China EV100
中国电动汽车百人会

调研报告

第 26 期

（总第 76 期）

车百智库　　2022 年 12 月 06 日

智能网联汽车数据安全防护技术发展的问题及建议

数据逐渐成为智能网联汽车的关键要素，以数据安全为核心的新汽车安全问题日益凸显，本文研究的是如何加快智能网联汽车数据安全防护技术的创新与应用，引导数据处理各方高度重视，以提高汽车全生命周期数据安全防护能力。

一、智能网联汽车发展对数据安全防护提出新要求

1、汽车智能化、网联化发展过程中暴露出的数据安全问题和风险日益突出。

汽车智能化、网联化打开了原有车内域、车间域、交通域、车云域的边界，打破了汽车控制系统原有的封闭生态，汽车数据将面临来自“云-管-端”三方面的安全风险。

汽车软件代码数量和对外接口增加，加大了车辆安全风险和防护难度。智能网联汽车集成了更多软件，其代码数量已是传统汽车的 4-5 倍，且在不断增长。智己 L7 的软件代码行数为 2.8 亿，特斯拉 S 更是超过 4 亿。相应的，汽车的系统漏洞数量和对外接口也随之增加，加大了黑客通过软件侵入车辆的风险。

例如，汽车数字身份漏洞会带来黑客攻击隐患，汽车网关、充电系统、智能钥匙、外部进程、3G/4G 网络等通信接口不断增多，且存在错综复杂的传输介质、协议等，导致汽车面临的攻击范围更大且受攻击点数量更多，数据安全防护难度较大。

车与云、车与车间数据频繁的交互，使云端、管端数据风险增加。一方面，是智能网联数据在云端存储导致的安全风险。智能网联汽车产生的数据量随智能化功能叠加而不断增多（见图表 1）。由于车端存储空间有限，云平台成为各类汽车数据的汇集点，具有极高价值。但目前私有云、公有云、社区云各有其潜在安全隐患，可能面临被攻击、劫持等风险，造成敏感信息泄露，不法分子甚至可以通过伪造、篡改指令和数据内容等方式非法控车。

另一方面，数据交互、数据共享等传输过程也存在信息泄露风险。智能座舱、哨兵模式等技术、功能的实现需要频繁进行车云交互，伴随功能丰富，车车、车路之间也会出现频繁的数据交互行为。但车内数据传输主要根据功能进行编码，按照报文 ID 进行标定和接收过滤，通讯网络很容易受到嗅探、窃取、伪造以及篡改等攻击威胁。通讯协议若是引入安全隔离、数据加密等防护技术，会造成较大时延，加大智能网联汽车行驶的安全风险。如何能在保障数据传输安全的前提下降低通信时延，是亟待突破的技术难题。

图表 1 自动驾驶汽车每日产生数据量

数据来源：百人会车百智库研究院整理

2、数据安全防护技术要根据汽车独特性进行创新。

传统汽车的功能安全、网络安全防护手段已无法有效解决新的数据安全问题，互联网、金融等领域的领先数据安全防护技术，也很难直接引入车端，需结合汽车产品及产生数据的特点，对安全防护技术进行创新。

（1）汽车数据安全防护的环境复杂性更高。汽车高速移动、空间有限、运行环境复杂的特点提高了对安全防护技术的要求。一是汽车移动过程中网络节点会高速切换，速度通常在 50km/h 以上，要同时满足数据传输的完整性、安全性和链路稳定性，对技术的要求很高。二是汽车作为消费产品，受成本和空间限制，芯片的高成本致使车端算力和存储空间很难持续叠加，需要控制安全防护技术对车端算力的消耗。三是汽车运行环境更为复杂，对车规级安全防护硬件的稳定性要求较高，需能抗腐蚀、抗震动、抗沙尘等。

（2）汽车数据安全防护对实时性要求较高。汽车数据具有随时间变化的动态特征。以感知算法为例，在产品迭代过程中算法也在迭代，数据和算法之间的关系也会随产品迭代而发生变化，这导致预先定义的规则具有了时效性，安全防护的规则也需要根据汽车数据的变化实时进行调整。

（3）汽车数据安全隐私的广度正不断增加。越来越多的量产车开始搭载自动驾驶、智能座舱、高精地图等新技术，尝试推出哨兵模式、远程拍照等新功能，智能网联汽车逐渐覆盖出行、娱乐、生活等多种场景。场景覆盖度的不断增加，使得汽车数据安全隐私的广度大幅拓展。数据一旦遭到泄露、篡改、窃取等攻击，不仅会侵犯个人隐私、损害个人财产、威胁个人生命，也对国家和交通安全带来极大隐患。

（4）汽车数据安全需要构建系统级的防护。汽车供应链较

长且涉及企业众多，数据应用接口也多，数据应用系统之间存在重叠区域，需要系统性的针对全供应链条进行安全防护，难度较高。例如，在整车架构体系下进行分解，需要在车厂合规部门统一规划下，分解到车厂各个部门和各级供应商，进行相应的处置和保护，但主机厂和零部件供应商进行安全保护时难以统一上下安全理念。

3、政策法规对汽车数据安全技术发展提出要求。

在“三法一条例”基础上，数据安全法律框架基本形成（见图表 2）。约束和指导行业开展汽车数据安全合规工作，除要求建设数据安全管理体系外，政策法规也明确了技术是保障智能网联汽车数据安全的有利推手。

例如，为满足《汽车数据安全管理若干规定（试行）》提出的汽车数据处理“四大倡导原则”[1]，汽车企业需要提高车端计算能力，发展脱敏技术、迭代算法训练技术等。

《关于加强智能网联汽车生产企业及产品准入管理的意见》中，对网络安全、数据安全和软件升级提出的要求分三方面：企业要构建主轴体系；企业的产品要合规；企业产品研发过程要有足够具有说明力的保证措施。这对企业提出了研发安全的新要求。《关于开展智能网联汽车准入和上路通行试点工作的通知（征求意见稿）》中，对智能网联汽车数据安全提出了企业保障能力、

[1] 1 车内处理原则，除非确有必要不向车外提供；2 默认不收集原则，除非驾驶人自主设定，每次驾驶时默认设定为不收集状态；3 精度范围适用原则，根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率；4 脱敏处理原则，尽可能进行匿名化、去标识化等处理

产品技术、过程保障、测试验证方面的具体要求。

行业政策将技术视为保障汽车安全的重要突破点。《车联网（智能网联汽车）产业发展行动计划》，提出技管结合以推动安全保障体系建立的要求，指出应重点突破产业的功能安全、网络安全和数据安全核心技术，增强产业安全技术支撑能力。《智能汽车创新发展战略》将搭建软硬件结合的安全防护体系，加强车载芯片、操作系统、应用软件的安全可靠性设计，视为保障数据安全的重要任务。

时间	部门	政策名称
2016.2	国家地理测绘局	《关于加强自动驾驶地图生产测试与应用管理的通知》
2021.7	国家网信办、国家发改委、工信部、公安部、交通部	《汽车数据安全管理若干规定（试行）》
2021.7	工信部	《智能网联汽车生产企业及产品准入管理指南（试行）》
2021.9	工信部	《关于加强车联网网络安全和数据安全工作的通知（征求意见稿）》
2021.9	工信部装备发展中心	《关于开展汽车数据安全、网络安全等自查工作的通知》
2022.4	工信部	《工业和信息化领域数据安全管理办法(施行）》（公开征求意见稿）
2022.4	工信部、公安部、交通部、应急管理部、市场监管总局	《关于进一步加强新能源车企安全体系建设的指导意见》
2022.4	工信部装备工业发展中心	《关于开展汽车软件在线升级备案的通知》
2022.5	网信办	《数据出境安全评估办法》
2022.6	工信部	《移动互联网应用程序个人信息保护管理》

时间	部门	政策名称
2022.11	工信部	《关于开展智能网联汽车准入和上路通行试点工作的通知（征求意见稿）》

图表 2 汽车数据安全管理法规条例

信息来源：百人会车百智库研究院整理

二、汽车数据安全防护技术发展与上车的难题

1、细化管理要求不明确，企业难以进行高效精准数据防护。

（1）汽车数据分类分级管理要求不统一，制约汽车数据差异化防护能力发展。汽车数据类型复杂且量大，包括车辆、道路环境、通信网络、行人等多方面数据，使安全防护难度大幅增加。分级保护是数据安全的先决条件，但目前汽车数据分类分级要求不统一，《车联网信息服务 数据安全技术要求》《车联网信息服务 用户个人信息保护要求》《自动驾驶数据安全白皮书》《汽车采集数据处理安全指南》等文件由于涉及的细分领域不一致，导致对汽车数据分类分级的方法也存在差异。

数据分类分级的具体细化要求不统一，在针对汽车数据敏感性实施差异性防护时，无法采用高度自动化技术进行精准防护，降低了防护效率。例如，汽车数据中包含大量非结构化数据，在没有明确数据分类分级情况下，无法对这部分数据进行自动化或半自动化防护，制约数据安全防护能力效率的提升。

（2）汽车数据处理权责划分不清晰，不利于从零部件源头

引入数据安全防护措施。汽车数据安全在供应链层面是乘法关系，不是加法关系，一旦有一个链条环节为零，最终的防护结果就是零，全方位保护汽车供应链的数据安全十分重要。强化“安全左移”防护理念，要在车辆硬件设计和制造阶段，就将数据安全防护技术预埋进去，以达到事半功倍的防护效果。

通常只有明确责任和义务后，企业才会更加重视数据安全合规工作。国标《信息安全技术 汽车数据处理安全要求》中只是规定了“由汽车制造商全面掌握其生产的整车所含各零部件收集、传输数据情况，对零部件供应商处理汽车数据的行为进行约束和监督”。但零部件供应商等参与主体，在车辆数据安全保护中应该承担什么角色、如何配合车企、如果数据出现安全问题，应该承担多大责任等具体问题尚无明确答案。光凭企业自制，可能较难引起零部件供应商的重视，不利于构建以零部件安全为基础的整车安全防护体系。

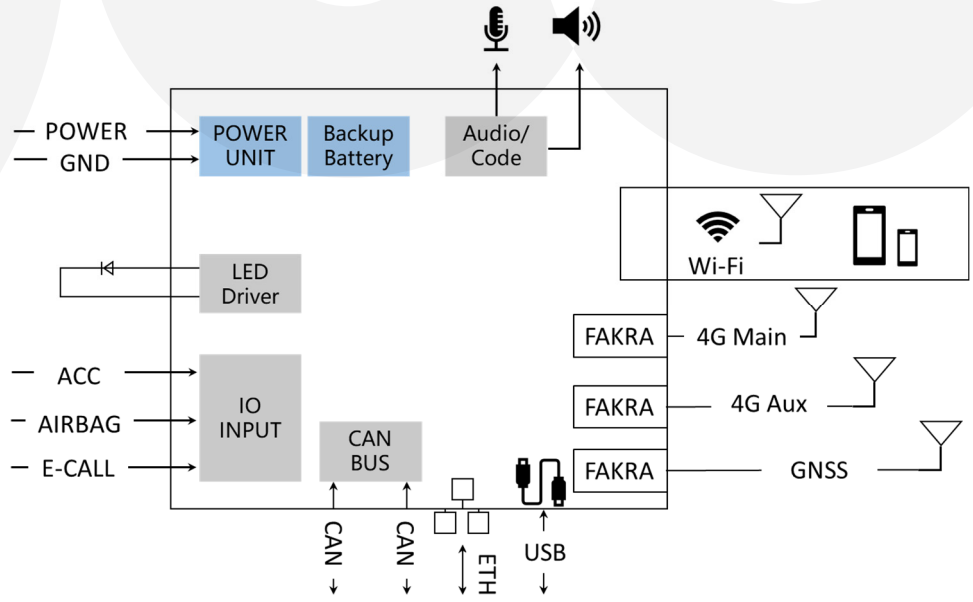
2、规范的安全技术标准体系不健全，在技术或产品构成上缺乏有效评判标准。

汽车数据需要关注全生命周期安全防护，当前还没有行业通用的数据安全防护技术标准和模型，导致企业落实数据安全时缺乏可操作性理论指导。工信部发布的《车联网网络安全和数据安全标准体系建设指南》中，数据安全技术标准仅包括密码应用、分类分级数据安全、重要数据记录系统、网约车服务四方面，缺乏汽车数据异常行为监测、数据传输、数据销毁等更多涉及汽车

数据安全领域的技术要求，导致企业在实际执行时存在困惑，一定程度上制约了汽车数据安全防护技术的迭代发展。

3、部分数据安全防护技术量产上车仍面临诸多难题。

（1）车端计算资源有限，无法支撑高规格数据加密技术。在构建智能网联汽车数据安全防护体系时，传统的防火墙、入侵检测等防护技术能直接迁移到汽车数据安全领域，但会受到车端算力的制约，要做轻量化处理。例如，T-BOX 是实现车载网络与车外网络交互的主要节点（见图表 3），某车企提出要把亚信安全的 IDS 安全产品引入 T-BOX 中，但仅预留 5%资源消耗给入侵检测，远不能满足产品的计算资源需求。如果增加车端硬件资源，会增加车端成本，但在有限的硬件资源下，实现安全能力的嵌入并能稳定运行，仍存在技术瓶颈。



图表 3 T-BOX 通信架构

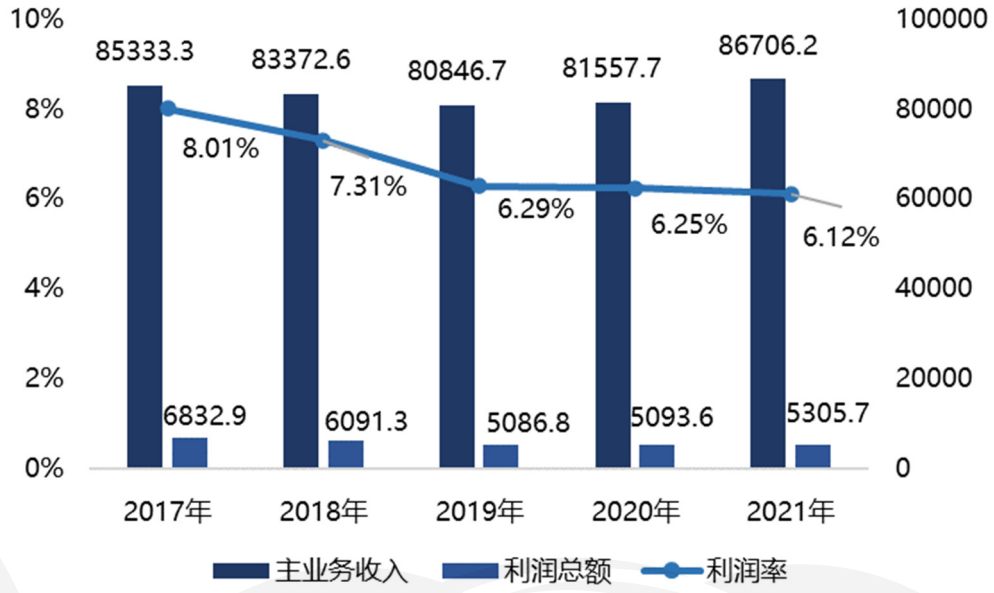
数据来源：中国互联网络信息中心，百人会车百智库研究院整理

（2）车端额外集成数据安全防护能力会拉高整车成本，一定程度上降低企业使用意愿。中国本土车企整体利润较低（见图表 4）。2021 年，我国车企平均利润率仅为 6.12%（见图表 5），新势力车企尚处于发展初期，离盈利还存在一定差距。数据显示，小鹏每卖一辆车就要亏损近 5 万元，而数据安全防护技术的引入会进一步拉高整车成本。例如，车辆主控制器芯片集成 HSM 硬件安全模块，可实现信息安全的集中管理，确保域控制器对所连接的 ECU 进行保护，但在集成安全启动、安全加密等功能后，单颗主控制器成本要增加 30-50 元。若要保障全车 ECU 的安全，需要在每个主控制器芯片上集成 HSM 模块，整车成本会大幅增加。据调研，一台车满足现阶段我国数据安全合规要求，所增加的成本最少 300 元。

车企	2021 年销售量（万辆）	2021 年净利润（亿元）	2021 年单车利润（元）
长城汽车	128.1	67.26	5251
吉利汽车	132.8	43.5	3276
通用汽车	600	638.69	10645
大众汽车集团	888	1069.07	12039
丰田汽车	1050	1593.76	15179

图表 4 自主品牌车企与国外车企利润差距

数据来源：汽车洋葱圈，百人会车百智库研究院整理



图表 5 我国近五年来规模汽车制造业利润情况

数据来源：国家统计局，百人会车百智库研究院整理

（3）车内通讯网络协议缺乏安全机制，加大了数据传输安全风险。CAN、车载以太网等车载网络协议缺乏安全设计，车内数据传输主要根据功能进行编码，按照报文 ID 进行标定和接收过滤，仅部分数据提供循环冗余校验，缺乏重要数据加密、访问认证等防护措施，导致车载网络容易受到嗅探、窃取、伪造以及篡改等攻击威胁，难以保障车载网络的安全性。

一方面，当前 CAN 总线缺乏必要的数据安全防护，主要体现在以下几个方面：缺乏加密和访问控制机制，汽车控制指令可被攻击者根据通信协议逆向分析，并用于攻击指令伪造；缺乏认证及消息校验机制，不能对攻击者伪造、篡改的异常消息进行识别和预警，加大物理侵入或远程侵入实施过程中的消息伪造、拒

绝服务及重放等攻击威胁；CAN 总线缺乏加密技术，广播的报文数据处于未加密状态，允许每个节点都能够捕捉 CAN 网络报文，任意节点被攻破就可能造成报文数据泄露。

另一方面，车载以太网架构本身安全系数不够高，存在加密、认证、重放、拒绝服务等安全性漏洞。其采用的实时通信协议缺乏时间戳和加密操作，容易受到拒绝服务攻击、数据篡改和中间人攻击等，会导致车辆网络带宽或者系统资源消耗过大，使网络或者系统不堪负荷，有车载通信网络瘫痪的风险。同时，缺乏数据可靠性和完整性校验，易造成重放攻击和拒绝服务攻击，导致车辆收到错误信息，影响驾驶员行车安全。

（4）车外通信安全防护机制不完善降低通信可信度。汽车对外通信过程中，网络拓扑结构会随车速频繁变化，通讯节点出现或消失随机性强，使数据吞吐量快速变化，导致数据传输信道堵塞，从而引发涉及安全的消息传输失败。例如，目前基于 GPRS 技术的安全消息广播技术的链路稳定性差，尤其无法保证较远距离且高速移动节点的链接可靠性。此外，在通讯节点不断变化的过程中，很容易被可疑车辆伪造通讯节点，篡改信道中的信息，降低通讯可信度，降低车辆安全。

车载 APP 缺乏针对性检测工具。车载 APP 已不仅聚焦车辆本身，而是集成控车、服务、社交等功能，成为厂家与用户间的高效沟通渠道。但当前车载 APP 安全防护不到位，会导致车主用户信息、车机系统日志等数据泄露风险，甚至会造成车辆运行

相关数据遭到篡改或者窃取。例如，腾讯科恩实验室通过远程登录到特斯拉车端 APP，不仅能够截取用户账户密码，还能够远程解锁车辆。目前市场上 APP 检测工具主要针对手机端，车机端 APP 监测缺乏高效或真正有用的工具。

（5）区块链、隐私计算等创新技术上车还需进行针对性的优化、适配。目前，车端无法支持全栈区块链技术的运行。以安全多方计算技术为例，其计算过程相对明文计算增加了电路转换、加密解密等过程，需要消耗额外的计算资源，目前最前沿的安全多方计算框架计算 64 位整数的两个 10 万元素向量内积时间在 10-2 至 10-1 秒级浮动，当前车端算力远不能满足需求。未来，还需进一步探索区块链、隐私计算等新一代信息技术在车端的应用的场景与路径。

4、汽车产业链各方主体防护意识明显不足，制约汽车数据安全防护的生态体系建立。

（1）企业多采用单点防护的方式，防护力度不足。目前很多车企在 T-BOX、车载信息系统交互、网关以及芯片硬加密/软加密方面做了很多工作。但整车企业、零部件供应商等更多是采用单一或单点的软件、硬件技术和产品进行安全防护，安全防护产品也“五花八门”，缺乏系统化构筑安全体系思维，既影响汽车产业链各方主体共同构建统一的数据安全防护生态体系，也很难有效应对智能网联汽车面临的车机 APP 和云端服务器漏洞、远程通信接口漏洞、车载网络指令被篡改等众多安全风险。

（2）中小型零部件供应商对数据安全重视程度不足，制约数据安全防护责任传递。汽车数据安全的责任主体为整车企业，从整车企业对数据安全的投入看，70%以上主机厂都自建了数据安全团队，配备了足够的安全人员，并在安全体系和防护产品方面建立起相关规范和要求。反观零部件供应商，除头部供应商十分重视数据安全防护，绝大多数中小型零部件企业在网络安全和数据安全管理机制方面还仍然有欠缺，甚至还没有配备齐数据安全团队。建设数据安全防护生态仅靠整车企业推动是不够的，还需提高整个行业的安全意识和水平。

例如，欧洲已经开始推进 ePrivacyseal 认证，以实现网络安全和数据安全责任向上游的传递。但国内很多零部件供应商在网络安全和数据安全管理机制方面仍有欠缺。除头部企业以外的绝大多数中小型零部件企业还未配备网络与数据安全团队。如何把数据安全责任向供应链上游传递是现在面临的最大问题。

5、智能零部件主要由外资供应商把控，掣肘企业建设数据安全防护体系。

目前智能网联汽车很多功能组件如 AEB、ABS 等，主要由外资 Tier 1 供应商整体打包提供，功能系统内部细节车企无法掌控。我国还未解决有和无的问题，更高的数据安全要求也无从谈起，这极大制约我国车企构建数据安全防护体系。

例如，Tier 3、Tier 4 层面有超过 95%的芯片依赖进口，且芯片底层代码掌握在国外芯片企业手中，国内零部件供应商很难鉴

别国外芯片底层代码是否留有安全后门，无法确保系统的安全性。

三、推动汽车数据安全防护技术创新发展的建议

1、创新管理措施，动态解决汽车数据安全面临的共性突出问题。

智能网联汽车产业的创新特点，决定了不可能用一两个法规解决所有问题。需要针对分类分级、数据确权、跨境传输等共性问题，逐个形成解决办法，且持续动态调整，才能更好满足企业在创新中遇到的政策和法规突破需求。

（1）分类分级保护是保障数据安全的先决条件，要尽快形成统一、细化的汽车数据分类分级意见，明确区分哪些是财产数据、哪些是隐私数据、哪些是经营类数据，针对不同类型、不同级别的数据，采取差异化的安全防护措施。

（2）现阶段还很难完全解决数据确权问题，建议可以进行模糊化处理，优先出台一份相对宽泛的汽车数据确权管理规范，再动态更新。既能填补管理空缺，给予企业指导，也能为企业创新保留一定空间。例如，在部分问题上可以做有期限的豁免。

（3）基于“急用先行”原则，推进汽车安全防护技术标准的制定。优先推动诸如数据脱敏、数据共享等与现阶段产业发展高度相关标准的制定，逐步建立起覆盖数据处理全生命周期、覆盖多类具体场景的技术标准体系，促进更多汽车智能化功能安全

可控的上车应用。

（4）充分发挥试行沙盒监管制度优势，为汽车数据合规下的技术发展提供可行路径。在数字贸易实验区、数字经济特区，充分发挥沙盒监管制度提供的试点机制，营造开放、包容环境，为智能网联汽车数据处理合规发展，提供技术创新的训练场。鼓励企业在监管沙盒内探索脱敏计算、隐私计算、区块链等安全技术在车端的应用，逐步攻克算力不足、数据接口不统一、软硬件配套不完善等诸多技术难点，推动技术创新发展。

2、加强公共服务平台建设。

（1）建立可信的汽车安全风险/漏洞信息发布平台。借鉴美国汽车制造商联盟和全球汽车制造商协会牵头成立的信息分享和共享中心经验，我国行业机构可以联合本土汽车生态企业建立共享平台，以汇集实践中遇到的安全风险和漏洞信息，如主流芯片或操作系统的漏洞平台等。鼓励企业进行漏洞共享与上报，引导“白帽”黑客对车企产品漏洞挖掘与报送。该漏洞平台能将多方实践的安全漏洞信息汇聚在一起，使企业能时刻了解最新的汽车漏洞信息并及时进行系统更新和技术迭代，全面提升汽车数据安全防护能力。

（2）建立省级、国家级数据安全监测平台。加强安全检测评估技术产学研用，变被动监测为主动监测，实时、动态、持续地监测汽车数据合规情况，提高监测时效性和全面性。通过车联网安全检测评估试点示范，加强相关技术手段和产品服务的产业

应用。建议根据汽车制造商、零部件和软件供应商、出行服务企业等不同责任主体，划分数据安全合规责任边界，把数据的保管责任从车企中解放出来。明确整车企业和零部件供应商不同的责任后，应进行明显标识以作为处理事故追责的凭证。

3、加快推进创新的数据安全防护技术上车。

（1）加强智能网联汽车核心部件的安全能力认证。为更好保障汽车数据安全，应针对操作系统、SoC 芯片、计算芯片等核心软硬零部件，建立信息安全能力认证体系。通过权威第三方检测机构的信息安全检测和认证，满足访问控制完整性检验、加密保护的安全技术要求，才可上车应用。从车辆底层技术入手，防止后门事件发生。

（2）推进国密算法在智能网联汽车上的应用。我国自主品牌车型仍有大量外资供应商提供的零部件，导致国密算法在车端上的应用较少。应通过试点示范，推动设备制造商接口协议和密码算法接口的统一，提倡我国自主品牌分阶段试用国密算法，重视国密在智能网联汽车上的应用。

（3）规范数据脱敏技术认证，推动其上车应用。哨兵模式、远程拍照、车内预警等汽车智能化功能，由于涉及人脸、车牌等个人隐私数据安全，被迫下架。目前，汽车脱敏技术已能达到上车标准，还需通过试点探索不同场景下车端应用数据脱敏技术的效果，攻克对硬件资源的消耗、可能加大通信延迟等痛点问题，形成标准的技术认证体系，推动脱敏技术实现量产上车。

（4）持续探索区块链、隐私计算等创新技术在汽车数据安全防护中的应用价值。“可用不可见”有助于实现数据隐私保护和价值挖掘的双重效果，但由于算力和成本等因素，区块链、隐私计算等技术在车端的应用相对较少。不应只聚焦于车端，建议围绕智能网联汽车涉及的不同技术、不同场景，多方试点、探索区块链、隐私计算等技术的创新应用。

以区块链技术为例，可以利用该技术建立包括企业自评估、跨境信息备案，以及主管部门安全审查和第三方安全评估等关键环节在内的智能网联汽车数据跨境管理平台，形成安全且标准化的数据跨境传输备案与审核。

4、引导推进各主体间的合作。

（1）建立汽车数据安全责任共担机制，强化数据处理主体的“自我规制”观念。构建数据安全防护生态体系，仅依靠车企从整车层面落实防护措施，成效非常有限，需要零部件供应商积极参与，将安全责任落实到全产业链各个环节。可参考云平台责任共担模型，由机构统筹，建立统一的数据安全防护观念，安全责任由汽车产业链上下游企业共担，使企业形成自律防护意识。

（2）引导生态企业共同突破关键技术难题。汽车数据安全技术发展，仅靠车企或安全服务商一家都难以实现，需要联合生态企业，在反复测试、应用的过程中不断迭代。可依托行业机构的协调作用，拉通整车制造、软硬零部件、安全技术等细分领域，构建起车企、零部件厂商、安全服务商之间的合作机制，共同突

破数据安全技术上车面临的技术难题。过程中，车企要发挥“链主”的带动作用，加强汽车产业链上下游企业与安全专家、安全服务商交流合作，通过建立反哺机制，加强数据安全防护技术的横向集成，探索安全防护技术在不同场景下的应用。

车百智库研究院“智能网联汽车数据安全监管体系与政策体系”课题组

课题负责人：张永伟

课题协调人：梁嘉琪

报 告 执 笔：梁嘉琪、贾浩、王晓飞

车百智库是中国电动汽车百人会联合权威机构、产业链头部企业共同发起成立的专业研究机构，主要围绕汽车电动化、智能化、网联化、绿色化以及能源变革、交通变革、城市变革等多个方向开展研究。

地址：北京市海淀区建材城中路 27 号金隅智造工场 N5 楼

电话：+86 010 82158701

网址：www.ev100plus.com