数世咨询
Digital World Consulting

# 智能网联汽车安全选型指南

数世咨询
Digital World Consulting

# 智能网联汽车安全

# 选型指南

数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展*的政策法规、管理措施、技术方法等安全手段的总和。

这里的风险，不再局限于围绕数字化资产的攻防对抗，还包括了数字资产所承载业务的稳定性、连续性和健康性。这里的安全不再特指有意还是无意，天灾还是人祸，保安还是保险，而是更为广义的安全状态（SecSafe）。

*“世界环境与发展委员会出版的《我们共同的未来》报告中，将可持续发展定义为：“既能满足当代人的需要，又不对后代人满足其需要的能力构成危害的发展。”

——数世咨询，2023 年 11 月


以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核的“数字安全三元论”。

“数字安全三元论”由“网络安全三元论”（数世咨询于 2020 年提出）更新迭代而来，旨在匹配数字中国建设的进程，保障数字基础设施稳定、可持续运行，保障数据有效流动、激发数据要素价值。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构 . 网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

**报告编委**

数世咨询 **刘宸宇**

**数世智库** 数字安全能力研究院

# 目 录

# 前言

据公安部交通管理局统计，截至 2025 年底，我国机动车保有量达 4.69 亿辆，其中汽车 3.66 亿辆，汽车驾驶人超过 5.25 亿人。新能源汽车保有量达 4379 万辆，智能网联汽车渗透率持续快速攀升。

从传统 IT 环境下的安全视角来看，如果将如此庞大保有量中的每一台汽车看做一台终端，这将是一个庞大的终端安全市场；如果将每一台汽车拆解开来，其中还会有数百个 ECUs、域控制器、AI 计算平台、传感器、总线、通信协议等安全可以覆盖的风险点，这将是一个更加庞大的安全工具与安全产品需求场景。

不仅如此，随着新能源、5G、人工智能等技术的快速发展，传统汽车产业正以极快的速度向智能网联汽车产业跨越。智能网联、自动驾驶驱动的智能网联汽车，已成为国民经济的重要支柱产业。如果我们将眼光从传统汽车终端向外延伸——扩展至路侧端、云端、人端——V2X 又将构成一个更大范围的业务安全场景。与之同步演进的，是 AI 算法正成为智能汽车的核心驱动力，感知模型、决策算法本身也成为全新的攻击目标，对抗样本、数据投毒等针对 AI 的新型威胁已经出现，这需要更高维度的安全解决方案来应对。

与此同时，国家监管体系已进入强制化阶段。《汽车整车信息安全技术要求》等强制性国家标准正式发布，《智能网联汽车 组合驾驶辅助系统安全要求》等强标已正式发布，安全能力已成为智能网联汽车市场准入的必备条件。

简单推演之下不难看出，“智能网联汽车安全”承接着从传统汽车终端到智能网联汽车产业的绝大部分安全需求，从汽车生产的全生命周期，到汽车运行的

全关键要素，智能网联汽车安全是一件必须做也值得做的事。

反观供给侧，国内外智能网联汽车安全团队要么是汽车主机厂自行孵化，要么是传统安全企业切入汽车产业转型而来，少有能同时做到既了解汽车产业，又具备嵌入式操作系统、AI 安全、预期功能安全等底层复合技术能力的团队。因此，不同团队所输出的安全能力有的更加贴合汽车行业标准，有的更加擅长网络安全，各有侧重的同时，难免以偏概全。产业内始终缺少一个客观中立的机构以第三方视角对其进行论述。鉴于此，数世咨询调研并撰写本报告，希望能抛砖引玉，综合智能网联汽车安全这一新兴赛道中各能力者的优势，为产业从业者提供参考。本报告在视角上主要面向整车主机厂及其供应链（Tier1／零部件）的安全与合规决策者，同时兼顾检测机构、示范区等读者的选型需求。

报告勘误或进一步交流沟通，请联系：liuchenyu@dwcon.cn。

# 关键发现

- 智能网联汽车安全所需的安全能力，应当覆盖从地面到云端的网络安全、数据安全、AI 算法安全等多个维度。
- 智能网联汽车安全需覆盖智能网联汽车全生命周期，从概念阶段、集成阶段、测试阶段到上市运营阶段均有对应的安全产品，形成整体的安全解决方案。
- AI 安全已成为与网络安全、数据安全并列的核心议题。感知模型的鲁棒性、AI 算法预期功能安全、模型防投毒与防窃取等能力，是新一代智能网联汽车安全的关键组成部分。
- 车辆端网络安全的保护对象，主要包括智能座舱、自动驾驶域、网关、域控制器等关键零部件，以及 CAN、FlexRay、车载 Ethernet 等主流通信协议。
- 云端网络安全，重点在于安全运营中心 VSOC，需结合车辆端的 IDPS 一体联动，同时集成 AI 威胁检测引擎，为车企构建覆盖网络与智能的整车安全态势感知平台。
- 智能网联汽车数据安全不能简单将每一台车看作一个数据终端，而是要从汽车内部 ECUs、域控、网关、TBox 等外延至汽车外部数据所流向的各方，根据数据流动性来打造智能网联汽车数据安全解决方案。
- 智能网联汽车是一个大终端，其入侵检测与响应一定是体系化的。既要在车辆端以 IDPS 组件的方式，覆盖智能网联汽车的多个区域，又要在云端以安全运营的思路，对多台车辆终端开展一体化威胁检测与响应，同时覆盖对 AI 模型异常行为的在线监测。

➢智能网联汽车安全的重要性业内已经形成共识，很多车企将其作为隐性成本并不愿意投入，但安全是成本，更是竞争力，更加重视安全的智能网联汽车会赢得更大的市场。

# 第一章 智能网联汽车安全概念及主要场景

## 1.1 智能网联汽车

智能网联汽车（Intelligent Connected Vehicle，ICV），是指搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信、人工智能与网络技术，实现车与车、人、道路、云端之间的智能信息交换和共享，且具备复杂环境感知、智能决策、协同控制等功能，可实现安全、舒适、节能、高效驾驶，并最终可实现替代人工操作的新一代汽车。整体而言，智能网联汽车不仅是汽车本身，更是汽车、电子、信息通信、人工智能、道路交通运输等行业深度融合的新型产业形态。

## 1.2 智能网联汽车安全

本报告中智能网联汽车安全指一种覆盖“车-路-云-网-数据-AI”全链条、全要素的综合防护体系。它不仅基于传统的网络安全攻防技术，更深度融合了功能安全、预期功能安全、AI 安全等新维度，围绕智能网联汽车所涉及的车辆端、路侧端、移动端、云端等基础设施，针对硬件设备、软件应用、系统架构、通信网络、汽车数据、AI 模型与算法等目标，提供覆盖设计、测试、运营、响应全生命周期的一体化解决方案。

**智能网联汽车安全主要场景：**

### 1.2.1 智能网联汽车安全测试

传统汽车的智能化、网联化所采用的无数新设备、新技术本就会带来无数新的安全漏洞，而传统汽车产业智能化、网联化的过程也是国内外主机厂争夺技术体系话语权的过程，这又会在主机厂及其各自的供应链生态之间，引发更加多样化的技术体系与发展路径，必然带来相比传统汽车更多的安全漏洞，因此需要针对智能网联汽车多个主流技术体系，覆盖全生命周期的不同阶段，开展有针对性的安全测试。

---

以操作系统为例：

安全测试在覆盖传统主机厂主流采用的 AUTOSAR 架构（包括 Classic 与 Adaptive）基础上，还要重点考虑到国内主机厂竞争激烈的智能座舱操作系统（QNX、Android 等）的安全测试，如果能力允许，还要覆盖像特斯拉（基于 Linux 的 Autopilot 架构）这样的具备整套自主“软件定义汽车”能力的主机厂。

---

在传统的网络与系统安全之外，测试范围已大幅扩展至 AI 模型和算法。需重点验证感知模型（摄像头、毫米波雷达、激光雷达等）对物理世界攻击（如特殊涂装、对抗补丁、强光干扰）和数字世界攻击（对抗样本）的鲁棒性。同时，针对组合驾驶辅助系统的人机交互逻辑和驾驶员监控（DMS）有效性的安全验证，也成为满足新强标的测试焦点。

这些不同的安全测试场景，有的侧重于合规（如出厂前的安全测试），有的则侧重于漏洞挖掘（如针对整车业务的渗透测试），有的专注于 AI 模型鲁棒性验证，

但目的都是为了尽力减少智能网联汽车潜在的漏洞风险，提升智能网联汽车的整体安全水平，本质上需要的是对各类嵌入式操作系统、AI 算法框架的底层基础安全能力。

### 1.2.2 智能网联汽车数据安全

相比传统汽车，智能网联汽车每秒实时产生的数据以 GB 为单位，这些数据涉及到车端、路端、人端、云端等多个相关方，因此智能网联汽车数据的分类分级、安全传输、合规处置成为智能网联汽车安全必然要关注的一个场景。

---

从合规角度来看：

《数据安全法》《数据出境安全评估办法》等上位法对智能网联汽车数据的合规要求做出了原则性要求，国标 GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》则给出了具体的汽车数据处理细则，《汽车整车信息安全技术要求》等强标进一步明确了数据安全的强制性要求。但仅仅满足合规是远远不够的。

---

在实际操作层面，数世咨询认为应当重点从数据流动性角度来考虑智能网联汽车的数据安全问题。同时特别关注以下细分场景：

- **车外环境数据匿名化**：针对行人、车辆号牌等敏感信息，实时匿名化处理技术（如动态人脸打码、车牌模糊化）已成为强标下的技术刚需。
- **座舱数据处理**：“默认不收集”、“车内处理”等原则，要求数据安全方案具备更强的用户知情同意机制和本地处理能力。
- **AI 训练数据安全**：车云一体架构下，海量数据用于 AI 模型训练时的流转

合规与防投毒安全问题日益突出。

智能网联汽车因数据流动程度的不同，数据安全的责任方与保护手段也不相同。一般针对数据中心与车辆端、V2X、第三方数据共享等不同的场景，分别对应着数据贮存安全、数据访问安全以及数据开放共享安全等三类不同的安全需求。对应的解决方案可以是单独交付的，亦可以是整车数据安全解决方案交付，后面的能力部分会有详述。

### 1.2.3 智能网联汽车数字钥匙

数字钥匙方案让用户通过手机控制汽车，对于消费者来说，这是汽车“智能化”最直观的感受，因此较快达成行业共识，加以普及推广。

---

从车辆端、移动端、行业标准三个方面来看：

车辆端，主要主机厂均已推出支持数字钥匙的车型，国内众多新能源汽车主机厂紧随其后；移动端，苹果、三星、华为、小米、OPPO 等智能手机厂商已原生支持 UWB 模块；行业标准加快跟进，CCC/ICCE/CCSA 等行业标准化基础框架与规范陆续出台，数字钥匙得以开始大规模量产应用。

---

但在这样的背景下，智能网联汽车数字钥匙的潜在安全风险，同时成为消费者最关心的安全需求之一 —— 除了车主本人，潜在攻击者是否也可以通过数字钥匙窃取信息甚至直接控制汽车呢？智能网联汽车消费者的这种“切身”疑虑，成为主机厂们另一个要关注并解决的安全场景。

### 1.2.4 智能网联汽车“车路云一体化”安全运营

智能网联汽车正从“单车智能”迈向“车路云一体化”的中国方案。全国多个城市已开展应用试点，提炼出十大典型功能场景。智能网联汽车安全运营覆盖司机端、车辆端、路侧端、路网及云端多方，涉及协同感知、协同决策、协同控制等复杂交互场景。

---

智能网联汽车，不止于汽车。

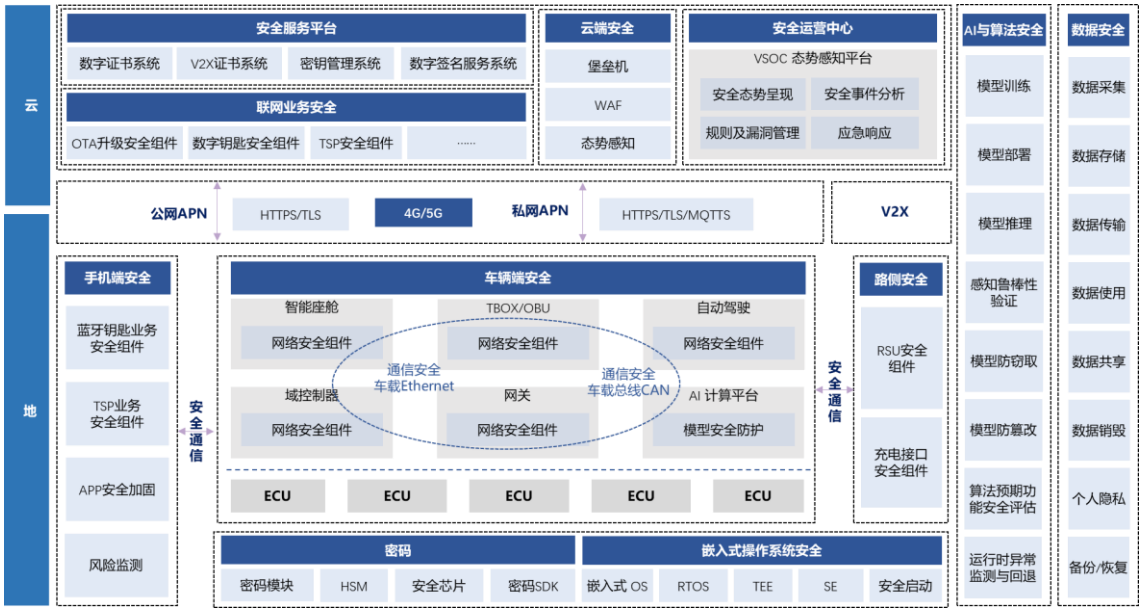
在汽车电子化、道路智慧化、车路云一体化等大趋势之下，智能网联汽车成为智慧城市、智慧交通中必不可少的关键一环，直接或间接带动了城市基础建设、通信网络、卫星定位、智能芯片、视频图像等数十个相关产业聚集。

---

该场景中，安全运营面临极为复杂的挑战：一是车路云各端之间的通信安全风险，需防止伪造路侧 RSU 信息、篡改云端下发的协同决策建议等攻击；二是数据非授权访问与泄露的风险，以及跨域数据交换中的隐私保护问题；三是车端/路端设备 OTA 升级风险，特别是云端控制链路的安全性与实时性保障；四是车辆在不同区域之间跨区运行时可能出现的各种风险与问题；五是针对协同业务逻辑的攻击，如诱导系统做出错误避撞决策等。

除上述已列举的场景外，还有多个场景这里不一一列举。接下来我们详细叙述场景背后所需的安全关键能力。

# 第二章 智能网联汽车安全能力框架




图例：智能网联汽车安全能力框架

如图例框架所示，智能网联汽车的网络安全防御需要覆盖从“云端”到“地面”各终端多层次的纵深防御体系。

从下至上，“地”侧涵盖了车辆端、路侧端及移动端安全。车辆端，需要覆盖智能座舱、自动驾驶、网关、域控制器等关键零部件的安全产品，特别需要在 AI 计算平台中集成模型安全防护模块；路侧端，需要覆盖 RSU、充电接口等安全方案；手机端的数字钥匙、TSP 等也需要安全产品来防御。

云-地之间，通过公网（HTTPS/TLS）和私网（HTTPS/TLS/MQTTS）以及 5G-V2X 融合通信网络打通连接。

“云”主要为安全服务平台、联网业务安全、云端安全及安全运营中心 VSOC。云端安全的堡垒机、WAF、态势感知等是比较成熟的安全防护技术。而安全运营

中心 VSOC 作为强标中明确要求的合规建设对象，需集成 AI 安全态势感知能力，能监测模型漂移、检测异常推理结果，并具备模型快速回退等响应能力。

同时，数据安全贯穿“云-地”，从数据采集、数据存储到最终的数据销毁、备份恢复等提供全生命周期的支撑。AI 算法安全作为新增维度，横跨感知层、决策层与执行层。

根据“云-地纵深防护能力框架”，智能网联汽车网络安全能力的建设首先要覆盖车辆端的车载网络安全防护，需拆解至车机、TBOX、域控制器、AI 计算平台等关键零部件并对其进行加固，形成全面、完整、系统级的安全防护。具体包括密码模块的应用、入侵检测与防御系统（IDPS）和车内网络的安全通信（SecOC、SSL/TLS、IPSec 等），形成针对车辆端的基础安全能力。

其次安全能力要涉及手机端的数字钥匙安全组件、TSP 安全组件等智能网联汽车网联安全需求。

第三，安全能力要包含云端，特别是安全运营中心 VSOC 的建设，VSOC 与车辆端部署的入侵检测与防御系统（IDPS）一体联动，在汽车量产后持续进行安全运营，为 OEM 提供威胁感知、安全分析、态势呈现、应急响应和处置、安全监控等支持。

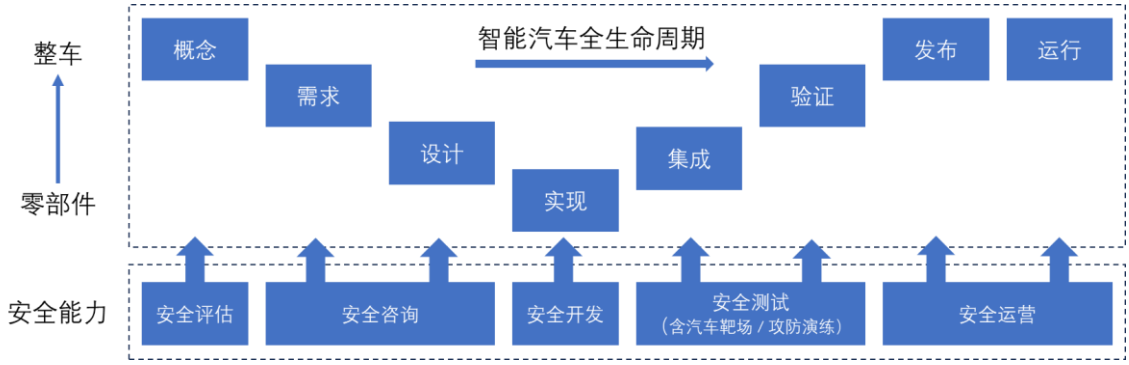
第四，AI 与算法安全能力贯穿车辆端与云端，覆盖模型训练、部署、推理全生命周期，包括感知鲁棒性验证、模型防窃取与防篡改、算法预期功能安全（SOTIF）评估、运行时异常监测与回退等关键能力。

最后，前述各个维度都会实时产生海量的汽车数据，因此还要有专门针对汽车数

据的安全能力覆盖。这几项自下而上的安全能力统一在安全运营平台中，为主机厂、运营方提供统一的安全视角与安全感知能力。当然，在交付客户的时候，可以根据客户需求，采取灵活多样的交付方式。

与传统 IT 产业相比，传统汽车产业，其供应链长度、深度以及复杂程度本就远甚于我们所熟知的传统 IT 设备，进入智能网联汽车时代后，传统汽车产业的供应链也一直在发生着重大改变，从以电机、电控等零部件为核心，发展为以电池、控制系统、AI 计算平台等为核心。

在这样的背景下，我们也可以将上述安全能力框架提炼、抽象后，与智能网联汽车全生命周期对应起来，即从零部件到整车，从汽车初期的概念、需求、设计，到进厂实现、集成、验证，再到最终发布运行，都有相对应的安全能力来覆盖。




图例 2：覆盖智能网联汽车全生命周期的安全能力

鉴于本报告的读者主要为安全行业从业者，下面我们以图例 1 中大家相对熟悉的 IT 安全视角为主，图例 2 中的汽车全生命周期为辅，对框架中主要的智能网联汽车安全能力分别进行论述。

# 第三章 智能网联汽车安全关键能力

## 3.1 嵌入式操作系统技术

嵌入式操作系统技术是智能网联汽车安全能力中的核心基础能力，需要在汽车生命周期的实现、集成、验证等阶段，针对供应链零部件、车载芯片、车载操作系统等目标，通过安全开发或安全测试等方式交付。

由于汽车的复杂性，在考虑网络安全层面的需求时，需突破汽车电子嵌入式基础软件的实时操作系统、通信及诊断等关键技术。智能网联汽车操作系统的漏洞容易导致设备瘫痪、非法程序植入、非法登录、信息窃取和拒绝服务等重大安全隐患。

嵌入式实时操作系统作为智能网联汽车网络安全设备中的核心软件，对设备的功能和性能具有重要影响。通过嵌入式实时操作系统的漏洞发现与识别技术，根据漏洞特征，形成面向特定操作系统的安全加固软件，能有效提升智能网联汽车的安全防护能力。

对车载芯片，重点关注固件安全以及固件中的源代码安全；对车载操作系统，特别是 QNX、以及基于 Linux 的 RTOS，重点关注密钥和证书的生成和存储，可信下载的安全保障与安全更新等。尤为重要的是，在 AI 时代，车载操作系统不仅要保障自身安全，还需为上层感知、决策算法提供安全运行环境（TEE/SE），保障 AI 模型和关键参数在存储和运行时段的机密性与完整性。

此外对 OS 自身以及 OS 中的第三方代码库的安全也应当加以关注，建议重点关

注各主流漏洞情报社区，第一时间掌握 OS 面临的潜在风险。

## 3.2 智能网联汽车架构安全

相比传统汽车，智能网联汽车所谓“智能”，其背后最大的变化就在于架构的变化。即从传统的基于分布式 CAN、面向信号（Signal-Oriented）的架构，转为了基于控制器集中化、面向服务（Service-Oriented）的架构。

新架构中，通信协议、传输内容、中间件、接口等都有了变化升级，同时增加了对摄像头、IVI、HUD 等智能传感器、控制器的支持。特别地，高性能 AI 计算平台（如 Orin、Thor 等）的引入，使得架构中出现了独立的 AI 域或功能模块。如此以新架构为基础，智能网联汽车的自动驾驶、OTA 升级等才成为现实。

因此智能网联汽车架构的安全能力中，要针对 CAN、FlexRay、车载 Ethernet 等主流通信协议，以及 SOA 架构等新一代 EEA 架构提供整体安全解决方案。安全能力要贴合 AUTOSAR SecOC 等行业安全通信标准，覆盖 SOA 架构中车辆端内部 ECUs、域控、网关、TBOX、智能座舱、AI 计算平台等单元之间的安全通信，同时还要覆盖车辆端与手机端、路侧端、云端等各端之间的通信安全；此外，还应当针对 OTA 升级、AI 模型更新等场景，提供有针对性的架构安全能力，重点关注 AI 功能相关服务调用的认证授权与接口安全。

## 3.3 智能网联汽车网联安全

智能网联汽车，所谓“网联”，即与智能网联汽车相关的移动端、人端、车端、路侧端、云端等各终端相互连接后形成的网络所面临的安全需求，这其中以数字钥匙、V2X 云控为主要代表。

数字钥匙，如“场景”部分所述，是智能网联汽车中离用户最近，车主们感受也最直观的一项。因此数字钥匙安全首要关注钥匙自身的高安全性，例如其安全等级要满足 WP29/ISO21434 标准要求，同时在机密性、完整性方面要具备防克隆、抗重放保护、业务异常操作监测等能力；其次，在网络连接方面，数字钥匙要注意高精度定位、蓝牙高稳定连接、多协议支持、以及移动端 APP 安全；最后，数字钥匙在云端一侧除了业务中台、用户管理、钥匙管理、车辆管理等管理功能外，云端自身要着重做好安全防护，避免“一锅端”这样的极端安全事件，因此数字钥匙云端通信相关的 VSOC、MES、PKI、KMS 等系统都应当同下面即将提到的云控体系一道，构建起体系化安全能力。

V2X 云控，在实现汽车高度智能化的同时，由于网络和平台的开放性，以及海量数据的采集和处理，导致其面临严峻的网络安全和数据安全风险，一旦其安全性遭受破坏，将导致系统功能失效，进而影响人身财产安全、交通安全，甚至社会安全和国家安全。

单就目前主流的 C-V2X（蜂窝 V2X）体系来说，针对车端和路端，为避免 OBU、MEC、RSU 等零部件面对的身份伪造、未加密传输、会话劫持等安全风险，其安全防护手段主要以可信安全芯片、密码模块 SDK、安全 SDK 等来实现。随着“车路云一体化”的推进，还需新增对车路协同消息（如 BSM、RSM、RSI）的多源验证、时空一致性校验能力，防止“幽灵车”或错误路况信息注入。云端，则在满足合规要求的基础上（等保三级安全建设），同时从 CA 建设、网络安全、通信安全、数据安全、OTA 升级、跨区域运行等多个维度，以系统化视角，对车、路、云等 V2X 各端提供整体安全解决方案。

此外，随着 5G NR-V2X 的标准落地，5G 网络自身安全特性的增强虽然一定程度上会提升 V2X 的基础安全能力，但 5G 网络带来的强时效性的特点更加突出，越来越多的“X”终端设备会接入 V2X 网络，加之 5G 边缘计算同时也会产生大量终端侧数据，因此总体而言 5G NR-V2X 的攻击暴露面是迅速扩大的，需关注 5G 空口的信令面与用户面安全增强、网络切片隔离，以及 MEC 平台上的应用安全和数据安全，这一点也应当提前考虑到。

## 3.4 智能网联汽车数据安全

相比于传统 IT 环境下的数据安全，智能网联汽车数据安全不能简单将每一台车看做一个数据终端，而是需要深入到汽车内部，从汽车端的 ECUs、域控、网关、TBox，一直延伸到汽车外部数据所流向的监管方、二手车与保险等第三方平台，以及合资、外资车企相关的境外平台。

因此，智能网联汽车数据安全首先要同时符合网络安全、数据安全相关法律法规以及汽车行业相关合规要求，然后在合规基础上，从汽车内的 ECUs 开始入手，一直到汽车外流向的各方，做好汽车数据的分类分级与安全防护。

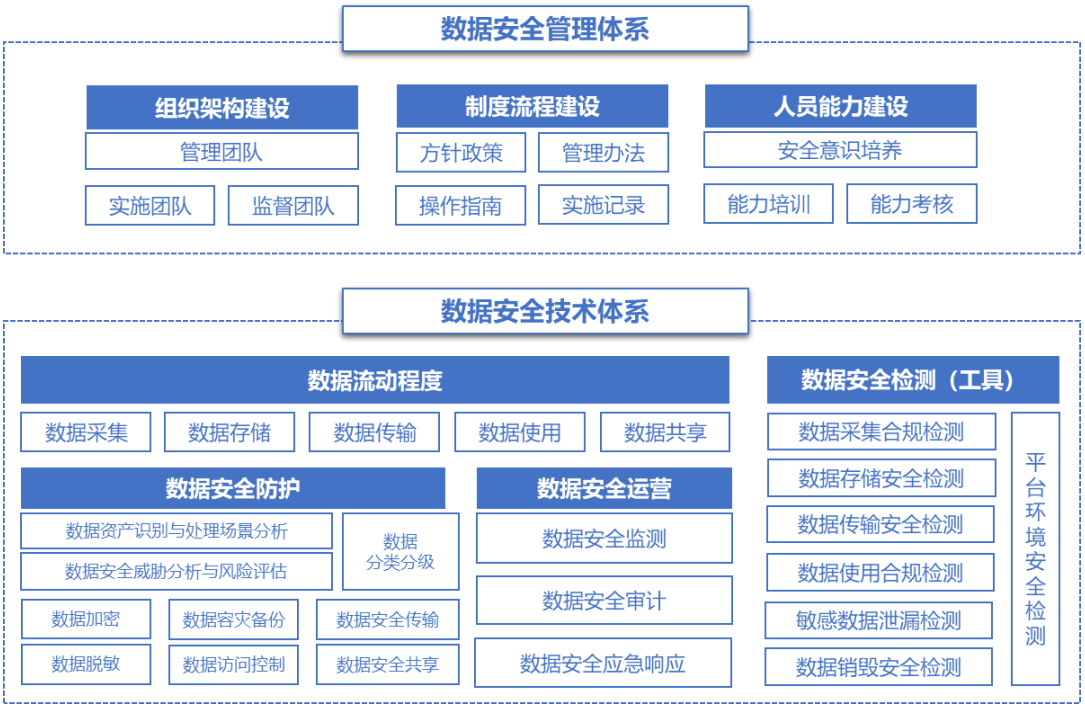
如场景部分中所述，智能网联汽车数据流动程度的不同，数据安全的责任方与保护手段也不相同。

例如对贮存在数据中心的数据，以及车辆端实时产生的行驶数据、驾驶员及乘客的影音数据——特别是只在车辆域内处置的数据——由汽车主机厂、运营方以数据合规要求为基础，行使“数据贮存安全”责任；对于在路侧端、云端等 V2X 各端间流动的数据，由主机厂与运营方负责，保护手段则以“安全访问域”为原则，

采用“数据访问安全”类解决方案；向监管方、第三方平台（二手车、保险等）开放共享的数据，则要在安全、有限、不泄露用户个人隐私的前提下，由各相关方共同行使责任，保护手段则以“可用不可见”为原则的“数据共享安全”为主。

特别需要关注的是，智能驾驶所依赖的高精度时空数据（高精地图、定位等测绘地理信息数据），需满足最高的安全保密管理要求。针对合资或外资车企的数据出境场景，须建立完整的数据出境安全评估、脱敏和审计技术方案。

对于有能力的安全企业，可以数据安全组件的方式，在 ECUs、域控、网关、TBox 等各关键环节，对数据以及数据的采集、脱敏、分析、传输、日志（包含数据处理日志与数据安全事件日志）等行为进行全程监测，满足上述数据安全需求，即业内所说的整车级数据安全解决方案。




图例：数据安全管理与技术体系

## 3.5 智能网联汽车 AI 与算法安全

AI 算法正成为智能汽车的感知大脑和决策核心，但其自身的安全脆弱性构成了全新且致命的威胁。感知系统可能被对抗样本欺骗，决策模型可能因数据投毒而产生错误判断，模型本身可能被窃取或植入后门。这些风险催生了 AI 与算法安全这一全新能力维度，需构建覆盖模型全生命周期的安全体系：

鲁棒性验证与增强：能对感知、决策模型进行系统性的对抗测试，包括但不限于对抗样本生成、物理世界模拟攻击测试（如对抗贴纸、特殊光照、形变物体等），并通过对抗训练、模型蒸馏等技术增强模型鲁棒性。

模型防窃取与防篡改：在模型存储、加载、运行时提供加密、完整性校验和代码混淆能力，防止核心算法 IP 泄露或被恶意植入后门。车载端需利用硬件安全模块（HSM）或可信执行环境（TEE）保障模型运行时的安全。

算法预期功能安全（SOTIF）评估：对因 AI 算法功能不足（如罕见目标漏检、传感器融合逻辑缺陷、ODD 边界识别不足）导致的危害场景进行系统性识别与评估，并建立针对性的风险减缓措施，这是智能驾驶准入的重要技术支撑。

运行时异常监测与回退：在 VSOC 和车端部署监测模块，实时分析模型输入（传感器数据流）的统计漂移和输出（决策指令）的可信度，一旦发现异常即触发告警或执行最小风险策略（如降级运行、安全靠边停车）回退。

AI 训练数据安全：具备数据投毒检测与清洗能力，确保用于模型迭代的数据集质量与安全性，防止恶意数据污染模型。

# 第四章 智能网联汽车安全代表企业

本章代表企业以公司简称首字母排序，排名不分先后。各厂商能力描述依据公开资料及访谈整理，个别厂商采用的“首个”“最早”等表述均出自厂商口径，未经独立第三方核实，仅供参考。

## 4.1 360 数字安全

**主要服务对象：**主机厂、Tier1

**差异化特点**

1. 集团安全底座赋能：依托 360 安全大数据、威胁情报与安全专家体系，车联网安全团队（Sky-Go）自 2014 年起研究智能网联汽车安全。
2. “车载安全大脑”体系：由多个车载安全引擎＋车载卫士构成，覆盖车辆控制、远程升级、自动驾驶、智能座舱、车路协同等六大场景。
3. 规模化云侧运营：VSOC／安全大脑（据 360 披露）累计为百万级智能汽车提供安全监测，云端监测与运营能力突出。
4. 开放生态打法：免费 SaaS 版 VSOC、开放车端 IDPS 能力与源码，低门槛切入车企供应链；同时具有以产业资本身份（哪吒汽车战略投资方）绑定车企的经历。

**部分用户**

战略合作：比亚迪；投资合作：哪吒汽车；合作客户：东风日产（联友科技）

**联系方式**

官网：https://360.net；热线 400-0309-360

## 4.2 梆梆安全

**主要服务对象：**主机厂

**差异化特点**

1. 移动安全切入车联网：以十余年移动应用安全积累切入车联网，覆盖 TSP 云平台 API、车载 APP、手机 APP、数字钥匙 SDK、手表／穿戴应用等手机端安全，形成“安全检测—防护加固—上线后监测”三段式能力。
2. 开展覆盖整车系统及关键零部件的深度安全测试，通过渗透测试及 R155、GB44495 等标准的合规测试，结合威胁建模、漏洞分析、漏洞利用等系统化方法，识别安全隐患与攻击路径，支撑企业满足国内外汽车信息安全标准认证。
3. 基于自动化合规检测平台与专家评估能力，为车联 APP、车载 APP 及车机 IVI 提供涵盖国内外法规的数据安全合规服务，实现高效精准的合规差距识别与整改支撑，助力企业满足监管要求。
4. 构建以“汽车信息安全测试系统”为核心的检测能力建设方案，通过集成化测试工具箱与统一管理平台，赋能车企实现标准化、系统化的安全测试流程；通过培训、测试项目指导，支持实验室自建与检测体系优化提升。

**部分用户**

国内主要金融机构及智能网联汽车产业链企业

**联系方式**

官网：https://www.bangcle.com

## 4.3 尺物科技

**主要服务对象：**主机厂、Tier1、检测机构

**差异化特点**

1. 二进制级安全、无需源代码：以"高级二进制级处理技术"为核心，直接对编译后的固件与二进制应用开展分析、检测与加固，支持 ARM、AArch64、MIPS、PPC、TriCore、X86、AMD64、RISC-V、龙芯等主流架构，以及 Linux、Android、QNX、RTOS、车机专有平台。
2. 车联网供应链安全全链条：覆盖 SBOM 自动化生成（可导出 SPDX/SWID/CycloneDX）、开源 License 合规、已知漏洞检测（集成 CVE/CNNVD/CNVD）、二进制代码质量评估（20+ CWE 检测项，覆盖 CERT-C/MISRA/AUTOSAR 规范），面向 OEM 与 Tier1/Tier2 供应商的固件供应链风险管控。
3. 0-Day 未知漏洞挖掘：自研漏洞分析引擎，独创虚拟执行引擎（单步执行汇编、监控 CPU 寄存器变化）与跨函数调用栈分析，结合代码大模型解释漏洞逻辑，误报率低、漏洞价值高。
4. 二进制应用加固：融合静态逆向对抗、动态反调试、指令集虚拟化等技术，无需源码一键加固，覆盖通信协议（T-BOX/网关）、ECU 控制器、自动驾驶 DCU 算法保护、智能座舱隐私保护等场景。
5. 合规与渗透测试：面向 UNECE WP.29 R155/R156、ISO/SAE 21434、GB 44495/44496-2024 等法规要求，提供整车/零部件渗透测试，覆盖 TSP 远程入侵、恶意刷写固件、控车指令、蓝牙/OBD/无线钥匙等攻击面。

**部分用户**

比亚迪、中国一汽、华为、中国汽研（CAERI）等车企及检测机构；中国信通院、中国电子技术标准化研究院、中国赛宝实验室等科研检测单位。

**联系方式**

官网：https://www.bit-sec.com；邮箱：support@bit-sec.com；电话：028-67136496

## 4.4 绿盟科技

**主要服务对象：**主机厂、检测机构

**差异化特点**

1. “云—管—端”一体化车联网安全监测与防护体系：以车端 IDPS（安全 SDK）＋云端 VSOC 态势感知平台协同，覆盖数据汇聚、分析、安全管理、资产管理、分层态势、工单、级联、知识库等能力。
2. 低资源占用、高并发：车载 SDK 平均 CPU 占用<10%、静态 2.4M／动态约 300K，平台支持百万级终端接入，适配分布式、域集中式等多种整车 E/E 架构。
3. 合规导向：满足 UN R155/WP.29、ISO/SAE 21434 等国际法规及国内车联网监管要求，参与建设工信部车联网安全态势感知平台。
4. 攻防实战与漏洞挖掘：多次获车联网攻防比赛一等奖（第三届车联网信息安全挑战赛第一名），具备整车级、部件级实战化漏洞挖掘能力。
5. 全生命周期安全服务：覆盖威胁分析、风险评估、安全设计开发、安全测试、安全运营、安全培训。

**部分用户**

一汽、长城、长安、北汽、奇瑞、吉利、柳汽等主流车企（数十款车型安全服务）

**联系方式**

官网：https://www.nsfocus.com.cn

## 4.5 木卫四

**主要服务对象：**主机厂、Tier1

**差异化特点**

1. AI 原生汽车安全平台：S3 Platform（Sight/Shield/Safe）以 AI 驱动，推出 130 亿参数汽车安全垂类大模型“蝴蝶”，支持私有化部署。
2. 团队源自百度 Apollo：创始人云朋曾任百度 Apollo 首席安全架构师，主导百度无人车信息安全体系，具备车企前装量产经验。
3. 非侵入式端云一体化：S3-VSOC 采用 AI＋云原生＋微服务架构，非侵入式分析 IVI、T-BOX、CGW 等 ECU 指令及 TSP/OTA/PKI 等云端服务。
4. 汽车专属威胁情报：S3-VTI 为国内较早专为智能网联汽车生态设计的威胁情报及漏洞管理方案。

**部分用户**

宝马中国、奇瑞、蔚来、福特、赛力斯等

**联系方式**

官网：https://www.callisto-auto.com

## 4.6 犬安科技

**主要服务对象：**主机厂、Tier1、检测机构

**差异化特点**

1. 全生命周期平台化：ThreatTrace 汽车安全管理平台贯穿“设计—开发—运营—维护—报废”，模型驱动、支持跨组织数据交换，对标 WP.29 R155/R156、ISO/SAE 21434 及国标。
2. TARA 自动化工具：DefenseWeaver 以 AI 辅助实现威胁分析与风险评估自动化。
3. 自研硬件测试设备线：GoGoBark 系列覆盖 LiDAR、UWB、蓝牙、车载以太网等前沿接口，支撑渗透与合规测试。
4. 攻防实战能力：全球汽车安全研究组织 ASRG 中国合作伙伴，国家车联网漏洞库（CAVD）技术支撑单位。

**部分用户**

小米汽车、联合汽车电子（UAES）、阿维塔、蔚来、宝马中国、一汽奔腾等

**联系方式**

官网：https://www.gogobyte.com

## 4.7 天融信

**主要服务对象：**主机厂、检测机构

**差异化特点**

1. 综合安全厂商的全栈能力：产品线覆盖车载防火墙、车载入侵检测与防御系统、车载安全 SDK、车联网安全运营平台（VSOC）、车联网安全检测实验室及安全服务，形成“安全合规＋威胁对抗＋安全运营”闭环。
2. 车载防火墙起家、重点深耕车载入侵检测：2017 年进入车联网，以车载防火

墙切入，重点聚焦车载入侵检测（IDPS），对车内网络与攻防积累较深。

3. 标准与联盟卡位：牵头《智能网联汽车网络安全检测技术要求》等标准，任 CCF 计算机安全专委会车联网安全工作组组长单位，参与 20+ 车联网安全标准及 10+ 行业联盟。
4. 自主可控与专利积累：车载防火墙、车载入侵检测等产品自主可控，100+ 专利创新积累。

**部分用户**

北汽、广汽、东风等主流车企，以及中汽创智、国家级检测机构

**联系方式**

官网：https://www.topsec.com.cn；服务热线 400-777-0777

## 4.8 为辰信安

**主要服务对象：**主机厂、Tier1、检测机构

**差异化特点**

1. 全栈全要素全生命周期覆盖：从密码模块、IDPS、安全通信（SecOC）到车辆安全运营中心（VSOC）、数字钥匙、汽车网络靶场、测试工具，覆盖智能汽车“云—管—端”全要素与概念、设计、集成、验证、运营全生命周期。
2. 嵌入式技术出身：核心团队源自军工体系，是国内较早从事嵌入式操作系统研究的机构之一，2000 年进入嵌入式 OS、2009 年承担“核高基”汽车电子基础软件重大专项，是少数同时吃透汽车产业与嵌入式底层技术的团队。
3. 标准与合规先发卡位：牵头制定国内智能网联汽车网络安全国家标准，落地国内汽车领域早期网络安全咨询项目（J3061），在 ISO 21434、WP.29 合

规咨询与认证方面有先发优势。

4. 大规模量产经验：产品覆盖主流 OEM、零部件厂商及检测机构，安全产品已大规模量产应用。

**部分用户**

覆盖国内主流 OEM、零部件厂商及检测机构（公开口径：服务客户 150+）

**联系方式**

官网：https://www.vecentek.com

## 4.9 信长城

**主要服务对象：**主机厂、Tier1

**差异化特点**

1. 以密码技术为基因底座：以组合公钥密码（CPK）为主、PKI 为辅，具备国密安全芯片、软件密码模块、密钥管理系统（KMS）等完整密码产品，可同时服务车联网安全与密评密改两块市场。
2. “密码＋AI”融合：在低算力车载环境实现整车数据加密、车载智能体可信身份认证。
3. 组件化、车规化前装量产：以“积木式安全组件”适配 NXP S32G、高通 SA8155、英飞凌 TC3xx 等主流车规芯片，强调前装量产交付。
4. 场景覆盖广：产品线覆盖 C-V2X 安全证书管理系统（V2X CA）、数字钥匙、SecOC 总线安全、OTA 安全升级、数据脱敏等关键场景。

**部分用户**

吉利、一汽、北汽、上汽、泛亚、奇瑞、零跑、滴滴、DeepWay 等

**联系方式**

官网：http://www.i-wall.com.cn

## 4.10 云驰未来

**主要服务对象：**自动驾驶公司、主机厂、Tier1、示范区

**差异化特点**

1. 自动驾驶场景深耕：国内较早深耕自动驾驶场景信息安全的团队之一，自 2018 年起为百度 L4 级无人驾驶车辆提供信息安全产品。
2. 稀缺的车规级硬件能力：自研车规级＋EAL4 认证的车载安全网关（D2000E）、5G/V2X 车规级多域互联中央网络控制器（CNCU/L3000）等硬件，满足智能汽车高安全、高性能、高可靠要求。
3. 软硬结合、车路云一体化：覆盖从概念设计（InTARA）到研发验证（安全中间件）、运营监控（inVSOC）的全生命周期，并配套 ISO 21434、WP.29（R155/R156）合规咨询（含出海）。
4. 客户卡位高：同时覆盖自动驾驶公司、OEM、Tier1 及示范区四类客户，作为信息安全供应商参与北京市高级别自动驾驶示范区场景。

**部分用户**

宝马、东风、百度 Apollo、京东物流、文远知行等。

**联系方式**

官网：https://www.inchtek.cn

## 4.11 泽鹿安全

**主要服务对象：**检测机构、主机厂

**差异化特点**

1. 攻防靶场／众测专业型厂商：主打真实车辆远程接入的众测与漏洞验证（区别于纯仿真），形成“众测靶场、漏洞验证靶场、科研实验靶场”三大靶场。
2. 政府／监管背书强：连续承办工信部“铸网行动”汽车安全演练，“强网杯”全国网络安全挑战赛车联网专项赛等多项国家级高水平赛事。
3. 漏洞研究积累：覆盖 50+车型、发现 600 +可验证安全漏洞，是工信部车联网漏洞库（CAVD/NVDB）首批技术支撑单位。
4. 攻防赛事运营能力：自研“太初封神台”线上攻防赛事平台，已成为 CCF 智能汽车大赛（汽车安全攻防赛）等行业赛事指定平台。
5. 定位清晰：聚焦检测／测试／合规服务，与车载前装安全件量产厂商形成差异化。

**部分用户**

比亚迪、北汽、零跑、蔚来等 16 家国内主流车企（靶场已服务二十余家整车厂六十余款车型）。

**联系方式**

官网：https://www.secdeer.com

## 4.12 智车信安

**主要服务对象：**主机厂、检测机构

**差异化特点**

1. 较早通过认证的 VSOC 平台：基于数据驱动的智慧车联网安全运营平台，可为数百万联网车辆提供安全运营服务，并通过数字孪生技术将能力扩展到功能安全、预期功能安全。
2. 较早推出 TARA 分析服务与自动化工具：依据 ISO 21434 构建，内置组件/威胁/措施/评分/路径五大知识库，图形化建模、跨项目协作、定制化报告，支撑 CSMS、VTA 认证落地。
3. IDPS 全维度防护：提供以太网 IDS、总线 CAN-IDS、主机 HIDS 三类组件，检出率>95%、误报率<1%，CPU 占用<5%（CAN-IDS RAM 低至 60KB），标准化接口、可移植、轻量化，运行参数与规则支持云端实时下发动态生效。
4. 较早切入车联网安全运营的团队（SINCE 2016）：全栈检测与渗透能力（资产发现覆盖率≥98%、源码审计精度≥95%、智能设备支持 50+ 协议栈），"检测・赋能・运营"三位一体。
5. 数据安全合规闭环：与具备司法鉴定资质的弘连网络合作电子数据存证，提供数据匿名化合规检测工具（便携"手提箱"形态，脱敏匹配精度>98%），覆盖 GB/T 44464、GB/T 44495 等法规要求。

**部分用户**

中国一汽、一汽-大众、北汽集团、路特斯（LOTUS）、亿咖通（ECARX）、极星汽车等车企，以及公安部第一/第三研究所、中国信通院、中汽中心等检测机构。

**联系方式**

官网：http://vsoc.vip

# 第五章 智能网联汽车安全未来展望

## 5.1 安全是成本，更是竞争力，重视安全才能赢得更大市场

《汽车整车信息安全技术要求》已正式发布，《智能网联汽车 组合驾驶辅助系统安全要求》等强标也已相继落地，智能网联汽车安全的重要性业内已经形成共识，很多车企将其作为隐性成本并不愿意投入，但安全是成本，更是竞争力，更加重视安全的智能网联汽车会赢得更大的市场。这一趋势将深刻重塑市场格局：一方面，能够提供“一站式过检”解决方案（覆盖整车信息安全、软件升级、数据安全、AI 安全）的供应商将获得显著竞争优势；另一方面，合规需求将推动安全测试、安全运营等细分市场加速成熟。

## 5.2 智能与安全深度耦合，AI 成为安全攻防新高地

智能网联汽车的安全战场正从传统网络边界延伸到 AI 模型本身。感知系统对抗样本攻击、决策模型数据投毒、算法逆向工程等新型威胁层出不穷。相应地，“AI for Security”（用 AI 检测威胁）和“Security for AI”（保障 AI 本身安全）的双向能力，将成为衡量安全企业技术实力的核心分水岭。安全方案需要从“为代码安全而设计”演进到“为模型安全而设计”，将安全能力嵌入 AI 研发与部署的全流程。

## 5.3 数据要素价值凸显，汽车数据安全从"合规底线"走向"价值底座"

智能网联汽车每时每刻产生的海量数据，其角色正从"需要保护的成本"转变为"

可流通、可交易的生产要素"。随着数据分类分级、数据资产入表、数据出境安全评估等机制逐步落地，汽车数据安全的内涵将从"满足合规、防止泄露"的底线思维，升级为"保障数据可信流通、释放数据要素价值"的价值思维。高精度时空数据、自动驾驶训练数据、座舱用户数据等核心资产，将成为车企数字化转型与商业模式创新的基础。相应地，数据安全能力也将从"成本中心"走向"竞争力来源"，谁能率先建立可信的数据治理体系，谁就能在数据要素时代赢得先机。

## 5.4 供应链复杂度持续攀升，安全从"单点防护"走向"全链条治理"

智能网联汽车供应链的长度、深度远超传统 IT 设备，OEM、Tier1、Tier2 乃至芯片、算法、开源组件层层嵌套。当供应商设备的源代码不可获取、开源组件激增、软件迭代周期缩短，传统"单点防护"已难以为继。软件物料清单（SBOM）、开源合规、供应商风险管理、固件二进制安全等全链条治理能力，将从"可选项"变为"必选项"，推动供应链安全成为新的独立赛道。

## 5.5 中国车企加速出海，全球合规能力成为新门槛

随着中国智能网联汽车加速走向全球市场，UN R155/R156、GDPR 及各国数据本地化等法规，成为出海车型必须跨越的门槛。CSMS、SUMS、VTA 等认证体系，以及数据出境安全评估、脱敏与审计等能力，将从"出海附加项"变为"全球化入场券"。能够提供"一站式出海合规"解决方案的安全厂商，将在中国车企全球化进程中扮演关键角色。

## 5.6 智能网联汽车需要“安全共生”理念成就健康产业生态

“叠积木”式的安全修补已难以为继。未来的安全能力必须像基因一样，在设计

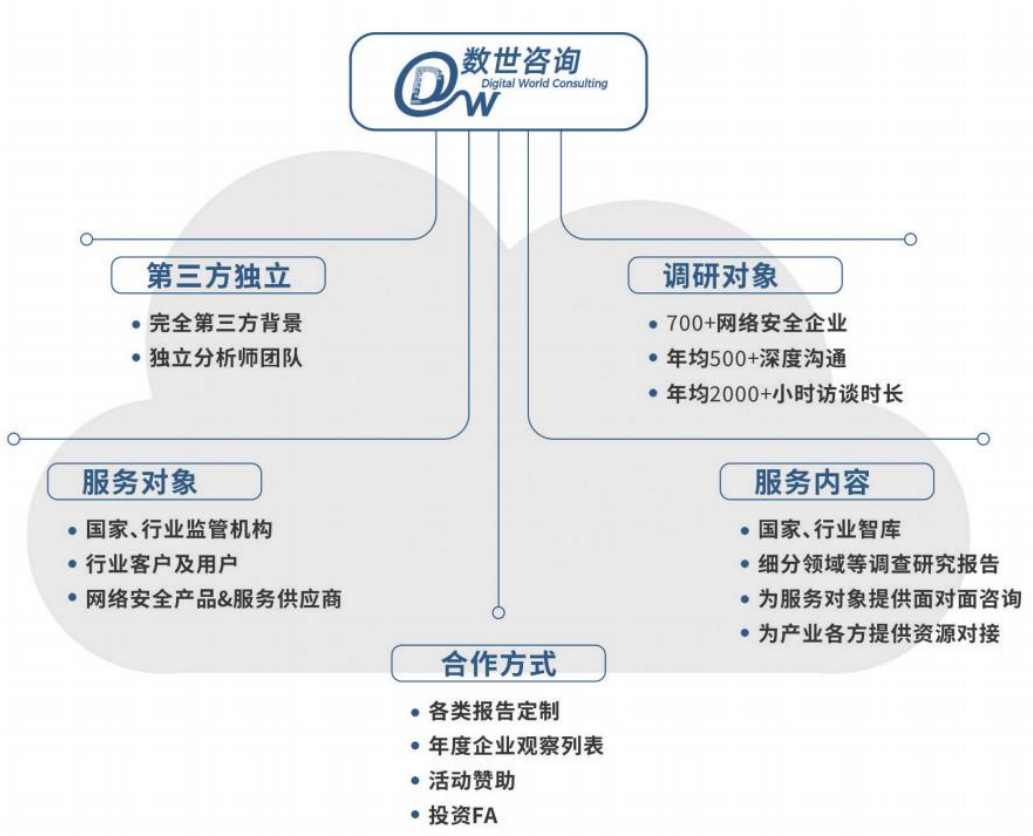
之初就融入汽车的 EE 架构、SOA 服务及 AI 模型中，实现“出厂即安全”。因此，功能安全、预期功能安全与网络安全的“三安全融合”将成为产业共识，推动汽车安全从单维防护走向系统化的安全生命周期管理。这就要求安全公司与主机厂、Tier 1 及 AI 芯片/算法公司建立更深度的产业合作关系，从需求定义阶段即协同参与，构建起“共生安全，共同价值”的新型产业生态。

# 附录：智能网联汽车安全主要行业标准与技术要求

| 标准名称 | 主要内容/重要性 | 状态/说明 |
| --- | --- | --- |
| ISO 21434 | 道路车辆-网络安全工程国际标准，覆盖全生命周期 | 已发布 |
| UN R155 / UN R156 | 车辆网络安全及软件更新国际法规 | 已生效，部分国家和地区已强制要求 |
| 《汽车整车信息安全技术要求》（GB 44495-2024） | **整车级信息安全的强制性国家标准，覆盖车辆全生命周期** | 已发布，2026 年实施 |
| 《汽车软件升级通用技术要求》（GB 44496-2024） | 汽车软件升级（OTA）安全的强制性国家标准，覆盖升级包真实性、完整性校验等 | 已发布，2026 年实施 |
| 《智能网联汽车 组合驾驶辅助系统安全要求》（GB 47955-2026） | **针对 L2 级 ADAS 系统的强制性国家标准，涵盖 DMS、人机交互、数据记录等** | 已发布，2027 年 1 月实施 |
| 《智能网联汽车 自动驾驶数据记录系统》(GB 44497-2024) | **要求配备类似“黑匣子”的数据记录系统** | 已发布，2026 年实施 |
| 《智能网联汽车 自动驾驶系 | 针对 L3/L4 级自动驾驶系统的强 | 已发布，2027 年 7 月 |

| 标准名称 | 主要内容/重要性 | 状态/说明 |
| --- | --- | --- |
| 统安全要求》(GB 44721-2026) | 制性国家标准，划定责任边界、明确系统安全水平与人机交互 | 实施 |
| **《机动车运行安全技术条件》（GB 7258 修订）** | **对加速控制、单踏板模式、隐藏式门把手等提出安全要求** | **征求意见中** |
| GB/T 41871-2022 | 信息安全技术 汽车数据处理安全要求 | 已发布 |
| 《汽车数据安全管理若干规定（试行）》 | 汽车数据安全管理专项规定 | 已实施 |
| AUTOSAR SecOC | 车内安全通信标准 | 持续更新 |
| CCC / ICCE | 数字钥匙行业标准 | 持续更新 |
| TC260 智能驾驶安全标准体系研究 | “端-网-云”智能驾驶安全标准体系，重点纳入 AI 安全 | 已发布研究报告 |
| UN R171 | 车辆驾驶员控制辅助系统（DCAS）国际法规 | 已发布，国内强标与之协调 |

**如果您对报告有任何问题或意见，包括引用、指正或合作，请通过电子邮件 liuchenyu@dwcon.cn 与我们联系。**




北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业800余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接、安全产品与企业推荐、企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www. dwcon. cn
联系邮箱：dw@dwcon. cn

小酒馆

数世咨询
Digital World Consulting
数字安全领域独立第三方调研机构