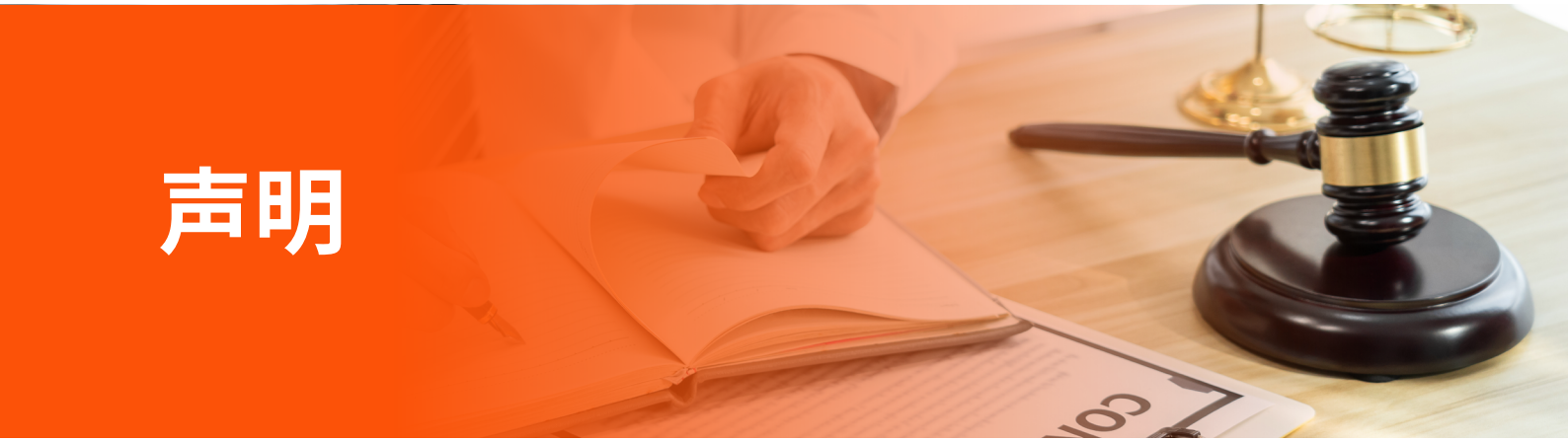
亚马逊云科技 | pwc

行稳致远 智驭未来

汽车行业新兴区域合规洞察报告

2025年11月

声明



本报告由普华永道商务咨询（上海）有限公司（以下简称“普华永道”）和 Amazon Web Services, Inc. 或其关联方（“亚马逊云科技”）分别撰写，双方就各自撰写的内容分别、独立享有相关知识产权。其中普华永道负责撰写第一部分“汽车出海智能网联合规解读”、第二部分“中东与拉美地区智能网联汽车合规要点”和第三部分“中国汽车企业布局海外市场的合规策略建议”中的正文以及“普华永道智能网联汽车合规服务”，单独享有该部分的知识产权；亚马逊云科技负责撰写第三部分“中国汽车企业布局海外市场的合规策略建议”中的“亚马逊云科技汽车行业解决方案”和“亚马逊云科技合规服务”，单独享有该部分的知识产权。

关于普华永道部分的说明：

本报告仅作为一般性指导，并不构成提供任何形式的法律咨询、会计服务、投资建议或专业咨询。本文件所提供的信息不能取代专业税收、会计、法律咨询或其他相关专业咨询建议。在作出任何决定或采取任何行动之前，您应该咨询专业顾问，并向其提供与您特定情况相关的所有事实。

本文件的信息来源于本次调研所收集的数据以及公开的资料，我们对信息的完整性、准确性或及时性概不作出任何保证或担保，也不提供任何明示或暗示的担保，包括但不限于对业绩、适销性和适用于特定用途的担保。在不同时期可能会得出与本报告不一致的观点。

本文件仅供一般参考使用，不构成具体事项和咨询意见，普华永道不对本报告内容承担审慎责任，且未就本报告内容作出任何明示或暗示保证。普华永道不就本报告内容向任何人士承担任何责任或义务，也不向任何人士承担因本报告所引起的或与本报告有关的任何责任或义务。读者不应依赖本文件内容作出投资或其他商业决定。如需具体意见，请咨询专业顾问。

关于亚马逊云科技部分的说明：

本部分内容陈述了亚马逊云科技在2025年11月的有关服务产品及实践，该等信息可能变化且亚马逊云科技不会另行通知。客户对于本部分的信息以及亚马逊云科技的产品或服务应自己做出独立的判断，该等内容都是“依现状”提供，不包含任何明示或者暗示的保证。本部分内容并没有创设来自亚马逊云科技、北京光环新网科技股份有限公司（“光环新网”）、宁夏西云数据科技有限公司（“西云数据”）、或其各自的关联方、提供方或许可方的任何保证、陈述、合同性承诺、条件或者担保。亚马逊云科技、光环新网、西云数据对其各自的客户的义务和责任均由适用的客户协议管辖。本部分内容不是亚马逊云科技、光环新网、西云数据和其各自的客户之间任何协议的组成部分，也不构成对任何协议的修改。本报告中凡是提及或引述亚马逊云科技中国区域或与之相关的服务等描述，均表明该等服务是由亚马逊云科技通过西云数据运营的宁夏区域和光环新网运营的北京区域来提供。亚马逊云科技中国区域的运营独立于亚马逊云科技全球其他区域。

目录

声明 1

引言 5

01 汽车出海智能网联合规解读 6

自动驾驶 7

车联网 10

02 中东与拉美地区智能网联汽车合规要点 14

中东篇 15

1. 市场洞察 15

2. 合规洞察 17

拉美篇 23

1. 市场洞察 23

2. 合规洞察 26

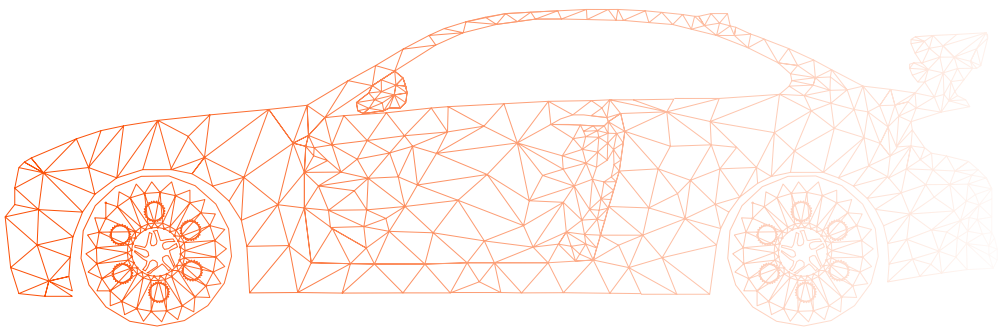
CONTENTS

03 中国汽车企业布局海外市场的合规策略建议 32

合规解决方案与服务 38

1. 普华永道智能网联汽车合规服务 39
2. 亚马逊云科技汽车行业解决方案 41
3. 亚马逊云科技合规服务 47

附录 51



引言

全球汽车产业正在发生重大变革，电动化、智能化、网联化趋势加速推动传统燃油车向智能网联汽车转型。智能网联汽车可实现环境感知、行驶决策、动作执行和联网交互等功能，已经成为汽车产业发展的重要方向。

与此同时，中国汽车产业正在经历新能源与智能网联技术发展的双重变革，新能源汽车对传统燃油车的替代速度亦不断加快。截至2024年，相比于传统燃油车，新能源汽车渗透率已连续五年实现高速增长，销量渗透率达到约40%。2025年，各大车企陆续发布高阶智驾计划，新能源汽车行业已从“上半场电动化”正式迈向“下半场智能化”。在这一变革中，智能网联技术与新能源汽车的深度融合推动了智能网联汽车的发展，相关政策的支持与技术研发的不断投入使得中国汽车行业在智能座舱、自动驾驶、车联网等领域成果斐然，不仅搭建起从核心零部件（如芯片、传感器）到整车生产的完整产业链，还通过“中国品牌、中国智造、中国技术”打动海外消费者，将汽车出口发展成为中国汽车市场新的增长极。2024年中国汽车出口总量达到586万辆，已成为全球最大汽车出口国，领跑全球市场。

鉴于国内智能网联汽车市场竞争日益激烈，领先的智能网联汽车企业已将视野扩展至海外市场。中汽协数据显示，2024年中国新能源汽车出口量达到128.4万辆，占所有动力车型出口的21.9%，同比增长6.7%。特别值得注意的是，中东与拉美地区因当地可再生能源等政策的支持和市场需求的增长，已成为中国新能源汽车出口的新热点，其中墨西哥和阿联酋已是新能源汽车出口重点区域，出口量同比分别增加约370%和102%。在这一进程中，企业需关注中东与拉美地区各个国家的监管环境，包括车联网技术监管和隐私保护等方面。

在此背景下，本报告旨在为有意拓展中东与拉美市场的智能网联汽车企业提供行业洞察与指导建议。本报告中，我们主要围绕智能网联汽车行业在中东与拉美地区的出海洞察、监管合规环境与合规解决方案这几个方面展开讨论。

01

汽车出海智能网联合规解读

随着中国汽车产业从“电动化”迈向“智能化”深水区，智能网联汽车成为新的增长极，加速企业在中东和拉美等战略市场的布局。

在这一国际化进程中，完善且与时俱进的合规体系将成为智能网联汽车产业全球化发展的关键支撑。面对多元化的国际监管环境，企业不仅需要考虑 UN R155[1]、UN R156[2]、ISO/SAE 21434[3] 等相关法规要求和国际标准，还需结合不同国家的数据主权、安全监管及本地化政策，针对不同业务场景灵活调整技术架构与数据流转路径，以实现“合规嵌入式设计”。通过将安全与合规内生化于技术体系之中，企业方可在确保车联网系统安全可控、数据合规流通的同时，增强整体业务韧性与可持续竞争力，为智能网联汽车的国际化落地奠定坚实基础。

> 在智能网联汽车的技术体系中，**自动驾驶**与**车联网**是两大核心驱动板块，也是合规高风险重点领域，不仅涉及敏感数据的采集、处理及跨境流转，还直接关联隐私保护、网络安全及技术准入要求。

自动驾驶

自动驾驶作为智能网联汽车产业的重要方向，具有高技术耦合、高数据密度、高安全敏感性等特征，其技术路径复杂、合规边界多元，出海过程中应以“安全为底线、合规为前提、技术为支撑”作为原则，构建覆盖数据流、算法流、通信流与运营流的系统化技术合规框架。

> 企业可从**基础设施建设**、**数据采集**、**高精地图制作**、**平台搭建、测试与部署**、**量产与优化**六个环节出发，分析全球化布局和业务落地中需要重点关注的技术合规要求，建立“**技术与合规并行**”的出海路径。

[1]R155：联合国法规第 155 号《网络安全及网络安全系统》（UN Regulation No.155 – Cyber Security and Cyber Security Management System），由联合国欧洲经济委员会（UNECE）的世界车辆法规协调论坛（WP.29）发布，为全球首个针对汽车网络安全的国际规范，规定了车辆制造商在整个汽车生命周期内必须实施的网络安全管理措施，以确保汽车的网络安全和防护能力。

[2]R156：联合国法规第 156 号《软件更新及软件更新管理系统》（UN Regulation No.156 - Software Update and Software Update Management System），由联合国欧洲经济委员会（UNECE）的世界车辆法规协调论坛（WP.29）发布，规范车辆软件更新及其管理系统的要求，旨在确保车辆软件更新的安全性、可追溯性与合规性，防止软件更新过程中的网络安全风险。

[3]ISO/SAE 21434：《道路车辆 – 网络安全工程》（Road Vehicles - Cybersecurity Engineering），由国际标准化组织（ISO）和美国汽车工程师学会（SAE）联合制定，用于指导汽车网络安全风险管理。该标准适用于车辆所有电子电气系统的全生命周期，帮助企业在各个阶段系统性地识别、评估和应对网络安全风险。

1 基础设施建设

企业通常根据自动驾驶测试、运营区域的海外路线规划和办公地点需求进行数据中心的选址和部署以及选择运营商或跨境专线方案。同时还需要确定数据量级对应的硬件规模和带宽需求，并在数据流转链路中设计加密与脱敏机制，确保数据从车端到云端到机房的安全传输与合规存储。该环节中需要关注的技术合规要点如下：

- **网络与专线安全：**专线建设应符合国际网络安全框架要求（如 NIST CSF[4]），采用 VPN（Virtual Private Network，虚拟专用网络）、TLS（Transport Layer Security，传输层安全性协议）等主流加密与认证技术，防止数据被泄漏和滥用。
- **机房安全与访问控制：**确保机房通过物理安全与信息安全评估，部署访问控制、入侵检测及日志留存系统，确保数据在采集、传输与上传环节的可追溯性与完整性。
- **数据加密与脱敏：**在车机端、机房及云端传输链路中使用端到端加密和数据脱敏技术，防止敏感信息暴露，特别是涉及地理位置、驾驶行为及个人数据的场景。

2 数据采集

自动驾驶车辆需采集道路、交通标志、环境、极端天气、行人及特殊场景等多维度数据，为高精地图制作及算法训练提供基础数据。不同自动化级别对数据采集精度和采集规模的要求差异较大，该环节中需要关注的技术合规要点如下：

- **隐私数据保护：**在数据采集端引入边缘计算与本地预处理技术，对车外路人面部、车牌等信息进行实时模糊或脱敏处理，确保在上传数据前最大限度地保护隐私。
- **数据采集设备的安全与合规：**确保传感器设备符合目标国家的无线通信及设备认证要求。同时，摄像头、雷达等采集设备应内嵌安全芯片和防篡改机制，防止数据在采集过程中被篡改或注入恶意代码。
- **数据最小化原则：**采用技术手段限制非必要数据的采集。例如，仅在检测到特定驾驶事件或系统故障时才触发高频数据记录，以降低数据过度采集风险。

3 高精地图制作

对于L3+自动驾驶/Robotaxi（无人驾驶出租车），通常需要依赖高精地图实现自动驾驶功能。高精地图的制作依赖对道路环境和地理空间信息的高精度采集与建模，需结合本地化数据进行道路要素提取、图层构建及更新维护，以用于支持自动驾驶系统的定位和决策。该环节中需要关注的技术合规要点如下：

- **地理信息测绘资质：**不同国家对地图测绘及地理信息采集有不同的监管要求。企业应依法取得测绘或地理信息采集资质或授权。
- **敏感区域与安全控制：**采集内容不得涉及军事设施、政府机构或其他受限制区域，应确保系统具备自动识别与屏蔽功能。
- **数据安全隔离：**确保高精地图的原始采集数据、处理数据和上车数据在存储和传输过程中，与其他通用数据保持物理或逻辑隔离，以满足高安全等级要求。

4 平台搭建

平台搭建是自动驾驶技术研发和运营的核心环节。企业通常需要在出海地区建设或接入多层次的平台体系，包括大数据管理平台、模型训练平台、仿真测试平台及车联网运营平台等，以支撑自动驾驶算法研发、驾驶场景复现以及远程管理和运维。该环节中需要关注的技术合规要点如下：

- **数据平台安全架构：**建立完善的元数据管理及权限管理机制，确保不同业务主体的数据访问边界清晰，防止越权使用或数据滥用。
- **算法与人工智能（AI）合规：**在训练与部署感知、预测和规划算法时，采用可解释性技术，保证算法决策透明可靠，降低因模型偏差引发的安全风险或合规争议。
- **仿真数据管理：**对模拟数据和真实采集数据进行分区存储与管理，确保仿真数据不会与敏感或个人数据混用，防止潜在的数据泄露或隐私违规。
- **车联网安全协议：**平台间通信应遵循国际安全标准设计（如 ISO/SAE 21434、ISO 24089[5]），确保车载系统与后台平台在认证、加密、OTA（Over-the-Air Technology，空中下载技术） 更新等环节的安全性。

5 测试和部署

测试和部署是自动驾驶技术走向实际应用的关键步骤，企业通常在这一环节中开展大规模路测，以验证算法稳定性、感知精度与运营效率，同时部署运营平台以支持车辆远程监控、数据采集与接管功能。该环节中需要关注的技术合规要点如下：

- **测试数据合规采集：**路测数据涉及公共空间时，应遵守当地交通与隐私监管规定，必要时向主管部门备案，以获得路测许可，并采取相应措施确保路测安全。
- **远程接管安全：**对远程控制模块实施多因素身份验证和防劫持机制，确保车辆控制信道安全。同时完整记录远程接管操作，并具备防篡改审计追踪能力。
- **EDR/DDR 数据处理规范：**确保 EDR（事件数据记录器） 或 DDR（驾驶数据记录器）的数据格式、记录时长、存储介质和数据提取接口均符合目标国家的强制性技术标准或行业规范。
- **渗透测试与漏洞管理：**在运营平台和车机系统部署前，由独立第三方进行渗透测试，并建立持续的漏洞披露和管理流程，以满足合规要求。

[4]NIST CSF：美国国家标准与技术研究院（NIST，National Institute of Standards and Technology）开发的网络安全框架（CSF，Cybersecurity Framework），是一套针对网络安全风险管理的自愿性指南，旨在协助组织评估和提升其预防、检测和应对网络安全风险的能力。

[5]ISO 24089：《道路车辆 – 软件更新工程》（Road Vehicles - Software Update Engineering），是一项关于道路车辆软件更新的国际标准。该标准与联合国第 156 号法规保持一致，旨在为车辆及其组件在整个生命周期内的软件更新提供系统化的管理方法，确保软件更新过程的安全性、可靠性和可追溯性。

[6]Corner Case：指在特殊或者极端条件下才会出现的问题或异常，例如车辆在极端天气或者复杂道路场景下触发的未预期行为，帮助确定问题发生的原因，从而有助于改进设计、提升车辆的稳定性和安全性。

6 量产与优化

进入车辆量产阶段后，企业通过车联网和运营平台对车辆进行实时监控与远程维护，持续收集新的 Corner Case[6] 数据，用于模型调优和 OTA 升级，实现自动化驾驶系统的闭环优化。该环节中需要关注的技术合规要点如下：

- **运营监控与应急响应：**部署实时的车联网络安全监控系统，对异常行为（如未经授权的访问、数据泄露尝试、异常通信）进行持续监测、告警和自动化响应。同时建立应急处理流程，确保事件能够快速定位、隔离和修复。
- **模型版本管理：**建立完善的模型库和版本控制系统，记录每次模型更新所用的数据集、训练参数和合规性测试结果，确保每次 OTA 升级都有完整的技术合规链条。
- **软件更新管理（OTA）：**车辆软件更新流程需遵循合规要求，包括软件组件识别、兼容性检查、完整性验证及签名机制。

车联网

车联网作为智能网联汽车的连接核心，通过车辆与车辆、车辆与基础设施、车辆与云平台的互联互通，支撑着远程信息服务、安全更新、远程诊断等关键功能。由于其直接与隐私数据、车辆实时状态及远程控制相关联，出海过程中同样需要针对车联网构建全面的技术合规框架，以保障系统安全、用户权益及业务可持续性。

> 企业可以**从网络与通信建设、车联网系统部署、联调与测试、数据分析应用部署、安全与合规运营、系统韧性与灾备规划**六个环节出发，建立一套可信赖的车联网技术合规体系。

1 网络与通信建设

车联网业务依赖稳定、安全的通信网络，企业通常需要选择合规的 APN（Access Point Name，接入点）物联网服务商、建设专线或跨境专线，确保网络覆盖及带宽满足车辆实时数据传输需求，从而实现数据传输的安全性和在地化合规性。该环节中需要关注的技术合规要点如下：

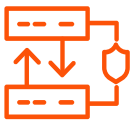
- **服务商资质：**选择运营商或物联网服务商时，应确保其在目标国家或地区具有合法资质，并遵守当地电信、网络安全及数据保护法规。
- **通信安全：**APN 网络、专线及跨境链路应采用国际认可的加密和认证技术，防止数据在传输过程中被窃取或篡改。
- **网络可用性与容灾规划：**网络设计应支持冗余链路和故障切换及灾备机制，确保关键业务在单点故障下仍能保持可用性。

2 车联网系统部署

车联网系统由多个关键组件构成，如 PKI（公钥基础设施）用于身份认证与授权、TSP（远程信息服务平台）提供车联网服务、OTA（空中升级）服务用于软件更新、以及用户端 APP（用户侧移动应用）等，这些组件的部署直接影响到车辆和用户的安全与隐私。该环节中需要关注的技术合规要点如下：

- **身份与证书管理：**PKI 支持车辆、终端及平台的身份认证和授权。证书生命周期管理应符合国际和当地标准，确保数据和通信安全。
- **TSP 安全防护：**TSP 平台需具备防 DDoS 攻击、SQL 注入、XSS 攻击等安全防护能力，并定期进行安全漏洞扫描和渗透测试以保障系统安全。
- **OTA 安全保障：**建立完善的软件更新管理系统。OTA 升级应支持软件完整性校验、数字签名验证及回滚机制，防止恶意更新或非法篡改。
- **APP/云端接口安全：**移动应用（APP）与云端服务接口（API）需遵循国际安全标准进行设计和测试，尤其是涉及身份验证、车辆远程控制和敏感数据访问的接口。
- **系统权限与访问管理：**对所有核心组件采取细粒度访问控制、操作审计和异常行为监测等安全措施，以防止未经授权的内部或外部访问。

3 联调与测试



联调测试是验证车联网系统功能、性能和安全性的关键环节，企业需在实验台架和测试车辆上进行系统联调和功能验证，以确保车联网系统和车辆端、云端平台的交互稳定可靠。该环节中需要关注的技术合规要点如下：

- **测试环境隔离：**联调测试环境与生产环境进行严格的物理或逻辑隔离。测试中产生的真实或仿真数据需加密存储，并遵循最小化数据原则，避免敏感信息泄露。
- **功能与安全机制验证：**联调过程需要覆盖针对关键功能和安全机制的验证，包括用户认证、数据加密、OTA 升级及异常处理、车端与云端交互接口的安全验证，以确保部署后的系统符合安全标准（如 ISO/SAE 21434）。
- **网络安全渗透测试：**在正式发布前对车机系统（TCU/IVI）、TSP 平台及相关移动应用进行独立第三方渗透测试，识别并修复已知漏洞。
- **E-Call[7]/B-Call[8] 功能合规验证：**对紧急呼叫（E-Call）和故障呼叫（B-Call）等生命安全相关功能进行功能性、可靠性和地域性合规测试（如欧盟的 E-Call 规范），以确保在紧急情况下系统可自动触发和准确定位。

[7]E-Call：紧急呼叫系统（Emergency Call），是一项车载紧急通信系统，当车辆发生严重交通事故时，系统会自动或由驾驶员手动向紧急救援中心发出呼叫请求，并传输车辆位置及相关传感器信息等必要事故数据，帮助救援部门快速定位事故现场并及时开展救援。
[8]B-Call：故障呼叫系统（Breakdown Call），是一项非事故道路救援通信服务，当车辆发生机械故障或其他非紧急状况（如电量耗尽、发动机故障、轮胎损坏）时，驾驶员可通过车载系统手动向道路救援服务平台发出呼叫请求，以便救援人员快速提供技术支持或现场救援服务。

4 数据分析应用部署

车联网系统会产生并汇聚车辆运行、能耗、电池健康及售后服务等多类数据，可在数据分析平台上进行处理，用于优化车辆性能、提高用户体验及支持商业分析。企业在部署相关数据分析与可视化平台时，应兼顾数据价值利用与技术合规风险控制。该环节中需要关注的技术合规要点如下：

- **数据分类与最小化：**仅收集必要数据并按敏感度进行分类管理，个人数据和敏感车辆信息需采用脱敏或加密处理。
- **跨系统数据流合规：**确保数据在车端、云平台和应用系统间的传输遵循数据保护法规及跨境数据要求。
- **数据存储与访问控制：**建立完善的权限管理和审计机制，确保只有授权主体才能访问和使用数据，避免滥用或泄露。
- **数据保留与销毁：**对不同类型的数据设置合理的保留期限，并确保数据储存期限到期后得到安全、不可逆的销毁。

5 安全与合规运营

安全与合规运营是车联网系统全生命周期中一个持续的过程，该环节要求企业将最新的法规要求、网络安全标准和行业最佳实践系统性地融入日常技术运维流程，确保车联网系统的常态化技术合规。该环节中需要关注的技术合规要点如下：

- **信息安全管理：**建立覆盖车端、云端及应用端的安全运营体系，持续开展威胁检测、漏洞修复与安全事件响应。相关措施应符合 UN R155/R156、ISO/SAE 21434 等国际标准要求，确保系统在防护、检测、响应和恢复各环节的合规性。
- **第三方技术合规管理：**对参与车联网生态的第三方数据处理者（如云服务商、软件供应商、车联网服务提供商）实施合规评估与管理，确保其在合同、数据处理和技术安全方面完全遵守目标国家/地区的法律法规及技术标准。
- **安全审计与合规报告：**构建系统化的安全与合规审计机制，定期记录并留存关键操作日志、安全事件处置记录和系统变更信息，形成可追溯的技术合规档案，以支撑监管检查和内部审计。

6 系统韧性与灾备规划

车联网的高互联性和高实时性特征决定了企业必须具备完善且强大的系统韧性与灾备能力，以应对网络中断、设备故障或恶意攻击等突发事件，确保关键业务的连续性。该环节中需要关注的技术合规要点如下：

- **跨区域冗余与高可用性设计：**核心系统（如 TSP、OTA）应在不同的地理区域部署异地冗余节点，采用负载均衡和自动故障转移机制，确保在一个区域发生灾难性故障时，服务能够自动切换，实现业务连续性。
- **数据备份与恢复能力验证：**制定明确的恢复时间目标和恢复点目标，并定期通过模拟演练验证灾难恢复流程，确保关键业务数据能够在最短时间内恢复。
- **数据主权与灾备地点合规：**灾备数据的存储与传输应符合目标国家或地区的数据主权及跨境传输监管要求。在数据本地化监管严格的市场，应将灾备中心设置在境内或采用合规的跨境传输机制。

针对**自动驾驶**和**车联网**两大核心技术领域的合规体系构建要素分析，确立了智能网联汽车出海应遵循的安全与合规内生化原则。然而，全球化合规框架的最终落地，必须与具体海外市场的地域性、文化性及法律监管环境深度融合。中国汽车企业在将全球技术框架落地中东和拉美市场之前，需要超越通用标准，深入了解目标区域的市场潜力、产业特点、政策导向以及特有的技术合规以及隐私保护监管要求。这种结合区域市场洞察以及监管环境分析的双向策略，是实现高效、低风险国际化运营的关键。因此，本报告将深入剖析中东和拉美两大战略市场的具体情况，为企业出海合规提供更具针对性的背景参考。

02

中东与拉美地区
智能网联汽车合规要点

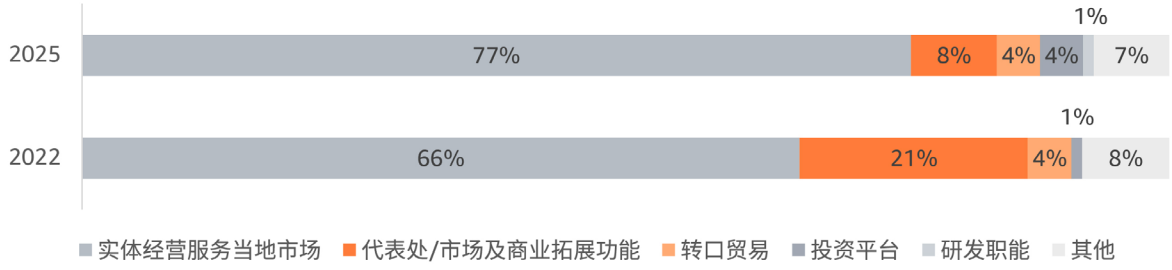
中东篇

1 市场洞察

1.1 智能网联汽车市场机遇

长期以来，中东一直是全球航运和贸易的重要枢纽，也是中国“一带一路”倡议框架下互联互通的战略桥梁。中国与中东地区的关系不断深化，背后既有经济层面的契合，也有外交层面的推动。在中东的主要国家中，中国已与阿联酋、沙特阿拉伯、巴林等国家建立全面战略伙伴关系，同时与卡塔尔、阿曼、科威特等国家建立战略伙伴关系。

在信心提升、经济回报吸引及政策支持转向的推动下，中国企业正将目光更多地投向中东市场。普华永道于2025 年 9 月发布了《中资企业信心提升，稳健深耕中东市场》研究报告，通过向 136 家在中东地区开展业务的中资企业发放问卷，围绕中东经济多元化转型加速的背景，调研企业在当地的发展现状、面临的机遇和挑战以及未来的商业规划。其中针对受访企业在中东地区经营模式的调研结果显示，2025 年 77%的受访企业以实体经营的形式服务当地市场，较 2022 年提高了 11 个百分点；仅设立代表处的比例则由 2022 年的 21%下降至 2025 年的 8%。这一经营模式的转变，反映出中资企业对中东市场的信心持续增强，业务布局已从初期的探索阶段向拓展阶段迈进。整体来看，中东市场对于中资企业而言，已不再是边缘性市场，而正逐步发展为具有战略意义的增长枢纽。



图表 1：受访中资企业在中东市场的主要业务定位

1.2 智能网联汽车市场概况

在全球人工智能、气候变化、贸易格局和能源结构重塑的大背景下，中东地区正积极推进能源转型，并通过国家战略投资和发展基金大力支持新能源汽车产业的发展，以吸引更多高品质新能源汽车企业前来投资兴业。然而该地区整体电动化程度尚未完全成熟，较欧美国家尚存在一定差距。

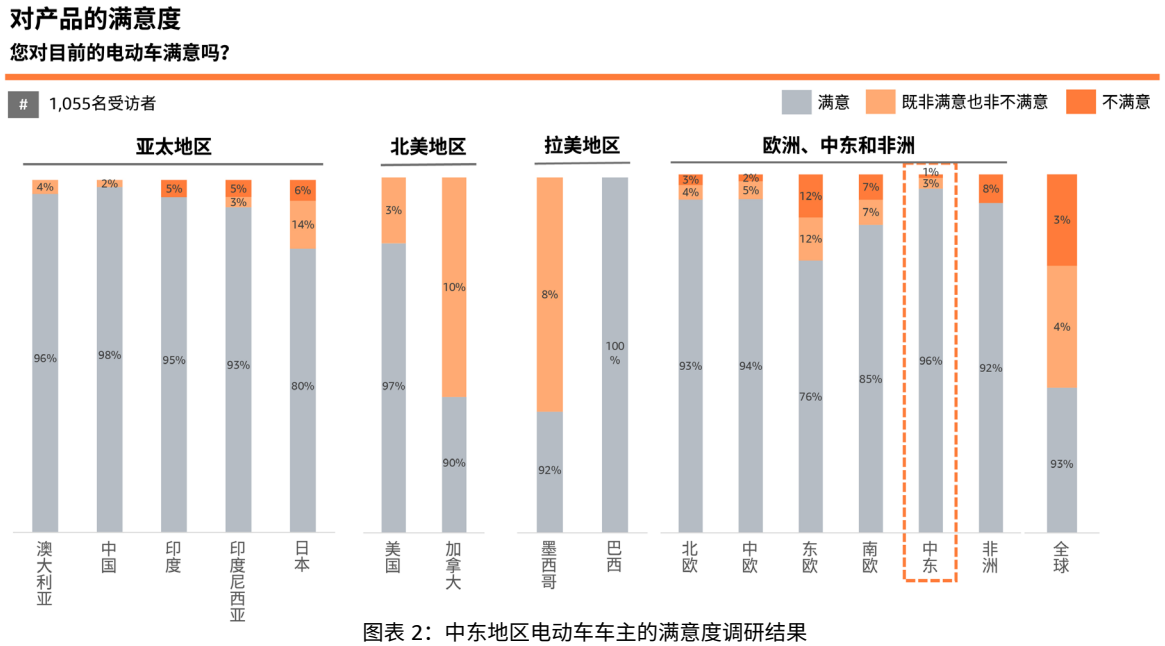
根据中国汽车工业协会整理的海关总署数据，2025 年 1 到 6 月，中国汽车出口总量达到 **308.3 万辆**，同比增长 **10.4%**。

> 其中，传统燃料汽车出口 **202.3 万辆**，同比**下降 7.5%**

> 新能源汽车出口 **106 万辆**，同比**增长 75.2%**，显示出强劲的增长势头

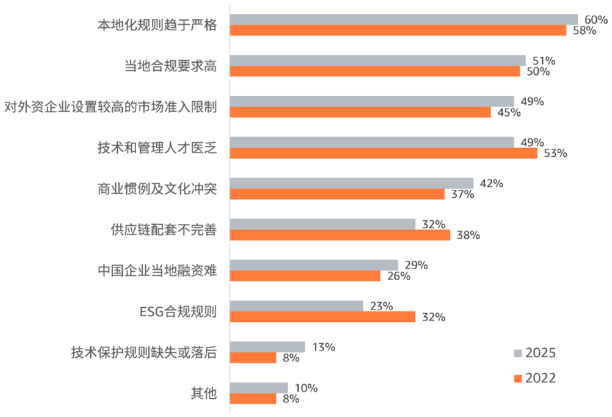
此外，全国乘用车市场信息联席会秘书长崔东树在“2025 中国汽车论坛”上指出[9]，中国汽车出口结构正在发生变化，出口重点正逐步转向中南美洲和中东市场，对阿联酋和沙特阿拉伯等国的出口显著增长，其中 2025 年上半年，在中国汽车出口累计量排名前十的国家中，阿联酋和沙特分别以 189,547 辆和 119,564 辆位居第二和第七；在出口增量方面，阿联酋表现尤为突出，以 **74,046 辆**的增量位居首位，成为中国汽车出口增长的主要贡献国。

普华永道发布的《2024 汽车电动化报告》中显示，中东国家的电动车车主对电动车的满意度高达 **96%**，明显高于全球平均满意度 93%。随着政策的进一步实施和市场的逐步开放，中东有望成为全球新能源汽车产业的重要增长点，为中国企业提供了广阔的市场机遇和合作空间。



图表 2：中东地区电动车车主的满意度调研结果

尽管中东智能网联汽车市场不断扩大，企业在监管政策方面仍需保持关注。普华永道《中资企业信心提升，稳健深耕中东市场》报告中表明，受访企业对监管政策的明确性与稳定性仍有担忧。在这种情形下，智能网联汽车企业应密切关注中东地区相关监管政策的最新动态，以便及时调整策略，确保业务的合规性和可持续发展。



图表 3：中资企业在投资过程和投后管理面临的主要挑战

[9]中国汽车上半年出口超 300 万辆，行业呼吁加强创新有序出海，https://www.yicai.com/news/102727502.html

2 合规洞察

2.1 智能网联技术监管

当前海湾六国尚未成为 WP.29[10] 任何协定书的缔约方。这表明在这些国家，WP.29 所制定的规则（如 R155 和 R156 法规）尚未被整合进国家级的法规体系中。然而，随着智能网联汽车技术的快速发展，中东各国正在逐步完善针对智能网联汽车的技术监管框架，旨在为智能网联汽车在当地市场的落地提供基础规范指引。以下是海湾六国在物联网、自动驾驶以及人工智能领域的主要监管政策：

国家	物联网	自动驾驶	人工智能
沙特阿拉伯	- 《物联网法规》，物联网设备必须获得通信、空间和技术委员会（CST）的批准并获得合格证书 - 车载紧急呼叫（eCall）技术要求规定	- 《沙特道路法规》引入了自动驾驶车辆的相关标准	
阿联酋	- 《物联网监管条例》，物联网数据类别分为机密、敏感、秘密、公开 4 级，高风险数据（机密&敏感&秘密）原则上须存储于阿联酋境内，除非满足特定充分性要求 - 车载紧急呼叫（eCall）技术要求规定	- 《2023 年迪拜酋长国自动驾驶车辆运营监管法》，适用于 L4+自动驾驶汽车及 Robotaxi	- 《智慧迪拜：人工智能伦理原则与指南》
卡塔尔	- 物联网设备必须获得通信监管局（CRA）的批准		
科威特	- 无线通信产品必须通过通信和信息技术管理局（CITRA）的批准并获得合格证书		
巴林	- 无线通信产品必须通过电信管理局（TRA）的批准并获得合格证书		
阿曼	- 无线通信产品必须通过电信管理局（TRA）的批准并获得合格证书		- 《人工智能系统安全和道德使用总体政策》对 AI 技术的开发与应用提出具体要求

来源：普华永道分析整理

[10]WP.29 即世界车辆法规协调论坛，是联合国欧洲经济委员会下为开展全球汽车技术法规协调和统一工作的国际组织。

物联网领域

智能网联汽车作为关键物联网终端，其对高精地图、传感器数据及云端平台的依赖，使得各国监管机构高度关注网络安全和数据安全问题。

- 阿联酋通信和数字监管机构发布的《物联网监管条例》对数据本地化提出了明确的要求，规定机密、敏感和秘密级别的数据原则上应优先存储在本地；
- 沙特通信、空间和技术委员会出台的《物联网法规》要求，智能网联汽车中装载的 T-Box 模块需作为物联网设备获取相关认证；
- 卡塔尔通信监管局则通过《IoT 与 M2M 服务政策文件》明确了物联网设备的审批及数据路由规定。

车联网领域

车辆通信安全、OTA 升级、数据完整性及跨境数据流转均是技术监管核心。

- 阿联酋和沙特参照欧盟标准发布了车载紧急呼叫（eCall）技术要求规定，对系统定位精度、抗冲击能力、系统自检以及隐私保护等提出明确要求，强化了车联网系统的安全和隐私保障；
- 相比之下，巴林和科威特尚未出台专门的车联网监管法规，但建议企业遵循一般信息安全和通信监管政策。

人工智能领域

阿曼交通、通信和信息技术部出台的《人工智能系统安全和道德使用总体政策》要求企业在开发和部署 AI 系统过程中，建立系统化的治理机制，包括开展定期风险评估、记录决策过程，并按监管机构要求提交合规报告。这一政策明确了 AI 在安全性与伦理层面的监管边界，为智能网联汽车中人工智能算法的安全应用提供了制度保障。

总体来看，尽管海湾六国在智能网联汽车技术监管框架建设方面起步较晚，尚未全面引入统一的技术法规，但在物联网、车联网及人工智能领域的监管正快速向国际标准接轨，并逐步结合本地产业政策与社会治理需求形成具有操作性的监管框架。企业在进入中东市场时，应提前规划技术架构设计与数据流转路径，建立完善的功能安全与网络安全控制机制，同时密切关注政策动态与监管趋势，确保系统在安全、合规、可持续的基础上实现本地化落地。

2.2 隐私保护合规

在中东地区，各个国家在隐私保护领域的立法进展显著，以适应数字化经济和智能网联汽车发展带来的隐私合规风险。阿联酋、沙特、阿曼、巴林、卡塔尔等国均已颁布或修订国家级的个人数据保护法律，建立起区域内较为系统的合规框架。总体来看，这些立法在理念和结构上多借鉴欧盟 GDPR（通用数据保护条例）的核心原则，以下是海湾六国以欧盟 GDPR 为基准的隐私保护合规差异图：

序号	合规领域		基准（欧盟GDPR）	沙特	阿联酋	阿曼	巴林	卡塔尔	科威特
1	隐私数据收集同意告知	个人同意	-						
2		数据采集	-			N/A		N/A	N/A
3		告知	-						
4		敏感个人信息处理	N/A		N/A				N/A
5		特殊主体保护（包括未成年人）	-			未明确年龄	N/A	未明确年龄	
6		个人数据的准确性	-			N/A	N/A	N/A	N/A
7		数据披露	N/A		N/A		N/A	N/A	
8		合法性基础	-		N/A	N/A	N/A	N/A	
9		数据处理/保护原则	-		N/A	N/A			N/A
10	数据主体权利行使机制	访问权	-				N/A		
11		复制权	N/A		N/A	N/A	N/A	N/A	N/A
12		反对权	-	N/A	N/A	N/A		N/A	N/A
13		知情权	N/A	N/A	N/A	N/A		N/A	N/A
14		数据可携带权	-	N/A			N/A	N/A	N/A
15		更正权	-	N/A					

序号	合规领域		基准（欧盟GDPR）	沙特	阿联酋	阿曼	巴林	卡塔尔	科威特
16	数据主体权利行使机制	删除权（“被遗忘权”）	-	N/A					
17		限制处理权	-			N/A		N/A	
18		撤回同意权	-		N/A		N/A		
19		停止处理权	N/A			N/A	N/A	N/A	N/A
20		不受自动化处理决策限制的权利	-			N/A	N/A	N/A	N/A
21		数据主体权利响应	-		N/A			N/A	
22	隐私保护默认和设计管理机制	隐私影响评估	-			N/A	N/A	N/A	
23		数据处理活动记录	-				N/A	N/A	
24		个人数据保护	-						
25		个人数据留存	-				N/A		
26		数据泄露通知	-						
27		隐私保护设计机制（PbD）	-	N/A	N/A	N/A	N/A	N/A	N/A
28	隐私数据跨境传输机制	跨境传输	-						N/A
29	第三方供应商安全管理机制	第三方管理	-						

序号	合规领域		基准（欧盟GDPR）	沙特	阿联酋	阿曼	巴林	卡塔尔	科威特
30	其他	数据保护官	-						N/A
31		审计	-		N/A		N/A		
32		直接营销	N/A				N/A		N/A
33		监管机构通知	N/A	N/A	N/A	N/A		N/A	
34		获取监管机构授权/登记/注册	N/A	N/A	N/A	N/A		N/A	N/A
35		保密义务	-	N/A	N/A	N/A		N/A	N/A
36		人员培训	N/A	N/A	N/A	N/A	N/A		
37		系统开发	N/A	N/A	N/A	N/A	N/A		N/A

来源：普华永道分析整理

注：高亮色块表示此领域较欧盟 GDPR 存在显著差异；N/A 表示此领域暂未有明确监管要求。

- 从**监管趋势**来看，中东各国普遍正朝着“**细化指引**、**强化执法**、**提升透明度**”的方向发展。
- 在**监管机构**层面，各国均已建立或指定了隐私合规监管机构，如沙特的数据与人工智能管理局（SDAIA）、阿曼的交通、通信和信息技术部（MTCIT）以及卡塔尔的合规与数据保护部门（CDP），以协助统筹隐私保护政策制定与监管执法。
- 在**监管立法**方面，中东各国隐私合规监管的核心多聚焦于个人数据处理告知和授权、敏感个人数据保护、数据跨境合规保障机制、数据保护影响评估以及个人数据安全事件应对等领域，在立法中明确了相关要求且各国呈现出监管差异。例如，
  - 阿联酋和沙特均设立了严格的跨境数据转移条件，强调企业需确保接收国具备与本国等同的隐私保护水平或者满足特定豁免要求；
  - 阿曼要求企业在处理敏感个人数据前需获得主管部门批准，并通过外部审计制度强化合规责任；
  - 卡塔尔规定，对以直接营销为目的的个人数据收集，需确保获取数据主体明确同意并为其提供便捷的退出机制。

此外，中东地区的隐私监管正在与智能网联汽车、物联网终端及人工智能应用深度融合。

智能网联汽车所涉及的高精地图、车联网数据、AI 算法等，均可能纳入隐私保护监管框架的适用范围。例如，

- 卡塔尔在其 PDPL（个人数据保护法）的监管指南中引入了“隐私默认设计”和“数据保护影响评估”等机制，推动企业在车联网系统开发和运营中嵌入隐私合规控制；
- 除了《个人数据保护法》，阿联酋还发布了《物联网监管条例》，对特定数据的本地存储提出了明确要求。

总体而言，中东地区的隐私合规监管体系正从“立法建设”向更加细致和严格的方向过渡。未来趋势可能包括进一步统一监管标准以及细化合规要求，并通过强化国际合作与数据跨境审查机制，构建兼顾安全、合规与创新的数据治理生态。对于计划进入中东市场的智能网联汽车企业而言，需结合各地不同的隐私保护要求以及执法重点，建立针对性的合规体系，并在设计、开发、运营等业务中落实隐私保护原则，以确保在动态发展的监管环境中实现合规落地与业务的可持续性。

拉美篇

1 市场洞察

1.1 智能网联汽车市场机遇

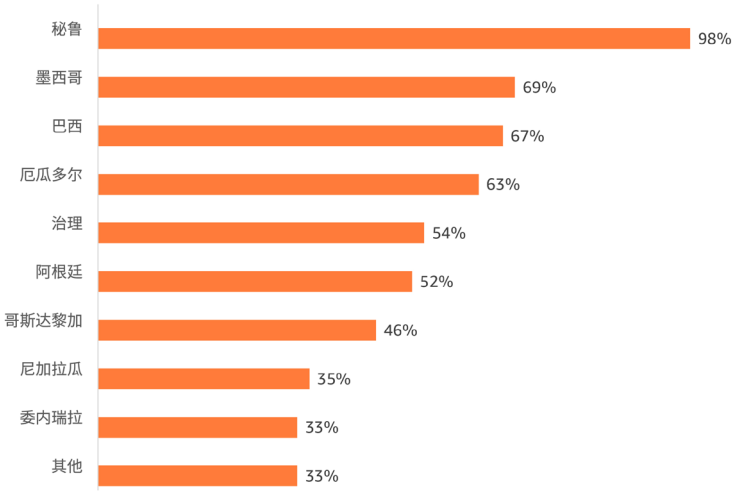
拉丁美洲是“21世纪海上丝绸之路”的自然延伸，是共建“一带一路”倡议的重要参与方。中国与拉美地区双边贸易连续七年保持高速增长。中国是拉美第二大贸易伙伴，也是巴西、智利、秘鲁等国家的第一大贸易伙伴。

> 2024 年，中国对拉丁美洲直接投资流量达到 **155.6 亿**美元，同比增长 **15.4%**，占总量的 **8.1%**，这使得拉美成为除东盟外中国第二大投资区域。

> 截至 2024 年，中国在拉美直接投资存量超过 **6,000 亿**美元，占中国对外直接投资总存量的 **20%**。

拉美作为新兴市场的重要增长极，是中国汽车产业推进“**技术与生态出海**”战略的关键布局区域，也是中拉经贸合作升级的核心载体。中国已与智利、哥伦比亚等多个拉美国家建立全面战略伙伴关系。随着中智自贸协定升级、中哥自贸协定等一系列制度性安排的逐步落地，根据商务部相关解读，智利与哥伦比亚将逐步削减甚至取消对中国生产的汽车及零部件等大多数产品的关税。例如中智自贸协定升级后，中国新能源汽车进入智利可享受零关税待遇；中哥自贸协定也明确将汽车及零部件纳入关税减免清单。这些安排不仅提升了贸易便利化水平，也为双方深化合作夯实了基础。

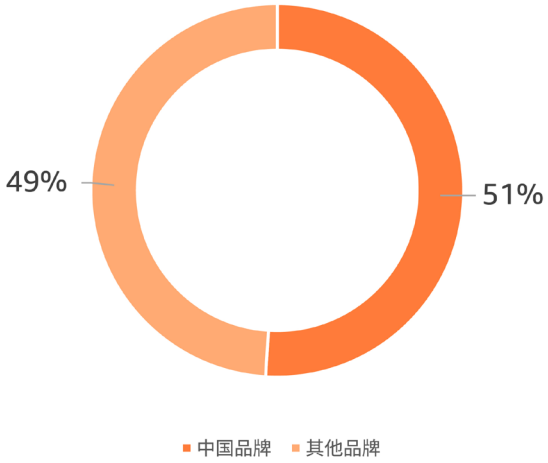
普华永道于 2025 年 11 月发布了《中国企业在拉美投资调研》报告，通过对 48 家在拉美地区开展业务的中资企业发放问卷，洞察企业在当地的发展现状、面临的机遇和挑战以及未来的商业规划。调研结果显示，哥伦比亚、秘鲁、墨西哥和巴西已成为中资企业的重点投资地，其广阔的市场前景和较高的经济增速持续吸引中国投资者扩大现有产品和服务的市场，绝大多数企业已入驻三年以上，深耕十年以上的企业超过三成；约半数受访企业对在拉美的投资表示满意，超半数企业实现盈利，近六成企业计划在未来三年内进一步追加投资，展现出对拉美市场长期发展的坚定信心。



图表 4：中资企业在拉美经营或拓展市场的分布情况

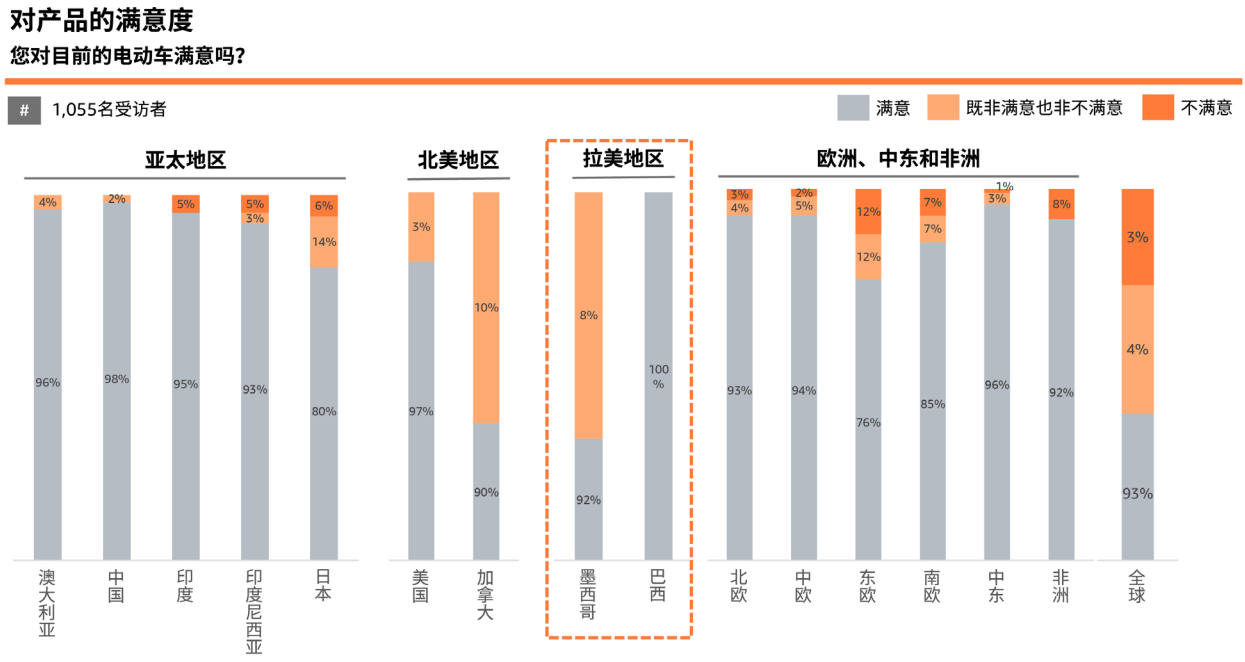
1.2 智能网联汽车市场概况

拉丁美洲汽车经销商协会最新发布的数据显示，2024 年拉美地区的新能源汽车销量达到 412,493 辆，在销售的新车中，有 51%来自中国品牌，其中巴西、墨西哥已成为核心市场与生产枢纽。据巴西电动汽车协会统计，巴西作为拉美最大汽车市场，2024 年新能源汽车销量达到 12.5 万台，其中比亚迪占据了 61.2%的市场份额，其次是长城汽车和沃尔沃。在墨西哥，中国新能源汽车出口促进了当地新能源汽车行业的发展，据中汽协统计，2024 年墨西哥成为中国新能源汽车出口总量的第六大目的国，出口总量为 80,552 辆。随着智能网联技术加速渗透，拉美正从边缘市场升级为中国车企全球化的战略增长枢纽。



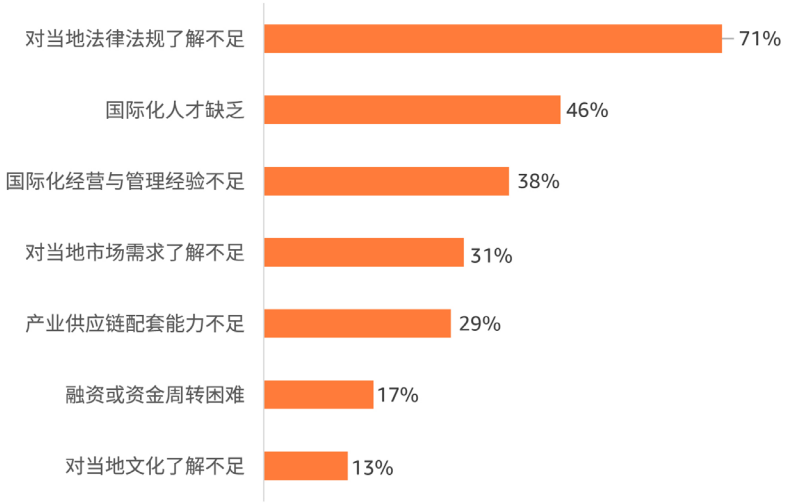
图表 5：拉美新能源汽车销量中国品牌占比（2024 年）

在全球汽车产业向电动化、智能化转型以及各国对可持续交通需求持续提升的背景下，拉美地区凭借消费者对新能源汽车的高度认可，正逐渐成为智能网联汽车产业发展的新兴市场。普华永道《2024 汽车电动化报告》显示，在拉美地区，墨西哥和巴西的电动车车主对电动车的满意度分别高达 **92%** 和 **100%**，且该地区消费者普遍对电动车和可持续交通持积极态度，这为智能网联汽车在当地市场的进一步渗透奠定了坚实的用户基础。



图表 6：拉美电动车车主的满意度调研结果

当前，拉美地区各国在车联网技术监管层面存在差异化要求，企业在市场布局过程中需重点关注合规风险。普华永道《中国企业在拉美投资调研》报告中表明，企业在拉美经营面临的最大挑战是对当地法律法规了解不足。



图表7：投资中后期经营管理中面临的主要困难和挑战

在此情况下，智能网联汽车企业应密切关注拉美各国监管政策的具体要求与最新动态，结合自身业务特点制定相应的合规策略，以确保在把握市场机遇的同时，实现合规运营与可持续发展。

2 合规洞察

2.1 智能网联技术监管

当前拉美国家尚未成为 WP.29 任何协定书的缔约方。这表明在这些国家，WP.29 所制定的规则（如 R155 和 R156 法规）尚未被整合进国家级的法规体系中。然而，拉美各国当前也在逐步构建和完善适应本地市场的技术监管框架，呈现出向国际标准接轨、以风险为导向的总体趋势。以下是拉美重点国家在物联网、自动驾驶以及人工智能的主要监管政策：

国家	物联网	自动驾驶	人工智能
巴西	- 无线通信产品必须通过国家电信局（ANATEL）的批准并获得合格证书		-《人工智能法案（暂未生效）》
墨西哥	- 物联网设备必须通过联邦电信研究院（IFETEL）的批准并获得合格证书		- 《人工智能法（草案）》，旨在建立 AI 技术的监管框架，涵盖包括智能网联汽车在内的高风险人工智能系统
阿根廷	- 无线通信产品必须通过通信局（ENACOM）的批准并获得合格证书	- 《交通法》新增对自动驾驶车辆的相关规定，包括自动驾驶车辆的定义、分级标准以及认证要求	- 《公共和私营实体关于负责任 AI 透明度和个人数据保护指南》，为公共和私营机构在应用人工智能时提供合规参考
智利	- 无线通信产品必须通过电信副秘书处（SUBTEL）的批准并获得合格证书		- 《人工智能系统规制法案（草案）》拟对人工智能系统建立分级监管机制，其中包括自动驾驶与车联网相关的高风险应用
哥伦比亚	- 无线通信产品必须通过通信监管委员会（CRC）的批准并获得合格证书		- 《人工智能伦理框架》，提出人工智能伦理原则
秘鲁	- 无线通信产品必须通过交通与通信部（MTC）的批准并获得合格证书		- 《促进人工智能使用有利于国家经济和社会发展的法律》及其实施条例，建立了基于风险的人工智能监管原则，设立了不同风险类别，并规定了透明度要求、人工监督义务以及数据治理机制等

来源：普华永道分析整理

物联网领域

巴西和墨西哥已建立针对智能设备和通信系统的网络安全与数据保护要求。

- 巴西国家电信局发布的《第 77 号法案电信设备网络安全要求》，明确了针对电信设备的网络安全要求以及对电信设备供应商的要求。
- 墨西哥联邦电信研究院则出台了《物联网（IoT）设备网络安全最佳实践准则》，为物联网设备的网络安全提供了实践指引。
- 智利和阿根廷也在其网络安全战略中将包括物联网（IoT）在内的新兴技术纳入风险视野，并提出加强关键基础设施网络安全的监管方向。

自动驾驶领域

阿根廷通过修订《交通法》明确了自动驾驶车辆的定义、分级标准以及强制认证要求。巴西和智利也正逐步推进自动驾驶监管框架建设。

- 其中巴西正在讨论相关立法草案，计划通过修订其交通法来启动自动驾驶汽车测试和行驶的监管工作，建立道路测试许可与测试报告制度，规范自动驾驶车辆在公共道路上的测试。
- 智利也开始探索制定相应的监管机制和安全评估要求。

总体趋势表明，拉美国家正逐步将自动驾驶监管纳入交通安全和技术创新双重框架中，兼顾发展与风险防控。

人工智能监管

是拉美国家政策创新中最为活跃的领域。

- 巴西的《人工智能法案》已通过参议院审议，确立了人工智能系统风险分级监管、数据安全与用户权利保护、以及算法透明度与可解释性等核心要求，为 AI 驱动车联网和自动驾驶系统提供了合规依据。
- 阿根廷公共信息获取机构发布了《公共和私营实体关于负责任 AI 透明度和个人数据保护指南》，强调了企业在 AI 全生命周期中应该考虑的安全要素，包括组建跨学科团队、开展影响评估、采取充分的安全与合规措施等。
- 智利也建立了《人工智能系统规制法案（草案）》，拟建立 AI 分级监管体系。
- 秘鲁作为拉美地区首个建立 AI 通用监管框架的国家，通过其法案及实施条例，提出了多项针对 AI 风险的合规义务，为 AI 算法在智能驾驶领域的安全应用提供了制度基础。

总体来看，拉美地区的智能网联技术监管体系正从分散的行业规范向系统化法规框架演进。各国普遍重视网络安全、数据保护和 AI 伦理责任，逐步将智能网联汽车纳入国家数字化与交通创新战略之中。企业在进入拉美市场时，应在架构设计阶段融入“**合规嵌入式**”理念，确保通信安全、功能安全与算法合规同步推进，从而在复杂多元的监管环境中实现可持续的市场落地。

2.2 隐私保护合规

拉美各国在政治背景、国情以及经济结构等方面存在差异，个人数据保护的立法进程正处于快速发展以及日趋层次分明的阶段，并在不同国家呈现出显著多样性。部分国家已经建立起相对健全的隐私保护法律体系，设立了独立监管机构并具备一定执法能力。相较之下，部分国家的隐私保护立法仍处于发展或完善阶段，监管机构或尚未成立，或在职能和资源方面相对有限。以下是拉美重点国家以欧盟 GDPR 为基准的隐私保护合规差异图：

序号	合规域		基准（欧盟GDPR）	巴西	墨西哥	阿根廷	智利	哥伦比亚	秘鲁
1	隐私数据收集同意告知	个人同意	-						
2		数据采集	-	N/A		N/A			N/A
3		告知	-						
4		敏感个人信息处理	N/A						
5		特殊主体保护（包括未成年人）	-		N/A	N/A			
6		个人数据的准确性	-	N/A				N/A	N/A
7		数据披露	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8		合法性基础	-		N/A	N/A		N/A	N/A
9		数据处理/保护原则	-			N/A			
10	数据主体权利行使机制	访问权	-						
11		复制权	N/A		N/A	N/A	N/A	N/A	N/A
12		反对权	-			N/A		N/A	

序号	合规域		基准（欧盟GDPR）	巴西	墨西哥	阿根廷	智利	哥伦比亚	秘鲁
13	数据主体权利行使机制	知情权	N/A	N/A	N/A		N/A		
14		数据可携带权	-		N/A	N/A		N/A	N/A
15		更正权	-						
16		删除权（“被遗忘权”）	-					N/A	
17		限制处理权	-		N/A	N/A	N/A	N/A	N/A
18		撤回同意权	-				N/A		
19		停止处理权	N/A	N/A	N/A	N/A	N/A	N/A	N/A
20		不受自动化处理决策限制的权利	-	N/A	N/A	N/A	N/A	N/A	N/A
21		数据主体权利响应	-						
22	隐私保护默认和设计管理机制	隐私影响评估	-		N/A	N/A		N/A	N/A
23		数据处理活动记录	-		N/A	N/A	N/A	N/A	N/A
24		个人数据保护	-						
25		个人数据留存	-		N/A		N/A		
26		数据泄露通知	-			N/A		N/A	N/A
27		隐私保护设计机制（PbD）	-	N/A	N/A	N/A		N/A	N/A
28	隐私数据跨境传输机制	跨境传输	-						
29	第三方供应商安全管理机制	第三方管理	-		N/A				N/A

序号	合规域		基准（欧盟GDPR）	巴西	墨西哥	阿根廷	智利	哥伦比亚	秘鲁
30	其他	数据保护官	-			N/A	N/A	N/A	N/A
31		审计	-	N/A	N/A	N/A	N/A	N/A	N/A
32		直接营销	N/A	N/A	N/A	N/A	N/A	N/A	N/A
33		监管机构通知	N/A	N/A	N/A	N/A	N/A	N/A	N/A
34		获取监管机构授权/登记/注册	N/A	N/A	N/A		N/A		
35		保密义务	-	N/A				N/A	
36		人员培训	N/A	N/A	N/A	N/A	N/A	N/A	N/A
37		系统开发	N/A	N/A	N/A	N/A	N/A	N/A	N/A

来源：普华永道分析整理

注：高亮色块表示此领域较欧盟 GDPR 存在显著差异；N/A 表示此领域暂未有明确监管要求。

拉美地区的隐私保护立法核心原则与全球主流趋势一致，包括数据处理的合法性、公平性与透明性，数据主体权利响应，敏感个人数据的特殊保护，以及对数据跨境传输的限制与保障机制，并在各国呈现出明显的分层特征。巴西作为区域内经济体量最大的国家，已经建立起成熟且严格的隐私保护法律框架。墨西哥和智利等国则通过全面修法，将早期框架过渡至更严格的新法，显示出监管升级的整体方向。多数国家已设立或明确指定了专门的监管机构:

巴西数据保护局（ANPD） | **墨西哥反腐败与良好治理部（MAGG）** | **哥伦比亚工业和商业监管局（SIC）** | **智利拟设立个人数据保护局（PDPA）**

这些机构正逐步细化实施细则并增强执法能力。

在具体合规领域，拉美不同国家的立法要求存在差异。例如，**数据跨境传输方面**，尽管各国普遍要求接收国应具备“同等个人数据保护水平”或采取适当保护措施（如标准合同条款 SCCs），哥伦比亚却更加依赖官方“白名单”，目的地不在名单内则需满足严格例外情形。

对于数据保护影响评估（DPIA），整体趋势也由“推荐”向“强制”或“监管有权要求”转变：

- 巴西 LGPD（通用个人数据保护法）虽未强制要求开展，但其监管机构有权要求企业执行；
- 智利 NDPL（个人数据保护法）则正在推进对特定高风险场景开展 DPIA 的强化要求。

对于敏感个人数据的保护方面，各国普遍采取了严格的监管措施：

- 阿根廷 PDPA（个人数据保护法）强调敏感数据的收集与处理需合法且符合公共利益，并禁止强制要求提供。

对于数据处理记录，各国也存在不同的要求：

- 巴西 LGPD 强调企业需妥善记录处理活动；
- 秘鲁则要求所有包含个人数据的数据库都应在国家平台 SIPDP （个人数据保护综合系统）上进行登记；
- 阿根廷同样要求数据库注册。

对于智能网联汽车企业，由于涉及大规模个人和敏感数据处理，在拉美地区的合规挑战较为突出。例如，

- 车联网系统采集的位置、驾驶行为甚至生物识别数据可能被认定为大规模或敏感数据，从而触发巴西、智利等国对 DPIA 的要求。因此，企业应将“隐私默认设计”和 DPIA 嵌入系统开发和运营初期。
- 出海运营涉及的数据跨境传输复杂性也会给企业带来合规压力，企业应基于各国认可的不同合规传输机制采取相应措施以进行应对。
- 此外，特定国家的本土化合规要求也需要重点关注，例如智利 NDPL 引入“违规预防模型”，鼓励企业自愿建立合规项目，其可以帮助企业在潜在违规判定中减轻责任。

总结而言，拉美地区隐私合规体系正从多样化并存向标准趋同、执法细化方向发展。未来趋势可能包括立法全面升级与更加严格的执法落地，针对自动驾驶、车联网、人工智能等特定数据处理场景的细化指引也将进一步完善，以平衡技术创新与隐私保护。同时，区域性合规框架建设和跨国协调合作也将成为趋势。计划在拉美市场进一步发展的智能网联汽车企业，建议建立兼顾各国差异化要求的动态合规体系，在设计、开发、运营各环节落实隐私保护要求，实现合规有效落地。

07

中国汽车企业布局海外市场的合规策略建议

鉴于中东和拉美等新兴市场的多元化特性，中国汽车企业在加速全球化布局的过程中，亟需将合规管理内嵌于企业核心战略。

本章将围绕**区域节点部署**、**车联网运营**，以及**关键合作伙伴**评估三大核心维度，深入剖析企业在海外拓展中必须考量的合规策略与体系构建要素，以期保障出海业务的长期稳健发展与可持续竞争力。

01 区域节点部署 » 02 车联网运营 » 03 关键合作伙伴

1 中东及拉美地区的数据中心节点部署合规

在中东与拉美地区布局智能网联汽车业务时，当地的**数据主权**、**数据本地化要求**以及**跨境传输限制**是企业在设计数据处理和存储架构时需要优先解决的核心问题，以确保架构设计符合各国法律规定和业务合规需求。近年来，中东主要国家（如阿联酋、卡塔尔）以及拉美核心市场（如巴西、墨西哥）均陆续出台了隐私保护法律法规，对数据存储位置及跨境流转提出了更加明确的要求。

中东地区

目前仅有阿联酋在其合规监管框架对车联网数据的本地化存储提出了明确且严格的要求，但这种数据本地化的监管趋势近年来正逐渐在整个中东地区蔓延。

- 具体而言，阿联酋电信和数字政府监管机构（TDRA）发布的《物联网监管条例》明确规定，公开数据可以存储在阿联酋境内或境外；涉及个人或企业的“机密”、“敏感”、“秘密”级别数据则原则上必须存储于阿联酋境内，除非满足特定充分性要求。

- 相较之下，沙特并未在其 PDPL（个人数据保护法）及配套的数据跨境传输条例中提出具体的本地化要求，而是主要聚焦于跨境传输的合规保障机制。然而在实际执行层面，沙特对关键业务数据及大规模个人数据的本地化要求呈现出强化趋势。尽管尚未直接针对车联网场景，但在实践中，仍建议智能网联汽车企业优先选择在沙特境内进行数据存储与处理，以降低监管合规风险。

- 其他中东国家（如卡塔尔、巴林和阿曼）目前尚未出台针对车联网或物联网数据的专门本地化要求，其隐私保护法规普遍侧重于数据跨境传输的审批或许可机制以及相应的数据保护要求。鉴于智能网联汽车行业涉及高敏感数据，监管部门已逐步表现出对数据主权和本地化解决方案的高度关注，并可能在未来通过行业细则或监管实践进行落实。

拉美地区

数据保护与跨境传输监管框架近年来也在快速发展，各国的隐私合规监管体系虽整体参考欧盟GDPR，但在数据本地化及跨境流转要求上存在差异，且在逐步强化对数据跨境传输合规与数据主权的管控。

- 巴西作为拉美地区隐私监管体系最为成熟的国家之一，其 LGPD 虽未强制要求数据本地化存储，但对涉及大规模或高敏感度个人数据的场景，监管机构在实践中倾向于引导企业优先进行本地化部署，以保障监管可控性。
- 墨西哥同样主要侧重于规范数据跨境传输合规机制，但在物联网领域，当地监管机构建议企业严格开展跨境数据传输风险评估，并确保充分保障数据主体的权利。
- 阿根廷、智利、哥伦比亚和秘鲁等国目前同样没有针对数据本地化的强制要求，但鉴于智能网联汽车行业涉及高敏感数据，监管部门已逐步表现出对数据主权和本地化解决方案的高度关注，并可能在未来通过行业细则或监管实践进行落实。

总体来看，中东和拉美两地在数据主权和跨境传输监管方面均处于持续强化阶段，但实施力度与监管成熟度存在差异。中东地区正逐步形成以阿联酋、沙特为核心的数据本地化合规格局，而拉美地区则以巴西和墨西哥为监管重心，强调跨境传输的合规机制和关键领域的安全保障。因此，建议采取**区域性数据中心**和**合规跨境传输机制**结合的混合策略。

在中东地区，优先将阿联酋与沙特作为区域性数据处理与存储节点，这更符合当前及未来中东地区的监管趋势与合规要求；

在拉美地区，建议在巴西或墨西哥建立区域数据中心，以满足主要市场的监管期望，同时通过适用数据跨境传输合规机制，确保与总部或其他地区节点间的数据流动合规；

对于合规风险较高的国家，可采用境内缓存结合境外备份的过渡性方案，以应对监管不确定性。

2 中东及拉美地区的车联网运营合规

车联网运营是汽车企业出海合规策略中需要考量的另一个核心因素，其面临的核心合规挑战在于对海量、实时、高敏感度隐私数据的合法处理。在强调数据主权和隐私保护的背景下，中国汽车企业必须构建一个以隐私保护为中心且覆盖数据全生命周期的运营体系。

> 需要强调的是，本节聚焦于隐私数据处理相关的运营合规，除此之外，车联网的系统准入、通信协议、无线认证以及网络安全（如 UN R155 / R156）等领域存在独立的监管要求，企业应将其作为独立合规事项进行整体考量。

建议出海企业围绕隐私数据，重点关注以下车联网运营合规要点：

功能变更与隐私保护评估

企业在推出新功能、进行功能变更或上线新应用前，应首先开展数据保护影响评估，以识别和评估潜在的隐私风险。同时，对涉及的数据字段进行严格的合规性校验，确保数据收集遵循最小化原则。任何隐私政策的实质性修改或个人数据处理范围和目的变更，都应通过清晰、透明的方式重新获得用户的明确同意。

OTA 升级与授权管理

OTA 升级是车联网运营中影响范围广泛的关键环节。企业必须确保升级流程遵循严格的合规要求，包括在升级前进行必要的 DPIA。在执行升级时，应通过弹窗等方式清晰告知用户升级内容，并获取用户的授权或同意。此外，对于所有参与车联网生态的第三方软件和系统，应建立严格合规审计和安全管控机制。

云平台运维与跨境数据安全

在云平台运维中，企业需严格实施权限管理，限制运维人员对海外数据节点的直接访问权限，并对访问行为进行审计。对于必须进行的跨境数据流转，应避免简单的直连访问，而应采用系统间接调用或数据脱敏等技术手段进行处理。此外，应确保系统日志等数据在脱敏或匿名化处理后，方可传回境内的总部平台，以满足当地对数据主权和跨境传输的合规要求。

总体而言，对于车联网运营合规，建议企业将隐私默认（Privacy by Default）和隐私设计（Privacy by Design）原则贯穿于功能开发、运维和数据处理的各个环节。通过对上述关键运营节点的精细化管理和合规嵌入，企业才能有效应对中东和拉美地区不断收紧的隐私监管要求，确保车联网服务的安全和用户权益的保障。

3 中东及拉美地区的合作伙伴评估

中国汽车企业在海外市场构建智能网联生态，必须依赖本地或全球化的合作伙伴，才能建起一个由云服务、智驾系统、智能座舱等核心技术提供商组成的生态体系。对这些合作伙伴进行系统化的合规评估，是保障自身业务在复杂监管环境下合法运营且维持数据安全底线的关键前提。

云计算合作伙伴

云计算平台是承载车联网和自动驾驶数据的核心基础设施，其合规性直接决定了企业数据主权和数据安全管理的底线。企业在选择云计算合作伙伴时，建议将以下要素纳入整体考量：

当地法律法规的遵循性

确保云计算合作伙伴在当地具备合法的运营资质和许可证。对其运营团队的在地化程度和股权架构进行尽职调查，这有助于评估其产品在全球范围内的一致性和连续性，以及满足特定市场对数据控制权和审查的要求。

全球化部署与韧性

评估云计算合作伙伴的全球化节点数量、服务可用性时长和数据安全机制，以支持跨区域业务的稳定运行与灾备需求。在数据本地化严格的市场，应优先选择在当地设有独立数据中心的合作伙伴。

合规认可程度及本地适应性

优先选择获得广泛全球化合规认可的云服务商，包括获得 ISO/IEC 27001 信息安全管理体系认证、SOC（System and Organization Controls）安全鉴证报告等；以及在全球拥有广泛基础设施和高度合规承诺的云计算合作伙伴，因为其可以更灵活地帮助企业在全球范围内满足严格的数据本地化和跨境传输要求。

生态合作伙伴与集成能力

评估云服务商的 ISV（独立软件开发商）和 MSP（托管服务提供商）生态系统的广度和深度。强大的生态合作伙伴能提供垂直行业的专业解决方案、定制化的集成服务以及本地化的部署与运维支持。

技术能力和创新

在生成式人工智能方面，应优先选择具备强大 AI 能力的云计算合作伙伴，其能提供全面的 AI 服务、优化的训练工具和高效的开发支持，可帮助企业减轻多模态 AI、合规性、伦理问题和系统集成等挑战，从而助力 AI 项目高效、稳定和可持续发展。

智驾合作伙伴

智能驾驶（包括 ADAS 辅助驾驶和 ADS 全自动驾驶）涉及高精地图、道路环境感知等高敏感度数据，因此对智驾合作伙伴的合规评估必须结合具体业务场景，审慎明确合规义务的归属和数据所有权。建议将以下要素纳入整体考量：

合规义务的场景化区分

针对不同智驾场景明确合作伙伴的合规责任。对于 L2 级辅助驾驶（L2 ADAS），合规主体责任主要在主机厂（OEM）。主机厂需确保智驾系统满足当地车辆准入要求（如电子电气架构安全），明确 ADAS 功能产生的数据（如驾驶行为数据）的所有权和使用权，并确保其采集和处理过程中的隐私合规。对于 L4 级自动驾驶（如 L4 Robotaxi），合规主体责任则由自动驾驶研发商、车辆制造商、车队运营商以及系统集成商共同承担。这类业务需满足当地更严格的准入要求，包括取得路测牌照和地图数据采集合规许可等。

技术监管的在地熟悉程度

中东与拉美市场正逐步建立针对功能安全、车联网络安全以及 AI 透明度的技术监管框架。因此，建议评估智驾合作伙伴对当地技术监管要点的熟悉程度和应对能力，例如针对 EDR / DDR 数据处理规范、人工智能算法透明度与可解释性，以及针对远程接管的安全与审计机制设计是否符合监管要求。

数据归属与共享机制

明确自动驾驶过程中所产生数据的所有权、使用权与责任界限。应通过合同约定和技术设计，确保在多主体合作或跨境流转中，数据采集、存储、处理和共享都遵循当地法规，避免后续出现合规争议。

座舱合作伙伴

智能座舱作为人机交互的核心界面，直接涉及大量敏感个人数据以及 AI 大模型的应用场景，例如语音识别和安全监测。因此，对座舱合作伙伴的合规评估应主要围绕隐私保护以及 AI 合规展开。建议从以下几个维度对座舱合作伙伴进行评估：

敏感个人数据的合规处理

评估合作伙伴在处理涉及用户人脸、指纹、语音生物特征等敏感个人数据时，是否遵循了最高级别的隐私保护标准，包括确保在数据采集前已获得了用户明确同意，以及采用了充分的安全技术措施。合作伙伴应能证明其有能力在座舱内、云端和传输过程中保障敏感个人数据的安全。

AI 伦理与算法透明度

针对座舱内基于 AI 大模型的应用（如智能语音助手、驾驶员状态监测），合作伙伴需遵循中东和拉美地区日益关注的 AI 伦理与安全原则。评估要点包括其算法的透明度、可解释性，以及识别和消除潜在模型偏见的能力。合作伙伴提供的 AI 系统应具备可审计性，能够证明其决策过程符合预期的合规标准。

合规解决方案与服务

随着智能化技术的快速迭代与应用，企业对人工智能、安全合规、供应链创新等核心能力建设的需求愈发迫切。秉承“**解决重要问题**，**营造社会诚信**”的企业使命，普华永道与亚马逊云科技于 2021 年在中国开始紧密合作、强强联手，为汽车、零售、制造、生命科学等行业提供解决方案，持续为客户创造价值。

通过与亚马逊云科技的合作，普华永道为中国企业提供了一个创新驱动的数字化平台，其中包括云迁移、数据分析、AI 智能化等关键技术，帮助企业在激烈的市场竞争中脱颖而出。

> 例如，在汽车行业，普华永道与亚马逊云科技合作，为中国汽车制造商提供了车联网、智能制造和自动驾驶等技术的集成方案，帮助企业提升生产效率并拓展国际市场。

随着数字化转型的不断加速，普华永道与亚马逊云科技的合作关系亦将不断深化，尤其在**跨国云服务解决方案**、**数据隐私保护和行业定制化应用**等方面。未来，我们将看到更多全球标准与本地实践相结合的创新合作。与此同时，普华永道中国将继续致力于为中国企业提供具有全球视野的技术解决方案，帮助企业更好地拓展国际市场。

跨国云服务解决方案

数据隐私保护

行业定制化应用

1 普华永道智能网联汽车合规服务

普华永道在服务中国汽车出海合规方面拥有大量成功案例，协助多家企业从 0 到 1 在全球实现业务合规落地，覆盖乘用车、商用车、特种车辆、零部件供应商等多类型企业，在过程中积累了丰厚的实践经验，能够快速响应企业在不同领域、不同业态的合规需求。我们的重点服务领域包括但不限于：

1.1 全球智能网联汽车准入咨询服务

随着汽车智能化、网联化发展，WP.29 发布了多项针对汽车产品新增的市场准入要求，这些要求将陆续在全球多个主流市场国家生效，需要企业在业务出海前提前应对。我们的服务包括：

- **R155 网络安全合规咨询服务：**对标 ECE R.155 法规和 ISO/SAE 21434 等法规标准，帮助企业搭建 CSMS 车辆安全管理体系，协助获取体系及 VTA 证书。
- **R156 软件升级合规咨询服务：**对标 ECE R.156 法规和 ISO/AWI 24089 等法规标准，帮助企业搭建 SUMS 车辆软件升级管理体系，协助获取体系及 VTA 证书。
- **R157 ALKS 合规咨询服务：**对标 ECE R.157 法规，指导企业开发符合准入要求的 ALKS（Automated Lane Keeping System，自动车道保持系统），并协助获取 VTA 证书。
- **R171 DCAS 合规咨询服务：**对标 ECE R.171 法规，协助企业对网络安全、功能安全和预期功能安全管理进行融合协调，指导开发符合认证要求的 DCAS（Driver Control Assistance Systems，驾驶员控制辅助系统），并协助获取 VTA 证书。

1.2 数据&隐私安全合规咨询服务

智能网联汽车的数据&隐私安全是目前海外主流市场国家监管重点关注的领域。当前，汽车已经发展成为一个复杂的集数据采集、处理、储存、传输为一体的综合智能终端。此外，由于车联网的业务特定常常具有数据跨境的场景，且伴随数据种类复杂，数据量大、后端利用场景复杂等特点，合规风险突增。我们的服务包括：

- **全球隐私监管合规咨询：**深度解读各地区隐私监管法规要求，贯穿隐私数据生命周期，囊括车联网业务、整车功能、企业管理等多个层面，评估企业隐私监管合规差距，并提出整改建设建议。
- **全球化站点部署及数据合规跨境路径规划咨询：**根据企业目标市场国家范围，基于目标市场国家本地化监管要求，设计最小化站点部署方案建议，并规划全球化数据合规跨境流动方案。
- **数据合规管理体系规划：**根据企业组织架构及业务模式，设计全球化数据合规管理体系，规划各区域实体间权责划分及风险隔离方案。

1.3 安全认证咨询服务

普华永道拥有丰富的认证咨询经验，能够帮助汽车行业尤其是汽车供应链上下游企业获取所需的安全认证，构建行业供应链安全信任。我们的服务包括：

- **ISO 21434 认证咨询：**根据 ISO/SAE 21434 标准要求，指导企业搭建网络安全管理体系，协助获取 ISO 21434 体系认证及产品认证。
- **ISO 26262 认证咨询：**根据 ISO 26262 标准要求，指导企业搭建功能安全管理体系，协助获取 ISO 26262 体系认证及产品认证。
- **GDPR Europrivacy 认证：**遵从 GDPR 要求，指导企业设计和实施完善的隐私保护体系，协助企业获得认证。
- **TISAX 认证咨询服务：**作为 ENX 协会认可的 TISAX 审计服务提供商，为中国客户提供一站式服务。根据 TISAX 认证要求帮助企业开展合规建设、协助获取 TISAX 认证。
- **其他认证&鉴证咨询：**ISO 27001、ISO 27701、ISO 29151、ISO 27018、SOC 鉴证报告等

1.4 汽车信息安全技术评估服务

普华永道拥有自己的车联网安全实验室和网络安全专业技术团队，能够为汽车行业企业提供各项技术服务，具体包括：

- **整车及重点零部件网络安全威胁分析与风险评估（TARA）：**评估典型应用场景，将威胁与评估对象、安全属性进行映射，形成对应关系；结合威胁和影响级别，对威胁与评估对象进行等级划分；将威胁、评估对象、安全属性和安全等级四个维度进行整合形成安全需求。以供在产品设计阶段考量相关安全保护要求，实施有效的安全管控措施。
- **车联网渗透测试服务：**针对车联网业务发展所涉及的信息系统、应用及产品，实施网络安全渗透测试等技术层面分析，识别现有应用所存在的网络安全风险，为企业提供精准的网络安全保护方案。

1.5 汽车行业专项研究服务

随着企业高管对安全合规的愈加重视，安全合规管理工作不断“左移”，在公司出海、产品及业务设计等领域需要专门的安全合规洞察以辅佐决策。我们的服务包括：

- **全球化隐私监管洞察：**调研并持续跟踪全球主流市场国家隐私监管动态，包括法规、标准、执法案例等，形成覆盖全球主流市场国家的隐私监管洞察报告；协助企业了解海外监管态势，预判合规风险。
- **全球化汽车安全技术监管洞察：**调研并持续跟踪全球主流市场国家关于汽车网络安全相关法规及标准监管动态，包括全球主流标准化组织、行业协会等；对安全标准进行解读和研判，形成全球化汽车安全技术监管洞察报告；协助企业了解海外安全标准，对内部产品合规情况进行对标，预判产品安全技术合规风险。

2 亚马逊云科技汽车行业解决方案

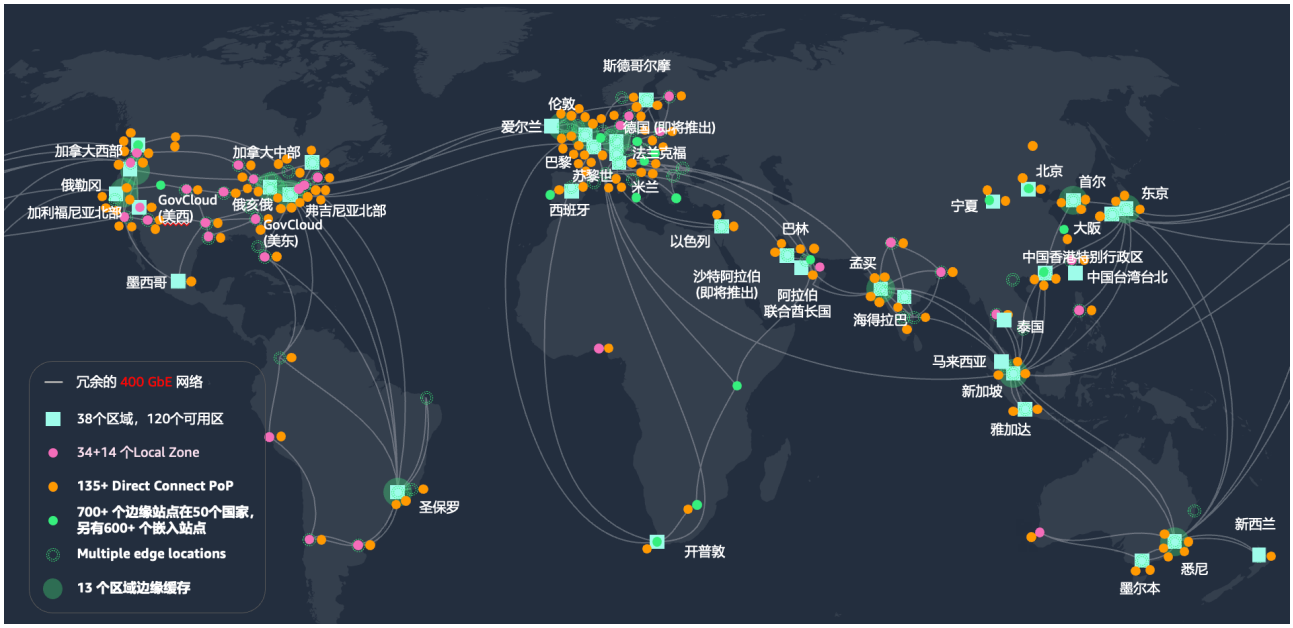
由前述分析可以看出，车企出海需要构建一个安全、合规且能持续迭代的后端方案。整个方案建设一般可划分为如下三个阶段：区域选择与网络建设、业务系统部署和测试、安全加固，涉及 PKI (公钥基础设施)、TSP（远程信息服务平台）、数据分析、OTA（空中升级）和辅助驾驶等业务系统，下面分别介绍亚马逊云科技三个阶段中典型的解决方案。

2.1 阶段一：区域选择与网络建设

出海的首要任务是建立安全和合规的基础架构，通过分析目标国家或地区的合规要求，在对应国家或地区进行后端部署，满足数据本地化存储和高可用等要求。基于中东地区的合规要求，亚马逊云科技战略性地部署了多个区域，为汽车制造商提供了理想的本地化数据存储解决方案。

> 在**中东地区**，亚马逊云科技通过其战略性布局的多个区域，包括巴林、阿联酋（UAE）和沙特阿拉伯(即将)，成为最有可能满足本地严格的合规要求的云服务提供商。这些区域不仅提供了广泛的地理覆盖，还确保了丰富的计算资源和服务选择，共同构成了一个强大的云基础设施网络，能更好地满足数据主权、本地化存储和低延迟访问等监管要求。

> 在**中南美地区**，亚马逊云科技已经推出巴西（2011）和墨西哥（2025）区域，同样各自提供三个可用区，智利区域也即将发布。这些资源使汽车企业能够灵活应对快速变化的市场需求，加速数字化转型进程，利用这些区域，车企可以有效平衡数据本地化与全球化运营需求，为在中南美洲的业务拓展奠定坚实的技术基础。(region 信息截止2025年9月)



除了区域资源，车企借助亚马逊云科技的全球骨干网络（不包含中国区域）这一基础设施，能够在几分钟内实现全球覆盖，构建自己的专有网络，并且即开即用，显著降低传统线路建设的高成本和长时间周期。同样基于广泛的全球运营商互联以及 Amazon Route 53 Resolver 功能，APN 网络建设周期也可以大大缩短。

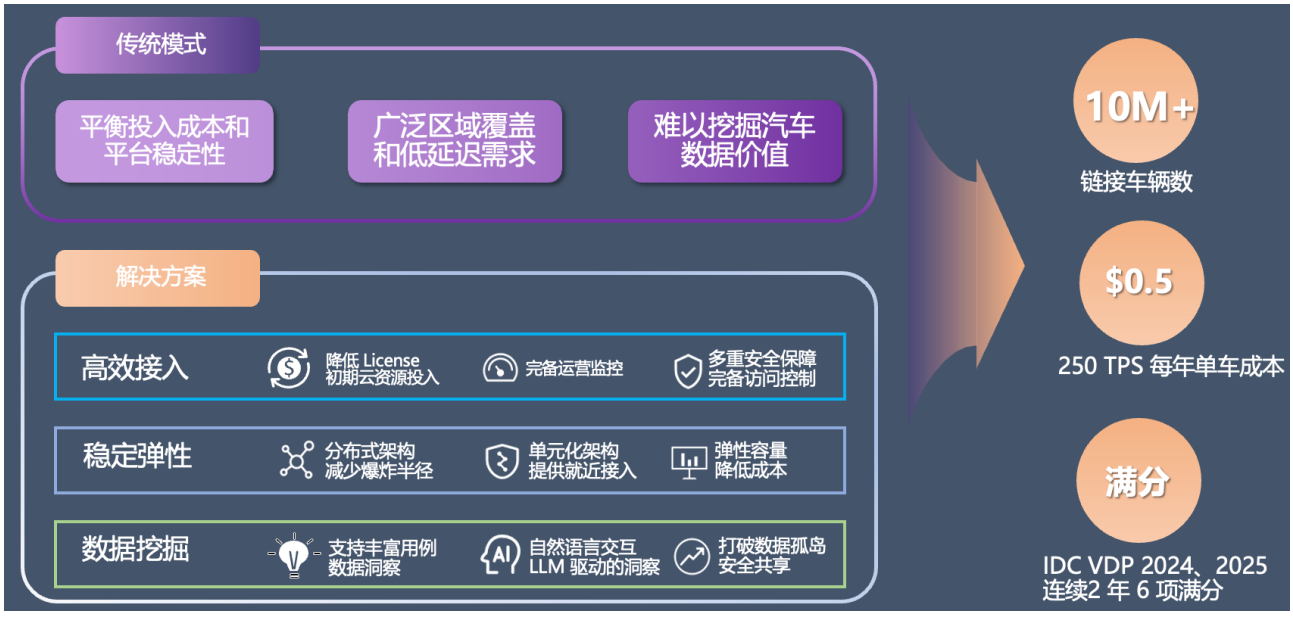
2.2 阶段二：业务系统部署与测试

一旦合规调研、区域选择和线路建设完成，下一步的关键就转向系统实施，确保智能网联系统包括 PKI、TSP、OTA 和辅助驾驶等核心系统能够安全、高效地在海外目标区域落地。中东地区因其独特的数据主权要求和严苛的环境条件，对部署细节提出了更高的挑战。亚马逊云科技为汽车行业打造了全面的解决方案，涵盖产品研发、软件定义汽车、车联网、自动驾驶、数字化用户体验等八大核心领域。

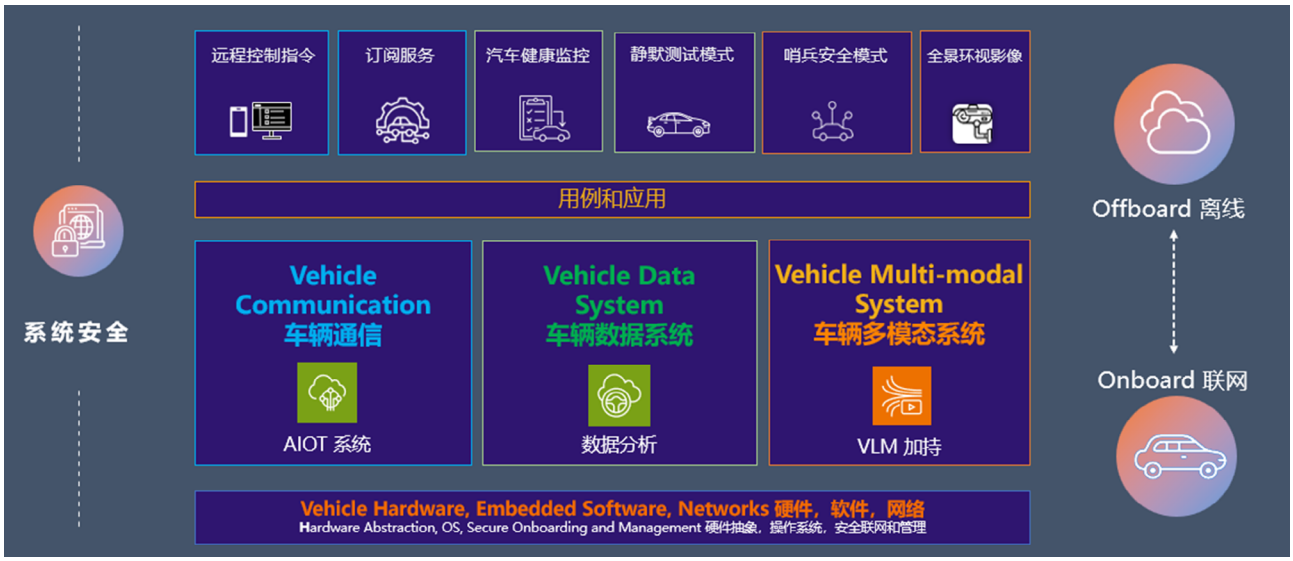
下面聚焦在车联网和辅助驾驶两个典型场景。

2.2.1 智能网联系统服务

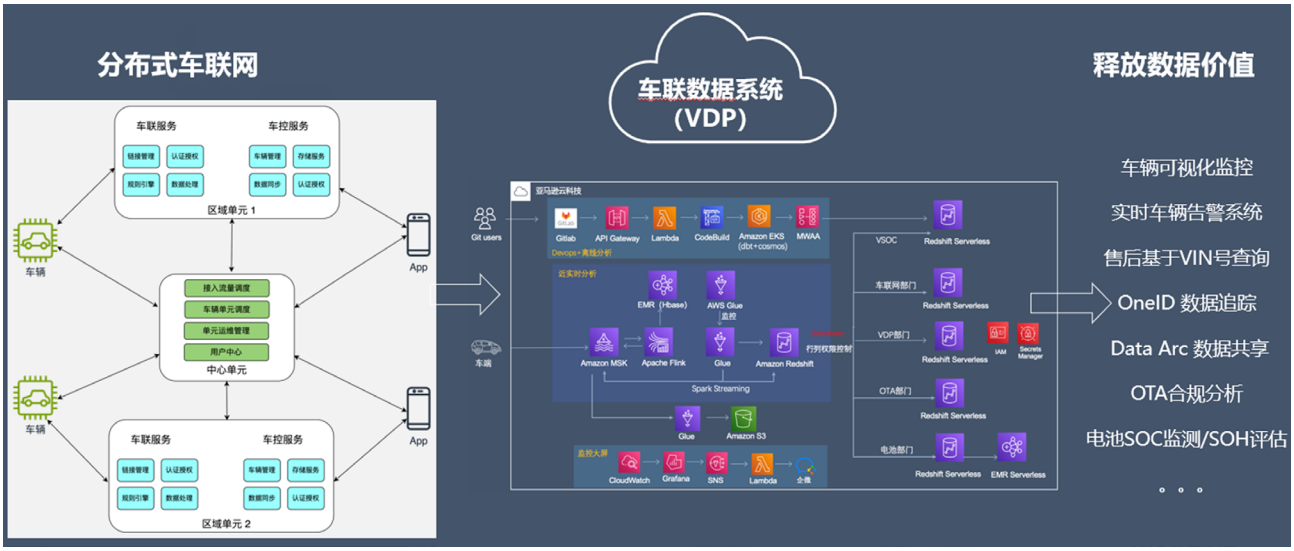
智能网联系统服务是当前新能源车辆的核心应用系统，OEM 都在对传统车联网架构进行升级改造，探索更加高效低时延的接入和数据采集解决方案，构建针对海量数据的、灵活的数据分析服务，释放数据价值。



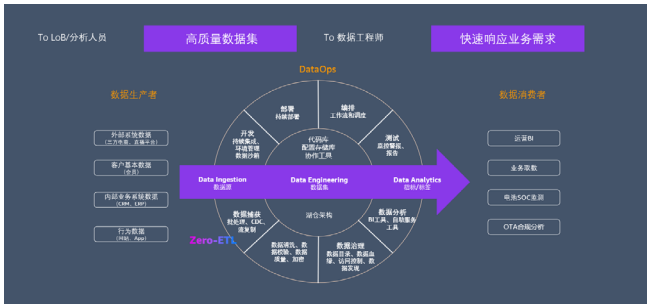
亚马逊云科技推荐基 于IoT Core 的 AIoT 解决方案构建智能网联服务，基于亚马逊云科技的单租户安全模块 CloudHSM 构建 PKI 系统，实现高效的车云通信。

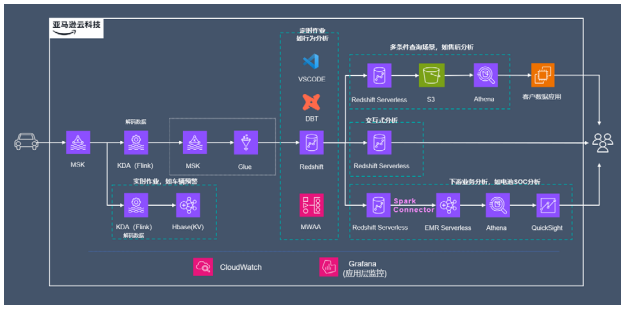


采用已在多个客户落地的分布式车联网架构应对新能源车辆增长带来的系统可靠性挑战。



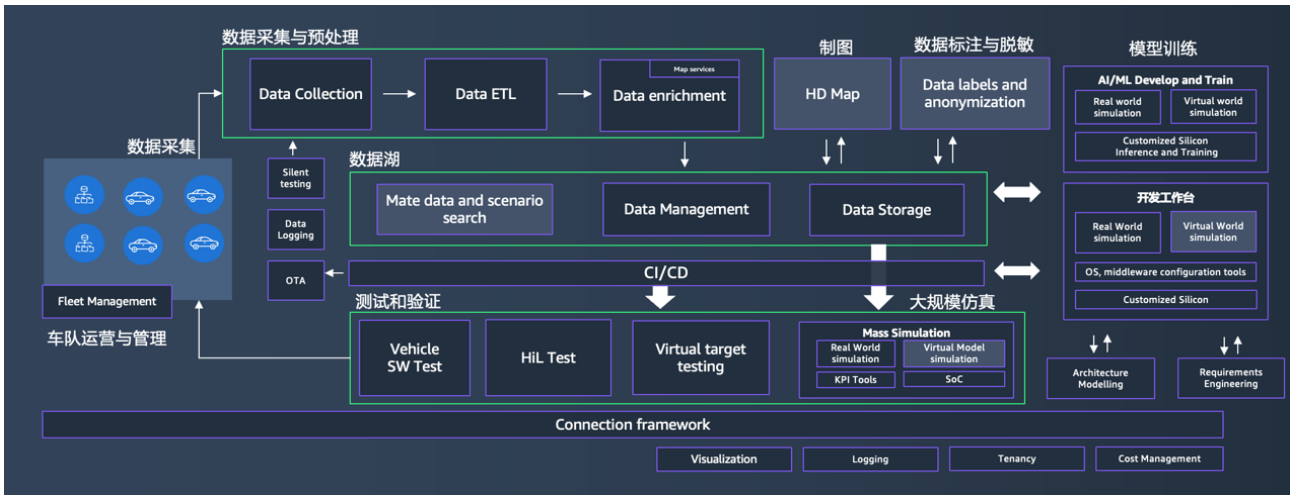
车联网数据服务需要整合多方数据源，提供采集、存储、分析和展示等功能，为上层业务提供数据服务。亚马逊云科技的云原生车联网数据方案提供了较高弹性、可扩展性，通过无服务器架构和服务选型降低运维负担，加速应用部署。数据湖技术（Amazon S3 +Iceberg）结合 Amazon Athena、Amazon EMR Serverless、Amazon Redshift 等无服务器服务，实现数据一次存储多处使用，提升运营效率和成本控制能力。



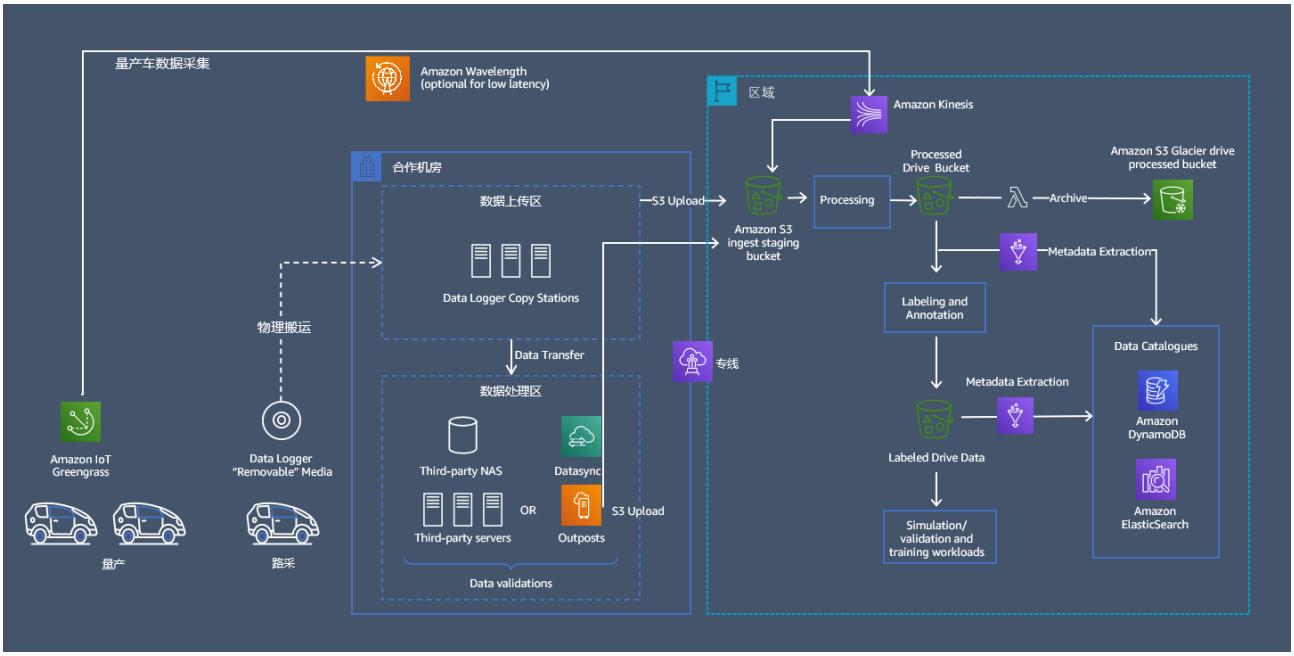


2.2.2 辅助驾驶

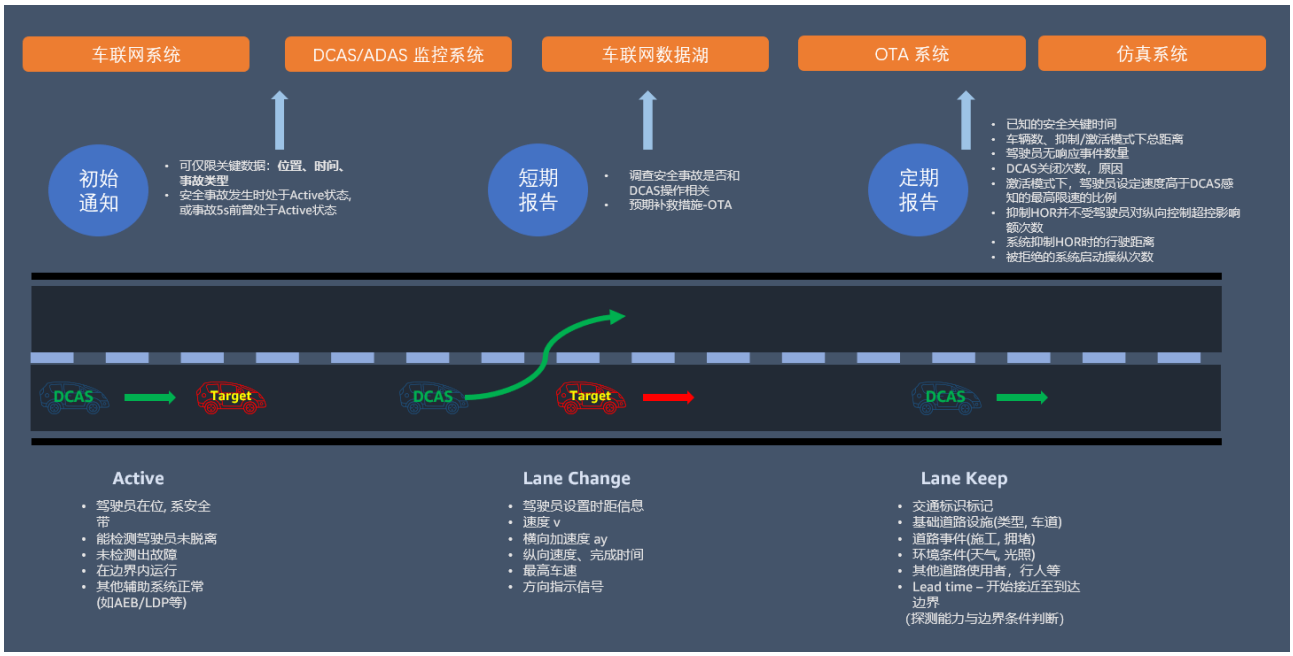
辅助驾驶在2025年从“功能可用”逐步走向“场景好用、用户愿用”，大量新技术被采用：端到端大模型全面上车，多模态大模型被普遍用来解决数据标注瓶颈，世界模型被用来解决长尾场景等。同时随着法规的落地，中国车企针对欧洲辅助驾驶功能法规 R171 已经进入体系认证和车型认证的加速期，以保持在智能化时代的持续领先优势。这些能力与法规建设必将能更好支撑中国 OEM 和辅助驾驶公司在欧洲、中东及全球更多地区的业务拓展。亚马逊云科技在数据方案构建、大规模训练和仿真等领域都有完善的解决方案和落地经验，支持国内 OEM 客户和辅助驾驶客户在海外多个国家和地区落地了生产环境，逻辑架构示意图如下：



实际架构如下，研发路采阶段数据会通过专线方式上传到云端对象存储，量产车的数据通过车联网收集，进入数据闭环。



从合规角度来看，欧盟 R171 法规对 OEM 智驾数据采集和管理实践给出了明确的指导，遵循这一法规对于全球智驾业务的开展有显著帮助。法规将影响 OEM 的数据处理流程和现有应用系统，通过分析典型场景，识别出数据收集、监控平台和数据平台三个关键领域需要进行的针对性改造和适配，如下图的法规中的三种典型场景需要采集和记录的信号以及三种运营中通知和报告义务。



2.3 阶段三：安全加固

随着基础架构搭建及应用系统部署的完成，在业务开展前，就需要完成各类安全加固，以应对日益增长的安全挑战。常见基础设施的安全会覆盖主机及容器安全，启用应用层及网络防火墙，车端安全会建设车辆安全运营服务 vSoC 等，同时还需要特别关注数据隐私、实时通信安全和大规模设备管理等特定领域。通过参考以下系统性安全实施建议，车联网企业可以全面提升其云环境的安全态势，有效应对行业特有的安全挑战，确保车辆数据的安全性和隐私保护。

安全领域	关键实践	相关 Amazon Web Services 服务	实施重点	预期效果
身份和访问管理	强化身份认证和授权机制	- Amazon IAM - Amazon SSO - Amazon Cognito	- 实施多因素认证 - 采用基于角色的访问控制 - 遵循最小权限原则	降低未授权访问风险，提高账户安全性
网络安全	构建多层防御体系	- Amazon Shield - Amazon WAF - Amazon Network Firewall	- 部署 DDoS 防护 - 实施网络分段 - 加强边界安全	保护车联网基础设施免受网络攻击
数据保护	全生命周期数据安全	- Amazon KMS - Amazon Macie - Amazon Backup	- 静态和传输中的数据加密 - 实施数据分类和治理 - 安全的数据备份和恢复	确保车辆和用户数据的机密性和完整性
应用程序安全	构建安全的车联网应用	- Amazon WAF - Amazon CodePipeline - Amazon Inspector	- 实施 Web 应用防火墙 - 采用安全开发生命周期 - 定期进行安全测试	减少应用层面的安全漏洞
监控和响应	建立全面的安全监控体系	- Amazon CloudTrail - Amazon GuardDuty - Amazon Security Hub	- 集中化日志管理 - 实时威胁检测 - 制定事件响应计划	快速识别和应对安全事件
合规性管理	满足行业特定的合规要求	- Amazon Config - Amazon Artifact - Amazon Macie	- 实施数据隐私保护措施 - 定期进行合规性评估 - 保持安全控制的文档化	确保符合相关法规和标准
设备安全	保障车载设备的安全性	- Amazon IoT Core - Amazon IoT Device Defender - Amazon IoT Device Manage-ment	- 实施安全的 OTA 更新机制 - 设备身份认证和授权 - 端到端加密通信	防止设备被篡改和未授权访问

亚马逊云科技还提供众多的合作伙伴方案，多层次助力客户的应用和数据安全以及合规。

3 亚马逊云科技合规服务

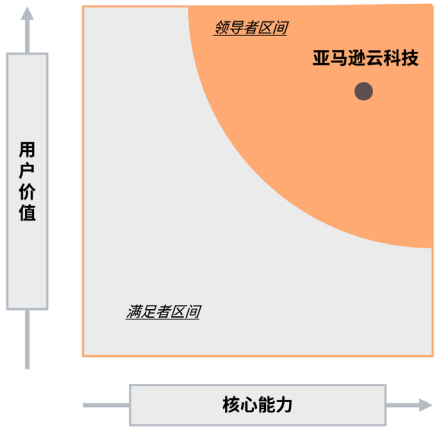
3.1 亚马逊云科技合规框架

亚马逊云科技从进入中国以来，持续帮助支持中国企业出海，近日，弗若斯特沙利文（Frost & Sullivan）联合头豹研究院发布了《2025年在华外商企业云计算服务采用研究报告》。

报告显示，外商企业在华投资持续回暖，外资新设企业数量与投资金额均保持增长。亚马逊云科技凭借在全球与本地的长期积累与领先实践，在**核心能力和用户价值两个维度均位列第一，获评在华外企云计算服务提供商领导者**。由此可见，亚马逊云科技不仅稳居"领导者区间"，还在增长指数和创新指数两关键维度上均名列前茅，展现出强劲的市场竞争力。

2025年在华外商企业云计算服务采用

——云服务综合竞争表现 Frost Corner ™



亚马逊云科技凭借近20年服务全球客户的丰富经验，支持各行各业数百万活跃客户实现数字化转型。基于这些广泛的行业经验，亚马逊云科技总结出安全合规的三个关键方面。

人员

制定规范、流程、根据法规定义哪些是敏感数据，发现和解决出现的安全问题

流程

应急响应流程、敏感数据导入导出流程、数据泄漏 72 小时通知流程等

技术

识别敏感数据、敏感数据脱敏、数据传输加密、数据存储加密等

另外，我们认为安全合规与用户的业务开展与持续进行紧密相关，安全不是独立的存在，而应与企业业务充分结合，作为业务开展的首要条件。

- 安全合规是基于设计而不是基于对事件的响应。安全的建设应该是未雨绸缪，根据业务的情况和系统的特点，主动从技术和管理的层面去建设。
- 亚马逊云科技除了为用户的应用提供了安全的基础架构以外，我们也在一直在安全服务领域不断创新，我们的安全服务围绕着以下预防，检测，响应，修复来展开，我们也建议客户以此来标准来构建安全体系。
- 亚马逊云科技支持广泛的安全标准和合规认证,包括 PCI-DSS、HIPAA/HITECH、FedRAMP、SEC Rule 17-a-4、欧盟数据保护指令和 FISMA 等，这有助于企业满足几乎所有全球监管机构的合规要求。

3.2 数据分级分类

车联网的海量数据上传到云端之后，数据的存储和处理成为车企一大挑战。针对中东地区严格的数据法规要求，特别是阿联酋物联网的四级数据分类标准，亚马逊云科技开发了云原生的敏感数据保护解决方案。

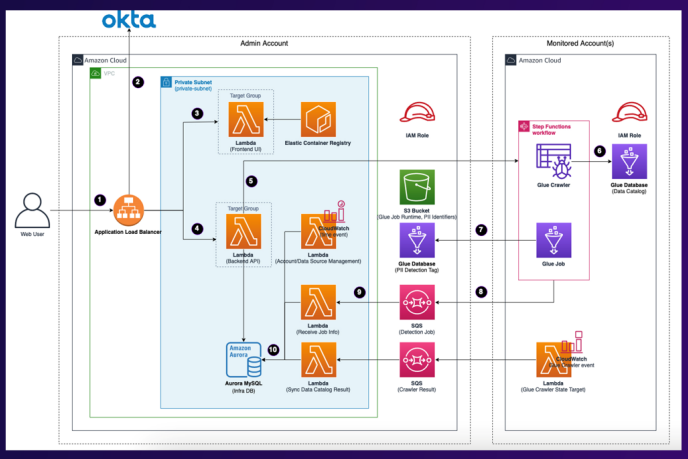
> 该方案采用**智能自动识别技术**，根据自定义的数据分类模板，客户可以对云端的海量数据进行精准识别和自动标记。同时，该方案还提供了**可视化仪表板**，为车企提供全面的敏感数据分布视图，包括数据资产的安全保护状态和合规风险评估。这种本地化的数据治理方法不仅助力了车企在中东的合规运营，还优化了数据安全管理流程，企业能够在满足严格的地区性数据保护要求的同时，大幅提升数据利用价值。

3.3 数据跨境解决方案

为解决企业数据处理和跨境传输的合规要求，亚马逊云科技提供全面数据管理和合规框架。

方案利用 Amazon Glue 服务构建元数据目录，进行敏感数据扫描和处理，确保数据在各账号内处理，避免跨账号传输。采用多账号结构，配备独立私有子网和安全组，强化数据隔离。集成企业 IDP 实现单点登录，提升安全性。架构限制内网应用对公网访问，降低泄露风险。利用 Amazon Lambda 和 Amazon S3 实现高效处理和存储。方案提供数据全生命周期安全防护，包括脱敏、访问控制、加密传输、跨境检测等功能。满足 GDPR 等法规要求，为跨国企业提供可扩展、安全的数据处理方案，展示亚马逊云科技在跨境数据传输和隐私保护的创新能力。

敏感数据保护解决方案 方案架构



架构特点

- 以 Glue Data Catalog 为基础构建元数据目录
- 以 Glue Jobs 为基础进行敏感数据扫描
- 敏感数据扫描在各账号完成，不涉及跨账号传输
- 可集成企业 IDP，如 Okta，Keycloak 进行单点登录
- 内网应用不涉及公网访问

附录

联合署名

普华永道

编写指导

普华永道中国汽车行业主管合伙人 金军

普华永道中国内地网络安全及隐私服务主管合伙人 李睿

普华永道中国亚马逊云科技联盟合伙人 黄财明

主编人员：

普华永道中国内地汽车交易战略团队高级经理 李末菲

普华永道中国内地网络安全及隐私服务团队高级经理 赵元勋

普华永道中国内地网络安全及隐私服务团队经理 杨雄

普华永道中国内地网络安全及隐私服务团队经理 任子同

普华永道中国内地网络安全及隐私服务团队高级顾问 王玲玉

普华永道中国内地网络安全及隐私服务团队高级顾问 李皓玥

普华永道中国内地网络安全及隐私服务团队顾问 童熙成

亚马逊云科技

编写指导

亚马逊云科技大中华区行业集群总经理 沈涛

亚马逊云科技大中华区产品总经理 陈晓建

亚马逊云科技大中华区解决方案架构师总经理 代闻

亚马逊云科技大中华区合作伙伴及初创计划总经理 苏小龙

主编人员：

亚马逊云科技大中华区解决方案架构师总监 梁睿

亚马逊云科技大中华区解决方案架构师经理 叶江荣

亚马逊云科技大中华区高级解决方案架构师 谢紫玲

亚马逊云科技大中华区云安全产品经理 范恂毅

亚马逊云科技大中华区合作伙伴解决方案架构师经理 吴迦德

亚马逊云科技大中华区合作伙伴解决方案架构师 裴峰

亚马逊云科技大中华区全球生态合作伙伴拓展高级经理 徐丽


亚马逊云科技
pwc