

汽车智能驾驶系统安全挑战与对策

► 李克强

智驾系统安全分析

汽车产业已经进入了智能网联时代。智能网联汽车是新一代的移动通信技术、信息技术，包括人工智能在内的信息技术与实体产业结合的产物，是一个已经引起世界各工业强国战略竞争的高地，欧盟、美国、日本等都颁布了国家层面的产业发展战略。我国也高度重视智能网联汽车产业的发展，将其作为我国推动制造强国、交通强国的重大战略任务之一。

在智能网联汽车技术迅速发展、产业快速推进的情况下，智能网联汽车发展的技术趋势、产业趋势已经发生了重大变化。当然，在不断推进的产业化过程中，实现产业高质量发展的战略路径趋势已经明确。从技术趋势上可以看到，智能化和网联化协同发展，基于大模型的汽车人工智能加速应用，智能汽车领域全域安全技术的要求更加明确。从产业趋势看，产品形态、产业生态、出行模式也在快速发生改变。发展战略、路径、趋势已经很清楚，主要有两个方面：一方面，人工智能与智能网联汽车深化融合发展，推动产业技术进步与产业变革；另一方面，“车路云一体化”将成为实现高级别自动驾驶产业发展的必然路径。

快速发展智能网联汽车产业已经成为全社会的共识。迄今为止，自动驾驶分级别产业发展已经取得了重大进展，L2级2025年新车装有量已经接近65%。4G、5G、C-V2X通信模块在快速普及。高级别自动驾驶相关的关键技术，包括传感器技术、激光雷达、芯片、操作系统。产业生态快速发展，起支撑作用的高级别基础设施也在快速发展，政府层面已经在推动相关的示范基地、示范测试区域快速

李克强

中国工程院院士，清华大学车辆与运载学院教授、智能绿色车辆与交通国家重点实验室主任、国家智能网联汽车创新中心首席科学家。



建设。

产业快速发展的同时，我国汽车智能化的产业发展已到了关键的临界点，在发展过程中要真正做到高质量发展、可持续发展，需要尽快解决面临的一系列挑战性问题：

第一，产业智能化的商业闭环、盈利模式尚不理想。原因有以下几点：一是安全可靠不足。自动驾驶首要属性是交通的安全，安全可靠不能保障，客户是不买单的，安全性可靠性不足也就没有形成盈利的闭环。实际在产品定义上很多方面尚未形成技术闭环，开发的成本高，产业协同也不够，企业都在低水平重复，资源不聚焦。

第二，产品的性能特别是安全性问题尚未被社会完全认可。安全性能是第一个亟待突破的问题，具体体现在没有很好的商业闭环，或者正在追寻商业闭环的临界点，产品的安全性尚未得到社会客户的认可。如果从技术来分析，产品定义不准、相关核心技术亟待突破。同时，还要加强法律法规的建设。

产业进步快速推进的同时，安全隐患问题必须解决。现在正在发生的一系列事故会引起社会公众的质疑，安全技术一直是制约大规模商业化的瓶颈。

本文为李克强4月11日在智能电动汽车发展高层论坛（2026）上的主旨演讲，本刊获“车百会研究院”公众号授权转载，略有编辑

当前，智能驾驶存在的固有技术瓶颈，已经成为威胁道路交通安全和智能驾驶规模化健康发展的重要因素，亟待突破。

通过梳理出现的安全问题可以看出，安全失效的问题主要有以下几个方面：

一是物理的感知极限与多维视角的缺失。平常人能看见的东西，常规的目标物，由于感知的遮挡、光线的原因，导致智能驾驶系统存在看不清、看错、看漏等问题，以及传感器物理特性导致的感知盲区，这些传感器物理极限是难以通过算法完成的。

二是长尾场景和少见目标识别失效。少数产品当中，仍然存在智能驾驶由于缺少提前训练、训练场景不足而出现罕见场景无法识别的问题。

三是逻辑决策瓶颈与接管机制失效。逻辑决策瓶颈与接管机制尚需要突破，比如突发难以接管的场景中，由于突然出现的障碍物，无法提前预判，事故风险显著增加。

四是车企算法研发的数据孤岛效应。从开发层面来看，传统的制造业、汽车企业大量投入做数据闭环，各个企业后续数据的收集、数据训练在平台上存在一系列问题，包括单车数据有限、车载传感器物理的限制、不同车机采集数据类型的不一致，各

家独立，无法共享，以及数据安全保障机制不足等，都限制了开发。

上述技术与工程痛点从技术层面概括为三点：

一是单车感知能力受限；二是端到端模型可靠性不足，AI大模型训练数据尚不全面；三是现在的产品架构都是烟囱型架构，缺乏统一基础底座，带来开发成本高、研发质量与效率低等问题，因此行业亟需一套面向差异化业务场景，并具备低代码、可快速重复迭代的计算机平台及开发系统。

行驶安全提升技术

智能网联汽车安全保障一定要有新范式出现。

新范式分为几个部分：感知维度方面，从“视觉内平视”到“超视觉的全感知”；决策逻辑方面，从“独立博弈”到“协同最优”；安全防线方面，要从“被动防御”到“内生安全”；产业生态方面，不仅仅从“造车竞争”到“生态共建”，也要按这样的思路推进系统的安全性能提升。

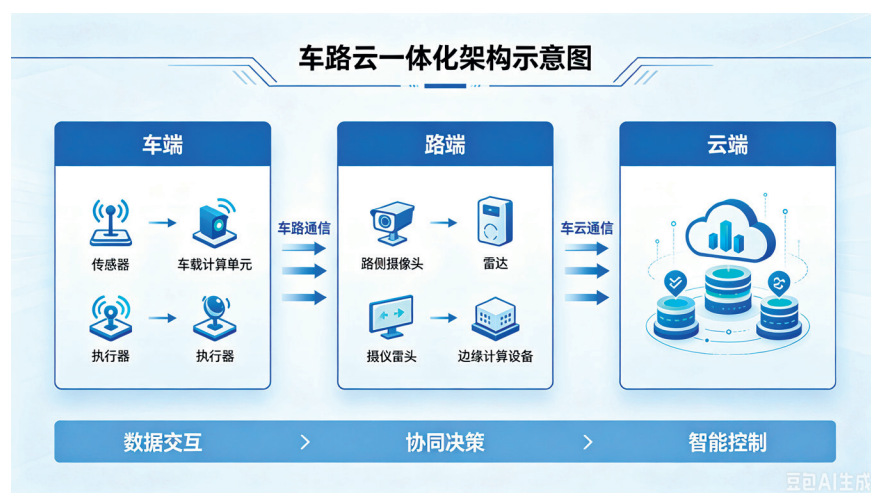
围绕“车路云一体化”体系架构，未来汽车的发展，要从传统意义上的单车智能、现在车企在云端的车云协同，最终达到“车路云一体化”协同发展的最理想的发展状态，只有通过技术整体架构设

单车智能-车云协同-车路云一体化的发展路线



车路云一体化系统通过分层解耦、跨域共用，可支撑不同的应用，包括智能驾驶系统的实时类和非实时类各种应用需求。“数据闭环”模式是车路云一体化的一种初级形态，而车路云协同下的“数据闭环”模式成本更低、效果更好。





绕“车路云一体化”架构，国家工信部、公安部、交通部等部委，在推动两个大的示范项目，一个是高级别L3级的城市准入和城市准入示范，另一个是要达到高级别自动驾驶需要基础设施支撑的“车路云一体化”示范。

产业化解决方案

2025年已经有15家国内

计，才能真正意义上解决上述安全问题。

“车路云一体化”的架构设置，能够对解决当前的安全问题提供系统性解决方案，具有多项核心优势：

一是为智能汽车行驶建立了安全的“数字轨道”。自由开车和在轨道上开车的要求不一样，比如传统的单车智能，去年有一家媒体做试验，高速之下，没有哪一家企业的自动驾驶系统能在前面突然躲闪后做到避免与头车碰撞。如果有了数字轨道，就能够真正意义上做到提前感知，规避风险。

二是为AI大模型训练建立了提升安全的“数字发电站”。提到AI大模型，AI有三要素，AI的数据也有三要素，即准确性、海量性、完备性。现在各家企业单独收集的数据，即使够多但也不全，数据多和全是两个维度，有了车路云一体化这套系统以后，通过上帝视角，再加上各个车的数据汇聚，再变化回车端训练，这样才能够真正做到提升安全的“数字发电站”。

三是CBDES是高质量算法开发的“基础底座”。针对现在的烟囱型架构，通过“分层解耦、跨域共用”方式，可以用低代码快速开发，提高开发效率。

在国家相关项目的支持下，推动“车路云一体化”系统的发展，能够在本质上解决安全问题。围

外主要车企联合在“车路云一体化”系统架构下开展了示范，包括中国一汽、东风汽车、长安汽车、丰田、比亚迪、蔚来、吉利等，一起来推动产业化示范相关场景，验证是否能解决前面提到的几大场景问题。

“车路云一体化”架构有完全可行的商业模式。有了路侧单元、通信标准以后，不仅能跟车企自家的数据单元打通，更重要的是数据汇聚到路侧单元的边缘云、区域云、中心云的三级技术平台，形成可以自主支撑的闭环，来解决上述几大关键问题。

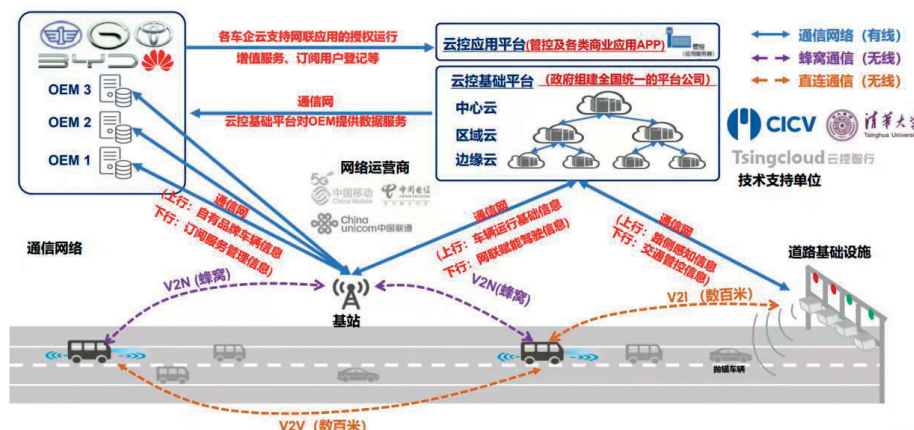
“车路云一体化”示范主要针对车企提出的17个应用场景，其中5个是去年媒体公布的都过不了关的场景，包括网联式前向避碰辅助、网联式滤波车速引导、网联式匝道汇入/汇出、鬼探头、网联式导航辅助驾驶场景。去年相关实验已经做完，今年正在做量产化推进。

针对“车路云一体化”系统架构现存的问题，也是大家都在讲的自动驾驶难以突破、难以做商业闭环的几个问题，业界在做各种尝试和推动：

一是网联式前向避碰辅助。目前在长春、北京、重庆等城市，我们都在推动安装这样的产品。

二是网联式绿波车速引导。司机想要一路遇到绿灯，现在用导航去做，很难。系统做好以后，在北京、重庆能连续通过5个以上的红绿灯路口，这是当前

车路云一体化系统运行商业模式概要



成本最低、普及范围最广，现在都在作为产业化试点的场景。

三是网联式匝道汇入 / 汇出。国外车企认为这是最容易出事故的场景。三辆车，后面车减速、前面车加速，无缝合并，这对安全、效率来说也是场景的刚需。

四是有遮挡的 VRU 安全辅助。用到“车路云一体化”系统以后，车在遇到“鬼探头”的情况下怎么做到安全通过，这样的试验也在推进。

这样一系列示范，去年在北京的 WSCV 世界智能网联汽车大会、重庆的中国汽车工程年会上都做了完整的产业化应用示范，示范以后得到非常好的结论，这是一项可行的没有成本增加且能够显著降低安全风险的技术。

结束语

首先，安全依然是行业亟待解决的首要问题，正视单车智能驾驶技术瓶颈是解决问题的首要前提，行业需摒弃急功近利的心态，时刻敬畏技术局限，回归安全本源，以系统工程思维，多维并举，筑牢智能驾驶技术守护生命的价值基础。

其次，“车路云一体化”系统为车辆提供多维数据输入。实现车、路、全域协同感知，增强环境

感知与风险预判能力，为智能驾驶汽车建立“数字轨道”，提升智能网联汽车驾驶安全性与通行效率，支撑智能交通高效稳定运行。

然后，“车路云一体化”系统的数据兼具“海量性”与“完备性”。融合车辆自主上报、路侧感知与交通指挥信号、交通事件等全维度数据获取模式，打破数据孤岛，为 AI 大模型训练建立提升安全的“数字发电站”，在保障智能驾驶安全的同时，降低模型训练成本，提升训练效率。

最后，计算基础平台和开发系统提升产品安全研发质量和效率。通过拆解复杂应用软件建立起来的功能组件库，实现分层解耦、跨域共用，提高模块复用率，并通过图形化工具实现低代码开发，降低开发难度和成本，支撑“车路云一体化”智能驾驶产品的安全高效开发。

当前，智能驾驶已进入规模化应用攻坚阶段。既要充分认识单车智能存在的技术局限，牢牢守住安全底线，也要坚定不移推进网联协同技术路线，坚决摒弃急功近利的发展模式。加快构建功能稳定可靠、覆盖范围更广的协同感知环境，为系统建设提供多维度、海量高质量训练数据，支撑智能驾驶产品安全高效研发应用，推动智能网联汽车在交通出行服务与城市综合治理方面实现深度融合应用。