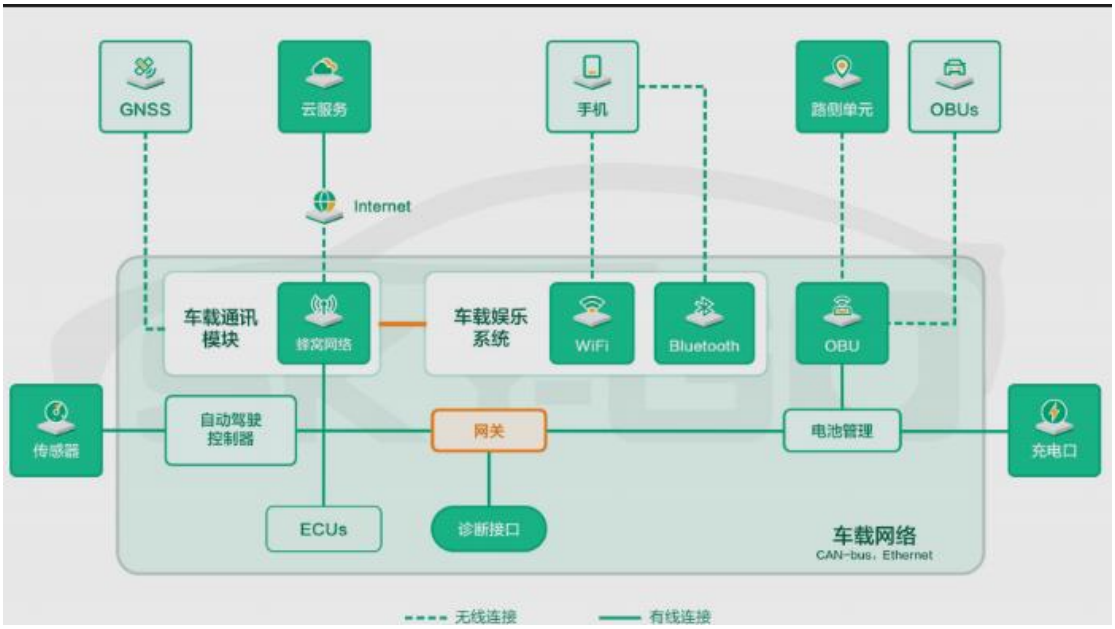


整个车联网信息安全问题主要萦绕在"云-管-端"三个层面。从车端来看，智能驾驶系统、动力系统、车身控制系统以及信息娱乐系统都是智能网联汽车被攻击的对象。



智能网联汽车网络安全是一个复杂系统的安全问题。既包括硬件

安全、固件安全、操作系统安全、应用安全等传统安全问题，还包括数据安全、人工智能算法安全、供应链安全等新型安全问题。车联网以"两端一云"为主体，路基设施为补充，涉及车-云通信、车-车通信、车-人通信、车-路通信、车内通信五个通信场景，而这五个通信场景中都可能存在潜在的攻击路径。



为积极应对车辆的智能化、网联化技术的快速发展，包括中国在内的世界各国都在积极加快体系化政策制定，持续推进建立健全合规体系。

因此为积极应对车辆的智能化、网联化技术的快速发展，包括中国在内的世界各国都在积极加快体系化政策制定，持续推进建立健全合规体系，我中心制定如下研究解决方案：

1. 网络安全工作机制将安全开发生命周期相关的信息安全管理部门纳入智能网联汽车网络安全管控体系中，从汽车规划、设计、研发等各个阶段完整的提供网络安全服务能力，能够从全生命链的维度保障智能网联汽车的整体安全性能。

2．自有远程升级（OTA）更新服务的建立，能够提供智能网联汽车操作系统、固件、应用等软件服务的远程升级更新，通过远程无人值守的方式进行功能更新或安全修复。

3.研发的硬件安全模块，将加密算法、访问控制、完整性检查嵌入到汽车控制系统，进一步加强了 ECU 的安全性，从底层硬件、配套算法等多维层面提升了硬件的安全性能，极大地强化了智能网联汽车的安全防护能力。