

智能网联汽车数据安全 合规建设与测评实践

文 / 王荣

智能网联汽车数据安全合规体系建设主要包括组织架构、流程制度以及技术保障。首先，建立分层级的组织架构；其次，建立数据安全流程制度；最后，采用防护技术和安全检测工具平台，实现基于数据全生命周期的安全技术保障。

在智能汽车中，信息安全已经成为其开发过程中不可或缺的关键要素。不断增加的车内系统复杂性和相关信息安全漏洞，将成为汽车产业共同面对的问题。

汽车数据安全标准法规

2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过并发布了《中华人民共和国数据安全法》。随着《中华人民共和国数据安全法》的出台，工业和信息化部、中央网信办等主管机构关于智能网联汽车数

据安全的政策相继发布。2021年7月30日，工业和信息化部发布《关于加强智能网联汽车生产企业及产品准入管理的意见》（以下简称《准入意见》），其中要求企业要强化数据安全能力，建立健全汽车数据安全管理制度，依法履行数据安全保护义务，明确责任部门和负责人。实施数据分类分级管理，加强个人信息与重要数据保护。建设数据安全保护技术措施，确保数据持续处于有效保护和合法利用的状态，依法依规落实数据安全风险评估、数据安全事件报告等要求。

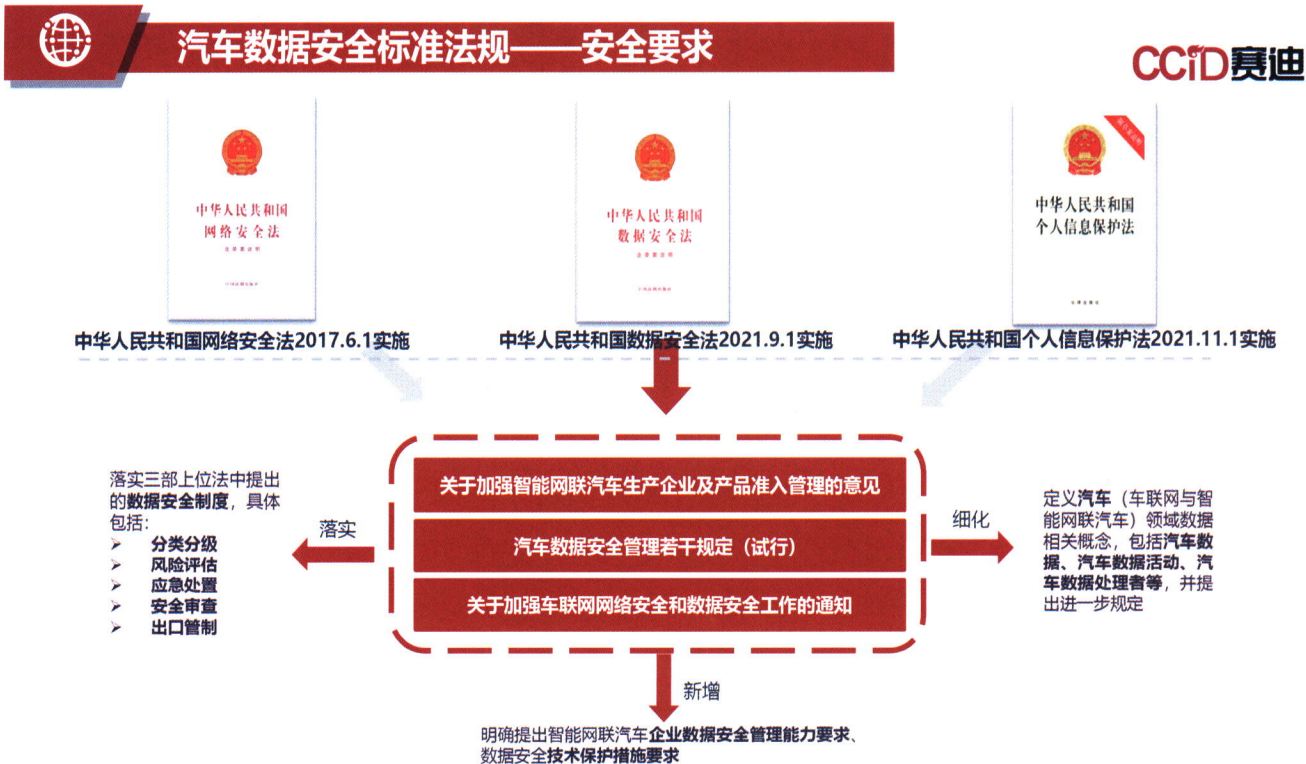
2021年8月-11月，中央网信办联合工业和信息化部、公安部

等多部门相继出台《汽车数据安全若干管理规定》《数据出境安全评估办法（征求意见稿）》和《网络数据安全管理条例》。

2022年7月，《数据安全出境评估办法》正式发布。同年10月，工业和信息化部发布《道路机动车生产准入许可管理条例（征求意见稿）》。

此外，在《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》三部上位法的基础上，工业和信息化部出台的《关于加强智能网联汽车生产企业及生产准入管理的意见》《汽车数据安全若干规定》（试行）中要求，落实上位法中提出的数

王荣 中国软件评测中心-智能网联汽车测评工程技术中心测评部副总经理



据安全制度，包括数据分类分级、风险评估、应急处置等；细化车联网与智能网联汽车领域相关概念，包括汽车数据、汽车数据活动、汽车数据处理等；新增对智能网联汽车企业数据安全能力要求、数据安全技术保护措施要求。

2020 年 12 月 17 日，工业和信息化部印发《电信和互联网行业数据安全标准体系建设指南》，指出，在基础共性标准、关键技术标准、安全管理标准的基础上，结合新一代信息通信技术发展情况，重点在 5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等重点领域进行布局，并结合发展情况，逐步覆盖其他重点领域。其中车联

网方向主要在车联网云平台、V2X 通信、智能网联汽车、车联网移动 APP 四个方面开展制定相关数据安全标准。

目前在标准方面，国家标准、行业标准、团体标准，都已在智能网联汽车数据安全方面开展深入研究及标准编制工作。其中，在国标出口汽标委、信安标委发布立项的《GB 整车信息安全技术要求及体验方法》《汽车采集数据处理安全指南》中，对汽车数据在采集、使用、传输、存储销毁等方面提出具体安全要求。

汽车数据安全合规建设

标准法规为企业的数据安全合

规建设提供顶层思路 and 依据。

2021 年 7 月 30 日，工业和信息化部发布的《关于加强智能网联汽车生产企业及产品准入管理的意见》提出，企业应当建立数据资产管理台账，实施数据分类分级管理，加强个人信息与重要数据保护，建设数据安全保护技术措施，确保数据持续处于有效保护和合法利用的状态。

因此，总的来说智能网联汽车的合规体系建设主要包括三个方面，组织架构、流程制度以及技术保障。首先，建立分层级的组织架构、明确各层级的人员角色与分工。其次，建立数据安全流程制度作为根本遵循，将数据安全制度体系融入现有研发流程，以分类分级

管理为基础，覆盖公司产品典型的业务场景。最后，采用防护技术和安全检测监测等工具平台实现基于数据全生命周期的安全技术保障。

在组织架构与流程制度的建立过程中，首先要设计“自顶向下”的安全组织，实现决策 - 管理 - 执行 - 监督闭环架构，对组织架构的建设划分层级，包括架构建立、职责分配和沟通协作。在各层级中，包括组成部门或者人员（角色）、各层级的工作职责、层级间的协调配合关系；其次制定对应流程制度，用于管理体系建设和执行，并根据合规要求及内部执行情况持续更新。其中，主要分为四级文件，一级方针政策中包括《数据安全总则》，二级管理规定中包括《账号与权限管理办法》《数据脱敏管理办法》，三级操作手册中包括《账号与权限分配操作指南》《数据脱敏规范》，四级各类表单、工单、记录中包括《访问控制记录清单》《脱敏操作日志工作模板》。

值得注意的是，数据分类是指通过具有某种共同属性或特征的数据归并其类别的属性或特征来对数据进行区别。自动驾驶领域可以结合不同的应用场景，对数据进一步分类。数据分级是指按照数据的价值、内容敏感程度、影响和分发范围不同对数据安全等级进行划分，为数据管控提供支撑。依据数据安全法以及行标 YD/T 3751 和 YD/T3746，对汽车数据分类分级提出如下参考，主机厂和其他相关厂商

可以基于本参考并结合自身实际进行进一步细分。

在技术保障层面，实现数据采集、存储、传输、使用、出境以及销毁的全生命周期安全防护需要应用安全存储、数据加解密、数据脱敏、数字签名、权限控制、通信加密、完整性校验、证书管理等技术手段。同时，在运维阶段实现数据安全的应急响应，通过应急预案制定、在线监测运营、检测响应、应急保障及评估上报进行闭环管理。建设完整的数据安全保护技术措施，确保数据持续处于有效保护和合法利用的状态。

中国软件评测中心在数据安全合规建设实践中，参照智能网联汽车企业产品开发全生命周期 V 模型，将数据安全和个人隐私保护融入到产品的各个环节。从设计开发阶段，就开始识别数据安全合规风险。在产品安全需求设计阶段，对产品进行数据安全风险评估分析，协助完成需求评审。在产品安全设计与开发阶段提供安全功能设计与规范制定并与产品网络安全需求整合，协助组件开发（软件、硬件），满足合规需求。根据安全合规需求，支撑客户数据隐私安全与合规团队及测试团队进行安全测试验证，并在运维阶段持续安全风险监测、漏洞发掘、安全运营以及进行安全合规评估与事件上报，通过提供专业的第三方咨询 + 认证 + 测试 + 工具，帮助企业实现最大程度的合规能力建设。

汽车数据安全测名实践

作为工业和信息化部唯一授权的“智能网联汽车软件检测中心”，国内首批获得 CMA 检验检测机构、CNAS 检测机构、CNAS 实验室认可的专业第三方质量保障机构，中国软件评测中心智能网联汽车测评工程技术中心未来将积极响应“十四五”规划，围绕电动化、智能化、网联化的发展趋势，以计算平台为抓手构建智能网联汽车“车 - 路 - 云 - 网 - 图”一体化生态，践行“为车联网行业做出技术贡献，让自动驾驶汽车安全行驶”的使命。

针对智能网联汽车安全防护情况，中国软件评测中心从 2020 年开始连续三年在全国范围内开展智能网联汽车渗透测试实践活动，并在 2020 年、2021 年、2022 年的世界智能网联汽车大会上隆重发布，受到行业内广泛关注。

在渗透测试活动中，中国软件评测中心提出了渗透测试指标体系，并针对数据安全和个人信息保护设计测试用例。一方面，依据出台的数据安全法和个人信息保护法，以及《准入意见》针对数据安全和个人信息安全方面的要求；另一方面，从安全技术方面检查是否存在非授权访问车辆数据、个人信息、敏感数据和关键数据存储是否安全等。

责任编辑：赵子旺
zhaoziwang@ccidmedia.com