

亚马逊云科技



普华永道

智能网联汽车 安全白皮书



声明

- 本白皮书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章、第二章、第三章和第四章中的市场趋势分析及法规要求和合规解读等部分，单独享有该部分的知识产权；亚马逊云科技负责撰写第二章中的亚马逊云科技汽车行业解决方案、第三章中亚马逊云科技的安全与合规以及第四章中与亚马逊云科技云计算服务相关的技术实践和解决方案部分，单独享有该部分的知识产权。文件中所有文字、数据、图片、表格，均受中华人民共和国著作权法及其它法律法规保护。未经普华永道和 / 或亚马逊云科技书面许可，任何机构和个人不得基于任何商业目的使用本报告中的信息（包含报告全部或部分内容），不得摘录、复制、储存在检索系统中，或以任何形式或通过任何手段（包括电子、机械、影印、录制或扫描）进行传播。如果任何机构和个人因非商业、非盈利、非广告的目的需要引用本报告中内容，需要注明“转载自普华永道商务咨询（上海）有限公司和 Amazon Web Services, Inc. 或其关联方联合发布的《智能网联汽车安全白皮书》”。
- 本文件仅作为一般性指导，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，并且未就本报告内容做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做出投资或其他商业决定。如需具体意见，请咨询专业顾问。
- 本文件中由亚马逊云科技负责撰写的内容陈述了亚马逊云科技在封面页所示日期的有关服务产品及实践，该等信息可能变化且我们不会另行通知。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或其关联方、供应商或许可方的任何保证、陈述、合同性承诺、条件或者担保。亚马逊云科技对其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和其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。




引言

1886年1月29日，两位德国人卡尔本茨和戈特利布戴姆勒获得世界上第一辆汽车的专利权，标志着历史上第一辆内燃机驱动汽车的诞生。时过境迁，汽车在变化不大的铁壳子下，内饰、功能和属性已经发生了翻天覆地的变化。

一百五十年过去了，新一代智能网联汽车（Intelligent Connected Vehicle）应运而生。电动化、自动化、网联化、共享化是智能网联汽车区别于传统汽车的地方，它搭载了先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车、路、人、云端智能信息交换、共享和协同化，具备复杂环境感知、智能决策、协同控制等功能，达到高效便捷、自动安全、环保节能的行驶目的，并最终可实现替代人来操作的新一代汽车。

根据《普华永道思略特2020年数字化汽车报告》、《普华永道思略特2021年数字化汽车报告》的分析与预测，全世界各国的智能网联汽车保有量将迅速增长。其中，美国将从2020年32%的保有率扩大至2035年的97%，欧盟将从2020年的25%比例扩大至98%，而中国也将从2020年16%扩大至2035年的72%，即超过2/3的保有率。很显然，智能网联汽车必将代替传统汽车成为汽车行业后现代化发展的重要方向。





与此同时，我国针对智能网联汽车的相关政策、法规研究制定也进入了紧锣密鼓期。《国家综合立体交通网规划纲要（2021年-2035年）》、《国家车联网产业标准体系建设指南（总体要求）》、《国家车联网产业标准体系建设指南（车辆智能管理）》、《国家车联网产业标准体系建设指南（智能交通相关）》、《道路交通安全法（修订建议稿）》以及各省、市政府级的标准建设指南相继出台。

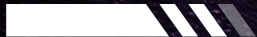
各大互联网巨头，科技公司也纷纷加入智能网联汽车竞争队伍中，利用自家的技术积累，共同打造智能网联汽车大生态。

本文中，我们试图围绕政府“十四五规划”与产业政策、智能网联汽车产业的发展现状、机遇与挑战、未来发展趋势这几个方面展开讨论。

目录



第一章：政府“十四五规划”与产业政策	08
第二章：智能网联汽车产业的发展现状	11
智能网联汽车产业的投融资情况	11
互联网科技公司争相涌入智能网联汽车赛道	13
智能网联汽车发展现状分析之数字技术驱动汽车行业的创新发展	14
智能网联汽车发展现状分析之营销服务创新	16
以用户直联和私域运营带动业务增长和服务体验提升	
亚马逊云科技汽车行业解决方案	19
第三章：智能网联汽车数字化技术融合进程中带来的挑战与应对	23
车辆网络安全与软件升级合规	26
WP.29 世界车辆法规协调论坛简介	26
WP.29 R155 & R156 法规概要	27
R155 合规要求解读	28
R156 合规要求解读	30
车辆型式认证适用车型范围	32



各车企法规应对现状	33
R155 & R156 合规应对解决方案	34
个人信息保护合规	36
GDPR 通用数据保护条例概要	36
GDPR 合规要求解读	37
GDPR 通用数据保护条例应对之道	39
亚马逊云科技的安全与合规	41
第四章：智能网联汽车未来发展趋势展望	49



01

政府“十四五规划” 与产业政策

—



第一章：政府“十四五规划”与产业政策

“十四五”规划纲要第八章、第十三章、第十八章中分别提出了深入实施制造强国、加快新型基础设施建设、营造良好数字生态的战略目标：

- **推动物联网全面发展**，打造支持固移融合、宽窄结合的物联接入能力。加快构建全国一体化大数据中心体系，强化算力统筹智能调度，建设若干国家枢纽节点和大数据中心集群，建设 E 级和 10E 级超级计算中心。**积极稳妥发展工业互联网和车联网；**
- **突破新能源汽车高安全动力电池、高效驱动电机、高性能动力系统**等关键技术，加快研发智能（网联）汽车基础技术平台及软硬件系统、线控底盘和智能终端等关键部件；
- **发展自动驾驶和车路协同的出行服务**。推广公路智能管理、交通信号联动、公交优先通行控制。建设智能铁路、智慧民航、智慧港口、数字航道、智慧停车场。

各省市政府也相继印发了配套支持汽车产业与道路交通发展的规划，以北京、上海、广东为例：

- 北京市人民政府印发的《北京市“十四五”时期高精尖产业发展规划》中明确提出“坚持网联式自动驾驶技术路线，推动车端智能、路端智慧和出行革命，加速传统汽车智能化网联化转型。并支持大力发展智能网联汽车整车、智能网联设施和关键部件、智慧出行服务等细分领域，力争到 2025 年汽车产业产值突破 7000 亿元，智能网联汽车 (L2 级以上) 渗透率达到 80%。

- 上海市人民政府印发了《上海市先进制造业发展“十四五”规划》，《规划》中明确了汽车产业集群重点领域及目标：到 2025 年，智能网联汽车总体技术水平和应用规模达到国际领先水平，实现特定场景的商业化运营；努力提升汽车全球话语权和市场份额，产业规模达到 1 万亿元；建设完善的智慧出行生态体系，建成具有全球影响力的智慧出行服务高地。
- 广东省人民政府印发《广东省制造业高质量发展“十四五”规划》。《规划》中支持以广州、深圳、惠州、东莞、韶关、肇庆等市为依托，加快布局发展智能网联汽车。支持广州建设基于宽带移动互联网的智能网联汽车与智能交通应用示范区，加快推进国家 5G 车联网先导区建设。支持广州、深圳在公共交通领域率先探索自动驾驶示范应用，打造具有世界级影响力的示范应用案例。支持惠州以东江高新科技产业园为依托，发展智能驾驶舱解决方案及车载信息娱乐系统、空调控制、胎压监测、高级驾驶辅助系统、车联网等。到 2025 年，汽车制造业营业收入超过 1.1 万亿元，打造具有国际影响力的汽车产业集群。



02

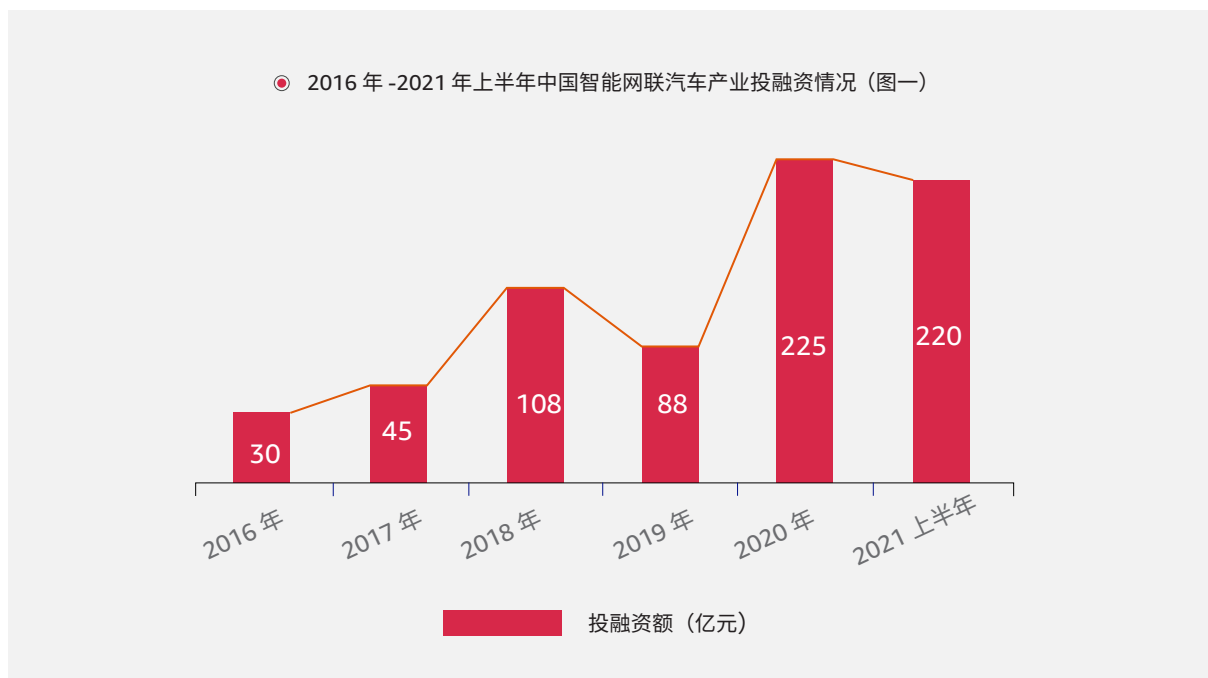
智能网联汽车产业的发展现状



第二章：智能网联汽车产业的发展现状

智能网联汽车产业的投融资情况

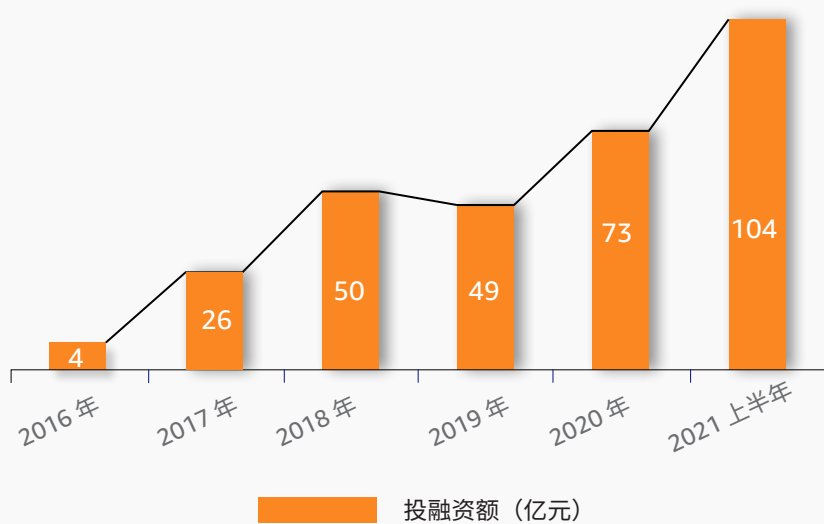
根据中国电子信息产业发展研究院赛迪智库发布的《2021年智能网联汽车投资环境和融资水平报告》，我国智能网联汽车产业投融资额飞速增长。年投融资总额从2016年的30亿元至2020年的225亿元，年平均增长速度为123%。仅2021年上半年，投融资额已几乎持平了2020年全年的水平，达到了220亿元。



资料来源：中国电子信息产业发展研究院赛迪智库《2021年智能网联汽车投资环境和融资水平报告》

2016年至2021年上半年中国智能网联汽车产业投融资情况如图一所示。2016至2021年上半年自动驾驶领域投融资情况如图二所示，自动驾驶的投融资额的年平均增长速度高达345%，成为了近几年最活跃，最有吸引力的细分领域。

● 2016年-2021年上半年自动驾驶领域投融资情况（图二）



资料来源：中国电子信息产业发展研究院赛迪智库《2021年智能网联汽车投资环境和融资水平报告》



互联网科技公司争相涌入 智能网联汽车赛道

除了传统车企外，BAT 互联网三巨头，华为、小米、360 等知名厂商也纷纷加入了“造车”热潮。各厂商在进军汽车细分领域中避开了硬件设计，整车制造等传统车企优势领域，转而聚焦在智慧出行、人工智能驾驶、道路及智能网联设施建设等生态领域，从而与传统车企进行协作互补。

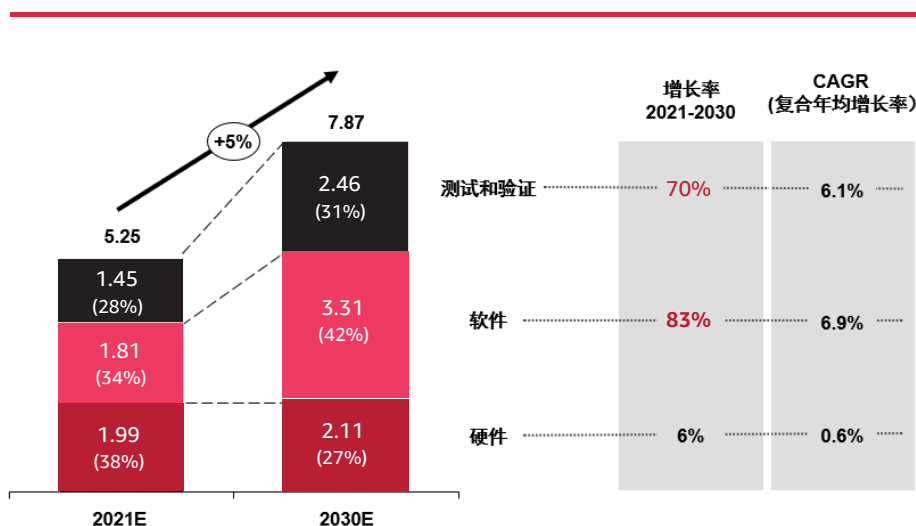
科技公司	聚焦领域
腾讯	车载娱乐与智慧出行
百度	AI 人工智能与自动驾驶
阿里	投资与物流
华为	通讯模组、芯片与操作系统

相比国内市场，海外科技巨头大多聚焦于自动驾驶领域。亚马逊旗下的公司 Zoox 发布的 Robotaxi 主要用于商业用途，为城市提供网约车服务；谷歌旗下的 Waymo 携手吉利控股集团提供无人驾驶专属车辆，后续将在美国进行商业化运营，将无人驾驶出租车部署到全美各地；苹果公司与现代合作的自动驾驶电动车也正在紧锣密鼓地谈判中。

智能网联汽车发展现状分析之数字技术驱动汽车行业的创新发展

随着越来越多的非传统车企涌入智能网联汽车赛道，我国的汽车发展进程已经迈入了新的里程碑，**即软件定义架构：从硬件为主到软硬分离，软件逐渐成为竞争核心。**

● 豪华汽车技术和功能投资的成本分析（图三）



注：以上投资成本不包括生命周期支持的开发成本

资料来源：普华永道思略特基于豪华汽车技术和功能投资的成本分析

长期以来，在传统汽车架构框架下，汽车是主要由硬件及其相关功能定义的设备，软件只是附着于硬件的服务角色。但随着智能网联变革趋势的推动，以及以科技造车新势力纷纷入局，硬件主导汽车的观点正在悄然发生变化，硬件正在走向标准化、抽象化，配置在相同硬件平台上的软件体验成为区分品牌和产品的差异化的关键所在。

根据《普华永道思略特 2020 年数字化汽车报告》、《普华永道思略特 2021 年数字化汽车报告》分析显示，到 2030 年，软件在消费者感知价值中的占比将达 60%，无人驾驶技术推动的新型拥车模式的发展将进一步提升这一比例。未来 10 年，随着用户期望提升和汽车新功能涌现，软件开发成本将增长 83%，几乎翻倍，行业将真正走入“软件定义汽车”的时代，只有打造软件驱动的车企才能在复杂多变的市场中持续捕获价值。

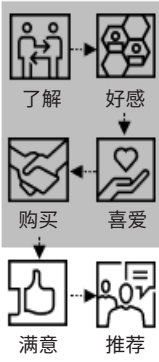
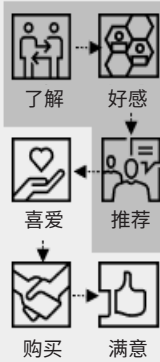
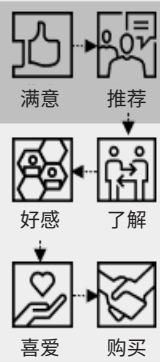


I 智能网联汽车发展现状分析之营销服务创新：以用户直联和私域运营带动业务增长和服务体验提升

从外部环境看，随着中国汽车市场逐步转向存量市场，公域流量见顶，汽车行业的营销压力与日俱增，传统的营销套路难以为继。2020年以来，移动互联网月活跃人数停滞在11.5亿，流量见顶导致汽车企业的公域获客成本以每年20-40%的速度增长，流量造假和网络灰产导致这一情况进一步恶化。

车企一度寄希望于精准营销，然而跨媒体平台的数据打通、媒体平台自身数据精准度不足、标签不合用等问题仍然困扰着企业。个人信息的获取难度增大，可能导致精准营销的效果将进一步下降。与此同时，用户本身和媒体平台也在不断分化演变，随着自媒体、信息流、短视频等崛起，消费者对垂直媒体的依赖度逐渐降低，而短视频平台上以种草、带货KOL为中心的打法，其影响力和转化能力可能超过任何一位顶尖的销售顾问和行业专家；车企数字营销体系也需要不断快速迭代更新。

◎ 不同模式下的战略、用户行为、目标和运营分析（图四）

	传统车企： 传统模式	某传统车企新品牌： 粉丝模式（探索）	某新势力车企	
战略定位	<ul style="list-style-type: none"> 主要关注如何让用户从“关注者”发展为“客户” 	<ul style="list-style-type: none"> 目前处于探索期，现阶段主要关注如何让用户从“关注者”发为“裂变传播者” 	<ul style="list-style-type: none"> 更关注如何让核心车主满意，成为涟漪的中心 	
理想用户行为				<p>共同之处</p> <ul style="list-style-type: none"> 用户运营直接目标与车辆销售脱钩 更加关注潜在客户、车主口碑扩散等长链条变现目标 为此加强用户直联，不断提升用户体验
目标及KPI	<ul style="list-style-type: none"> 提升新用户转化率促进购买 	<ul style="list-style-type: none"> 促进新用户提升好感，裂变传播 促进粉丝群增长，积累线索 	<ul style="list-style-type: none"> 提升老用户满意度 促进老用户推荐新用户进入车企朋友圈，获得大量潜客 促进老用户转化潜客 	
运营重点	<ul style="list-style-type: none"> 寻找潜在用户 促成：识别高意向用户并促进成交 促熟：促进低意向用户向高意向转化 	<ul style="list-style-type: none"> 目前处于探索期现阶段主要关注如何让用户从“关注者”发展为“裂变传播者” 	<ul style="list-style-type: none"> 在现有用户群识别核心用户 重点维护老用户，提升老用户满意度，激发老用户推荐 帮助老用户方便，有效地推荐（推荐新用户、同化现有用户） 	

资料来源：普华永道《车企上云之路白皮书》

传统模式下，用户价值战略定位以潜客转化为主，以推动潜客沿着“了解—好感—喜爱—购买”链条迁移为核心运营逻辑。某造车新势力则在汽车行业里首次落地了挖掘用户影响力的涟漪模式，并判断车主影响力更为强大，以围绕车主的“满意—推荐”作为最核心的运营逻辑，从而将车主裂变拉新和同化转化粉丝潜客的影响力最大化。新一轮互联网造车势力预计也会将其差异化的互联网用户运营逻辑引入到汽车行业。



亚马逊云科技汽车行业解决方案

亚马逊云科技开发了一套非常完整的汽车专用服务和解决方案,涵盖软件定义车辆、车联网、自动驾驶、数字客户互动、制造、供应链和车辆工程。亚马逊云科技通过 AI/ML、IoT、高性能计算 (HPC) 和数据湖的最大功能集以及亚马逊和具有深厚行业专业知识的亚马逊云科技合作伙伴的全球网络支持行业的数字化转型。

亚马逊云科技汽车行业解决方案（图五）

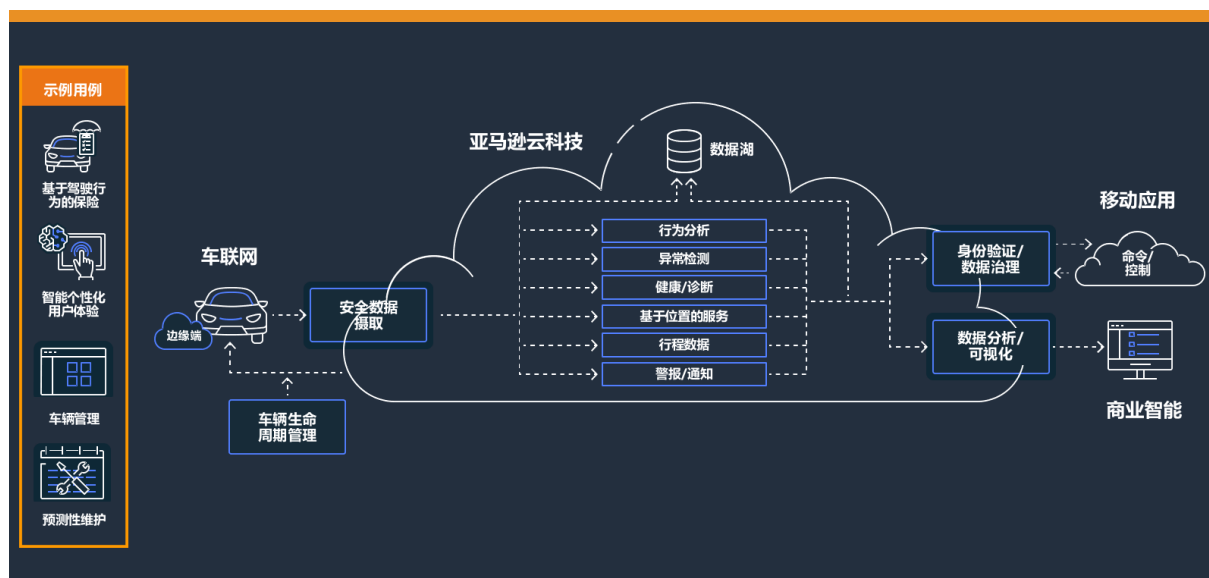


在智能网联汽车产业中，车联网和自动驾驶是最重要的两个解决方案。

亚马逊云科技车联网解决方案支持车辆内本地计算、复杂的事件规则以及数据处理和存储功能。该解决方案旨在提供一种车联网服务框架，让您能够专注于扩展解决方案的功能，无需过多的管理底层基础设施的运行。您可以基于这个框架来构建应用程序以用于各种使用场景，例如语音交互、导航及其他基于位置的服务、远程车辆诊断和运行状况监控、预测性分析和必需的维护通知、媒体流服务、车辆安全服务、汽车音响主机应用程序以及移动应用程序。

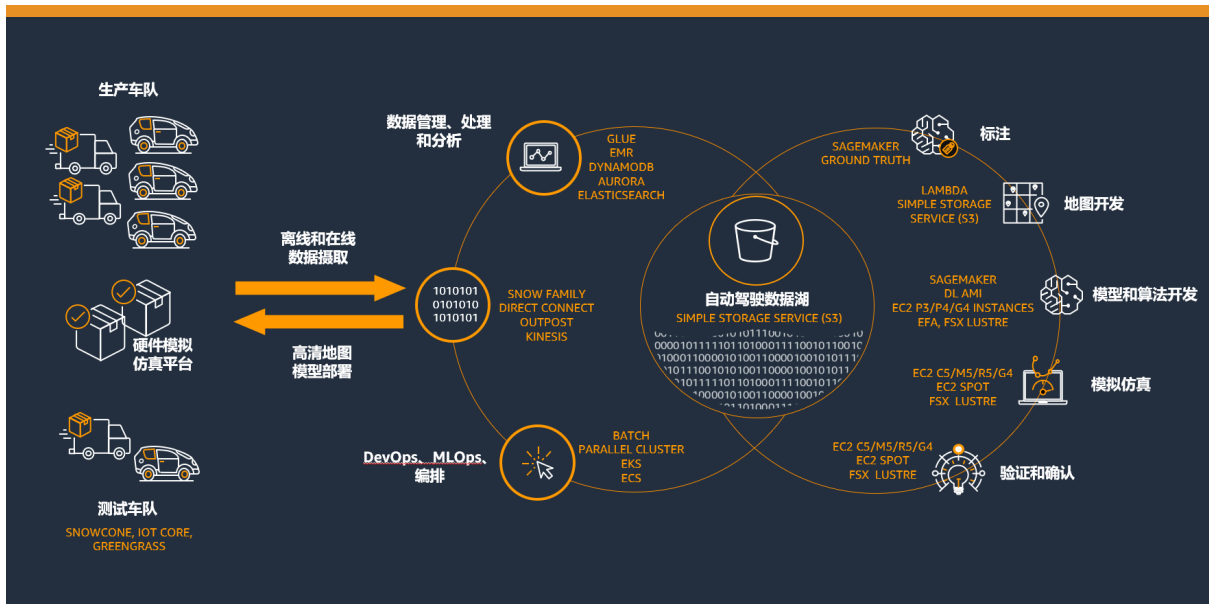


● 亚马逊云科技汽车联网解决方案（图六）

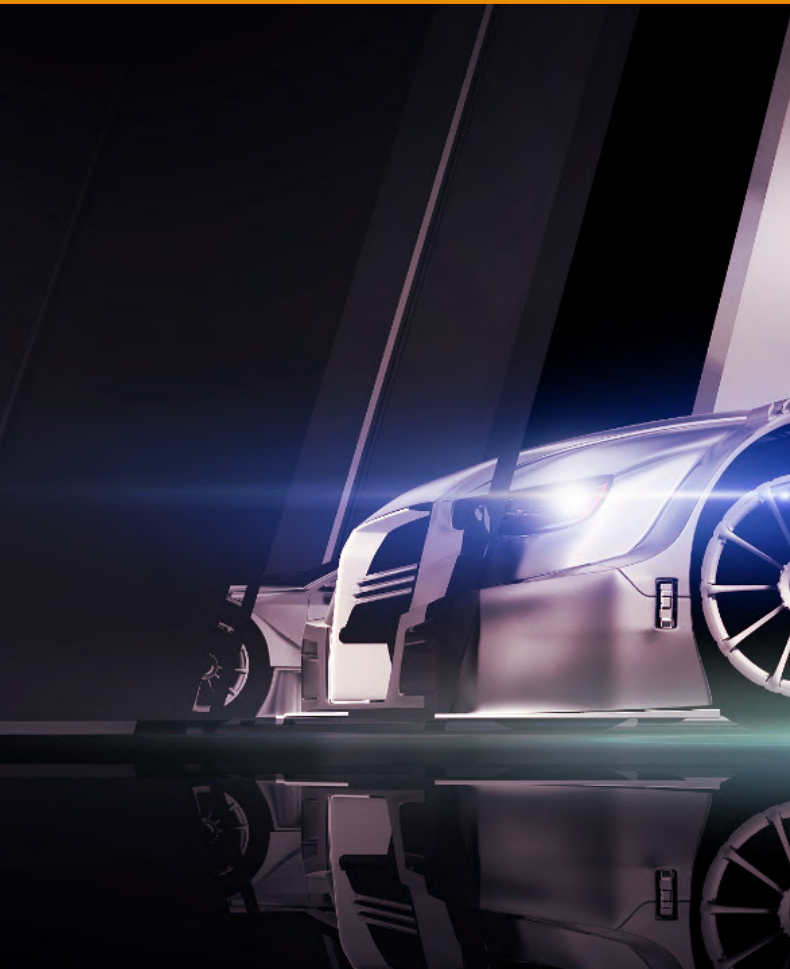


开发和部署高级驾驶辅助系统（ADAS）和自动驾驶（AV）系统需要一个具有高度可扩展的计算、存储、网络以及分析和深度学习框架的开发平台。该平台需要允许收集、摄取、存储、处理和分析、标记和注释、地图开发、算法和模型开发、模拟、验证和确认以及工作空间管理功能（包括 MLOps 和 DevOps）的功能。领先的汽车客户将亚马逊云科技作为他们的 ADAS/AV 开发平台，以利用我们广泛而深入的托管服务、解决方案、经验和合作伙伴社区，以提供开发安全、可靠和成本优化的自动驾驶和 ADAS 所需的架构和技术系统。

● 亚马逊云科技汽车自动驾驶解决方案 (图七)



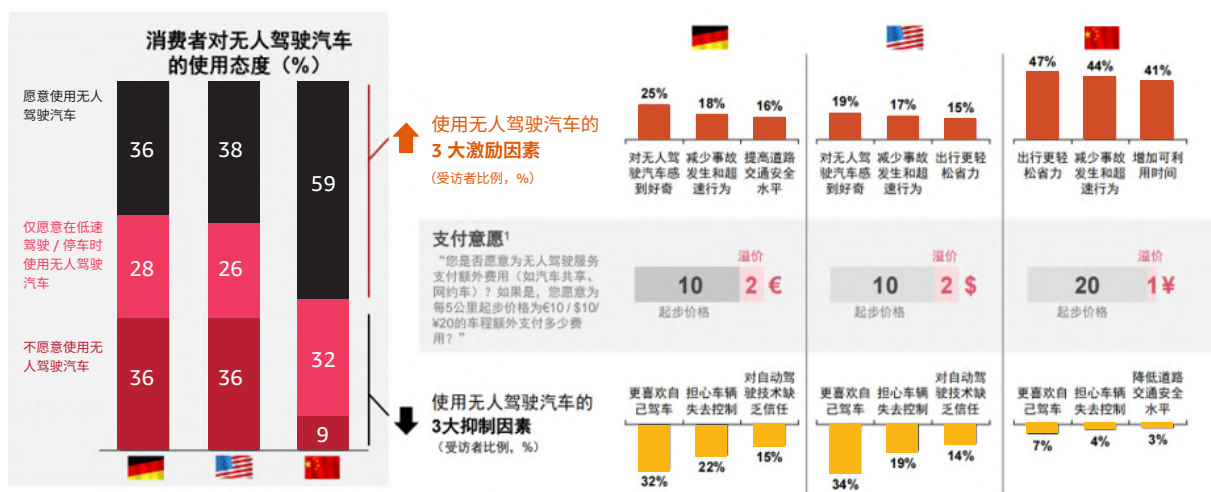
智能网联汽车数字化 技术融合进程中带来 的挑战与应对



随着电动化、自动化、网联化、共享化进程的深入，中国汽车产业正走入急剧变化和充满挑战的时代。新四化与数字化技术力量相互驱动和融合，正迅速重构着汽车产业的游戏规则和致胜能力，并改造了从产品研发、制造，再到营销和服务等每个价值链环节。这背后也考验着车企对于云计算、大数据、人工智能等数字技术的认识和运用能力，落后者很难在全新的市场环境中形成竞争优势，甚至面临严峻的生存挑战。

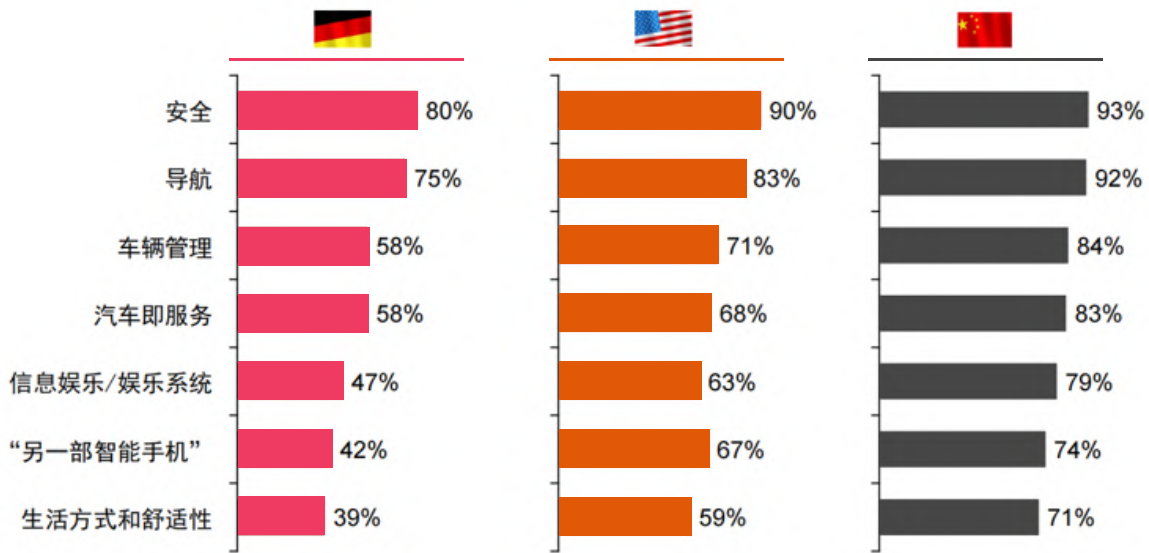
以自动驾驶为例，《普华永道思略特 2021 年数字化汽车报告》中对德国，美国，中国汽车市场消费者进行了调查。调查显示，64% 的德国人与美国人愿意尝试无人驾驶，而在中国更有超过 90% 的比例。各国消费者对新鲜事物的尝试，以及无人驾驶的便利程度给市场带来了潜力与机会。但是，无人驾驶过程中是否“安全”也成为了消费者们考虑的主要因素，无人驾驶的消费者态度、影响因素和支付意愿分析如图五所示，不同国家（中美德）对互联服务功能的倾向性如图八所示。

● 无人驾驶的消费者态度、影响因素和支付意愿分析（图八）



资料来源：《普华永道思略特 2021 年数字化汽车报告》

不同国家（中美德）对互联服务功能的倾向性（图九）



资料来源：《普华永道思略特 2021 年数字化汽车报告》

由此可见，车辆安全已经成为车主在购买车辆时最为关心的要素之一。在此背景下，世界各地的监管机构陆续出台了相关的法律法规，加强了对车辆安全的保护。在汽车出海的大浪潮下，各车企需要面临车辆相关法律法规带来的愈发严峻的合规挑战。如下表所示，出海车企主要需要应对车辆网络安全、车辆软件升级与个人信息保护三方面的合规要求。

本章节将会把重点放在下表所述的三大法规标准的解读以及针对车企应该如何应对提供我们的洞见。

● 海外汽车安全相关主要法规标准

领域	法规 / 标准名	生效时期	适用范围	强制 / 推荐
车辆网络安全合规	联合国 WP.29 R155 车辆网络安全管理体系	2021.01	58 协议国	强制
	ISO 21434 道路车辆 - 网络安全工程标准			推荐
车辆软件升级合规	联合国 WP.29 R156 软件升级管理体系	2021.01	58 协议国	强制
	ISO 24089 道路车辆 - 软件升级工程标准 (DIS)			推荐
个人信息保护	欧盟通用数据保护条例 (GDPR)	2018.05	欧盟各国	强制
	车联网个人数据保护指南			推荐

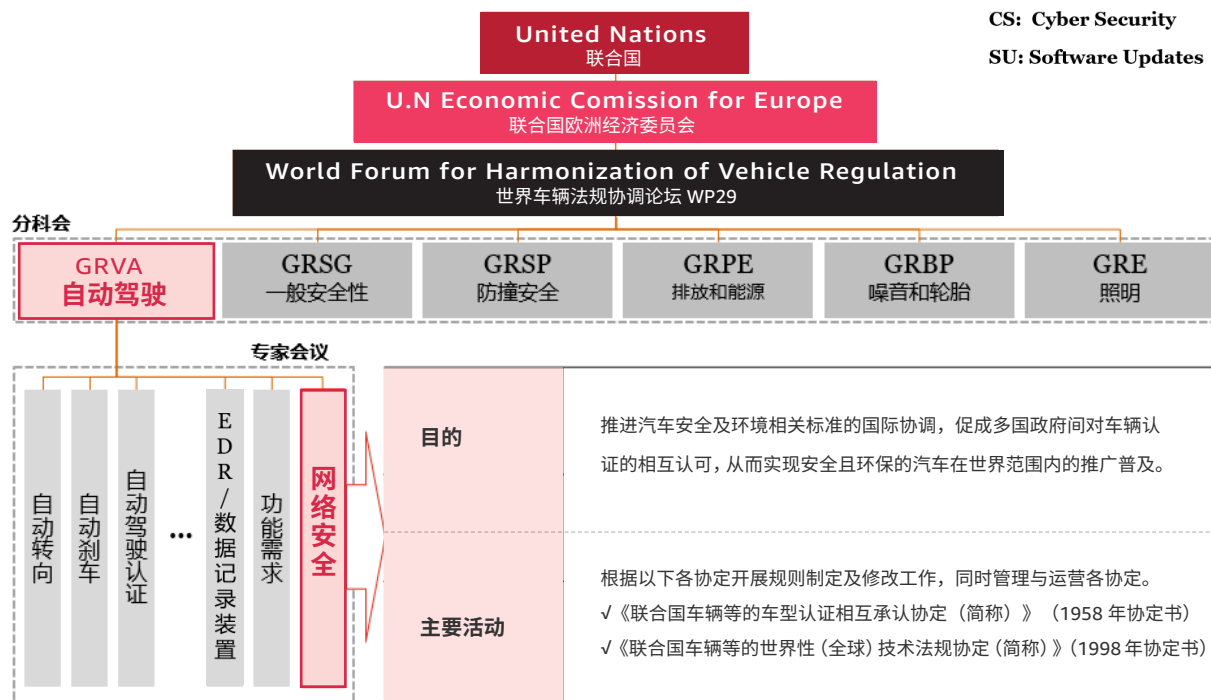


车辆网络安全与软件升级合规

● WP.29 世界车辆法规协调论坛简介

WP.29 全称为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一个国际组织。WP.29 内针对不同的领域分别成立不同的管理委员会，作为其工作的领导层面。WP.29 下的 GRVA 的主要任务是汽车网络安全的法规的探讨与制定，其中包含 R155（车辆网络安全）以及 R156（车辆软件升级）等，其法规的主要适用范围包括了欧洲 / 日本 / 韩国等 ‘1958 协议’ 缔约国（以下简称 “58 协议国”）。

● WP.29 世界车辆法规协调论坛简介（图十）

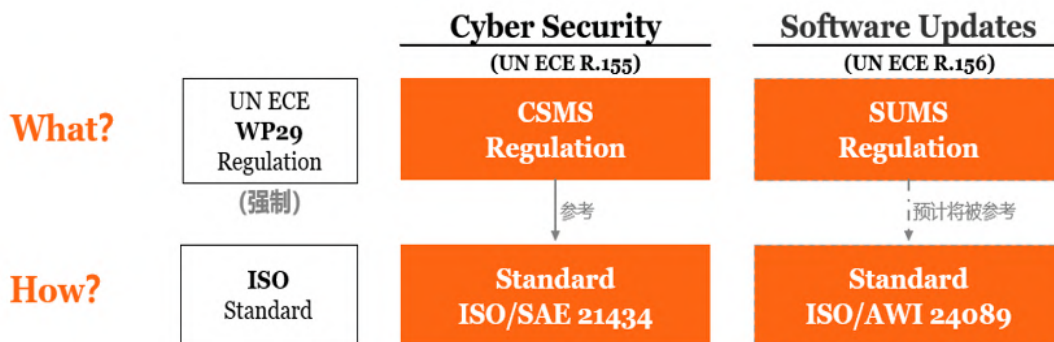
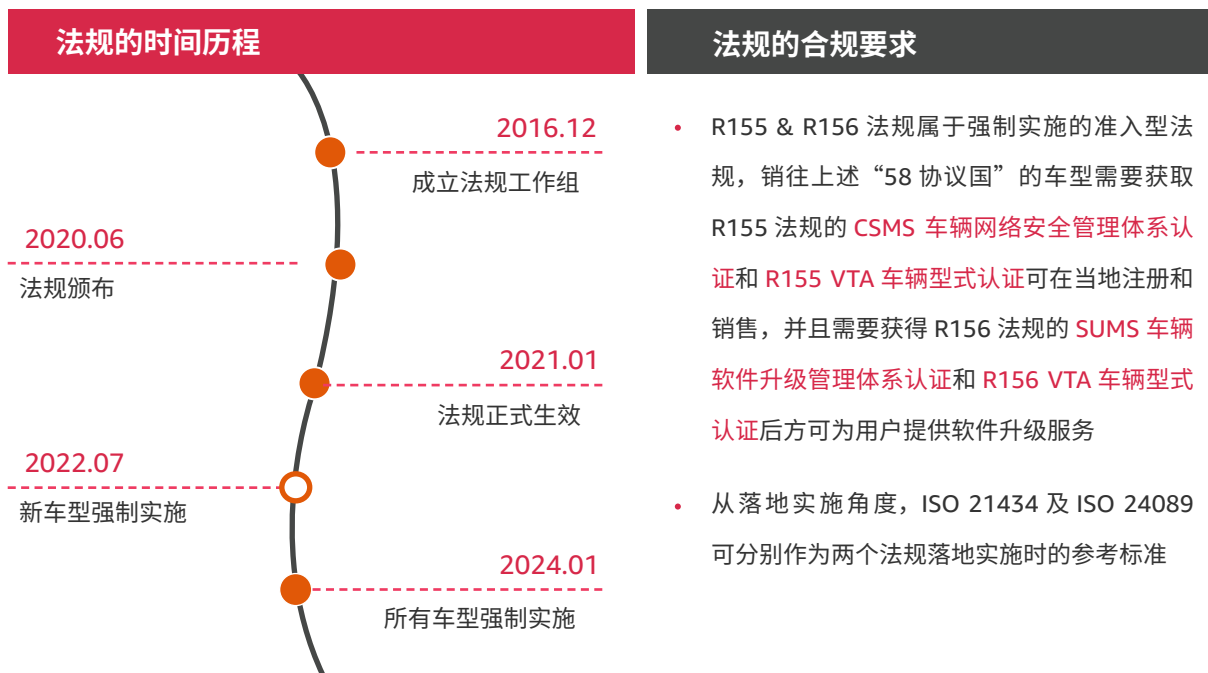


* 由普华永道根据各种公开信息创建

出典：https://unece.org/trans/main/wp29/meeting_docs_wp29.html

● WP.29 R155 & R156 法规概要

● R155 & R156 法规概要 (图十一)



● R155 合规要求解读

1. CSMS 车辆网络安全管理体系认证

搭建能够映射到法规要求的 CSMS 车辆网络安全管理体系，并有效运行。

■ CSMS 证书获取条件

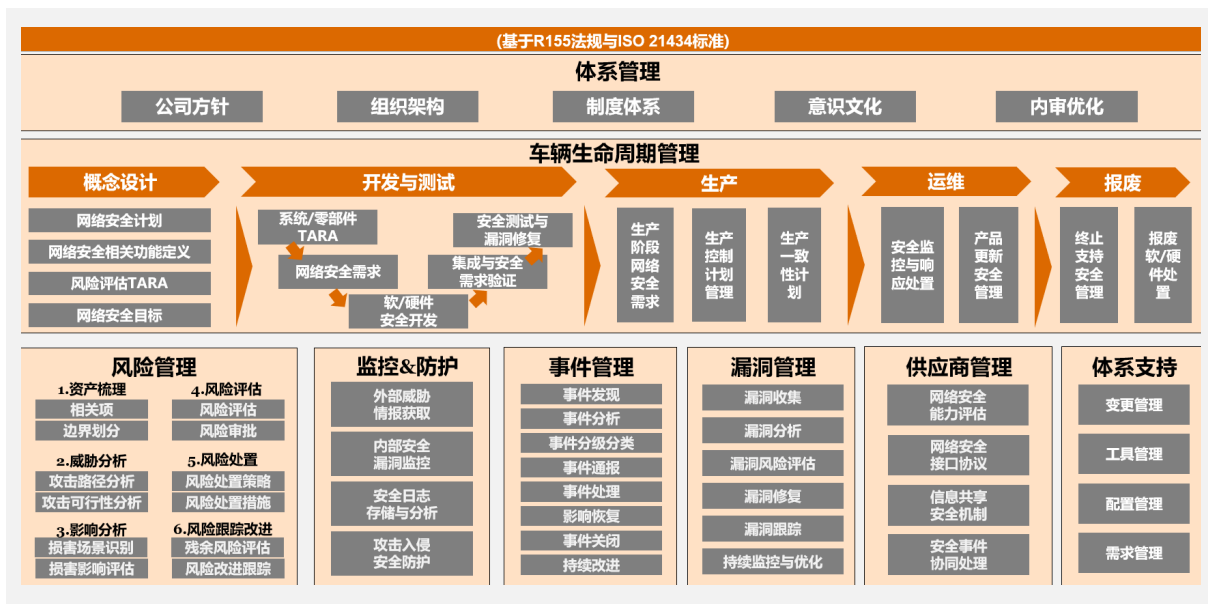
- 主机厂 OEM 签署《制造商 CSMS 合规声明》以向认证机构或技术服务机构证明其已经开始运行能够符合规定的网络安全管理体系流程，并且持续维护；
- 授权认证机构对主机厂进行评估后，判断主机厂已发布一系列符合规定条款的 CSMS 文件且有符合 R155 网络安全要求的一系列流程。

■ CSMS 证书维护条件

- 认证机构可随时查验已发放的 CSMS 证书，若查验其不符合要求，可随时撤销认证；
- CSMS 证书每三年定期评估一次，经认证机构再次评估后确认是否延长证书有效期或重新发放证书；
- 若主机厂在变更过程中存在与 CSMS 相关的变更，应及时告知认证机构并沟通确认是否需要重新评估。



● CSMS 实施框架 (图十二)



2. R155 VTA 车辆型式认证

在具体车型上开展必要的网络安全活动，如 TARA（车辆网络安全威胁分析与风险评估）等，并保留记录。

■ VTA（车辆型式认证）申请

提交材料：

- 需提交已经通过的 CSMS 合规证书；
- 需提交信息文档声明中的车型说明部分；
- 若需提交的信息有包含车企机密的知识产权或技术，应提供经处理后的信息供审核。

车型技术审核：

- 认证机构单独或与主机厂协同对车型进行抽样测试，以确认车辆制造商实际落实了其记录的网络安全需求。

● R155 车辆网络安全 VTA 框架（图十三）



● R156 合规要求解读

1. SUMS 车辆软件升级管理体系认证

搭建能够映射到法规要求的 SUMS 车辆软件升级管理体系认证，并在某车型上有效运行。

■ SUMS 证书获取条件：

- 主机厂已搭建符合标准的 SUMS 管理体系，能够从软件升级管理，基础设施设计开发，车辆系统设计开发，软件包开发及软件升级活动管理，全面科学有效管理车辆软件升级中的风险；
- 主机厂在现有的软件升级管理流程中导入 SUMS 体系，并在某车型落实 R156 认证要求。

■ **SUMS 证书维护条件：**

- 认证机构可随时查验已发放的 SUMS 证书，若查验其不符合要求，可随时撤销认证；
- SUMS 证书每三年定期评估一次，经认证机构再次评估后确认是否延长证书有效期或重新发放证书；
- 若主机厂在变更过程中存在与 SUMS 相关的变更，应及时告知认证机构并沟通确认是否需要重新评估。

2. R156 VTA 车辆型式认证

在具体车型上开展必要的软件更新活动，并保留相关记录

■ **VTA (车辆型式认证) 申请**

需保证

- 已通过 SUMS 认证并可用于道路车型；
- 能够读取车辆的软件识别号 (RXSWIN) 并对其进行保护；
- 通知车主软件更新情况；
- 确保软件更新传输机制的完整性和真实性；
- 能够进行远程软件更新并在更新失败时恢复旧版本或进入安全状态等。

● 软件升级各个环节所要满足的合规要求 (图十四)



● 车辆型式认证适用车型范围

R155 & R156 法规将对象车型分为 M 到 T 六种车辆类型，具体车辆类型可参考下图。

● VTA 车型认证适用车辆类型（图十五）

车辆类型	概要
M 	• 以运载乘客为目的、4轮以上安装有发动机的车辆（小汽车、大巴等）
N 	• 以运输货物为目的、4轮以上安装有发动机的车辆（卡车、翻斗车、牵引车等）
O 	• 半挂车、全挂车
R 	• 农林业用挂车
S 	• 功能性农业·林业用挂车
T 	• 农林业用拖拉机

  两轮车不包括在对象车辆类型内

● 各车企法规应对现状

在海外法规层面，目前针对 R155 体系层面的认证，第一批中国出海车企正在积极响应中，其中部分车企已经率先获得 R155 体系认证，而其他车企也都相继进入到预审核的阶段；而由于车企研发周期普遍较长，VTA 车辆型式认证方面的工作还在有条不紊地进行中。

同时，由于 R156 生效条件还存在不确定因素，出海车企针对 R156 的应对节奏整体晚于 R155。但是各大头部车企均已将法规认证提上日程，于去年年底今年年初积极立项，启动法规应对。

在国内法规层面，国家强制性标准《汽车整车信息安全技术要求》与《汽车软件升级通用技术要求》已分别于 2021 年立项，预测计划于 2022 年底发布。相比 R155 & R156，国内标准还补充定义了车型认证的

试验方法，对主机厂及评测机构软件升级认证的落地提供了强有力的指导。在此背景下，一些无出海业务的头部合资主机厂也开始针对国内即将出台的法规积极开展对应，进行差距分析和体系建设规划工作。

另一方面，零部件供应商们也开始立项进行 ISO 21434 的合规应对工作，以此来应对和满足主机厂在车辆网络安全相关领域的合规要求。



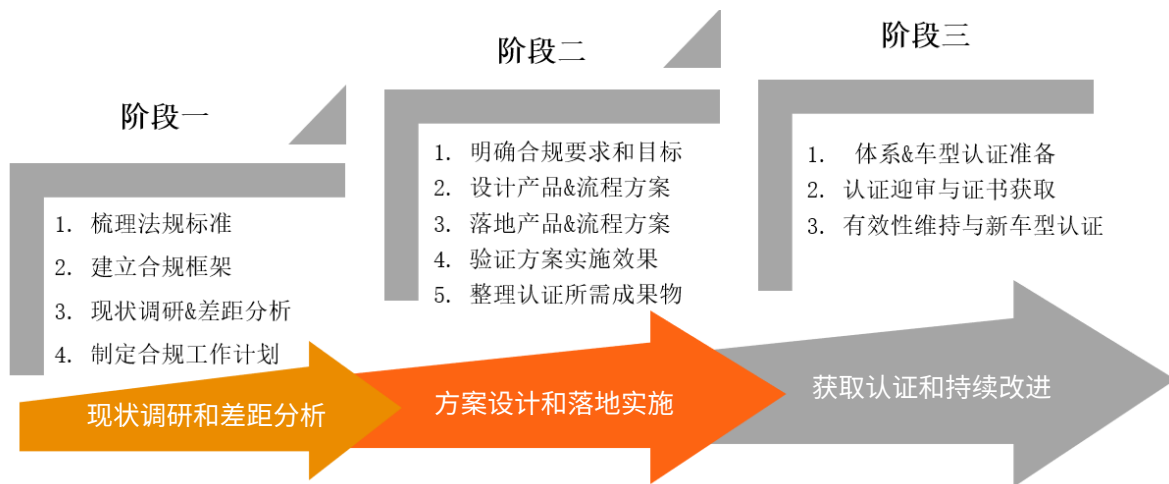
● R155 & R156 合规应对解决方案

近年来，普华永道积极参与车辆网络安全，车辆软件升级和自动驾驶国内外法规和标准的起草和制定。同时基于扎实的技术沉淀、丰富的全球专家资源以及行业前沿技术洞察，为多家主机厂和供应商提供专业的车辆网络安全、车辆软件升级和隐私保护咨询服务，积累了**丰富的出海合规实践经验**。并在全球各地开设60余个网络安全实验室，并在中国广州率先引入和创建专业的**车联网实验室**。普华永道结合中国、日本及德国团队的丰富经验，至今已为多家车企提供专业的

智能网联和自动驾驶咨询服务，助力汽车行业的高速合规发展。

为了让车企更系统、高效地应对车辆软件升级的法规和标准，提升自身的软件升级管理水平和技术能力，普华永道建议企业在合规应对工作上分三步走。

● 普华永道合规应对步骤（图十六）



在阶段二的实施落地的过程中，普华永道团队携手拥有大量海外车云项目经验的亚马逊云团队，为客户提供更加高效落地的合规应对方案。作为汽车行业数字化转型的关键推动者，亚马逊云在全球有多达 185+ 的汽车云伙伴，为全球前 10 的 OEM 主机厂、全球前 10 的供应商和全球排名前 5 的汽车科技公司提供专业的服务来协助车企完成合规挑战。



个人信息保护合规

GDPR 通用数据保护条例概要

GDPR 法规概要 (图十七)



● GDPR 合规要求解读

1. GDPR 的适用范围

- 在欧盟境内设有业务机构的组织，只要这些业务机构在欧盟境内的活动中处理个人数据。（属地）
- 如某一组织虽不在欧盟境内设立业务机构，但却处理欧盟境内个人（欧洲居民）的个人数据，并且此类处理行为与向欧盟居民提供商品或服务相关，无论该等商品或服务是否收费，则也应当适用 GDPR。（属人）

2. GDPR 中的关键角色

- **数据控制者**：指单独或者与他人共同确定个人数据处理的目的、条件和手段的自然人、法人、公共机构、政府部门或其他机构。如针对用户在车企 app 或者电商平台、网站的注册信息，企业是数据控制者。
- **数据处理者**：指代表数据控制者处理个人数据的自然人、法人、公共机构、政府部门或其他机构。如企业针对企业客户提供服务、提供产品所协助处理或者存储的数据，是数据处理者，比如云基础设施提供商、自动驾驶服务提供商等。

3. GDPR 数据主体权利

- GDPR 中对于包括知情权、访问权、更正权、删除权（被遗忘权）、限制处理权、数据可携权、拒绝权、不受制于自动化决策权在内的 7 项权利进行了规定。

4. GDPR 个人数据处理七原则

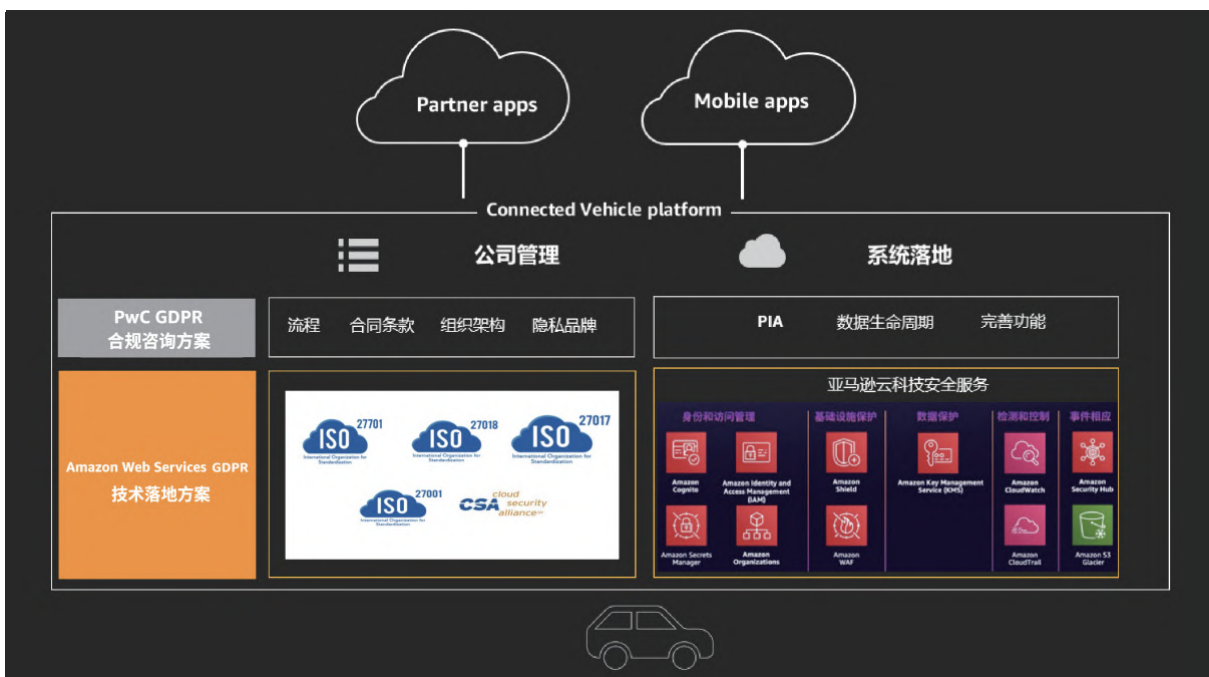
原则	原则描述	合规解读	适用的角色	
			数据控制者	数据处理者
合法、正当、透明	<ul style="list-style-type: none"> 数据主体的个人数据应当以正当、合法、透明的方式被处理 	<ul style="list-style-type: none"> 个人数据、敏感数据、儿童数据、雇主数据 记录同意、撤回同意 正当性：提供信息（隐私通知） 透明性：提供信息的方式 	√	N/A
目的限制	<ul style="list-style-type: none"> 个人数据应当基于具体、明确、合法的目的收集，不应以与此目的不相容的方式进一步处理 	<ul style="list-style-type: none"> 新目的合法性 匿名化 	√	N/A
数据最小化	<ul style="list-style-type: none"> 处理的个人数据应与处理数据的目的是适当、相关且必要的 	<ul style="list-style-type: none"> 充分、不超乎适度、必要 	√	N/A
准确性	<ul style="list-style-type: none"> 个人数据应当是准确的，并在必要的情况下及时更新 根据数据处理的目的，采取合理的措施确保及时删除或修正不准确的个人数据 	<ul style="list-style-type: none"> 数据的准确性 	√	N/A
存储期限最小化	<ul style="list-style-type: none"> 存储个人数据不超过处理目的所必要的期限 	<ul style="list-style-type: none"> 留存、销毁方式 	√	N/A
完整性与保密性	<ul style="list-style-type: none"> 采取必要的技术或组织措施确保个人数据的适度安全，包括防止未授权或非法处理个人数据、数据丢失或毁损 	<ul style="list-style-type: none"> 风险评估、技术与组织措施、加密、化名、访问控制、监控数据泄漏 	√	√
可归责	<ul style="list-style-type: none"> 数据控制者需负责且能展示遵从上述原则 	<ul style="list-style-type: none"> 记录政策与流程、数据处理活动 	√	√

5. GDPR 罚则

GDPR 中规定，违反对数据控制者和处理者的要求，如 PbD、数据处理记录、安全保护、数据泄露通知、DPIA、DPO 等，处以 1000 万欧元或全球营业额的 2% 的处罚；而违反数据处理基本原则，包括同意等、违反数据主体权利保障要求、违反跨境数据转移要求、未遵守监管机构的数据处理限制，拒绝执法调查等或违反各成员国法律基于 GDPR 授权规定的特定场景下数据处理要求时，处以 2000 万欧元或高达全球营业额的 4% 的处罚。所以各车企需对 GDPR 合规予以高度重视，避免因违反 GDPR 合规要求而遭受到严重的经济损失。

● GDPR 通用数据保护条例应对之道

● 普华永道 & 亚马逊云解决方案 (图十八)



为了更好地站在企业的角度梳理及明确合规义务，有条理、体系化地应对 GDPR 下新的合规工作，普华永道结合亚马逊云科技成熟的技术落地能力，从公司管理及系统落地两个层面帮助企业客户梳理以及解决业务场景下的合规风险。

1. 公司层面

首先，在组织架构层面，普华永道帮助客户梳理和完善现有架构，例如数据保护官（DPO- Data Protection Officer）的设置，制定相关 KPI 以及完善组织和人员能力；其次，从合同条款层面，帮助客户拟定符合 GDPR 要求的相关条款及整改建议，除隐私政策外还包括中国和海外分公司间的数据跨境标准合同条款（SCC – Standard Contractual Clauses）、和第三方合作伙伴间的数据处理协议（DPA – Data Processing Addendum）等，结合亚马逊与客户签署的 GDPR DPA 数据处理附录中的标准条款，能够更好的约束和规范在 GDPR 要求下各自的权利和责任；最后，协助客户搭建完备的制度流程体系，包含将隐私保护融入研发流程（PbD - Privacy by Design）、设计应急响应规范等。

2. 技术落地

普华永道基于 GDPR 的要求，结合亚马逊的自动化工具以及大量过往项目中的经验，协助客户识别云、管、端各系统 / 功能（包括 TSP、CRM、DMS、智能驾舱等）所收集的个人信息（Amazon Macie），通过个人信息影响评估（PIA）持续进行风险与合规分析，梳理数据全生命周期中的合规差距并提供技术落地方案：如加密传输 / 加密存储，云端审计功能（Amazon Audit Manager）等。



● 亚马逊云科技的安全与合规

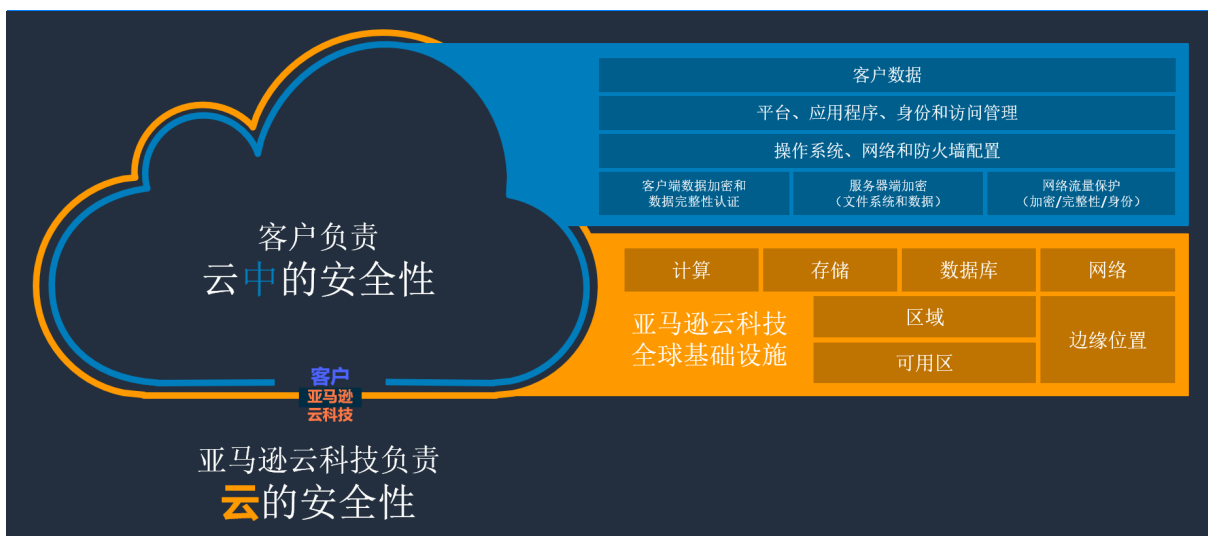
1. 责任共担模型

安全性和合规性是亚马逊云科技和客户的共同责任。

当车企客户将他们的计算机系统和数据迁移到亚马逊云科技时，客户和亚马逊云科技之间会分担安全责任。亚马逊云科技负责保护运行亚马逊云科技中提供的所有服务的全球基础设施。对于非实例化的服务，例如 Amazon S3 和 Amazon DynamoDB，亚马逊云科技还负责操作系统和平台的安全。作为数据控制者或数据处理者的客户和 APN 合作伙伴对他们放入云中或连接到云的任何内容负责。这种责任区分通常被称为云的安全性与云中的安全性。这种共享模型可以帮助减轻

车企客户的运营负担，并为他们提供必要的灵活性和控制力，以便在亚马逊云科技中部署他们的基础设施。GDPR 不会改变亚马逊云科技的责任共担模型，该模型继续与专注于使用云计算服务的客户和 APN 合作伙伴相关。责任共担模型是一种有用的方法来说明亚马逊云科技（作为数据处理者或子处理者）和客户或 APN 合作伙伴（作为数据控制者或数据处理者）在 GDPR 下的不同责任。

● 亚马逊云科技安全责任共担模型（图十九）



2. 亚马逊云科技的安全合规

亚马逊云科技在我们所有的全球运营中持续保持高标准的安全性和合规性。安全一直是我们的重中之重——真正的“零工作”。亚马逊云科技定期接受独立的第三方证明审计，以确保控制活动按预期运行。更具体地说，亚马逊云科技会根据区域和行业的各种全球和区域安全框架进行审计。目前，亚马逊云科技参与了 50 多个不同的审计计划。

这些审核的结果由评估机构记录，并通过 Amazon Artifact 提供给所有亚马逊云科技的客户。Amazon Artifact 是一个免费的自助服务门户，用于按需访问 Amazon Artifact 提供给所有亚马逊云科技合规性报告。当新报告发布时，它们会在 Amazon Artifact 中提供，从而允许客户通过立即访问新报告来持续监控 Amazon Artifact 提供给所有亚马逊云科技的安全性和合规性。

客户可以利用国际公认的认证和认可，证明其符合严格的国际标准，例如云安全的 ISO 27017、云隐私的 ISO 27018、SOC 1、SOC 2 和 SOC 3、PCI DSS 1 级等。亚马逊云科技还帮助客户满足当地安全标准，例如 BSI 的通用云计算控制目录 (C5)，这是德国政府支持的证明。

有关亚马逊云科技认证计划、报告和第三方证明的更多详细信息，请参阅亚马逊云科技合规计划（<https://aws.amazon.com/cn/compliance/programs/>），有关特定于服务的信息，请参阅合规范围内的亚马逊云科技服务（<https://aws.amazon.com/cn/compliance/services-in-scope/>）

◎ 亚马逊云科技安全服务产品概览（图二十）



3. 亚马逊云科技针对 GDPR 的准备

亚马逊云科技自身在 2018 年 5 月 25 日的执行期限前两个月完成 GDPR 服务就绪审核的全部工作。亚马逊云科技已经宣布，所有亚马逊云科技的云服务都可以按照通用数据保护条例 (GDPR) 使用。这意味着，除了受益于亚马逊云科技已经采取的所有维护服务安全的措施之外，客户还可以将亚马逊云科技的服务作为其 GDPR 合规计划的关键部分进行部署。他们可以和亚马逊云科技的合作伙伴共同部署环境，自信地在亚马逊云上构建属于自己的与 GDPR 兼容的产品、服务和解决方案。



■ 亚马逊云科技数据处理附录 (DPA)

亚马逊云科技提供了一项符合 GDPR 的数据处理附录 (GDPR DPA)，使客户能够符合 GDPR 合同义务。亚马逊云科技 GDPR DPA 包含在亚马逊云科技服务条款中，自动适用于需要亚马逊云科技遵守 GDPR 的全球所有客户。

根据 GDPR 的规定，亚马逊云科技既是数据处理者，也是数据控制者。亚马逊云科技作为数据处理者，GDPR 第 32 条规定，控制者和处理者必须“实施适当的技术和组织措施”，同时考虑到“现有技术和实施的成本与处理的性质、范围、背景和目的，以及处理给自然人的权利和自由带来的不同可能性和严重程度的风险”。

当客户和亚马逊云科技解决方案供应商使用亚马逊云科技服务来处理其内容中的个人数据时，亚马逊云科技充当数据处理者。客户和亚马逊云科技解决方案供应商可以使用亚马逊云科技服务中提供的控制措施（包括安全配置控制措施）来处理个人数据。在这些情况下，客户或亚马逊云科技解决方案供应商可能充当数据控制者或数据处理者，而亚马逊云科技则充当数据处理者或子处理者。亚马逊云科技提供了一项符合 GDPR 的数据处理附录 (DPA)，其中包含亚马逊云科技作为数据处理者的承诺。

当亚马逊云科技收集个人数据并确定处理此类个人数据的目的和方式时，此时它充当数据控制者。例如亚马逊云科技作为数据控制者，可存储账户信息，用于帐户注册、管理、服务访问、客户联系和支持。

亚马逊云科技同时在帮助客户遵守 GDPR 方面提供了特定的功能和服务，它们将有助于客户符合 GDPR 要求：

如下，我们将列举一些服务帮助大家更好的理解：

1. 访问控制：只允许授权的管理员、用户和应用程序访问亚马逊云科技资源，

包括：

- Multi-Factor-Authentication (MFA)
- 对 Amazon S3 存储桶 /Amazon SQS/Amazon SNS 等中的对象的细粒度访问
- API 请求验证
- 地理限制
- 通过 Amazon Security Token Service 获取的临时访问令牌

2. 监控和日志记录：用于获取亚马逊云科技资源相关活动的概况，

包括：

- 通过 Amazon Config 执行资产管理和配置
- 通过 Amazon CloudTrail 执行合规性审核和安全性分析
- 通过 Amazon Trusted Advisor 确定配置方面存在的挑战
- 细粒度记录对 Amazon S3 对象的访问通过 Amazon VPC 流日志获取网络中流量的详细信息



- 通过 Amazon Config 规则执行基于规则的配置检查和操作
- 通过 Amazon CloudFront 中的 Amazon WAF 功能筛选和监视对应用程序的 HTTP 访问

3. 加密：用于在亚马逊云科技上加密数据，包括：

- 使用 AES256 (EBS/S3/Glacier/RDS) 对闲置的数据加密
- 集中化托管密钥管理 (按亚马逊云科技区域)
- IPsec 通过 VPN 网关进入亚马逊云科技
- 通过 Amazon CloudHSM 在云中使用专用 HSM 模块

4. 强大的合规框架和安全标准：用于证明遵守严格的国际标准，例如：

- ISO 27001, 适用于技术措施
- ISO 27017, 适用于云安全性
- ISO 27018, 适用于云隐私性
- SOC 1、SOC 2 和 SOC 3、PCI DSS 1 级
- BSI 的 Common Cloud Computing Controls Catalogue (C5)
- ENS 高级认证

■ CISPE 行为准则

CISPE (Cloud Infrastructure Services Providers in Europe) 是一个云计算的领导者联盟，为数百万欧洲客户提供服务。CISPE 数据保护行为准则 (CISPE Code) 是第一个根据欧盟通用数据保护条例 (GDPR) 第 40 条针对云基础设施服务提供商的泛欧数据保护行为准则。它于 2021 年 5 月获得欧洲数据保护委员会 (EDPB) 的批准，并于 2021 年 6 月由作为主管监管机构的法国数据保护局 (CNIL) 正式采用。

CISPE 准则向组织保证其云基础设施服务提供商满足 GDPR 下适用于数据处理器的要求。这让云客户更有信心，他们可以选择经过独立验证符合 GDPR 的服务。

CISPE 准则超越了 GDPR 合规性，要求云基础设施服务提供商让客户可以选择专门在欧洲经济区内存储和处理客户数据的服务。云基础设施服务提供商还必须承诺，他们不会访问或使用任何客户数据，除非是提供和维护声明的服务所必需的。特别是云基础设施服务提供商必须承诺不将客户数据用于自己的目的，包括用于数据挖掘、分析或直接营销。 (<https://www.codeofconduct.cloud/public-register/>)。

亚马逊云科技支持的安全标准和合规性认证比任何其他云提供商都多，随着监管环境的发展，我们会不断审查客户的需求。CISPE 准则为我们的客户提供了更高级别的保证，即亚马逊云科技的服务可以按照 GDPR 使用，并满足我们客户目前的合规性要求。

■ 来自亚马逊云科技合作伙伴的帮助

您可以在 亚马逊云科技 Partner Solutions Finder 中搜索“GDPR”的功能，以帮助查找拥有有助于实现 GDPR 合规性的产品和服务的 ISV、MSP 和 SI 合作伙伴。客户还可以在 亚马逊云科技 Marketplace 上搜索“GDPR”解决方案。

智能网联汽车未来 发展趋势展望



第四章：智能网联汽车未来发展趋势展望



汽车行业正面临前所未有、来自多方面的挑战。

汽车行业正在形成如下新的趋势，需要引起高度重视。

新技术 - 5G 以及人工智能和机器学习的改进正在催生新的应用场景和服务 - 例如从简单的路端状况通信到更复杂的支持边缘计算的自动驾驶开发场景。

数据监管 - 全球日益严格的数据监管塑造了公司收集、处理和分析客户数据的方式。如果汽车制造商（OEM）能够发现、解锁和共享其客户棘手问题中的数据，则可以将这种能力作为开发切实可行的业务见解和新产品功能的重要资产。

文化 - 随着汽车制造商的发展，许多汽车制造商正在从传统的金属加工公司转变为软件驱动的技术公司。要做到这一点，就需要关注数字人才、创新和敏捷开发。

工业 4.0 - 互联的企业。我们看到围绕互联的企业和行业，甚至全行业数据湖的强劲趋势正在日益形成。企业将其制造工厂连接到机器级别，以更深入了解其运营情况。

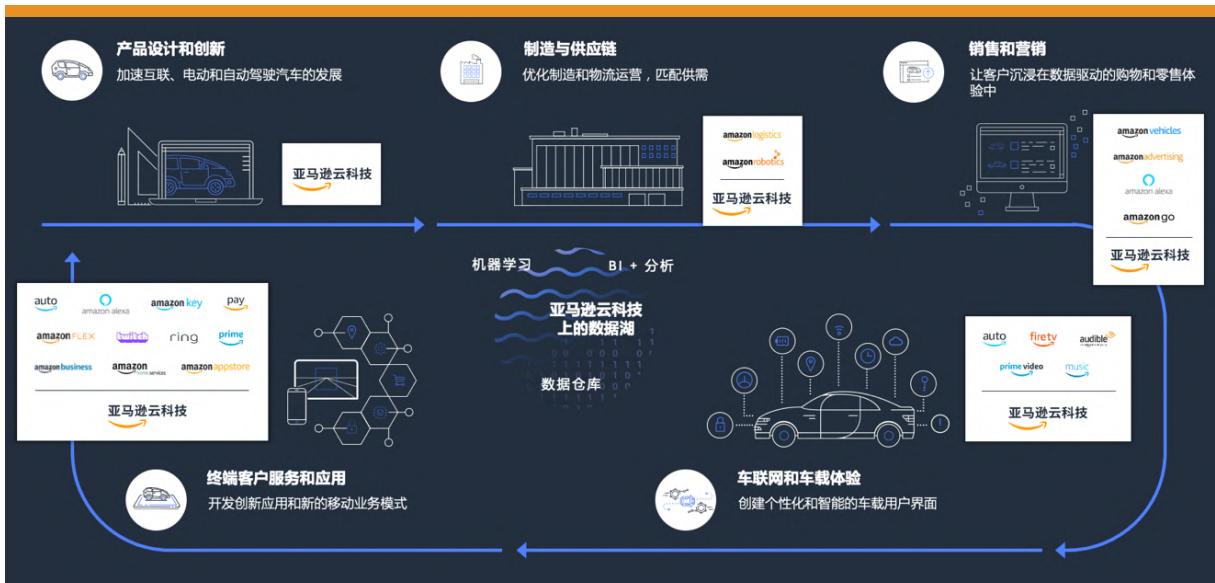
云计算和亚马逊云科技可以支持汽车公司适应并管理这些趋势。通过消除繁重的工作，车企可以专注于品牌差异化并为客户提供创新的产品和服务。

- 新趋势需要管理层引起关注；
- 云通过允许车企专注于品牌差异化来帮助管理这些趋势；
- 云可以帮助车企应对新技术，同时满足严格的数据法规要求 - 车企可以随时控制数据。

目前，大多数车企独立承担了制造，产品设计（研发 / 工程），销售 / 营

销或车联网等业务职能。对于大多数公司来说，这种组织结构也反映在他们处理数据的方式上 - 企业中存在各种数据孤岛。

● 消除数据孤岛 (图二十一)

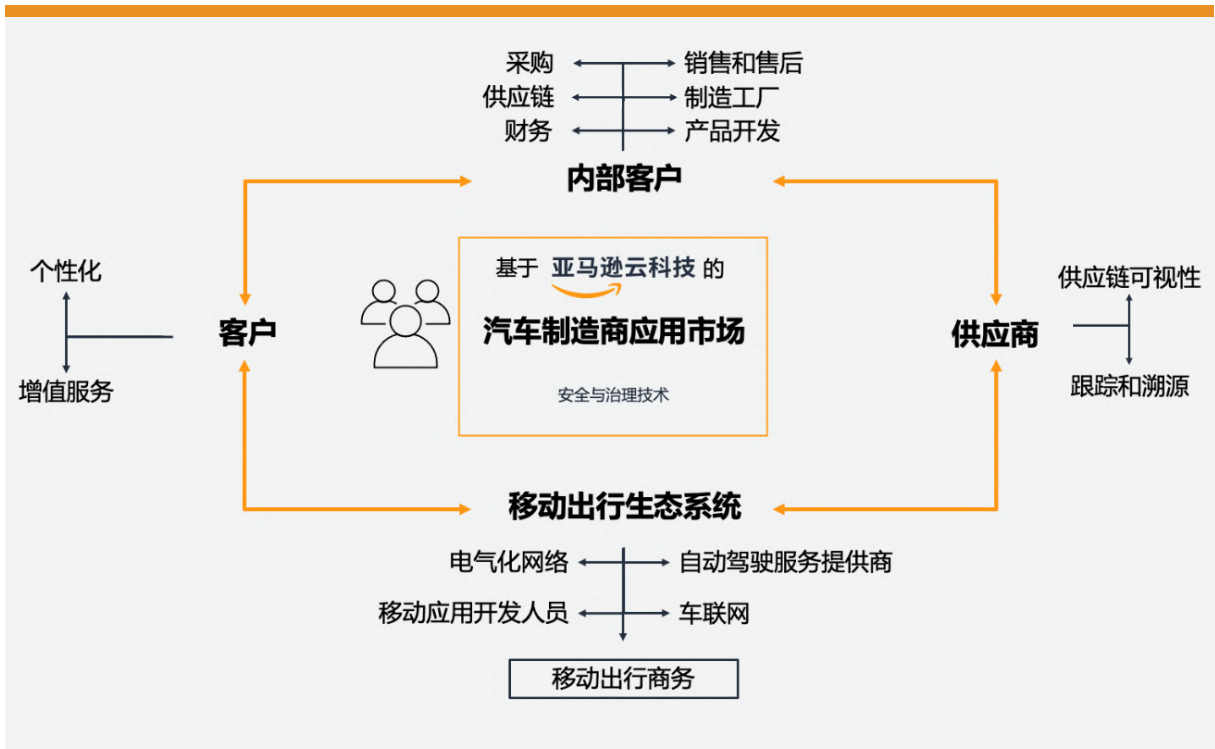


亚马逊云科技可以帮助汽车公司突破这些孤岛，创建企业范围的数据湖。凭借广泛、深入的数据仓库、分析和机器学习服务，我们帮助企业使用其数据并在整个价值链中实现改进。

- 亚马逊云科技 / 亚马逊的一个独特差异化因素是，我们在与汽车价值链保持一致的不同业务领域拥有面向生产应用的第一手经验。
- 在制造业 - 亚马逊正在为我们的运营中心开发自主和互联的机器人；
- 在供应链方面 - 亚马逊物流运营着世界上最复杂的供应链之一的系统；
- 在销售 / 营销方面 - 亚马逊广告帮助公司通过网络接触消费者 - 亚马逊 Go 商店彻底改变了零售购物体验；
- 在车联网中，亚马逊 Alexa 和 Music 与大多数汽车制造商的主要新车集成在一起；
- 在终端客户服务中，亚马逊 Alexa 是世界上采用最多的虚拟助手。通过亚马逊 Prime Video 和 Twitch，我们运营着两个领先的流媒体平台，用于电影 / 体育和游戏。

亚马逊的业务遍及整个汽车价值链，包括众多知名消费品牌。我们在汽车价值链的各个环节都拥有深厚的专业知识，贯穿始终的数据也使经销商 / 汽车制造商 / 供应商之间能够实现更紧密的协作。

● 广泛触达的汽车制造商应用市场（图二十二）



亚马逊科技为汽车行业客户带来了独特的市场能力，

- 基于数据安全和领先技术的基本要素，我们与汽车企业合作创建数据市场，允许连接所有内部数据，同时引入供应商，移动生态系统和客户数据，以实现整个企业数据的 360 度视图。
- 通过与第三方共享传感器数据，或为客户开发新服务，亚马逊科技上的汽车制造商市场是允许在整个移动出行生态系统中实现数据货币化的基础。

亚马逊科技和亚马逊与汽车价值链中几乎所有的公司合作，从汽车制造商到一级供应商、汽车技术公司以及新的移动出行初创公司。亚马逊科技通过全面的专用云功能集、丰富的经验以及例如普华永道这样的合作伙伴和开发人员社区，加速汽车行业的数字化转型。

编写指导：

■ 普华永道中国

汽车行业主管合伙人 金军

风险及控制服务市场主管合伙人 徐世达

网络安全及隐私保护服务合伙人 姜敏

■ 亚马逊云科技中国

大中华区创新成长企业及合作伙伴生态系统事业部总经理 倪殿令

大中华区战略业务发展部总经理 顾凡

大中华区解决方案架构部总监 代闻

主编人员：

■ 普华永道中国

网络安全及隐私保护服务高级经理 王爽

网络安全及隐私保护服务高级经理 武文俐

网络安全及隐私保护服务经理 顾吉杰

网络安全及隐私保护服务经理 张史捷

网络安全及隐私保护高级顾问 钦丽菡

网络安全及隐私保护咨询顾问 张绍仪

■ 亚马逊云科技中国

行业解决方案架构师高级总监 苏卓

汽车行业首席解决方案架构师 许军

解决方案架构师高级经理 刘天龙

解决方案架构师 胡正光

解决方案架构师高级总监 周玉林

解决方案架构师高级经理 邵士毅

高级产品营销专家 李昕

产品营销专家 吴佳敏

