自动驾驶卡车

量产白皮书

赢彻科技
INCEPTIO TECHNOLOGY

序言

量产正成为自动驾驶行业的主旋律。同时，正向设计、前装量产自动驾驶系统和整车的技术挑战极大，行业普遍感到相关能力稀缺，知识经验较为匮乏和碎片化。经过赢彻科技与中国卡车主机厂近三年的联合开发，搭载赢彻科技全栈自研 L3 级别自动驾驶系统的智能重卡于 2021 年底成功量产，得到干线物流用户认可，规模化生产和运营投放节奏开始加速。赢彻科技的技术团队将三年量产的实践与探索做了深度总结与复盘，并撰写成《自动驾驶卡车量产白皮书》，与行业共享共创。

此白皮书在以下领域分享赢彻科技的自动驾驶量产开发方法论和技术创新：

- 一套针对自动驾驶卡车使用场景的系统性正向功能定义方法。融合了功能安全和信息安全的标准与规范，并配套完整的指标体系和测试方案。
- 一套完整的自动驾驶卡车量产开发体系与全栈自研的核心技术。覆盖车端和云端的全部构成，包括自动驾驶（感知、定位、规划控制、节油、系统软件、自动驾驶域控制器和硬件套装）、电子电气、线控底盘、人机交互、网络安全、云基础设施和数据闭环。分享了在成本、安全和物流运营多重苛刻要求下的自动驾驶重卡核心技术创新与工程优化，介绍了量产后里程数迅猛增长情况下对高效数据闭环的探索与实践。
- 一个以“正向开发、兼顾敏捷”为原则的自动驾驶卡车研发流程体系。将汽车行业的 V 模型开发流程与软件行业的敏捷开发模式进行了创新性融合，首次将高阶自动驾驶开发过程融入卡车整车开发的全流程，并建立了业内最完整的自动驾驶卡车量产测试验证体系。
- 一个贯穿研发到量产全周期，涵盖整车到核心系统，跨越赢彻科技全组织，并协同多个量产伙伴的自动驾驶安全开发体系。从流程安全、整车安全和系统安全三个维度入手，为自动驾驶卡车实现充分的可靠性和安全性（Safety and Security）。针对自动驾驶技术在车辆安全方面的全新挑战，在量产过程中持续改良，务实探寻新方案。
- 一个具备自我演进能力的全新无人驾驶技术路线。赢彻科技针对当前主流算法和系统架构的潜在瓶颈，提出一个端到端深度神经网络方案，并通过结合深度强化学习 DRL（Deep Reinforcement Learning）和神经辐射场 NeRF（Neural Radiance Fields）技术的仿真器来训练端到端模型，实现自动驾驶能力的高效自我演进，最终走向无人。

在量产开发过程中，我们深刻感受到：

- 自动驾驶技术的前装量产要求涵盖自动驾驶整车和全部核心系统的技术能力和非常完整的开发体系。量产成功需要遵循木桶理论，不能有任何短板。这对自动驾驶公司普遍追求的全栈自研提出了更高的能力要求，不仅要能自研算法、软件和自动驾驶域控制器，还要能够与产业伙伴共同开发线控底盘、电子电气架构和人机交互系统，并且具备极为完整严格的整车测试验证能力和丰富的供应链与生产管理能力。需要对车辆的正向研发和前装量产保持高度敬畏，耐心积累。
- 卡车自动驾驶的技术创新和工程极致，来源于对卡车物理特性、苛刻安全要求、量产一致性、成本压力、运输时效和安全员特点等多重挑战的深度认知和极致追求。这是技术的真正源动力，对自动驾驶的算法演进、架构创新和工程实践提出了更高的要求。
- 自动驾驶推动汽车走进深度学习和软件定义汽车的新时代，也带来了整车正向开发的严谨性、软件开发的敏捷性、自动驾驶算法与需求的不确定性之间的巨大冲突。问题和冲突远未解决，需要全行业一起不断实践，融合创新。
- 人机共驾在相当长时间内是高等级自动驾驶落地应用的主流模式，与安全密切相关，对商用车人力成本优化和乘用车驾乘体验影响极大。全行业的实践积累还非常有限，需要从人因工程和安全设计切入，大力发展。
- 走向无人的道路上，当前主流的自动驾驶技术栈可能首先在监督学习所需的海量数据获取效率与代价、经典的机器人框架等方面遇到瓶颈。需要更多富有想象力的新方案，百花齐发，加速探索。

这本白皮书汇集了东风商用车有限公司、中国重型汽车集团有限公司等卡车自动驾驶产业链上下游五十余家合作伙伴的群体智慧。“前沿创新、极致求实”的共同技术价值观和“安全高于一切”的共同理念，凝聚所有量产伙伴携手前行。

我们本着极度坦诚的态度，透过这本白皮书分享赢彻科技和产业伙伴的早期量产实践和前沿探索，其中定会有未尽和不足之处。非常期待大家通过 whitepaper@inceptio.ai 反馈指正，一起共享共创，推动自动驾驶产业完成量产的关键一跃！

目 录

CONTENTS

CHAPTER 1

第一章

用户需求与技术挑战

1 干线物流用户需求与痛点

中国干线物流行业现状

万亿级市场，规模巨大。由中重卡承运的干线运输占到整体公路货运市场的 82%，全国中重卡保有量约 730 万台[1]，市场规模达 4.6 万亿元[1]，体量全球第一，超过同城物流及乘用出租市场规模之和。同样，在世界上其他主要经济体，干线运输都是规模最大的物流细分市场。

运营成本非常高，成本管理以 TCO（Total Cost of Ownership，全生命周期成本）为导向。油耗和人力成本占到单车年度 TCO 的 50% 以上，存在巨大优化潜力；而车辆购置成本仅占约 10%，若高端车型可使整体 TCO 优化，则购车决策者不会仅拘泥于初始车辆购置成本的增加。

劳动密集型行业，复杂低效。运输的安全、时效和油耗情况高度依赖于驾驶员个体的驾驶能力、责任心和身体状况，驾驶员个体差异巨大，运输管理复杂。

典型重卡年度 TCO 构成

主要成本项	油耗成本	路桥费用	人力成本	车辆成本	其他	合计
年度成本（万元 / 年）	~35	~35	~25	~12	~13	~120
占比	30%	30%	20%	10%	10%	100%

干线物流主要痛点

驾驶员难招难管，人力成本高

目前，我国卡车驾驶员缺口持续增加。由于工作环境恶劣，造成驾驶员难招难管、供需失衡、人力成本上升等问题。国内卡车驾驶员招聘的年龄要求已从 24-50 岁放宽至 22-60 岁，仍难以招募，25 岁以下年轻人仅占 1.4%，行业驾驶员缺口高达 1000 万人[2]。

为应对长时间高强度驾驶的疲劳风险，在以快递快运为代表的高密度长途干线运输中，每车往往需 2-3 名驾驶员轮班，导致人力成本进一步增加。

油耗高度依赖个体驾驶员表现，极难管控

油耗成本是公路物流成本的重要组成部分，约占整体成本的 30%[3]。然而油耗水平的个体差异较大，优秀驾驶员（拥有多年驾龄的高水平驾驶员）油耗表现较行业平均油耗水平可节省约 9%[4]。

安全问题频发

据《中国公路货运行业智慧安全白皮书》披露，2019 年我国公路货运百万公里事故数为 3.7[5] 起；而基于对头部快递快运公司的访谈，当前人工驾驶场景下，赔付成本超过 5 万元人民币的百万公里事故率为 0.1~1 次。

自动驾驶技术的潜在价值

降低人力成本，解决驾驶员供给不足问题

L3 级自动驾驶技术能够大幅度降低驾驶员劳动强度，并有机会在双驾线路上减少 0.5-1 名驾驶员。未来的 L4 级自动驾驶技术可以进一步实现完全无人驾驶，从而显著降低 TCO。

节约能耗，降低排放

通过学习最节油人类驾驶员的驾驶行为，自动驾驶系统可以首先达到人类驾驶员的顶尖节油水平；再通过更长感知、更优规划和更精控制，自动驾驶有望超越优秀人类驾驶员水平。

提升货运安全系数，降低事故发生率

自动驾驶卡车可以避免因人类驾驶员能力局限或车辆故障导致的事故发生，也可避免人类驾驶员的疲劳、分心等危险驾驶行为，从根本上实现比人类驾驶员更安全的驾驶，提升货运安全系数。

经赢彻科技初步测算，相较人工驾驶，自动驾驶技术在中国干线物流市场有机会实现：

- 每公里运费降低 5%-15%
- 每年碳排放量减少 950 万 -3800 万吨
- 每年为干线物流创造 2500 亿 -1.3 万亿元的经济效益

信息来源：

1: BCG《中国公路货运市场发展趋势》

2: 中国物流与采购联合会《2021 年货车司机从业状况调查报告》

3: 全国道路货物运输价格指数

4: 2018 沃尔沃卡车节油挑战赛比赛数据

5: 普华永道、G7、中国交通报《中国公路货运行业智慧安全白皮书》

2 自动驾驶卡车前装量产的要求

赢彻科技成立伊始即选择正向设计、前装量产的路线，以实现自动驾驶技术的产品化，这是自动驾驶卡车实现安全可靠、合法合规和规模化商业投放的唯一路径。

2.1 自动驾驶卡车的特点与挑战

赢彻科技专注于重卡的自动驾驶。重卡主要运行在相对封闭的高速公路，相较城市道路场景看似更简单。但是，由于重卡特有的物理特性、运行环境和商业运营要求，相较于乘用车的自动驾驶系统，重卡的自动驾驶系统对车辆的感知距离和精度、系统响应速度以及车辆控制的精准性都提出了更高要求：

- **很长的制动距离。**重卡在 100km/h 车速下的制动距离通常超过 100 米，相较于乘用车在 40 米以内的制动距离，要求自动驾驶系统需要具备更远的感知距离，以及更快的端到端响应速度。
- **外形尺寸和重量巨大。**重卡外轮廓尺寸标准宽达 2.55 米、高达 4 米、长度最长可达 17 米，在不同挂车装载下整车质量变化高达 500%（9 吨~49 吨），车头与挂车之间的非刚体连接和挂车惯性，增加了自动驾驶控制的难度。此外，重卡运行环境复杂，经常面对各种不同的道路环境，如低附地面路面、碎石路面、非标准车道等，对重卡自动驾驶的规划控制提出了更大挑战。
- **重卡线控系统的响应速度更慢，精度也相对更低。**以制动系统为例，重卡普遍采用气制动技术，相比于乘用车的液压制动需要更长的建压过程。重卡的制动系统响应时间通常在 400ms 左右，而乘用车可以做到 100ms 以内。克服被控系统的延时、实现精确控制，给自动驾驶控制系统带来了比较大的挑战。
- **重卡车辆参数的公差范围大，随着行驶里程的增加，车辆参数会出现更大范围的漂移。**以方向盘转角偏置为例，乘用车出厂时为 1°以内，重卡出厂时可以达到 7°。再以方向盘空行程为例，有实验数据表明，运营时间 12 个月的重卡，空行程相较出厂时劣化 43%，从平均 8.4°劣化到超过 12°。上述方向盘参数公差问题要求自动驾驶控制系统有能力及时识别到参数的变化，并及时加以自动修正。
- **干线物流场景下的综合平衡要求。**干线物流场景对重卡运营提出了安全、时效和成本三大方面的要求，这三方面要求形成了一个此消彼长的三角关系。例如，如果追求时效，则意味着更快的平均车速，但却导致更高的油耗，并对安全提出了更高要求。对于整个自动驾驶系统而言，需要综合考量，在保障安全的前提下，给出全局最优解。

2.2
自动驾驶前装的必要性

法规标准的要求

在中国，要让一辆智能卡车（辅助驾驶或自动驾驶）合法合规地上路行驶和开展商业运营，必须依据相关法规标准，通过工信部等部门的产品认证，取得车辆产品公告资质和车辆运营资质。因此，任何购买车辆进行后装改制的方案只能用于试验场内，无法合法地大规模上路和开展商业化运营。

复杂的整车系统交互

自动驾驶系统作为车辆的关键系统，需要整车层面多方面系统设计的配合，包括底盘系统、动力总成、车身系统、人机交互系统、网联系统等。只有前装的正向研发模式才能满足如此复杂的系统交互要求，而后装的改制模式只能实现基础功能，无法满足安全和性能所必需的全系统设计要求。以 L3 级别自动驾驶的转向系统为例，后装改制模式只能沿用传统转向机，设计时无法考虑安全员在自动驾驶模式下手扶方向盘的使用场景，可能出现由于安全员手力矩干扰导致转向器输出角度追踪不到位的问题，进而产生“画龙”的安全风险。

可靠性与耐久性要求

商用车的运营环境对产品的可靠性和耐久性要求非常严苛，零部件选型和整车系统集成设计与开发都需要符合相应的严苛标准，且通过严谨的测试验证得到确认。以摄像头为例，在正向开发中，一方面，零件本身必须通过一系列的机械性实验与各类环境性实验；另一方面，摄像头需要和支架、线束、接插件、护罩、玻璃等关联部件共同设计、测试，通过整车级的车规试验标准考验。后装产品仅能关注零件自身的功性能，无法在整车布置设计时通盘考虑自动驾驶系统的全场景要求，如散热与通风的设计缺失，导致视野前玻璃易起雾，造成系统可用性不满足要求。

2.3
自动驾驶卡车前装量产的开发原则

自动驾驶车辆的开发一般始于改制的概念验证车，但完成概念验证和路测只是自动驾驶量产道路上的一小步。为了实现大规模前装量产，需要在设计与验证、批量生产和维护、商业化等方面满足广泛而严苛的要求。

在量产开发实践中，赢彻科技总结出指导自动驾驶卡车量产开发的 8 项原则。

赢彻科技 - 自动驾驶卡车前装量产的八项开发原则

原 则	要 求	说 明
安全至上	全天候 全生命周期 功能安全 Fail-Operational 信息安全	以明确定义的功能安全目标和 Fail-Operational 作为总体安全目标，从流程安全、整车安全和核心系统安全三个维度进行设计和实施，确保整车、自动驾驶等各子系统和零部件均达到安全目标，在大规模制造和部署的情况下仍可实现全生命周期和全天候的安全目标 自动驾驶系统需能有效应对各种天气、动静态目标和道路环境，实现规模部署条件下的全天候安全运行 车上软件代码符合 MISRA 和 AUTOSAR 标准
正向前装	正向开发 V 模型开发流程	从整车层面出发对多个系统进行全方位匹配设计，达成自动驾驶的全部功能性能和安全目标 开发始于全面正向设计，对自动驾驶卡车全部相关系统提出需求定义，包括自动驾驶系统，电子电气架构、线控底盘、人机交互、和其他整车集成要素 针对设计逐级进行测试验证，确保功能性能和可靠性达标
车规标准	整车产品认证 零部件车规 算力优化	整车要满足各项法规标准要求，通过产品认证、取得产品公告目录，才能合规生产、合法上路 零部件要满足车规级要求，通过 DV、PV 和 PPAP 认证。商用车对硬件的电气、电磁兼容性、机械、环境耐久、振动、寿命等有更高要求，尤其在振动和寿命方面，如耐久寿命要达到 2 万小时 自动驾驶系统需能够在车规要求下进行算力使用等方面的优化，以应对车规级器件相比普通器件可高达 50% 的性能下降

规模生产	算法适应性 生产效率 制造质量	自动驾驶系统相关算法需具备自适应调整能力，以应对大规模量产车辆的生产尺寸公差和底盘性能差异等 针对自动驾驶系统进行量产产线工艺优化，下线车辆的节拍达到分钟级 严格控制产线的装配、检测和标定等关键过程，确保制造质量
可靠耐久	系统稳定性 环境适应性 使用寿命	重卡在全生命周期内、全天候运行都要有足够高的可靠性和稳定性，并且寿命要达到 120-150 万公里 自动驾驶软硬件系统需进行专门的高可靠性设计 自动驾驶系统和整车需经历严格的仿真和道路测试，并通过寒区和热带等环境试验以及耐久试验考核
维护简易	诊断便利性 维修效率 维修成本	自动驾驶系统需具备车云协同能力，支持远程车辆状态监控和管理，通过云服务对车辆问题进行自动分析并反馈到售后支持 开发专用售后诊断工具，普通维修站操作技师就可进行维修
交互友好	易用性 客户体验	人机共驾阶段的人机交互设计应能够有效地帮助安全员获取到自动驾驶相关的关键交互信息，提升对系统的信任，减少使用过程中的焦虑与疲劳 驾驶员只需非常简单的培训
成本最优	公里成本最优 管理成本最优	卡车用户为总体拥有成本 TCO (Total Cost of Ownership) 导向。自动驾驶系统的设计和量产应通过人力成本、能耗成本、维保成本等的降低，真正带来单公里成本的优化 卡车自动驾驶技术应通过提升安全员体验、显著降低疲劳和事故发生率，来降低安全风险和安全成本，降低驾驶员日益难招难管引起的管理成本上升。最终，通过无人化本质上降低管理成本

2.4
赢彻科技的自动驾驶重卡量产进程

赢彻科技分别与中国领先的重卡主机厂东风商用车有限公司及中国重型汽车集团有限公司于 2019 年启动了 L3 能力级别智能重卡的联合开发和量产合作。

项目合作严格遵循**正向设计、前装量产**的原则，赢彻科技全栈自研重卡自动驾驶系统，包括算法、软件、自动驾驶域控制器 ADCU（Autonomous Driving Control Unit）和线控底盘接口。赢彻科技与主机厂在整车集成、线控底盘、电子电气架构、网络安全、人机交互和功能安全等方面进行了正向联合开发。

赢彻科技和主机厂协同 50 多家产业链上下游合作伙伴，在传感器、自动驾驶域控制器（ADCU）、线控底盘、人机交互等核心零部件和系统层面进行了紧密合作，推动行业在零部件和系统的车规级可靠性、功能安全和人机共驾体验方面首次达到量产要求。

2021 年底，赢彻科技与主机厂伙伴联合开发的首个自动驾驶智能卡车车型实现量产，并成功投放商业运营。

历时 3 年时间，赢彻科技不仅开发了行业首个面向量产、全栈自研的卡车自动驾驶系统，而且在与主机厂伙伴联合量产开发的过程中，共同实现了多个行业首创：

- 创新性的卡车自动驾驶算法：有效克服了重卡独有物理局限和量产限制条件带来的挑战，实现了一套能满足重卡应用场景的感知、定位和规控算法。
- 全自研的自动驾驶系统软件：不但为卡车自动驾驶系统提供高性能、高安全、高可靠的中间件服务，也为产品研发效率提供了强大的支撑，创造了一个更友好的集成环境。
- 卡车领域首个全冗余、高算力、车规级的自动驾驶域控制器（ADCU）。
- 行业首个域集中式全冗余、多通讯链路、具备整车 OTA（Over The Air，在线升级）能力的电子电气架构。
- 行业首个全冗余线控底盘，涵盖冗余转向、冗余制动和冗余电源。
- 行业首个车规级硬件套装认证，包含多传感器融合和计算单元冗余，性价比有竞争力，全面实现量产。
- 行业首个多模态全冗余人机交互系统，具备听觉、视觉、触觉等多重提醒功能。
- 行业首个商用车全方位网络安全设计方案，涵盖云、管、车端入口、车内网络等，可应对多种商用车应用场景攻击。

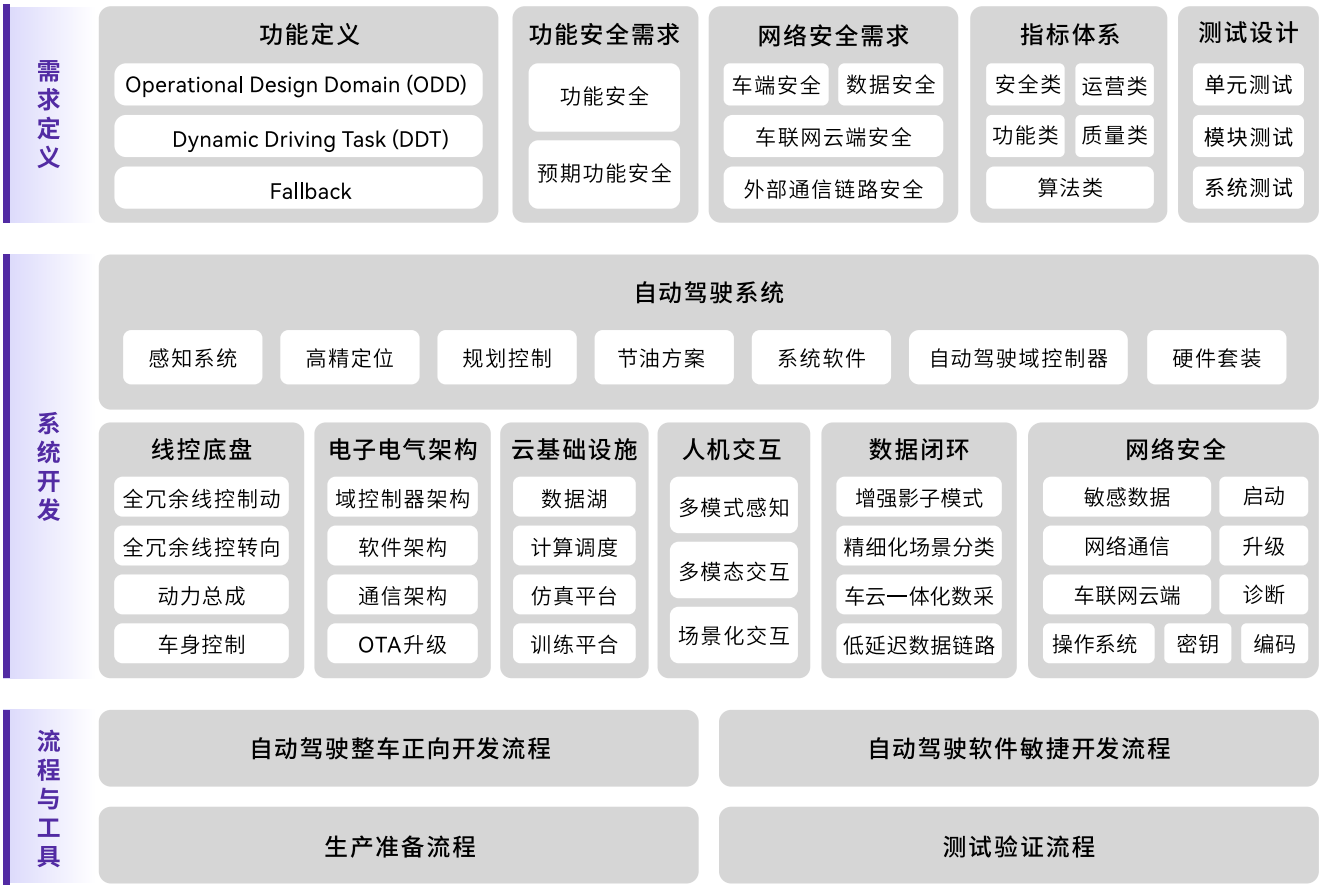
CHAPTER 2

第二章

赢彻科技
自动驾驶卡车量产方法论与实践

1 自动驾驶卡车量产方法论概述

经过历时 3 年的自动驾驶重卡开发与量产，赢彻科技形成了一套较为完整的自动驾驶卡车量产开发体系。



* 图：赢彻科技 - 自动驾驶卡车量产开发体系

这个体系完整覆盖了自动驾驶卡车的核心设计任务，并进行了大量的技术创新与产业融合：

- **需求定义：**首次提出了针对自动驾驶卡车使用场景的正向功能定义方法，融合了功能安全和信息安全的标准与规范，并配套完整的指标体系和测试方案。
- **系统开发：**完整深入地覆盖了自动驾驶卡车在车端和云端的全部构成，包括自动驾驶、电子电气、线控底盘、人机交互、网络安全、云基础设施和数据闭环。
- **流程与工具：**将汽车产业的 V 模型开发模式与软件行业的敏捷开发模式进行了创新性融合，首次将高阶自动驾驶开发过程融入卡车整车开发的全流程，建立了业内最完整的自动驾驶卡车量产测试验证体系。

2 需求定义

2.1 正向设计的功能定义

符合前装量产标准的功能定义，当前对于自动驾驶而言极具挑战。一方面，自动驾驶尚在早期，功能定义的原则、方法和需求范畴均不成熟。另一方面，前装量产遵循正向设计的原则，要求自动驾驶的功能定义严格符合 V 模型，即功能定义作为整个开发活动的起点，能系统性地讲清楚需求和设计，并为验证和验收提供输入和依据。

为了应对上述功能定义方面的挑战，赢彻科技采用了循环往复、逐步深入的三个步骤：

* 图：赢彻科技 - 自动驾驶系统功能定义三步骤

DDT/ODD 定义

按照 SAE 3016 标准的指导，高级别自动驾驶的核心定义要素有三个方面：

- 运行设计域 ODD（Operational Design Domain），即自动驾驶功能所要应对外部环境；
- 动态驾驶任务 DDT（Dynamic Driving Task），即自动驾驶关键的驾驶行为表现；
- Fallback，即自动驾驶应对自身能力边界或者系统异常时的人机交互。

为完成上述三个核心要素的定义，行业里有多种不同的路径。以 DDT 作为切入点为例，将自动驾驶关键的驾驶行为拆分为多个功能。在这些功能中，除了常规的巡航、跟车、车道居中控制等，赢彻科技还结合商用车和干线物流运营的特点，增加了智能避让、高速拥堵辅助、全局速度规划等安全和时效相关的功能。

在对每个功能进行定义时，都会着重思考其在高速干线上的行为表现，尤其是面对 5 大类 60 余种 ODD 要素组合形成的复杂环境。同时，对于每个功能，还要定义其在应对系统异常、车辆异常、环境异常和安全员状态异常等情况下的 Fallback 交互策略以及 Fallback 接管过程中的控车行为，必要时切换至冗余系统进行安全停车。在赢彻科技看来，DDT/ODD 定义的完整步骤，需要结合实际的 ODD 场景，全面地设计好每个功能在正常和异常时的行为表现。

示例

DDT/ODD 定义示例

DDT	ODD					Fallback
	基础设施	操作限制	目标物信息	环境条件	区域条件	
智能避让	**车道线实线**：抑制借道避让 **隧道**：抑制避让等	**车速范围：**在（30KPH，80KPH）内允许触发等	**超宽车：**触发避让 **锥桶：**触发避让等	**NA**	**GPS 信号弱区域：**抑制避让等	**系统异常：**避让过程中侧向感知异常触发接管提醒并取消此次避让等
巡航及跟车	**无车道线**：切换为 LCC（Lane Centering Control）模式 **匝道**：调整巡航目标车速为匝道限速	**车速范围：**跟车车速范围（0KPH，100KPH） **跟车时距范围：**（2s，4s）等	**限速标志：**调整巡航目标车速为道路限速等	**光照：**支持夜间运行等	**NA**	**环境异常**：跟车过程中遇到大雨触发接管提醒 **车辆异常**：巡航过程中制动系统异常触发接管提醒并使用冗余系统安全停车等

专项研究

如果说 DDT/ODD 定义的步骤侧重于功能定义的广度，旨在综合全面地考虑如何应对不同 ODD 下功能正常和异常，那么专项研究的步骤则侧重于功能定义的深度，以便解决特定的重点难点问题。为此，赢彻科技设立了多个不同类型、跨不同功能的专项。

以进出匝道优化为例，该专项研究涉及了导航功能的精准有效、车道级路径规划功能的同步匹配、智能变道功能的及时执行以及匝道内巡航功能的限速调整和大曲率弯道控车优化等。专项研究的步骤，需要每个细节都经过深思熟虑和反复推敲，深刻理解和定义具体场景下的功能表现。

示例

专项类别及示例

专项类别	专项举例
驾驶行为类	进出匝道优化；避让抑制时邻道目标车跟车策略优化等
性能指标类	重刹优化等
系统稳定性类	诊断策略精准化等
人机交互类	系统启动过程信息透明化等

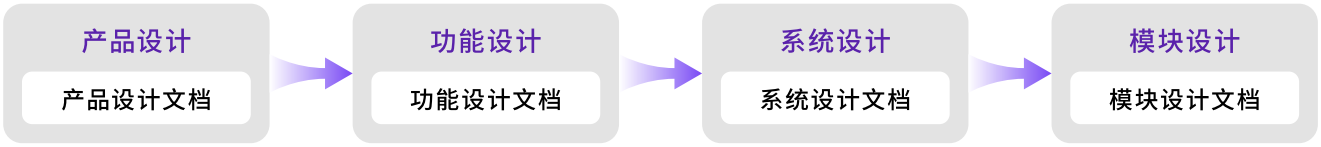
冲突融合

自动驾驶是个高复杂度的产品，按照细化功能开展DDT/ODD 定义和专项研究，能有效地将复杂问题具体化、简单化。但自动驾驶本身是一个完整的产品，不同功能最终要在一个系统内进行融合。功能融合的本质是冲突管理。在这一点上，赢彻科技的实践经验是加强事前管理以预防冲突发生。每个功能的定义都要经历产品设计、功能设计、系统设计和模块设计的过程。

通过不同功能团队对上述设计文档的详细评审，能有效地提前发现功能定义过程中的冲突，并及时采取有效措施进行干预，最终融合成完整的产品。

除了上述的方法论之外，赢彻科技在开展功能定义时，还坚持两个重要的理念：

- **强调系统和架构的重要性。**从整车的电子电气架构，到自动驾驶系统，到软硬件架构，每个功能的定义都依托于这些系统和架构的设计，并且也反过来有效地促成其完善。
- **强调数据驱动的优化。**功能定义不是一蹴而就的活动，也是逐步完善和迭代的过程。实际的测试和运营数据，正是驱动功能定义不断完善的原动力。



* 图：功能定义设计过程

基于上述方法和设计理念，赢彻科技形成了一套详细的功能清单，并在日常的工作中进行实时维护和更新，以此来驱动功能定义的展开。通过正向设计的功能定义方法和过程，赢彻科技在业界率先将自动驾驶系统落地于量产整车项目上。结合运营端的实际场景，前期针对性地进行功能定义及顶层设计，后期基于实际运营数据进行快速迭代，满足了干线物流运输的实际需求。

示例

功能清单示例

DDT		ODD	专项	
纵向功能	**横向功能**		**驾驶行为类**	**性能指标类**
巡航及跟车 高速拥堵辅助 紧急制动 安全停车 智能节油模式 全局速度规划	车道保持 基于指令的变道 智能避让 智能变道 匝道辅助驾驶 智能进出匝道	锥桶、碎片避让及提醒 恶劣天气应对	避让抑制	重刹优化 车辆非线性优化
座舱管理	**司机安全管理**		**稳定性问题类**	**人机交互类**
系统启动及提醒 驾驶员干预 Fallback 分级提醒 智能导航 语音交互	驾驶员状态管理 远程司机唤醒 远程通话		诊断策略优化 系统重启策略	系统启动过程信息透明化 文字及语音优先级

2.2
功能安全

根据《中国公路货运行业智慧安全白皮书》，中国公路货运行业百万公里事故数为 3.7 次，相当于平均每个驾驶员每 16 个月就会发生一次交通事故，平均每年的事故保险赔付额约为 3 万元 / 车。事故产生的最主要原因有两种，驾驶员因素占 37%，辅助设备不足因素占 35%。自动驾驶系统通过智能感知、智能决策和智能车控来辅助或代替驾驶员执行驾驶任务以期显著提高驾驶安全性。为了实现这一安全性目标，自动驾驶系统本身的设计开发就必须达到足够的安全要求。进行功能安全和预期功能安全 (SOTIF, Safety of The Intended Functionality) 开发，是目前实现这些安全性目标最有效的手段。

传统汽车产品的功能安全开发已有比较成熟的方案。与之相比，如何开发和验证自动驾驶系统的安全性还面临着诸多挑战：

- ISO 26262 和 ISO 21448 并没有详细的、可执行的开发方案
- 自动驾驶中广泛采用的深度学习算法在某些情况下不可解释、不可预测
- 深度学习算法的训练和验证流程没有行业公认的方案
- 用于训练和验证的数据的缺乏统一的质量保证体系
- 自动驾驶系统的安全评估缺乏统一的行业标准
- ……

功能安全与预期功能安全

目前，赢彻科技主要根据 ISO 26262 进行功能安全开发，根据 ISO 21448 进行预期功能安全 (SOTIF) 开发，从而提高自动驾驶卡车的安全性。

功能安全主要为了解决电子电气系统中的以下两类问题：

- **系统性失效。**如由于缺乏严格的设计、代码评审和测试，编程时错误地将 u16 数据类型当作 u8，使得超过 255 的数值产生错误结果。
- **随机硬件失效。**如由于系统中某个电阻发生短路故障，导致系统功能不正常。

预期功能安全主要为了解决自动驾驶系统中的以下两类问题：

- **功能 / 性能不足。**如在暴雨、积雪等天气情况下，摄像头感知能力变差 (没有故障)，导致系统不能正确识别障碍物或车道线，进而造成交通事故。
- **可预见的安全员误用。**如因为人机交互界面 (HMI, Human Machine Interface) 设计不合理，安全员接管提醒不充分或难以理解，造成因安全员接管不及时而产生交通事故。

针对上述四大类安全问题，赢彻科技的应对策略是：

- 开展 10000 种以上场景的危害分析和安全评估 (HARA, Hazard Analysis and Risk Assessment)。
- 提出 18 条整车级别的安全目标 (Safety Goal)，如防止车辆非预期加速、车辆非预期转向、自动驾驶系统非预期退出、Fallback 等级过低等问题发生，全面涵盖加速、制动、转向、安全员接管、

系统降级等所有与安全相关的功能。

- 逐步细化出超过 10000 条功能安全需求 FSR（Functional Safety Requirement）、子系统级别的技术安全需求 TSR（Technical Safety Requirement）、硬件安全需求 HSR（Hardware Safety Requirement）和软件安全需求 SSR（Software Safety Requirement）等各级安全需求。

功能安全设计与应对

为了应对自动驾驶系统的系统性失效，赢彻科技从公司文化、组织架构和研发流程体系等方面进行了以下两大类相关设计和开发：

- 完整的安全文化和研发流程。赢彻科技是自动驾驶重卡领域全球首个通过 ASIL D 级别功能安全流程认证的企业。
- 严格的系统设计和评审，包括整车 E/E 架构、自动驾驶系统、硬件、基础软件和算法架构设计等。

示例

针对系统性失效的解决方案示例

问题	赢彻科技解决方案	产出物举例
系统性失效	按照整车、系统、硬件、软件等，分层级实施全面的架构设计	整车 E/E 架构设计 自动驾驶系统架构设计 软件架构设计 硬件架构设计
	按照整车、系统、硬件、软件等，分层级定义完整的设计需求，且保持需求之间的一致性和可追溯性	整车级别的 18 条安全目标 整车系统级别的功能安全需求（FSR） 子系统级别的技术安全需求（TSR） 硬件安全需求（HSR） 软件安全需求（SSR）
	严格地进行技术评审	每一份架构和需求设计文档和软硬件都经过相关人员通过严格评审才批准发布
	系统地进行测试验证	硬件集成测试、软件单元测试、集成测试、系统集成测试、整车测试和验证 综合运用 SIL（Software In Loop，软件在环）、HIL（Hardware In Loop，硬件在环）、DIL（Driver In Loop，驾驶员在环）等测试环境
	完善的配置管理、变更管理和问题管理机制等支持性流程	对软硬件版本进行严格管理 对变更需经过相关人员专业分析后做出开发决定和计划，并规范存档 对评审和测试中发现的问题进行规范化地统一管理

系统性失效和随机硬件失效都会对安全造成直接影响。因此，赢彻科技从系统设计和开发的角度，对所有的安全目标进行了完整的安全开发。以防止非预期转向这一条安全目标为例：

示例

防止非预期的转向功能安全开发示例

问题	开发活动 / 产出	安全设计 / 需求
因系统性失效或随机硬件失效导致非预期转向	危害分析和安全评估（HARA）	在高速公路最右侧车道以 80km/s 速度行驶时发生非预期转向，撞向左侧车道车辆（ASIL D）
	安全目标（Safety Goal）	防止非预期的转向。故障处理时间间隔 FHTI（Fault Handling Time Interval）为 1000 毫秒（ASIL D）
	安全状态（Safe State）	维持正常的转向功能，直到在当前车道安全停车
	紧急操作（Emergency operation）	控制车辆在 10 秒内在本车道内安全停车
	功能安全需求（FSR）	传感器系统必须正确识别车道线 ADCU 必须正确计算出所需的转向扭矩 转向系统必须根据自动驾驶系统的输出，正确执行转向控制
	系统安全需求（TSR）	ADCU 对所计算的转向扭矩进行安全校验 如果 ADCU 检测到所计算的转向扭矩请求超过安全边界，应向安全监控模块报告故障，并在 100 毫秒内激活安全降级 ADCU 与转向系统之间的通信应受到 E2E 机制的保护
	硬件安全需求（HSR）	ADCU 的随机硬件失效指标 PMHF（Probabilistic Metric for Random Hardware Failure）应小于 10 FIT（Failures in Time），即每 10 亿小时工作时间，不超过 10 个 ADCU 内部电源监视器应在系统初始化期间进行一次自检，以避免潜在的电压监视器故障 安全相关的 RAM 数据必须进行 ECC（Error Correcting Code，纠错码）机制保护
	软件安全需求（SSR）	感知融合模块必须正确识别目标的外包围框（Bounding Box），误差不大于 10 cm 安全关键软件运行的内存区间应受到保护，避免低安全级别的软件改写高安全级别软件所在的内存区间

* 表格中所有需求和数据为示例而用，仅供参考，不代表真实系统设计

预期功能安全设计与应对

在预期功能安全开发方面，针对可能的功能 / 性能不足以及可预见的安全员误用，赢彻科技从以下几个方面进行了开发和优化：

示例

预期功能安全设计解决方案 - 示例 1

问题	赢彻科技解决方案	具体安全措施
功能 / 性能不足	系统改善	多个毫米波雷达、摄像头、激光雷达的充分冗余 通过传感器的融合感知，以及优化相关的算法，提高感知距离和准确率 反复优化算法，提高感知、定位和控制的精度 通过优化算法，有针对性地提高每个功能的能力边界 通过仿真、测试去识别极端情况（Corner Case），并进行有针对性的开发，扩大对极端情况的支持范围
	功能限制	通过仿真和测试，明确性能边界 对超过系统性能边界的场景，优化功能限制和降级策略 将所能支持的 ODD 和性能边界写进用户手册，并对安全员进行培训
可预见的误用	改进接管逻辑	通过理论研究、仿真和测试，优化接管时间 优化驾驶接管操作的简便性
	改进人机交互设计	确保对安全员的提醒的及时性和有效性 确保对安全员的提醒的简洁性和易懂性 优化不同提醒的优先级，避免提醒之间的冲突

针对深度学习的安全性和可靠性，赢彻科技从以下几个方面进行了加强：

示例

预期功能安全设计解决方案 - 示例 2

问题	赢彻科技解决方案	具体安全措施
深度学习不可解释、不可预测性	开发流程	制定完整的深度学习开发流程，并对其进行 PFMEA（Process Failure Mode and Effects Analysis，过程失效模式和影响分析）分析和优化 严格遵循以上流程来进行开发、评审、测试和验证 对所用到的软件和数据都进行安全评估 对深度学习的软件和参数都进行配置管理

深度学习不可解释、不可预测性	软件需求定义	定义清晰和完整的需求，并对系统级需求、测试用例进行追溯 定义超过 200 项衡量深度学习性能的指标 对数据集按照训练集、验证集和测试集进行分类管理
	软件架构设计	将深度学习模块当作一个软件模块进行模块化设计 采用异构冗余架构，采用不同的深度学习算法 充分考虑功能安全和预期功能安全需求，对软件架构进行安全分析，如 FMEA（Failure Mode and Effects Analysis，失效模式及后果分析）、DFA（Dependent Failure Analysis，相关性失效分析）等
深度学习安全性缺乏统一评判标准	软件测试	对采用的第三方软件库和开源工具进行安全鉴定 综合运用故障注入测试和神经元覆盖度测试 完整进行软件单元测试和集成测试
	系统安全验证	综合运用仿真和实车测试，达到时间、经济成本和测试有效性之间的平衡 根据 ODD 定义和实际运营场景，设计相应的测试场景库，并不断更新，尽可能地涵盖更多场景 对测试里程进行综合设计，追求有效性，而非一味追求里程数据 定义清晰而合理的安全评价指标，形成企业标准

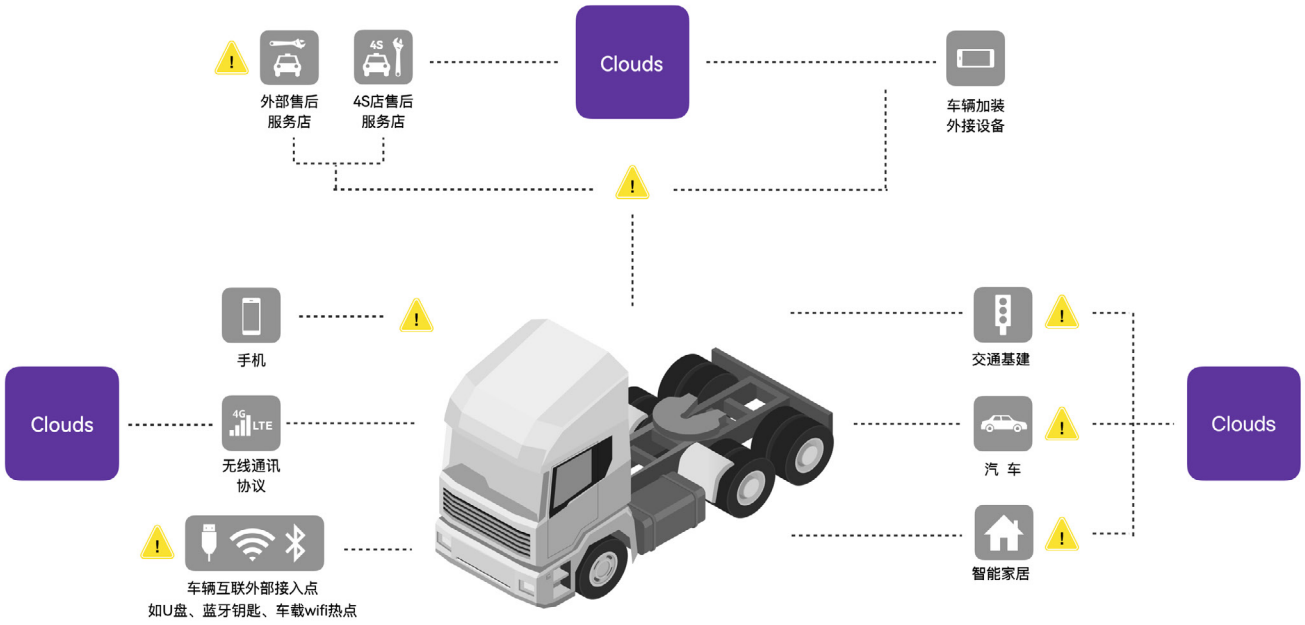
赢彻科技重卡自动驾驶功能安全设计实践

传统整车和电子零部件的功能安全方案已经非常成熟，而且都由驾驶员介入作为最后的安全措施，系统的安全等级相对可以较低（比较常见的是 ASIL B 或以下）。自动驾驶系统不仅复杂度更高，而且自动化等级越高，对安全员接管的要求越低，进而导致对系统功能安全等级的要求更高（基本都要 ASIL D）。此外，最新版的 ISO 标准缺乏对自动驾驶系统的完善支持，不管是开发还是验证都缺乏统一的行业标准。尽管面对诸多挑战，赢彻科技在安全方面，坚持采用行业最新的安全技术，在参考 ISO 26262 和 ISO 21448 的标准前提下，采用最先进的安全策略，在概念、系统、软件、硬件、测试等每个环节都进行了充分的安全设计和开发，使得赢彻科技自动驾驶系统的安全性达到行业最高水平。

自动驾驶的安全性不管是从设计和开发的角度，还是从验证和评估的角度，都还有很多未知的领域尚待研究和完善。作为智能重卡量产的先行者，赢彻科技在创立之初就将安全高于一切作为自身基因的一部分，持续设计、开发、验证和完善各种系统架构和算法的安全性，建立对标基准，向行业分享。同时，赢彻科技持续与行业上下游的伙伴、科研院所和相关监管部门进行合作与共同探索，促进自动驾驶行业安全规范化和标准统一化。

2.3
网络安全

随着智能网联汽车网联能力越来越开放，由于信息安全漏洞导致车辆被攻击的案例在过去几年中不断爆出。提高自身车联网信息安全水平，保障用户生命财产及个人隐私安全，成了一个重大课题。重卡作为商用车，其通信接口的标准化导致黑客能够更为轻而易举地获取车辆原始信息。同时，智能网联汽车存在更多近场通信和远程通信的暴露度。因此自动驾驶重卡的信息安全防护能力变得刻不容缓。



* 图: 自动驾驶重卡信息安全挑战

国家和汽车行业高度重视日益凸显的汽车信息安全问题，相关标准陆续出台：

- **国内法律法规层面：**为引导和规范智能网联汽车行业安全发展，各部委基于《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》制定了一系列的标准和法规，工信部于 2021 年密集颁布了如《智能网联汽车生产企业及产品准入管理指南》、《智能网联汽车道路测试与示范应用管理规范》、《汽车信息安全通用技术要求》、《车载信息交互系统信息安全技术要求及试验方法》、《汽车网关信息安全技术要求及试验方法》等标准，并且《汽车整车信息安全技术要求》将在 2023 年形成强制国标。
- **国际标准层面：**国际标准化组织（ISO）和美国汽车工程师学会（SAE International）共同制订的国际标准《ISO/SAE-21434- 道路车辆信息安全工程》于 2021 年 8 月正式发布实施。

汽车信息安全本质上是一种动态安全，随着产品、技术、应用、网络的变化和发展而变化。但在变化中不变的是：

- **信息安全的目标：**保证生命安全，保护资产（包括实物资产、数字资产等）不受信息安全威胁，保证系统功能安全运行，保证国家和个人数据安全。
- **信息安全应对策略：**1）有效的安全设计，消除信息安全风险；2）实时监控，抵御网络安全攻击；3）多方联动，及时发现、上报、处置网络安全威胁。

汽车整车信息安全技术的基本应对原则主要包括如下 4 个方面，也是设计的核心要求：

- **车端安全：**包括消息认证、安全区域划分、访问控制、报文健康检查、诊断服务检测、异常行为监测、身份管理、证书密钥管理、安全日志等。
- **汽车外部通信链路安全：**远程升级安全、远程控制安全、V2X 安全、远程访问安全、定位安全等。
- **数据安全：**基础数据、车控数据、服务数据、隐私数据等。
- **车联网云端安全：**入侵防范、身份认证安全、接入安全、通信安全、系统安全等。

信息安全测试可以分为正向和逆向两个方面，需要做相应的设计：

- 正向验证是从工程开发层面确保安全设计和实施达到预期效果，实施内容包括如代码的静态扫描发现代码漏洞、模糊测试检测协议栈缺陷、安全测试用例验证安全策略、漏洞跟踪和扫描、及时打补丁等，保证安全需求适时地形成闭环。
- 逆向验证是通过安全攻防，模拟黑客攻击产品，通过固件逆向、通讯劫持、信号干扰、CVE（Common Vulnerabilities & Exposures，公共漏洞和暴露）漏洞利用等，利用实战反向验证产品的安全性。

2.4
指标体系

自动驾驶系统是一套庞大、复杂、数据驱动且对安全性要求极高的系统。如何准确评价自动驾驶产品的表现既重要又充满挑战，科学系统的指标体系是构建自动驾驶产品的前提和基石。指标体系的构建包含三方面：指标定义、指标监控和指标运用。

指标定义

指标定义需要满足三个特性，包括系统性、体验一致性和可量化性：

- **系统性：**对自动驾驶系统建立全面的多维度指标，以便全面掌控系统的运行状态。
- **体验一致性：**确保安全员主观的体验感受与指标客观的衡量在统计意义上保持高度一致。
- **可量化：**任何指标必须是可量化且客观，以便准确评价性能的提升或是降低，以及具体的变化幅度。

从指标体系系统性的角度，为了衡量量产自动驾驶卡车的性能，可以将指标整体分为以下几大类：安全类、运营类、功能类、质量类、算法类：

- **安全类：**衡量自动驾驶系统在道路上持续运行的风险，反映其安全性。
- **运营类：**衡量自动驾驶重卡在运营场景中商业价值的达成度，反映所取得的经济效益。
- **功能类：**衡量自动驾驶各类功能的执行成功率，反映具体功能在实际应用中的可用性和成熟度。
- **质量类：**衡量自动驾驶系统在长时间运行条件下能否持续保持在预期工作状态，反映量产自动驾驶重卡的可靠性。
- **算法类：**衡量感知、定位和规划控制系统的输出是否稳定准确，反映自动驾驶算法系统整体的精确性。

示例

自动驾驶卡车指标定义 - 示例

	类别	具体指标举例	指标释义
车辆性能指标	安全类	MPD（Mileage Per Disengagement）	产生人工接管的间隔里程数
		MPD0	因发生安全风险需要人工接管的间隔里程数
		重刹频次	百公里发生超过 -2m/s^2 减速度重刹的次数
		画龙频次	百公里发生车辆在车道中周期性左右晃动的次数
		压线行驶频次	百公里压线行驶次数
		…	

车辆性能指标	运营类	时效达成率	早于基准时效到达目的地的趟数 / 总运单趟数
		油耗	百公里耗油
		安全员疲劳度	千公里安全员疲劳次数
		百万公里事故次数	百万公里发生事故次数
		…	
	功能类	拨杆变道成功率	拨杆变道成功次数 / 拨杆变道使用次数
		nudge 成功率	车道内避让成功超车次数 / 车道内避让触发次数
		超车抑制百分比	超车时被抑制时长 / 总超车时长
		匝道通过成功率	自动驾驶状态通过匝道次数 / 总通过匝道次数
		HMI 体验	HMI 系统使用便捷性以及系统提醒合理性
		…	
	质量类	0KM PPM (Parts Per Million)	厂内自动驾驶系统故障件总数 / 自动驾驶系统出货件总数 *1000000 件
		12 MIS (Month In Service)	12 个月内车辆故障数 /12 个月内生产车辆总数 *100%
		AD (Autonomous Driving) 占比	自动驾驶里程 / 高速运营里程
		系统启动成功率	自动驾驶系统启动成功次数 / 自动驾驶系统启动次数
		系统启动时长	自动驾驶系统启动的时长
		Fallback 频次	百公里系统故障提示安全员接管次数
		AD 平均时速	自动驾驶状态下的平均时速
		…	
算法性能指标	算法类	车辆检测准召率	感知算法对车辆检测的准确率和召回率
		车辆检测横纵向误差	感知算法对车辆检测的平均横向和纵向误差
		定位误差	定位算法的平均误差
		…	

上述评价指标会受到外部场景因素的影响，如不同时间、天气、线路等等。需要区分统计不同场景的性能表现，以便进行针对性的优化。

外部因素	具体场景
时 间	白天，夜晚
天 气	晴天，雨天，雪天，雾天
线 路	华北线路，华中线路，华南线路

指标监控

在大规模运营的条件下，需要对自动驾驶重卡的运营状态进行密切有效的监控，以便相关人员根据情况采取不同的应对措施。按照时效性不同分为：

- **实时监控：**在运营过程中，运营管理人员实时监控反映车辆状态的相关指标。当有单车表现异常的时候，可及时与安全员联系并确认车辆和安全员状态，确保安全驾驶，尽早发现车辆故障并排查维修。
- **延迟监控：**研发及测试人员对一定周期的数据进行指标分析和统计，用于评估系统能力边界并指导研发迭代。

指标运用

赢彻科技目前已经建立了超过 50 个车辆性能指标和超过 100 个算法性能指标，精确地评估车辆性能和算法性能，其应用原则如下：

- **短板原则：**在衡量量产产品的指标运用方面，要采用“短板思维”，产品的整体性能水平，取决于最短板关键指标的性能。
- **精简原则：**指标运用注重精简，衡量指标如不精简分级，就会形成冗余而混乱的评价体系。过多或者过于复杂的指标会造成指标变化参差不齐，反而让人无法做出正确判断。赢彻科技在研发迭代过程中，使用约 20 个核心指标重点评价迭代中的性能变化。
- **关注波动性：**由于自动驾驶产品的算法会受到自车和各种外界因素的干扰，且算法具有一定的概率性和随机性，导致指标概率上升或者下降，因此，要充分评估数据波动性。比如，当某个指标上升时，不一定意味着产品性能提升，或许是因为受到外界因素（如天气、车流量等）影响，或者因测试里程不足而导致指标波动。因此，要仔细分析外部影响因素，以及波动相对收敛的最低里程要求，从而做出可靠的判断。

赢彻科技所建立的指标体系，在量产实践过程中不断完善，显著促进了其重卡自动驾驶系统的快速迭代。例如，为了对 MPD 进行专项优化提升，先根据安全员接管原因的一级大类进行分类，如车辆画龙导致接管、重刹导致接管、连接路问题导致接管、系统故障提醒安全员接管等。然后对于每一大类问题，进行根因层级细分，包括算法模块、系统设计和产品设计等。进而可以统计出根因子类出现的百公里频次，以此将每一次接管对应的优化职责细分到对应的具体研发模块或者对象。接下来各模块就可以根据整体的优化目标，制定对应子项的优化目标设定，形成自上而下的拆解，通过达成每个小目标，最终实现大目标的达成。建立科学的指标体系，并坚持按照方法论执行，是赢彻科技不断进步的有力保障。

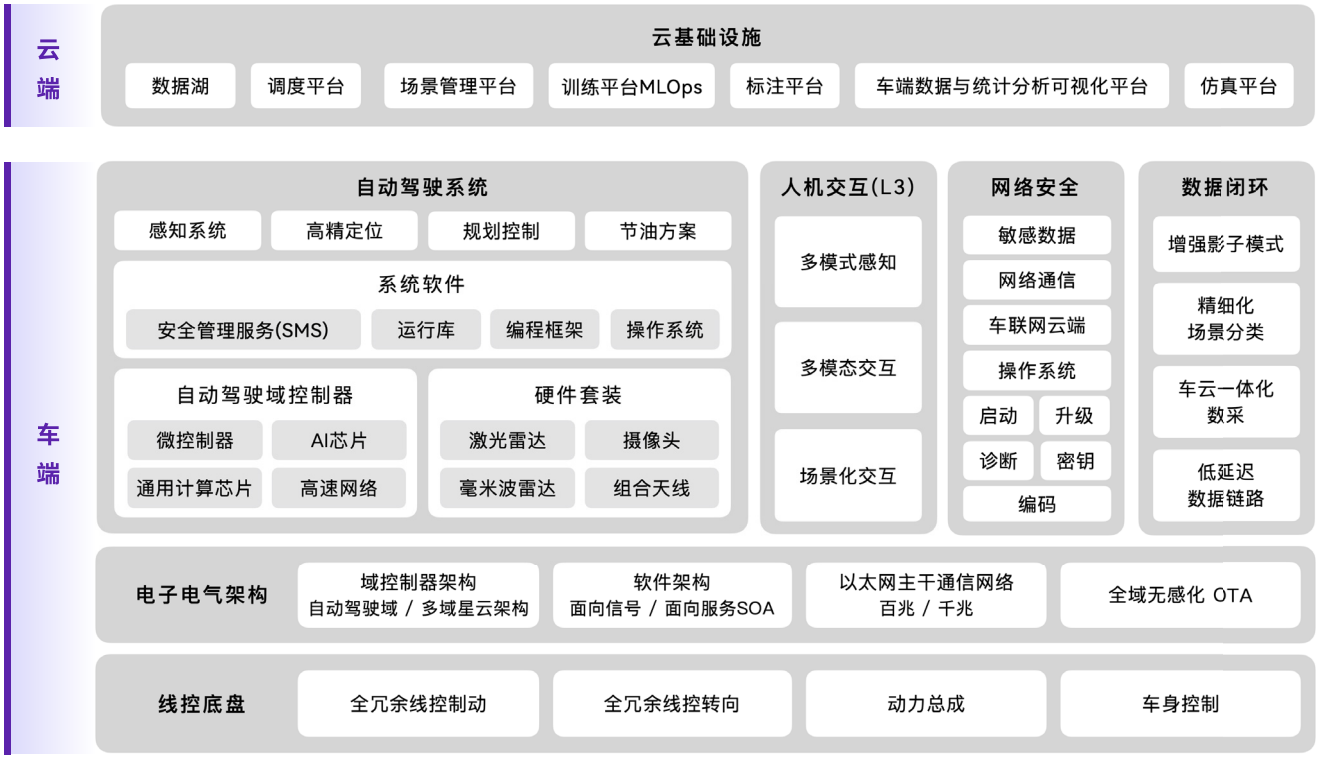
3 系统开发

3.1 自动驾驶卡车系统概述

我们认为自动驾驶技术真正的量产落地，是横跨车辆工程、半导体、系统软件、人工智能以及云计算等多个领域和技术栈的系统工程。打造一款成功的自动驾驶卡车，必须把这些领域的核心能力进行全栈整合。

赢彻科技自 2018 年创建之初，即坚定选择自动驾驶卡车核心领域的全栈自研。我们坚信全栈自主研发是取得量产成功、技术加速迭代并成功走向全无人驾驶的关键。

- 首先，完整技术链条的构建，可以充分发挥跨技术领域的深度融合优势。通过软件、硬件和车辆的协同设计，可以综合各种系统资源，最大限度地挖掘整个系统的潜能，使得整个自动驾驶系统高效运转的同时，还能有效降低整体成本。
- 其次，全栈技术能力可以非常灵活地适配不同场景、不同车辆，进而拓展生态，为加速自动驾驶技术量产与产业化提供强有力的保障。
- 最后，在核心环节上拥有充分自主权，能够在量产的每一个关键环节，比如供应链、成本优化等，拥有足够的能力规避各种风险，顺利高效率地达成量产目标。



* 图：赢彻科技 - 自动驾驶卡车系统全景图

赢彻科技在**自动驾驶算法**上，创新性地克服了卡车独有的物理局限和量产的限制条件所带来的挑战，实现了一套能高性能地满足商用车应用场景的感知、定位、规控和节油算法。全自研的**自动驾驶域控制器**是卡车领域首个自带全冗余且高算力的车规级车载计算平台，并且已经成功量产。赢彻科技自研的**系统软件层**，不仅为自动驾驶卡车提供高性能、高安全、高可靠的中间件服务，也为产品研发效率提供了强大的支撑，创造了一个更友好的集成环境。在**云端**，赢彻科技打造了“三横两纵”的基于云原生的技术栈，为量产提供了规模化的实时数据分析服务。在车端，赢彻科技域集中式**电子电气架构**，减少了系统复杂度，并提供高通讯带宽、整车信息安全以及整车 OTA 的能力。**线控底盘**方面，赢彻科技的全冗余技术实现了精准安全的车辆控制和流畅的人机共驾，保证了车辆安全平稳运行。赢彻科技的**人机交互系统**解决了安全员对系统的信任以及疲劳管理问题。此外，赢彻科技集成的**传感器套装**，达成了 OEM（Original Equipment Manufacturer，主机厂）认可的生产件批准程序 PPAP（Production Part Approval Process，生产件批准程序），是真正意义上的行业内首套商用车车规级自动驾驶系统硬件套装。

3.2 自动驾驶系统

* 图：赢彻科技 - 卡车自动驾驶系统全景图

3.2.1 感知系统

感知系统的核心任务是通过处理分析多种传感器的信号输入，实现对环境的深度理解，为车辆了解周边环境并作出后续规划控制提供保障。在自动驾驶系统中，感知系统作为第一环，是规划控制系统的上游，其结果的准确性及鲁棒性直接决定了自动驾驶系统的能力边界。

重卡对感知系统的特别要求

- **更远的感知距离：**卡车的制动距离更长，相比于乘用车 40 米的制动距离，卡车的制动距离会超过 100 米。因此，相比于乘用车 100 米左右的感知距离要求，卡车所要求的感知距离一般在 200 米以上，甚至达到千米级别。
- **更高的横向精度：**卡车宽度相比于乘用车更宽，宽度可达 2.8 米，高速公路车道线宽 3.75 米，当两个卡车在相邻车道并排居中行驶时，两卡车的最近距离只有 95 厘米。相比而言，乘用车车宽 1.6 米，乘用车和卡车会车时的距离空间有 155 厘米，约为卡车会车距离的 1.6 倍。因此，重卡对目标车横向位置的精度要求比乘用车更高。
- **后向感知：**由于卡车带挂，并且挂车无法安装量产传感器，所以正后方视角无传感器可以直接观测，对后向感知的精度及距离带来挑战。
- **传感器布局：**相比于乘用车，卡车更宽更长，传感器的分布更加离散且不在同一刚体上，不同传感器的视场 FOV（Field of View）重叠度较低，标定参数失效会对算法的精度带来挑战。

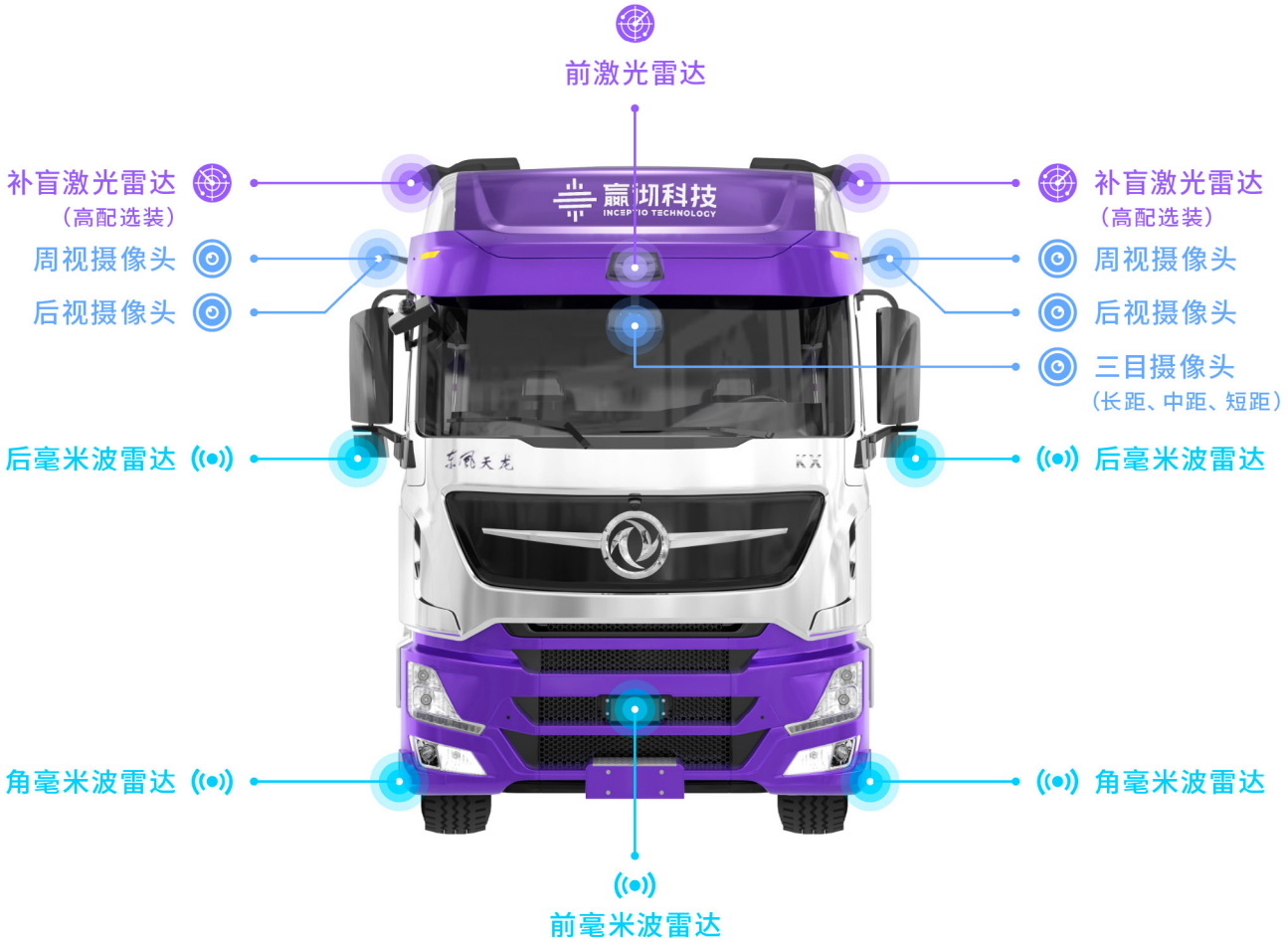
感知系统的量产挑战

- **SoC 架构和算力瓶颈：**为了满足车规、功能安全和量产成本等要求，ADCU 平台算力受限，且采用复杂的异构系统架构，对算法的计算性能和多模态计算带来巨大挑战。在高算力高带宽的负载情况下，亦对系统稳定性造成空前压力。
- **传感器选型：**为了满足车规、成本等量产要求，需要考虑相关传感器的量产时间线，选型受限制，性能滞后于行业尖端水平，需要提升感知算法在硬件能力边界的应对策略，拓展能力边界以满足量产功能定义的要求。

传感器配置与设计

赢彻科技的自动驾驶方案采用摄像头 - 毫米波雷达 - 激光雷达配置，实现车体 360°环境感知覆盖。传感器安装位置如下图，为满足不同级别配置的需要，左右两侧补盲激光雷达为高配选装。

- **摄像头：**基于成像模组进行了定制化产品设计。
- **毫米波雷达：**选用国际供应商第五代面向商用车设计的长距与角向雷达，同时对输出数据进行了专属开发。
- **激光雷达：**选用当前性能与成熟度综合最优，且符合车规的 MEMS 产品，并基于实际的卡车商业运营场景对基础功性能进行了适配开发。



* 图：赢彻科技 - 自动驾驶系统传感器布置方案

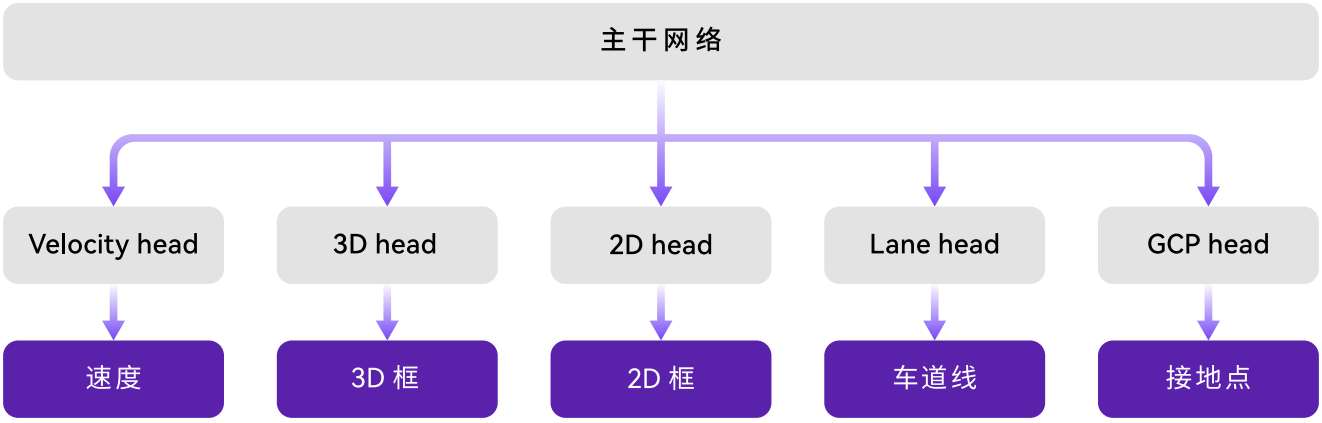
赢彻科技对传感器的安装布置进行了不同程度的优化设计，以便于满足商用车相关法规要求，并充分考虑实际运营场景中的潜在问题与风险：

- 将后向毫米波雷达融入后视镜的一体化布局，多处传感器支架进行了应对碰撞的溃缩吸能设计。
- 新增适应实际长时间运营的激光雷达清洗功能。
- 舱外传感器分别满足对应位置的防水防尘要求（部分甚至可达 IP6K9K），且均经过验证，在商用车的高强度、长时间振动环境下，达到与整车运营时间相匹配的零件寿命（最高 3 万小时）。

赢彻科技感知系统技术路线

为了实现量产，感知系统需突破瓶颈限制，力求看得更远更准、耗时更低。为此，赢彻科技充分融合多传感器信息，将重点聚焦于：

- **长距离感知：**利用非监督学习，融合百米级探测距离的高精度激光点云和千米级视距的长焦摄像头图像信息。利用近处的激光点云对低精度的背景点云进行高精度约束，并通过注意力转移算法实现精准的千米距离感知，深度误差低于 5%。
- **高精度横向感知：**结合目标实例分割、车道横向偏移量预测和目标物点云模糊轮廓提取等技术，实现障碍物检测算法，横向误差在相同测试集下比国际知名厂商低 54%，达到业内领先水平。
- **多任务深度神经网络突破算力局限：**采用加权多任务学习策略和 Warm-Up 策略，在确保充分节省算力的前提下，重点提升难训练任务和重要任务的训练效果。成功解决了 GradNorm、PcGrad 等算法在多任务学习中的精度下降难题。在保证精度不变的条件下，实现了 5 倍以上的加速，大幅度改善算力局限带来的影响。



* 图：多任务深度神经网络

- **多模多视角 Transformer 的前融合感知，全方位提升感知精准度：**对于不同类型传感器（如激光雷达、毫米波雷达和摄像头）的输入，我们设计并实现了在 BEV（Bird's Eye View，鸟瞰视角）视角下融合不同数据源的前融合框架。此框架首先基于 Transformer 方法，将摄像头视角映射到 BEV 视角下，其次利用 Transformer 将不同数据源的 BEV 特征图充分融合，最后利用长短期记忆 LSTM（Long Short-Term Memory）的时序融合网络获得视频流的感知结果。相比于前一代的后融合方法，我们的前融合大模型在多项感知任务和场景上表现出更强和更稳定的性能，以及更加简洁的推理流程。目前业界常用的前融合框架通常会为每类数据源设置单独的 BEV 主干网络，并通过将不同源的特征图堆叠后进行局部卷积实现融合。为了在融合过程中更加高效地获取更多有效信息，我们将投影后的 BEV 特征直接进行融合，并共享 BEV 下的特征编码（Feature Encoder）与多任务头（Multi-Task Head），此融合方式能节省约 10% 的计算量与参数。同时，相较于将不同源的特征图（Feature Map）堆叠再局部卷积，我们使用 Transformer 能同时捕捉到局部和全局的相关信息。经过评测，相较于业内领先的算法 BEVFusion，这套前融合感知方案在检测任务上超过 2%mAP/NDS，将部署于赢彻科技下一代高算力 ADCU。

- **数据增强解决小样本难题：**为了降低标注成本，针对领域自适应语义分割任务，提出了一个基于区域的主动学习方法，目的是自动地查询一小部分区域给予标注，同时最大化网络性能。为此，我们提出了基于区域不纯度和预测不确定性的主动学习 RIPU（Active Learning via Region Impurity and Prediction Uncertainty），能够捕捉图像区域的空间邻接性以及预测置信度。相比于基于图片和像素的挑选策略，基于区域的挑选策略能够更有效地利用有限的标注成本。RIPU 系统还增强了源域图像中像素与它邻近像素之间的局部预测一致性。另外，负学习损失（Negative Learning Loss）的引入也使得特征更具辨别力。大量实验证明该方法仅需少量标注即可得到趋近于全监督的性能，在跨领域分割任务上，较业界领先算法 MADA 性能领先 9.71%。

针对重卡业务场景，重视成本 - 安全 - 效率三角平衡

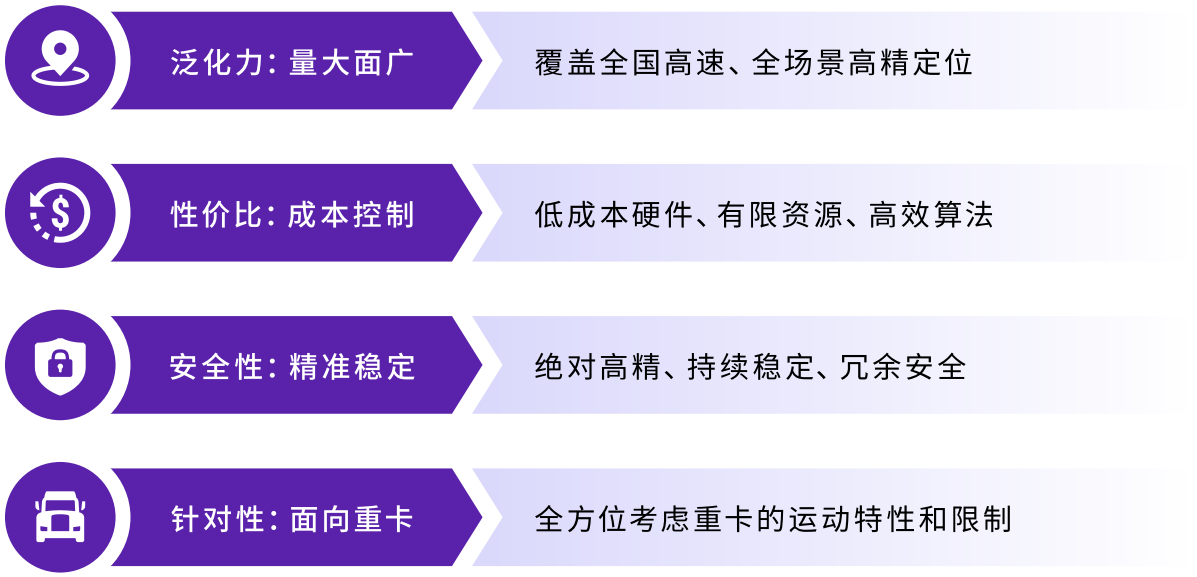
赢彻科技自动驾驶感知系统，面对量产要求、高速干线场景和物流运营商业化要求，建立了高效的研发迭代体系，支持针对性解决特定问题，从而实现成本 - 安全 - 效率的三角平衡，包括：

- **建立完善的指标体系，全面监控感知系统的准确性及稳定性指标，并充分评估复杂场景下的感知表现。**除了沿用通用的 Precision/Recall/mAP 等精确度指标之外，额外设计了稳定性指标。例如，Lane-Change Rate 用于表征连续帧之间车道线检测的横向位置变化率；类似的，Label-Change Rate 用于表征连续帧间检测类别的变化率。除了变化率之外，还需监控每个指标的方差，设计了 On-Lane Ratio 3 Sigma 用于表征障碍物压线量的方差。针对实际长尾问题，建立垂直场景集，一问题一规则，针对性设计回归测试指标，精准挖掘复杂问题上的算法表现。
- **干线场景下目标时速高、形态差异大，对感知系统提出更高的安全性要求。**高速上存在形态各异的异型车，需要感知系统对其外廓进行精准识别。高速上目标车速较快，除了看的远，还要反应快，因此感知系统在设计时需要尽量减少链路中的串行模块数量。
- **卡车作为物流服务承载工具，需要应对复杂的物流外部环境，且对成本和时效也有严格要求。**需要支持复杂照明、天气、路况等条件的稳定感知。当超出能力边界时，需有降级策略。

3.2.2 高精定位

高精定位为自动驾驶系统提供车辆在各个时刻下的位姿、速度、加速度、角速度等信息，是规划和控制等系统正常执行的前提条件。

针对干线物流的重卡场景，自动驾驶定位系统需要重点考虑四个方面的要求：泛化力、性价比、安全性和针对性。高精定位的几个主要挑战也源于此四项要求、以及它们之间的内在冲突。



* 图：重卡自动驾驶系统高精定位的要求

重卡对高精定位的独特挑战

重卡的高精定位与乘用车相比，需要考虑重卡带来的限制以及卡车自身的特性，主要有以下几点：

- **空间小：**卡车离车道边界的距离都很小。对于超宽的挂车，其侧面到车道边界的距离在 35cm-40cm，相比乘用车要少 50cm 以上。因此针对自车定位，在各个场景（如隧道）都要求有精确的定位输出（比如横向位置误差 <10cm）。
- **驾驶室与底盘的非刚性连接：**由于传感器（GNSS/IMU、摄像头、LiDAR 等）大部分是与驾驶室刚性连接，但驾驶室与底盘有相对运动。直接基于传感器估算的车身位姿与车辆实际运动有差异，影响控制模块对车辆的控制。
- **震动大：**由于卡车自身的特性，车身的震动相比乘用车要高将近一个数量级，因此给传感器带来比较大的噪声。

量产对高精定位的苛刻要求

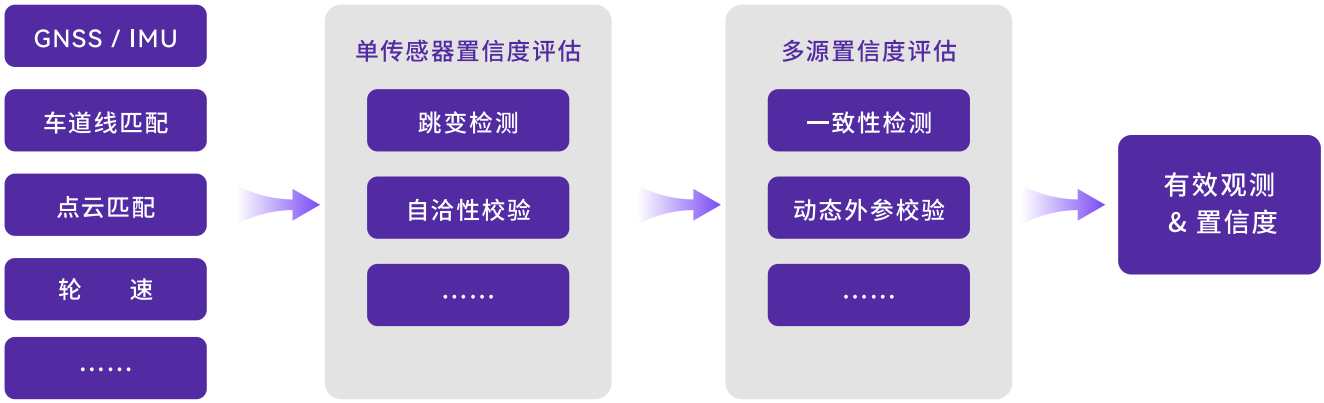
面向量产的卡车自动驾驶方案，既对成本控制有严格的要求，又要求系统具有高泛化能力，以支持全国主要干线物流高速路网：

- 演示车中常见的高精卫导、惯导设备已不适用。需要用满足车规和功能安全要求的低成本方案。由此带来的性能下降，对软件系统提出了更高要求，尤其是应对低成本方案在复杂工况下的精度和稳定性下降。
- 高精地图作为定位（以及规划等模块）的重要先验，需要能覆盖全国的高速路网（双向大于 30 万公里），并且提供足够的鲜度（小于天级别的限速、线型等属性更新，小于周级别的车道线等几何信息的更新）。对于自动驾驶中常用于定位的点云数据，由于其数据量与作业成本，在覆盖率和更新效率上的挑战更高。除此之外，由于存储空间的限制，对三维点云的存储效率也同样有较高要求。
- 需要能支持全场景，包括隧道、匝道、山区等。

基于多传感器融合的量产高精定位系统

面向量产落地的要求，赢彻科技设计研发了带有多重校验和冗余的高效融合定位算法，能够有效地抵抗各类噪声，通过融合低成本 GNSS/IMU、视觉、LiDAR、轮速等传感器信息，实现在不同工况下均能提供高精度的定位输出。系统重点模块如下：

- **面向卡车的运动模型：**针对驾驶室与底盘的相对姿态、挂车的相对角度进行动态估算，综合对卡车的运动进行建模。能有效缓解驾驶室与底盘非刚性连接带来的问题，并能在弯道、变道的场景下提供更精准的位姿估算。
- **全方位的置信度模型：**结合单传感器的置信度评估和多源置信度评估，对每一个传感器输入进行多维度校验，自适应地去除不良观测带来的影响，在不同场景下都能利用最有效的观测来提供精准定位，实现高稳定性。



* 图：高精定位系统观测置信度模型

- **动态传感器标定：**通过提取的特征信息（角点、车道线等），在线动态检查和更新传感器外参，消除传感器之间由于路况、震动等导致的位姿误差。
- **高效、轻量级的 3D 点云匹配：**点云地图本身数据量巨大，采用原始点云数据很难量产泛化。常用方式是将 3D 点云降级到 2D 栅格地图，虽然能大幅度减少数据量，但会导致信息的丢失。赢彻科技采用基于等高线的表达方式，既能一定程度保留 3D 信息，又能有效降低数据量。让覆盖全国高速、推向量产成为可能。
- **安全芯片上的冗余定位：**在主系统异常失效的情况下，在安全芯片上利用惯导推算提供自车轨迹，配合其他冗余模块对车辆进行紧急状态下的安全应对，让车辆能持续处于安全可控的状态。

此外，赢彻科技还在研发基于深度学习的特征表达与匹配，用于点云和视觉定位，进一步提升单位数据的有效性。面向未来，既能应对高速场景，也能在非高速场景下实现精准和稳定的定位。

赢彻科技通过独有的算法设计，所研发的基于多传感器融合的高精定位算法系统，对关键指标进行了重点优化：横向定位精度 <7cm 以及航向角精度 <0.3 度，很好地支持隧道（包括长隧道、连续隧道等）、匝道、夜间等不同工况。

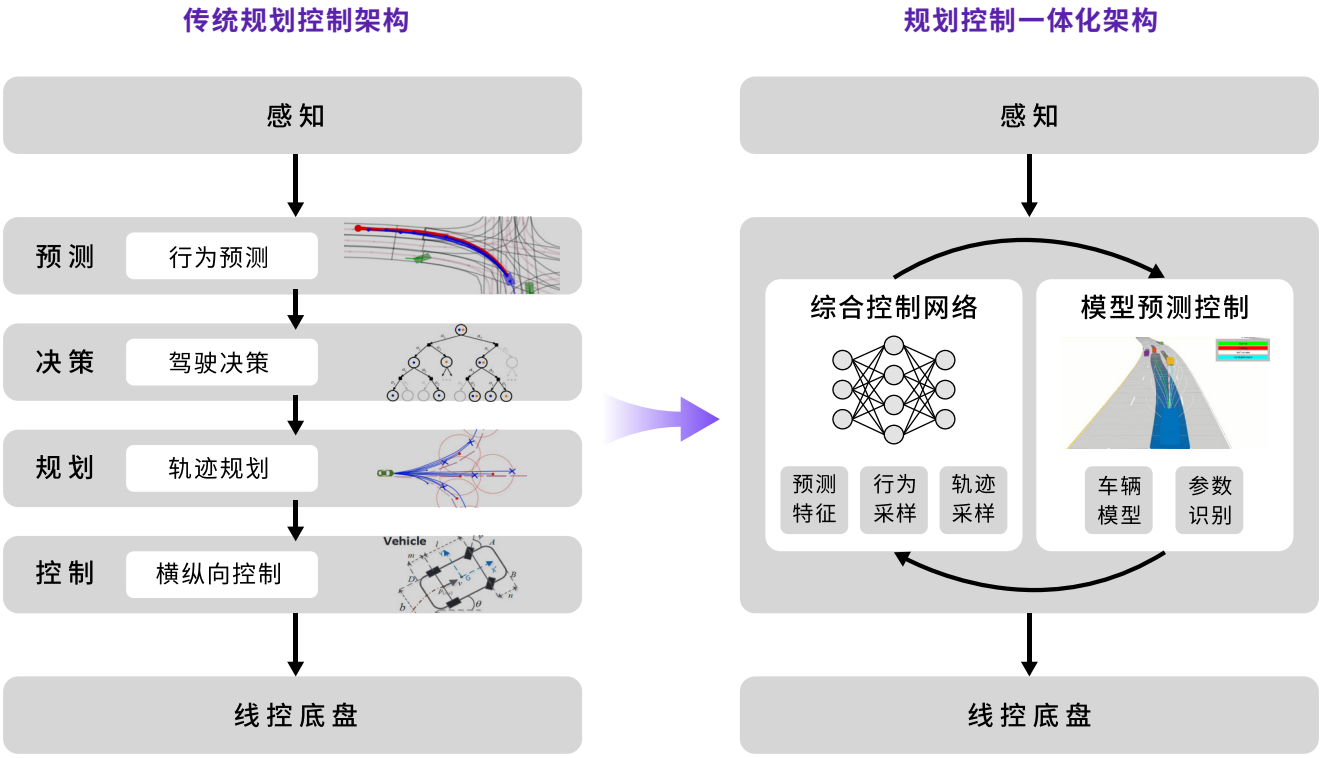
3.2.3 规划控制

卡车的规划控制系统需要为客户提供安全的驾驶、精确的控制、舒适的乘坐、经济的使用和良好的耐用性这五大价值，挑战在于如何在安全、舒适、经济和耐久中找到平衡和最优解。主要存在如下难点：

- **精准建模与一车一调的矛盾：**对车辆参数进行准确建模是实现精准控制的前提。针对车辆参数和环境参数问题，目前业界会对车辆进行静态建模和参数标定，对每一台车都进行独立的精细标定和建模。从大数据反馈来看，由于柔性挂车、横坡横风等带来的不确定性，单一静态模型很难覆盖车辆的参数变化和适配所有的营运场景。同时，在大规模运营之后，为每台车进行精细参数调整成本变高，车辆参数也会随着运营里程增加造成的机械磨损而逐步劣化偏移。以转向器间隙为例，有实验表明，100 万公里下转向系统空行程劣化会超过 40%，这对于模型控制提出了很大的挑战。
- **精确控制与耐久性、经济性的矛盾：**在规划控制提出的安全、精确、舒适、经济和耐久五大目标中，有些目标是此消彼长的。例如，如果过度追求精确性，必然导致执行器的频繁调整，从而影响到系统耐久性。基于人机共驾特点和客户价值最大化，需要在追踪精确性与耐久性等多个维度上综合考虑，取得全局最优。针对不同客户价值，需要在矛盾中寻找平衡。目前业内比较常见的误差追踪算法，只能通过调整参数在有限范围内对于驾驶行为进行微调，难以在所有维度上求得统一规划的最优解。
- **规划控制分层和融合的矛盾：**典型的规划控制算法通常分为多个层次，如行为决策、轨迹规划

和控制等。分层结构中，典型的规划侧算法更多聚焦理想状态空间中的求解，而控制侧算法聚焦基于复杂车辆模型的状态追踪。这类分层架构较融合的方案更易工程实现，鲁棒性高，但存在性能天花板，不易于实现精确性、耐久性的多个维度全局最优，其驾驶行为表现也很难接近优秀人类驾驶员的水平。

规划控制一体化



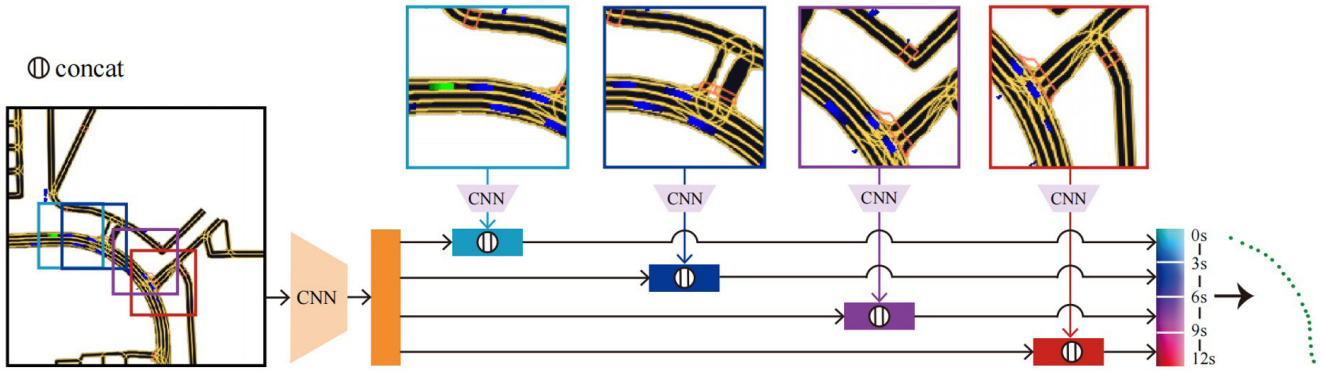
* 图：赢彻科技 - 规划控制一体化架构

赢彻科技为了解决上述问题，对于规划控制系统在车辆参数建模和算法架构等方面开展一系列创新，形成了独特的规划控制一体化架构，以满足商业重卡量产需求。

目前行业中普遍采用的是分层规划控制架构，即预测、决策、规划和控制分步进行。自动驾驶系统是一个极其复杂的软件系统，需要大量团队人员协作开发，这种相对简洁的分层规划方式有益于工程实现，在自动驾驶公司中较为流行。然而，这类分层架构在全局误差最优，舒适、经济和耐久的动态平衡，适配重卡底盘控制延迟等问题上存在很大的技术瓶颈，无法满足商业重卡的技术需求。赢彻科技的规划控制一体化架构包含了一系列的技术创新：

- **长时长预测模型：**与城市场景中通常 3s、5s 的预测时长不同，高速场景车辆速度快，重卡控制延迟大，需要更长的预测时长以实现提前的控制行为。长时长预测（Long-Term Prediction）即对周围车辆进行长达 10s 以上时间的行为、轨迹预测，典型方案在长时长预测上精度较差，无法满足重卡规划控制的要求。

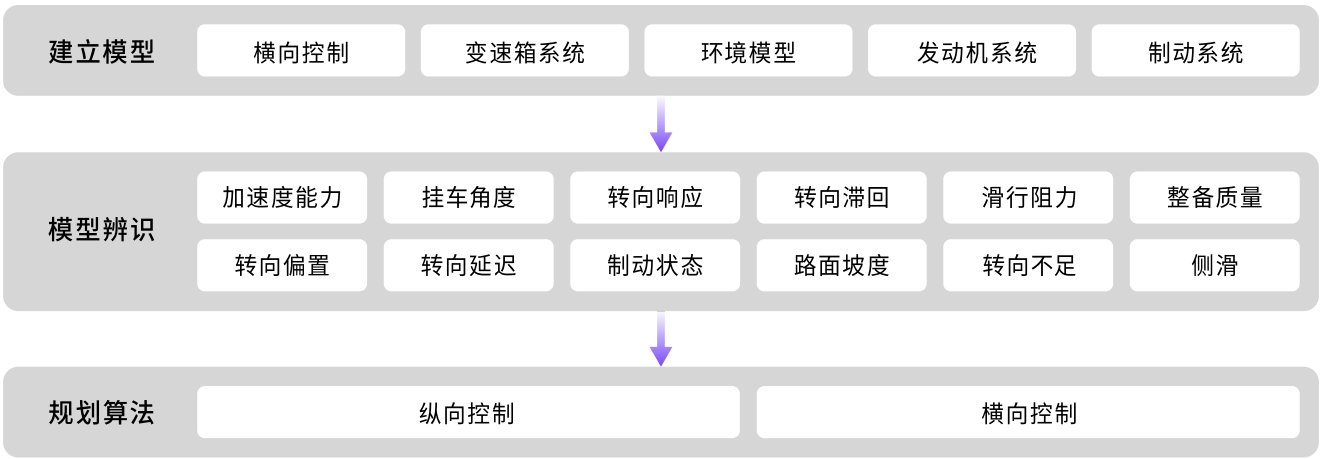
  赢彻科技开发的时序分解方案 TDPred（Temporal Decomposition Prediction），通过将完整时长分解为多个短时组合，通过金字塔式卷积操作，实现精确的高速长时长预测。



* 图：长时长预测模型

- **后决策模型：**典型的规划控制算法中，通过规则和优化算法结合的方式生成车辆的行为决策和轨迹，仅能考虑简单的车辆模型，加重了轨迹追踪产生的体感和经济性损失，如更耗油。通过引入更复杂的车辆模型，使用采样方式生成车辆可达到的所有动作空间，并使用神经网络综合决策最优的驾驶行为，获得安全、舒适、经济和耐久综合最优的驾驶策略，满足商业重卡的运营需求。

- **车辆参数自适应建模：**构建自适应的模型辨识技术成为量产条件下控制技术的重要组成部分。在车辆的运行过程和不同动态下，对于车辆和环境进行了一系列的建模，同时通过在线学习的方法实时更新模型参数，并反馈给控制器，从而解决商用车车辆生产精度低、运营过程中车辆参数偏移和复杂运营环境等方面的问题。



* 图：车辆控制参数自适应建模

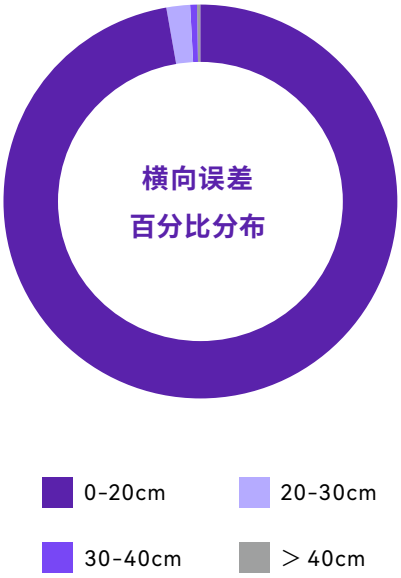
- **基于模型的预测控制：**通过模型预测算法，在设置的安全边界内尽量减少控制调整，兼顾舒适性、经济型和耐久性。同时还需要在横纵一体控制算法方面取得突破，整合车辆的横向控制和纵向控制，从整体上给出系统最优驾驶行为。

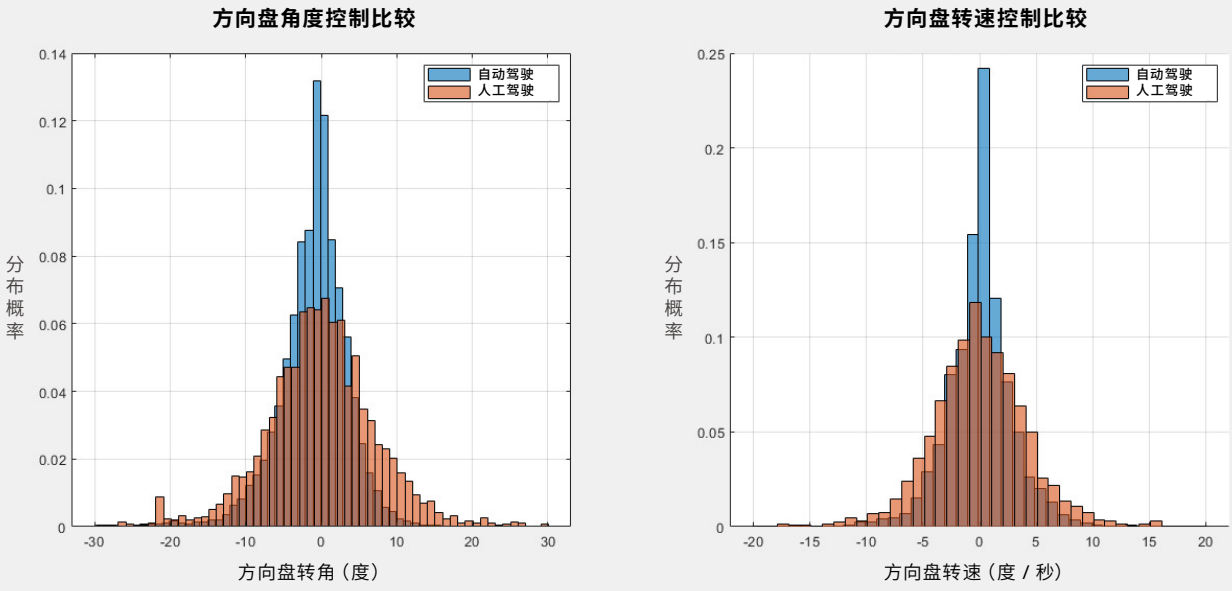
- **车辆底盘多系统控制：**将传统的仅实现对车辆的横向（方向盘）、纵向（加减速踏板）控制，逐步升级为增加对车辆辅助制动系统的控制、对车辆电子手刹系统的控制，乃至未来实现对车辆变速箱的控制。通过对底盘多系统的控制，实现兼顾舒适性和耐久性。

规划控制一体化应用

赢彻科技结合量产落地，通过独创的车况自适应模型辨识技术和核心算法，成功克服了车辆精度低、参数漂移等难题，成功落地到实际运营中：

- 横向控制的平均误差控制在 5.5cm 以内，其中 0-40cm 超宽挂车不压线的占比达到了 99.825%，0-20cm 无体感偏差占 97.45%。
- 方向盘的调整角度和调整转速都低于人类驾驶员，在保证安全和高精度的同时，综合保证了车辆的耐久性。基于在相同路段条件下的实验，对比自动驾驶系统和人类驾驶员的横向控制能力（方向盘转角与转速），结果表明：自动驾驶系统更倾向于以小角度对方向盘进行小幅调整，且方向盘调整转速明显低于人工驾驶。不仅确保了更舒适的乘坐体验，而且对底盘系统机械件磨损更小，提升耐久性。





* 图：方向盘控制转角转速时长分布

3.2.4 节油解决方案 FEAD (Fuel Efficient Autonomous Driving)

重卡是重要的交通运输工具。在中国，重卡运营中的油耗成本在 TCO 中的占比达 30%，是商业运营中的高度敏感项。因此，节油减排是刚性需求和关键能力。

节油优化的目标

重卡行驶过程的油耗，与三种车辆控制行为紧密相关：

- 车速：让车辆工作在最佳巡航速度
- 刹车：尽可能减少刹车带来的能量损耗
- 油门：尽可能稳定地控制油门

节油优化的切入点

商业运营环境中存在大量影响油耗的限制因素，使得重卡节油无法简单地对以上三点进行理想化的独立优化。基于赢彻科技的探索与实践，商业运营条件下的重卡节油可从以下四方面同时切入：

- **小时级效果优化——时效与油耗平衡：**运营重卡通常有严格的时效要求，在满足时效要求的条件下，平均时速越低越省油，但是在长达 10 小时以上的重卡运输任务过程中，做到这一点并不容易，要充分考虑全程的载重、交通拥堵和时效等因素的影响。
- **分钟级效果优化——起伏坡道工况：**运营重卡在上下坡过程中，速度受重力影响较大，优秀的人类驾驶员会通过一系列精确的冲坡、溜坡等操作达到可观的节油收益。因此在连续坡道工况下，如何在爬坡过程中以能量最优的方式降低车速，如何避免在下坡过程中使用制动减速等问题，都需要通过技术手段进行解决。
- **秒级效果优化——局部交通流：**经验丰富的人类驾驶员对周围车辆的行为通常都有准确的预判，同时会配合变道、避让和弹性跟车等多种保护性驾驶策略实现保证安全情况下的平稳驾驶和油耗最优。自动驾驶重卡在应对局部、微观交通流时，如何像优秀的人类驾驶员一样节油仍是极具挑战的技术问题。
- **亚秒级效果优化——发动机和变速箱控制：**在微观车辆控制层面，自动驾驶技术如何智能地控制变速箱挡位，实现发动机尽可能靠近最佳燃油经济区也是技术难题之一。

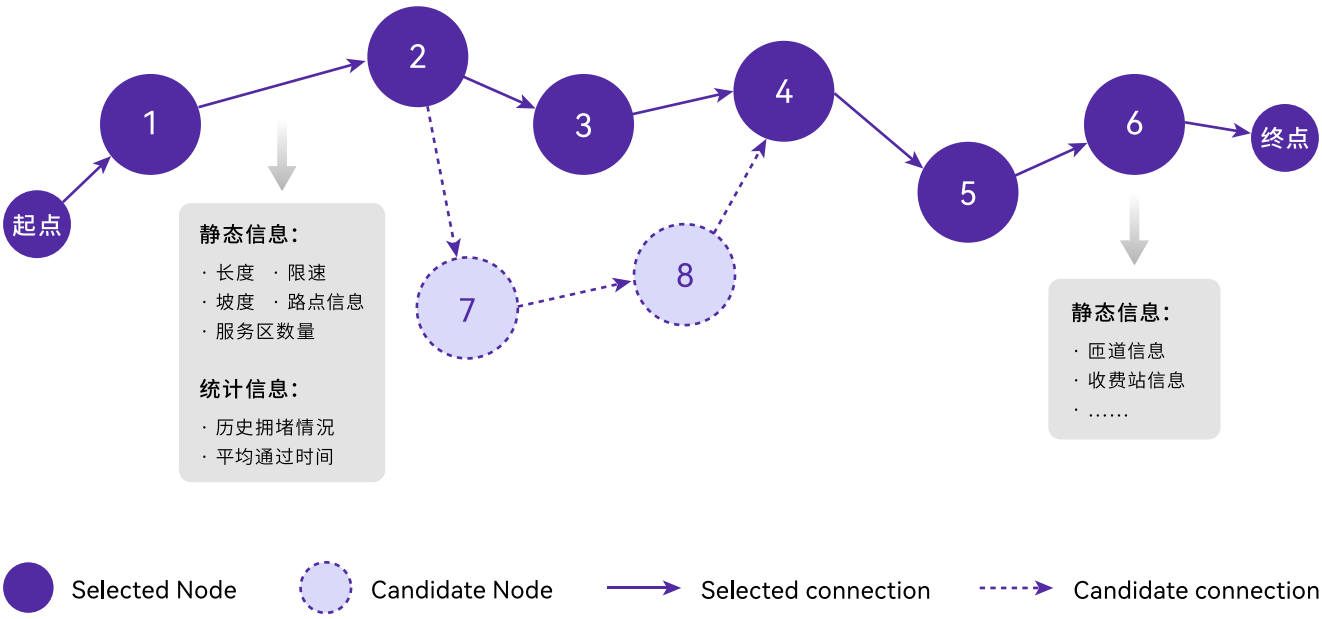
* 图：赢彻科技 - 节油算法技术路线

赢彻科技节油解决方案 FEAD (Fuel Efficient Autonomous Driving)

赢彻科技的节油技术路线构建了一套完整的技术栈，从以上 4 个切入点出发，形成综合性的 FEAD 解决方案，取得了商业运营环境下良好的节油效果：

- 在车辆使用周期内，选择风阻优化与最优轮胎。
- 小时级 - 车云协同全局速度规划：基于图神经网络 GNN (Graph Neural Network) 技术，在云端建立以关键途径点为节点的图神经网络，利用历史经验数据和即时交通数据，实现最优的速度推荐。

针对每一条运营路线，根据历史运营数据特征（拥堵、平均车速等）和实际道路特征（坡度、车道数、服务区等）构建有向无环图，并利用图神经网络和历史数据训练进行训练，以获得兼顾时效和油耗的全局巡航车速分配策略。训练时，基于增量学习 / 终生学习 LLL (Life Long Learning) 技术不断加入最新的运营数据，持续更新并优化策略。实际运营时，依托车云协同链路，实时获得运营车辆的位置、拥堵、预计到达时间等信息，并结合离线训练的网络参数，实现最优的速度分配快速推理输出，并通过车云协同链路对每辆车实时下发定制化速度分配策略，以获得时效和油耗的最优平衡。



* 图：基于图神经网络的全局速度规划

- 分钟级 - PCC (Predictive Cruise Control) 预测性巡航：基于最优化理论，引入坡路信息以优化冲坡、溜坡策略，以得到未来 2~3KM 的最优效率的发动机功率输出。
- 秒级 - 弹性跟车、智能避障等决策规划策略：融合自动驾驶决策算法，以实现更节油的自动驾驶策略。
- 亚秒级 - 油门与变速箱控制等多种控制策略：基于最优控制理论，优化油门和变速箱控制，实现更节油的微观控制。

效果评估

在实际商业运营中，自动驾驶重卡的最终油耗表现受到多方面因素影响，暂无统一准确的评估方案，且存在较大挑战：

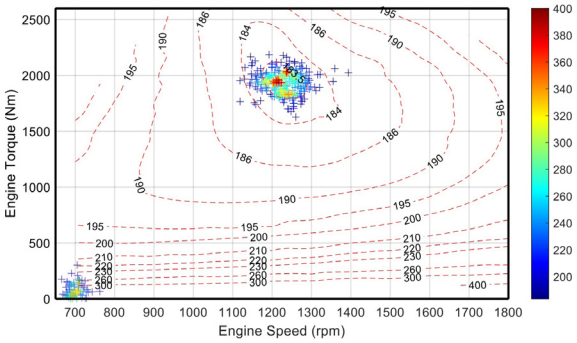
- 单次运营结果呈现一定波动性，缺乏具备统计意义的评估数据。
- 缺乏统一、精确的油耗基准。
- 缺乏针对理论节油上限的分析。

为了建立符合统计意义的油耗基准，需要将影响油耗表现的因素进行分类，建立对应的人工基准油耗查找表。建立过程中将考虑 1）运营路线：如华北线、华南线等，并统计对应山路 / 平路占比；2）负载重量：快递货（8~15 吨）、快运货（15~25 吨）和专线货（25~30 吨）；3）时效要求：根据在途高速路程，利用平均速度进行划分等。过程中还需要对大量实测数据进行处理和挖掘。

基于上述评估体系，在多条商业运营线路上，智能重卡相比于快递快运行业的金牌驾驶员，达到了 2%-5% 的节油收益。

重卡自动驾驶节油上限分析

油耗水平可通过发动机燃油消耗率图 BSFC（Brake-Specific Fuel Consumption）的分布进行表示。理想状态下，发动机始终工作在最佳状态，即 BSFC 图等高线中心，如右图所示。油耗优化的目的在于让发动机工作状态的分布向 BSFC 图等高线中心逼近。

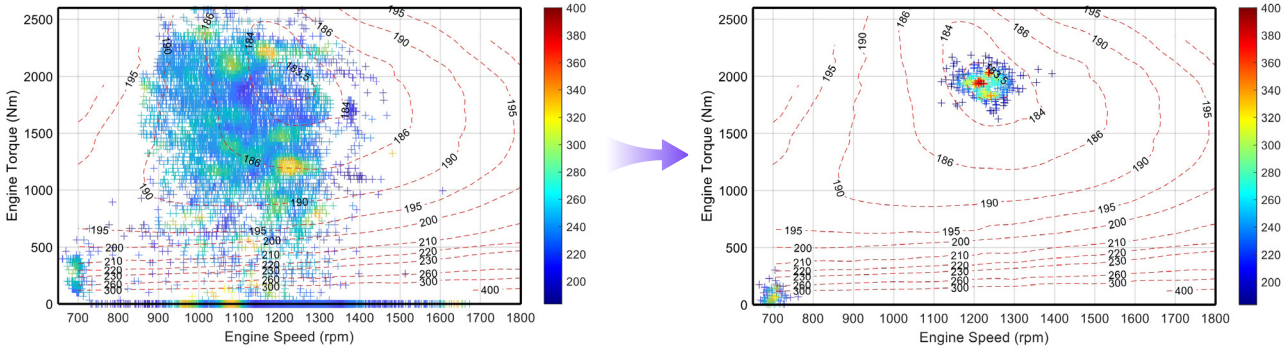


* 图：发动机效率理想分布

我们统计了多位金牌驾驶员的油耗分布。以下是一位金牌驾驶员的典型油耗状况，具有代表性。金牌驾驶员数据来自典型丘陵 - 山区综合工况，测试车辆为联合量产的智能重卡，发动机型号为康明斯 Z14-560，车辆满载，搭载货运典型的超宽超高挂，车货总重 48.5 吨。

将金牌驾驶员的发动机工作分布的每一个落点移动至 BSFC 图等高线中心，即可计算出同等任务条件下的理想油耗。

通过金牌驾驶员人工驾驶油耗和理想油耗的对比，我们看到自动驾驶相对于金牌驾驶员的节油上限约为 7%。



发动机效率实际分布　　发动机效率理想分布

* 图：发动机效率优化上限分析

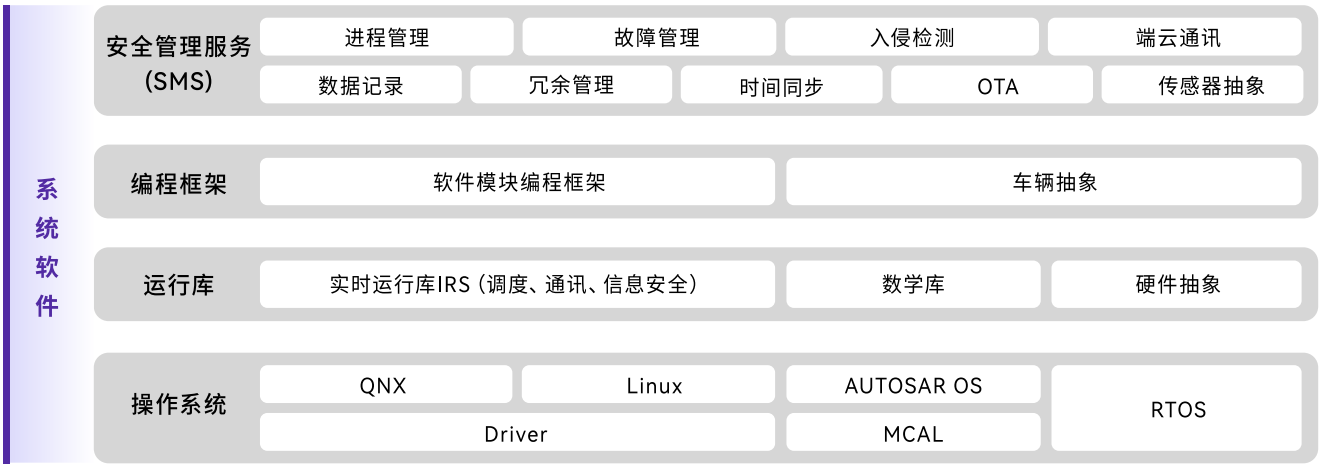
3.2.5 系统软件

为了实现高级别自动驾驶系统的成功量产，对其可靠性、性能、安全性以及研发效率提出了严苛要求。系统软件介于算法和计算平台之间，承上启下，是满足上述要求的关键。

自动驾驶系统软件的具体要求

要求	描述	系统软件的作用
可靠性	系统的稳定运行	检测各种软硬故障和外部攻击，确保系统在任何情况下都能自我恢复，保持稳定运行
性能	整体系统的延迟，影响到算法性能和系统的 FHTI（Fault Handling Time Interval，故障处理时间间隔）	降低任务的等待延迟和任务间的通讯延迟
安全性	车辆的安全	在意外情况下，确保车辆的安全以及安全员能及时地接管
研发效率	友好的开发集成环境	提供高效的开发 API（Application Programming Interface）和工具，减少开发人员的手工代码量，帮助开发人员校验代码的正确性，提高调试的效率

赢彻科技系统软件设计理念与实践



* 图：赢彻科技 - 卡车自动驾驶系统软件架构

为满足量产对系统软件的上述四项要求，赢彻科技在系统软件设计上，对软件进行了合理细致的分层设计。遵循 SOA（Service-Oriented Architecture，面向服务的架构）理念，上层应用软件与底层硬件（ADCU、车辆）解耦，以提升迭代效率，顺应业界发展趋势。同时，底层软件设计针对硬件特性进行优化，提升整体系统的性能。层与层之间、模块与模块之间的标准化接口设计，大幅度减少系统复杂性，提高代码的重用，不仅为工程师提供友好的集成环境，也增强了整体系统的可靠性。赢彻科技系统软件自下而上包括：

- **操作系统：**赢彻科技对操作系统、驱动和微控制器抽象层 MCAL（Microcontroller Abstraction Layer）进行了集成定制，以支持自研的 ADCU。考虑到不同任务对计算性能、功能安全和实时性等要求不尽相同，在 ADCU 的不同功能域中采用了多种不同的操作系统，以高效满足不同应用软件的需求。

ADCU 上不同功能域的操作系统选型

功能域	操作系统	选择理由及作用
安全域	AUTOSAR OS 操作系统	AUTOSAR OS 有 ASIL-D 功能安全等级，能帮助系统软件在失效情况下降低危险
AI 计算域	实时操作系统 RTOS	RTOS 能有效提高感知模块的实时性，降低系统 CPU 资源的消耗，通常 SoC（System on Chip）的 CPU 算力不高，且软件模块较单一
通用计算域	从 Linux 过渡到 QNX	Linux 由于开发门槛低，软件生态健全，能有效提升开发落地效率。QNX 的实时性可靠性更好，还有功能安全等级，对系统的稳定运行更有保障

- **运行库（Runtime）：**赢彻科技自研了三项运行库，给上层算法应用和系统服务提供基本的系统功能。

自动驾驶系统运行库（Runtime）

运行库	作用
实时运行库（IRS，Inceptio Robotics System）	提供一系列自研的基本系统功能，包括资源调度、模块间通讯、信息安全、数据记录、日志和诊断等功能
数学库	定制了赢彻科技算法软件常用的算子，包括矩阵、聚类、滤波、张量等运算
硬件抽象	赢彻科技自定义的标准化 ADCU 监控与操作接口（比如上下电、诊断监控、外设访问等等），进一步对上层应用软件和 ADCU 进行解耦

- **编程框架：**赢彻科技自研的编程框架提供声明式的编程模型，按照软件模块的架构定义，自动生成 C++ 代码，并对整个软件部署方案进行正确性校验。支持车辆抽象，提供车辆功能的标准化通讯和调用接口，使上层应用软件能快速适配不同车型。
- **安全管理服务：**提供一系列赢彻科技自研的自动驾驶系统基本服务，确保系统在整个生命周期里的持续安全稳定运行。

自动驾驶系统安全管理服务

服务	作用
进程管理	调度和监控所有自研系统内的软件模块的执行，确保在软件运行出现异常时，对软件模块进行重置，确保软件平稳运行
故障管理	监控自研系统内所有软硬件故障（诊断），确保在故障发生时，进行合理的安全操作
AD 状态机管理	管理整个系统的自动驾驶状态机，协同所有软硬件和车辆底盘的进、退 AD 操作，确保进退 AD 操作的安全
入侵检测	监控系统的各项行为，检测并报告可疑的黑客入侵
端云通讯	执行赢彻科技卡车和云服务之间的实时双向通讯，并确保通讯的安全和稳定
数据记录	记录并保存系统的各项数据，支撑自研的数据闭环，加速迭代开发，并在事故发生时提供关键数据
冗余管理	监控卡车和 ADCU 的主备系统状态，确保在主系统发生故障时，执行冗余切换操作
时间同步	负责 ADCU 上各芯片和传感器之间的时间同步
OTA	负责各软件模块和硬件固件的升级，支持智能卡车上所有电子控制单元（ECU）的升级
传感器抽象	提供传感器数据的标准化接口，使自研的上层应用软件能灵活适配各种传感器型号

首先，设计了基于声明式编程（Declarative Programming）的编程框架，让开发人员聚焦于算法等应用逻辑层面。相较于传统的命令式编程（Imperative Programming），以更加简洁的配置方式定义整个自动驾驶系统中各软件模块的运行、调度、交互、监控和数据记录等。此外，通过代码生成（Code Generation）技术，支持非算法和业务逻辑代码的自动生成和校验，以及硬件和车辆抽象的定义与配置，大幅度提高了软件研发的效率和代码质量，为多种车型的可靠量产提供了强有力支撑。

其次，针对自动驾驶系统的延迟指标进行创新设计。长延迟会降低跟踪精度和系统反应能力。赢彻科技自研的运行时库 IRS（Inceptio Robotics System）为整个系统提供了高性能的板载实时通讯与调度功能，采用了创新的跨域全局调度和通讯优化算法，让系统能自动地以最优的方式调度软件模块和执行模块间的通讯，极大的提升了整体系统的延迟表现，以满足自动驾驶算法软件对系统性能的高要求。

最后，设计安全管理服务层 SMS（Safe & Security Management System），确保自动驾驶基础服务的安全高效。SMS 的创新设计包括独有的多级冗余设计（车辆、计算平台、系统软件）、实时错误监控和自恢复（监控 30+ 车端零部件、2000+ 诊断）、基于 ISO21434 设计的信息安全管理、高实时高吞吐的数据记录和车云通讯、高精度时钟同步（30ns）等。上述设计为卡车提供强大安全保障，并提高了算法性能和迭代效率。

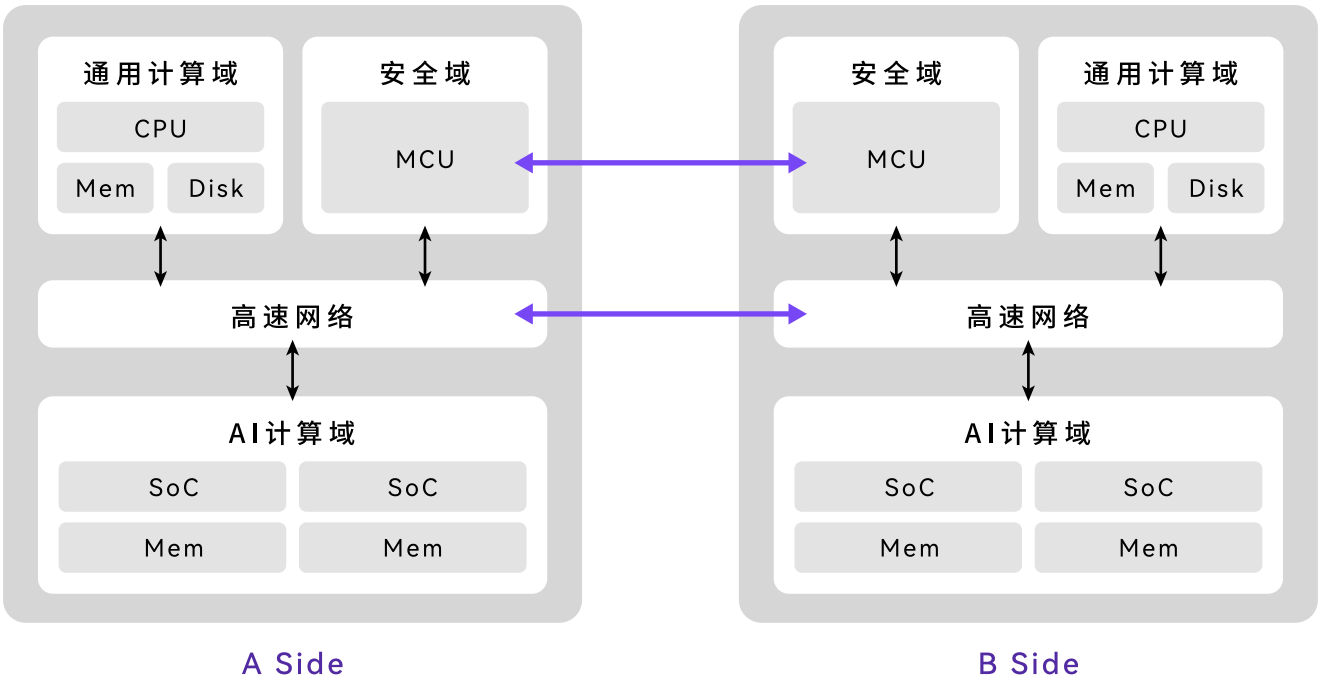
3.2.6 自动驾驶域控制器（ADCU）

为达成计算性能、综合成本和功能安全的系统集成要求，赢彻科技选择自主研发自动驾驶域控制器（ADCU），其核心任务包含：

- 为实时运行的自动驾驶算法和应用提供重要的计算、存储和网络通信能力。
- 提供重要的基础服务功能，包括电源管理、软硬件健康监控、系统诊断、失效处理恢复、功能冗余、时间同步等。
- 系统全栈自研，确保赢彻科技在设计流程、功能开发、集成验证、生产规范等诸多环节均能高效地达成商用重卡车规级的量产需要。

在设计研发和量产生产阶段，ADCU 系统的异构复杂性和商用车车规对工程设计研发能力提出了极高要求：

- **异构复杂性：**自动驾驶软件系统由大量模块组成且非常复杂，不同模块对 AI 算力、浮点算力、功能安全、网络吞吐和数据存储等存在不同需求。为了满足多样化的需求，ADCU 必须采用异构化的设计，需要不同能力的芯片和元器件，显著增加了 ADCU 硬件设计的复杂性，且需要保证规模量产条件下的稳定可靠。
- **商用车车规：**ADCU 系统的设计目标是应用于前装量产级的商用卡车，必须符合商用车车规。这对硬件的电气、电磁兼容性、机械、环境耐久等方面提出了非常高的要求，对震动和寿命的要求比乘用车更高。



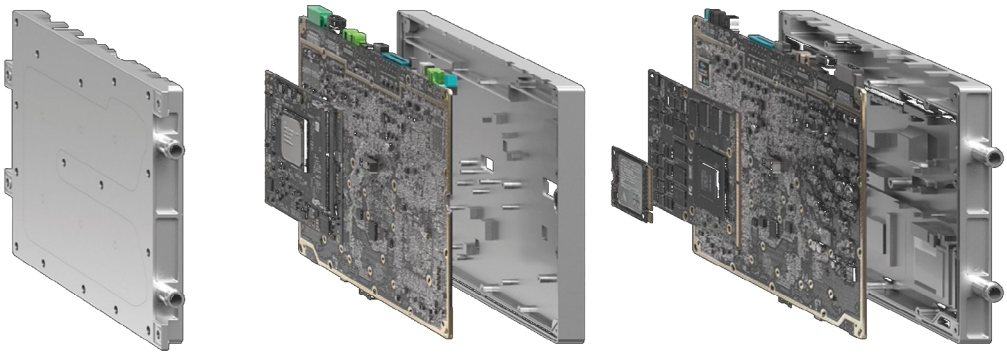
* 图：赢彻科技 -ADCU 硬件架构示意图

赢彻科技的 ADCU 采用了异构设计方案，多个不同的功能域满足不同核心任务的需求。通过模块化的设计方式，各功能域分布在原理图和 PCB（Printed Circuit Board）的不同区域，域与域之间采用统一的高速网络架构相连。不仅方便硬件的升级和适配，也支持系统软件层的硬件抽象。此外，基于两块板子之间的高速连接，还实现了 A/B 双面全冗余的设计，在安全方面满足了 L4 及以上高阶自动驾驶的需求。赢彻科技 ADCU 在设计上包含的功能域如下：

ADCU 多功能域定义

功能域	主要芯片	功能	描述
安全域	MCU	车辆行驶安全	自动驾驶状态机管理，车辆控制信号安全检查和校验，冗余管理，ADCU 和车辆健康监控，系统诊断和失效处理
		基础硬件服务	电源管理，ADCU 与车通讯服务
AI 计算域	SoC	感知	视觉感知，激光雷达感知，预测
通用计算域	CPU	感知、定位和规控	感知，规划，控制，定位，标定
		通用系统服务	车云通讯，数据记录，信息安全，时间同步 master
高速网络	Switch	通讯	板载通讯，高精度时间同步

赢彻科技第一代 ADCU 系统，是卡车领域算力领先的车规级计算平台，已成功量产。系统具备高算力、高能效、高安全的特点，车规级的算力达到 355K DMIPS + 46 TOPS，最高算力可达 245TOPS，能效比高达 1.53TOPS/W。系统支持丰富的高阶自动驾驶传感器接入，最高可支持 12 路 4K 高清摄像头、10 路以上 1000/100 Base T1 以太网、22 路 CAN（Controller Area Network，控制器局域网络）接口、内置 GNSS 传感器等，均为行业领先水平。ADCU 支持时间同步精度达到 30 纳秒的 TSN（Time-Sensitive Networking），确保不同传感器的高精度时钟同步，显著提升了感知融合的精度。



* 图：赢彻科技 - 第一代量产 ADCU 设计

赢彻科技第二代 ADCU 在满足商用车车规的前提下，对 AI 计算域、通用计算域和高速网络进行了全面升级。

- **性能方面：**单板车规级的算力高达 256 TOPS，提供 16Gbps 的高速 PCIe 带宽，用于芯片间的数据传输，大幅度提升深度学习的能力，进一步提升感知的精度和距离。
- **功能安全方面：**通用计算域具有功能安全等级，具备全新的故障监控设计和自恢复设计，显著提升系统安全性。

赢彻科技 ADCU 的设计创新

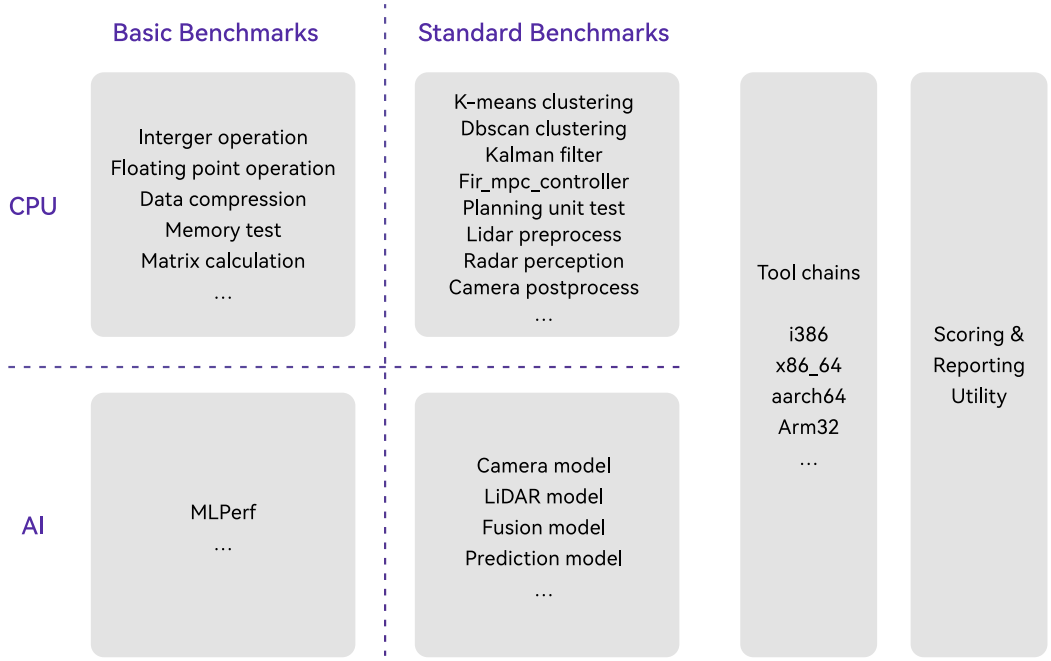
首先，赢彻科技在 ADCU 设计层面充分保证整体自动驾驶系统的可靠性、高可用性和功能安全：

- 支持对 ADCU 上的主要芯片以及车载电子控制单元（ECU）进行状态监控以及重置；
- 支持对不同域的故障进行风险隔离；
- 具备足够的冗余设计，即使出现不可恢复的故障，仍保证车辆操作安全可靠。

自动驾驶系统是由成千上万元器件构成的复杂系统。ADCU 中的任何元器件都有可能在任何时间出错。上述设计是确保整车自动驾驶功能稳定可靠的重要一环，对量产卡车在道路上的安全行驶起着至关重要的作用。

其次，赢彻科技形成了一套业界领先的 ADCU 性能评价标准。这套标准为设计出更满足自动驾驶量产要求的 ADCU 提供了指引。自动驾驶系统高度复

杂，对硬件性能的要求是多方面的，单一指标不能合理且全面地反映出硬件在自动驾驶方面的综合能力。传统的硬件性能指标，如 DMIPS（Dhrystone Millions of Instructions Per Second）和 TOPS（Tera Operations Per Second），只能反映出硬件在某些特定运算操作上的算力性能，并不能真实地体现自动驾驶所使用的各种复杂算法在该硬件上的性能，更不能反映出硬件的内存带宽、网络带宽、ISP（Image Signal Processing）的处理能力等。为此，赢彻科技沉淀积累了一套标准的自动驾驶系统与应用的性能评测程序集 ISPEC（Inceptio Standard Performance Evaluation Code），收集了多种自动驾驶有关的典型运算程序，并由不同工具链在不同硬件平台上编译执行。该方案为评估不同硬件平台在自动驾驶上表现出的综合能力提供了真实可靠的依据，包括 CPU 和 AI 算力、内存吞吐率、对不同算法模块的适配性能、工具链的易用性等。



* 图：赢彻科技 - 自动驾驶性能评测集 ISPEC

最后，着眼于未来 L4 发展要求，赢彻科技 ADCU 的硬件架构充分考虑了高算力的延展性。

- **高算力：**赢彻科技 ADCU 在原理图和 PCB 上都采用了模块化设计，支持更灵活地对 AI 计算域的 SoC 进行升级。在将来 SoC 算力升级到 500~1000TOPS 时，赢彻科技 ADCU 能平滑演进支持 L4、L5 级别的自动驾驶能力。
- **冗余：**赢彻科技 ADCU 的硬件架构支持 A/B 双面全冗余，当一面硬件失效后，另一面可以平滑接管车辆控制，保持正常的安全行驶操作，为 L4 级别无人驾驶车辆应对复杂场景提供了充分的安全保障。
- **高速通讯：**赢彻科技 ADCU 的网络设计也考虑了未来自动驾驶算法应用的需求，由以太网构成各芯片之间的骨干网络，支持 30 纳秒的时间同步精度，以满足高阶自动驾驶感知对时间同步精度的要求。另外，设计 PCIe 网络，用于 AI SoC 之间的高速数据交互，以及 SPI（Serial Peripheral Interface）连接用于高可靠的诊断监控，和以太网互为补充，共同组建高效且可靠的网络结构。未来当 ADCU 算力满足 L4 所需时，基于这套硬件架构的赢彻科技自动驾驶系统可以方便升级到 L4 无人驾驶。

3.2.7 车规级硬件套装

自动驾驶硬件套装构成

硬件是自动驾驶系统运行的基石。赢彻科技硬件套装由自研自动驾驶域控制器 ADCU、长距及补盲 MEMS 激光雷达、毫米波雷达、摄像头、舱内监控摄像头、多功能集成天线、网关、智能通讯终端、多媒体控制器等器件组成。该套装具备传感器清洗、安全员管理、通讯与网络安全管理、人机交互等功能，并为自动驾驶系统提供了车身周边 360°多传感器融合的冗余环境感知信息。

毫米波雷达

摄像头

补盲激光雷达

长距激光雷达

自动驾驶域控制器

网关

智能通讯终端

多媒体控制器

组合天线

* 图：硬件套装主要部件

车规级要求与验证体系的建立

车规是量产的基础要求。汽车产业的百年经验证明，工业级或消费级零件在车载工作中不仅无法表现出实验室条件下的优良性能，还会出现更高频的失效、故障与寿命锐减等更严重的安全风险问题。

相比乘用车，商用车的生产工具属性及应用场景的特殊性对零部件提出了更苛刻要求，要求零部件必须在更恶劣的环境中保持更长的连续工作时间。

鉴于行业规范与通用标准尚不完善，赢彻科技自主制定了零部件测试企标。基于商用车行业的通用国标 GB/T 28046，参考了乘用车行业成熟经验，补充完善了诸多功能测试项，并基于实际场景拓展设计了对应的性能测评条目，形成了一套完整的符合商用车需求的硬件车规级要求与验证体系。

选型与开发原则

车规量产是首要衡量标准。商用车行业上下游在自动驾驶方面的开发经验不够成熟，以激光雷达为代表的供应链成熟度相对不足，一些关键测试与评价方法也存在欠缺。在各部件的选型与开发过程中，赢彻科技并不一味追求短期便利性或极端性能表现，而是始终坚持车规级标准与量产一致性要求，以保证整套系统功性能的稳定与可靠。

产业链合作

产业链的合作是成功路上必不可少的一环。一方面，赢彻科技深度参与了供应商的设计评审、制造改善、测试执行、性能优化等零件级开发与释放全流程；另一方面，赢彻科技和 OEM 合作进行了关联件设计、装配验证、功性能测评等系统与整车级的研发与验证。通过三方联合、快速迭代、贡献各取所长，共同推动了产业与行业的进步。

前激光雷达

补盲激光雷达

周视摄像头、后视摄像头

后毫米波雷达

角毫米波雷达

前毫米波雷达

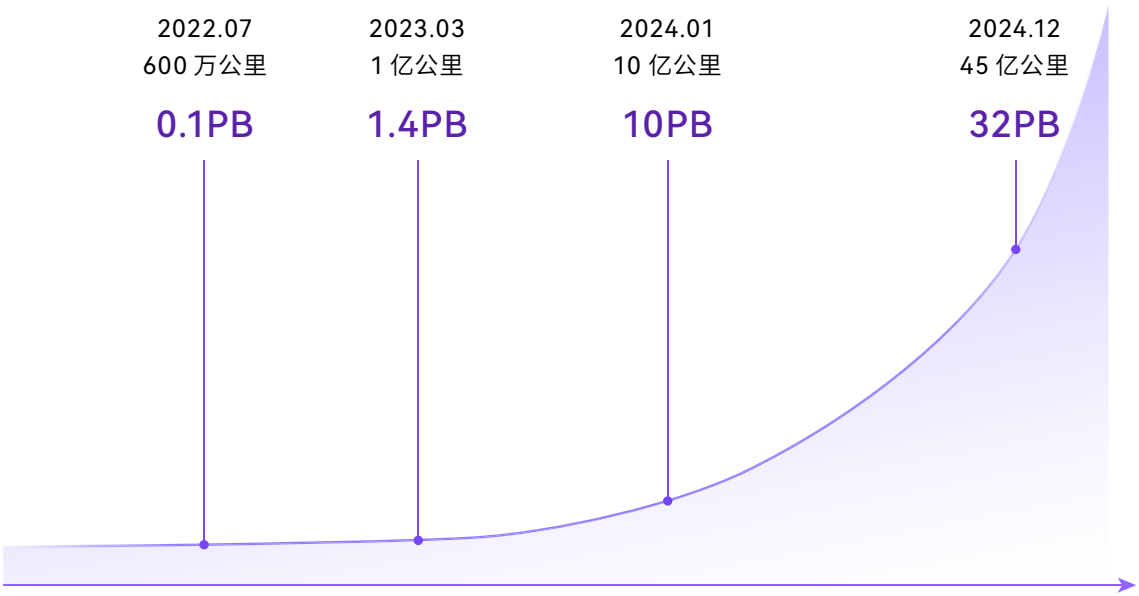
* 图：与整车融合设计的前装量产硬件套装

伴随着整车量产，硬件套装中每个部件均历经了完整的 EV（Engineering Verification，工程开发试验）、DV（Design Verification，设计试验）和 PV（Production Validation，生产过程验证），参与了整车的高寒、高温与耐久测试，达成了 OEM 认可的 PPAP（Production Part Approval Process，生产件批准程序），是真正意义上的行业内首套商用车车规级自动驾驶系统硬件套装。

3.3
云基础设施

随着自动驾驶进入量产和商业化落地阶段，自动驾驶公司所获取的数据量呈指数级上升。云基础设施贯穿于自动驾驶研发全流程，面临全新挑战：

- **海量异构数据处理：**自动驾驶数据的典型特征是结构化、半结构化及非结构化并存，且数据应用场景复杂多样。量产自动驾驶车辆所产生的海量数据对云基础设施提出极致要求，尤其是在提供算力资源、安全可靠和支持弹性灵活的业务需求等方面。
- **高度自动化：**自动驾驶进入量产阶段，单纯依靠人工无法支撑高阶自动驾驶算法的快速持续迭代，尤其是数据标注和缺陷分析（Issue Triage）等。
- **研发效率提升：**自动驾驶不同研发阶段的工具需要全链打通，以提升系统迭代和运维效率，降低开发成本，加速数据闭环。
- **高可移植性：**基础设施需要适配多种运行环境，应对不同云厂商和运行环境的变更适配。



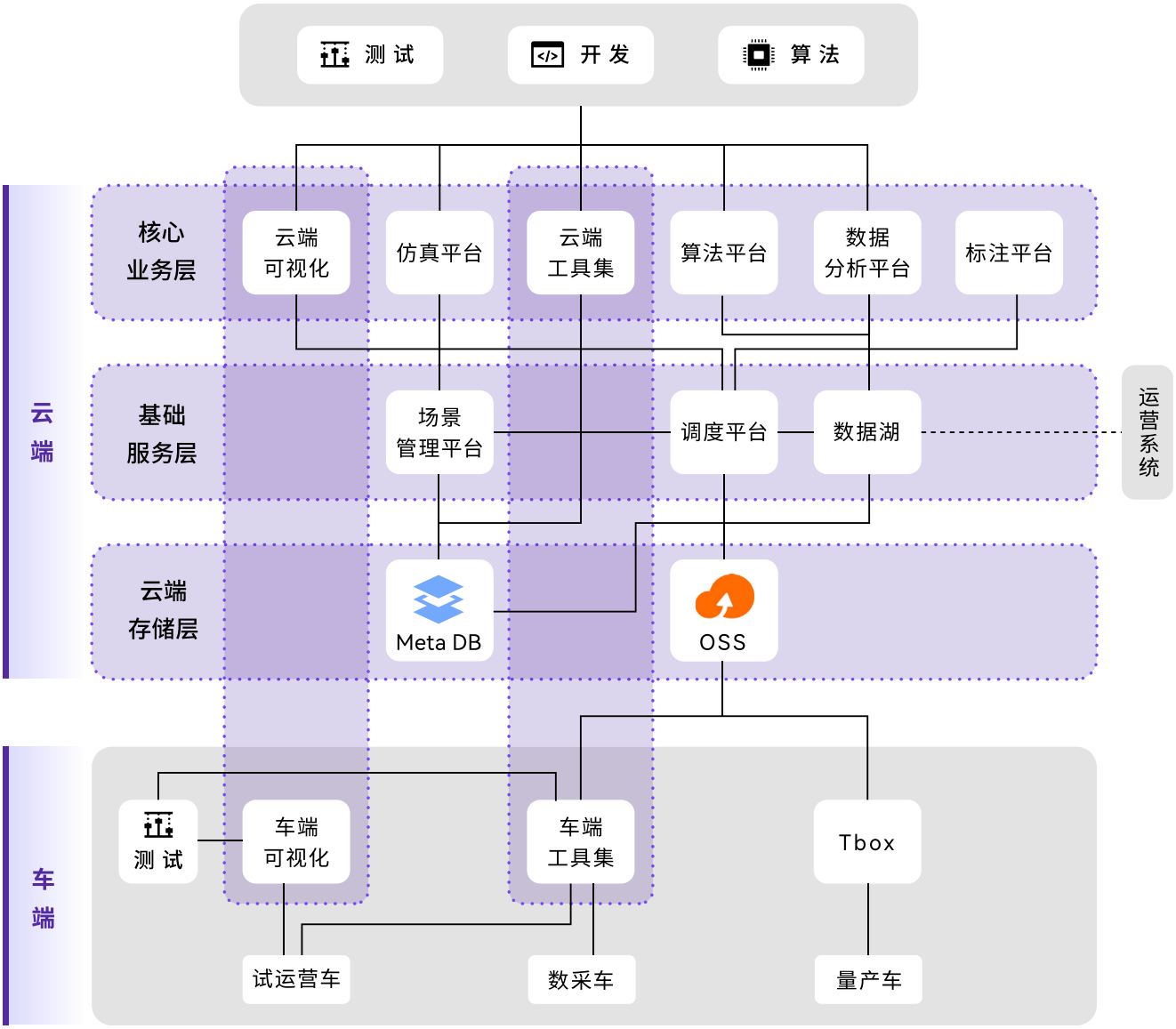
* 图：赢彻科技自动驾驶数据规模增长趋势

基于可扩展性、成本、安全可靠性和研发效率等需求，上云已经成为自动驾驶公司从开发到商用的行业趋势。赢彻科技作为一家为量产而生的自动驾驶公司，云端基建是其始终如一的技术战略方向，历经三年多时间，在云端打造了“三横两纵”的基于云原生的技术栈：

- **三横：**云端存储层、基础服务层、核心业务层。
- **两纵：**车（云）端可视化平台 Overwatch、车（云）端工具集 Chariot。

基于云上基建，赢彻科技目前已实现：

- 数据采集、数据标注、模型训练、大规模仿真验证和模型部署上线的周期缩短至 3 周以内；
- 跨云（x86 架构）和边（ARM 架构）的边云协同仿真；
- 日均处理数据量达 PB 级别；
- 支持多云；
- 单集群并发度破万；
- 计算集群可水平扩展，支撑量产车辆数达万级；
- 核心指标端到端延迟达亚秒级别。



* 图：赢彻科技 - 自动驾驶云基础设施系统架构

自动驾驶数据湖

数据作为赢彻科技的核心资产，通过建立数据湖对来自车辆、运营以及内部工具产生的数据进行管理，主要有以下的特性：

- **统一的数据管理：**通过提供统一的元数据管理，给数据使用方提供一致的读写方式，屏蔽底层的差异化。
- **高效的存储：**使用云上对象存储作为数据湖的存储方案，相对于传统的 HDFS（Hadoop 分布式文件系统）方案效率更高，成本更低且更易扩展。
- **云原生的存算分离架构：**大规模量产所产生的海量数据，需要高算力进行处理和分析。我们采用存算分离的架构，相较于本地数据中心，成本降低 50% 以上。通过云原生方式管理所有计算节点，使得计算集群能够按需快速拓展，以满足并发度过万、日处理数据量达 PB 级别、核心指标端到端延迟在亚秒级别等大规模分布式计算的要求。
- **数据安全合规：**赢彻科技对高度敏感的数据存储及使用采取了一系列安全措施，根据数据安

全相应的法律法规及处理指南采用如安全访问控制、脱敏处理、数据软加密、硬件加密存储等多种措施保证数据的机密性、完整性、可靠性、可用性等一系列安全属性。

- **一站式的数据应用开发：**大数据的使用有较高的门槛和开发成本。我们端到端地打通了数据链路，并提供了一套成熟的数据开发流程，使内部用户能够轻松地对数据进行开发、调试及可视化，大大降低数据平台的使用门槛。

调度平台

赢彻科技的日常迭代需要大量的计算作业，为了高效地协调计算资源，我们搭建了调度平台，提供以下的能力：

- **标准化的资源管理：**计算集群存在多种异构硬件（CPU、GPU、NPU），分散在多个集群和多个云厂商，且不同的计算任务差异较大，高效管理存在巨大挑战。我们建立了基于 Kubernetes 的统一的资源申请和使用方式，通过任务流对计算任务进行编排，增强了多租户和多集群管理，大大减少了运维和管理的难度，能够快速调度多个云厂商的计算节点。
- **弹性的基础设施：**现阶段计算任务通常是短时的任务类型，并且具有潮汐效应，需要高效的弹性计算。通过将所有任务进行容器化，以容器作为调度单元减少调度时长，同时利用云厂商的弹性实例来动态卸载突发的大量计算任务。从而实现了分钟级上万的并发计算，且在业务空闲时及时释放计算节点，相比于传统的自建机房和基于虚拟机的计算，具备更快的资源调度，节约了大量成本。

场景管理平台

场景集作为算法和仿真的燃料，在自动驾驶的研发过程中十分重要，因此我们建立场景管理平台，覆盖自动驾驶研发全生命周期。通过打通场景管理和仿真平台，建立起场景识别、数据使用、回归反馈的闭环流程，支持自动驾驶研发全生命周期的场景数据服务，保障场景数据在自动驾驶业务中持续发挥价值。

仿真平台

为了持续提升自动驾驶算法能力，仿真平台成为最核心的云端应用之一。基于云原生的基础架构，赢彻科技构建了仿真平台，聚焦于仿真真实性、高吞吐下的成本控制、混合硬件架构下的边云协同仿真等优化方向。

- **仿真真实性：**为了保证仿真平台具备高置信的算法性能验证能力，赢彻科技使用“仿真输出与真实路测数据一致性对比”的方式进行仿真真实性的客观量化评测。在此基础上研发的高精度仿真复现引擎，在感知、定位、规划控制等算法方向的仿真一致性达到 90%。
- **高吞吐条件下的成本控制：**为了评估仿真平台的运行效率，赢彻科技精细测算“每公里产生的仿真花费”。通过优化任务调度器，配合灵敏的仿真节点监督，实现了高达万级别的并发仿真能力，并降低了云端计算资源浪费。此外，通

过充分利用缓存系统，在存储组件上实现了带宽和容量申请的弹性分配策略，进一步提升了仿真运行效率。

- **基于混合硬件架构的边云协同仿真：**为了支持大规模异构硬件环境下的仿真，赢彻科技建设了横跨云（x86 架构）和边（ARM 架构）的边云协同仿真（SoC-Edge Simulation）。一方面，基于真实车规硬件大幅度提升仿真真实性和运行效率；另一方面，基于边云统一调度，进一步提升了仿真全链路的自动化水平，并降低了错误率。

算法训练平台 MLOps

算法平台用于模型训练、模型管理和 GPU 资源申请，主要有以下特点：

- **高效的 GPU 集群调度：**算法平台通过灵活的多队列调度、多租户、硬件分组和动态资源调度等调度策略，使得 GPU 集群的利用率超过 90%。
- **深度的训练优化：**根据自动驾驶的特性，选用更加高效的文件存储系统和训练通信网络，并针对 GPU 计算场景深度优化，压缩训练时间达 50%。
- **完整的模型生命周期管理：**通过自研的模型训练跟踪机制，打通了边云的模型评估验证流程，大幅缩短算法迭代周期，提升开发效率达 60%。

标注平台

为了提升标注效率，赢彻科技自研了标注平台，具有以下特性：

- **自动化：**自动化体现在标注的不同环节，自动化质检覆盖率达到 95% 以上，通过自动化标注降低成本 70% 以上。
- **定制化：**承接算法和测试环节的定制化标注需求，相比外部供应商，需求响应速度更快，标注质量更高，标注周期缩减 70%。

数据可视化平台

大规模量产对问题分析效率和快速解决提出了更高要求，数据可视化是提效的关键手段，因此赢彻科技建设了自动驾驶系统和车辆状态的可视化平台，特点如下：

- **支撑场景丰富：**可视化平台支持车端实时监控、本地数据调试、云端实时回放和仿真数据对比等多种场景下的数据可视化应用。
- **信息丰富：**支持 3D 激光雷达点云、毫米波雷达点云、摄像头视频、地图车道线、诊断报错、日志分析和指标图表等 200 余项功能的可视化展示，覆盖全部的传感器和 100 多种主题数据，满足研发和运营需要。
- **插件化设计：**用户可以在数据流的生成、处理和展示等多个环节编写插件，完成数据定制化处理，满足多变的用户需求，适应产品快速迭代的需求。

3.4
数据闭环

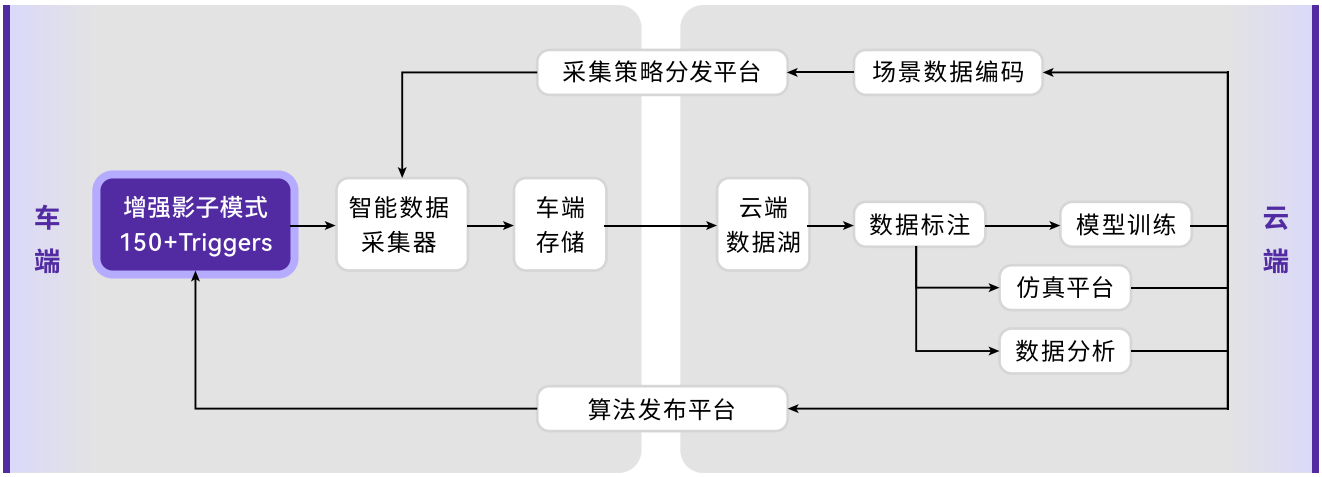
数据是自动驾驶系统的核心驱动力，海量数据、算法迭代和规模化运营构成了正反馈闭环，其关键步骤包括数据采集、数据传输、数据存储、数据处理、数据建模、数据服务等。庞大的数据规模和复杂的处理流程导致资源耗费巨大，以最低成本和最高效率获取到最具价值的数据，成为数据闭环高效推动系统迭代的关键。

自动驾驶重卡的大规模量产对数据闭环的挑战

自动驾驶重卡的大规模量产，对自动驾驶系统的可靠性和迭代速度提出了苛刻要求，进而要求数据闭环能够在缺陷发现、方案验证和持续迭代三个方面发挥显著作用：

- **同时评估“瞬时决策”和“长时行为”，全面检测系统缺陷：**系统能力缺陷将导致接管，接管前后的驾驶行为对于衡量和提升自动驾驶能力水平至关重要。“长时行为”缺陷的发现以及优化，对于 L3/L4 级别的规划控制算法不可或缺。市场主流的影子模式方案只能识别出“瞬时决策”类的能力缺陷，无法进行有效的“长时行为”相关问题识别。例如对卡车避让过程的缺陷识别，从观测、触发到最后完成整体超车动作往往需要长达分钟级的持续判定。对卡车节油策略的缺陷识别，则需要小时级别的持续判定。
- **全时段实时 A/B test，实现极速验证反馈和精准效果评估：**自动驾驶系统大规模部署前的 A/B test，对于确保系统迭代效果至关重要。A/B test 基本前提是“在相同条件下”进行 A/B 两种方案的对比。为了尽量达到“相同条件”的要求，传统的 A/B test 有 2 种做法：①先后部署 A/B 两种算法，并拉长测试周期，以令 A/B 两次实验的场景覆盖趋同，此方案缺点是：时效低，无法快速获得缺陷情况（Issue Case）并进行分析；②将部署 A 算法得到的数据全量上传云端，再对 B 算法执行云端仿真，此方案缺点是：数据采集和回收成本较高。
- **基于高价值场景甄别的数据成本控制：**自动驾驶系统持续优化所需的高价值数据日趋长尾化，这越来越多地需要全角度、全传感器、更长时、场景覆盖率更广的数据积累，对数采的数据质量和全面性提出了很高的要求。降低数据成本的难度极速提升。

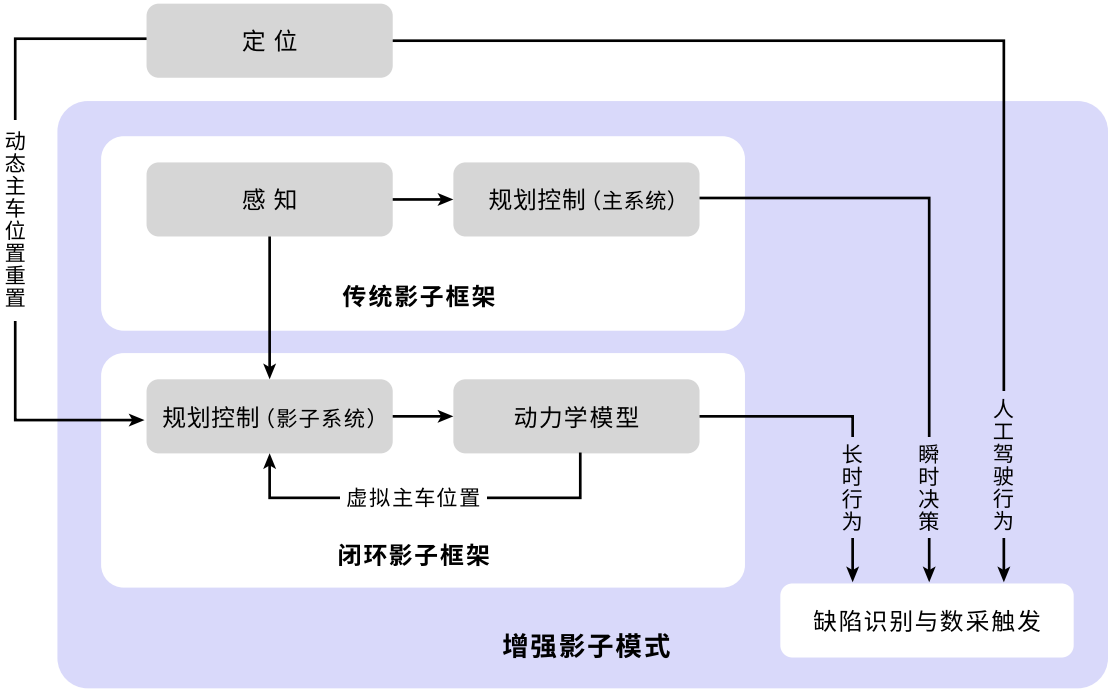
基于增强影子模式的数据闭环体系



* 图：赢彻科技 - 基于增强影子模式的数据闭环体系

为了解决自动驾驶大规模量产中面临的上述问题，赢彻科技在构建数据闭环时特别考虑从数据源头进行独特设计，研发了**基于增强影子模式的车云一体数采框架**，大幅提升了车端自动驾驶系统的缺陷检测、方案验证和高价值数据甄别的效率，大幅提高了场景数据获取的及时性，大幅降低了云传输与存储的成本。

增强影子模式——关键场景的触发



* 图：增强影子模式原理

在传统影子模式里，触发器（Trigger）能够对规划（Planning）输出的瞬时决策合理性进行判断。随着自动驾驶走向 L3/L4 高级别，算法不仅需要满足瞬时决策合理性，更需要优化长时行为合理性。为了在数据闭环中高效生成此类长时行为，赢彻科技在传统影子模式基础上增加了闭环影子模式，形成赢彻科技独特的增强影子模式。

在上述新增的闭环影子模式中，引入了影子规控模块和卡车动力学模型，以此构成一个虚拟闭环，在局部空间生成长时行为，满足了 L3/L4 级别自动驾驶算法对识别长时行为缺陷的要求。

增强影子模式与传统影子模式对比

	特点	适用场景
增强影子模式	引入了虚拟主车（Virtual Ego）的概念，虚拟主车和真实主车相独立，利用虚拟主车行为作为“长时行为” 规划控制系统 Planning & Control 内部状态构成真实闭环	传统影子的全部能力 可测试控制算法策略，例如画龙等 可测试绝大多数依赖长时状态窗口的 L3/L4+ 级别决策规划策略（例如变道、避让、匝道相关、连续博弈等）
传统影子模式	统一的主车	感知和定位的问题场景识别 L2 级别决策规划策略（例如 AEB 等功能的问题场景识别）

赢彻科技在实现增强影子模式过程中，解决了关键技术难题：

- **虚拟主车真实性：**闭环影子模式所需的虚拟主车需要具有很高的真实性，才能满足正确触发关键数据的要求。我们应用了高精度卡车动力学模型，使其在一定范围内能够精确地反映车辆的横纵向行为。
- **减少关键场景丢失：**为了降低关键场景的丢失率，我们针对长时行为缺陷识别引入了数十个触发器（Trigger），例如避让合理性、变道合理性、匝道通过合理性、画龙等，对虚拟主车行为进行判定，全方位提升对关键场景的召回能力。

为了满足大规模量产所需的“全时段快速 A/B test 验证”，我们设计了一套增强影子模式的全时段应用方式。

增强影子模式在 A/B test 中的应用

驾驶模式	增强影子模式应用方式	业务价值
自动驾驶状态	主系统 = 已发布版本算法（A） 闭环影子系统 = 预发布版本算法（B）	实时 A/B test。生成结论的时效性从周级别降低到天级别
接管瞬间	主系统 = 人工接管（A） 闭环影子系统 = 已发布版本算法（B）	对“如果不接管，是否会产生事故”进行动态判定，更精确的进行人机对比
人工驾驶状态	主系统 = 人工驾驶（A） 闭环影子系统 = 已发布版本算法（B）	对“决策准确性”和“行为准确性”进行长时人机对比

增强影子模式——高价值场景鉴别

增强影子模式完成了关键场景触发后，定义了更精细的场景分类树，据此能够对高价值数据进行更精准的描述和识别，可大幅降低云传输和存储的成本。

传统场景分类的维度过粗，无法对高价值场景进行精确刻画，导致误判率较高。因此，赢彻科技在传统场景定义的基础上，新增了缺陷（Issue）以及根因（Root Cause）两个新的维度，能够为场景表达提供更精细的算法特质相关的刻画，避免了高价值场景数据的沉没。

这种更精准的场景分类，能够较好地平衡“分类精度”和“分类泛度”，最大程度地移除了低质量重复场景数据，控制数据成本。

* 图：数据闭环场景分类树定义

基于增强影子模式的数据闭环体系应用

自 2021 年底，随着量产智能重卡投放车辆和数据规模快速增长，赢彻科技已经建成了自动驾驶卡车领域第一个实质性的海量数据闭环。增强影子模式在数据闭环中的使用卓有成效：

- **车端基于影子模式的高质量采集触发：**影子模式支持 150 多个触发器（Trigger），能够识别并触发绝大多数有效接管类问题。在闭环影子模式下，避让、变道、匝道等关键场景，长时行为缺陷的召回率 >70%（准确率 >90%）。数据压缩率 <1%。数据在云端的可用率 >80%。
- **低延迟的数据采集：**常规缺陷场景数据上传的时效性达到小时级，紧急场景数据上传时效性可达到分钟级。量化统计分析类数据时效性达到亚秒级。
- **精细化场景分类能力：**基于超过 600 万公里的开放道路数据，抽象归纳出高价值场景语义分类，约 7 大类、200+ 子类、问题分类约 70+ 类、对应算法原因分类 100+ 类。多维度组合后的精细化场景分类空间达到万级规模。

3.5
线控底盘

线控底盘属于自动驾驶系统中的执行层，是实现自动驾驶控制意图及控制安全的执行机构。线控底盘开发主要包含线控转向、线控制动、线控油门、线控挡位等线控功能，保证车辆在自动驾驶控制行驶中稳定、安全、平顺和经济。商用车的特点是整车寿命长达 150 万公里，车辆总质量较重、工作时长较长、转向力矩和制动力输出较大、系统延迟较大。随着行驶里程的增加，制动器间隙、转向系统间隙和其他机械间隙会出现较大衰减，从而影响控制安全。线控底盘的开发，难点在于：

- 如何保证实现线控底盘系统安全
- 如何实现 L3 级别人机共驾
- 如何保证线控执行器与自动驾驶系统预期性能的一致性

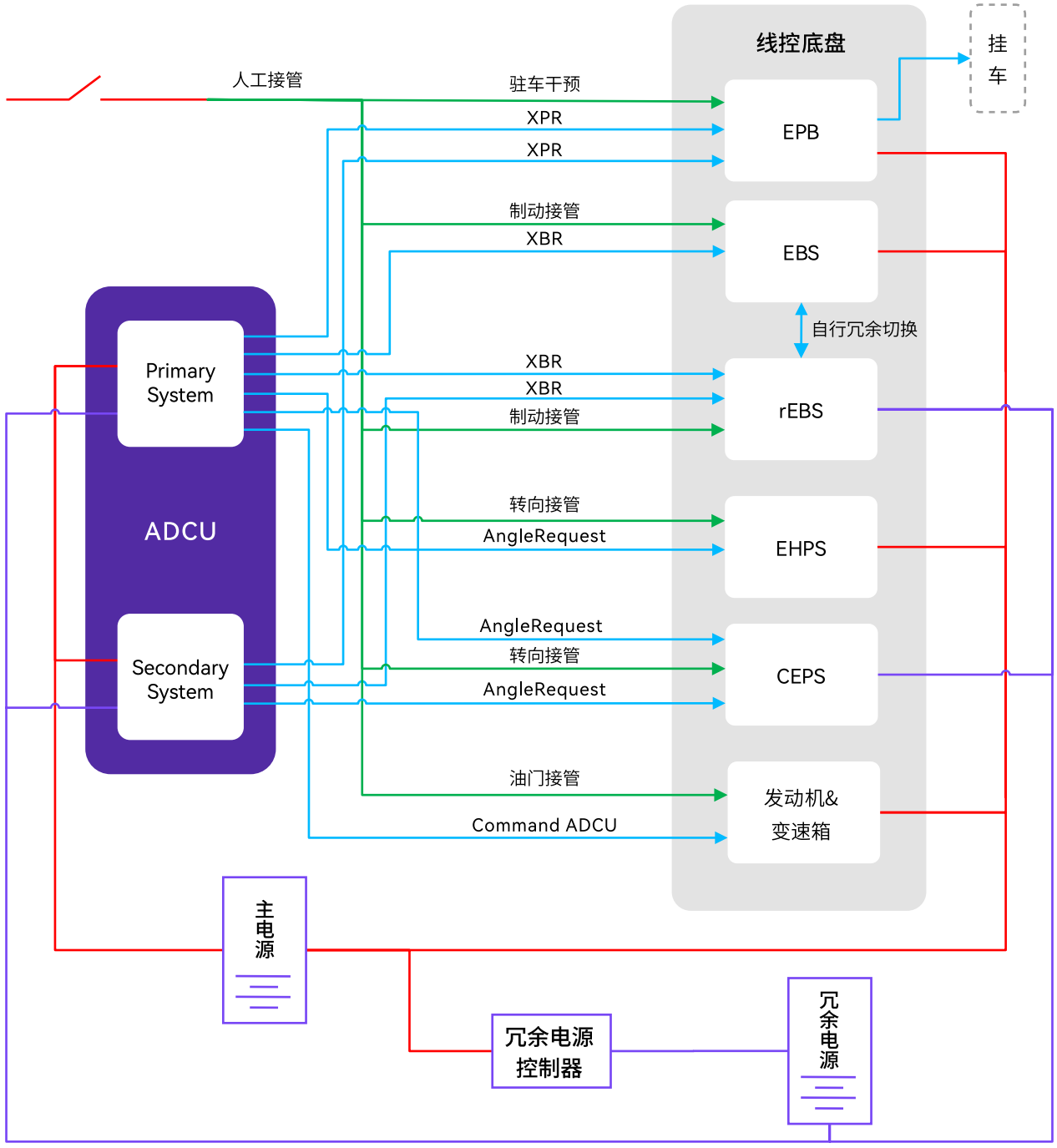
线控底盘开发

线控底盘的开发是一项系统工程，需要综合考虑线控功性能目标、产品资源、方案可实施性、时间和成本等因素来决定实施路径，过程如下：

- **线控功性能目标确定：**需要根据市场研究并结合自动驾驶的功能定义、性能定义的目标要求来确定；
- **实施方案可行性评估：**包括供应商资源、车辆布置可行性、功能安全实现路径、功性能实现的可行性、自动驾驶线控接口可行性、开发成本及时间周期的满足性；
- **设计与验证：**方案确认后，进入系统和零件设计，以及系统测试与验证；
- **联调验收：**车辆与自动驾驶系统一起完成联调联控验收，完成线控底盘各个系统的功性能验收，锁定线控底盘性能参数，释放初版软件；
- **正式发布：**车辆可靠耐久验证后，正式释放线控底盘 SOP（Start of Production）软件。

赢彻科技线控底盘重点关注以下四个方面：

- 保证车辆安全平稳运行
- 保证系统控制的精确执行
- 人机共驾和接管设计
- 线控底盘指标体系


线控底盘
挂车
人工接管
驻车干预
XPR
XPR
EPB
制动接管
XBR
EBS
自行冗余切换
Primary System
XBR
XBR
制动接管
rEBS
ADCU
转向接管
AngleRequest
EHPS
AngleRequest
转向接管
AngleRequest
Secondary System
CEPS
油门接管
Command ADCU
发动机&变速箱
主电源
冗余电源控制器
冗余电源

* 图：线控底盘控制框图

车辆平稳运行的安全保障设计：智能卡车线控底盘采用全冗余设计，通过制动、转向、电源管理系统，对因人和机器非预期行为带来的风险，采取冗余设计和设置安全保护措施，防止自动驾驶车辆因系统失效或故障导致车辆出现安全问题和非预期行为带来的安全风险。

- **线控制动采取双重冗余设计：**制动系统采用行业首创的双重冗余设计，主制动 EBS（Electronic Brake Systems）+ 冗余制动 rEBS（Redundant Electronic Brake Systems）+ 冗余制动 ETB（Electronic Trailer Brake）方案。系统由三套独立控制模块组成，每个系统有独立的电子控制单元（ECU）、供电电源、EBS 和 rEBS 具备独立的轮速传感器。每个系统能够完全独立工作，系统之间的交互通过 CAN 总线传输，EBS 和 rEBS 之间通过私 CAN 传输。当主制动 EBS 失效时，冗余制动 rEBS 在 20ms 内自主完成制动系统的接管和实现车辆控制；当主制动 EBS 和冗余制动 rEBS 均失效时，接受 ADCU 仲裁指令后，冗余制动 ETB 可以实现对挂车进行制动控制来保证车辆行驶安全。
- **线控转向采取冗余和液压失效检测设计：**转向系统冗余设计采用的是行业首创的主转向EHPS（Electronic Hydraulic Power Steering）和冗余转向 CEPS（Column Electric Power Steering）方案。系统由两个独立的电子转向系统串联组成，每个系统具备独立的 ECU 和电机、角度传感器和扭矩传感器、供电电源，能够分别完全独立工作。两套系统之间的交互信息通过 CAN 总线传输。当主转向 EHPS 失效时，冗余转向 CEPS 接受自动驾驶控制器 ADCU 的仲裁指令和控制指令接管和控制车辆。当车辆通过液位传感器发出指令或主转向 EHPS 检测到液压失效时，接受 ADCU 的仲裁指令后，冗余转向 CEPS 会控制 HPS（Hydraulic Power Steering）安全接管和控制车辆。
- **供电电源采用冗余设计：**车辆供电系统采用主电源和冗余电源的设计，并采用冗余电源控制器 SES（Smart Emergency Switch）进行管理，当车辆主电源失效时，冗余电源控制器将在 1ms 内将两侧回路切断，车辆由冗余电源进行供电来保证车辆供电系统的安全。
- **对防止非预期安全采取的安全防护：**在防止非预期转向、非预期紧急制动及安全员的潜在误操作影响等方面，通过设置安全阈值进行非预期保护。

系统控制的精确执行：线控主制动与冗余制动最大减速度完全相同。线控制动 XBR（External Brake Request，外部制动请求）的响应时间缩短 33%，超调量减少 50%。线控主转向与冗余转向的性能指标完全相同，在集成冗余转向系统后，主转向系统在响应时间、超调量、稳态时间和稳态误差等方面的性能指标都可保持独立运行时的水平。线控油门响应时间缩短 10% ，档位切换响应时间缩短 20%。

人与自动驾驶域控制器 ADCU 的共驾设计：线控制动、线控转向、线控油门和线控换挡，均实现了自动驾驶与人工驾驶模式的状态机接口设计，并通过多场景下的反复调参实现人与机器的平顺切换，适应于 L3 级别自动驾驶人机共驾场景下的各种潜在接管需求。

线控指标评价体系设计

- 线控制动性能评价指标包括：响应时间、稳态时间、稳态误差、超调量、冗余接管时间、最大制动减速度和辅助制动最大减速度。
- 线控转向性能评价指标包括：响应时间、稳态时间、稳态误差、超调量、相位延迟、截止频率、冗余接管时间、空行程和切换力矩波动。
- 线控动力总成性能指标体系包括：油门响应时间和档位切换时间。

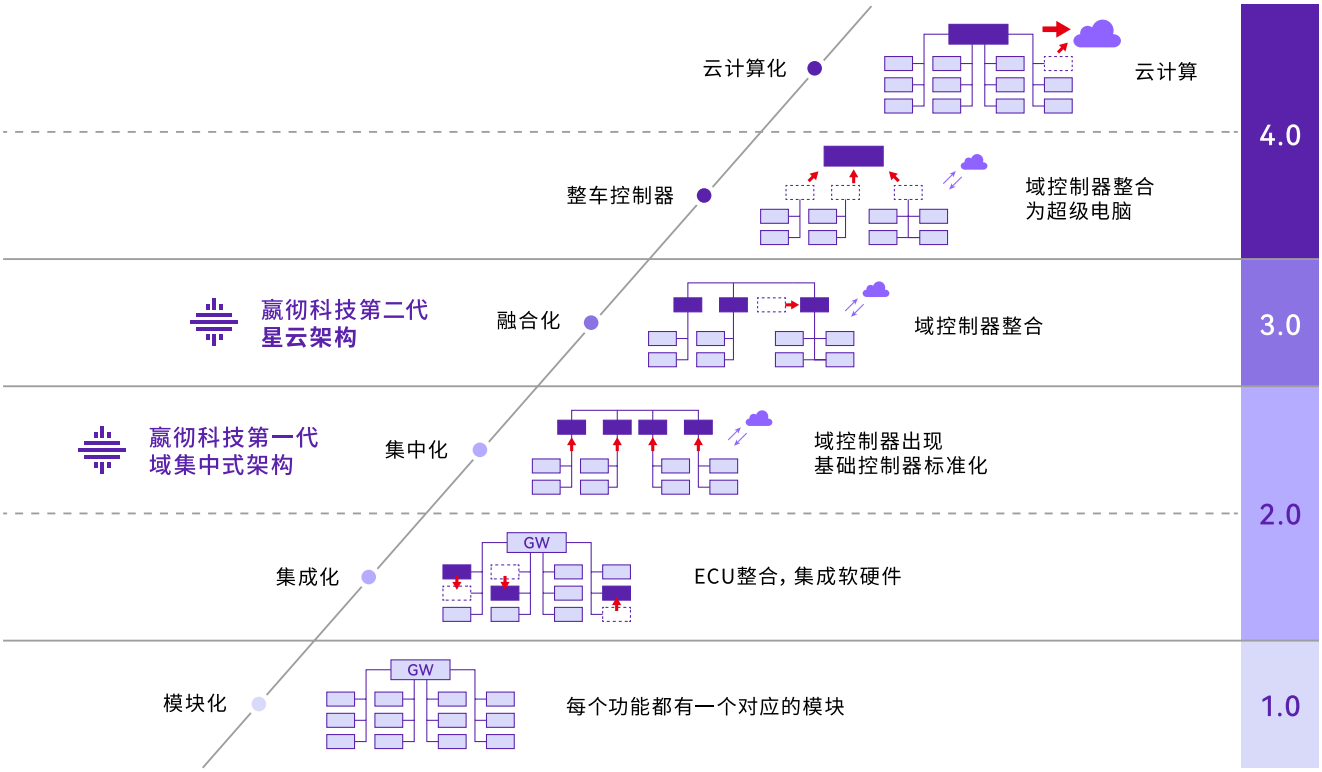
赢彻科技线控底盘开发实践

全冗余线控底盘技术架构可以支持 L4 技术平台，是行业首款具备可前装量产、满足系统功能安全等级 ASIL D 的线控底盘。线控制动及转向冗余系统分别通过了等效 300 万公里的接管可靠性试验和等效 150 万公里的冗余切换可靠性试验。同时在整车层面累积进行了 400 万公里的道路耐久验证。

全冗余线控底盘系行业首创，解决了行业 L3 级别自动驾驶车辆底盘系统痛点，具备“Fail-Operational”能力，故障下可运行功能。但在冗余系统接管时间、冗余方案技术复杂性、冗余制动 ABS 非独立性、冗余制动控制响应时间、成本等方面还需继续进行优化和改善。高度集成全功能的自冗余系统，是满足未来自动驾驶安全需求的主流技术方向。

3.6
电子电气架构

汽车电子电气架构 EEA（Electrical/Electronic Architecture）是指将汽车上所有的电子和电气部件设计为一体的整车电子电气解决方案。行业普遍共识的博世电子电气架构演进图展示了电子电气架构发展的不同阶段：分布式阶段（模块化、集成化）、域集中式阶段（集中化、融合化）和中央式阶段（车载超级电脑化、云计算化），而商用车当前绝大部分的车型架构还处于模块化向集成化的转型过程。



* 图：博世电子电气架构演进示意图

赢彻科技第一代域集中式电子电气架构

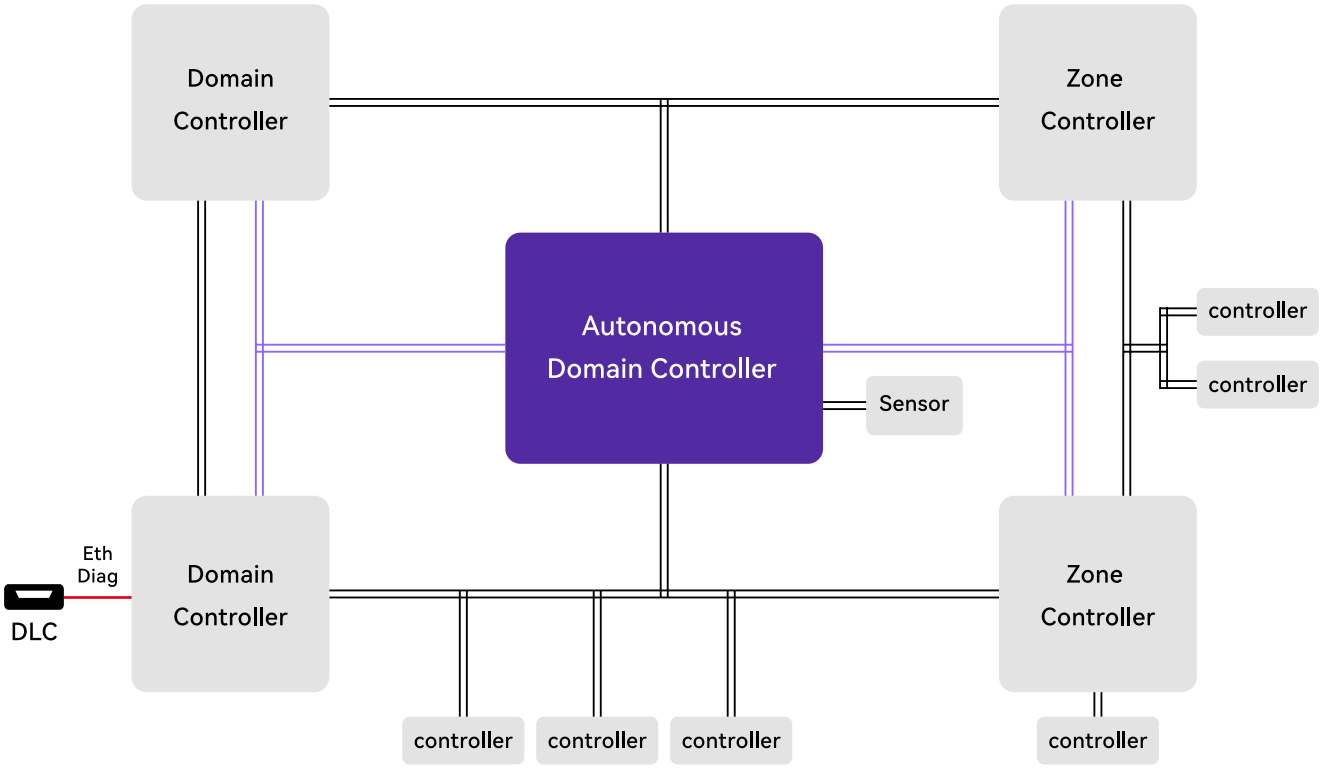
赢彻科技与主机厂合作的第一代智能重卡，是基于现有的重卡平台进行改型，第一代产品已经实现量产，其电子电气架构具备以下特点：

- **快速融合的域控制器架构：**秉持兼顾现状、快速融合的思路，在既有分布式 EEA 的基础上，构建具备自动驾驶功能的域控制器。
- **持续迭代的 OTA 能力：**自动驾驶域具备完整 OTA 能力，并且达到 100% 域内芯片及控制器可被远程升级，使得赢彻科技的自动驾驶产品能够不断的自我进化，始终保持对于市场需求的高速迭代，不再是传统机械产品汽车的量产即过时。
- **高速网络通信能力：**在局部域内，通过百兆以及千兆以太网的配置同比提升通信速率 100 倍以上，扫除了带宽瓶颈的焦虑。

赢彻科技第二代星云电子电气架构设计

继第一代产品的量产投放，赢彻科技已着手研究第二代 EEA——星云架构（中央计算 + 区域控制星形连接架构形态），力图解决商用车电子电气架构“安全、实时性、带宽瓶颈以及成本”等方面的痛点，从如下四方面进一步提升架构整体竞争力：

- **硬件架构升级：**功能域控制器（自动驾驶域控制器 & 智能网联域控制器）与位置域控制器并存（中部车身域控制器），可使传统 ECU 数量减少约 30%，线束回路减少约 20%，解决商用车线束布置局促的先天限制，并且实现硬件资源高度集中化从而实现成本最优化。
- **软件架构升级：**通过引入标准化服务的 SOA 架构理念，使软硬件解耦分层，实现软硬件设计分离，从而带来软件 / 固件 OTA 升级性、软件架构的实时操作系统的可移植性，以及采集数据信息多功能应用性。有效减小硬件需求量，真正实现软件定义汽车。
- **通信架构升级：**商用车首次以千兆以太网构建主干通信，数据传输能力可提升 1000 倍以上，有效解决传统 CAN/LIN 总线传输低效的带宽瓶颈，为数据深度融合提供了更好的基础。
- **迭代体验升级：**通过硬件架构和软件架构升级，带来软硬解耦以及接口标准化，大大缩短开发周期，使得产品升级迭代更为高效。通过域的高度整合以及通信架构的升级，使得全域 OTA 升级控制在 45 分钟以内。



* 图：赢彻科技 - 第二代星云电子电气架构

3.7
网络安全

赢彻科技在量产开发过程中，始终坚持安全至上的原则，坚持正向信息安全设计和开发，开展各类信息安全测试验证活动，持续监控和解决各类潜在网络风险，严格审核各类数据的采集、使用、存储的合规性，确保量产自动驾驶车辆能满足信息安全法规要求，守护用户生命财产及个人隐私安全。

构建行业领先的车辆信息安全开发体系

赢彻科技严格遵循 ISO/SAE-21434 开发方法论，搭建了行业领先的信息安全开发体系，构建了涵盖产品定义、研发设计和生产运营的全生命周期闭环的信息安全方案，引领商用车信息安全的最佳实践。目标是于 2022 年内获得商用车行业首个《ISO/SAE 21434 道路车辆 - 信息安全工程》管理体系认证。

量产级信息安全需求和安全方案

- 通过对 300+ 商用车应用场景深入研究，建立从正向出发的信息安全风险评估方法。
- 识别出了 179 类网络安全风险，并形成赢彻科技特有的漏洞库。
- 打造了 6 层纵深防御体系，涵盖云 - 管道（AirLink）- 车端入口（T-Box）- 车端咽喉（网关）- 车内网络 - 关键零件。
- 提出了近 500 多项安全需求，涵盖编码、密钥、诊断、操作系统、升级、启动、车联网云端信息、网络通信、敏感数据管理与防护等九类。
- 将隐私计算等前沿安全技术与产品功能融合，涵盖云、管、车端入口、车内网络，设计验证了一系列安全方案使得产品的信息安全能力达到了行业领先水平。

信息安全测试验证

- **正向验证：**安全团队构建了自动化安全测试平台，结合安全需求和信息安全漏洞，导入了一批安全测试项及一系列安全测试用例，包括调试口访问安全、远程登录安全、内网通信等，构建了标准化、快速、批量的完成网络安全测试的能力。

- **逆向验证：**赢彻科技联合全球领先的腾讯科恩实验室对整车及自动驾驶系统开展安全测试验证，通过顶尖黑客对车辆系统模拟攻击，范围涵盖了接触式、近场、远程等多个种类，验证车辆的信息安全能力。赢彻科技与主机厂联合开发的自动驾驶重卡通过了各项严格攻击测试，综合评估产品的信息安全能力达到了商用车领先水平，在行业内也达到了先进水平。

产业合作伙伴联防联控

伴随着汽车联网和软件频繁升级迭代，汽车不再是一锤子买卖，网络安全逐渐成为动态变化的问题。为及时应对层出不穷的各类全新信息安全问题，赢彻科技与地图、差分定位、网络运营商等产业合作伙伴已经打通应急响应机制，联防联控地开展持续性网络安全监控和应急响应，确保能够及时发现、响应、处置各类安全风险，7x24 小时保障车辆信息安全。

3.8
人机交互系统

量产自动驾驶卡车在人机交互方面的挑战

对处于人机共驾阶段的 L3 能力级别智能重卡，人机交互系统的设计至关重要。友好的人机交互设计可以有效地帮助安全员获取到自动驾驶相关的关键交互信息，提升对系统的信任，减少自动驾驶使用过程中的焦虑与疲劳，最终让整个行车过程更加安全和高效。

对于高级别的自动驾驶，由于涉及到驾驶权的转移，显著增加了人机交互设计和实现的难度。根据 NHTSA（National Highway Traffic Safety Administration，美国高速公路安全管理局）的调研，在其所著的 *Human Factors Design Guidance for Level 2 And Level 3 Automated Driving Concepts* 一文中指出，L2 及以上级别自动驾驶系统有一系列的设计难点。赢彻科技对其进行了归纳整理并针对各难点建立了相应的设计原则。

高级别自动驾驶系统人机交互的设计难点及其设计原则

设计难点	赢彻科技设计原则
对自动驾驶的信任	提升安全员对于自动驾驶能力的信任，并且愿意使用和依赖系统所提供的交互信息
自动驾驶的误用、弃用及滥用	有效减少安全员在不合理的场景下对自动驾驶的误用甚至滥用，并能减少频繁错误提示造成的弃用
安全员不在环的注意力保持	让安全员不在驾驶状态的情况下又能保持一定的注意力，及时获取到关键的交互信息
自动驾驶失效的及时接管	让安全员能够及时获取到自动驾驶系统的失效信息，并减少接管的时长
自动驾驶引发的疲劳	降低安全员在无驾驶任务情况下的无聊和困倦
笨拙的自动驾驶	提升自动驾驶系统帮助人解决更具挑战的驾驶任务的能力，而不仅仅是辅助人实现简单的驾驶操作
驾驶模式的模糊	让安全员及时且清晰的意识到车辆驾驶模式和驾驶主体的变化

在商用车和干线物流的应用场景下，除了行业本身在人机交互层面的乏善可陈和技术制约外，上述的设计难点突出体现在：

- 长距离、高强度的运输任务容易导致疲劳，尤其在夜间驾驶时段。
- 长时间使用自动驾驶，行驶在较单调的高速场景下，如何保持注意力。
- 货车安全员群体所需的清晰且明确的交互信息和操作提示。

多模态全冗余的人机交互系统

基于上述的设计原则和商用车干线物流的特殊场景，赢彻科技设计并实施了业界首个视觉、听觉、触觉多模态全冗余的人机交互系统。

该系统主要有三个方面的特点：

- 多种方式获取安全员关键信息，除了用常规的方向盘和踏板信息了解安全员的驾驶操作之外，该系统还使用了 DMS（Driver Management System）安全员监控系统、HOD（Hands Off Detection）手握状态检测系统，用于实时监控安全员的疲劳、分心、离座以及驾驶手势等状态。
- 多维度的交互，让安全员及时有效了解自动驾驶系统运行的状态，通过视觉、听觉、触觉的多模态交互传递各类关键信息，确保安全员快速建立对当前场景的意识与判断。
- 不同场景下分阶段的交互策略，让安全员从容处理不同紧急程度的事件。以接管请求为例，对于紧急程度高的事件，会同时触发视觉、听觉、触觉等多重提醒，期望安全员在更短时间内接管车辆；而对于紧急程度低的事件，会优先以更柔和的方式提醒安全员，让安全员更平稳地接管车辆。

* 图：赢彻科技 - 多模态全冗余人机交互系统

人机交互评价指标

在一系列人机交互设计的基础上，结合实际运营的经验，基于安全性的考虑，赢彻科技总结出了三个核心的人机交互评价指标：

- **安全员激活自动驾驶系统的平均时长：**从人机交互的角度，自动驾驶系统的运行可分为未就绪、已就绪、激活中、Fallback 等状态。在各类内外部条件都满足后，自动驾驶系统会提示系统已就绪。此时，安全员激活系统的平均时长越短，说明安全员越愿意使用该系统，也越信任该系统的综合表现。
- **百公里疲劳次数：**将安全员的疲劳等级根据人脸的状态、眼球的活动、面部的姿态等进行划分。友好的人机交互应能有效降低各级疲劳发生的次数。
- **接管绩效：**自动驾驶系统的人机交互，需要权衡接管的及时性和接管质量，让安全员在及时接管的同时又能兼顾每次接管的质量，从而确保该次接管是足够平稳和安全的。

4 流程与工具

4.1 流程与工具概述

* 图：赢彻科技 - 自动驾驶整车与软件开发流程

流程与工具是保障自动驾驶重卡产品研发制造质量与效率的重要基础，贯穿设计、开发、验证和生产制造的全过程。赢彻科技通过实践，以**“正向开发、兼顾敏捷”**为原则，构建了基于 V 模型理念的研发流程体系，包含整车正向开发流程、生产准备流程、测试验证流程和自动驾驶软件敏捷开发流程等四项关键流程：

- **整车正向开发流程**由赢彻科技与主机厂伙伴联合制定，面向整车和核心零部件的联合研发，保障自动驾驶整车与零部件研发的严谨性和合作效率，其中包括生产准备流程和测试验证流程。
- **生产准备流程**面向整车产品的生产制造，贯穿整车开发全过程，包括制造方案策划、实施、验证及验收确认等，确保产品成本、生产交付以及质量目标的达成。
- **测试验证流程**通过构建完整的测试验证体系，从软件、硬件、系统、车辆各层面进行充分验证，保证自动驾驶卡车达到各级设计目标、安全可靠。赢彻科技的测试验证流程包括 SIL（Software In Loop，软件在环）、HIL（Hardware In Loop，硬件在环）、DIL（Driver In Loop，驾驶员在环）、LST（Large Scale Test On Proving Ground，封闭场地测试）、ORT（Open Road Test，开放道路测试）共 5 个环节。
- **自动驾驶软件敏捷开发流程**是赢彻科技为支持自动驾驶系统以数据驱动的方式快速迭代而专门建立的。在遵循量产车型正向开发严谨性的前提下，应对自动驾驶系统中深度学习算法和需求定义的不确定性对开发过程所带来的挑战。

赢彻科技的研发流程体系源于自动驾驶卡车量产开发过程中的持续实践与探索，试图解决整车正向开发的严谨性、软件开发的敏捷性、自动驾驶算法与需求的不确定性之间的冲突与融合对行业带来的全新挑战，在持续优化中。

4.2
自动驾驶软件敏捷开发流程

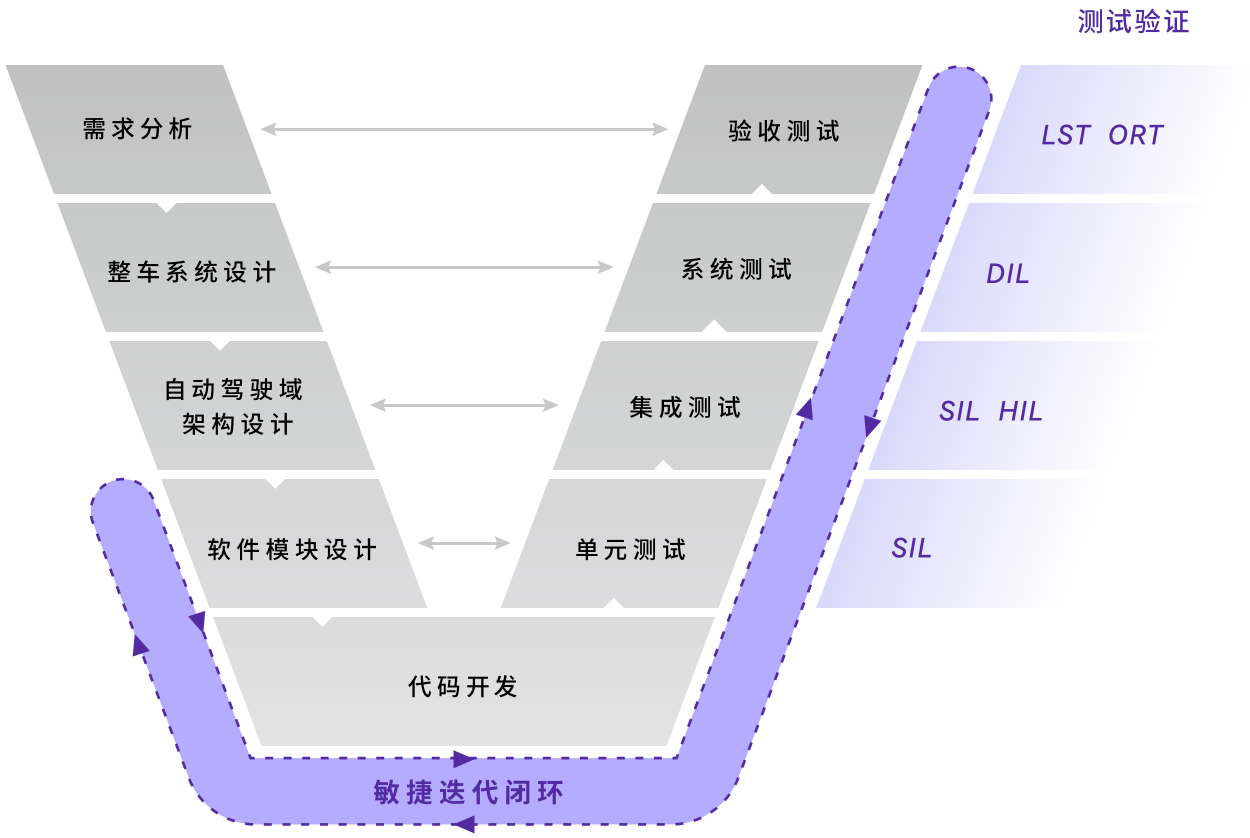
自动驾驶卡车的量产涉及到极为复杂的软硬件一体化系统的开发，既要遵循正向开发的严谨性，也要应对自动驾驶系统中被大量应用的深度学习算法和需求定义的不确定性。赢彻科技在量产实践中对 V 模型开发、敏捷开发和测试验证体系进行了创新性融合，建立了自动驾驶软件敏捷开发流程。

V 模型开发模式是汽车研发体系的经典开发模式。V 模型的左半边对应需求分解传递过程，确保每一条需求都正确传递到开发端；其右半边对应测试验证过程，确保每一条需求都得到正确的实现。V 模型的优势在于：

- 需求正向传递、层层分解，各层级解耦，有利于复杂系统集成。
- 各层级需求可追溯，避免需求遗漏。
- 分阶段测试，提前验证，有利于及早发现问题。
- 测试及需求可追溯，有利于快速定位问题原因。

敏捷开发模式在软件产业中被广泛应用，根据需求的价值优先级，分多次持续快速地将软件交付给客户，收集使用反馈并进行不断优化。特点是快速迭代、小步快跑，非常适用于需求变化快、响应速度要求高的情形。

测试验证体系确保自动驾驶卡车可以安全可靠地大规模投入应用，经受全场景、高强度的运输任务考验。赢彻科技的测试验证体系包括 SIL（软件在环）、HIL（硬件在环）、DIL（驾驶员在环）、LST（封闭场地测试）、ORT（开放道路测试）共 5 个环节。



* 图：赢彻科技 - 自动驾驶软件敏捷开发流程

自动驾驶软件敏捷开发流程的设计

- **需求定义与设计：**V 模型左侧对应设计过程，自顶向下共计四层，依次为需求分析、整车系统设计、自动驾驶域架构设计、自动驾驶软件模块设计。
- **测试与验证：**V 模型右侧对应测试验证过程，与左侧设计层次一一对应，自底向上依次为单元测试、集成测试、系统测试、验收测试。每个层次的测试都从赢彻科技测试验证体系中分配了相应的完整测试步骤。
- **敏捷迭代闭环：**在 V 模型左侧的软件模块设计和 V 模型右侧的四层测试验证过程之间，通过敏捷开发模式贯穿起来，获得足够的敏捷性和效率。

测试验证流程与方法

	SIL	HIL	DIL	LST	ORT
验收测试				✓	✓
系统测试			✓		
集成测试	✓	✓			
单元测试	✓				

自动驾驶软件敏捷开发流程的使用

自动驾驶软件敏捷开发流程可以有效解决实际开发过程中的需求与挑战：

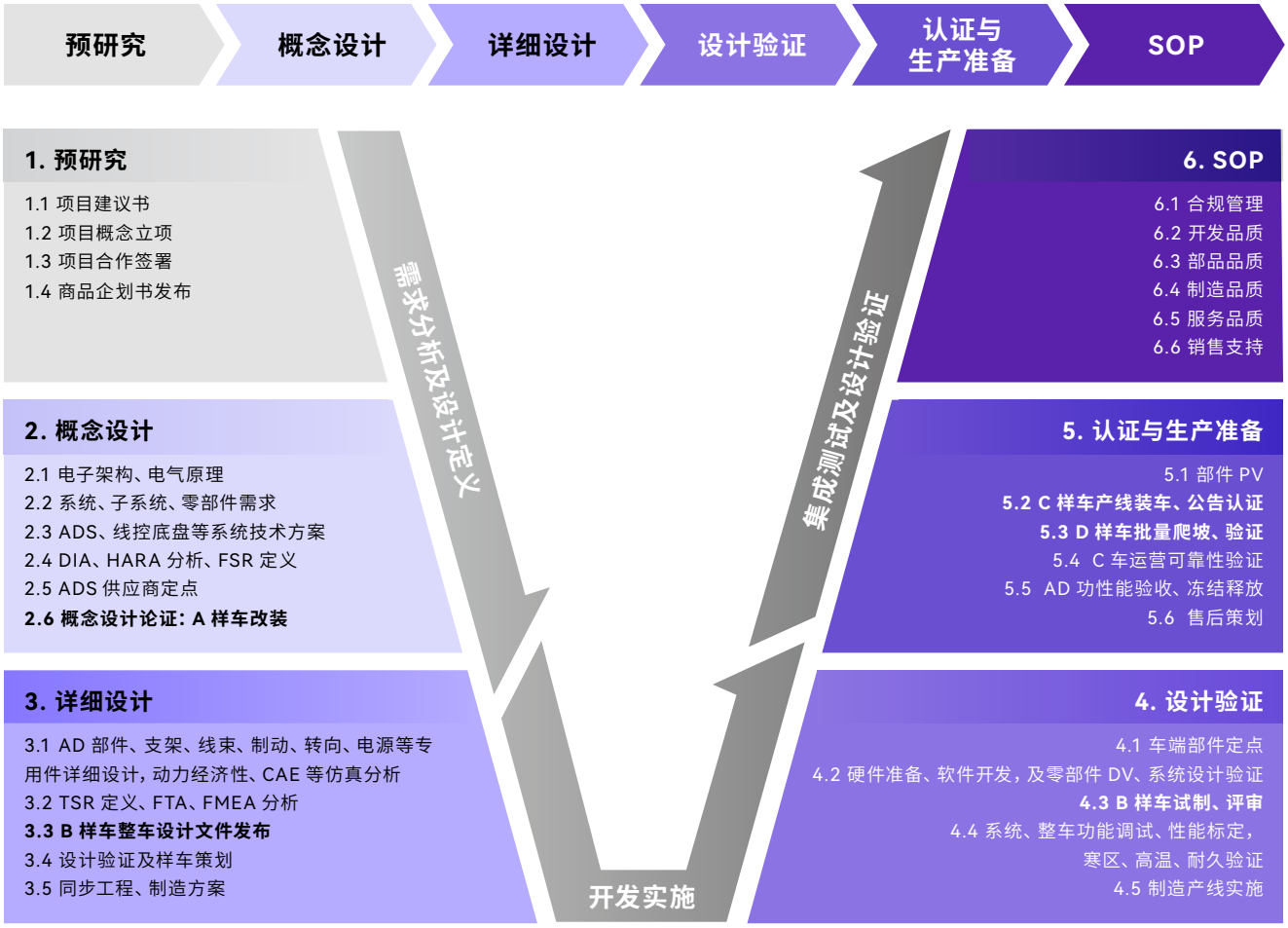
- **开发缺陷修复（Bug Fix）：**自动驾驶因其系统和运行环境的高度复杂性，以及早期系统设计需求的不完美和不确定性，导致在 V 模型右侧测试阶段很难如传统 V 模型一样对左侧对应层级的设计进行彻底充分的验证。为了解决该问题，赢彻科技部分融合敏捷开发的思路，相较于传统 V 模型，在模型右侧进行更广泛层级的迭代测试，直到充分发现并修复开发缺陷。例如，在自动驾驶避让功能的测试验证过程中，不仅在低层模块级和跨模块级测试中采用 SIL 和 HIL 进行大量仿真性的压力测试，还在高层系统级和验收级测试中采用封闭测试场和开放测试路段进行路测，过程中发现的开发缺陷都会快速纳入下一次迭代中。这个迭代过程不断快速循环，直到开发缺陷充分收敛，满足软件释放质量要求。
- **对确定性需求的性能持续优化：**赢彻科技在实践中体会到，自动驾驶系统在应用中发现的大量问题不是由于系统功能开发缺陷导致的，而是源于系统应对复杂场景的性能不足。只有在真实道路上长时间地运行才能发现系统能力短板，尤其是出现频次很低、较难复现的长尾问题。对于此类问题，可结合敏捷开发的思路，在符合安全设计要求的条件下，尽可能快速地投入实际运行环境，收集反馈、迭代优化性能。比如，“车辆画龙”是重卡自动驾驶系统运行中遇到的一个典型问题，其受到诸多长尾因素的影响，包括运行状态（超车 / 直行）、定位误差、地图错误和底盘转向器性能缺陷等。在大规模运行情况下，每个因素都是概率性的、影响权重不同且可能与运行环境高度相关，导致不可能一次解决所有问题根源。应当快速迭代，收集实际运行数据并统计分析影响权重，制定有针对性的优化策略。整个过程不断迭代，直至最终彻底解决。

- **对不明确需求定义的持续迭代：**自动驾驶重卡作为一个极为复杂的新技术产品，既要满足安全、时效、成本三方面的要求，也要在很长时间内满足人机共驾的特殊需求。这导致大量需求定义必须从多种不同维度考虑和权衡，从而使需求定义很难做到一步到位，只能逐步迭代。例如，在自动驾驶重卡产品开发的早期，对控制精准性的极度追求导致频繁转向制动，显著影响油耗水平和零部件的耐久性，导致产品不具备商业落地的可行性。此类问题需要通过敏捷开发快速迭代，基于大量道路运行数据逐步优化 V 模型左侧的需求定义。

4.3
整车正向开发流程

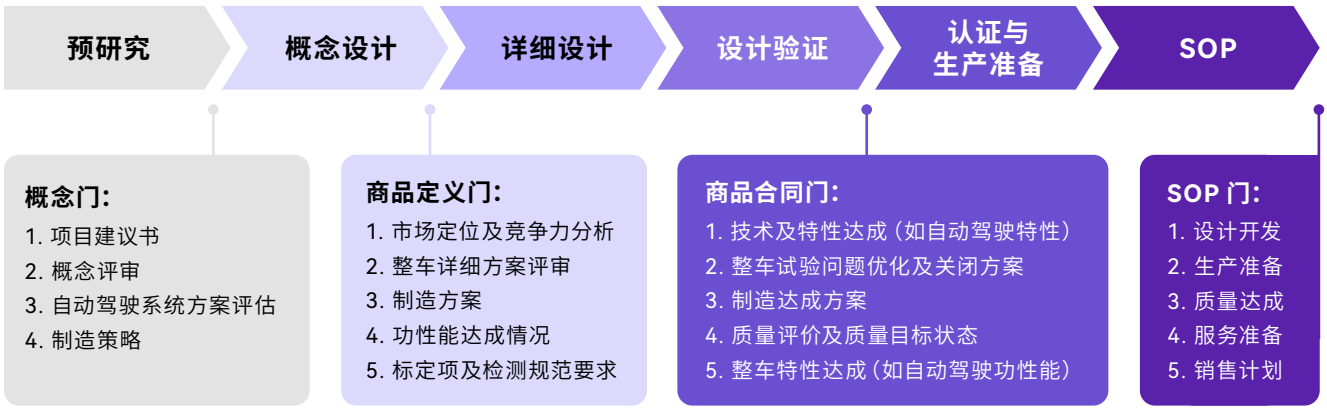
整车开发需要遵循严格的正向开发过程和产业链上下游的紧密配合，涉及到赢彻科技、主机厂和供应商合作伙伴。

为充分保证自动驾驶重卡量产项目的开发及质量目标，赢彻科技与 OEM 伙伴在项目初期共同商定了整车项目的开发流程，以“V”模型开发流程为基础，并兼顾软件开发的敏捷迭代，将汽车开发与软件开发的流程创新性融合，有效支持了这一全新项目的开发效率和交付质量。



* 图：整车开发流程图示

整车开发的质量管控采用了“质量阀门评审”的管理方式，由赢彻科技和 OEM 质量团队根据项目的具体情况设置阀门交付内容及评审节点，并随项目主计划按节点邀请双方项目指导委员会进行阀门评审，以保证赢彻科技自动驾驶系统满足车规前装量产的要求，同时保证整车开发阶段性目标的达成。过程中基于阀门评审要素和通过标准，组织各专业组按照项目计划节点管理要求，完成阀门交付物的编制、评审、归档等工作。



* 图：质量阀图示（各质量门仅列举部分评审项）

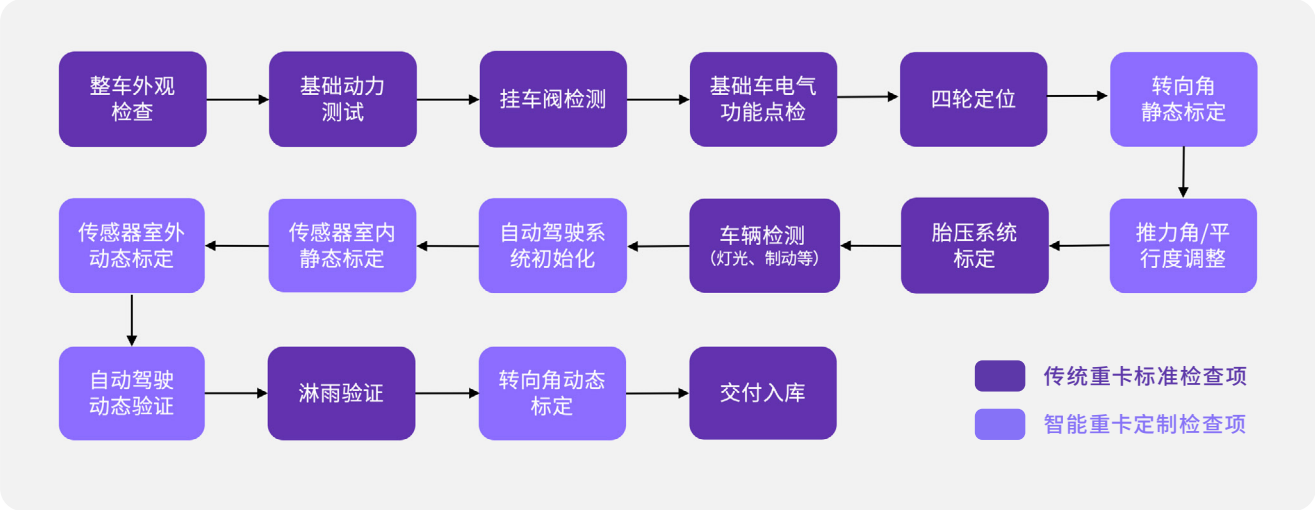
4.4 生产准备流程

生产准备作为整车量产开发项目的一项重要内容贯穿整个项目的各阶段。在项目初期便需要开始进行方案策划，并随项目的进展一同开展制造方案实施，验证及验收确认等工作。生产准备工作的质量最终影响项目的成本、周期以及商品质量目标的达成。自动驾驶技术量产同其他新技术的应用一样，不仅对于开发端，对于制造端同样面临着全新而又复杂的挑战。

* 图：生产准备工作概述

自动驾驶重卡整车量产项目并不需要新建整车产线，但需对 OEM 已有产线进行升级与改造，主要包括两方面工作：

- 新增智能部件（包括传感器、ADCU、线控系统等）的装配工艺，对现有产线的整车制造工艺顺序、生产工艺文件及工装设备进行新增或调整。
- 整车装配下线后，需针对自动驾驶系统，实施特定的检测、调试和标定工艺，从而实现自动驾驶系统产品的高精度装配、系统性调试及质量检测。



* 图：自动驾驶整车下线调试检测过程示意

工艺环节关键质量特性的管控是自动驾驶量产的重要前提，直接影响到量产车辆制造质量，并进一步影响自动驾驶系统的安全、舒适性和稳定性：

- **硬件安装精度控制：**自动驾驶感知部件的高精度探测要求有赖于整车尺寸链的严格控制，这要求核心车身部件均需 100% 电子检测以保障部件尺寸、安装角度及平整度，确保车辆在长期运行过程中依然可以保障传感器相对于整车的位置精度；
- **线控底盘标定及检测：**要求高精度的转向及制动系统的标定和调校，保障车辆在自动驾驶状态下的动力学性能；
- **传感器及定位系统的动静态标定：**确保各传感器及定位系统输出信号的准确性；
- **自动驾驶功性能的动静态检测：**保障车辆在出厂状态下具备完整的自动驾驶功性能，并得到测试确认。

以赢彻科技与主机厂联合开发的智能重卡量产项目为例，双方联合构建的自动驾驶生产工艺方案及工艺要求为自动驾驶系统的前装量产奠定了坚实的制造技术基础。

赢彻科技与主机厂联合开发智能驾驶项目产线准备方案示例

类 型	方案样例
零部件生产及品控	进行设计及生产图纸尺寸的公差收严
	增设零部件检测工位及电子检测工具
总装工艺与调试	新增生产线安装工位，调整生产工序
	联合汇编自动驾驶制造工艺及质检文件
	定向开发产线端自动驾驶故障诊断功能
	联合汇编自动驾驶测试案例及调检项目
	实施整车全扭矩控制、整车悬架调平等工艺要求
	增设整车调试检测流程
总装产线建设	建设自动驾驶感知部件标定场地
	建设冗余转向及冗余制动标定工位
	建设智能驾驶测试跑道

赢彻科技与主机厂伙伴在实现首个自动驾驶卡车量产开发的过程中，经历了不同阶段的量产准备工作，随着自身技术和产品的不断完善及与量产合作伙伴的深入合作，逐步完成了全栈自研车规级产品的稳定交付，实现了与整车制造的融合及工艺定制化升级，建立了稳定的规模化量产交付能力，为智能重卡市场及物流行业提供持续的产品供应。

4.5
测试验证

自动驾驶车辆安全可靠地投入实际运营前，既要确保其功能和性能满足设计要求，又要确保车辆可以满足全国各地高强度的运输任务考验。这些量产要求给自动驾驶的测试验证带来了诸多挑战：

- 海量测试场景的覆盖
- 深度学习算法的验证
- 功能安全和环境耐久带来的严苛测试要求

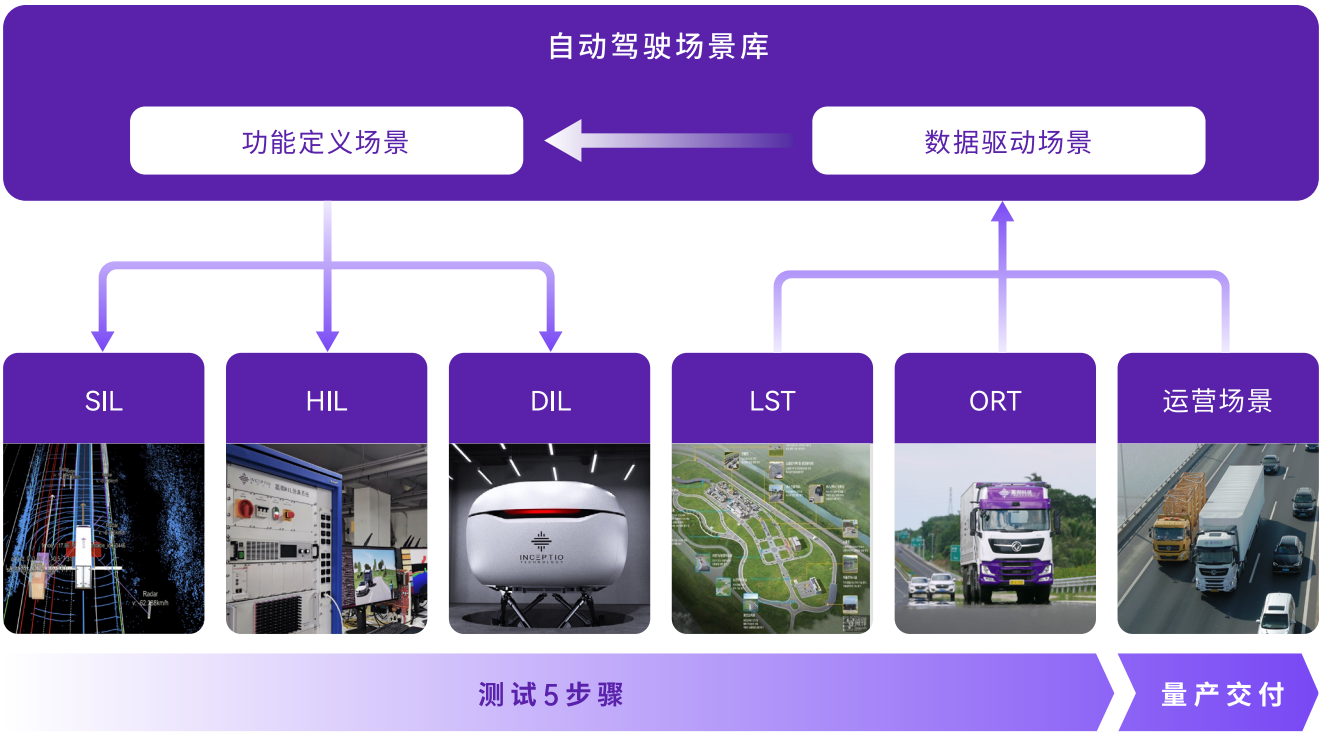
为了应对这些挑战，保证自动驾驶车辆的安全可靠，必须构建一套完整的测试验证体系，从软硬件、系统、车辆各层面进行充分的验证。

赢彻科技的智能重卡量产测试验证体系基于 V 模型与敏捷开发流程进行了创新性拓展，对需求与交付物做到“可追溯”、“可解释”、“可评估”。

赢彻科技的测试验证体系包括基于云平台的自动驾驶场景库和 5 个具体的测试实施步骤：

- **仿真测试：**包括 SIL（Software In Loop，软件在环）、HIL（Hardware In Loop，硬件在环）和 DIL（Driver In Loop，驾驶员在环）。
- **实车测试：**包括 LST（Large Scale Test On Proving Ground，封闭场地测试）和 ORT（Open Road Test，开放道路测试）。

在赢彻科技的测试验证体系中，软硬件必须全部通过5个测试步骤才能允许投放到量产运营的车辆中。

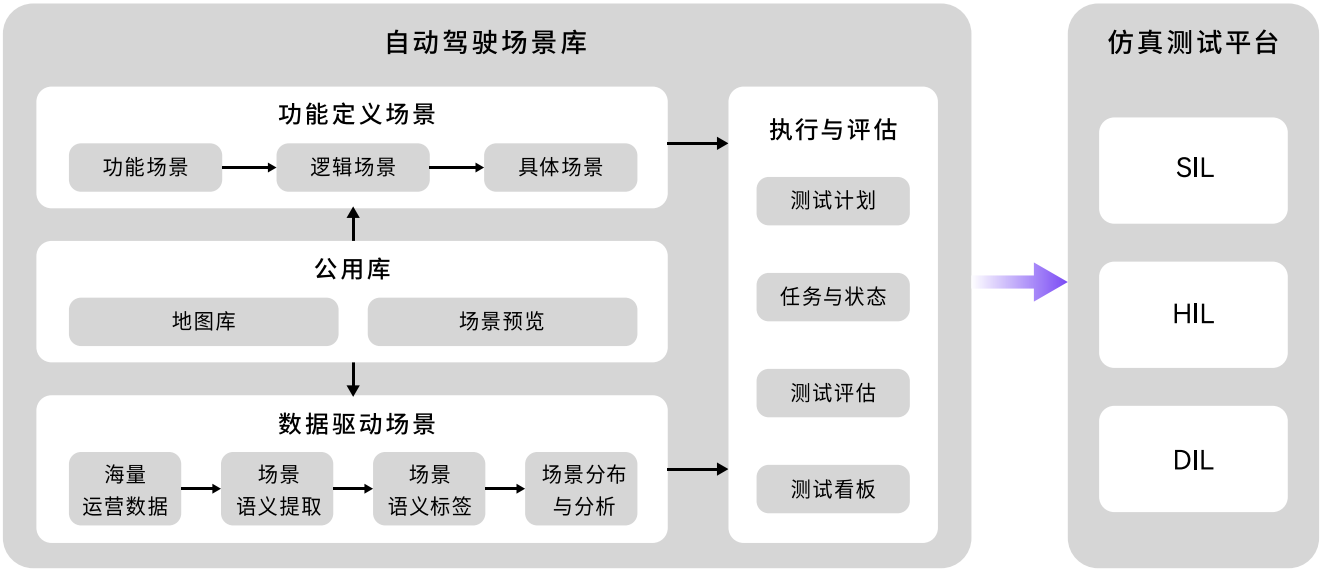


* 图：赢彻科技 - 测试验证体系

自动驾驶场景库

场景库是自动驾驶测试体系的纽带，也是核心资产。充分挖掘场景数据，并高效利用这些数据是开发与测试的关键。赢彻科技的自动驾驶场景库由功能定义场景、数据驱动场景、公用库、执行与评估 4 个模块组成（如下图所示）。其中：

- 功能定义场景与数据驱动场景是赢彻科技基于场景的不同来源进行的分类，这有利于场景的多维分析。
- 公用库基于统一的场景标准格式，提供场景地图和虚拟车辆等核心元素，并设置了预览功能。公用库显著地提升了场景设计的效率，也有利于场景的泛化。
- 执行与评估模块与特定的仿真平台建立连接，高效带动了整个场景的运转，通过高效的协同机制，促进开发与测试的迭代优化。



* 图：赢彻科技 - 自动驾驶场景库

赢彻科技场景库中的功能定义场景是基于产品定位和系统需求设计的虚拟场景，也称为基于知识分析的场景。功能定义场景模块具备从“功能场景”到“逻辑场景”再到“具体场景”的设计能力。顶层的“功能场景”是基于抽象化语义定义的场景，包括“基础功能场景”、“法规标准场景”、“功能安全场景”、“预期功能安全场景”、“事故场景”、“极端情况场景（Corner Case）”共 6 大类，数量在 1000 个左右。中间层的“逻辑场景”基于标准协议设置了完整的参数空间，定义了明确的动作类型，数量在 1 万个左右。底层的“具体场景”是可以加载到具体仿真平台的可执行文件，由“逻辑场景”泛化而来，数量在 10 万个以上。“具体场景”可基于不同的测试计划生成“场景集”，服务于不同的测试任务。

赢彻科技场景库中的数据驱动场景是指量产投入商业运营的车辆采集的海量真实场景。通过对采集得到的海量数据进行自动化语义分析，为原始数据加入结构化语义标签。赢彻科技基于 600 万公里运营数据，积累了超过 200 万个真实片段场景，对其中高价值场景，赋予了 7 大类一级标签、200 多个二级标签，生成了面向自动驾驶各环节的 70 个场景子集。基于一致的语义标签，“数据驱动场景”能够反向补充“功能定义场景”，该能力提升了赢彻科技自动驾驶场景库的广度和精度，使测试获得极高的覆盖率。

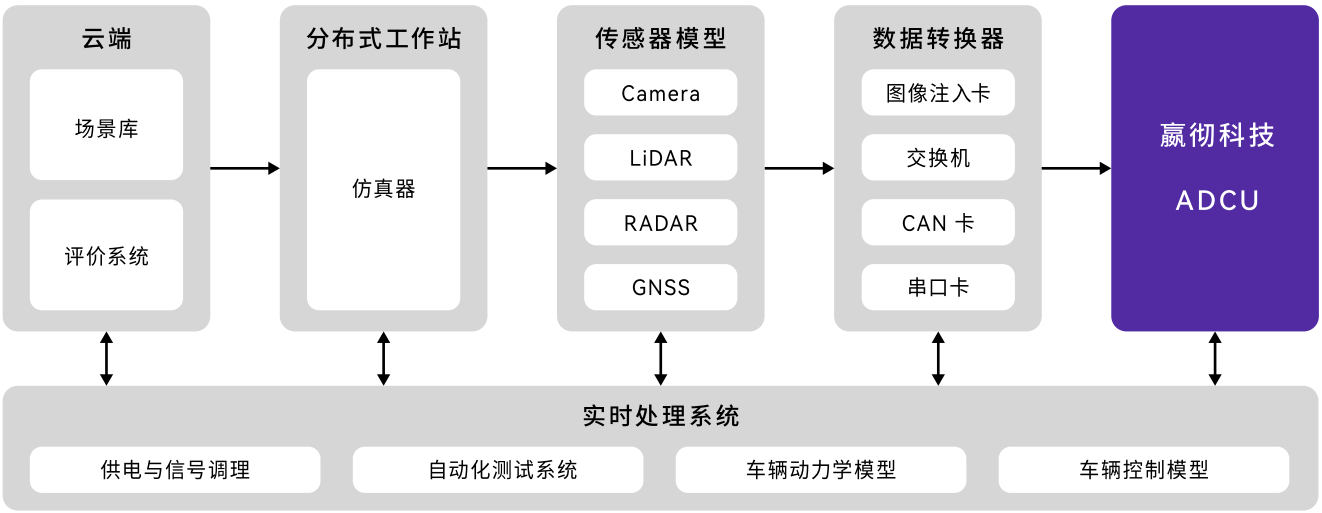
基于仿真的测试

赢彻科技采用 SIL、HIL、DIL 三级仿真方案，分别面向软件、硬件、系统功能进行验证。从“高置信度”、“高覆盖率”、“高自动化”三个维度提升仿真的能力。

- **SIL（Software In Loop，软件在环）：**赢彻科技 SIL 平台充分利用场景库中海量数据，可获得较高的测试覆盖率。自主开发的高保真仿真引擎，具备与实车高度相似的一致性，可顺利完成从问题复现，到诊断、验证、回归测试的完整迭代闭环。分布式的云端部署方式，拥有高达数万主车并行仿真能力。SIL 仿真平台中集成了 200 多个度量指标（Metrics），能够对单个任务内的数千个场景，从 200 多个维度进行全面的效果评估。

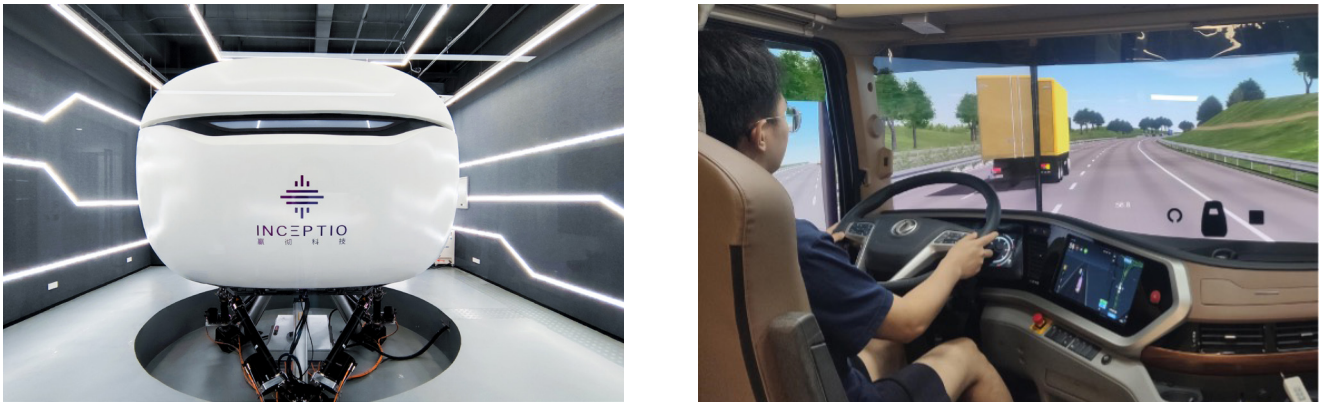
* 图：SIL 仿真测试过程

- **HIL（Hardware In Loop，硬件在环）：**自动驾驶系统的 HIL 系统由仿真器、传感器模型、车辆动力学模型、数据转换器、实时处理系统组成。HIL 系统可以快速地实现自动化测试，并能灵活注入故障，完成功能安全测试和压力测试任务。赢彻科技的 HIL 系统在多个方面进行了创新设计，力求获得高置信度的传感器仿真数据、高精度的车辆动力学模型和高覆盖率的测试场景。在传感器仿真上，基于合作伙伴的特定型号开发了摄像头、激光雷达、毫米波雷达和 GNSS 的物理模型并加入了噪声。基于合作伙伴的重型卡车开发了多自由度车辆动力学模型，模型物理属性与实车保持高度一致。在场景设计上，采用高精度地图作为底图设计动态交通流。赢彻科技的 HIL 系统与 SIL、DIL 共用了云端场景库，海量的测试场景提升了测试的覆盖率。



* 图：赢彻科技 HIL 系统框架

- **DIL（Driver In Loop，驾驶员在环）：**人机共驾是自动驾驶行业必须认真对待的课题。赢彻科技自主开发了一套功能完整的 DIL 系统来研究并解决这一难题。为了获得较高的驾驶沉浸感，赢彻科技 DIL 系统采用了与实车高度一致的内舱设计，同时在人机交互系统上提供视觉、听觉、触觉多维接口。为了便于模拟真实的场景，DIL 系统的静态路网完全基于实采高精度图创建，并叠加可动态设置的交通流模型。赢彻科技的 DIL 系统是行业内首个嵌入了真实自动驾驶域控制器（ADCU）和 HMI（Human Machine Interface）控制器的驾驶员在环系统，使这套系统既满足研究需求，同时又具备了高置信度的自动驾驶功能测试能力。



* 图：赢彻科技 DIL 系统的外舱（左）与内舱（右）

基于实车的测试

赢彻科技与合作伙伴联合开发量产的智能重卡，严格遵循汽车及零部件的相关试验标准。所有的自动驾驶相关零部件都需要经历严苛的振动、高低温冲击、盐雾、电磁干扰等诸多环境耐受度试验。同时整车层面也需要经历高温耐久、低温耐久、加速耐久等多项实车测试，确保车辆满足 120~150 万公里的耐久要求。除了以上量产标准化测试以外，量产智能重卡的测试验证体系结合干线物流 ODD 及自动驾驶功性能要求，完整建立了封闭道路的 LST（封闭场地测试）和开放道路的 ORT（开放道路测试）来进行验证。

- **LST（Large Scale Test On Proving Ground，封闭场地测试）：**封闭道路的 LST 测试主要基于干线物流高速 ODD 以及商业运营重点关注指标来设计测试场景。从 3500 个测试场景中进行针对性提取，并结合隧道、匝道、上下坡和多车道等道路环境，设计不同目标和驾驶行为。测试评判标准从安全性、经济性和功能完整性进行充分评估，对涉及安全类的问题零容忍，保证所有后续释放到公开道路的软件符合设计预期，且在公开道路上遇到的小概率场景上做到 100% 安全。
- **ORT（Open Road Test，开放道路测试）：**开放道路的 ORT 测试在 LST 之后执行。每一版本软件释放公开道路后，单车首先要在固定路线进行小范围压测，对测试结果从自动驾驶系统功性能表现及 20 多项指标上进行多方位评价。所有指标和性能相比上一周期版本指标需在有明显优化，且无安全类风险事故发生的前提下，释放到更大范围商业运营路线上做 ORT 测试。此时完全按照干线物流客户的载重、单日里程、行进轨迹等要求全面复制运输过程，从时效、油耗、系统稳定性上再次进行评估。上述所有指标及表现在满足要求后，释放到量产车辆，保证正式交付版本的安全、高效、可信赖。

CHAPTER 3

第三章

赢彻科技安全方法论与实践

1 安全理念：安全高于一切

赢彻科技自创立伊始，即将安全文化植入企业的DNA。赢彻科技认为，对自动驾驶系统最重要的要求就是具备足够的可靠性和安全性（包含 Safety 和 Security）。“安全高于一切”的理念贯穿于赢彻科技产品从研发到量产的整个周期。公司要求每个赢彻科技人都坚持风险控制和安全保障，充分实施经长期检验的安全方法论。同时，赢彻科技对于当前自动驾驶系统在安全方面所面临的诸多挑战有清晰认识。力求在量产过程中持续改良现有方法，务实探寻新的解决方案。

2 安全开发准则

为保证自动驾驶系统和智能重卡的安全性，赢彻科技建立了明确的设计开发步骤：

- 首先，对配备自动驾驶系统的智能重卡提出了明确的功能安全设计目标和 Fail-Operational（系统发生故障时仍能使用）要求。
- 然后，将这两项最高目标具体化为流程安全、核心系统安全和整车安全三个维度的子目标。
- 最后，将安全目标分解成各个子系统和零部件的安全需求，并基于重卡和自动驾驶的技术现状，分阶段付诸实践。

2.1
流程安全

- **功能安全流程：**赢彻科技坚持正向研发，严格按照 ISO 26262 ASIL D 的流程要求实施智能重卡的功能安全开发，并要求该流程体系通过认证。
- **预期功能安全流程：**按照 ISO 21448 的流程实施预期功能安全开发，并最大程度上实现其与功能安全流程的融合。
- **网络安全流程：**在网络安全开发工作中，遵循 ISO/SAE 21434 的流程要求，并以通过流程认证为目标。
- **支持性流程 (Supporting Process)：**功能安全和网络安全流程的实施，离不开组织架构配合和项目执行中的支持性流程，包括问题管理、上升 (Escalation) 、持续改进和决策机制等配套流程体系。

2.2
整车安全

一辆具备自动驾驶功能的重卡必须具备高度的可信任性 (Trustworthiness) 。车规级是汽车行业最基本的要求。从安全的角度，自动驾驶智能重卡需要满足明确的功能安全设计目标和 Fail-Operational 要求。

- 车规级要求是指智能重卡要在机械、电气、电磁兼容性、环境耐久等方面要符合其使用环境所要求的最低技术指标。车规级要求包括环境要求，振动和冲击等机械方面的要求，以及可靠性和一致性要求等。
- 满足功能安全设计目标是指整车必须达到一定安全级别的安全目标。如整车须避免非预期的加速这一安全目标是 ASIL D 级别的。其中 ASIL D 表示汽车安全完整性等级达到汽车功能安全领域的最高标准，意味着整车系统的随机硬件失效概率指标低于 10^{-8} 每小时，单点故障指标等于或高于 99%，潜伏故障指标等于或高于 90%。
- Fail-Operational 是指发生故障后，整车安全相关的功能还能继续运行，主要用来保障系统失效后的安全性。

通过满足以上几方面的设计需求，赢彻科技与主机厂伙伴联合开发的智能重卡，不仅具备丰富的舒适性功能，更重要的是具备高度的可靠性和安全性。

2.3
核心系统安全

基于整车层面的安全目标，在自动驾驶功能实现链路上的各个核心系统，将各自承接特定等级的安全需求和 Fail-Operational 要求。

- **自动驾驶系统：**为满足从整车层面所继承的功能安全等级和 Fail-Operational 要求，传感器、域控制器、算法、软件等组成部分都需承担从整车层分配下来的功能安全等级要求。

  传感器的安全需求可分为功能安全部分和预期功能安全部分。从功能安全角度来说，每个传感器都需要按照各自的功能，满足从顶层分配的功能安全等级要求，同时在单个传感器失效时，保持总体功能可用。从预期功能安全角度来说，传感器的选用和布置应该根据其特性，做到相互补充和加强，以提升整个系统的性能。

  自动驾驶域控制器 ADCU 需要从硬件角度满足所承担的安全等级要求的指标，如随机硬件失效概率度量指标等。ADCU 所提供的基础功能，如存储、网络通信、供电、时间同步等，都需达到上层设计所需的功能安全等级。Fail-Operational 的需求同样适用于 ADCU，并且十分重要。

  系统软件需要按照所需的单点故障指标和潜伏故障指标等要求，对发生的故障进行诊断，并在检测到系统故障时确保车辆安全，并支持安全员的及时接管。同时，系统软件还要能够检测外部攻击，确保系统的稳定运行。

  自动驾驶算法同样需要符合所分配的安全需求。从功能安全角度，包括算法的架构设计、开发过程、所用开发工具、软件发布等各个环节都应符合对应功能安全等级的具体要求，确保算法的输出安全可靠。从预期功能安全的角度，算法的能力需涵盖 ODD 范围内各种典型场景，并尽量提高极端情况 (Corner Case) 的覆盖度，制定应对措施，提高产品安全性。

- **线控底盘：**智能重卡采用的线控底盘中的转向、制动等执行器单元都需要有主、辅至少两套控制系统，其中转向、制动和动力系统各自作为一个整体负责承担 ASIL D 级别的安全目标。主系统和冗余系统可以存在一些合理的安全分解，从而降低对单个零件的要求。每个执行器单元都应满足各自的功能安全需求，同时主、辅系统相互配合，合理切换。

- **电子电气架构：**E/E 架构中自动驾驶域控制器、智能网联域控制器、车身域控制器，须各自承担从整车层分配下来的特定功能安全等级要求。各控制器之间的信号交互须按照功能安全要求进行通信保护，满足数据完整性要求。各子系统的供电也需满足所分配的功能安全等级和 Fail-Operational 要求。

- **网络安全：**自动驾驶智能重卡需要确保其免受网络安全攻击。赢彻科技在网络安全方面的开发目标可以总结为两点：第一，能够保护智能重卡抵御各类潜在的网络攻击风险；第二，能够保证各类数据采集、使用和存储的合规性。

- **人机交互系统：**人机共驾阶段，人机交互在自动驾驶任务中不仅比重很大，而且跟安全息息相关。赢彻科技要求人机交互系统的设计能提升安全员对自动驾驶能力的信任。人机交互系统从功能上须具备可用性，即需要提供人机共驾任务中必需的交互信息，避免提醒过度或提醒不足。人机交互系统能准确监控安全员的状态，安全协调人工驾驶和自动驾驶之间的切换。人机交互系统系统中各个零部件都需满足特定的功能安全等级。从预期功能安全角度，系统所提供的交互模式要易于理解和操作，有效减少安全员可能的误用。

3 安全开发实践

为满足智能重卡的第一设计要求——安全，赢彻科技从流程到技术实现，从整车到核心系统，均进行了非常体系化的开发实践，也在一些行业尚无成熟解决方案的问题上持续进行探索。

3.1 安全流程实施

组织文化	开发流程	量产后流程
安全至上的文化	ODD 内万余种场景的安全分析	严格的生产和质量把控流程
以安全为核心的组织架构设计	涵盖概念、系统、软件、硬件的安全设计和需求，相互可追溯	规范的运营、操作、维护和报废流程，易于使用、维护和升级
功能安全能力建设	完善的设计和需求评审	详尽而专业的安全员培训体系
质量管理体系	严格的代码审查	
根据项目进行安全开发管理	综合运用 SIL、HIL、DIL 和实车等多种测试方法	

* 图：赢彻科技 - 功能安全流程实践

赢彻科技的功能安全开发流程全面涵盖整车和零部件开发，并于 2021 年通过 ISO 26262 ASIL D 认证。在整个组织架构和项目层面，赢彻科技严格遵循 ISO 26262 的相关要求进行功能安全设计和开发，涵盖概念设计、系统开发、软硬件开发、测试验证和生产等产品全生命周期。针对深度学习算法和 Linux 操作系统不符合功能安全要求的现状，赢彻科技主要在模块化架构设计、软件单元安全鉴定、算法冗余、针对深度学习和 Linux 操作系统的测试验证等方面进行强化。

赢彻科技根据 ISO 21448 进行完整的 SOTIF 开发，并促进 SOTIF 和功能安全开发流程的融合。赢彻科技从系统改进、请求安全员接管和人机交互优化等角度提出了一系列 SOTIF 安全需求。经过有针对性的测试和验证，提高了系统和功能的能力边界值，减少了安全员可能的误操作，确保搭载赢彻科技自动驾驶系统的智能重卡具备高度的可信任性（Trustworthiness）。

赢彻科技依据 ISO/SAE-21434 开发方法论，建立了涵盖产品定义、研发设计和生产运营的全生命周期闭环的信息安全方案，并正在进行《ISO/SAE 21434 道路车辆 - 信息安全工程》管理体系认证。

在公司和项目层面，赢彻科技建立了完善的支持性流程，并配备了相应的工具，在量产项目中将其付诸实施。其中，问题管理流程支持问题发现、报告、分析、解决和关闭的全过程。针对本层级无法解决

的问题，会根据上升（Escalation）机制，逐层上报，直到问题被有效地讨论、决策和解决。对于安全相关的决策，会根据影响范围和严重程度，由相关专家和管理团队进行决策。在公司层面成立了安全委员会，负责对重大安全事项做最后决策。另外，公司根据项目实践经验，持续改进公司的各项流程和管理策略，优化公司的安全开发工作。

目前，自动驾驶行业针对未知的不安全场景尚无公认的场景库和应对措施。赢彻科技在分析理解大量实车运行场景的基础上，不断探索提高仿真的真实性和有效性，从而利用仿真覆盖更多的场景。

另外，在评估自动驾驶系统的安全性方面，行业还非常缺乏明确、完整和统一的标准。赢彻科技认为，平均每次接管的行驶里程间隔 MPD 只是评价自动驾驶能力的指标之一，但不是证明其安全性的充分条件。赢彻科技基于测试样车和快速增多的量产车的大量运行实践，不断开发各种安全度量指标（Metric），逐步建立和完善卡车自动驾驶系统的安全评估体系。

3.2 车规级达标实践

考虑到商用车相对恶劣的使用环境和更长的寿命要求，赢彻科技对各核心零部件建立了一套详尽的测试标准。这套标准与商用车通用国标 GB/T28046 的要求相比更为严格。此外，赢彻科技结合自动驾驶的特性，针对实际场景，拓展了多项功能、性能测试内容。

结合上述完整的硬件车规要求和验证体系，赢彻科技从机械、电气、电磁兼容性、环境耐久等方面对各零部件和整车进行了严格测试。历经 EV、DV 和 PV 等各个阶段，使得智能重卡所采用的硬件套装全都符合车规级要求，包括 ADCU、传感器、天线、网关以及底盘子系统等。

3.3 自动驾驶系统安全实践

赢彻科技的自动驾驶系统，从硬件上已基本达到 Fail-Operational 要求，并在核心部件和软件模块上实现了从顶层分配下来的功能安全需求。目前正在针对更多的具体场景持续完善相应的安全策略。

在功能定义上，根据触发原因和风险等级不同，赢彻科技设计的多级应急（Fallback）策略，支持不同时间间隔的安全员接管，并且在紧急情况下可以自动安全停车，从而满足 Fail-Operational 要求。

赢彻科技的自动驾驶系统采用激光雷达 + 毫米波雷达 + 摄像头的多种类型、冗余设计的传感器配置，实现全车 360°环境感知覆盖。感知算法支持多路传感器冗余输入。各传感器分别按照所需的功能安全等级来选型和开发。在单个传感器发生故障的情况下，整个感知系统可以维持安全行驶所需的基本功能。各传感器相互弥补短板，保证整个感知系统在 ODD 范围内应对各种场景都有足够的性能。

赢彻科技自研的自动驾驶域控制器 ADCU 是行业首个全冗余、高算力、车规级自动驾驶域控制器。它采用 CPU + SoC 的方案，充分利用 CPU 的高性能和 SoC 的高安全等级。安全相关的软件、算法运行在符合功能安全要求的芯片上。ADCU 实现了电源管理、系统诊断、失效处理恢复、时间同步等安全相关

的功能和监控。同时，A/B 面的设计可以在一套系统失效的情况下，冗余系统在设计时间内及时接管，实现 Fail-Operational。

软件和算法从故障诊断、故障响应、性能强化三个方面进行安全开发，支持 5 大类超过 2000 项实时故障监控。一旦检测到故障，系统立即触发对应等级的 Fallback 机制，并在有需要时执行主备控制系统的热切换。赢彻科技独创的 ISC（Inceptio Safety Checker）安全校验可同时覆盖功能安全和预期功能安全，识别因系统故障或性能不足所引发的安全风险。一旦识别到碰撞风险，系统将通过人机交互系统通知安全员，并在必要条件下执行安全停车。

当前，自动驾驶系统中采用的部分硬件和软件不完全符合功能安全要求，例如，部分芯片不符合功能安全要求，深度学习算法的安全验证还没有行业统一的方案，等等。赢彻科技正在持续不懈地解决这些行业新问题，并在过程中与产业伙伴紧密合作。

此外，如何平衡自动驾驶的安全性和舒适性，尚处于探索过程中。在当前技术条件下，如果为了更智能的功能和更高的自动驾驶占比，而放松一些安全限制，就会增大自动驾驶车辆的安全风险。如果因为探测到安全风险而频繁触发 Fallback，那么自动驾驶功能的可用性和安全员体验就会打折扣。赢彻科技在不断优化系统的性能边界和安全策略，力求在保证安全的前提下，尽可能提升系统的可用性和安全员体验。

3.4 线控底盘安全实践

赢彻科技与主机厂伙伴联合开发量产的智能重卡的底盘是行业首个全冗余线控底盘，支持 10 秒以上安全运行，并可实现安全停车。其中，线控制动系统具备三重冗余设计，主系统失效时，两套冗余系统可按照设定的策略依次接管。线控转向系统有一套主转向和一套冗余转向组成，为重卡业内首创，同样可在主转向发生故障的情况下由冗余转向系统接管。针对整车层面的防止非预期减速和非预期转向等安全目标，赢彻科技在自动驾驶系统中开发了部分针对线控底盘的故障诊断和响应机制，保证行车安全。

当前，供应商伙伴提供的部分底盘子系统（如转向系统）的功能安全开发只满足了赢彻科技提出的一部分安全需求。赢彻科技通过自动驾驶系统加强监控来补足安全性，但这尚不是最高效的手段，正在联合供应商伙伴进行相关子系统的补充开发，令其达到功能安全的要求。同时，推动供应商启动研发完全符合自动驾驶和功能安全要求的新一代线控底盘子系统。

3.5 电子电气架构安全实践

赢彻科技与主机厂伙伴对商用车行业的整车电子电气架构进行了大量的重新设计和优化，成为行业首个域集中式、全冗余、多通讯链路、具备整车 OTA 能力的架构。另外，赢彻科技通过仿真台架和实车测试充分验证各子系统集成后的配合情况，测试确认功能要求和性能要求的达成度；并通过故障注入测

试、回归测试等方法，测试确认功功能要求和性能要求的达成度，安全目标是否达成。

相对于乘用车领域主流的电子电气架构和技术指标，商用车的电子电气架构在功能安全方面的成熟度要低很多。因此，赢彻科技与主机厂伙伴合作进行的大量重新开发，保证了当前量产车型电子电气架构的安全性。

同时，赢彻科技在联合主机厂伙伴进行正向研发，目标是在下一代智能重卡的电子电气架构中完全满足自动驾驶和功能安全的要求。

3.6 网络安全实践

赢彻科技针对智能重卡设计了全方位网络安全方案，涵盖云、管、车端入口、车内网络等。可应对多种商用车应用场景攻击，全面保障自动驾驶系统的密码安全、数据安全、通信安全和系统安全。例如，对 ADCU 硬件设置 HSM（Hardware Security Module）、SHE（Secure Hardware Extension）等特定的安全硬件，可以对数据进行加密、解密、密钥存储、签名验证等操作。通过实施数据机密性保护、完整性保护等机制，对系统和应用敏感数据（如密钥、密码等）进行保护，防止系统、应用和用户因未经授权的访问而导致的敏感数据的盗窃和损坏等安全或隐私风险，为自动驾驶重卡的运营构建安全的环境。

3.7 人机交互系统安全实践

在智能重卡的人机交互系统研发方面，赢彻科技与主机厂伙伴进行了大量合作，综合运用多模态、全冗余交互，提高系统的安全性。将安全相关的信息和提醒，通过听觉、视觉、触觉等多种模式以及不同屏幕传递给安全员，确保提醒充分。在设计方面，根据交互的类型和请求接管的原因、危险和紧急程度等，赢彻科技制定了不同的接管优先级。在内容方面，赢彻科技的人机交互系统通过多种可视化信息增强安全员对自动驾驶系统的信任度。

在预期功能安全方面的实践方面，尤其关注防止可预见的安全员误操作，一方面，赢彻科技不断优化安全员状态监控和提醒策略，提升对安全员状态识别的准确度。另一方面，通过优化不同模态提醒的组合方式，逐步实现人机交互系统的易用和好用，即易于理解、易于使用、不存在过度设计和防止误用，增强安全员对于自动驾驶系统的信心。

在如何设计一套优秀的人机交互系统方面，赢彻科技结合人因工程研究和设计的经验，正在实践中继续探索优化。

4 行业性挑战

在智能重卡和自动驾驶系统的量产开发实践中，我们深刻体会到自动驾驶系统的安全开发任重道远，有一系列的行业性质的全新挑战有待解决，例如：

- **如何保证 ODD 内极端场景的覆盖：**目前自动驾驶全行业正在大量累积数据，用数据驱动算法迭代。但是，对于自动驾驶而言，需要覆盖的 ODD 范围是复杂且多变的，多个维度的 ODD 要素往往以矩阵式的关系交织组合在一起，造成了场景的指数增长。针对更高阶的 L4 自动驾驶，面对充分覆盖 ODD 场景所形成的组合爆炸（Combinatorial Explosion），现有的数据采集模式和测试方法难以满足要求。基于仿真和数据增强的技术会被越来越多的应用。
- **深度学习模型的不可解释性和不可预测性：**深度学习是一个基于统计学的人工智能技术。对于自动驾驶这样极其复杂的场景，其泛化能力比较差，对于极端情况（Corner Case）的结果有不确定性，这对传统的安全分析机制提出了挑战。业界也充分认识到这一个问题并尝试解决，比如添加一套基于规则的校验机制，以及新的方法论（SOTIF）。这些措施有效性尚待在实践中的验证。
- **自动驾驶操作系统的功能安全合规：**自动驾驶系统要求操作系统具备实时性，满足功能安全、信息安全等要求，而 Linux 操作系统并不满足这些要求。行业的应对方式是在 Linux 内核上进行二次开发，或将 Linux 与符合安全要求的操作系统（如 QNX）搭配使用，但这些方式都比较碎片化、效率低、开发成本高。基本上，致力于通过安全认证的车规 Linux 都还处在开发过程中。

赢彻科技正在自己的量产项目中积极探索解决方案，更希望与行业伙伴加强合作，加速推动这些问题的解决。

CHAPTER 4

第四章

展望未来：
自我演化，走向无人驾驶

展望未来：自我演化，走向无人驾驶

赢彻科技通过 3 年多的努力，实现了 L3 能力级别智能重卡的量产落地。为了进一步实现 L4 级别的自动驾驶重卡量产落地，还需实现三个跨越：

- **更好的 ODD 覆盖率，应对各类突发的动态场景。**由于不再依赖安全员，在特定路段内，需要系统可以自主应对各类潜在动态事件。比如，可以应对雨雪雾等低能见度极端天气，响应临时限速标牌，自主绕行临时施工隔离路段，响应交警的人工指挥，主动避让各类异物等。这就要求，静态 ODD（与地图类的道路结构相关）覆盖率需由当前的 99.8% 提升至 100%，动态 ODD（与天气、临时施工、交警指挥等相关）覆盖率需由当前的 95% 提升至 99.99%。
- **MPD 上若干数量级的提升。**基于对头部快递快运公司的访谈，当前人工驾驶条件下，赔付成本超过 5 万元人民币的百万公里事故率为 0.1~1 次。这意味着，有显著事故的 MPD 范围在 100 万公里 -1000 万公里。可以预见，在全无人驾驶场景下，人们对事故的容忍度将大幅度降低。假设容忍度降低 10 倍，相应 MPD 的要求范围将会在 1000 万公里 -1 亿公里。
- **更强的 Fallback 控制能力。**首先通过稳定性及冗余系统设计优化，将 Fallback 频次降至极低水平。同时升级 MRC（Minimal Risk Condition，最小风险状态）能力，使车辆具备自主在应急车道安全停靠，跛行回家甚至远程驾驶的能力。

为了实现上述目标，自动驾驶重卡及系统需要在以下四方面提升：

- 算法迭代升级，以应对更高的 MPD 及 ODD 要求。这个对自动驾驶技术提出了极高的要求，我们下面会展开详细讨论。
- 持续改进和升级冗余系统设计，优化功性能及稳定性表现，包括传感器、ADCU 和线控底盘系统。为了满足 L4 级自动驾驶产品的更高要求，线控底盘系统的主系统与冗余系统应是高度集成一体化的设计，可以支持故障时毫秒级的无缝切换，同时在功能、性能方面与主系统完全相同，并且可长时间工作。在传感器和 ADCU 方面，也需要做到在任何单一部件故障情况下，仍可支持继续自动驾驶。在稳定性方面，通过当前产品投放运营后的磨砺和实战检验，不断提升硬件系统和整车层面的系统稳定性，将系统 Fallback 频次降到无人驾驶可接受水平。
- 升级 MRC 机制，确保在各类极小概率的 ODD 场景及失效模式下，系统依旧可以支持自主行驶到预设的安全地带停车。在确保安全的同时，避免对社会交通产生影响。
- 开发远程驾驶系统：依托于 5G 网络“高带宽、低时延”的特性，将车载摄像头、雷达等传感器采集到的车辆周围场景信息传输到虚拟驾驶舱，在偶发场景下 MRC 停车后通过安全员远程控制，实现避障绕行恢复运行能力。

赢彻科技的 L4 级别无人驾驶研发与探索

赢彻科技通过 L3 能力级别智能重卡的量产实践，在硬件平台和系统架构方面均建立了坚实的发展基础。接下来，将继续提升数据资产、核心算法和算力。随着量产里程的不断积累和产业在核心零部件上的不断升级，我们的系统将向 L4 级不断逼近。

2021 年 12 月，赢彻科技已经成功完成了 L4 级方案验证。L4 级验证方案大量复用当前 L3 能力级别智能重卡量产车型：

- 感知方面，将两台远程激光雷达和一台工业 PC 加装到 L3 能力级别智能重卡量产车上，工业 PC 只用于所加装激光雷达的检测计算。加装激光雷达的检测结果作为额外信息，输入到赢彻科技已量产的 L3 能力级别自动驾驶系统。
- 规划控制方面，对规划算法进行了升级，以处理施工等复杂场景，但算法整体依然运行在量产系统上。
- 为了加强安全预防措施，增加了远程控制功能。
- 除此之外，对量产自动驾驶系统和整车没有做任何改变。

我们在封闭高速公路上成功实现了完全无人驾驶的测试验证。整个行程是完全自主的，没有任何人为干预。为了对 L4 进行全面验证，全程模拟了国内最丰富、高难度和真实的场景和交通流：

- **道路结构：** 高速公路长 24 公里，包含多种坡度的上下坡道、大曲率弯道、长隧道、桥梁、出入高速匝道和收费站等典型高速道路结构。
- **交通场景：** 自动跟车、车道保持、自动变道、施工车辆及场景识别、自动避让、自动跟停及驶入收费站等典型场景。

L4 级的技术验证令人振奋，这证明了赢彻科技已量产的自动驾驶软硬件架构和整车面向 L4 具备高度的可扩展性。当然，从验证到批量生产还有很长的路要走，需要更多突破性的技术进步，才有可能真正实现无人化。

* 图：赢彻科技 -L4 能力级智能重卡验证方案

自我演进，走向无人驾驶

为了实现千万级别的 MPD，需要在冗余系统、硬件性能、算法能力等方面同步改善。根据目前对商用车产业的了解，预计 2024 年左右，商用车头部供应商将会发布满足 L4 级要求的高度集成、自冗余的线控底盘产品，L4 级卡车开发执行器层面的瓶颈问题将得到解决。

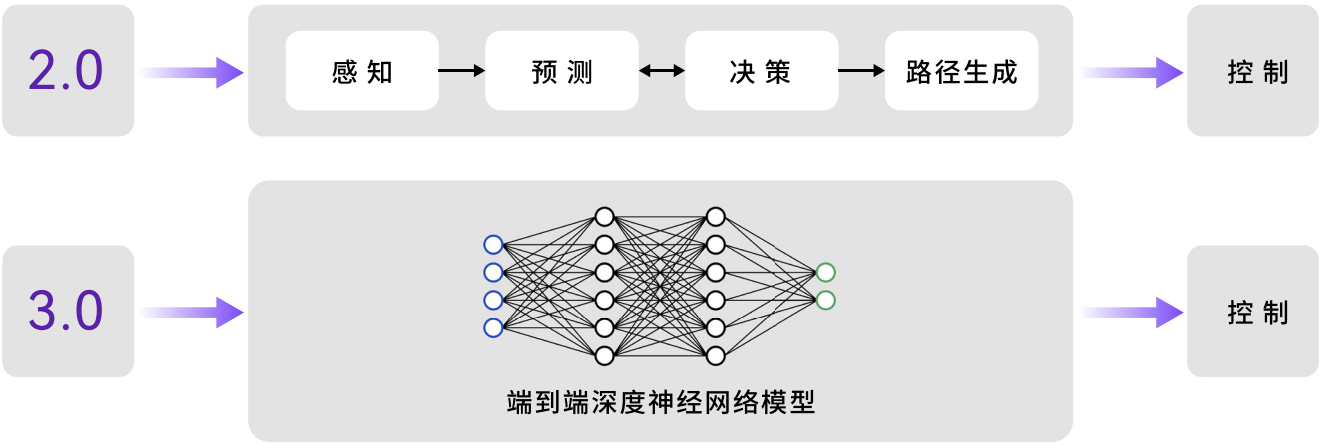
随着自动驾驶行业内相关传感器成熟度的不断提高，自动驾驶域控制器（ADCU）算力的快速提升，预计到 2025 年左右，激光雷达、毫米波雷达等传感器的有效检测距离都将提升至 300 米，ADCU 算力可达 2000TOPS 以上。

因此我们认为冗余及硬件领域将不会成为 L4 技术路线上的瓶颈。主要的挑战将集中在软件算法层面，需克服如下三方面的技术障碍：

- **获得监督学习所需的人工标注数据，代价巨大。**考虑到测试和验证自动驾驶系统的安全性需要数亿甚至数十亿公里的驾驶数据，而传统的基于监督学习的自动驾驶系统高度依靠人工筛选和标注数据，很难扩大到所需的数据规模。
- **基于规则的建模和决策系统无法应对复杂交通场景。**在十字路口等复杂场景，对交通参与者的意图、交互、甚至博弈进行建模，即所谓的行为建模，超出了当前主流基于规则的建模和决策系统的能力。
- **传统自动驾驶系统架构遭遇瓶颈。**传统架构基于经典的机器人框架，该框架将整个自动驾驶过程划分为感知、规划和控制等几个子模块。信息以单向形式从传感器到执行器流转，无法捕捉自动驾驶车辆与其周围环境之间的双向相互作用。

整个自动驾驶行业都在大力解决这些瓶颈。自动化数据挖掘、半自动化数据标注正在逐步走向应用。数据驱动的决策和规划方法也在被融入现有的基于规则的框架之中，感知和预测的边界正被打破。

基于这些趋势，我们大胆设想一种全新的自动驾驶架构，该架构可以拆除自动驾驶系统子模块之间人为设计的边界，并将其替换为端到端的深度神经网络。



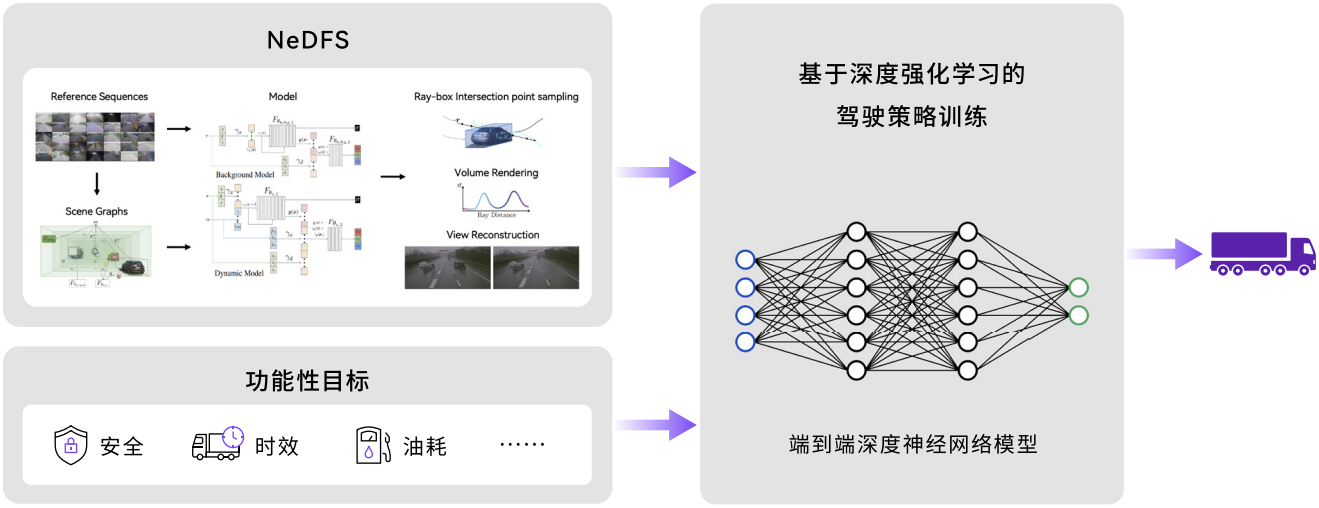
* 图：基于端到端神经网络的下一代自动驾驶系统

与以前简单地将传感器输入与车辆执行器连接的方法不同，我们端到端的网络输入为传感器输入，输出是轨迹安全包线，经典控制算法可以根据轨迹要求和车辆状态自适应地控制车辆。我们认为经典控制方法仍然非常适合轨迹跟踪，并具有可以保证误差范围和安全裕度的优势。

我们受到最近两项技术进步的启发：

- **首先是深度强化学习在驾驶游戏中的应用。**通过强化学习的 AI Agent 可以在超逼真的赛车游戏中超越专业玩家的表现，已经获得证明。
- **第二是神经辐射场 NeRF（Nerual Radiance Fields）。**NeRF 提供了一种超逼真的方式，可从视频输入合成新视图，而无需手动操作。与目前基于 CG（Computer Graphics）的模拟器相比，NeRF 可以以极低的成本提供和真实世界几乎无法区分的逼真图像。

我们相信行业正处于开发终极驾驶模拟器的风口浪尖，可以实现直接从传感器输入中学习驾驶策略。通过基于 NeRF 的模拟器，可以使用强化学习的技术来训练深度神经网络，只需定义一个奖励函数（比如安全、高效和舒适），便可获得良好的驾驶行为。



* 图：训练端到端的自动驾驶深度学习网络：利用基于 NeRF 的仿真器可以通过强化学习的手段自主学习驾驶策略

这种端到端框架提供了一个关键优势，即它是无监督的。它不需要手动标记数据，只需要来自真实场景的数据。这些数据由自动驾驶或手动驾驶车辆捕获。驾驶环境的基本表示，以及所有交通参与者的交互影响，都是从数据中隐式学习的，而不是由经验丰富的开发人员手工制作的。因此，它的扩展性可以拥抱现实世界驾驶中的极端复杂性。

实现这一目标面临许多挑战，预计未来还需要多年的研发。主要挑战有三项：

- **训练难度：**当一个大型深度学习网络所代表的空间几乎不受限制时，如何有效地训练它？
- **安全保证：**如何保证这个系统可以满足自动驾驶的安全要求？这个问题会因为深度学习的大量使用变得尤为突出。和传统的基于规则或者模型的方法相比，深度学习的网络没有很好的解释性，结果没有办法进行误差分析，因此，传统安全设计的方法论有待突破。
- **样本质量：**如何确保样本在一个自演化系统里不被不合规的行为（如超速）污染？

尽管面临挑战，自动驾驶必须从目前的监督方法转向弱监督或无监督方法，以满足现实世界交通中完全自动驾驶的最严格要求。最近在视图合成、模拟和深度强化学习方面的技术进步使我们相信，一个自我进化和可扩展的自主自动驾驶量产方案必将可以实现！该项突破是自动驾驶领域的重大突破，适用于所有车辆。

赢彻科技在无监督自动驾驶系统的演进中具备优势。公路卡车运输可以首先从我们的端到端结构中受益，因为路线是点对点的。受限制的运营路线和不太复杂的流量，使网络的训练相对简单。

赢彻科技利用高保真卡车动态模型开发了独特的仿真环境。同时，赢彻科技正在开发基于 NeRF 的渲染引擎来支持动态流量，打破了目前 NeRF 仅适用于静态环境的限制。

预计到 2025 年，赢彻科技的端到端系统将开始在车队上得到验证。届时自动驾驶能力将快速增长，迈向全无人驾驶！

附录：英文缩略语及含义

英文	全称	中文释义
ABS	Antilock Brake System	制动防抱死系统
AD	Autonomous Driving	自动驾驶
ADCU	Autonomus Driving Control Unit	自动驾驶域控制器
API	Application Programming Interface	应用编程接口
ASIL	Automotive Safety Integration Level	汽车安全完整性等级
AUTOSAR	Automotive Open System Architecture	汽车开放系统架构
BEV	Bird's Eye View	鸟瞰视角
BIOS	Basic Input/Output System	基本输入输出系統
BSFC	Brake-Specific Fuel Consumption	燃油消耗率图
CAN	Controller Area Network	控制器局域网络
CEPS	Column Electric Power Steering	管柱式电动助力转向
CVE	Common Vulnerabilities & Exposures	公共漏洞和暴露
DDT	Dynamic Driving Task	动态驾驶任务
DFA	Dependent Failure Analysis	相关性失效分析
DIA	Development Interface Agreement	开发接口协议
DIL	Driver In Loop	驾驶员在环测试
DMIPS	Dhrystone Millions of Instructions Per Second	测量处理器运算能力的最常见基准程序之一
DMS	Driver Management System	驾驶员监控系统
EBS	Electronic Brake Systems	电子制动系统
ECC	Error Correcting Code	纠错码

英文	全称	中文释义
ECU	Electronic Control Unit	电子控制器
EEA	Electrical/Electronic Architecture	汽车电子电气架构
EHPS	Electronic Hydraulic Power Steering	电子液压助力转向
ETB	Electronic Trailer Brake	电子挂车制动
FEAD	Fuel Efficient Autonomous Driving	节油自动驾驶算法
FHTI	Fault Handling Time Interval	故障处理时间间隔
FMEA	Failure Mode and Effects Analysis	失效模式与影响分析
FoV	Field of View	视野范围
FSR	Functional Safety Requirement	功能安全需求
FTA	Fault Tree Analysis	故障树分析
GNN	Graph Neural Network	图神经网络
HARA	Hazard Analysis and Risk Assessment	危害分析与风险评估
HIL	Hardware In Loop	硬件在环测试
HMI	Human Machine Interface	人机界面
HOD	Hands Off Detect	方向盘手握监测
HPS	Hydraulic Power Steering	液压助力转向
HSM	Hardware Security Module	硬件安全模组
HSR	Hardware Safety Requirement	硬件安全需求
IRS	Inceptio Robotics System	赢彻科技机器人系统
ISO	International Organization for Standardization	国际标准化组织
ISP	Image Signal Processing	图像信号处理
ISPEC	Inceptio Standard Performance Evaluation Code	赢彻科技标准性能评测程序集
LCC	Lane Centering Control	车道居中控制

英文	全称	中文释义
LIN	Local Interconnect Network	本地互联网络
LLL	Life Long Learning	持续学习
LST	Large Scale Test	封闭场地测试
LSTM	Long Short-Term Memory	长短期记忆
mAP	Mean Average Precision	全类平均正确率
MCAL	MicroController Abstraction Layer	微控制器抽象层
MPD	Mileage Per Disengagement	每次人工接管的行驶里程间隔
MRC	Minimal Risk Condition	最小风险状态
NHTSA	National Highway Traffic Safety Administration	美国高速公路安全管理局
ODD	Operational Design Domain	运行设计域
OEM	Original Equipment Manufacturer	主机厂
ORT	Open Road Test	开放道路测试
OS	Operating System	操作系统
OTA	Over The Air	在线升级
PCB	Printed Circuit Board	印制电路板
PCC	Predictive Cruise Control	预测性巡航控制
PCIe	Peripheral Component Interconnect Express	一种高速串行计算机扩展总线标准
PFMEA	Process Failure Mode and Effects Analysis	过程失效模式和影响分析
PMHF	Probabilistic Metric for Random Hardware Failure	硬件随机失效度量指标
PnG	Pulse and Glide	脉冲加速滑行的驾驶策略
PPAP	Production Part Approval Process	生产件批准程序
RIPU	Active Learning via Region Impurity and Prediction Uncertainty	基于区域不纯度和预测不确定性的主动学习

英文	全称	中文释义
RTOS	Real-Time Operating System	实时操作系统
SAE	Society of Automotive Engineers	美国汽车工程师学会
SES	Smart Emergency Switch	冗余电源控制器
SHE	Secure Hardware Extension	安全硬件扩展
SIL	Software In Loop	软件在环测试
SMS	Safety & Security Management System	安全管理系统
SOA	Service-Oriented Architecture	面向服务的架构
SoC	System on Chip	单片系统
SOP	Start Of Production	批量生产
SOTIF	Safety of the Intended Functionality	预期功能安全
SPI	Serial Peripheral Interface	串行外设接口
SSR	Software Safety Requirement	软件安全需求
TCO	Total Cost of Ownership	全生命周期成本
TOPS	Tera Operations Per Second	代表处理器每秒钟可进行一万亿次操作
TSR	Technical Safety Requirement	技术安全需求
XBR	External Brake Request	外部制动请求

承载物流的美好

WE MAKE LOGISTICS GRACEFUL

扫码关注
赢彻科技公众号
www.inceptio.ai

2022 年 9 月版