

智能网联汽车 数据安全白皮书

WHITE PAPER ON DATA SECURITY
FOR INTELLIGENT CONNECTED VEHICLES

数据驱动智能出行 · 安全护航未来交通

SAFER DATA SMARTER MOBILITY A BETTER TOMORROW



编 著：禹慧丽 刘西蒙 王传银 王 进 张浩龙
谢天瀛 许勔璠 任 哲 杨 珍 李延凯

主编单位：智能汽车安全技术全国重点实验室
重庆长安汽车股份有限公司

参编单位：中国汽车工程研究院股份有限公司
西安交通大学
西安电子科技大学
上海零数科技有限公司
北京原语科技有限公司
陕西源擎智能科技有限公司



目录

前言.....3

术语与缩略语表.....5

一、 态势与挑战篇.....8

 (一) 当前态势 8

 (二) 行业现状 18

二、 治理篇：从合规防御到价值驱动的数据安全治理.....27

 (一) 治理目标：四层价值递进.....28

 (二) 治理体系：三层架构纵深防御.....34

 (三) 治理专项：五大业务场景驱动的差异化治理.....37

 (四) 治理维度：四类能力协同发力.....40

 (五) 治理实践：以车型全生命周期为主轴的闭环运行.....42

 (六) 轻量化路径：面向中小车企与零部件企业的渐进式实施建议.....45

三、 技术篇.....48

 (一) 数据采集 50

 (二) 数据存储 51

 (三) 数据处理 52

 (四) 数据传输 58

 (五) 数据共享 60

(六) 数据销毁 61

(七) 安全运营 63

四、 实践篇..... 67

(一) 研发设计数据安全..... 67

(二) 生产制造数据安全..... 72

(三) 驾驶自动化数据安全..... 79

(四) 软件升级服务数据安全..... 85

(五) 联网运行数据安全..... 90

(六) 安全事件分级、报告时限与缺陷召回衔接..... 95

五、 展望篇..... 97

(一) 未来趋势：重塑汽车数字免疫系统的五大前沿引擎..... 99

(二) 给车企的战略建议：面向未来的数据安全战略行动框架..... 104

参考文献..... 110



前言

在数据要素加速融入国家战略、汽车产业向“电动化、智能化、网联化”深度演进的当下，车联网数据已成为驱动业务创新与产业竞争的核心生产要素，同时也带来了前所未有的安全与合规挑战。一方面，车端、云端、用户端之间高频交互催生了数据权属、隐私保护与跨境流动等新型风险；另一方面，监管要求持续加码、网络攻击手段日益复杂，行业既有实践在体系化建设层面仍存在明显短板，“重业务、轻安全”、“重合规、轻治理”的传统模式已难以为继。

本文围绕“真实世界（车）—虚拟世界（云）”双向联动的核心场景，从态势与挑战出发，梳理宏观环境与产业实践带来的双重压力；进而以治理篇回答“为什么治、如何治”，构建从合规防御走向价值驱动的“四价值—三层级—五场景—四能力—四路径”治理框架；以技术篇回答“用什么建”，覆盖数据采集、存储、处理、传输、分析、销毁的全生命周期安全能力，配套加密、访问控制、身份管理、异常检测与应急响应等核心功能；以实践篇回答“怎么落地”，围绕车辆设计、生产、使用、报废的全生命周期形成闭环运营；最终以未来展望与建议收束，从内部能力筑基与外部生态协同两个维度，给出面向中长期演进的行动指引。

全文遵循“战略—治理—技术—实践—展望”的递进逻辑，力求为车企、Tier1、出行平台及监管机构提供一份可参照、可落地、可度量的数据安全一体化建设蓝图，整体架构如图 1。





图 1 智能网联汽车数据安全白皮书架构图

术语与缩略语表

为便于全文统一理解，本白皮书在正文前设置术语与缩略语表。正文中首次出现的缩略语，除特别说明外，均以表 1 所给全称与中文释义为准；个别在特定法规或标准语境下有专门含义的术语，随文另行说明。

表 1 术语与缩略语表

缩略语	英文全称	中文含义
ABE	Attribute-Based Encryption	属性基加密
AI	Artificial Intelligence	人工智能
CAN/CAN FD	Controller Area Network	控制器局域网及其可变速率扩展
CCPA	California Consumer Privacy Act	美国加州《消费者隐私保护法》
CDSO	Chief Data Security Officer	首席数据安全官
CSMS	Cyber Security Management System	网络安全管理体系
C-V2X	Cellular-V2X	基于蜂窝通信的车联网技术
DHR	Dynamic Heterogeneous Redundancy	动态异构冗余架构
DLP	Data Loss Prevention	数据防泄漏
DSMM	Data Security Maturity Model	数据安全能力成熟度模型
DSPM	Data Security Posture Management	数据安全态势管理
DSSAD	Data Storage System for Automated Driving	自动驾驶数据记录系统
ECU	Electronic Control Unit	电子控制单元
EDR	Event Data Recorder	事件数据记录系统
ERP	Enterprise Resource Planning	企业资源计划系统
GB 39732-2020	—	《汽车事件数据记录系统》
GB 44495-2024	—	《汽车整车信息安全技术要求》
GB 44496-2024	—	《汽车软件升级通用技术要求》
GB 44497-2024	—	《智能网联汽车 自动驾驶数据记录系统》
GB 45438-2025	—	《网络安全技术 人工智能生成合成内容标识方法》
GB/T 41871-2022	—	《信息安全技术 汽车数据处理安全要求》
GB/T 43697-2024	—	《数据安全技术 数据分类分级规则》
GB/T 44464-2024	—	《汽车数据通用要求》
GB/T 45652-2025	—	《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》
GB/T 45654-2025	—	《网络安全技术 生成式人工智能服务安全基本要求》



缩略语	英文全称	中文含义
GB/T 45674-2025	—	《网络安全技术 生成式人工智能数据标注安全规范》
GDPR	General Data Protection Regulation	欧盟《通用数据保护条例》
GNSS	Global Navigation Satellite System	全球导航卫星系统
HSM	Hardware Security Module	硬件安全模块
IAM	Identity and Access Management	身份与访问管理
IMU	Inertial Measurement Unit	惯性测量单元
ISO/SAE 21434	Road vehicles — Cybersecurity engineering	道路车辆网络安全工程国际标准
KMS	Key Management System	密钥管理系统
LVLM	Large Vision-Language Model	大视觉语言模型
MES	Manufacturing Execution System	制造执行系统
MFA	Multi-Factor Authentication	多因素认证
ML-KEM/ML-DSA	Module-LWE Key Encapsulation / Module-LWE Digital Signature	NIST 抗量子密码标准算法
OTA/FOTA	Over-The-Air/ Firmware Over-The-Air	软件在线升级/固件空中升级
PIA	Privacy Impact Assessment	个人信息保护影响评估
PLC	Programmable Logic Controller	可编程逻辑控制器
PLM	Product Lifecycle Management	产品生命周期管理系统
PQC	Post-Quantum Cryptography	抗量子密码
QKD	Quantum Key Distribution	量子密钥分发
QMS	Quality Management System	质量管理体系
RAG	Retrieval-Augmented Generation	检索增强生成
RSU	Road Side Unit	路侧单元
SAST/DAST	Static/Dynamic Application Security Testing	静态/动态应用安全测试
SBOM	Software Bill of Materials	软件物料清单
SCA	Software Composition Analysis	软件成分分析（开源组件安全检测）
SCADA	Supervisory Control And Data Acquisition	数据采集与监视控制系统
SDV	Software Defined Vehicle	软件定义汽车
SNDL	Store Now, Decrypt Later	“先存储，后解密”攻击
SOA	Service-Oriented Architecture	面向服务的架构
SOAR	Security Orchestration, Automation and Response	安全编排、自动化与响应
SOC	Security Operations Center	安全运营中心

缩略语	英文全称	中文含义
SUMS	Software Update Management System	软件升级管理体系
TARA	Threat Analysis and Risk Assessment	威胁分析与风险评估
TSN	Time-Sensitive Networking	时间敏感网络
UN R155	UN Regulation No.155	联合国法规，规定车辆 CSMS 认证要求
UN R156	UN Regulation No.156	联合国法规，规定车辆软件升级管理体系（SUMS）认证要求
V2G	Vehicle-to-Grid	车辆与电网之间双向充放电交互
V2X	Vehicle-to-Everything	车对外界信息交互（含 V2V 车-车、V2I 车-路、V2P 车-人、V2C 车-云）
VIN	Vehicle Identification Number	车辆识别代号
VSOC	Vehicle Security Operations Center	车辆安全运营中心
ZTNA	Zero Trust Network Access	零信任网络访问



一、 态势与挑战篇

当前，智能网联汽车正经历从“交通工具”向“移动智能终端”的深刻转型。这一变革不仅重塑了汽车产业的价值链条，更将数据安全推至前所未有的战略高度。据国家工业信息安全发展研究中心监测，智能网联汽车面临高频次、常态化的网络探测与攻击。数据安全已从合规选项演变为产业发展的生命线。

(一) 当前态势

1. 产业变革：从交通工具到数据载体的定位跃迁

(1) SDV 加速落地

随着电子电气架构从分布式向域集中、中央计算式演进，车辆功能日益由软件定义。OTA 升级、智能座舱、自动驾驶等核心能力高度依赖数据采集、传输与处理。

数据规模爆发式增长：截至 2025 年底，全球联网汽车保有量约为 3.38 亿辆，预计 2030 年将增长至 5.83 亿辆，年复合增长率约为 11.5%。同时，车端数据也迅速增长，据行业统计，一辆智能网联汽车每日可产生 TB 级别数据，部分车型甚至可达约 10TB/天，涵盖环境感知、车辆状态、驾驶行为、用户偏好等多维度信息。

安全内涵深刻转变：在此背景下，数据安全不再是传统网络安全的附属项，而是与整车功能安全、用户体验深度绑定的“刚性需求”。数据泄露、篡改或滥用，可能直接威胁车辆运行安全与用户人身安全。2024 年 8 月，国家市场监督管理总局、国家标准化管理委员会批准发布了由工业和信息化部组织制定的三项强制性国家标准（GB 44495-2024《汽车整车信息安全技术要求》、GB 44496-2024《汽车软件升级通用技术要求》、GB 44497-2024《智能网联汽车自动驾驶数据记录系统》），其中，GB 44495-2024《汽车整车信息安全技术要求》和 GB 44496-2024《汽车软件升级通用技术要求》已于 2026

年 7 月 1 日正式实施，GB 44497-2024《智能网联汽车自动驾驶数据记录系统》已于 2026 年 1 月 1 日起实施，标志着汽车数据安全进入强制合规时代。

大模型带来的新挑战：随着端到端自动驾驶大模型的应用，训练数据的质量与完整性直接影响模型安全性与可靠性。用于迭代自动驾驶 AI 大模型的训练数据可能含有重要数据，对数据采集、标注、存储和跨境流动提出了更严格的合规要求。

上述风险已不再停留于技术与管理建议层面，而是被成文的合规义务所固化。《生成式人工智能服务管理暂行办法》（国家互联网信息办公室等七部门令第 15 号，2023 年 8 月 15 日施行）第四条从五个方面设定了底线要求：坚持社会主义核心价值观；在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取有效措施防止产生民族、信仰、国别、地域、性别、年龄、职业、健康等方面的歧视；尊重知识产权、商业道德，保守商业秘密；不得危害他人身心健康，不得侵害他人肖像权、名誉权、荣誉权、隐私权和个人信息权益；提高生成式 AI 服务的透明度，提高生成内容的准确性和可靠性。与之配套的安全基本要求也已由技术文件升级为推荐性国家标准，主要包括 GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》、GB/T 45652-2025《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》、GB/T 45674-2025《网络安全技术 生成式人工智能数据标注安全规范》，上述标准均于 2025 年 4 月 25 日发布、2025 年 11 月 1 日实施；生成合成内容标识另有强制性国家标准 GB 45438-2025《网络安全技术 人工智能生成合成内容标识方法》（2025 年 9 月 1 日实施）。

(2) “车路云一体化” 加速推进

2024 年以来，国家车路云一体化应用试点全面铺开，北京、上海、重庆等 20 个城市纳入首批试点。这一模式打破了单车智能的局限，构建起“车-路-云-网-图”协同的智能交通体系。

数据交互范式根本性变革：

数据交互主体激增：传统车-云双向交互，扩展为“V2V”、“V2I”、“V2P”、“V2C”等多维



立体交互。

数据流动路径复杂化：数据不再局限于车端与单一云端平台，而是在 RSU、边缘计算节点、区域云平台、中心云平台之间形成复杂的网状流动。

数据实时性要求提升：V2X 应用（如闯红灯预警、协作式自适应巡航）对数据传输时延要求达到毫秒级，安全机制必须在不显著增加时延的前提下保障数据真实性与完整性。

这种复杂的交互形态，使得数据安全边界从“车内”扩展到“车外”，传统基于边界防护的安全理念面临根本性挑战。

(3) 数据从“副产品”向“核心资产”跃迁

数据价值释放路径日益清晰：

研发层面：海量路采数据是训练自动驾驶模型、优化算法性能的核心“燃料”。2025 年世界智能网联汽车大会发布成果显示，“车路云一体化”为汽车 AI 应用建立了“数据发电站”，为自动驾驶 AI 大模型的开发、训练、评价提供高效、可信、完备的数据集。

运营层面：车辆实时运行数据支撑远程诊断、预测性维护、能耗优化等增值服务，成为提升用户体验、降低运营成本的关键。

商业层面：脱敏后的车辆数据可赋能保险定价、智慧交通、出行服务等第三方生态，开辟新的收入来源。北京、杭州、济南等地已开展公共数据授权运营探索，推动交通信号灯、交通流量、公共停车等数据与智能网联汽车深度融合。

这一转变意味着数据安全的内涵正在发生深刻演变：从单纯的“风险规避”转向“价值保障”。数据安全能力不再仅是成本中心，而是支撑数据资产化、价值化的基础能力。



2. 国家战略：从数据安全总体布局到汽车领域的纵深推进

(1) 从通用数据安全到汽车领域的合规演进

全球数据安全立法经历了从通用型保护向行业纵深管控的演进过程。早期以欧盟 GDPR、美国 CCPA 为代表的立法，主要聚焦个人信息保护的普适性原则，尚未针对智能网联汽车的特殊数据形态（如车辆实时运行数据、高精度地理信息、V2X 通信数据）建立专门规则。

随着智能网联汽车成为“移动的数据收集器”，各国监管呈现三大转变：

从“个人信息保护”扩展到“全量数据管控”。汽车数据不仅包含驾驶员生物特征、行踪轨迹等敏感个人信息，更涉及国家安全层面的重要数据（如军事管理区地理信息、关键基础设施布局）。“重要数据”概念最早见于中国《网络安全法》；《数据安全法》进一步确立了数据分类分级保护制度与重要数据目录管理要求。欧盟《数据法案》将“联网产品数据”纳入规制，均突破了传统个人信息保护的边界。

从“事后追责”转向“全生命周期准入”。UN R155/R156、中国 GB 44495-2024 等强制性标准，要求车企在车型上市前即建立 CSMS 并通过第三方认证，将合规节点前移至产品设计阶段。

从“单一国家规制”演变为“数据主权博弈”。数据本地化存储、跨境传输安全评估、技术自主可控等要求，使汽车数据安全深度嵌入地缘政治竞争。中国要求重要数据境内处理，欧盟通过《数据法案》构建“数字主权护城河”，美国则依托长臂管辖实施技术封锁。

全球主要经济体汽车数据安全法规与标准对比见表 2 所示：

表 2 全球主要经济体汽车数据安全法规与标准对比

维度	中国	欧盟	美国
顶层法律架构	《网络安全法》（2017 年施行，2025 年修正，2026 年 1 月 1 日起施行）《数据安全法》《个人信息保护法》	GDPR（2018）+《数据法案》（2025）+《人工智能法案》（2024）	CCPA/CPRA（加州）

维度	中国	欧盟	美国
汽车专项法规	《汽车数据安全若干规定（试行）》（2021） 《汽车数据出境安全指引（2026版）》	UN R155/R156（2020-2021，强制性） 《数据法案》第2章（2025，联网产品数据开放）	NHTSA《网络安全最佳实践》（指南性） EPA OTA 法规（2021）
强制性标准	GB 44495-2024《汽车整车信息安全技术要求》（2026.1.1 实施） GB 44496-2024《汽车软件升级通用技术要求》 GB 44497-2024《智能网联汽车 自动驾驶数据记录系统》（2026.1.1 实施）	UN R155（CSMS 认证） UN R156（SUMS 认证） ISO/SAE 21434（技术实现路径）	无联邦强制性标准 SAE J3061/J3101（行业自愿）
行政法规与数据分类分级基础标准	《网络数据安全条例》（国务院令 第790号，2025年1月1日施行）； 《数据安全法 数据分类分级规则》（GB/T 43697-2024，2024年10月施行）； 《汽车数据通用要求》（GB/T 44464-2024，2024年8月发布） 三级分类（一般/重要/核心数据） 汽车重要数据目录（工信部组织制定）	GDPR（2018）确立数据保护框架； 《数据治理法》（2023）规范公共数据再利用 个人数据/非个人数据二分 敏感数据特殊保护 联网产品数据强制开放	无联邦统一数据保护法，各州立法分散

(2) “数据要素×”及“车路云一体化”战略部署

2024 年，国家数据局等 17 部门联合印发《“数据要素×”三年行动计划（2024-2026 年）》，将“数据要素×交通运输”列为重点行动方向。文件明确提出：推动交通运输领域数据要素“跨领域、跨区域、跨层级”流通应用，提升多式联运效率、赋能自动驾驶发展、优化交通治理能力。这一定调释放了明确信号：数据不仅要管好，更要用好。数据安全是数据价值释放的前提，安全能力必须与数据流通应用同步演进。

工业和信息化部等五部门联合发布的《关于开展智能网联汽车“车路云一体化”应用试点工作的通知》，将数据安全列为试点工作的核心内容之一。通知明确要求：试点城市需建立覆盖“车—路—云—网—图”的数据安全管理制度，落实数据分类分级、重要数据保护、跨境数据管理、安全监测与



应急响应等要求。这意味着数据安全已成为地方政府参与试点的“准入条件”，也是车企进入相关市场的“合规门槛”。

3. 地缘政治：全球数据主权割裂对跨国车企的冲击

(1) 数据主权上升为国家竞争焦点

近年来，各国围绕数据主权的立法博弈日益激烈。数据被定位为国家基础性战略资源，其流动与利用受到严格管控。2025 年 6 月，工业和信息化部等八部门就《汽车数据出境安全指引》公开征求意见，并于 2026 年 2 月正式印发 2026 版，标志着我国在汽车数据跨境流动监管领域迈入精细化治理新阶段。

在汽车领域，这一趋势尤为明显。智能网联汽车采集的地理信息、交通流量、用户行为等数据，可能涉及国家安全、公共安全与个人隐私，成为各国监管重点。

(2) “一地研发、全球销售”模式面临挑战

传统跨国车企多采用“全球研发、全球部署”模式：在总部完成研发测试，将同一车型销往全球市场。这一模式在数据安全领域面临三重挑战：

数据本地化要求：中国、欧盟、印度等主要市场纷纷出台数据本地化法规，要求重要数据在本土存储。特斯拉在中国建立数据中心、大众在合肥设立研发中心并配套数据存储设施，成为应对之策。

数据出境限制：中国《数据出境安全评估办法》《个人信息出境标准合同办法》等法规，对数据出境设置了严格的评估与备案流程。涉及重要数据或大规模个人信息的跨境传输，需通过国家网信部门的安全评估。2025 年 4 月，国家互联网信息办公室发布《数据出境安全管理政策问答》，进一步明确仅对重要数据和个人信息实施出境管控，一般数据可自由跨境流动，在涉及重要数据的 44 个评估项目中，不通过 7 个、不通过率 15.9%；44 个项目申报的 509 个重要数据项中，准予出境 325 个，占申报数据项总数的 63.9%。



技术标准分化：欧盟 UN R155/R156、美国 NHTSA 网络安全指南、中国《汽车数据安全管理办法（征求意见稿）》等标准在具体要求上存在差异，增加了车企合规的复杂性。GB 44495-2024《汽车整车信息安全技术要求》第 7.4.7 条明确，车辆不应直接向境外传输数据，但用户使用浏览器访问境外网站等用户自主行为不受该条款限制。

(3) 供应链重构与数据安全协同

地缘政治因素叠加数据主权要求，正在重塑全球汽车供应链格局：

研发本地化：跨国车企加速在华设立研发中心，将核心研发能力、数据存储与处理能力向主要市场转移。

供应商区域化：受美国“敏感外国实体”规定、欧盟关键原材料法案等地缘政治因素影响，跨国车企被迫放弃全球统一供应体系，转向“区域化隔离”策略。特斯拉、通用等美系车企要求供应商在 2027 年前构建非中国供应链，而宝马、大众等欧系车企采取“中国+1”策略维持中国市场深耕同时培育替代来源。与此同时，安波福、采埃孚等跨国零部件供应商反而加速中国本土化，开发不受出口管制限制的中国方案。这种“车企分散、供应商集中”的悖论，反映出全球汽车供应链正从效率优先转向“安全并重”，三大区域供应链体系（中国、北美、欧洲）加速形成，技术标准与数据安全法规的地缘政治化成为供应链重构的核心驱动力。

技术自主可控：国产车载芯片、操作系统、安全方案加速上车，以降低对海外技术的依赖。上汽集团等企业已基于国产密码技术建设了完整的 V2X-PKI 认证体系，支撑车云认证、FOTA 安全、数字钥匙等应用。

在这一过程中，如何保障跨国供应链中的数据安全协同，成为车企必须面对的新课题。

4. 安全威胁：从数字风险到物理危害的升级

随着智能网联汽车深度融入社会生产生活，数据安全威胁正从传统的信息泄露风险，向直接威胁



车辆控制、人身安全乃至公共安全的物理危害升级。据 Upstream 发布的《2026 年全球汽车与智能出行网络安全报告》统计，2025 年汽车及智能出行领域共发生 494 起公开报道的网络安全事件，其中 71% 的攻击来自黑帽黑客，92% 的攻击以远程方式实施，86% 的攻击无需物理接近车辆。攻击面持续扩大、AI 技术被恶意利用、勒索手段升级、供应链漏洞频发，共同构成 2026 年汽车数据安全的核心挑战。

(1) 攻击面持续扩大：从车内到车外的全域暴露

车内网络攻击常态化。传统 CAN/CAN FD 总线架构在设计之初缺乏安全考量，已成为攻击者的主要突破口。2025 年披露的 “PerfektBlue” 蓝牙攻击事件揭示了这一风险的严重性——研究人员在 OpenSynergy BlueSDK 蓝牙协议栈中发现多个严重漏洞，攻击者可通过蓝牙连接远程执行代码，入侵梅赛德斯-奔驰、大众、斯柯达等品牌数百万辆汽车的车载信息娱乐系统，进而实现位置追踪、音频窃听、电话簿访问，甚至可能横向移动至转向、雨刷等关键功能。

据木卫四威胁情报中心监测，2025 年共发现汽车安全事件 206 起、漏洞 238 个，安全事件数量较 2024 年有所回升，漏洞数量进一步上升。攻击方式以远程攻击为主，部分攻击已不再以单一 ECU 为目标，而是通过云端配置错误、API 接口滥用或车辆外部接口作为入口，逐步向车内关键系统渗透。

V2X 通信成为新型攻击面。车路云一体化的加速推进，使 V2X 通信成为数据安全的新战场。最新学术研究表明，针对 C-V2X 的协议合规型攻击已具备现实可行性。2025 年 8 月发布的一项实地测试研究显示，攻击者可通过 UDP 泛洪和超大 BSM 消息淹没等方式，在不违反协议规范的前提下实施拒绝服务攻击——UDP 泛洪攻击可使数据包传输率下降高达 87%，时延增加至 400 毫秒以上；当两种攻击同时执行时，可导致前向碰撞预警系统完全失效。

此外，2026 年 3 月，美国乔治梅森大学研究人员提出的 “资源饥饿攻击” 发现，攻击者可利用 5G NR-V2X 资源分配机制的漏洞，使自动驾驶系统对时间敏感应用的安全服务水平降低最多 15%，直接威胁道路安全。研究团队建立了基于信息年龄的离散时间马尔可夫链分析模型，并通过仿真验证

了此类攻击的可行性和破坏性。

传感器欺骗威胁感知系统可靠性。自动驾驶高度依赖摄像头、毫米波雷达、激光雷达等传感器数据，而传感器间的时空同步机制正成为新的攻击靶点。2026 年 3 月发布的研究成果揭示了“DejaVu”攻击——攻击者通过入侵车载以太网（采用 TSN）的 gPTP 时间同步协议，可对多模态传感器融合系统实施时序错位攻击。实验结果显示，单帧激光雷达数据延迟即可使物体检测平均精度下降高达 88.5%；三帧摄像头数据延迟可使多目标跟踪准确度下降 73%。研究人员在 Autoware 自动驾驶仿真平台和硬件在环测试中验证了此类攻击可导致碰撞和幽灵刹车等严重后果。

充电基础设施成新兴攻击面。2026 年 1 月举行的第三届 Pwn2Own Automotive 赛事中，网络安全专家成功揭示汽车软件系统中存在的 76 个独特的零日漏洞，涉及特斯拉信息娱乐系统到电动汽车充电桩等多种目标，赛事奖金超过 100 万美元。研究人员在电动汽车充电桩中发现越界写入漏洞和时间窗口漏洞，攻击者可控制充电流程、篡改计费、窃取用户数据，甚至通过 V2G 接口反向干扰电网负载调度。

(2) AI 新风险：人工智能武器化的安全挑战

对抗样本攻击。自动驾驶模型在训练和推理阶段均面临对抗样本攻击风险。2026 年 3 月，中国科学院计算技术研究所程学旗团队在 CVPR 2026 发表的研究提出随机参数剪枝攻击，通过随机屏蔽模型参数生成对抗样本，使攻击在不同神经网络架构间的迁移能力大幅提升。实验表明，该方法在跨架构攻击任务中成功率提升约 11.7%-17.5%，在对抗训练模型上的攻击成功率可达 88%，显著高于现有攻击方法。这类攻击的通用性提升意味着攻击者可在代理模型上生成对抗样本，直接应用于未知的自动驾驶系统。

环境文本提示词注入攻击。随着 LVLM 进入智能座舱，物理世界的文本信息可能成为攻击入口。加州大学圣克鲁兹分校 2026 年 1 月发布的 CHAI 攻击研究首次系统探索了这一威胁——攻击者通过在物理环境中放置误导性文本（如伪造路牌、广告牌），可劫持自动驾驶系统决策。实验结果显示，

该方法在无人机目标跟踪场景攻击成功率达 95.5%，在自动驾驶场景达 81.8%，在无人机着陆场景达 68.1%。研究人员在真实物理环境中验证了攻击有效性，一辆搭载 LVLM 的自动驾驶车辆在识别到伪造文本后，导航指令被成功覆盖。

训练数据投毒与模型后门。自动驾驶 AI 模型的性能高度依赖训练数据的质量与完整性。攻击者可通过数据投毒方式，向训练数据集中注入恶意样本。用于迭代自动驾驶 AI 大模型的训练数据往往包含海量路采信息，其中可能混入对抗样本或后门触发模式，使模型学习错误的特征关联。这类攻击具有潜伏期长、隐蔽性强的特点，一旦训练数据被污染，可能影响整个自动驾驶模型的安全性与可靠性。

(3) 勒索软件 2.0：从数据加密到车辆劫持

针对云端训练集群的勒索攻击。据 Upstream 报告统计，2025 年汽车及智能出行领域勒索软件攻击显著激增，44%的安全事件涉及勒索软件，数量较 2024 年翻倍增长。攻击目标已从 IT 系统扩展至实际车辆——2025 年年中，攻击者通过获取车主 App 访问权限，远程锁定车主、控制点火和门锁功能，要求支付赎金才能恢复访问。

针对企业系统的供应链级勒索。2025 年最重大的安全事件发生在一家欧洲整车厂，攻击导致该企业生产和企业系统瘫痪数周，迫使地方政府提供财政支持。此次攻击的连锁反应波及大量供应商，甚至对地区 GDP 造成可观测影响。这一案例表明，针对整车企业的勒索攻击已具备系统性破坏能力。

攻击成本降低与自动化。AI 技术的滥用使勒索攻击实现自动化。攻击者可利用生成式 AI 自动发现漏洞、生成恶意代码、绕过安全检测。据相关报告统计，67%的安全事件涉及远程信息处理和云系统攻击向量，API 作为智能出行生态系统的“神经系统”，成为相当一部分事件的入口。

(4) 供应链风险：软件与硬件层面的系统性脆弱性

开源组件与第三方软件安全隐患。现代智能汽车软件系统中，开源组件占比日益提升，其安全质量参差不齐。2025 年披露的多个高危开源组件漏洞涉及 OTA 升级、网络通信等关键模块，影响范围

广泛。木卫四威胁情报中心统计显示, 2025 年漏洞数量较 2024 年进一步上升, 主要集中在智能座舱、车主应用、云平台、OTA、车载外部接口及通信接口等核心资产。

地缘政治驱动的供应链重构风险。2025 年 3 月, 美国联邦法规《保护信息和通信技术与服务供应链: 网联汽车》最终规则正式生效, 禁止交易由中国或俄罗斯“拥有、控制或受其管辖”的实体所设计、开发、制造或供应的特定软硬件。该规则设置了关键时间节点: 2026 年 3 月 17 日前设计、开发且此后未由受限实体修改的软件子组件在确保相关代码此后不再由受限制实体参与维护(即从受限实体处收回或切断维护权限)的前提下, 方可适用“遗留代码”豁免。

第三方服务商成为攻击跳板。通过第三方服务提供商平台入侵, 已成为攻击者的常用手段。2024 年 6 月, 针对汽车经销商软件供应商的勒索软件攻击导致超过 1.5 万家北美经销商运营受阻。这类攻击利用车企与供应商之间的信任关系, 绕过直接防护, 实现“曲线入侵”。

(二) 行业现状

1. 智能网联汽车数据概况

智能网联汽车已演变为移动的数据中心, 其数据具有以下显著特征:

多源异构性:数据来源广泛, 既包括车载传感器(摄像头、雷达)采集的环境数据, 也包括座舱内的人机交互数据, 以及车辆运行状态数据; 数据格式涵盖视频、图像、音频、文本、二进制代码等多种形式。

高敏感度与隐私性:数据中包含大量能直接识别自然人身份的信息(如人脸、声纹、行踪轨迹)以及能反映国家地理环境、交通状况的重要数据, 涉及个人隐私安全与国家安全。

全生命周期流转:数据在“端—管—云”之间高速流转, 经历收集、存储、使用、传输、删除等环节, 每个环节都存在潜在的安全风险。

合规要求严苛:依据标准, 数据处理需遵循“默认不收集”、“车内处理”、“精度范围适用”



原则，且对敏感个人信息和重要数据提出了极高的加密、脱敏（匿名化）和本地化存储要求。

从车路云一体化技术架构出发，按数据产生来源分为四大类。四大类数据及其来源关系见图 2。

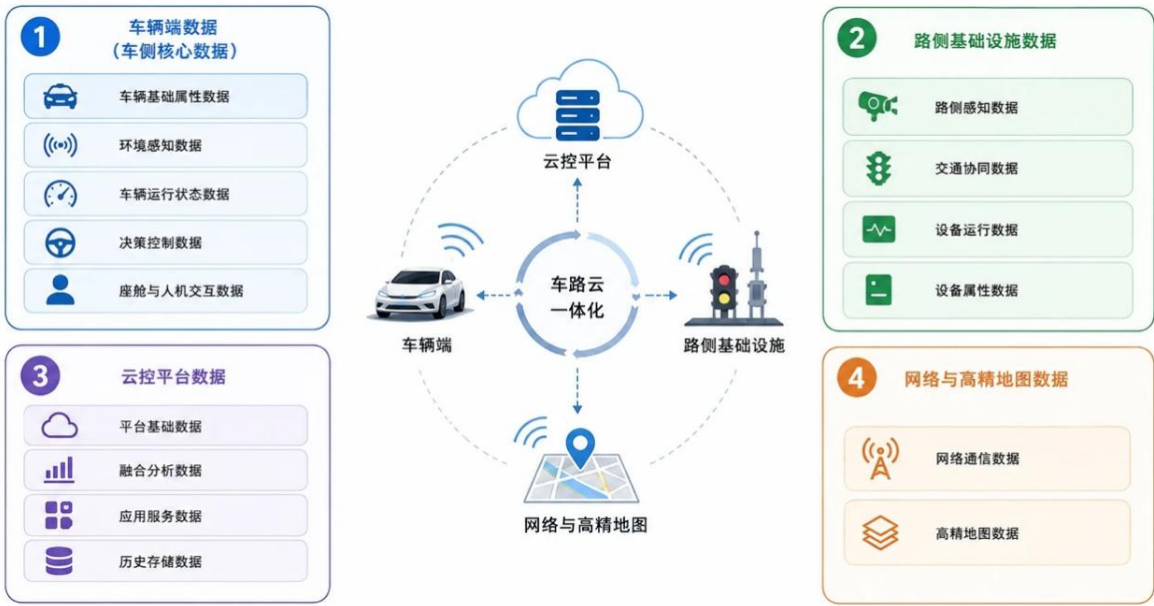


图 2 智能网联汽车数据分类及来源

(1) 车辆端数据

智能网联汽车自身采集、产生的数据，是数据体系的核心，细分为 5 个子类，具体数据见表 3。

表 3 车辆端数据子类及具体数据项

数据子类	具体数据项
车辆基础属性数据	VIN、车架号、电机/发动机编号、ECU 软硬件版本、车辆配置参数、核心零部件标识
环境感知数据	视觉感知：车内外摄像头采集的道路影像、交通标志、行人车辆画面、驾驶员监测画面 雷达感知：毫米波雷达、激光雷达采集的点云数据、目标物的距离/速度/方位数据 定位姿态：GNSS 定位数据、IMU 惯性测量数据、轮速数据、车辆俯仰/侧倾角度 车身感知：雨量、光照、胎压、车内温湿度等车身传感器数据
车辆运行状态数据	动力系统：车速、加速度、油门开度、制动深度、电机/发动机转速与扭矩 底盘系统：转向角度、制动系统压力、ESP/ABS 工作状态、悬架参数 能源系统：电池 SOC/SOH、充放电功率、电压电流、续航里程 车身状态：车门/车窗状态、灯光、空调、座椅位置等车身电子状态
决策控制数据	决策层：路径规划结果、行驶决策（超车/跟车/变道）、目标车速与车距设定 控制层：转向、加速、制动的控制指令，自动驾驶模式切换记录

数据子类	具体数据项
	系统状态：自动驾驶运行模式、故障告警、人工接管请求与记录
座舱与人机交互数据	交互操作：语音指令、触控操作、导航目的地设置、娱乐应用使用记录 座舱状态：车内人数、座椅调节、空调设置、车内空气质量 用户服务：车机账号信息、个性化设置、车载服务订单与支付记录

(2) 路侧基础设施数据

车路协同场景下，路侧设备产生与采集的数据，具体数据见表 4。

表 4 路侧基础设施数据子类及具体数据项

数据子类	具体数据项
路侧感知数据	路侧摄像头、雷达采集的全域交通目标数据，包含车辆、行人、非机动车的位置与速度信息
交通协同数据	信号灯状态、交通标志信息、道路施工/事故预警信息、绿波通行建议
设备运行数据	路侧设备工作状态、故障信息、通信状态、功耗数据
设备属性数据	设备编号、安装位置、设备型号、软硬件版本

(3) 云控平台数据

云端平台汇聚、处理、生成的数据，具体数据见表 5。

表 5 云控平台数据子类及具体数据项

数据子类	具体数据项
平台基础数据	云平台身份标识、系统配置参数、用户权限管理数据
融合分析数据	全域交通流融合数据、交通态势分析结果、区域出行统计数据
应用服务数据	导航服务数据、OTA 升级包、远程诊断指令、出行服务订单数据
历史存储数据	云端归档的用户个人信息、全量车辆运行历史数据

(4) 网络与高精地图数据

主要包括网络通信数据与高精地图数据两类，具体数据项见表 6。

表 6 网络与高精地图数据子类及具体数据项

数据子类	具体数据项
网络通信数据	车联网通信信令、网络流量数据、链路状态数据、身份认证与密钥数据
高精地图数据	高精度道路拓扑数据、车道级属性数据、动态交通事件图层、定位辅助图层

2. 车企数据建设安全建设总体进展

基于中国信息通信研究院、国家工业信息安全发展研究中心及行业公开数据，当前中国智能网联汽车数据安全建设呈现以下特征：

(1) 建设阶段分布：头部企业体系升级，中小企业合规筑基

合规基础能力初步建立（2021-2025）。根据中国汽车工业协会等机构通报，汽车数据安全合规检测按企业自愿送检原则组织：2024 年 4 月发布的第一批结果中，6 家企业的 76 款车型符合 4 项合规要求；2025 年 12 月 19 日发布的第四批结果中，9 家企业的 43 款车型符合 5 项合规要求（在“车外人脸信息匿名化处理、默认不收集座舱数据、车内数据处理、个人信息显著告知”4 项基础上新增“精度范围适用”）。需说明的是，检测采取自愿送检原则，通过情况反映送检企业的合规水平，不等同于行业整体水平。这一阶段标志着行业基本完成了从“无法可依”到“有规可循”的过渡。

领先车企进入价值运营探索期。部分头部企业已超越合规层面，开始将数据安全能力转化为市场信任和商业价值。例如，特斯拉通过中国数据安全合规认证，为其完全自动驾驶功能入华扫清障碍；蔚来构建“VSOC+智能体中枢+精英运营人员”的端云协同安全运营模式，实现安全事件的自动识别与响应。数据安全正从成本中心向信任资产转型。

(2) 投入水平：从边缘预算到战略投资

a. 资金投入显著增长

GB 44495-2024《汽车整车信息安全技术要求》、GB 44496-2024《汽车软件升级通用技术要求》、



GB 44497-2024《智能网联汽车自动驾驶数据记录系统》，对新申报公告车型实行准入一票否决制，直接倒逼全产业链加大合规改造投入。

本土车企合规改造成本：

- 单车型检测认证直接费用：据检测认证行业公开报价信息（三项强标检测无全国统一价目表），按车型智能化程度分级，基础燃油车三项国标合并检测费用约 18-32 万元；主流智能网联新能源车型 35-60 万元；搭载高阶智驾、多域控制器、全域 OTA 的高端车型，因测试场景大幅增加，检测成本 65 万元起步，若叠加国密硬件改造、漏洞复测，费用进一步上浮；
- 体系化长期投入：车企需配套搭建全生命周期信息安全管理体系、车载加密硬件植入、OTA 安全架构重构、数据分类分级平台、漏洞响应机制等。大型自主品牌车企（年销量 50 万辆以上）为适配三项强标，含研发改造、实验室能力建设、第三方咨询、年度运维在内的据业内估算，中长期整体投入规模通常以亿元计；中小车企多采用联合送检、复用供应商安全方案、外包安全运营模式压降一次性支出；
- 隐性持续成本：每年生产一致性核查、车型改款复测、安全人员薪酬、渗透测试、漏洞库订阅等为常态化年度刚性开支。

跨国车企本地化合规增量成本：

依据道可特律师事务所 2026 版《汽车数据出境安全指引》深度研究报告，受中国车载重要数据境内存储、数据出境安全评估、本地算力训练等本地化强制规则约束，在华跨国车企智能网联汽车整体开发成本较合规前上浮约 14%。

b. 组织架构升级

独立安全官设置：比亚迪、潍柴动力等设立首席可持续发展官/首席安全官，推动 ESG 与数据安全工作落地。蔚来汽车设立全球网络安全负责人职位，由具备亚马逊云、微软中国首席安全官背景的专家担任。



跨部门协同机制: 吉利汽车设立专门工作组, 建立延伸至二级及以下供应商的数据安全评价体系。

(3) 头部车企数据安全实践进展

头部车企在治理架构、技术部署与重点举措上已形成差异化实践, 对比如表 7 所示。

表 7 主要车企数据安全治理与技术部署实践对比

车企	治理架构	技术部署	重点举措与差异化优势
长安汽车	三级联防联控机制: 网络安全和信息化委员会办公室、推进办公室、二级单位; 安全委员会直接向管理层汇报; 拥有行业唯一的“智能汽车安全技术全国重点实验室”	端云一体数据安全防护方案: 智能车云平台技术底座; 车端数据加密传输; 业务平台与私有云数据中心专线传输; HTTPS 协议+数据验证信息; 9 重纵深防御体系+三端一体化态势感知平台; ASIL D 级功能安全流程; 七重冗余架构 (感知、控制、电源、转向等)	合规标杆+全栈自研: 三车型 10 款车全部通过国家 4 项数据安全合规检测; 通过 UN R155 车辆 CSMS 认证; 制定《数据安全治理框架 1.0》《海外网络和数据安全管理体系 1.0》; L3 级自动驾驶安全设计: 引入 45 项法规标准+39 项企业标准, 百万公里级三层场景池支撑 ODD 定义; 阿维塔科技获 PIA 二星级标识, 在车内摄像头、虚拟 E 值交易等敏感信息保护领域通过第三方权威认证
特斯拉	全球首席信息安全官+中国首席安全官双轨制; 上海超级工厂设立独立数据安全团队	中国数据中心本地化存储; 通过 ISO 27001 认证; FSD 数据合规改造	数据本地化标杆: 2021 年建成上海数据中心, 实现数据不出境; 2024 年通过国家数据安全 4 项合规要求, 解除禁停禁行限制; 与百度地图合作解决测绘资质问题
蔚来	设立全球网络安全负责人 (前亚马逊云、微软中国 CSO); 安全委员会直接向 CEO 汇报	部署端云一体 VSOC 平台; 车端 IDPS 系统; 零信任架构	端云协同领先: 构建“VSOC+智能体中枢+精英运营人员”模式, 实现安全事件自动识别和响应; 安全运营向“智能体中枢化”演进
小鹏	自动驾驶中心与智能座舱中心合并为通用智能中心 (2026 年重组), 安全嵌入研发全流程	与阿里云共建“扶摇”智算中心; 专属托管集群模式; 联邦学习框架	AI 安全前瞻: 采用“数据不动模型动, 知识共享数据不共享”策略, 利用联邦学习和同态加密保障数据隐私



车企	治理架构	技术部署	重点举措与差异化优势
理想	设立 CDSO；产品安全委员会统筹研发与运营安全	全链路数据加密；车内数据本地处理；用户可控数据开关	用户信任构建：默认不收集座舱数据，敏感数据处理需用户明确授权；通过隐私增强技术实现数据最小化
比亚迪	首席可持续发展官统筹 ESG 与数据安全；成立专项工作组推进 GB 44495 合规	自研车规级安全芯片；国密算法全栈应用；V2X-PKI 认证体系	技术自主可控：国产密码技术上车，降低对海外技术依赖；刀片电池数据与车辆数据融合安全保护
吉利汽车	设立数据安全专项工作组；建立延伸至二级供应商的安全评价体系	多层次异构算力协同安全架构；跨运营商算力互通安全认证	推动形成主机厂—供应商—服务商责任追溯链，将安全要求纳入供应商准入体系，并将信息与数据安全纳入供应商可持续发展能力审核维度
上汽集团	网络安全与数据安全委员会统筹；各品牌（乘用车、大通）独立安全团队	基于国产密码的 V2X-PKI 体系；海外 VSOC 节点（巴黎、法兰克福）；40+ 车型部署	出海合规先行：VSOC 解决方案已应用于 40 多个车型、250 万辆车，云端部署遍布欧洲节点，满足 GDPR 和 UN R155/R156 要求
长城汽车	首席安全官（CSO）制度；安全部门参与产品定义阶段	定制化 ECU 信息安全防护；轻量化安全组件部署；电池护照数据安全	出海数据合规：重点应对欧盟《新电池法》下“电池护照”数据安全挑战，建立跨境数据流通合规方案

3. 零部件企业数据安全建设实践

当前车端零部件数据安全研究主要围绕三大主线展开：产品内生安全技术层面，重点攻克国密芯片集成、HSM、安全通信协议及入侵检测探针等嵌入式安全能力，使安全成为零部件的内生属性而非外挂附加；智驾数据流通安全层面，聚焦车端采集数据在“车企—供应商—云厂商”流转中的实时脱敏、端到端加密和责任边界划分，解决海量路测与用户数据合规支撑模型迭代的难题；供应链协同安全基础设施层面，正通过隐私保护计算、联邦学习、可信执行环境等技术构建“可信数据空间”，实现零部件溯源、碳足迹核算、电池 ID 协同等场景下跨企业数据的“可用不可见”，推动数据安全从

单一企业能力向产业链共享基础设施演进。

表 8 部分零部件企业数据安全治理实践对比

厂商/ 参与 方	企业类型	具体数据安全实践	关键技术/标准/认证
华为	Tier1（智能汽车部件）	1. 建立自上而下数据治理架构，基于“设计中构建隐私”理念； 2. 车端推出“隐私声盾”防止语音数据泄露； 3. 云端采用匿名化、双向身份认证、全链路端到端加密； 4. 获 ISO 21434 和 TISAX Level 3 认证。	隐私声盾、端到端加密、ISO 21434、TISAX Level3
金龙客车	整车及关键零部件（T-BOX）	1. T-BOX 率先通过 GB44495、GB44496、GB32960 三项国家强标认证； 2. 搭载国密二级安全芯片，全流程加密； 3. 全国产车规级芯片，深度融合国产北斗定位系统。	国密二级安全芯片、全流程加密、GB44495/44496/GB32960-2025
RTI 公司	Tier2（中间件/DDS 供应商）	1. Connex Drive 3.1 同时满足 ASPICE CL1、ISO 21434、ISO 26262 三项标准； 2. 采用“安全设计”方法，满足零信任架构需求。	DDS 协议、ASPICE CL1、ISO 21434、ISO 26262
经纬恒润	汽车电子系统供应商	1. 协助客户搭建 GB 44495、R155、ISO/SAE 21434 等标准的信息安全流程体系，开展 TARA 分析； 2. 提供 HSM 平台固件、安全 Bootloader、SecOC 和 IdsM 协议栈； 3. 引入 SBOM 管理，通过 SCA 管控开源组件风险。	HSM、SecOC、IdsM、SBOM、TARA、ISO/SAE 21434
四维图新	地图与数据服务商	1. 车端采集数据实时脱敏； 2. 商用密码端到端加密，数字证书建立安全传输通道； 3. 搭建数据安全监管平台；	实时脱敏、商用密码、端到端加密、数字证书（国家数据局典型案例）

厂商/ 参与 方	企业类型	具体数据安全实践	关键技术/标准/认证
		4. 构建“车企—四维图新—云厂商”三方责任分工体系。	
梦达 驰	国际零部件 供应商	1. 采用有线无线一体化集中管理架构； 2. 强化 802.1X 身份访问认证、VLAN 与 ACL 网络隔离、日志审计； 3. 围绕 TISAX 框架提升信息安全管理成熟度。	TISAX、802.1X 认证、 VLAN/ACL 隔离
中国 汽研	检测机构	1. 承建“汽车行业可信数据空间”国家试点（18PB 数据集，支撑 18 类场景）； 2. 牵头“国资央企可信数据空间”试点（聚焦智驾保险定责、充电安全预警）； 3. 深度参与 GB44495/44496 等国标制定，具备整车及零部件网络安全检测、渗透测试、数据出境合规测评等资质能力。	隐私保护计算、联邦学习、 多方安全计算、可信执行环境
威联 通	数据基础设施提供商	1. 为某全球 Tier1（覆盖大众、丰田、特斯拉）提供 5 大工厂 5000+台设备的数据管理； 2. AI 驱动的入侵检测系统 + WORM 不可变存储技术锁定工艺参数； 3. AES-256 硬件加密保障 GDPR、ISO 27001 合规。	AI 入侵检测、WORM 不可 变存储、AES-256 加密、 ISO 27001
为辰 信安	车联网安全 方案商	1. 基于亚马逊云部署 VSOC； 2. 车载 IDPS 探针覆盖座舱、动力、自动驾驶关键域实时监测； 3. 帮助多家车企满足 WP.29 R155、ISO 21434，通过 VTA 认证。	VSOC、IDPS、WP.29 R155、ISO 21434、VTA 认证



二、治理篇：从合规防御到价值驱动的数据安全治理

智能网联汽车数据安全治理框架是在依据通信行业标准《数据安全治理能力通用评估方法》(YD/T 4558-2023) 的基础上, 针对智能网联汽车产业“车—路—云—网—图”高度融合的独特数据生态, 结合国家已发布的强制性标准与行业监管要求, 进行系统性适配与重构的产物。该框架以“安全保障与产业发展协同共进”为核心指导思想, 遵循《数据安全法》提出的“以数据开发利用和产业发展促进数据安全, 以数据安全保障数据开发利用和产业发展”的基本原则, 将数据安全能力深度植入智能网联汽车的产品定义、设计研发、量产上市及全生命周期运维的每一个环节, 致力于实现从“辅助性合规工作”向“核心产品属性”的范式跃迁。

框架的构建严格遵循两大依据。其一是全国汽车标准化技术委员会归口、工业和信息化部提出的国家标准《智能网联汽车 数据安全管理体系规范》(征求意见稿), 该标准为汽车企业建立系统化的数据安全管理体系提供了顶层架构指引; 其二是 2026 年 2 月由工业和信息化部、国家互联网信息办公室、国家发展和改革委员会、国家数据局、公安部、自然资源部、交通运输部、国家市场监督管理总局等八部门联合印发的《汽车数据出境安全指引(2026 版)》, 该指引从业务运行视角将汽车行业涉及重要数据的场景划分为研发设计、生产制造、驾驶自动化、软件升级服务、联网运行五大类别, 为本框架治理专项的划分提供了权威的业务场景分类依据。框架整体由治理目标、治理体系、治理专项、治理维度与治理实践五大核心板块有机构成, 各板块之间形成从“方向确立”到“体系构建”再到“重点聚焦”、“能力建设”直至“落地运行”的完整逻辑链条。治理框架总体结构见图 3。





图 3 智能网联汽车数据安全治理框架

(一) 治理目标：四层价值递进

汽车数据安全治理的核心目标在于构建系统化、层次化的治理框架，实现安全合规、风险防御、价值创造与用户信任的有机统一。相较于传统治理模式仅关注“防御已知威胁”的单一维度，智能网联汽车数据安全治理目标已全面升级：合规维度从满足最低要求向实现合规自动化演进，将监管要求实时映射为技术控制策略；安全维度从防御已知威胁向构建主动免疫能力提升，实现对未知风险的预测与“治未病”；价值维度从将数据安全视为成本中心向数据安全赋能业务创新转变，使其成为企业的差异化竞争力。基于对国内外法规标准与行业最佳实践的系统分析，本框架将汽车数据安全治理目标构建为以下“四层递进式”体系。

1. 第一层：合规底线——治理基石

合规是汽车数据安全治理的起点与基石。汽车数据处理者须满足国内外强制性法规要求，确保市场准入资格，有效规避监管处罚风险。当前，全球主要汽车市场已形成覆盖法律、行政法规、部门规章及强制性或推荐性标准的多层次规范体系，构成了完整的合规约束网络。

国内方面，以《网络安全法》（2017 年施行，2025 年修正，2026 年 1 月 1 日起施行）、《数据安全法》《个人信息保护法》三部基础法律为顶层架构，以《网络数据安全条例》（国务院令第九 790 号，2025 年 1 月 1 日起施行）为三部法律之下最重要的行政法规，辅以《汽车数据安全若干规定（试行）》等行业性规章，并引用《数据安全技术 数据分类分级规则》（GB/T 43697-2024）、《汽车数据通用要求》（GB/T 44464-2024）等基础性国家标准，以及自 2026 年 1 月 1 日起强制实施的 GB 44495-2024《汽车整车信息安全技术要求》、GB 44496-2024《汽车软件升级通用技术要求》和 GB 44497-2024《智能网联汽车 自动驾驶数据记录系统》等三项国家标准，构成了完整且严密的合规框架。

如《汽车数据安全若干规定（试行）》将汽车数据分为“个人信息”和“重要数据”两大类，倡导“车内处理”、“默认不收集”、“精度范围适用”、“脱敏处理”四项原则，要求处理个人信息须通过显著方式履行告知义务，处理敏感个人信息须取得单独同意。《汽车数据出境安全指引（2026 版）》则进一步规定了申报安全评估、订立标准合同、通过认证三种数据出境管理方式的适用条件，提出了九类豁免情形，并面向研发设计、生产制造、驾驶自动化、软件升级、联网运行五大场景细化了重要数据判定规则。三项强制性国家标准分别从整车信息安全、软件升级安全、自动驾驶数据记录三个维度对车辆产品提出了具体的、可验证的技术要求，其中任何一项不满足都将导致车辆无法获得型式批准。

国际方面，联合国世界车辆法规协调论坛颁布的 UN R155 与 UN R156 是全球首个针对汽车信息安全的强制性法规系列。UN R155 要求汽车制造商建立覆盖车辆全生命周期的 CSMS，制造商须先获



得 CSMS 合规证书方可进行车辆型式认证。UN R156 则要求汽车制造商建立 SUMS，同样作为车辆型式认证的前置条件，并要求 OTA 升级须具备升级失败回滚能力，保护软件升级的真实性和完整性，防止未经授权的访问和篡改。这两个法规构成了进入欧盟、日本、韩国等市场的前提条件。欧盟 GDPR 与《数据法案》则从个人数据保护与数据共享维度对智能汽车提出严格约束，其中 GDPR 确立的个人数据处理的合法性、公平性、透明性等基本原则以及数据最小化、存储限制等要求，对处理欧盟居民个人数据的汽车企业具有强制约束力；《数据法案》自 2025 年 9 月 12 日起强制执行并具有域外效力，要求数据持有者遵循公平、合理、非歧视原则提供数据访问。

在合规底线的构建中，企业应当系统梳理上述国内外法规与标准，建立动态更新的合规知识库，并将各项合规要求分解为可量化、可执行的技术控制指标，实现从人工对标向自动化合规监测的演进，使合规状态可感知、合规风险可预警、合规证据可追溯。

2. 第二层：风险防御——治理核心

合规底线强调“依法治理”，解决汽车数据处理活动是否符合外部监管要求的问题；风险防御强调“主动防护”，解决数据在复杂业务场景和动态威胁环境下如何保持安全的问题。相较于以满足法规要求为目标的合规治理，风险防御更加关注安全风险的主动发现、持续控制和动态响应，推动企业由被动满足监管要求向构建自主安全能力转变。

智能网联汽车区别于传统汽车的最大特征在于其已成为持续产生、传输和处理数据的移动智能终端，数据安全风险不再局限于单一环节，而是贯穿数据采集、传输、存储、分析、共享和销毁全过程。汽车数据具有“多源异构、高频流动、多主体参与、高价值敏感”等特点，其风险来源更加复杂：车外环境数据涉及人脸、车牌、道路环境及高精度地理信息，既关联个人隐私保护，又可能涉及国家安全和重要数据保护；车内座舱数据包含语音交互、视觉感知、乘员行为甚至生理特征，是高度敏感的个人隐私数据；车辆运行数据涉及电池状态、电控参数、驾驶行为、车辆轨迹等信息，既具有商业价

值，也可能成为攻击者窃取企业核心能力或实施精准攻击的重要目标。因此，智能汽车数据安全治理面临个人隐私、商业利益、产业安全和国家安全多重风险叠加的挑战。

合规治理关注“满足监管要求”，风险防御更加关注“降低实际安全风险”。当前行业主要面临三方面核心挑战：

(1) 数据风险识别能力不足

随着车路云一体化、自动驾驶、智能座舱等业务快速发展，汽车数据类型和应用场景持续扩展，传统基于业务系统的数据管理方式难以准确识别数据价值和风险等级。虽然《数据安全法》《汽车数据安全 安全管理若干规定（试行）》等法规已提出重要数据、个人信息等分类要求，但企业仍需进一步建立面向汽车业务场景的数据分类分级体系，将法规中的原则性要求转化为车辆采集、智能驾驶、远程服务、研发测试等具体场景下的数据识别规则，实现数据风险的精准评估。

(2) 安全防护能力存在短板

智能汽车数据链路覆盖车端传感器、车载控制系统、通信网络、云平台及第三方服务生态，任何一个环节的安全薄弱点均可能形成攻击入口。传统以边界防护为核心的安全模式难以应对数据持续流动和多方协同处理需求，企业需要构建覆盖数据全生命周期的纵深防御体系。在数据采集阶段，应通过数据最小化、敏感信息识别和脱敏处理降低源头风险；在传输阶段，应利用商用密码、身份认证和安全通信机制保障数据传输可信；在存储和处理阶段，应通过访问控制、数据隔离、可信执行环境、隐私保护计算等技术降低数据泄露和非法使用风险；在运行阶段，应依托安全监测平台开展异常访问检测、风险预警和安全审计，实现由事后处置向主动防御转变。

(3) 供应链安全风险突出

智能汽车产业链涉及整车企业、零部件供应商、软件服务商、云服务平台及数据运营机构等多个主体，数据处理链条长、参与方多，导致单一企业难以独立控制全部安全风险。中国汽车工程研究院股份有限公司在相关研究中指出，当前汽车行业仍存在供应链安全体系建设不足、上下游企业安全能

力不均衡等问题。供应商软件漏洞、第三方接口风险以及数据共享过程中的权限失控，都可能成为攻击突破口。因此，企业需要建立覆盖供应商准入、安全评估、数据访问授权、持续监测和退出管理的供应链安全治理体系，实现从“保护自身系统”向“管理生态风险”转变。

在风险防御体系建设方面，行业应以“主动发现、持续防护、动态响应”为目标，构建覆盖数据资产识别、风险评估、安全控制和监测响应的闭环机制。具体而言，应建立数据资产目录和数据流转地图，实现数据去向可追踪；建立动态权限管理体系，实现数据访问最小授权；结合密码技术、隐私保护计算、可信计算等技术，实现敏感数据安全利用；建设安全运营平台，实现异常行为检测、风险分析和事件响应。

因此，合规底线解决的是汽车数据安全治理的“准入问题”，确保企业达到监管要求；风险防御解决的是汽车数据安全治理的“能力问题”，确保企业面对复杂威胁时具备持续防护能力。二者共同构成汽车数据安全治理体系的基础，其中合规提供边界，风险防御提供韧性。

3. 第三层：价值创造——治理引擎

在保障安全与合规的前提下，汽车数据安全治理应致力于释放数据价值，将数据安全从“成本中心”转变为“价值中心”。数据安全治理的价值创造功能体现在三个层面：

直接价值层面，安全合规本身就是市场准入的前提，直接关系到产品能否上市销售，不合规意味着市场禁入，这已不再是成本问题而是生存问题；

间接价值层面，良好的数据安全治理可降低违规罚款、数据泄露赔偿、品牌声誉损失等潜在风险成本，减少不确定性的经济代价；

增值价值层面，在安全合规框架下有序流通的数据，可支撑自动驾驶算法迭代、车联网服务创新、精准营销等高价值业务场景，创造增量收益。

《汽车数据安全管理办法（试行）》倡导汽车数据处理者在开展汽车数据处理活动中坚持“车



内处理”、“默认不收集”、“精度范围适用”、“脱敏处理”等原则，减少对汽车数据的无序收集和违规滥用，这本质上是在引导行业走向精细化、有节制的数据利用模式，避免“先收集后治理”的粗放发展路径。通过隐私保护计算、联邦学习等前沿技术，企业可在保护数据隐私与安全的前提下开展多方数据协作，支撑自动驾驶算法训练、车联网服务创新、精准营销等高价值场景。例如，多家车企已探索通过联邦学习框架，在不直接交换原始驾驶数据的前提下，实现多家企业驾驶行为数据的联合建模，提升自动驾驶模型的泛化能力与安全性。

4. 第四层：信任构建——治理高地

数据安全治理的最终目标是将安全能力转化为品牌信誉，建立长期稳定的用户信任。智能汽车因其持续采集座舱内生物特征、精确位置轨迹、日常出行习惯等高度敏感信息，用户天然对数据的使用方式与安全保障存在较高的焦虑水平。一旦发生数据泄露或违规滥用事件，不仅将面临严厉的监管处罚，更会影响用户对企业的信誉，而品牌信誉的修复往往需要数年时间和巨额投入。

《汽车数据出境安全指引（2026 版）》通过建立透明、可预期的数据出境管理体系，展现了促进数据安全有序流动的治理智慧，为全球汽车产业数据跨境治理提供了行之有效的“中国方案”，进一步增强国际社会对数据治理政策的理解与信任。这种制度层面的透明度与可预期性，也为企业建立用户信任提供了稳定的政策环境和合规参照。

四层递进式目标体系呈现出自下而上的层层递升逻辑：合规底线是进入市场的“通行证”；风险防御是持续运营的“压舱石”，确保业务在安全边界内稳定运行；价值创造是转型发展的“发动机”，使安全投入转化为经济回报；信任构建则是品牌竞争与产业发展的“制高点”，为企业在全球市场的长远发展奠定不可替代的信誉资产。四者共同构成了智能网联汽车数据安全治理完整的目标金字塔。



(二) 治理体系：三层架构纵深防御

治理体系是框架的技术骨架与运行底座。本框架以国家标准《智能网联汽车 数据安全管理体系规范》征求意见稿中确立的体系架构为指导，构建了从战略指引到全流程管控再到基础支撑的纵深式三层治理体系，分别是数据安全战略层、数据全生命周期安全层和基础安全支撑层。三个层级之间形成自上而下的传导机制与自下而上的反馈机制，确保战略能够落地为具体管控措施，而运行中的实际问题也能够及时反馈至战略层进行动态调整。

1. 数据安全战略层

该层处于体系的最顶端，是推进数据安全治理各项具体工作的战略保障模块。该层要求企业在启动任何具体的安全建设工作之前，必须首先确立清晰的数据安全方针与战略规划。依据国家标准征求意见稿关于组织与职责的要求，战略层需要明确数据安全治理的组织架构与职责分配方案，通常采用决策层、管理层、执行层三层架构。

决策层一般以数据安全领导小组的形式存在，由企业高层领导及相关业务板块负责人组成，负责审批数据安全整体目标和发展规划、发布数据安全管理制度及规范、为各项治理工作提供必要的人力与资金资源保障，并在重大数据安全事件发生时承担统筹协调与最终决策职能。

管理层通常由数据安全管理部门牵头，负责制定具体的管理办法与执行标准、推进数据安全风险评估与合规检查等专项工作的开展、组织数据安全意识培训与技能考核，同时承担与行业监管部门及标准组织的对外协调沟通职能。执行层则由各业务部门与技术支持团队构成，负责将数据安全管理体系要求在本部门的具体业务场景中加以贯彻落实，制定相应的操作细则，并反馈实际工作中遇到的安全需求与改进建议。

战略层强调数据安全文化的培育与沟通共享机制的建立，确保数据安全意识从组织高层向基层全员渗透，形成“人人有责、层层把关”的安全文化氛围。战略层还需要统筹考虑国内外法规的适用性

问题，对于有出口业务或全球研发协同需求的企业，需在战略层面明确不同法域之间的合规优先级与冲突协调机制。

2. 数据全生命周期安全层

该层是体系的核心执行模块，要求企业以数据的采集、传输、存储、使用与加工、提供与公开、删除六大环节为基本管控轴线，针对每个环节中车辆端、路侧设施、云端平台等不同数据驻留环境的特点，设置差异化的安全管控节点与管理流程。

在数据采集环节，重点落实《汽车数据安全管理办法（试行）》倡导的车内处理优先原则，对座舱内人脸、声纹等生物特征数据的采集实施单独的告知同意机制，确保采集行为合法、合规、正当且最小必要，同时采集行为应与汽车的设计、生产、销售、使用、运维等直接相关，不得过度收集与业务无关的数据。在数据传输环节，依据数据敏感程度配置分级加密保护策略，区分车内总线通信、车—云远程通信、车—路侧设施通信等不同传输路径实施差异化的加密强度与认证方式，对涉及重要数据和大量个人信息的传输活动实施增强型保护。

在数据存储环节，明确区分车辆端本地存储与云端集中存储的不同安全要求，对存储介质实施全生命周期管理，对达到使用寿命或需要报废的存储设备执行符合标准的数据清除或介质销毁操作，防止因介质处置不当引发的数据泄露。

在使用与加工环节，建立数据处理环境的分级安全保护机制，对涉及重要数据和大量个人信息的数据处理活动实施双人操作、权限分离等增强管控措施，VPN、堡垒机、云桌面等远程访问通道须经严格的身份认证与权限校验。

在提供与公开环节，对数据对外共享、合作方数据交换、数据出境等场景建立前置审批流程，确保每一次数据对外流动均经过合规评估与授权审批，数据接收方的安全保障能力应经过事前评估。

在数据删除环节，制定明确的数据保留期限与删除触发条件，确保过期数据、无效数据能够被彻

底删除且不可恢复，防止因数据滞留引发的隐私泄露风险。值得注意的是，该层特别嵌入了《汽车数据安全 安全管理若干规定（试行）》所倡导的“车内处理优先”原则，即在功能可实现的前提下，优先将数据处理活动置于车辆端而非云端完成，从物理层面降低数据出车带来的风险暴露面。

此外，在用户个人信息权利响应方面，企业应在车端、车主 App 及官网等主要触点建立统一的用户权利请求受理入口，为用户提供查询、复制、更正、补充、删除个人信息以及撤回同意、注销账号、停止个性化推荐等便捷途径。依据《个人信息保护法》与《网络数据安全管理条例》的要求，企业应明确处理时限（一般权利请求应在十五个工作日内答复，涉及敏感、批量或复杂请求的，可依法延长处理期限并向用户说明理由），并建立覆盖车端存储、云端平台及第三方合作方系统的“跨系统联动删除”机制，确保删除请求被同步执行到全部下游副本与备份。对依法须留存或技术上无法删除的场景，应采用脱敏、匿名化或隔离封存等方式替代处理，并记录处理过程以备监管核查。该机制与前述告知同意机制共同构成完整的用户数据权利保障闭环。

3. 基础安全支撑层

该层位于体系的最底部，是为全生命周期各环节提供可复用通用安全能力的基础模块。该层涵盖分类分级、身份认证与访问控制、监控审计、安全事件应急响应、合作方安全管理等五项通用安全能力。

分类分级是整个体系运转的逻辑起点，企业应当依据《数据安全法》确立的分类分级保护制度，结合《数据安全技术 数据分类分级规则》确立的分类分级技术方法、《汽车数据安全 安全管理若干规定（试行）》关于个人信息和重要数据的分类框架以及行业标准关于四个数据级别的划分规则，制定符合自身业务特征的数据分类分级操作规范，为差异化的安全策略提供依据。

身份认证与访问控制解决的是“谁能以什么权限访问什么数据”这一核心问题，要求企业建立统一的身份管理体系与权限管理矩阵，遵循最小权限原则，防止未授权访问与权限滥用。



监控审计要求企业在车端和云端分别部署日志采集与安全监测工具,对数据的访问行为和操作记录进行持续监控与定期审计,及时发现异常行为并触发告警,实现“监控—识别—追溯”的联动机制。

安全事件应急响应要求企业制定分级应急预案,明确不同类型数据安全事件的响应流程、处置时限与上报路径,并定期开展应急演练检验预案的有效性,确保在数据安全事件发生后能够第一时间阻断威胁、控制影响范围、启动溯源分析。

合作方安全管理则针对智能网联汽车产业链高度分散、涉及大量上下游供应商和第三方服务商的现实特点,要求企业在与外部机构建立数据合作关系之前,对其数据安全保障能力进行背景资质审查与安全评估,并将数据安全要求以合同条款的形式嵌入合作协议,建立合作过程中的持续监督与定期复评机制,防止因供应链环节的安全薄弱而导致整体防护失效。

(三) 治理专项：五大业务场景驱动的差异化治理

治理专项是治理体系的业务载体,解决汽车数据安全治理对象划分问题。由于智能网联汽车覆盖研发设计、生产制造、自动驾驶、软件升级、联网运行等复杂业务环节,不同阶段产生的数据类型、价值属性、敏感程度和安全风险存在显著差异,无法采用统一模式进行管理。因此,本框架依据《汽车数据出境安全指引(2026版)》提出的五大业务场景,将汽车数据安全治理划分为研发设计数据安全、生产制造数据安全、驾驶自动化数据安全、软件升级服务数据安全和联网运行数据安全五大专项。治理专项的核心作用在于将抽象的数据安全要求映射到具体业务场景,明确不同场景下的数据保护重点、风险来源和管控要求,实现“分类治理、精准施策”。

1. 研发设计数据安全

此部分聚焦于车辆量产前的产品研发与测试阶段,核心任务是在不干扰研发效率的前提下,对研发过程中产生的物料清单、设计文档、源代码、测试影像及标注数据实施精准合规管控。

本专项治理重点关注两类数据：产品研发数据的重点管控对象为物料清单、研发设计文档及开发源代码。产品测试数据为开展产品仿真、场地和实际道路测试过程中，收集和产生的标注场景、仿真场景、测试场景数据。

2. 生产制造数据安全

此部分聚焦于车辆量产阶段的生产制造过程，涵盖冲压、焊装、涂装、总装等制造环节产生的工艺数据、设备运行数据和质量检测数据。一辆高阶自动驾驶测试车日均可产生高达 10TB 量级数据，生产制造环节同样面临大规模数据保护压力。

生产制造场景下的重点数据管控对象包括：工艺物料清单与配方数据、生产控制程序源代码、质量检测与缺陷分析数据。治理难点在于生产制造数据涉及多主体协同场景：零部件供应商、整车厂、第三方服务商之间存在频繁的数据交互，需厘清各主体的数据安全责任界面。

3. 驾驶自动化数据安全

此部分聚焦于组合驾驶辅助或自动驾驶功能的开发、部署、应用全过程，涵盖算法设计、模型训练、功能部署及运行监测等环节产生的数据。L3 级及以上自动驾驶车辆需配备 DSSAD，该系统在车辆运行过程中需记录车辆及系统基本信息、车辆状态及动态信息、自动驾驶系统运行信息、行车环境信息、驾乘人员操作及状态信息等，为事故责任认定及原因分析提供技术支撑。

驾驶自动化场景下，治理数据类别主要包含以下几类：驾驶自动化算法文件与算法数据、驾驶自动化算法训练数据、驾驶自动化算法特征数据。

在上述三类数据中，驾驶自动化算法训练数据的合规复杂度最高，也是生成式 AI 专门合规义务与汽车数据安全规则的交汇点。其治理要求来自两条并行的规范轨道：



(1) 汽车数据安全轨道

训练数据作为汽车数据处理活动的产物，须落实《汽车数据安全若干规定（试行）》确立的“车内处理、默认不收集、精度范围适用、脱敏处理”等原则，按照 GB/T 43697-2024 开展数据分类分级，识别其中可能构成重要数据的内容（如可推导敏感地理信息、交通运行信息的汇聚类数据），并依据《汽车数据出境安全指引（2026 版）》判定出境合规路径。需特别指出的是，“车内处理”原则与大模型训练对大规模集中数据集的需求之间存在客观张力，企业应通过脱敏处理、匿名化与分级授权机制，在满足训练样本规模要求的同时落实最小必要原则，不得以模型训练需要为由绕过采集侧的合规约束。

(2) 生成式 AI 轨道

当相关模型能力面向境内公众提供生成式服务时，训练数据须同时满足语料与训练数据的专门安全要求：语料来源合法、可追溯，不得侵犯知识产权与他人合法权益，涉及个人信息或他人知识产权的应具备合法授权或处理依据；数据标注须建立标注规则、标注人员管理与质量抽检机制，标注过程留痕、结果可核验可追溯；预训练与优化训练数据的来源安全、内容安全与标注安全要求，可参照 GB/T 45652-2025 与 GB/T 45674-2025 执行。

(3) 衔接与去重

两条轨道在“重要数据识别与出境管控”上高度重叠。企业应以要求较严者为准建立统一基线，避免按场景分别达标导致同一批训练数据形成两套分级结论；训练数据的重要数据判定结论，应同时作为出境申报、模型发布前安全评估与供应链协作边界划分的共同输入。

4. 软件升级服务数据安全

此部分聚焦于车辆量产上市后的 OTA 全过程，涵盖升级包开发、版本管理、升级任务下发、升级执行及失败处理等环节产生的源代码和相关数据。本场景的核心管控对象为涉及安全驾驶、电池管

理功能的升级软件包对应的源代码。

5. 联网运行数据安全

此部分聚焦于车辆量产上市后联网运行全过程，涵盖车辆与车联网平台、路侧设备、云端系统之间的数据交互、汇聚、分析与应用环节。

(四) 治理维度：四类能力协同发力

治理维度是治理体系的能力支撑，解决如何保障专项要求有效实施的问题。仅明确治理对象并不足以形成实际安全能力，还需要建立与业务场景相匹配的组织、制度、技术和人员保障体系。因此，治理维度从企业治理能力建设角度出发，围绕“谁负责、如何管理、依靠什么技术、具备什么能力”四个方面展开。其中，组织架构明确安全责任主体，制度流程规范治理运行机制，技术工具提供风险防护手段，人员能力保障治理要求有效执行。四类能力共同作用，将五大业务场景中的安全要求转化为可执行、可监督、可评价的治理措施。

在组织架构维度，企业应当参照国家标准征求意见稿中确立的职责分配框架，建立决策层、管理层、执行层三层协同的数据安全组织体系，确保数据安全责任有部门承担、有岗位落实、有人员执行。决策层由企业高层领导组成的数据安全领导小组承担，负责从企业战略高度确立数据安全工作的总体方针与资源保障方案，并对重大大数据安全事项行使最终决策权。管理层由数据安全管理部门牵头，协调法务、合规、风控、内审、业务、人力资源等多个职能部门共同参与，负责将决策层的战略意图转化为可执行的管理制度与工作方案，推进各项专项治理工作的有序开展，并对执行层的工作质量进行监督与指导。执行层由各业务部门和技术团队构成，承担将数据安全要求在日常业务操作中加以落实的直接责任，包括制定本业务场景的操作细则、部署必要的技术防护措施、参与安全培训与考核、及时报告安全事件与风险隐患等。考虑到智能网联汽车产业生态的特殊性，组织架构的建设还需兼顾企

业内部治理与外部生态协同两个层面。在内部，应设置职责明确的“汽车数据安全官”岗位，直接向企业高层汇报数据安全重大事项，该岗位应同时具备数据安全专业技术能力和法律法规解读能力；在外部，应积极参与行业组织、标准化机构、监管部门的沟通协作，及时跟踪政策法规变化与行业最佳实践演进，避免闭门造车式的孤立治理。

在制度流程维度，企业应当构建起分级分类的制度文件体系，通常可分为四个层级。一级文件是由决策层发布的数据安全管理方针与基本原则，体现企业对数据安全工作的总体态度与战略定位。二级文件是由管理层制定的通用管理办法与制度标准，例如数据分类分级管理办法、数据安全事件应急预案、数据出境安全管理制度等，这类文件在整个企业范围内具有普适性的约束力。三级文件则是由管理层与执行层共同制定的面向具体业务场景的操作指南与实施细则，例如智能座舱数据采集操作规范、OTA 升级包安全审查流程、自动驾驶路测数据管理细则等，这类文件需要紧密结合具体业务特征进行定制化编写，避免照搬通用模板导致无法落地。四级文件属于辅助性的过程文档，包括工作计划表、申请审批单、审核检查记录、系统操作日志、数据清单目录等，这类文档虽不直接构成制度规范，但却是制度执行情况的客观凭证，也是内部审计与外部合规检查的重要依据。在制度体系建设中，应当特别注意将 GB 44495、GB 44496、GB 44497 三项强制性国家标准的技术要求转化为企业内部的管理制度与技术规范，确保制度文件与标准条款之间形成可追溯的映射关系。

在技术工具维度，智能网联汽车的技术架构显著区别于传统 IT 系统，其治理工具必须顺应“车端—通信链路—云端或路侧”三层技术架构进行系统性部署。在车端，应部署车用安全芯片与安全网关，实现车内数据加密存储与安全隔离，对座舱摄像头、麦克风等敏感传感器实施基于硬件级可信执行环境的权限管控，确保即便车辆操作系统被攻破，传感器数据也无法被非法获取。同时，车端应部署轻量级入侵检测系统，对车辆控制总线（如 CAN 总线、车载以太网）上的异常数据帧进行实时检测与上报，车外数据中的人脸、车牌目标匿名化检出率应满足行业标准要求。在通信链路端，应实施车—云通信数据的全程加密，采用 TLS、IPsec 等成熟协议保障传输通道安全，同时依托通信运营商

的网络管道能力，对车联网卡的数据流量行为进行安全审计与异常流量建模分析，及时发现数据外传异常。在云端和路侧设施端，应部署数据安全运营管理平台，实现多源安全数据的统一汇聚与态势感知，对重要数据的访问行为实施实时监控与风险预警。对于需要与第三方合作方（如自动驾驶算法开发商、地图服务商等）进行数据协作的场景，可引入隐私保护计算、联邦学习、数据沙箱和机密计算环境等技术手段，使合作方在无法直接接触原始数据的前提下完成模型训练与算法验证，实现“数据可用不可见”的安全协作模式，这既是技术防护的手段，也是价值创造的途径。

在人员能力维度，数据安全治理的最终效果取决于具体执行人员的意识水平与技术能力。企业应当根据不同岗位的角色职责，建立差异化的能力要求与培养机制。对于决策层人员，培养重点在于使其了解数据安全法律法规的基本框架、具备数据安全战略意识、知晓常见的数据安全决策陷阱；对于管理层人员，要求其熟知数据安全法律法规的具体条款、能够识别业务运行中的主要数据安全风险、熟悉合规评估与风险处置的工作流程；对于执行层人员，要求其了解基本的数据安全法律要求、具备相应的安全技术操作能力、熟悉本岗位涉及的数据安全操作规范。在培养方式上，应采取意识培养与技能实训并重的策略。意识培养可通过安全事件案例宣导、数据安全宣传月活动、违规操作情景还原等方式定期开展，帮助员工纠正日常工作有意或无意的危险操作习惯。技能实训则应构建线上线下相结合的培训环境，通过线上学习平台提供标准化课程、线下实战演练（如红蓝对抗、数据泄露应急演练）实现“以战代练”，将静态的理论知识转化为动态的实战能力。为确保培训效果落到实处，还应当建立配套的能力考核机制，将安全意识考核与技能实操考核纳入员工绩效评价体系，形成“培训—考核—反馈—再培训”的人员能力管理闭环。

（五）治理实践：以车型全生命周期为主轴的闭环运行

治理实践是治理体系的运行机制，解决治理能力如何融入业务生命周期的问题。治理专项明确了不同业务环节的安全要求，治理维度提供了支撑这些要求落地的能力基础，而治理实践进一步将二者

嵌入车型生命周期全过程，实现数据安全治理与产品开发、生产制造、运营服务同步推进。本框架以车型生命周期为主轴，将治理要求贯穿规划、建设、运营、优化四个阶段：在规划阶段完成风险识别和合规设计，在建设阶段落实安全能力开发，在运营阶段开展持续监测和风险响应，在优化阶段基于事件反馈和法规变化持续改进，最终形成“规划—建设—运营—优化”的动态闭环。

1. 规划阶段：开展业务场景识别与安全需求设计

规划阶段对应车型定义、项目立项和总体方案设计环节，是数据安全治理前置化实施的起始阶段。该阶段重点围绕五大治理专项开展数据资产识别和风险分析，明确车型全生命周期的数据安全治理要求。

针对研发设计数据安全专项，重点梳理车型开发过程中涉及的设计文档、软件代码、仿真数据、测试数据等研发资产；针对驾驶自动化数据安全专项，重点识别算法模型、训练数据、自动驾驶测试数据以及运行数据的处理边界；针对生产制造数据安全专项，分析制造工艺、生产控制、质量检测等数据流转过程；针对软件升级服务数据安全专项，明确 OTA 升级包、版本管理及升级流程中的安全要求；针对联网运行数据安全专项，梳理车辆、云平台、路侧设施及第三方服务之间的数据交互关系。

在此基础上，依托治理维度中的组织和制度能力开展车型级数据安全规划。企业应明确车型项目数据安全责任主体，建立数据分类分级、风险评估、合规审查等管理流程，并结合技术能力建设要求，形成安全架构设计方案、数据流转分析报告和安全需求清单，为后续研发建设提供依据。

2. 建设阶段：推动安全能力融入产品研发与系统实现

建设阶段对应车型设计研发、测试验证和量产准备环节，是治理要求转化为产品安全能力的关键阶段。该阶段以治理专项确定的数据保护对象为基础，将安全能力嵌入产品设计、系统开发和测试验证全过程，实现“安全左移”。



针对研发设计数据安全专项，应加强研发环境安全管理，通过权限控制、代码保护、测试数据脱敏等措施保障研发资产安全；针对驾驶自动化数据安全专项，应围绕算法开发、模型训练、自动驾驶数据记录等环节，落实数据采集、存储和使用安全要求；针对生产制造数据安全专项，应加强生产工艺、制造程序和质量检测数据保护；针对软件升级服务数据安全专项，应落实 OTA 升级包签名验证、完整性保护和安全传输机制；针对联网运行数据安全专项，应建设车云通信加密、身份认证和访问控制能力。

具体实施过程中，应依托治理维度中的技术、制度和人员能力完成安全能力建设。将 EDR 数据安全、座舱数据脱敏处理、OTA 升级包数字签名验证、远程诊断数据传输加密等安全功能纳入产品需求文档，在系统架构中预留安全芯片、安全启动、安全存储等资源。其中，针对 EDR，应依据 GB 39732-2020《汽车事件数据记录系统》要求，对车辆碰撞前后的关键状态信息进行记录，并通过加密存储、访问控制和完整性校验等措施保障 EDR 数据真实性、完整性和可追溯性。

研发过程中，应通过安全开发规范培训提升人员安全能力，将隐私保护设计原则融入研发流程。在产品发布前，通过仿真测试和实车测试验证安全功能有效性，重点检验 GB 44495-2024、GB 44496-2024、GB 44497-2024 等强制性标准要求是否满足。

3. 运营阶段：开展持续监测与动态风险控制

运营阶段对应车型量产上市后的持续运行环节，是数据安全治理由产品建设向长期运营转变的重要阶段。该阶段围绕车辆实际运行环境，对五大治理专项涉及的数据处理活动开展持续监测和风险控制。

针对联网运行数据安全专项，重点加强车辆联网通信、云端平台处理和数据共享过程中的安全监测；针对驾驶自动化数据安全专项，持续保障自动驾驶运行数据、环境感知数据和系统状态数据安全；针对软件升级服务数据安全专项，保障 OTA 升级过程中的身份可信、版本安全和数据完整；针对研

发设计和生产制造数据安全专项，加强售后服务、技术支持及供应链协作过程中的数据访问管理。

运营阶段依托治理维度中的技术、组织和制度能力实现持续防护。企业应建设车端安全监测机制和云端数据安全运营平台，通过异常访问检测、数据流量分析、安全审计等技术手段及时发现风险；建立安全事件响应机制，明确风险处置流程和责任主体；持续完善数据访问、共享、出境等管理制度，确保车辆运行过程满足法规和标准要求。

对于涉及重要数据跨境传输的业务，应按照《汽车数据出境安全指引（2026 版）》要求开展安全评估、标准合同备案或认证，并做好相关日志留存，实现数据安全责任可追溯。

4. 优化阶段：基于治理反馈推动体系持续演进

优化阶段对应车型生命周期持续改进环节，是数据安全治理能力动态提升的重要过程。该阶段通过对治理专项实施效果进行评估，结合安全事件、风险评估结果以及法规标准变化，对治理措施进行持续优化。

企业应围绕五大治理专项开展周期性复盘。例如，根据联网运行过程中的异常事件优化数据访问控制策略，根据自动驾驶功能升级调整训练数据和运行数据保护方案，根据 OTA 技术演进完善软件升级安全机制，根据供应链变化优化研发设计和生产制造数据管理要求。

优化过程依托治理维度中的组织、制度、技术和人员能力协同推进。通过完善组织职责、更新制度规范、升级技术防护措施、强化人员培训和能力评价，实现治理体系持续迭代。最终形成覆盖车型全生命周期的数据安全治理闭环，使数据安全能力随着业务发展、技术演进和监管要求变化不断提升。

(六) 轻量化路径：面向中小车企与零部件企业的渐进式实施建议

前述治理框架主要面向具备完整研发体系、数据平台和安全运营能力的大型整车企业设计，其特点是业务链条长、数据处理规模大、参与主体多，需要通过组织体系、制度流程、技术平台和运营机

制的系统建设，实现覆盖车辆全生命周期的数据安全治理。然而，对于中小车企、新势力初创企业以及零部件供应商而言，其业务范围、数据规模和组织资源与大型整车企业存在显著差异，若直接复制大型企业的治理体系，容易出现建设成本过高、专业人员不足、制度与业务脱节等问题。因此，中小企业的的天数据安全治理不宜追求“大而全”的体系建设，而应结合自身业务定位和数据处理特点，采取风险导向、成本可控、能力递进的轻量化治理路径。

中小企业实施数据安全治理的核心目标，不是在短期内建设完整的数据安全管理体系，而是在满足监管要求的基础上，优先识别自身最关键的数据风险点，并通过资源复用、能力借力和重点投入逐步形成安全能力。具体而言，应遵循“先合规、再加强、后体系化”的渐进式实施路线。

第一阶段：合规筑基阶段——满足准入要求，建立基本治理能力。

对于资源有限的企业，应优先围绕监管明确要求开展基础建设，重点满足《汽车数据安全若干规定（试行）》以及 GB 44495-2024、GB 44496-2024、GB 44497-2024 等强制性标准提出的数据安全要求。企业无需一开始建设复杂的数据安全运营平台，而应首先完成数据资产识别、数据分类分级、个人信息保护、重要数据识别、安全责任明确等基础工作。在技术层面，优先落实车外数据匿名化处理、敏感数据加密存储、默认不收集、数据访问权限控制、安全传输等关键措施，形成满足车辆产品准入要求的“最小可合规能力集”。

第二阶段：风险增强阶段——聚焦高风险环节，提升关键防护能力。

在完成基础合规建设后，企业应根据自身业务特点开展风险识别，避免平均投入导致资源浪费。对于整车企业，应重点关注智能座舱、自动驾驶、OTA 升级、远程诊断等高数据价值场景；对于零部件企业，则应重点关注研发数据、软件代码、测试数据以及与整车企业交互过程中的数据安全风险。企业应按照数据敏感程度和业务影响范围实施差异化投入，将有限资源优先配置于重要数据、敏感个人信息以及外部共享频繁的数据环节。例如，可优先采用成熟的数据加密组件、身份认证服务、安全开发工具，而非投入大量资源自主研发完整安全体系。



第三阶段：体系完善阶段——形成持续运营的数据安全治理能力。

随着企业业务规模扩大、车型数量增加以及数据应用场景丰富，企业应逐步从满足单点安全要求向体系化治理转变。此阶段可逐步完善数据安全治理组织、制度流程、安全运营平台和供应链管理机制，建立覆盖数据采集、传输、存储、使用、共享、销毁全过程的治理闭环。对于暂无能力自建安全运营团队的企业，可通过第三方安全服务、行业公共平台以及产业链协同机制，实现安全能力共享。

在实施方式上，中小企业应充分利用产业生态降低治理成本。一方面，可通过联合检测、共享测试资源、复用整车企业或头部供应商成熟安全组件等方式减少重复投入；另一方面，可采用云安全服务、托管式安全运营服务、密码服务平台等方式，以服务采购替代大规模基础设施建设。同时，应积极参与行业组织和公共服务平台建设，利用行业安全监测预警、标准培训、漏洞响应和技术指导等公共能力，弥补专业人才不足的问题。

轻量化治理并不意味着降低安全要求或规避监管责任，而是在企业资源约束条件下，对治理内容进行优先级排序和能力复用。无论企业规模大小，只要涉及个人信息、重要数据以及车辆安全相关数据处理活动，均必须满足法律法规规定的强制性要求。轻量化路径的本质，是通过“重点保障关键风险、逐步完善治理能力、充分利用产业生态”的方式，使中小企业能够以可承受成本建立适应自身业务特点的数据安全治理体系，实现从“满足监管要求”向“具备持续安全能力”的平稳演进。



三、 技术篇

技术能力框架是智能网联汽车数据安全治理体系的技术底座与能力中台,为数据安全策略的落地执行提供系统化技术支撑。本章严格遵循汽车数据全生命周期安全保护的内在逻辑,按照数据采集、数据存储、数据处理、数据传输、数据共享、数据销毁、安全运营保障七个环节,对关键技术能力进行体系化梳理与阐述。

在体系定位上,数据生命周期技术能力构成横向底层支撑,与研发设计、生产制造、驾驶自动化、软件升级、联网运行五大治理专项形成纵向映射关系——前者回答“用什么技术手段保障安全”,后者回答“在什么业务场景中落地应用”。不同生命周期阶段的安全技术,依据汽车数据在不同业务域的流转特征,在各治理专项中承担核心主导或辅助支撑作用。

特别地,随着大模型与智能体技术在汽车研发、制造和运营体系中的深度渗透,可将智能体能力作为贯穿全生命周期的智能增强层,嵌入资产自动发现与分类分级、动态访问控制策略推演、风险行为关联分析、安全运营自动化编排等环节,通过语义理解、多源信息融合与任务自主编排,显著提升安全治理的感知深度与响应效率。但需要明确边界:加密、身份认证、访问控制执行、数字签名等确定性安全机制仍由传统安全组件独立承载;涉及权限变更、生产控制指令下发、模型版本发布和 OTA 升级包推送等高风险操作时,最终授权必须由策略引擎裁决、审批流程流转及人工复核完成,智能体仅提供辅助决策依据。

表 9 系统梳理了各数据生命周期阶段的核心技术能力,及其在五大治理专项中的支撑关系与作用强度。

表 9 数据安全技术与业务场景映射矩阵

数据生命周期	核心技术能力	研发设计	生产制造	驾驶自动化	软件升级	联网运行
数据采集阶段	数据可信采集技术	○支撑	●核心	●核心	○支撑	●核心

数据生命周期	核心技术能力	研发设计	生产制造	驾驶自动化	软件升级	联网运行
	数据资产自动盘点与分类分级	●核心	●核心	●核心	●核心	●核心
数据存储阶段	数据加密与密钥管理	●核心	●核心	●核心	●核心	●核心
	存储访问控制与零信任架构	●核心	●核心	●核心	●核心	●核心
数据处理阶段	数据脱敏与隐私保护	●核心	○支撑	●核心	○支撑	●核心
	隐私保护计算与安全多方计算	○支撑	○支撑	●核心	○支撑	●核心
	算法模型与训练数据安全	○支撑	—	●核心	●核心	○支撑
	工业数据处理安全	—	●核心	—	—	○支撑
数据传输阶段	安全通信与完整性保护	●核心	●核心	●核心	●核心	●核心
数据共享阶段	可信数据空间与跨主体安全共享	○支撑	○支撑	●核心	○支撑	●核心
数据销毁阶段	数据安全删除与生命周期管理	●核心	●核心	●核心	●核心	●核心
安全运营保障	安全监测、审计与合规运营	●核心	●核心	●核心	●核心	●核心
	软件供应链与OTA安全	●核心	○支撑	○支撑	●核心	○支撑

(一) 数据采集

采集安全是数据生命周期安全防护的起点,其安全性直接决定后续各环节所依赖数据基础的可信程度。

技术目标:数据采集是汽车数据生命周期的起始环节,目标是保障车辆运行数据、道路环境数据、生产设备工况数据、业务系统操作数据等在产生源头即具备可信身份与完整链路,防止因非法终端接入、数据伪造篡改或采集链路中间人攻击,导致后续数据分析、模型训练和业务决策失效,从根本上扼制数据质量风险向安全风险的传导。

技术原理:数据可信采集通过终端身份认证与双向鉴权、采集环境可信度量、数据采集接口安全管控、数据完整性实时校验等机制,对数据生产主体和采集过程实施端到端的安全验证。

具体技术路径分层展开如下:

车端采集:依托车载安全芯片、可信执行环境及安全启动链,确保摄像头、毫米波雷达、激光雷达、GPS/惯性导航等传感器的数据采集环境可信;采集数据经由数字签名后上传,平台侧对每一条数据进行源身份验证与完整性核验。

生产端采集:通过工业控制系统的设备身份认证、安全接口网关和操作审计,确保产线机械臂、焊接设备、检测仪器等生成的工艺参数和工况数据可靠进入MES,防止虚假数据注入生产溯源链条。

云端接入:部署统一的数据接入认证网关,对来自车端、RSU、移动应用及第三方平台的每一条外部数据进行来源可信验证、格式合规检查和完整性校验,确保数据湖和实时计算引擎的输入干净可信。

成熟度与选型要点:设备认证、硬件安全芯片和可信执行环境等技术已具备较高的产业成熟度,在智能网联汽车和工业互联网领域已有规模化部署实践。当前技术供给充裕,选型的核心挑战在于车企差异化需求的精准匹配。

选型时应重点关注以下维度:



表 10 数据采集技术选型关注重点

关注方向	评估要点
终端覆盖能力	是否支持车载 T-BOX/域控制器、路侧感知设备、工业控制器及传感器等异构终端的统一认证接入
协议兼容性	是否同时支持车载以太网/CAN/DDS 等车载协议及 Modbus/OPC UA 等工业协议的深度解析与安全校验
实时性保障	采集认证与完整性校验的时间开销是否满足车端毫秒级实时响应要求及产线节拍要求
密码合规性	可信根是否支持国密 SM2/SM3/SM4 算法体系，HSM 是否通过国家密码管理局认证
扩展性	是否支持亿级终端规模下的认证吞吐量弹性扩展

(二) 数据存储

存储安全解决数据“静态”时的机密性、完整性与可用性问题，是数据安全防御的纵深屏障。

技术目标：保障汽车数据进入数据库、数据湖、分布式文件系统及边缘存储节点后，在生命周期全过程中始终保持机密性与完整性，防止因存储介质物理丢失、数据库注入攻击、内部越权导出、云存储配置错误或运维人员误操作等造成大规模数据泄露，确保即使存储载体失陷，数据内容仍不可解读。

技术原理：通过体系化的数据加密机制与集中式密钥管理服务（KMS），对静态存储数据实施多层次、差异化的密码保护。

核心技术能力包括：

存储级加密：针对云存储桶、分布式文件系统实施卷级或文件级透明加密，对已落盘数据提供无感知的底层保护，对上层业务应用透明。

字段级加密：针对高敏感字段（如车主身份证号、手机号、精准位置坐标、生物特征模板）在应用层进行单独加密存储，即使数据库被整体导出，敏感字段仍保持密文状态。



数据库透明加密：在数据库引擎层面对表空间、日志文件进行透明加密，无需改造上层应用代码，兼顾安全强度与部署效率。

密钥生命周期统一管理：KMS 系统负责密钥的生成、分级存储、版本管理、自动轮换、备份恢复及安全销毁，实现密钥与数据隔离存储、密码资源统一调度与审计。

在架构设计上，推荐采用“密钥加密密钥（KEK）—数据加密密钥（DEK）”两层密钥体系，DEK 负责具体数据加密并可频繁轮换，KEK 负责加密保护 DEK，二者分离存储、权限独立管控。

成熟度与选型要点：数据加密技术和 KMS 产品目前已高度成熟，国内外主流云服务商及安全厂商均提供企业级解决方案。加密算法、密钥轮换、硬件密码机等基础能力已形成标准产品矩阵。

选型时应综合评估以下要素：

表 11 数据存储技术选型关注重点

评估方向	具体要求
密码算法合规性	须完整支持国密 SM2（非对称）、SM3（杂凑）、SM4（对称）算法体系，并通过国家密码管理局商用密码产品认证
性能影响	加密解密操作对数据库 QPS/TPS 的影响应控制在 10%以内，满足车联网海量数据并发写入和查询的性能要求
密钥管理能力	支持基于时间的自动轮换策略、基于角色的最小权限隔离、密钥版本追溯及合规审计
多环境适配	需同时覆盖公有云、专有云、边缘节点和车端嵌入式环境的统一密钥分发与同步
容灾与高可用	支持多机房 KMS 实例的主备切换，密钥材料跨地域备份，RPO≤30 分钟

(三) 数据处理

数据处理涵盖数据清洗、融合计算、模型训练与推理等环节，是数据价值释放的核心阶段，也是安全风险最为集中的环节。



1. 数据脱敏与隐私保护技术

技术目标：在数据加工、分析、建模及可视化过程中，对数据中包含的个人信息、商业机密等高敏感内容实施去标识化处理，确保数据在使用流通过程中既充分发挥价值，又不会直接暴露原始敏感信息，实现“用而不见”的安全效果。

技术原理：数据脱敏通过一系列数据变换算法，在保留数据统计特征与业务可用性的前提下，对敏感信息进行不可逆或可逆的变形处理。

核心技术手段包括：

静态脱敏：对生产数据库中的原始数据进行一次性脱敏处理后导入开发测试环境、数据分析平台或第三方合作环境，脱敏后的数据不可还原，适用于非生产场景的数据使用。

动态脱敏：在应用系统或数据中台查询数据时，依据访问用户的身份属性、权限等级和访问场景，实时对返回结果中的敏感字段进行遮掩或模糊化处理，不改变底层存储数据。

去标识化与匿名化：通过泛化、抑制、扰动、微聚集等隐私保护模型（如 k-匿名、l-多样性、t-接近性），在保留数据可用性的前提下降低个体可识别风险，满足个人信息保护法中的去标识化合规要求。

差分隐私：通过向查询结果或统计数据中添加校准噪声，确保输出结果不泄露任何特定个体的存在信息，在统计发布和模型训练场景中提供可量化的隐私损失保障。

成熟度与选型要点：数据脱敏技术已在金融、政务、医疗等行业得到广泛部署，汽车行业正处于快速引入和适配阶段。差分隐私技术在学术界已有成熟理论，产业应用逐步从互联网广告场景向汽车数据发布场景延伸。

选型应着重考量表 12 中重点：



表 12 数据脱敏与隐私保护技术选型关注重点

评估方向	考量要点
敏感数据识别准确性	是否内置针对车辆 VIN、位置坐标、人脸图像、声纹等汽车特有敏感数据的识别规则库和脱敏算法库
脱敏效果不可逆性	静态脱敏是否采用不可逆算法，动态脱敏是否支持策略热更新且不落盘中间结果
数据可用性保持	脱敏后数据是否仍支持模型训练、统计分析、关联查询等典型业务操作，失真度可量化评估
实时性要求	动态脱敏对查询响应时间的额外开销是否在可接受范围内（通常<50ms）
审计追溯	脱敏操作日志是否完整记录原字段与脱敏后字段的映射关系（静态脱敏）或脱敏策略匹配记录（动态脱敏），支持合规审计

2. 隐私保护计算与安全多方计算技术

技术目标：在多方参与的数据协作场景中（如跨车企数据联合建模、车路云协同计算），实现在各方原始数据不出域的前提下完成联合统计、联合查询和联合模型训练，破解“数据孤岛”与“数据共享”之间的安全悖论。

技术原理：隐私保护计算是一类面向数据隐私保护的计算范式总称，核心思想是将计算逻辑而非原始数据进行流动，确保数据在协作过程中“可用不可见”。

关键技术路线包括：

安全多方计算：多个参与方各自持有私有数据分片，通过秘密共享、不经意传输、混淆电路等密码协议，在互不泄露各自输入的前提下共同计算目标函数，得到正确输出结果。

联邦学习：各方在本地数据上训练模型子模块，仅上传模型参数梯度（而非原始数据）至中心服务器进行聚合，实现“数据不动模型动”的协作学习范式，同时可通过差分隐私、同态加密等手段进一步增强梯度传输安全。



可信执行环境：基于 CPU 硬件级别的安全隔离环境（如 Intel SGX、ARM TrustZone），在内存中划分出与操作系统隔离的 Enclave，数据仅在飞地内部解密并计算，外界无法窥探。

数据沙箱：在安全隔离环境中提供标准化的数据分析和建模工具，合作方可将数据导入沙箱执行既定分析脚本，但无法将原始数据携带出沙箱环境，实现受控使用。

成熟度与选型要点：联邦学习在汽车行业已有初步落地（如自动驾驶场景的跨场景联合模型优化），安全多方计算和可信执行环境处于从技术验证向小规模部署过渡阶段。整体而言，隐私保护计算技术成熟度呈现出“场景驱动、梯度演进”的特征。

车企选型时需关注：

表 13 隐私保护计算和安全多方计算技术选型关注重点

评估方向	考量要点
计算效率	密码学协议带来的通信轮次和计算开销是否在工程可接受范围（通常 MPC 比明文计算慢 2~3 个数量级）
安全假设	协议所依赖的安全模型（半诚实模型/恶意模型）是否与实际合作方信任关系匹配
算法兼容性	是否支持线性回归、逻辑回归、XGBoost、神经网络等主流机器学习算法
部署门槛	是否具备标准化接口和跨平台部署能力，降低跨企业协作的技术对接成本
监管合规	计算结果是否满足“不还原个体信息”的合规要求，是否支持监管审计接口

3. 算法模型与训练数据安全技术

技术目标：保障自动驾驶算法模型从训练数据准备、模型开发训练、模型测试验证到模型部署上车的全链路安全，防止训练数据投毒、模型后门植入、模型参数逆向还原、模型知识产权窃取等新型安全威胁，确保算法决策的可靠性与可控性。

技术原理：算法模型安全是一个横跨数据层、模型层和部署层的系统性工程，主要技术措施包括：

训练数据安全：对训练数据集的来源进行可信校验，防止攻击者通过污染标注数据或注入恶意样本来改变模型决策边界；实施数据版本管理和溯源追踪，确保每条训练样本的来源、标注记录和预处理操作可审计。

模型鲁棒性增强：采用对抗训练、输入预处理器加固、不确定性估计等方法，提升模型对对抗样本（如道路标志贴纸攻击、雨雾噪声干扰）的抵抗能力，降低模型在极端场景下的误判风险。

模型后门检测与防御：通过神经元覆盖率分析、差分测试和逆向触发分析等技术，检测模型中是否存在嵌入的隐蔽后门，识别模型在特定触发条件下产生恶意输出的安全隐患。

模型知识产权保护：采用模型水印（在模型权重或预测行为中嵌入唯一标识）、模型混淆和加密部署等手段，防止模型参数被非法复制、盗用或逆向提取。

模型安全评估与验证：建立模型上线前的安全测评体系，覆盖功能安全、预期功能安全和网络安全的多维度评估，对模型在未知场景下的决策边界进行充分测试。

成熟度与选型要点：训练数据溯源管理和模型鲁棒性测试工具已有初步商业化产品；对抗训练和后门检测技术主要处于学术研究和早期工程化阶段；模型水印和加密部署在 IT 领域较成熟，针对自动驾驶模型的适配仍在演进中。

选型关键评估维度如表 14：

表 14 算法模型与训练数据技术选型关注重点

评估方向	考量要点
场景覆盖度	是否支持感知模型（目标检测/语义分割）、规控模型（决策规划）和多模态融合模型的安全评估
测试有效性	对抗样本生成和鲁棒性评估是否覆盖雨雾光照变化、物理贴纸攻击、数字域攻击等多维威胁模型
侵入性	安全加固措施对模型精度（mAP/准确率）和推理延迟的影响是否可接受（精度损失≤2%，延迟增加≤5%）

评估方向	考量要点
合规溯源	训练数据溯源管理系统是否完整记录数据版本、标注审核、预处理操作及关联模型版本的完整谱系

4. 工业数据处理安全技术

技术目标：保障生产制造场景中工业控制系统、MES、过程控制系统所产生的工艺参数、设备运行日志、质量检测数据、能耗数据等工业数据在采集、存储、处理全过程中的机密性与完整性，防止工业数据泄露导致核心工艺外流，同时保障数据在工业大数据分析平台中的安全使用。

技术原理：工业数据处理安全针对工业数据“高价值、强时效、低延迟、高可靠”的业务特征，设计差异化的安全技术方案：

工业数据分类与分级管控：依据数据对生产安全和商业价值的影响程度，将工业数据划分为不同安全等级，实施差异化的加密、脱敏和访问控制策略，避免“一刀切”式的过度保护影响生产效率。

工业时序数据安全处理：针对产线传感器产生的海量时序数据（如温度、压力、振动频率），在保证毫秒级写入吞吐的前提下，对敏感标签字段进行轻量级加密或编码混淆，降低数据泄露风险。

工业数据质量校验：在数据进入分析平台前进行异常值检测、数据对齐校验和一致性核查，排除因传感器故障、通信干扰或恶意注入导致的异常数据干扰生产决策。

生产数据隔离与沙箱分析：对涉及核心工艺参数的生产数据在分析环境中实施网络隔离和虚拟沙箱，分析师仅可通过预定分析接口操作数据，无法直接访问原始工艺文件。

成熟度与选型要点：工业数据安全在能源、制造等行业已有成熟实践，汽车制造领域正处于从“工控安全”向“工业数据安全”的延伸扩展阶段。时序数据加密和沙箱分析方案已有可用产品，需重点关注对汽车行业特殊工艺场景的适配能力。



表 15 工业数据处理技术选型关注重点

评估方向	考量要点
工业协议兼容性	是否兼容 OPC UA、Modbus TCP、PROFINET、EtherCAT 等主流工业以太网协议及现场总线协议的数据特征
实时性能保障	安全处理引入的延迟是否控制在 5ms 以内，是否满足产线节拍和闭环控制的时间约束
系统高可用性	安全组件故障时是否支持自动旁路（Fail-open）机制，避免因安全系统异常导致产线停产
工艺数据保护粒度	是否支持对 MES 中特定工艺参数表的列级加密和行级访问控制

(四) 数据传输

传输安全确保数据在车-云、车-车、车-路、云-云等异构网络节点间流转时，不被窃听、篡改或劫持。

技术目标：保障汽车数据在网络传输过程中的机密性、完整性与真实性，防止数据在传输链路中被中间人截获、窃听、篡改或重放，同时确保通信双方的身份真实可信，构建覆盖车内外全通信链路的端到端安全传输通道。

技术原理：安全通信通过加密协议、身份认证和完整性校验的组合机制，构建多层次的传输安全体系：

车云安全通信：基于 TLS 1.3/DTLS 等标准化安全传输协议，结合国密算法套件，建立车载终端与云端平台之间的双向认证加密通道；采用证书体系（X.509 或国密证书）进行设备身份认证，防范中间人攻击和假冒终端接入。

车内网络安全通信：对车载以太网、CAN/CAN-FD 总线等车内通信实施 MAC（消息认证码）或数字签名保护，确保 ECU 之间的通信报文来源合法且未被篡改；对关键控制指令（如制动、转向）采用更高级别的安全保护，防止恶意报文注入。



V2X 安全通信：基于蜂窝车联网直连通信和 PC5 接口，按照标准定义的证书体系实现车辆与路侧设备、车辆与车辆之间的安全认证和消息签名，保障 V2X 消息的真实性、完整性和防重放，支持假名证书机制以保护车辆隐私。

云际安全通信：在多云环境和跨数据中心场景中，部署云间加密隧道和微服务网格中的 mTLS 双向认证，保障企业级数据在不同云平台和管理域之间传输时的安全。

完整性校验与防重放：对每条传输消息附加基于 HMAC 或数字签名的完整性校验值，配合时间戳和序列号机制，有效检测和阻断数据篡改与重放攻击。

成熟度与选型要点：TLS/DTLS 协议栈和 PKI 证书体系已高度成熟，在车联网领域已有规模化商用部署。V2X 直连通信安全基于 C-V2X 标准体系，国内已建成多个根 CA 和中间 CA 体系，产业生态逐步完善。车内 CAN 总线的安全保护（如 SecOC）在主流车企中正加速部署。

选型重点考量：

表 16 数据传输技术选型关注重点

评估方向	考量要点
协议栈完备性	是否完整支持 TLS 1.3、DTLS 及国密 SSL 协议套件，证书格式是否兼容 X.509 和国密双证书体系
车端资源适配	安全通信协议对车端计算资源（CPU 占用率<5%）和功耗的影响是否可控，是否支持硬件加速（如 QAT）
V2X 证书体系兼容性	是否兼容国内 V2X 根 CA 及中间 CA 体系的证书格式、吊销列表（CRL）分发机制和假名证书管理策略
连接弹性与容错	是否支持断线重连、会话恢复和网络切换时的连接保持，是否具备弱网环境下的自适应安全降级策略
通信低延迟	安全握手和加密处理引入的额外延迟是否满足车端实时控制要求（端到端额外延迟<20ms）

(五) 数据共享

数据共享在释放数据要素价值的同时，也引入了数据跨信任域流动的泄露风险，需要在开放与安全之间建立精密的平衡机制。

技术目标：在数据跨企业、跨平台、跨行业共享协作场景中，保障数据在共享全过程中的可控、可审计、可追溯，实现数据所有权与使用权的分离——数据提供方不失去对数据的控制权，数据使用方在授权范围内高效使用数据，防止数据被滥用、超范围使用或二次转售。

技术原理：可信数据空间（Trusted Data Space）提供了一套数据主权可控的共享技术框架，核心机制包括：

数据使用控制策略：数据提供方在共享数据时绑定细粒度的使用策略，包括“可使用多少次”、“可合并哪些数据字段”、“计算结果是否可导出”、“有效期多长”等约束条件，由可信中间方或可信执行环境执行策略强制，确保数据使用行为严格遵循授权协议。

联邦计算与密文计算共享：在数据不出域的前提下，通过联邦学习、安全多方计算等技术完成跨企业联合分析任务，各方仅获得最终分析结果（如统计报表、联合模型参数），无法获取其他参与方的原始数据。

数据溯源与沙箱审计：在数据共享分析环境中记录完整的数据访问和计算操作日志，包括数据被谁访问、何时访问、执行了什么操作、输出了什么结果，支持事后审计追责；配合区块链技术，实现操作日志的不可篡改存储，增强追溯可信度。

数据使用权凭证体系：基于数字凭证机制，数据需求方每次申请数据使用权限时，平台自动生成具有唯一标识和策略绑定的访问凭证，数据访问时验证凭证的有效性和策略匹配性，实现最小权限的数据共享授权。

数据安全分级共享策略：依据数据敏感度分级（如 L1-L4），制定差异化的共享策略——L1 级公开数据可直接共享；L2 级内部数据经脱敏后对外共享；L3 级高敏数据通过沙箱或联邦计算方式共享；

L4 级核心数据原则上不允许对外共享。

成熟度与选型要点：可信数据空间理念在欧盟及国内数据要素市场建设中受到高度关注，已有多个行业级和城市级数据空间试点项目推进。汽车行业处于从概念验证向场景落地过渡阶段，技术标准和应用规范尚在形成中。联邦学习和隐私保护计算相对成熟，可优先部署；使用控制策略执行引擎和区块链溯源系统需进一步行业适配。

选型需侧重以下方面：

表 17 数据共享技术选型关注重点

评估方向	考量要点
策略表达能力	策略描述语言是否支持时间约束、频次约束、聚合条件、用途约束等典型共享场景策略的声明和动态组合
执行安全性	策略执行点（PEP）是否具备防绕过能力，策略决策点（PDP）的决策逻辑是否可独立审计
数据共享性能	共享分析任务的吞吐量和延迟是否满足业务需求，大规模并发场景下策略评估的响应时间是否可控
汽车行业适配	是否内置针对车路协同、售后数据共享、保险联合建模、交通管理数据协作等汽车典型共享场景的策略模板和接入标准

(六) 数据销毁

数据销毁是数据生命周期的终点，也是防止数据“终身泄露”的最后一道关口。

技术目标：确保汽车数据在超出法定保存期限、业务不再需要或应数据主体删除请求时，数据及其所有副本被彻底、不可恢复地删除，防止已销毁数据被通过数据恢复工具、存储介质物理分析或备份残留等手段重新获取，从时间维度上彻底关闭数据泄露通道。

技术原理：数据安全删除需覆盖从逻辑删除到物理销毁的多层级技术手段，并贯穿数据全生命周期的末端管理：



逻辑安全删除：对数据库记录、文件系统中的数据执行多次覆写（如 DOD 5220.22-M、Gutmann 等标准算法），使原始数据无法通过常规数据恢复工具还原；对云存储对象执行分片覆写后删除元数据索引，确保底层存储块不可恢复。

密钥销毁式删除：对于加密存储的数据，通过直接销毁对应的数据加密密钥（DEK），使密文数据在数学意义上永久不可解密，实现“秒级销毁”效果，尤其适用于大规模云存储场景的数据快速销毁。

存储介质物理销毁：对于硬盘、固态硬盘、车载存储芯片等物理介质，通过消磁、物理破碎、高温熔融等方式彻底破坏存储单元，确保即使介质物理丢失也不会导致数据泄露，适用于报废车辆和退役设备的存储介质处理。

备份数据同步删除：建立数据删除的级联机制，在删除主数据的同时自动追踪并删除所有关联副本，包括离线备份、异地灾备、边缘缓存、数据分析临时表等，消除因备份残留导致的数据恢复风险。

删除确认与合规存证：对每一条数据删除操作生成不可篡改的删除凭证（包括删除时间、执行人、删除方式、验证结果），满足监管审计和用户知情权的追溯要求。

成熟度与选型要点：数据覆写删除和物理销毁技术在 IT 领域已非常成熟；密钥销毁式删除近年来随云存储普及而快速发展；备份同步删除和全链路删除追踪需要存储架构层面的系统性设计，对既有系统的改造成本需审慎评估。

选型评估重点见表 18：

表 18 数据销毁技术选型关注重点

评估方向	考量要点
删除粒度与精准度	是否支持按数据表、按字段、按存储桶、按车型、按用户 ID 等灵活粒度的精准删除，避免误删或漏删
删除时效性	删除操作是否支持指定时间窗口内的自动调度执行，是否支持紧急情况下的即时删除（<1 分钟生效）

评估方向	考量要点
副本追踪完整性	是否具备数据流向追踪能力，可自动发现并处理经 ETL 任务、数据复制、备份策略产生的所有数据副本
介质适配性	是否兼容 HDD、SSD、NVMe、eMMC 等主流存储介质类型的不同擦除特性（SSD 需额外关注块擦除和磨损均衡的影响）
合规存证能力	删除凭证是否包含加密数字签名和时间戳，是否支持第三方审计机构的独立验证

(七) 安全运营

安全运营保障技术为全生命周期的数据安全提供态势感知、持续监测、风险响应和体系改进能力，是数据安全治理体系的“中枢神经”。

1. 安全监测、审计与合规运营技术

技术目标：实现对汽车数据全生命周期安全状态的持续监测与动态感知，及时发现数据异常访问、越权操作、数据泄露及合规偏离等安全事件，并具备快速溯源、取证分析和自动化响应处置能力，推动安全运营从事后被动应对向事前主动防御演进。

技术原理：安全监测与审计通过数据采集、分析研判和响应处置的三层能力架构，构建闭环的安全运营体系：

全链路数据安全监测：在数据流转的关键节点（采集网关、数据库、API 网关、数据共享接口、终端设备）部署轻量级探针，实时捕获数据操作行为日志和流量元数据，构建覆盖数据全链路的安全监测视图。

用户与实体行为分析：基于机器学习算法对数据访问行为建立基线模型，自动识别偏离正常模式的异常行为（如非工作时间的大量数据导出、非常用 IP 的权限提升操作、异常高频的数据查询），降低对固定规则的依赖，有效检测内部威胁和账号失陷。



数据安全态势感知与可视化：通过安全信息与事件管理（SIEM）平台对多源日志进行归一化处理 and 关联分析，以数据流向拓扑图、风险热力图、合规态势仪表盘等形式可视化呈现数据安全整体态势，支持决策者快速掌握风险全貌。

智能告警与自动化响应：基于预定义的响应剧本（Playbook），对低置信度的异常事件自动执行调查取证操作，对高置信度的攻击事件自动触发阻断、隔离、降权等响应动作，结合智能体技术实现告警降噪与上下文增强，将安全运营人员的平均响应时间（MTTR）大幅缩短。

合规运营与审计报告：内置数据安全法规（如《数据安全法》《个人信息保护法》《汽车数据安全 全管理若干规定（试行）》）合规映射规则库，支持自动化合规检查、差距分析和审计报告生成，确保安全运营与合规要求保持同步。

成熟度与选型要点：SIEM 和 UEBA 技术在 IT 安全领域已发展多年，成熟度较高，但在汽车行业的落地需解决车端日志异构性、数据量大、语义复杂等挑战。智能体驱动的自动化响应为近年兴起方向，需循序渐进推进，不宜追求全自动化。

选型评估侧重见表 19：

表 19 安全监测、审计与合规技术选型关注重点

评估方向	考量要点
汽车数据源适配性	是否支持接入车端 T-BOX 日志、OTA 平台日志、DSSAD、V2X 通信日志等特有数据源和格式解析
实时数据处理能力	是否支持每秒百万级数据操作事件的实时采集、索引和分析，满足车联网规模下的监测吞吐量需求
智能分析准确率	异常检测模型的误报率和漏报率是否控制在可接受范围（误报率<5%，漏报率<1%），是否支持模型在线更新
自动化响应安全性	自动化响应动作是否设有安全围栏和人工确认机制（尤其是涉及车辆控制的操作），是否支持响应操作的回滚

评估方向	考量要点
合规规则更新	合规映射库是否支持法规更新的动态同步，是否具备自定义合规规则的低代码配置能力

2. 软件供应链与 OTA 安全技术

技术目标：保障汽车软件从开发构建、第三方组件引入、测试验证到 OTA 升级交付的完整供应链安全，防范开源组件漏洞、SBOM 不透明、构建过程被篡改、升级包被仿冒或劫持等供应链侧攻击风险，确保每一行运行在车端的代码和每一个软件版本来源可信、内容完整、过程可追溯。

技术原理：软件供应链安全覆盖从代码到车端的完整链路，OTA 安全作为供应链交付环节的关键承载，二者紧密耦合：

SBOM 管理：建立完整的软件成分清单，系统记录每一个开源组件、第三方库、中间件的名称、版本、许可证和依赖关系，与 CVE/NVD 等漏洞库联动，及时识别和修复供应链已知漏洞。

安全开发与构建：在 CI/CD 流水线中集成 SAST、SCA、容器镜像扫描等安全工具，对构建过程中使用的编译器和构建工具进行完整性校验，防止构建环境被污染导致植入恶意代码。

数字签名与升级包保护：对 OTA 升级包使用车企私钥进行数字签名，车端在安装前验证签名有效性，确保升级包来源于合法发布者且内容未被篡改；升级包分发过程采用加密通道，防止在下载过程中被劫持替换。

OTA 安全协议与终端验证：车端与 OTA 平台之间采用双向认证和会话密钥协商，建立安全升级会话；升级前对终端 ECU 的软硬件版本和兼容性进行验证，防止版本回退攻击和不匹配升级导致的车辆异常。

升级失败回滚与应急响应：建立升级失败的安全回滚机制，确保升级过程中断或验证失败时车辆能够恢复到上一个稳定版本；对升级过程中的异常事件进行实时上报和应急响应，最小化升级风险对车辆运行的影响。



成熟度与选型要点：SAST/SCA 工具在 IT 领域高度成熟，需适配嵌入式 C/C++ 及 AUTOSAR 等汽车软件栈的特殊检测需求。OTA 安全协议和升级包签名机制已在主流 OTA 方案中得到商用部署，版本回退防护和失败回滚能力需根据车端存储资源和升级策略进行定制化设计。

选型评估侧重见表 20：

表 20 软件供应链与 OTA 技术选型关注重点

评估方向	考量要点
汽车软件栈适配	SAST 工具是否支持 AUTOSAR C++14 编码规范、MISRA 规则的静态分析，SCA 工具是否覆盖嵌入式领域常用开源组件库
SBOM 标准化	是否支持 SPDX、CycloneDX 等主流 SBOM 格式的生成、导出和自动化漏洞关联分析
OTA 安全协议完备性	是否支持升级包端到端签名、车端验签、版本防回退、分片校验和断点续传的安全保障机制
终端环境适配	车端验签的计算开销是否满足 ECU 资源约束，升级安全策略是否支持不同域控制器（智能座舱域/自动驾驶域/车身域）的差异化配置
应急与回滚能力	是否支持升级失败的自动回滚、灰度升级的安全观察期策略以及升级异常事件的实时上报通道



四、 实践篇

智能网联汽车数据安全治理最终需要依托技术体系落地实施。随着 SDV、车路云一体化、AI 和数据要素市场的发展，汽车数据已呈现出来源多元、流动复杂、价值密集等特点，传统以边界防护为核心的安全模式已难以满足全生命周期的数据安全需求。当前行业正逐步形成“车端可信、通信可信、云端可控、数据可管、价值可用”的一体化安全体系，将数据安全能力深度嵌入研发设计、生产制造、联网运行、驾驶自动化及软件升级等全过程，实现安全能力由“事后防御”向“内生安全、持续运营、价值赋能”转变。实践中，应结合不同治理场景的业务流程、数据类型和风险特征，对技术篇所述各项安全能力进行组合配置，并将智能体能力融入其中，用于辅助处理跨系统信息关联、复杂风险研判和安全流程协同等传统单一工具难以高效完成的任务。以下分别围绕研发设计、生产制造、驾驶自动化、软件升级和联网运行五类场景，说明相关技术能力的具体落地方式。技术篇表 9 已从数据生命周期视角梳理各项技术能力与五类业务场景之间的支撑关系。本篇在此基础上，进一步结合各场景的具体业务流程和风险特征，将主要安全风险与重点技术能力进行对应，并通过场景图示呈现其具体应用关系。

(一) 研发设计数据安全

研发设计场景涉及车型与系统设计、软件与算法开发、模型训练、仿真测试、版本发布及供应商协同等业务环节，其主要安全风险及重点技术能力如图 4 所示。





图 4 研发设计场景风险与技术支撑

1. 场景特点

研发设计阶段是汽车数据和核心技术形成的源头，覆盖车型定义、系统架构设计、软件开发、算法训练、仿真测试、场地测试及实际道路测试等活动。该阶段的数据具有以下特点：

- 软件源代码、自动驾驶算法、ECU 配置参数、数字样车模型、BOM 物料清单、标定参数等数据，直接体现企业的产品架构和核心技术能力。
- 数据类型复杂且关联性强。除结构化的配置参数、物料清单外，还包括测试影像、点云数据、场景数据、标注数据、模型参数、仿真结果及研发日志等非结构化或半结构化数据。单项数据可能敏感程度不高，但在与车辆型号、道路环境、传感器参数及算法版本汇聚关联后，可能形成更高等级的数据安全风险。
- 数据流转主体多、链路长。研发数据通常需要在整车企业、零部件供应商、算法公司、测试机构、地图服务商和云服务商之间流转，且可能涉及跨组织协同开发、远程调试和境内外联合研发。
- 研发效率与安全管控存在平衡要求。研发活动具有高频修改、快速迭代、多人协同和算力资源

源动态调度等特征，过度依赖人工审批容易影响研发效率，因此需要将数据安全策略嵌入代码仓库、数据平台、仿真平台及 CI/CD 流水线，实现自动化控制。

2. 主要安全风险

研发设计阶段的安全风险不应仅理解为单一的数据泄露风险，而应从“身份—数据—平台—模型—供应链”完整攻击链进行分析，主要包括：

- 研发人员、供应商人员或外包人员账号被盗用，导致攻击者越权访问源代码、算法模型和测试数据；
- 访问密钥、数据库口令、云服务令牌等秘密信息被硬编码在源代码或配置文件中，并随代码提交至公开仓库；
- 研发数据分类分级结果未与技术策略联动，重要数据仍可通过邮件、即时通信工具、移动存储介质或公共网盘外发；
- 训练数据来源不明、标注过程不可追溯或样本被恶意修改，造成模型精度下降、决策偏差或植入后门；
- 仿真平台、测试工具或场景库被篡改，使测试输入、测试过程或测试结果失真，影响产品安全验证结论；
- 开源组件、第三方 SDK、开发插件、容器镜像和构建工具存在漏洞或恶意代码，引发软件供应链风险；
- 联合研发和委外开发过程中，合作方安全能力不足，出现代码仓库配置错误、研发数据违规留存或未经授权转交等问题。



3. 技术实践体系

研发数据安全技术实践的核心，是将分类分级、最小权限与全生命周期保护转化为研发工具链中的可执行策略，并形成可追溯的技术证据。本场景最具特色的是“源代码与秘密防泄露”能力：通过代码仓库管控、硬编码秘密扫描与秘密管理平台联动，从源头阻断核心资产外泄。本场景的完整技术实践直接承接技术篇数据资产自动盘点与分类分级、源代码与软件供应链安全等能力（见技术篇表9），以下结合研发场景特点展开落地要点。

(1) 建立数据资产自动发现与安全标签体系

将源代码、测试数据、算法模型、仿真场景、研发文档、BOM 及云资源纳入统一资产目录。通过接口扫描、元数据采集及内容识别，自动标注数据所属项目、类型、密级与使用限制，形成机器可读的安全标签（如“L4 级算法—禁止外发”）。对于研发文档、训练数据、仿真场景及模型文件等难以依靠关键词和固定规则准确判断的对象，可进一步由数据治理智能体结合项目、车型、算法版本、数据来源及既有分级规则进行上下文分析，补充识别其敏感属性及关联汇聚后的升敏风险，并形成待确认的分类分级建议。涉及重要数据、禁止外发和跨境限制等关键标签时，经规则校验或人工复核后再正式写入标签体系。

(2) 建设隔离化、零信任研发环境

分域隔离办公、开发、算法、仿真、路测及供应商区，阻断跨域数据无序流转。基于身份、项目、终端状态及行为动态授权，高权限采用即时审批、用后即收。核心区使用虚拟桌面或安全空间，防数据落地；供应商通过堡垒机接入，受限传输与剪贴板。验证重点：MFA、权限时效、非受信终端访问、人员/供应商权限回收。

(3) 强化源代码与秘密防泄露

代码仓库实施分支保护、审核签名及敏感操作审计，核心模块增加双人复核。密钥、口令、令牌等秘密统一存储于管理平台，运行时动态调用，实行短有效期与自动轮换。提交阶段部署扫描拦截，

防止硬编码秘密入库；持续监测公开平台，及时发现凭据和代码泄露风险。为避免秘密扫描、代码检测、组件漏洞和权限审计等结果相互割裂，可通过研发代码安全智能体进行关联研判，识别组合风险、分析影响范围并生成处置优先级和修复工单。经确认发生泄露后，再由代码仓库、秘密管理平台和身份系统执行代码拦截、凭据吊销、密钥轮换及权限调整等处置措施。

(4) 构建训练数据与模型可信链

覆盖数据全流程，记录来源、处理过程与版本，生成哈希防止无痕覆盖。自动化检测样本异常、标签错误及数据损坏，关键场景引入交叉标注与算法审核。模型发布前进行数据投毒与后门检测，包括样本分布校验、差异分析、对抗测试及版本比对。在上述检测结果基础上，可利用模型安全智能体关联数据来源、样本异常、标注质量、数据版本和模型性能，辅助定位异常是否与特定数据批次、标注过程或版本变化有关，提高投毒和后门风险的追溯效率。完成安全检测和风险复核后，正式模型再通过数字签名和发布审批进入部署环节，防止未授权替换。

(5) 保障仿真场景与结果可信

对场景包、模型及脚本实施版本管理与哈希校验。测试自动记录环境参数，确保结果可复现；建立可信基线场景库，变更后自动回归测试，显著偏差触发人工复核。测试报告与原始日志关联存储，关键数据采用时间戳或签名防篡改。

(6) 将供应链安全嵌入 DevSecOps

覆盖开源组件、第三方软件、容器及工具链，不只依赖源码扫描。参照 NIST 与 CISA 要求，禁止使用来源不明或高危组件，引入 SBOM 管理，提升透明度与漏洞响应能力。

(7) 建设受控的供应商协同空间

优先通过企业平台交付代码与数据，按项目、车型、任务隔离，设置有效期、下载限制与水印。沙箱环境允许分析而不导出原始数据；确需导出时，自动核验并执行脱敏、加密、水印及合规审批。跨境传输需衔接数据出境流程。



(8) 形成可量化监测审计闭环

打通人员、设备、代码、模型、流水线日志，构建关联证据链。重点监测批量下载、非授权访问、异常数据传输及模型突变等行为。在统一日志和监测结果基础上，可通过研发安全运营智能体聚合异常访问、秘密泄露、组件漏洞、训练数据异常及模型版本变化等多源事件，补全事件上下文，辅助判断影响范围、归集相关证据并生成处置工单，降低跨平台人工检索和研判成本。在此基础上，设置 MFA 覆盖率、秘密扫描率、血缘完整率、SBOM 生成率等内控指标，持续改进，避免设定缺乏标准依据的阈值。

4. 行业实践实例

丰田 T-Connect 事件：外包商误将含密钥源码公开至 GitHub，影响 29 万用户。教训：覆盖外包仓库、提交前扫描密钥、禁用静态密钥、持续监控公开平台，泄露后同步删除与轮换。

奔驰 GitHub 令牌泄露：员工公开提交含过高权限的访问令牌，或导致内部代码受控。启示：令牌最小权限、短周期、自动轮换，并实时检测公开仓库。

自动驾驶投毒攻防验证：研究显示，污染训练样本可植入模型后门。提示：需检测样本分布、标签逻辑、数据来源，结合交叉标注、后门测试与模型红队评估降低风险。

(二) 生产制造数据安全

生产制造场景涉及供应商与物料协同、生产管理 IT 域、IT/OT 交互、生产执行 OT 域以及质量检测与整车下线等业务环节，其主要安全风险及重点技术能力如图 5 所示。





图 5 生产制造场景风险与技术支撑

1. 场景特点

生产制造阶段是智能网联汽车硬件落地、软件预装与整车功能交付的核心环节，覆盖冲压、焊装、涂装、总装四大传统工艺，以及车载系统刷写、整车标定、下线智能检测、生产端 OTA 配置等智能网联专属生产活动。该阶段的数据具有以下特点：

- 工艺配方、产线控制程序、核心物料清单、质量检测数据及车载固件、自动驾驶标定参数、车端通信密钥等数据，兼具工业制造价值与智能网联属性，直接决定整车制造质量与智能功能交付能力。
- OT 与 IT 深度融合，数据类型庞杂且汇聚升敏。除结构化的工艺参数、设备运行数据外，还包括下线检测影像、标定点云、软件镜像、生产调试日志等非结构化或半结构化数据。单项数据敏感程度有限，但与车辆 VIN 码、软硬件版本、产线工艺参数关联汇聚后，可能形成更高等级的数据安全风险。
- 供应链协同主体多元，数据交互链路长、责任边界模糊。生产数据通常需要在整车企业、多

级零部件供应商、软件服务商、工控设备厂商、第三方检测机构及物流服务商之间流转，且涉及跨组织工艺协同、远程设备运维、代工厂协作等多类场景。

- 生产连续性与安全管控存在平衡要求。汽车制造属大规模流水线作业，产线停摆经济损失高，且车载软件迭代快、版本调整频繁，过度依赖人工审批与强阻断式管控易影响生产节拍，因此需要将数据安全策略嵌入产线系统与作业流程，实现自动化、无感式控制。

2. 主要安全风险

生产制造阶段的安全风险不是单一的工业数据泄露风险，而是“身份—数据—系统—产线—供应链”完整攻击链，风险同时波及企业核心资产、生产运行连续性与整车交付安全，主要包括：

- 生产管理人员、产线运维人员及第三方服务商账号被盗用或滥用，导致攻击者越权访问工艺配方、产线控制源代码、质量检测数据与车载标定参数，甚至可直接向现场工控设备下发操作指令。
- 工控系统访问凭证、车载固件刷写密钥、生产数据库口令、接口调用令牌等秘密信息被硬编码在产线脚本、控制程序或配置文件中，随生产安装包、运维工具流转扩散，易被窃取并滥用。
- 生产数据分类分级结果未与技术防护策略联动，工艺物料清单、核心配方参数、整车标定数据等重要数据仍可通过工位终端外设、移动存储介质、即时通讯工具或公共网盘违规外发，跨安全域数据流转缺乏有效拦截。
- 质量检测样本、缺陷标注数据来源不明、过程不可追溯或被恶意篡改，造成下线质检 AI 模型漏判、误判；工艺参数、标定数据被非法修改且无完整性校验机制，引发整车制造质量偏差与智能功能交付缺陷。
- PLC 控制程序、机器人作业脚本、车载刷写平台、下线检测系统被篡改，使得工艺执行、软

件预装、质量检测的过程或结果失真，既可能造成生产节拍中断、产线停摆，也可能导致带质量缺陷、带恶意代码的车辆流入市场。

- 工控设备固件、生产管理系统、第三方检测工具、工业软件组件及容器镜像存在已知漏洞或恶意代码，工业软件供应链风险沿 IT-OT 融合链路传导，直接渗透至核心生产控制域。
- 零部件供应商、代工厂、第三方检测机构、设备运维商等合作方安全能力参差不齐，跨主体数据交互责任边界不清，存在生产数据违规留存、超范围使用、未经授权转交等管控盲区。

3. 技术实践体系

生产制造数据安全技术实践的核心，是将工业数据分类分级要求、最小权限原则与全生命周期保护转化为生产控制系统、产线设备与供应链协同链路中的可执行策略，在保障生产连续性与运营效率的前提下，形成可追溯、可审计的技术防护证据链，覆盖工艺落地、产线运行、质量管控、供应链协同全环节。本场景最具特色的是“OT/IT 网络边界隔离与工业协议深度解析”能力：通过工业防火墙、单向网闸与工业协议白名单管控，在保障生产连续性的前提下阻断跨域风险传导。本场景的完整技术实践承接技术篇工业控制网与生产数据安全、零信任与统一身份访问控制等能力（见技术篇表 9），以下结合产线场景特点展开落地要点。

(1) 建立工业数据资产自动盘点与分级标签体系

将工艺物料清单（BOM）与配方数据、产线控制程序源代码、质量检测与缺陷分析数据、设备运行参数、生产调度日志、供应链协同数据等全部纳入统一资产目录。针对工业场景 OT 与 IT 融合的特点，通过工业网关流量识别、MES/PLM/QMS 等系统元数据对接、产线终端探针采集等方式，自动识别数据所属产线、工艺环节、车型批次、处理主体与流转路径，依据工业数据分类分级规则自动标注敏感等级，生成机器可读的安全标签（如“总装核心工艺配方—重要数据—禁止跨境传输”）。标签体系需支持多源数据汇聚后的敏感度自动升档，识别单项数据不敏感但汇聚后形成的重要数据风

险。年营收位于各省行业排名前列的规模以上工业企业，需优先完成全量生产数据资产的盘点与标签落地，形成明确的重要数据目录。

(2) 构建 OT/IT 分域隔离的零信任生产访问环境

按照工业网络安全与数据安全防护要求，划分核心控制域（PLC、工业机器人、现场传感器等）、生产监控域（SCADA、DCS、工业历史数据库）、生产管理域（MES、PLM、QMS、ERP）、办公协同域、外部服务商接入域五大安全域，域间采用工业防火墙、单向网闸实施严格边界管控，默认禁止跨域数据无序流转，仅开放白名单内的工业协议与定向数据流向。基于人员身份、工位终端、操作时段、生产工单实施动态授权，对修改工艺参数、下发现场控制程序等高风险操作，执行双人复核、即时授权、操作后权限自动回收机制。对于“账号具备合法权限但实际行为偏离当前任务”等传统身份规则难以直接判断的情况，可进一步由生产身份与权限分析智能体关联人员角色、工单、终端、访问设备和历史行为，辅助识别异常操作、供应商超任务范围访问及长期冗余权限，并向 IAM 或堡垒机提供权限调整和处置建议；具体权限变更仍由确定性策略和审批流程执行。核心控制区采用安全工业桌面，禁用外接存储与外设接口；外部服务商通过专用堡垒机接入，限制操作指令范围、剪贴板权限与文件传输方向。验证重点包括：工业协议白名单覆盖率、跨域数据流向合规率、非授权终端接入拦截率、离岗人员与服务商权限及时回收率。

(3) 强化产线控制程序与核心工艺数据防泄露

将 PLC 控制程序、机器人作业脚本、产线控制源代码等统一纳入工业代码仓库管理，实施分支保护、版本管控、提交审核与全操作审计，核心工艺段的程序变更必须经过仿真验证与双人复核，禁止直接在线修改现场控制器程序。工艺配方、核心 BOM、关键质量检测报告等重要数据采用字段级加密存储，按工位、工序、角色开放最小必要数据字段，禁止整表批量导出。在生产终端、网络边界部署 DLP 能力，精准识别工业设计文件、工艺文档、检测报告等敏感内容，阻断通过邮件、即时通讯、移动存储介质、公共网盘等渠道的违规外发。产线与上层系统间的数据传输采用加密工业协议，

同步开展数据完整性校验与敏感内容识别。涉及 OTA 升级软件包源代码等与召回相关的生产数据，按监管要求履行事先报告程序后可适用相应豁免条款，同步留存完整备案记录。

(4) 构建工艺参数与质量检测数据全链路可信链

覆盖工艺参数下发、产线执行、数据采集、质检分析的完整流程，为每一批次产品关联对应版本的工艺参数、设备运行日志、质检原始数据与检测结论，生成唯一数据哈希指纹，防止数据被无痕篡改。质量检测的影像数据、缺陷标注、尺寸测量结果自动同步存证，关键检测结论叠加可信时间戳与电子签名，确保质量问题可追溯、检测结果可复现。建立工艺参数可信基线库，对参数变更自动开展偏差校验，对显著偏离基线的操作及时告警并触发人工复核，防范因异常或恶意修改工艺参数引发产品质量与安全风险。对于仅依靠偏差幅度难以判断风险性质的复杂情况，可进一步由生产数据安全智能体关联工艺参数、设备状态、生产批次、质检结果及历史基线，辅助区分正常工艺调整、设备故障和潜在恶意操作，并向生产与质量人员提供关联证据和复核建议。针对质检 AI 模型，对训练样本、标注数据、模型版本做全链路血缘管理，定期开展对抗测试与鲁棒性验证，避免缺陷漏检、误判。

(5) 保障产线控制程序与生产流程可信执行

对 PLC 控制程序、机器人作业脚本、MES 生产调度指令实施严格的版本管理与哈希校验，程序下发至现场设备前，必须完成安全扫描、仿真验证与合规审批，禁止未授权程序直接写入产线控制器。建立生产操作全量审计机制，完整记录程序下发、参数修改、设备调试、系统配置等所有高危操作，关联操作人身份、操作时间、操作内容与审批记录，形成完整操作追溯链。关键生产控制系统采用可信计算底座，对系统启动、程序加载、配置变更做完整性校验，防范恶意代码植入与系统篡改。建立生产数据分级备份机制，重要数据采用“在线+离线”多副本异地存储，定期开展数据恢复与生产应急演练，保障勒索攻击等极端场景下的生产连续性。

(6) 将工业供应链安全嵌入生产协同全流程

覆盖零部件数据交互、工艺协同、设备运维、物流对接等全供应链场景，建立统一的供应链数据

接入标准与安全规范。参照工业领域供应链安全管理要求，对供应商按合作等级与交互数据敏感度分级管理，涉及重要数据的协同场景，强制采用加密传输通道、数据脱敏与溯源水印。引入生产数据物料清单（SBOM）与数据血缘管理能力，明确协同数据的来源、流转路径、使用范围与销毁要求，厘清各主体的数据安全风险界面，提升供应链数据透明度与漏洞响应效率。对工业设备固件、第三方工控软件、运维工具包统一开展安全检测与漏洞扫描，禁止使用来源不明或存在高危风险的工控程序与工具，防范软件供应链风险传导至生产系统。

（7）建设多主体受控的生产协同数据空间

搭建统一的生产协同平台，按车型项目、合作主体、任务类型做数据隔离，为每个合作方分配独立的工作空间，设置数据访问有效期、操作权限与下载配额，所有协同数据内置不可篡改的溯源水印。核心工艺参数、原始质量检测数据等重要数据，优先通过沙箱环境向合作方开放，支持在线查看、分析与标注，禁止原始数据直接导出；确需导出的，自动触发敏感核验、脱敏处理、水印叠加与合规审批流程。针对代工厂、第三方检测机构的数据回传，实行自动格式校验、病毒查杀与敏感内容检测，防止恶意文件、异常数据流入内部生产系统。涉及境外供应商、跨境生产协同的数据交互，自动衔接数据出境合规审批流程：重要数据依法申报安全评估，一般数据按标准合同或认证路径执行，留存完整的出境申报、传输、接收全链路记录。

（8）形成工业场景可量化的安全监测审计闭环

打通 OT 域设备操作日志、工业网络流量日志、IT 生产系统日志、人员访问日志、供应商操作日志，构建生产数据全链路的关联证据链。建立生产安全行为基线，重点监测批量导出重要生产数据、越权修改工艺参数、非授权程序下发、异常跨域数据传输、非工作时段高危操作等行为。在上述监测基础上，可由生产安全运营智能体关联 OT 设备、MES/PLM/QMS、生产工单及供应商运维等多源信息，辅助判断非计划程序下发、异常参数修改和异常运维行为，自动归集相关证据并形成事件摘要和处置工单。考虑生产连续性和现场安全要求，智能体不得绕过工业控制白名单直接向 PLC、工业机器

人等关键设备下发控制指令。由此形成“监控—识别—研判—追溯—处置”的联动机制，并设置可量化的内控指标体系，包括重要数据加密覆盖率、控制程序变更审计率、工业协议白名单命中率、供应商权限及时回收率、数据出境合规率、重要数据备份可用率等。按监管要求每年至少开展一次全面的数据安全风险评估，及时报送评估报告与重要数据目录备案。持续跟踪工业领域数据安全监管规则的动态调整，及时更新内部分级标准与管控措施，实现动态合规。

4. 行业实践实例

捷豹路虎供应链渗透停产事件：黑客通过零部件供应商系统漏洞渗透车企生产网络，导致其英国三家整车工厂及斯洛伐克工厂等停产近六周，核心工艺数据存在外泄风险。教训：IT-OT 融合场景下供应链是核心攻击入口，需强化跨域边界隔离、供应商最小权限管控与生产容灾备份能力。落地建议：对供应商开放的生产网段实施最小权限代理接入并全量审计；核心工艺数据实施“在线+离线”多副本异地备份并定期演练恢复；对高风险供应商实行半年一次渗透测试与安全复评。

沃尔沃供应商数据泄露事件：两家第三方供应链服务商遭网络攻击，导致生产排程、零部件供应等数据外泄，因事前责任边界不清，风险溯源与整改滞后。教训：需将数据安全要求嵌入供应商准入与合同条款，对重要生产数据跨主体流转实行全链路审计与脱敏管控。

(三) 驾驶自动化数据安全

驾驶自动化场景贯穿数据采集与标注、模型训练与验证、模型发布，以及车端感知、自动驾驶运行、DSSAD 记录、运行监测和事故追溯等环节，其主要安全风险及重点技术能力如图 6 所示。



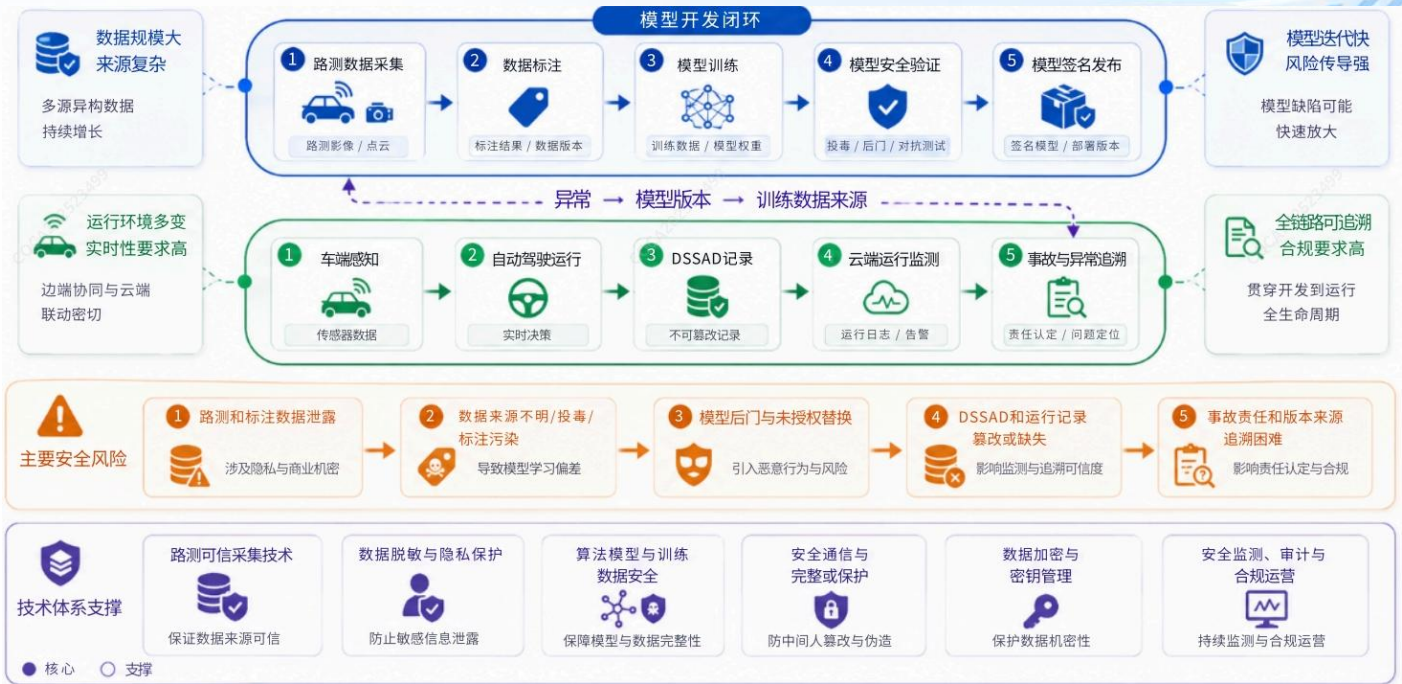


图6 驾驶自动化场景风险与技术支持

1. 场景特点

驾驶自动化阶段是智能网联汽车核心功能落地与运行的关键环节，覆盖算法设计、模型训练、功能部署、车端运行、数据回传及事故追溯全流程，贯穿产品研发、量产交付到上路运行的全生命周期。该阶段的数据兼具技术资产属性、行车安全属性与监管合规属性，主要特点如下：

- 算法源代码、模型权重、训练数据集、特征数据集是企业核心技术资产，直接决定自动驾驶能力层级；同时自动驾驶记录数据是事故责任认定的核心依据，受强制性国家标准严格约束，数据价值与合规权重双重突出。
- 数据类型多元、车内外联动，汇聚衍生风险显著。既包含算法参数、车辆状态等结构化数据，也包含路测影像、雷达点云、场景标注、座舱感知等非结构化数据。单项数据敏感程度有限，但多车、多时段数据汇聚后，可还原敏感区域地理信息、交通运行规律，衍生更高等级的数据安全风险。
- 数据流转链路长，跨场景、跨主体合规要求复杂。数据在算法训练平台、车端系统、云端监

测平台、监管平台之间多向流转，涉及车企、算法服务商、地图厂商、监管机构等多类主体，同时需满足数据出境、事故报送、强制标准等多重合规要求，不同场景的数据处理规则差异大。

- 数据安全与功能安全深度绑定，强制性约束强。自动驾驶数据直接影响系统决策与行车安全，L3 级及以上车型需满足 GB 44497 等强制标准对数据记录、存储、耐撞、信息安全的硬性要求；车外数据匿名化、座舱数据最小化也有明确国标规范，安全管控必须守住强制合规底线。

2. 主要安全风险

驾驶自动化阶段的安全风险贯穿算法开发、模型训练、车端部署到运行追溯全链条，不仅涉及核心技术资产泄露，更会直接影响自动驾驶功能安全与公共道路安全，主要包括：

- 算法开发、运维人员账号被盗用或越权滥用，导致自动驾驶源代码、模型权重、核心训练数据集等高价值资产泄露，甚至被恶意篡改算法逻辑、植入功能后门。
- DSSAD 防护不足，事故数据、运行数据被非法篡改、删除或违规读取，导致事故责任认定失真；车外影像、座舱感知数据违规外泄，触发隐私保护与数据合规风险。
- 训练数据来源不合规、标注过程不可追溯，或样本被恶意投毒，导致自动驾驶模型出现决策偏差、场景漏判，引发行驶安全隐患；数据汇聚衍生的地理、交通敏感信息未被识别，存在合规风险。
- 自动驾驶 OTA 升级包、算法模型在部署传输过程中被篡改，恶意代码或异常模型刷写入车端，直接导致自动驾驶功能异常，甚至被远程控制。
- 车外感知数据、座舱数据未按国标要求完成匿名化、最小化处理，违规向第三方提供或出境，违反数据安全、个人信息保护相关法规与强制性标准。
- 自动驾驶运行监测、事故报送机制缺失，数据记录不满足强制标准要求，无法与监管安全云

平台有效对接，触发监管合规风险与召回责任风险。

- 算法合作方、数据标注服务商等第三方安全能力不足，训练数据、算法特征数据违规留存、超范围使用，形成供应链数据安全管控盲区。

3. 技术实践体系

驾驶自动化数据安全技术实践的核心，是将数据分类分级要求、强制性国家标准与全生命周期保护原则，转化为算法平台、车端系统、云端监测链路中的可执行策略，在保障自动驾驶功能迭代效率的同时，形成合规可追溯的安全防护体系。本场景最具特色的是“算法模型可信防护与 DSSAD 合规”能力：以数据血缘管理、投毒与后门检测、模型签名验证保障算法可信，以 DSSAD 安全技术满足 GB 44497 的强制性要求。本场景的完整技术实践承接技术篇自动驾驶算法与数据安全、数据传输安全防护等能力（见技术篇表 9），以下结合算法平台场景特点展开落地要点。

(1) 建立自动驾驶数据资产盘点与分级标签体系

按算法开发项目逐一盘点算法源代码、模型权重、训练数据集、特征数据集、车端运行记录数据，全部纳入统一资产目录。基于数据敏感程度、汇聚风险、监管要求自动分级标注，重点识别可推导敏感地理信息、经济运行信息的汇聚类数据，生成机器可读的安全标签，形成清晰的重要数据目录。

(2) 构建算法训练与模型全生命周期可信防护

对训练数据实行全链路血缘管理，完整记录数据来源、标注过程、版本迭代，生成哈希校验值防止数据被无痕篡改。自动化检测样本异常、标签错误与投毒风险，关键场景引入交叉标注与算法交叉审核。模型训练、发布、部署全流程执行数字签名校验，发布前开展后门检测、对抗测试与鲁棒性验证。依托上述数据血缘和模型验证结果，可由算法模型安全智能体进一步关联样本异常、标注质量、模型版本及各类测试结果，辅助识别潜在投毒、异常模型行为及其可能的数据来源，并形成发布前风险摘要和待复核事项。完成安全测试和风险复核后，再由数字签名与发布审批控制正式版本，车端仅

加载通过签名认证的模型。

(3) 落实 DSSAD 合规与安全防护

严格对标 GB 44497-2024 强制性标准，保障数据记录完整性、存储可靠性、耐撞性能与读取合规性。对记录系统实行权限隔离与加密存储，防止非法篡改、删除行车数据；车外感知数据向车外传输前，按 GB/T 41871 要求完成人脸、车牌等信息的匿名化处理；座舱数据严格执行“默认不收集、车内处理”原则，最小化采集范围与数据留存周期。

(4) 强化算法与 OTA 部署全链路安全管控

自动驾驶算法包、OTA 升级包实行端到端加密传输与完整性校验，车端设置多重签名验签机制，未授权数据包禁止刷写。升级过程建立全流程审计，记录版本信息、操作时间、对应车辆与操作主体，支持升级失败自动回滚。涉及召回、安全事件处置的 OTA 相关数据，按规定履行事前报告程序，留存完整合规凭证。

(5) 建设运行监测与事故追溯技术能力

搭建自动驾驶运行数据监测平台，按监管要求对接安全大数据云平台，建立事故触发自动报送机制。实现车辆状态、系统运行、环境感知、驾乘操作等数据的全量留存与不可篡改存证，关键数据叠加可信时间戳与电子签名，保障事故溯源时数据完整可信。依托上述可信记录，当车辆出现异常决策、安全事件或事故时，可进一步利用智能体关联 DSSAD 记录、车辆运行状态、环境感知信息、当前模型版本、算法测试记录及对应训练数据批次，辅助形成从“车辆运行异常—模型版本—训练数据来源”的追溯链，缩短跨平台证据检索与问题定位时间。完善数据读取、提取的授权审批流程，满足监管调查与责任认定的合规要求。

(6) 筑牢数据出境与跨主体协同合规防线

严格按数据分级结果落实出境合规路径：重要数据（核心算法源代码、大规模训练数据集等）依法申报数据出境安全评估，不拆分申报；一般数据按标准合同或保护认证路径执行。对算法服务商、

数据标注商等第三方实行分级管理，合同中明确数据安全责任与使用范围，重要数据协同通过沙箱环境开展，禁止原始数据直接外泄，留存全链路操作审计记录。

(7) 落实生成式 AI 训练数据专门合规义务

将训练数据合规从事后审查前移至语料入库与标注环节。建立语料来源合法性审核机制，逐批记录语料来源、授权凭证与使用范围，涉及知识产权、个人信息的内容须具备合法授权或处理依据；按 GB/T 45674-2025 建立标注规则、标注人员管理与质量抽检机制，标注过程全程留痕，抽检合格后方可进入训练集；按 GB/T 45652-2025 落实预训练与优化训练数据的来源安全、内容安全与标注安全要求，并与汽车数据分类分级结果衔接，同步完成训练数据的重要数据识别与出境路径判定。企业自动驾驶模型能力若以智能座舱对话、内容生成等形式向境内公众提供生成式服务，还应按《生成式人工智能服务管理暂行办法》履行安全评估与算法备案义务，按 GB 45438-2025 落实生成合成内容的显式标识与文件元数据隐式标识，并将上述义务的履行证据纳入模型发布前的安全评估材料。

(8) 形成标准跟踪与动态合规闭环

建立汽车数据安全、自动驾驶相关标准的动态跟踪机制，同步跟进功能安全、预期功能安全、数据记录等标准的制修订进度。可在该机制中引入合规辅助智能体，对新增或修订的标准要求与企业现有数据处理流程、系统功能和技术控制项进行辅助映射，识别受影响环节并生成待复核的整改任务和合规检查事项；正式合规判断和监管报送仍由相关责任部门审核确认。同时设置可量化的合规内控指标，包括重要数据识别准确率、车外数据匿名化达标率、数据记录系统标准符合率、事故数据可追溯率等，定期开展合规评估，及时迭代内部管控措施与技术策略。

4. 行业实践实例

特斯拉 Autopilot 数据泄露事件：第三方服务商运维漏洞导致超 100G 自动驾驶路测影像、标注数据及车主行车记录外泄，涉及大量道路环境与个人信息，触发多地区隐私监管调查。教训：需严格

管控第三方数据访问权限，车外数据对外流转前必须完成匿名化，行车敏感数据实行最小范围共享。

落地建议：为第三方服务商设立隔离账号与数据访问沙箱，遵循“最小可完成工作”原则；对路测影像等敏感数据设置自动过期策略并全量留痕，对接入权限实行季度复审与即时回收。

自动驾驶模型投毒攻防验证事件：安全研究证实，污染少量训练样本即可在自动驾驶模型中植入后门，导致特定场景下系统误判障碍物、做出错误决策。教训：需建立训练数据全链路可信机制，常态化开展样本异常检测与模型后门测试，结合对抗验证保障算法决策安全。

(四) 软件升级服务数据安全

软件升级场景贯穿代码与第三方组件、编译构建、安全检测、数字签名、版本管理、OTA 任务下发、车端校验、安装执行及异常回退等环节，其主要安全风险及重点技术能力如图 7 所示。



图 7 软件升级场景风险与技术支持

1. 场景特点

OTA 阶段是智能网联汽车全生命周期功能迭代、缺陷修复与体验优化的核心环节，覆盖升级包

开发编译、版本管理、任务下发、车端执行、失败回退及运营监测全流程，贯穿车辆量产后的完整服役周期。该阶段的数据兼具核心技术资产属性、行车安全属性与强监管属性，主要特点如下：

- 涉及安全驾驶、电池管理等核心功能的升级包源代码是企业核心技术资产，同时直接关联车辆行驶安全，且受 GB 44496 强制性标准、召回管理条例多重监管约束，数据价值与合规权重双重突出。
- 数据端云链路长、影响范围广。升级数据从开发侧、版本管理平台经云端 OTA 系统批量下发至海量在网车辆，覆盖开发、运营、车端多节点。单点数据被篡改或泄露，风险会批量传导至全部适配车辆，安全影响的量级与烈度远高于单车辆场景。
- 全流程合规性要求强，可追溯性是核心底线。依据 GB 44496 强制要求，升级前测试验证、风险评估与用户告知，升级中可靠执行与异常回退，升级后状态记录与日志留存均有明确标准，同时 OTA 升级活动需履行监管备案义务，全环节需满足可审计、可追溯要求。
- 安全管控与升级效率、用户体验存在平衡要求。OTA 升级面向海量车辆批量推送，强调迭代速度与用户无感体验，过度依赖人工审批与强阻断式管控会拖慢缺陷修复节奏、影响用户使用感受，因此需将安全策略嵌入 OTA 自动化流水线，实现无感式安全防护。

2. 主要安全风险

软件升级服务阶段的安全风险贯穿升级包开发、云端下发到车端执行全链条，风险不再局限于单一技术资产泄露，可批量传导至海量在网车辆，直接威胁行车安全与公共安全，主要包括：

- OTA 管理平台、版本仓库的运维或开发人员账号被盗用、越权操作，导致核心功能升级包源代码泄露，甚至恶意篡改升级版本、违规下发高危升级任务，批量影响在网车辆安全。
- 升级包未落实强数字签名与完整性校验机制，在云端存储、网络传输、车端加载环节被恶意篡改或植入恶意代码，导致车辆动力、制动、电池管理等核心功能异常，甚至被远程控制，

引发规模化行车安全风险。

- 核心功能 OTA 源代码未按要求开展分级识别，重要数据未纳入重点管控，通过违规渠道外泄，或未经安全评估擅自出境，违反数据安全与出境管理相关规定。
- 升级失败回退机制缺失或失效，升级中断、版本不兼容等异常场景下无法回退至安全可用版本，导致车辆功能瘫痪，引发用户权益与行车安全双重风险。
- OTA 升级操作日志、版本记录、通信日志留存不完整或可被篡改，无法满足监管追溯要求；升级活动未按规定履行备案义务，擅自新增或变更车辆核心功能，触发行政合规风险。
- OTA 升级包集成的开源组件、第三方 SDK 存在安全漏洞，随升级批量下发至车端，形成软件供应链风险，大范围暴露车辆网络安全短板。
- 用户告知与授权机制不规范，未向用户清晰告知升级内容、风险影响与所需时长，擅自静默升级车辆核心功能，违反用户权益保护与监管要求，易引发合规与舆情风险。

3. 技术实践体系

软件升级服务数据安全技术实践的核心，是将 GB 44496 强制性标准要求、数据分类分级规则与全生命周期安全原则，嵌入 OTA 升级全流程自动化体系，在保障升级效率与用户体验的前提下，形成合规可追溯、风险可管控的技术防护闭环。本场景最具特色的是“升级包强签名与车端可信执行环境”能力：以多重验签、加密分发与失败自动回退保障升级全链路安全。本场景的完整技术实践承接技术篇 OTA 全链路安全技术、源代码与软件供应链安全等能力（见技术篇表 9），以下结合 OTA 平台场景特点展开落地要点。

(1) 建立 OTA 数据资产分级与全链路标签体系

按功能模块逐一盘点升级包源代码、版本固件、升级任务数据、车端升级日志，全部纳入统一资产目录。重点针对安全驾驶、电池管理等核心功能的升级包源代码，对照重要数据判定规则自动分级

标注，同步叠加出口管制、两用物项相关判定规则，生成机器可读的安全标签，形成清晰的重要数据清单。

(2) 搭建符合国标的 SUMS 技术底座

严格对标 GB 44496-2024 要求，将 SUMS 要求落地为覆盖升级前、升级中和升级后的自动化技术流程：升级前嵌入全量测试验证、风险评估与用户告知模块，确保升级包完成安全校验、风险可量化，并向用户清晰告知升级内容、时长与注意事项。同时，可由 OTA 安全智能体综合代码安全检测、组件漏洞、车型适配测试、历史升级结果及风险评估信息，自动归集版本风险并生成发布前待确认事项，为人工审批和灰度发布策略制定提供辅助依据；升级中内置断点续传、异常实时校验能力；升级后自动核验升级结果、同步记录车辆版本映射关系，全流程配套升级失败自动回退机制，保障异常场景下车辆基础功能可用。

(3) 强化升级包全链路完整性与机密性防护

升级包从编译生成到车端加载实行全链路安全防护：编译完成后同步生成官方数字签名与哈希校验值，存储与传输过程全程加密；车端升级前强制执行多重签名验签与完整性校验，未通过校验的升级包一律禁止加载。采用安全加密传输通道下发升级包，全程保障升级包源代码与固件的保密性与完整性。

(4) 落实 OTA 数据出境分级合规管控

严格按数据分级结果匹配对应出境路径：属于重要数据的核心功能 OTA 源代码，依法通过境内法人主体申报数据出境安全评估，不拆分申报；因消除产品缺陷、实施召回需要且已向监管部门完成备案的 OTA 升级包，按规定适用豁免路径，留存完整的备案凭证与出境目的证明材料。建立出境数据自动核验闸门，未经合规审批的数据禁止跨境传输。

(5) 建设 OTA 全流程安全监测与审计追溯能力

对 OTA 平台操作、升级任务下发、网络通信、车端升级执行全环节开展安全监测，重点监测异



常版本下发、批量任务违规操作、非授权升级包传输等高风险行为。全量留存网络流量日志、操作行为日志、安全告警日志与车端升级记录，采用可信时间戳与防篡改存储机制，日志留存期限不少于 3 年，满足监管追溯与事故调查要求。依托上述监测与审计数据，在灰度发布和批量升级过程中，可进一步引入 OTA 安全智能体，对升级版本、车型配置、SBOM、漏洞信息及车辆异常日志进行关联分析，识别失败率异常上升、特定车型集中异常及版本兼容性问题，并为暂停推送、扩大验证范围或启动回滚提供辅助决策依据。涉及升级任务发布、停止及回滚等高风险操作时，智能体仅承担风险分析和建议生成职责，不得绕过既有发布审批、数字签名及车端强制验签机制直接执行相关操作。

(6) 筑牢 OTA 软件供应链安全防线

将 OTA 升级包的开源组件、第三方依赖、SDK 统一纳入供应链安全管理，升级包发布前自动开展漏洞扫描与恶意代码检测，禁止含高危漏洞的组件随版本下发。建立升级包 SBOM 清单，实现组件版本可追溯、漏洞可快速定位响应。在形成可追溯的 SBOM 和漏洞信息基础上，可进一步利用软件供应链安全智能体，将 SBOM、组件漏洞、第三方 SDK 来源、版本依赖关系及历史安全事件进行关联，辅助识别高风险依赖、判断漏洞影响范围和确定优先修复对象，提高升级包供应链风险分析效率。对第三方开发服务商实行权限最小化管控，核心功能升级包的发布执行双人复核与分级审批机制。

(7) 形成备案管理与动态合规闭环

按工信部汽车 OTA 备案要求，建立升级活动备案管理模块，自动归集升级版本、功能影响、适用车型等备案信息，支撑合规备案申报。重要数据识别结果按要求向地方行业监管部门备案。建立监管政策与标准动态跟踪机制，同步跟进 GB 44496 正式实施要求与 OTA 监管规则更新，定期开展合规自评估，及时迭代内部管控策略与技术能力。

4. 行业实践实例

升级签名校验缺陷引发数据泄露事件：2026 年 4 月，AI 模型部署工具 X inference 的官方 Python

软件包遭供应链投毒，攻击者上传含恶意代码的 2.6.0 至 2.6.2 版本，用户安装或引入该工具时，恶意代码自动执行并窃取云平台凭据、API 密钥、数据库密码、加密货币钱包及环境变量等敏感信息，回传至远程命令与控制服务器。国家网络安全通报中心监测发现后发布处置建议，要求受影响用户卸载恶意版本、更新全部敏感凭证并封禁恶意域名。教训：软件分发环节的完整性校验与来源认证是数据安全的核心防线，必须对软件包发布实施强制签名验证与仓库准入审核，杜绝未授权代码进入分发链路。

(五) 联网运行数据安全

联网运行场景覆盖车辆端、路侧基础设施、云平台以及网络与高精地图之间的数据交互、汇聚和共享，其主要安全风险及重点技术能力如图 8 所示。

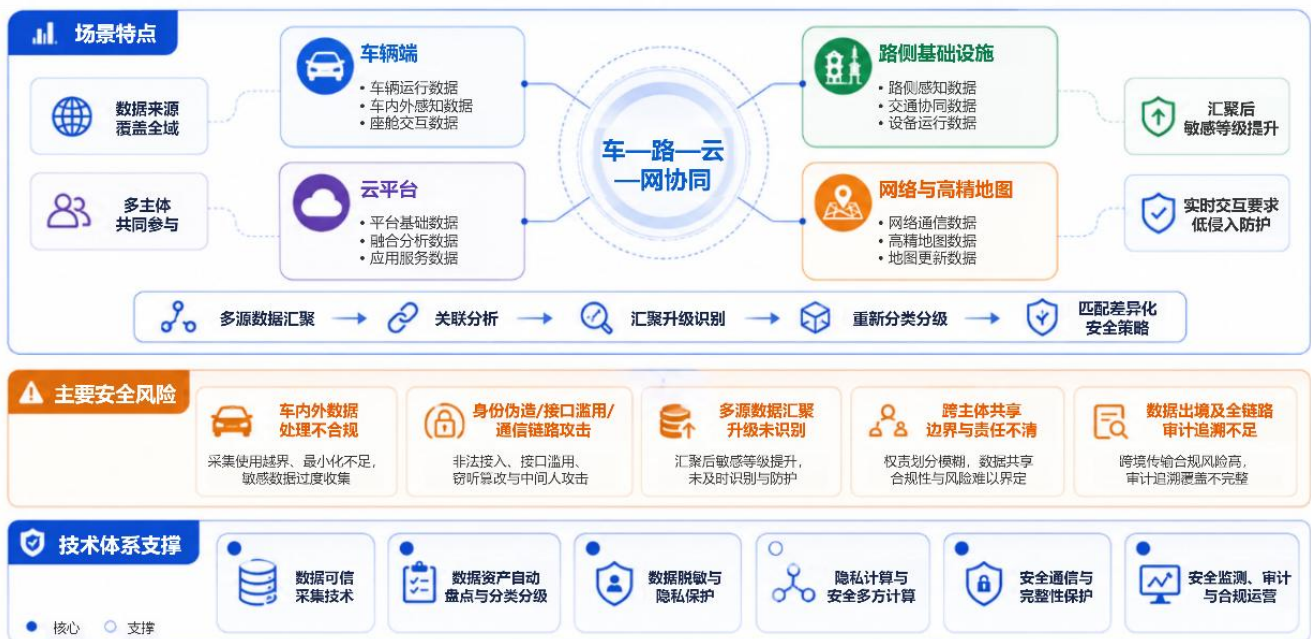


图 8 联网运行场景风险与技术支持

1. 场景特点

联网运行阶段是智能网联汽车量产后全域数据交互的核心环节，覆盖车端联网服务、路侧感知协

同、云端运营分析、车路协同应用等全场景，贯穿车辆完整服役周期。该阶段的数据来源分散、流转链路长、参与主体多，兼具业务服务价值、公共安全属性与强监管属性，主要特点如下：

- 数据来源覆盖全域，类型丰富且合规维度多元。数据可划分为车端、路端、云端、网络端四大类，既包含车辆运行、感知决策等车端数据，也包含路侧感知、交通状态等路侧数据，还有云端服务、监控管理等平台数据，同时涉及地理信息、个人信息、公共交通等多重合规要求，重要数据识别场景复杂。
- 多源数据汇聚特征突出，衍生敏感风险显著。单车运行数据、路侧感知数据、交通管理数据单项敏感程度有限，但跨主体融合汇聚后，可推导敏感区域高精度地理信息、城市交通运行规律、用户群体出行轨迹，数据敏感等级大幅提升，存在“汇聚升敏”的次生合规风险。
- 参与主体多元，数据权责边界复杂。联网运行涉及整车企业、路侧运营商、交通管理部门、地图服务商、云服务提供商等多类主体，数据跨组织、跨行业共享流转，数据权属、安全责任与使用边界难以清晰界定，车路协同场景下协同治理难度突出。
- 数据交互实时性强，安全防护需兼顾业务连续性。联网数据支撑智能驾驶辅助、动态导航、实时监控等高频业务，对传输时延与可用性要求高，安全管控不能中断正常业务运行，需适配海量终端接入、持续数据流的场景，实现自动化、低侵入的安全防护。

2. 主要安全风险

联网运行阶段的安全风险贯穿车端、路侧、云端、传输链路全链条，不仅涉及数据泄露与合规风险，还可直接影响车辆行驶安全与城市交通运行秩序，主要包括：

- 车联网平台、路侧管理系统账号被盗用或越权操作，攻击者可非法访问海量车辆运行数据、路侧感知数据，甚至向车辆下发虚假控制指令与交通信息，批量威胁在网车辆行驶安全。
- 车外实景影像、雷达点云等感知数据未按国标要求完成匿名化处理，座舱数据违反“默认不

收集、车内处理”原则，违规上传、共享或对外提供，触发个人信息保护与地理信息安全双重合规风险。

- 多源数据汇聚未开展专项风险评估，车端、路端、云端数据融合后衍生出敏感地理信息、交通运行规律等重要数据，未按对应等级管控，甚至违反测绘地理信息相关管理规定。
- 车—路—云数据传输链路防护缺失，未采用加密传输与完整性校验机制，易遭受中间人攻击篡改数据，如篡改路侧感知结果、交通信号灯信息，误导车辆自动驾驶决策，引发行车安全事故。
- 联网运行数据分类分级不到位，重要数据未纳入重点管控，未经安全评估擅自出境或向第三方提供，违反数据安全与出境管理相关法规，触发行政合规风险。
- 车路协同多方安全治理机制缺失，合作方安全能力参差不齐，数据共享协议未明确安全责任边界，出现数据超范围使用、违规留存、擅自二次转发等问题，形成跨主体管控盲区。
- 联网运行安全监测与日志留存能力不足，异常数据传输、非法访问行为无法及时发现处置，日志记录不完整、可被篡改且留存期限不达标，安全事件发生后无法实现全链路溯源，不满足监管审计要求。

3. 技术实践体系

联网运行数据安全技术实践的核心，是将数据分类分级规则、国家标准要求与多主体协同治理原则，落地到车—路—云—网全链路中，在保障联网业务实时性与连续性的前提下，构建全域覆盖、可管可控、可溯可审的安全防护体系。本场景最具特色的是“多源数据汇聚风险评估与高精度地理信息合规处理”能力：通过汇聚前风险评估识别数据融合后的敏感升级，通过坐标偏移与脱敏处理满足测绘地理信息合规要求。本场景的完整技术实践承接技术篇车路云协同数据安全、安全监测审计与合规运营等能力（见技术篇表9），以下结合联网运行场景特点展开落地要点。

(1) 建立联网运行数据资产全景盘点与分级标签体系

按车端数据、路端数据、云端数据、网络端数据四大类别，全面梳理全量联网数据资产，逐项对照重要数据判定规则开展分级标注。对于规则能够明确判定的数据，直接按照既定标准生成安全标签；对于车端、路端和云端数据关联形成的新数据集，可利用数据治理智能体结合数据来源、业务用途、时空关系及关联路径，辅助识别数据组合后产生的衍生敏感属性和汇聚升敏风险，并将分析结果提交分类分级规则校验。经确认达到更高敏感等级的，自动提升管控级别。涉及测绘地理信息的特殊数据，叠加自然资源部相关管理规则校验，生成机器可读的安全标签，形成清晰的重要数据目录。

(2) 落实车内外数据分类合规处理机制

严格执行 GB/T 41871 标准要求：车外实景影像、点云等感知数据向车外提供前，必须完成人脸、车牌等敏感信息的匿名化处理，未达标数据禁止流出车端与 RSU；座舱数据遵循“默认不收集、车内处理”原则，按需最小化采集范围与数据留存周期，非业务必需不上传至云端。

(3) 构建车—路—云全链路传输安全防护体系

车辆与车联网平台、路侧设备、云端系统之间的数据交互，全程采用加密传输通道与完整性校验技术，保障数据传输的保密性与完整性。建立境外数据接收方身份鉴权机制，未通过身份核验的主体禁止接收数据。对联网运行的网络通信行为、系统主机操作行为开展持续安全监测，全量留存流量日志、操作日志与安全告警日志，采用防篡改存储机制，满足监管留存要求。

(4) 建立多源数据汇聚风险专项管控机制

针对车、路、云多源数据融合场景，建立汇聚前风险评估流程，对已有明确判定规则的数据组合自动开展敏感属性校验；对于传统固定规则难以覆盖的复杂组合关系，可由车路云数据安全智能体分析车端运行数据、路侧感知数据、交通状态数据和云端业务数据之间的语义关系、时空关联及组合路径，辅助判断融合后是否可能推导敏感地理信息、交通运行规律和群体出行特征。对融合升级为重要数据的数据集，自动匹配对应等级的安全管控策略。涉及自动驾驶地图、测绘地理信息的数据，严格

遵守自然资源部相关管理规定，落实资质审核与审批流程要求。

(5) 搭建车路协同多方安全治理协同机制

与路侧运营商、交通管理部门、地图服务商等合作主体签订数据安全专项协议，明确各方数据安全全责任边界、数据使用范围与防护要求。对数据合作方开展常态化安全能力评估与持续监督，数据共享遵循最小必要原则，优先通过脱敏接口、沙箱分析环境提供数据服务，严格限制原始敏感数据直接流出管控域。

(6) 落实联网运行数据出境分级合规管控

根据数据分级结果匹配对应出境合规路径：经识别为重要数据的联网运行数据，依法通过境内法人主体申报数据出境安全评估，不拆分申报；涉及安全漏洞修补、安全事件处置的相关数据，按规定事先向工业和信息化部、国家市场监督管理总局等部门报告备案后，可适用豁免条款，留存完整的备案凭证与出境目的证明材料。设置跨境数据传输自动核验闸门，未经合规审批的数据禁止跨境传输。

(7) 建设全域安全监测与审计追溯能力

打通车端、路侧、云端、网络端的安全日志数据，构建全链路关联分析与异常监测能力，重点识别非授权批量数据访问、敏感数据违规外发、异常跨域传输等高风险行为。在此基础上，可由车路云安全运营智能体进一步聚合车辆异常访问、路侧设备异常通信、云端接口调用等分散告警，关联数据流转记录和相关日志，辅助还原事件在车、路、云之间的传播路径，并生成风险摘要和处置建议。同时建立数据全链路血缘追溯机制，完整记录数据流转路径、处理主体与使用场景，满足监管审计与安全事件溯源调查要求。

4. 行业实践实例

大众汽车车联网平台数据泄露：车联网服务平台接口存在未授权访问漏洞，导致数十万车辆的行驶轨迹、位置信息及用户关联数据外泄，触发多地监管部门的隐私合规调查与处罚。教训：需强化车

联网平台身份鉴权与接口安全管控，对车辆运行数据实行分级访问权限管理，常态化开展漏洞扫描与安全渗透测试。落地建议：对车联网平台接口实行“鉴权—限流—审计”三位一体管控，敏感接口强制双向 TLS；建立漏洞“发现—验证—修复—复测”闭环，高危漏洞在限定周期内完成修复验证并留存证据。

(六) 安全事件分级、报告时限与缺陷召回衔接

安全事件的分级、报告与召回衔接是贯穿五大治理场景的共性合规义务。《网络数据安全管理条例》与 GB 44495、GB 44496、GB 44497 三项强制性国家标准，以及《汽车数据安全若干规定（试行）》，均对安全事件报告提出了明确要求。企业应建立与车辆全生命周期相适应的安全事件管理流程，形成“事件分级—报告时限—缺陷召回”的闭环衔接机制。

其一，事件分级。建议参照《数据安全法》关于数据安全事件的分类分级框架与网络安全事件应急预案的要求，结合事件对人身安全、财产损失、隐私权益及国家安全的潜在影响，将汽车数据安全事件划分为一般、较大、重大、特别重大四个等级，明确各级事件的判定标准、响应优先级与处置资源投入，并定期演练检验。

其二，报告时限。发生网络数据安全事件后，企业应及时启动应急处置，并按照《数据安全法》《个人信息保护法》《网络数据安全管理条例》及三项强制性国家标准的规定履行报告与通知义务：涉及个人信息泄露的，应及时通知受影响用户；涉及重要数据的，应及时向有关主管部门报告；同时配合监管部门的调查与证据调取。建议企业将外部法定时限映射为内部 SLA，在事件管理系统中固化上报模板、责任人与升级路径，避免人工流转延误。

其三，与缺陷召回衔接。当安全事件暴露出的软件缺陷可能影响行车安全、构成产品缺陷时，应依据《缺陷汽车产品召回管理条例》启动缺陷调查与召回评估；涉及 OTA 升级修复的，按照 GB 44496 与工信部软件升级备案要求履行程序，实现从“事件处置”到“缺陷修复”再到“升级召回”的闭环



管理，并将整改结果沉淀为风险知识库反哺研发与运维环节。



五、 展望篇

智能网联汽车已从单纯的交通工具演变为集感知、计算、通信于一体的移动智能终端，数据安全也随之从早期的合规要求，演变为影响产品竞争力与用户信任的基础能力。本章在前述形势分析、治理框架与技术实践的基础上，对未来五到十年汽车数据安全的技术演进方向与车企战略选择进行前瞻性分析。需要说明的是，前瞻性判断基于当前技术发展态势与监管趋势作出，存在不确定性，企业应结合自身业务实际动态调整。

面向未来，汽车数据安全将同时受到技术演进与监管演进的驱动：一方面，地缘政治博弈带来的数据主权要求、算力革命带来的攻击与防御手段升级，以及深度伪造等 AI 技术被恶意利用的风险，将持续改变威胁格局，大模型与智能体的深入应用也将进一步拓展汽车数据安全的治理边界；另一方面，以强制性国家标准为代表的监管框架不断细化，企业对合规与安全能力建设的颗粒度要求不断提高。本章从两大主线展开：一是未来五到十年主导智能网联汽车数据安全的前沿技术趋势，二是面向车企高管层的四大战略行动建议。

表 21 智能网联汽车数据安全前沿技术趋势总览

前沿技术分类	核心驱动力与解决的痛点	关键技术突破	典型演进场景应用	预计规模化商用节点
内生安全架构	驱动力：应对集中式 E/E 架构下零日漏洞、供应链后门等“未知的未知”威胁。解决的痛点：突破传统静态特征库匹配与物理边界隔离防御机制在面对变异攻击时失效的瓶颈，防止车辆物理控制权被恶意接管。	基于 DHR 与拟态裁决机制，融合动态性、异构性、冗余性三要素，实现异常执行体实时发现与剔除，将网络安全转化为广义可靠性。	1.拟态防御域控制器：采用异构多核并行运行冗余算法，从硬件底层阻断恶意接管。2.车路协同内生安全网关：抵御 V2X 协议栈模糊测试攻击与伪造指令注入。	2028-2030 年（随着中央计算平台与高阶智驾域控架构的大规模量产落地而普及）

前沿技术分类	核心驱动力与解决的痛点	关键技术突破	典型演进场景应用	预计规模化商用节点
AI 驱动的 深度安全推理引擎	驱动力：应对生成式 AI 与大模型带来的自动化、智能化攻击（如批量恶意代码生成、深度伪造生物认证），以及大模型与智能体深入应用后出现的新型安全风险。解决的痛点：解决传统 SOAR 体系依赖规则驱动导致的响应迟滞、易被绕过及 SOC “告警疲劳” 瘫痪问题。	基于安全垂域大模型与 RAG 技术，具备深度推理与上下文理解能力，提升复杂攻击分析、攻击链研判和动态响应能力；进一步结合安全智能体，实现跨系统安全工具协同与处置流程编排，推动安全运营向智能化、协同化方向演进。	1.车端 AI 威胁检测与自愈：轻量化部署 AI 代理，实时监控总线异常并秒级下发动态控制策略阻断横向移动。 2.云端全域安全智能脑：多模态分析 PB 级日志，自动化追踪 APT 并反哺车端防御策略库。	2026-2028 年（随着端云协同算力成本下降与安全大模型轻量化技术成熟而落地）
“管检一体化” 安全测试平台	驱动力：满足车云路全生命周期安全验证与全球监管常态化需求。解决的痛点：解决传统测试工具碎片化、用例非标准化、黑盒测试效率低下问题，应对数亿行代码迭代导致的“带病上市” 及 OTA 海量漏洞修复压力。	构建标准化测试工具链接口打破数据孤岛，支持安全需求建模到测试用例自动转换，结合虚拟仿真与硬件在环（HIL），实现零部件到整车级的高保真动态验证闭环，并逐步引入 AI 辅助测试用例生成、任务编排与结果分析能力。	1.CI/CD 流水线原生安全左移：代码提交构建阶段自动触发静态分析与模糊测试。 2.量产车远程安全巡检：通过 OTA 下发探针动态评估 HSM 健康状态，自动生成 R155/R156 合规报告实现“一车一档”。	2025-2027 年（受全球 R155/R156 强制法规驱动，车企合规刚需促使工具链快速整合）
“数字安全免疫力” 新范式	驱动力：保障 TB 级核心数据在车、云、路、图多方高速流转中的数据主权与隐私合规。解决的痛点：解决传统边界防御在去中心化跨域交互下失效导致的内部数据“裸奔” 问题，应对数据跨境与合规流转的多重监管压力。	构建以数据为核心、业务为驱动的自适应架构，涵盖 DSMM、ZTNA、隐私增强计算并逐步融合智能风险分析能力，根据数据敏感等级、业务场景和实时风险动态优化防护策略，实现“数	1.零信任车云数据交互架构：车端 ECU 与云端每一次请求持续身份验证，结合 ABE 实现最小权限访问。 2.隐私保护计算与智能联邦学习：不	2027-2030 年（随数据要素市场化流通政策完善及高阶自动驾驶模型联邦训



前沿技术分类	核心驱动力与解决的痛点	关键技术突破	典型演进场景应用	预计规模化商用节点
		据在哪，安全域就在哪”的伴生式动态防护与自愈。	泄露原始隐私数据前提下实现跨域联合智驾模型训练（可用不可见）。	练需求爆发而落地)
量子安全	驱动力：抵御未来 5 至 50 年量子算力突破（Shor 算法）带来的传统公钥密码体系秒级破解威胁。解决的痛点：解决汽车长达十余年生命周期内面临的 SNDL 致命威胁，防止高精地图、车主生物特征等高价值数据被批量窃听囤积后解密。	基于格密码 ML-KEM(Kyber)、 ML-DSA(Dilithium)等 PQC 算法构建密码敏捷性架构；结合天地一体 QKD 技术，提供抵御量子算力降维打击的物理层绝对安全防护。	1.PQC 敏捷迁移框架：HSM 中运行传统密码与 PQC 的“混合密码体系”。2.抗量子 V2X 互信与车内网络：抗量子证书广泛应用于车与路侧基础设施（RSU）身份核验，杜绝城市级交通网络劫持。	2028-2030 年（随着 NIST PQC 标准全面落地及车载 HSM 芯片算力升级逐步上车，并在 2030 年后防范 Q-Day 临近而规模化部署)

(一) 未来趋势：重塑汽车数字免疫系统的五大前沿引擎

在数字世界与物理世界深度融合的下半场竞逐中，以下五大技术方向将彻底重塑智能网联汽车的数据安全防御范式。

1. 内生安全架构

汽车电子电气架构向集中式演进，高度依赖数亿行代码的面向服务的架构和大量开源组件。传统基于特征库匹配和静态边界隔离的防御机制，只能抵御“已知的未知”攻击，面对零日漏洞、供应链后门及 AI 变异攻击等“未知的未知”威胁时形同虚设。一旦核心域控制器被攻破，黑客可轻易实现



权限提权并接管车辆物理控制权，造成不可逆的灾难性后果。

(1) 技术内核解析

内生安全理论通过引入 DHR 架构，将防御机制内生。其核心在于利用“动态性、异构性、冗余性”三要素，通过多套异构执行体同时处理相同输入，并基于拟态裁决机制实时对比输出结果。当某个执行体被攻击或存在后门触发异常时，裁决器能立即发现偏差并剔除异常组件，从而在不确定环境中实现系统的广义可靠性与高生存能力。

(2) 汽车场景前瞻应用

拟态防御域控制器：在高阶智驾域控制器或中央计算平台中部署 DHR 架构，采用异构多核处理器并行运行功能安全与网络安全冗余算法，确保即便单一架构存在未知漏洞，也无法形成一致的错误输出，从硬件底层阻断恶意接管。车路协同内生安全网关：在 V2X 通信与车云数据交互节点应用内生安全机制，抵御针对通信协议栈的模糊测试攻击和伪造指令注入，保障车路云一体化协同过程中的动态信任与数据完整性。

2. AI 驱动的深度安全推理引擎

随着生成式 AI 与大模型技术的爆发，网络攻击已进入自动化、智能化时代。攻击者利用 AI 工具批量生成恶意代码、自动化挖掘车载系统漏洞，并通过深度伪造技术伪造车主声纹或面部特征以绕过生物认证。传统依赖人工分析日志、规则库拦截的安全编排自动化与响应体系在面对海量数据流和变异攻击时，响应迟滞且极易被绕过，导致车企安全运营中心陷入“告警疲劳”瘫痪状态。

(1) 技术内核解析

该技术基于安全垂域大模型构建，结合 RAG 技术，将海量历史攻防数据、汽车漏洞库与业务上下文深度融合。在传统规则检测基础上，它进一步不再依赖静态规则，而是具备深度推理与上下文理解能力，能够自主分析攻击链路、预测攻击者意图，并动态生成微隔离策略或拦截脚本。其本质是建

立具备自主决策能力的 AI 安全智能体，实现从“规则驱动”到“认知驱动”的跨越。随着安全大模型进一步向可调用工具、执行多步骤任务的智能体形态发展，还可通过安全智能体实现跨系统工具协同和处置流程编排，进一步提升安全运营的自动化水平。与此同时，智能体自身的身份权限、工具调用和运行行为也将成为新的安全治理内容，需要在既有安全策略和授权机制下对其能力边界进行约束。

(2) 汽车场景前瞻应用

车端 AI 威胁检测与自愈：在车端轻量化部署 AI 安全代理，实时监控车内总线流量异常与 SOA 服务调用行为。当发现未知威胁时，AI 引擎可结合车辆状态、服务调用关系等信息辅助判断受影响的业务节点，并联动预设的访问控制、隔离和服务降级策略，快速阻断风险扩散，实现秒级受控自愈。

云端全域安全智脑：构建基于云端的智能安全运营中心，利用大模型对 PB 级车云日志、OTA 升级数据及用户行为进行多模态分析，自动化追踪持续性高级威胁，并反哺更新车端防御策略库，形成“车云协同、以 AI 制 AI”的动态防御闭环。

3. “管检一体化”安全测试平台

智能网联汽车的车云路一体化发展导致攻击面无限延伸，车企在研发、生产、路测及量产后的全生命周期中，面临着安全测试工具碎片化、用例难以标准化、测试环境与真实场景割裂等痛点。传统“黑盒式”交付验收与人工渗透测试效率低下，无法应对动辄数亿行代码的迭代速度，极易导致带病上市。

(1) 技术内核解析

“管检一体化”平台是一种集资产管理、测试用例编排、自动化执行、漏洞追踪闭环于一体的安全底座架构。其核心在于构建标准化的测试工具链接口，打破不同供应商测试工具的数据孤岛。平台支持安全需求建模到测试用例的自动转换，利用虚拟仿真技术与硬件在环结合，实现从零部件级、系

统级到整车级的高保真动态安全验证。在此基础上，生成式 AI 与智能体还可结合系统架构、历史漏洞和测试结果，辅助生成新的测试用例、优化测试任务编排，并对测试结果进行关联分析，提高复杂攻击路径和跨组件风险的发现与验证效率。

(2) 汽车场景前瞻应用

CI/CD 流水线原生安全左移：将“管检一体化”平台接入车企研发的持续集成/持续交付流水线。在代码提交、软件构建阶段即自动触发静态代码分析与模糊测试，确保漏洞在交付前被拦截。量产车辆远程安全巡检与合规追踪：针对已售车辆，平台通过 OTA 接口下发轻量化探针或安全检测任务，动态评估车端 HSM、密钥管理与通信链路的健康状态，自动生成符合 R155/R156 等法规要求的合规报告，实现“一车一档”的动态合规追踪。

4. “数字安全免疫力”新范式

智能网联汽车每天产生高达 TB 级的数据，数据作为核心生产要素在车、云、路、图多方间高速流转。传统以“网络边界”为中心的防御体系在复杂的跨域交互与去中心化架构下全面失效。同时，车企在数据跨境、合规流转及隐私保护方面面临多重监管压力，单一维度的加密或访问控制已无法满足全局数据安全需求。

(1) 技术内核解析

“数字安全免疫力”摒弃了传统的堆叠式安全产品部署，构建以数据为核心、业务为驱动的自适应安全架构。其内核涵盖数据全生命周期管理、ZTNA、隐私增强计算以及融合式风险管理。它强调安全系统应具备自我感知、动态策略调整与自愈能力，通过对数据资产进行精细化分类分级与流转测绘，实现“数据在哪，安全域就在哪”的伴生式防护。随着智能体与数据血缘、身份管理和策略引擎进一步融合，系统还可根据数据敏感等级、业务场景和实时风险动态优化防护策略，使数据安全能力由静态配置进一步向持续感知和自适应调整演进。



(2) 汽车场景前瞻应用

零信任车云数据交互架构：对车端 ECU 与云端服务器之间的每一次数据请求进行持续身份验证与动态授权。结合属性基加密，确保高价值数据在计算与传输过程中的最小权限访问。隐私保护计算与智能数据联邦学习：在智驾模型训练与数据跨境流转场景中，应用联邦学习、多方安全计算等隐私增强技术。车企可在不泄露车主原始隐私数据的前提下，实现跨区域联合模型训练与数据可用不可见。

5. 量子安全

当前，全球智能网联汽车的车云认证、OTA 数字签名、V2X 通信几乎全部依赖 RSA、椭圆曲线和 Diffie-Hellman 等传统公钥密码体系。然而，随着量子计算技术的突破（尤以容错量子计算机的发展为标志），基于 Shor 算法的量子算力预计在未来 5 至 50 年内将具备秒级破解传统公钥密码的能力。由于汽车的物理生命周期长达十余年，黑客目前正在大规模截获并囤积加密的汽车高价值数据（如高精地图、车主生物特征），等待“量子霸权”降临后进行批量解密，这就是极其致命的“先存储，后解密”威胁，或者“等待量子计算机足以破解现行公钥密码之日到来后批量解密”。

(1) 技术内核解析

PQC 是基于格密码、多变量密码、哈希密码、编码理论等全新数学难题构建的加密算法，其数学复杂度能够有效抵御已知量子计算机的算力降维打击。例如，NIST 确立的 ML-KEM 与 Dilithium 算法，以及被 ISO 选为国际标准的 Classic McEliece 算法，均可在当前古典计算机上运行并抵御量子计算机的 Shor 算法破解。此外，基于量子纠缠分发原理的量子通信技术，在自由空间信道的损耗随距离增长显著低于光纤，适合广域组网；QKD 可在密钥分发环节提供基于物理原理的信息论安全性。

(2) 汽车场景前瞻应用

PQC 敏捷迁移框架：车企将不再把密码算法“硬编码”在底层系统中，而是构建密码敏捷性架构。支持在现有的 HSM 中同时运行传统密码与 PQC，形成“混合密码体系”。参考谷歌在 FIDO2 安

全密钥中采用的 ECC/Dilithium 混合签名模式，车企可利用仅 20KB 内存的优化实现，在车端受限硬件上部署抗量子签名。抗量子 V2X 互信与车内网络：随着车路协同网络带宽的提升，抗量子证书将被广泛应用于车辆与路侧基础设施的身份核验。参考苹果在 iMessage 中升级 PQ3 协议及微软在核心加密库引入 ML-KEM 算法的做法，车企可在 TLS/SSL 协议中添加抗量子签名与密钥封装算法，建立抗量子攻击的车云安全加密信道。天地一体量子保密通信网：依托“墨子号”等量子科学实验卫星构建的天地一体广域量子通信网络，车企可将 QKD 技术应用于车云高价值数据传输，实现“一话一密”的超高安全保障，抵御包括量子计算机在内的各种安全威胁。

(二) 给车企的战略建议：面向未来的数据安全战略行动框架

前沿技术趋势的落地，需要企业将数据安全纳入业务战略，并形成相互衔接的行动安排。面向未来，建议车企沿着“由内而外、由点到面、持续演进”的主线推进建设：以战略先行确立企业内部的组织责任、决策规则与车云协同机制；以摸清家底将治理要求落实到具体数据资产，并沿数据血缘贯通全生命周期；以管控生态把内部规则延伸至供应链与合作伙伴；以投资未来持续补足复合人才、前沿技术和资源保障，支撑前三项行动不断升级。

这一路径体现了治理边界从企业内部向产业生态拓展、治理对象从单项数据向业务链路和协作网络贯通。四项建议可协同推进，其中人才培养与技术投入应贯穿全过程，并根据业务风险、治理成效和技术变化持续调整，形成“组织定向—数据落地—生态协同—能力反哺”的闭环。各项建议分别衔接前述治理框架与技术能力，构成车企面向未来的数据安全战略行动框架。





图 9 车企数据安全战略行动框架

1. 战略先行 从企业内部确立治理方向

战略先行是整套行动的组织起点，重点解决谁来负责、如何决策以及安全要求何时进入产品与业务流程的问题。车企应将车云一体的安全要求纳入组织职责和研发管理，在新车型立项及电子电气架构设计阶段同步明确，为后续数据治理与生态管控提供统一依据。若在产品架构定型后再补充安全措施，往往会增加改造成本和系统协同难度。

确立“安全即业务”的董事会议题：将数据安全与网络安全管理委员会提升至由 CEO 直接挂帅的战略高度，引入“一票否决权”机制。在任何新车型立项、新业务（如出海扩展）启动前，必须通过强制性的安全与合规风险评估。

全面践行安全开发运维一体化：将安全属性“左移”至整车研发的灵魂深处。从需求捕获、架构设计、代码编写、仿真测试到最终 OTA 交付，构建全自动化、车云协同的安全工具链。随着 AI 辅助编程和研发智能体逐步应用，可将 AI 生成代码及高风险代码变更纳入安全检测范围，并利用安全大模型辅助开展漏洞分析和修复建议生成，同时确保数据采集与埋点符合最小必要原则。

构建车云协同的一体化防御纵深：打破车端研发域与云端互联网 IT 域的部门隔离。建立统一的身份认证体系与数据流动规范，使车端微隔离、加密传输与云端 API 管控、态势感知形成无缝咬合的

整体，确保黑客无论从哪个锚点入侵，都会陷入纵深防御的泥沼。本条与治理篇“治理目标”中风险防御与价值创造的目标定位相呼应，其技术落地可参见技术篇零信任与统一身份访问控制、安全监测审计与合规运营等能力。

2. 摸清家底 从数据对象贯通业务流程

在组织责任与治理规则明确之后，车企需要把战略要求落实到具体的数据资产，回答保护什么、数据流向哪里、如何实施管控的问题。动态分类分级应以数据对象为起点，结合血缘追溯与标签策略联动，逐步贯通采集、处理、传输、使用等业务环节。仅依靠静态问卷或人工台账，难以及时反映数据汇聚、用途变化与跨域流转带来的风险。

引入 AI 驱动的 DSPM 平台：摒弃人工分类分级。利用基于大语言模型与自然语言处理技术的自动化分类分级引擎，对接研发台架、云端数据湖、车联网边缘节点等全域资产库，持续开展自动化扫描、特征识别与动态打标。对于语义复杂或多源汇聚的数据，可由智能体辅助分析其敏感属性和升敏风险，生成分类分级建议；涉及重要数据认定等关键事项时，仍需结合既定规则完成最终确认。根据《汽车数据安全若干规定》与重要数据识别指南，进行全天候的自动化扫描、特征匹配与动态打标。

构建三维立体的“数据血缘图谱”：理清数据的来龙去脉。详细记录某一项敏感数据（如用户人脸特征）是从哪个车端传感器采集，经过了哪个域控制器的清洗，通过哪个 API 接口上传至云端，最终被哪个业务流（如账号登录或支付鉴权）调用。当发生外部合规审计或面临泄露风险时，能够在几分钟内精准定位受影响的数据集范围及阻断节点。

实施基于标签的动态管控策略：分类分级绝非为了造册束之高阁，而是作为安全管控的基础路由。建立策略联动引擎，当具有“极高敏感度”标签的数据被异常批量调用或试图流经未加密通道时，系统应能够自动触发脱敏、加密或阻断机制，实现“数据级别”与“防护力度”的动态智能匹配。本条

回指治理篇数据全生命周期安全层与基础安全支撑层中的分类分级机制,以及技术篇数据资产自动盘点与分类分级、安全监测审计与合规运营等技术的具体方案。

3. 管控生态 从企业内部延伸至合作伙伴

当内部数据资产与流转关系逐步清晰后,治理边界还需沿供应链向外延伸。智能网联汽车的软硬件、开源组件与数据服务由多方共同交付,任何一方的漏洞或安全事件都可能通过组件依赖、数据接口和业务协作传导至整车及云端。车企应将内部形成的安全规则转化为合作伙伴的准入、交付、运维和应急要求,把企业内部管控扩展为生态协同治理。

将安全管控边界极限向外延伸:车企必须承担起生态“链主”的绝对责任。不仅要审查一级供应商,必须将数据安全与网络安全的准入审计、漏洞披露要求、应急响应时效等硬性条款,通过穿透式协议直接约束至底层二、三级供应商。建立“不合规即一票否决”的生态黑名单制度。

强制推行 SBOM 全生命周期管理:要求所有供应商在交付软硬件包时,必须提供详尽的 SBOM 文件,包括内部调用的所有开源库名称、版本、许可证及已知漏洞。当诸如 Log4j 等级别的全球高危漏洞爆发时,车企能够通过 SBOM 系统在数秒内排查出受污染的模块,并定向下发 OTA 修复补丁,消除信息差带来的致命迟滞。

储备“断供”与“长臂管辖”应对预案:建立敏捷的国产化替代与底层逻辑剥离机制。重点布局具备自主知识产权的国密算法芯片、微内核车载操作系统等底层核心技术栈。针对某些国际市场的极端审查,设计支持跨国业务安全隔离的数据合规“软硬解绑”架构,避免因单一地缘政治冲突引发全球数据业务的瘫痪。本条回指治理篇基础安全支撑层中的合作方安全管理能力,以及技术篇源代码与软件供应链安全、数据传输安全防护等技术的落地要点。



4. 投资未来 为治理全流程提供持续支撑

治理边界越广、业务与技术变化越快，越需要持续的人才培养和技术储备。投资未来贯穿前述三项行动，通过复合人才支撑组织统筹，通过前沿技术增强数据识别与防护能力，并通过持续投入保障供应链协同和应急能力的演进。车企应将人才培养、技术研究与试点验证纳入中长期安排，并结合治理成效与风险变化滚动调整投入重点。

设立 CDSO 并赋予实权：CDSO 不应是一个虚职，而应直接向董事会汇报。该岗位需具备统筹法务合规、IT 基础设施与整车研发架构的跨界指挥能力。

打造“汽车+安全+AI”的三栖复合型特种部队：打破行业壁垒，高薪引入具备大型互联网公司底层架构经验、白帽黑客背景以及熟悉大模型算法的高尖端人才。建立内部的安全攻防红蓝对抗实验室，通过常态化的“实战演习”（攻陷自己的系统），倒逼防御体系的持续进化。随着大模型和智能体逐步进入研发、安全运营和生产辅助等环节，还需加强 AI 安全测试、智能体权限管理和对抗性安全验证等新型能力建设。同时，与顶尖高校联合设立定向培养基金，从源头锁定跨学科的未来智力资源。

敢于对“看不见收益”的前沿技术进行战略投资：虽然隐私保护计算（如多方安全计算、同态加密）、PQC、神经形态安全芯片等技术在短期内看似无法直接转化为卖车利润，但它们构筑的是车企在未来五到十年应对监管红线、释放数据变现潜力的底层基础设施。将企业网络与数据安全投入中确定比例的部分（建议以“占研发投入比例”为口径设定目标值，并从中单列不低于一定份额）专门圈定为“下一代数据安全和合规科技前瞻研发基金”，纳入三年滚动预算管理，作为面向中长期监管演进与技术升级的战略储备。建议以“投入占研发费用比例”、“重要数据自动化识别覆盖率”、“安全事件平均响应时间”三项指标作为年度评估依据，由 CDSO 牵头于下一预算周期内完成首轮编制并报董事会审议。本条与本篇前述内生安全架构、AI 驱动安全推理、量子安全等前沿技术趋势相衔接，相关技术原理与演进节奏详见本篇“未来趋势”各节。

综合来看，智能网联汽车数据安全正处于从合规驱动向价值驱动过渡的关键阶段。对车企而言，数据安全能力已不仅是应对监管检查的合规要求，更是支撑用户信任构建、数据要素价值释放与全球化布局的基础保障。企业应结合自身规模与业务特点选择差异化的实施路径，并保持投入的持续性与确定性。随着大模型与智能体应用不断深化，AI 在提升安全分析和治理效率的同时，也将带来新的安全边界和治理要求。

落实这一主线，应以企业内部的组织治理为起点，以数据资产与全生命周期管控为抓手，将安全责任延伸至供应链生态，并以人才、技术和持续投入推动能力演进。车企可结合自身规模与业务特点同步安排四项行动，通过风险评估、实施验证与效果复盘持续改进，在守住安全与合规要求的同时支撑业务发展和数据价值释放。



参考文献

- [1] 电子科技大学, 车载信息服务产业应用联盟, 广东为辰信息科技有限公司. 智能网联汽车信息安全测试白皮书[R]. 2025.
- [2] 路特斯科技, 普华永道. 智能网联汽车数据安全合规白皮书[R]. 2023.
- [3] 中国信息通信研究院. 车联网网络安全白皮书[R]. 北京: 中国信息通信研究院, 2023.
- [4] Upstream Security. 2026 Global Automotive and Smart Mobility Cybersecurity Report[R]. Birmingham, MI: Upstream Security, 2026.
- [5] 木卫四(北京)科技有限公司. 木卫四 2026 年汽车威胁报告[R]. 北京: 木卫四, 2026.
- [6] Berg Insight. The Global Automotive OEM Telematics Market[R]. Gothenburg: Berg Insight, 2026.
- [7] National Highway Traffic Safety Administration. Cybersecurity Best Practices for the Safety of Modern Vehicles[R]. Washington, D.C.: U.S. Department of Transportation, 2022.
- [8] 国家互联网信息办公室, 国家发展和改革委员会, 工业和信息化部, 等. 汽车数据安全管理办法(试行) [A/OL]. (2021-08-16). https://www.gov.cn/zhengce/zhengceku/2021-08/20/content_5632470.htm.
- [9] 国务院. 网络数据安全管理条例: 中华人民共和国国务院令 第 790 号 [A/OL]. (2024-09-30). https://www.gov.cn/zhengce/content/202409/content_6977767.htm.
- [10] 国家互联网信息办公室. 数据出境安全评估办法 [A/OL]. (2022-07-07). https://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm.
- [11] 国家互联网信息办公室. 促进和规范数据跨境流动规定[A/OL]. (2024-03-22).
- [12] 国家互联网信息办公室. 数据出境安全管理政策问答 (2025 年 4 月) [EB/OL]. (2025-04).
- [13] 工业和信息化部, 国家互联网信息办公室, 国家发展和改革委员会, 等. 汽车数据出境安全指引 (2026 版) [A/OL]. (2026-02-03).
- [14] 国家数据局, 等 17 部门. “数据要素×”三年行动计划 (2024-2026 年) [A/OL]. (2023-12-31).
- [15] 工业和信息化部, 公安部, 住房和城乡建设部, 等. 关于开展智能网联汽车“车路云一体化”应用试点工作的通知[A/OL]. (2024-01).
- [16] 国务院. 缺陷汽车产品召回管理条例[A]. 2012-10-22.
- [17] European Parliament, Council of the European Union. Regulation (EU) 2016/679: General Data Protection Regulation[A]. Official Journal of the European Union, 2016.
- [18] European Parliament, Council of the European Union. Regulation (EU) 2023/2854: Data Act[A]. Official Journal of the European Union, 2023.
- [19] UNECE. UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system[S]. Geneva: United Nations, 2021.
- [20] UNECE. UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system[S]. Geneva: United Nations, 2021.



- [21] U.S. Department of Commerce, Bureau of Industry and Security. Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles: Final Rule[A/OL]. (2025-01-16).
- [22] 国家市场监督管理总局, 国家标准化管理委员会. GB 44495-2024 汽车整车信息安全技术要求[S]. 北京: 中国标准出版社, 2024.
- [23] 国家市场监督管理总局, 国家标准化管理委员会. GB 44496-2024 汽车软件升级通用技术要求[S]. 北京: 中国标准出版社, 2024.
- [24] 国家市场监督管理总局, 国家标准化管理委员会. GB 44497-2024 智能网联汽车 自动驾驶数据记录系统[S]. 北京: 中国标准出版社, 2024.
- [25] 国家市场监督管理总局, 国家标准化管理委员会. GB/T 44464-2024 汽车数据通用要求[S]. 北京: 中国标准出版社, 2024.
- [26] 国家市场监督管理总局, 国家标准化管理委员会. GB/T 43697-2024 数据安全 数据分类分级规则[S]. 北京: 中国标准出版社, 2024.
- [27] 国家市场监督管理总局, 国家标准化管理委员会. GB/T 41871-2022 信息安全技术 汽车数据处理安全要求[S]. 北京: 中国标准出版社, 2022.
- [28] 国家市场监督管理总局, 国家标准化管理委员会. GB 39732-2020 汽车事件数据记录系统[S]. 北京: 中国标准出版社, 2020.
- [29] ISO/SAE 21434:2021, Road vehicles — Cybersecurity engineering[S].
- [30] 中国汽车工业协会. T/CAAMTB 77-2022 汽车传输视频及图像脱敏技术要求与方法[S]. 2022.
- [31] 乐俊君, 谭州勇, 张迪, 等. 面向车联网数据持续共享的安全高效联邦学习[J]. 计算机研究与发展, 2024, 61(9): 2199-2212.
- [32] Tine J M, Aldeen M, Enan A, et al. Real-World Evaluation of Protocol-Compliant Denial-of-Service Attacks on C-V2X-based Forward Collision Warning Systems[EB/OL]. arXiv: 2508.02805, 2025.
- [33] Ashik M H, Hossain M. Analyzing the Impact of Adversarial Attacks on C-V2X-Enabled Road Safety: An Age of Information Perspective[EB/OL]. arXiv: 2603.03462, 2026.
- [34] Shahriar M H, Barat M M A, Sundar H, et al. Temporal Misalignment Attacks against Multimodal Perception in Autonomous Driving[C]//Proc of the IEEE Conf on Secure and Trustworthy Machine Learning (SaTML). 2026.
- [35] Burbano L, et al. Command Hijacking Against Embodied AI (CHAI)[C]//Proc of the IEEE Conf on Secure and Trustworthy Machine Learning (SaTML). 2026.
- [36] RaPA: Enhancing Transferable Targeted Attacks via Random Parameter Pruning[C]//Proc of the IEEE/CVF Conf on Computer Vision and Pattern Recognition (CVPR). 2026.
- [37] 中国汽车工业协会, 国家计算机网络应急技术处理协调中心, 中国信息通信研究院, 等. 关于汽车数据处理 5 项安全要求检测情况的通报 (第四批) [EB/OL]. (2025-12-19). http://www.caam.org.cn/chn/1/cate_2/con_5236973.html.
- [38] PCA Cyber Security. PerfektBlue: 1-Click RCE in Bluetooth[EB/OL]. (2025-07). <https://perfektblue.pcacybersecurity.com/>.