关于智能网联汽车数据安全治理框架的探究

宋　琦[1]，武　波[2]，刘永东[1]
（1. 国家工业信息安全发展研究中心，北京　100040；2. 北京理工大学　网络信息技术中心，北京　100081）

摘　要：随着智能网联汽车市场快速发展，智能网联汽车数据量增长迅猛，数据交换愈加频繁。高价值和高敏感特性，使得如何保证数据安全成为智能网联汽车行业监管部门和车辆生产企业共同关注的重点。目前，针对智能网联汽车数据安全治理并没有统一的实践标准，基于智能网联汽车数据安全合规要求，从数据安全控制角度出发，对智能网联汽车数据安全治理框架进行初步探索，以数据分类分级为基础，以数据生命周期安全管理为主线，构筑包括数据安全管理、数据安全技术、数据安全运营和数据处理场景安全管理在内的整体数据安全治理框架，为智能网联汽车数据安全提供一种体系化治理路径。

关键词：智能网联汽车；数据安全合规；数据治理；参考框架
中图分类号：TP391　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.03.001
引用格式：宋琦，武波，刘永东. 关于智能网联汽车数据安全治理框架的探究［J］. 网络安全与数据治理，2024，43(3)：1-9.

Research on data security governance framework of intelligent connected vehicles

Song Qi，Wu Bo，Liu Yongdong
（1. China Industrial Control Systems Cyber Emergency Response Team，Beijing 100040，China；
2. Network Information Technology Center，Beijing Institute of Technology，Beijing 100081，China）

Abstract：With the rapid development of the intelligent connected vehicle market，the data volume of intelligent connected vehicles is growing rapidly，and data exchange is becoming more frequent. The high value and high sensitivity characteristics make how to ensure data security become a key concern for both regulatory authorities and vehicle manufacturers in intelligent connected vehicle industry. At present，there is no unified practice standard for the data security governance of intelligent connected vehicles. Based on the compliance requirements for data security in intelligent connected vehicles and from the perspective of data security bottom line control，this paper makes a preliminary exploration on the data security governance framework of intelligent connected vehicles. Taking data classification and grading as the basis and data life cycle security management as the main line，this work builds an overall data security governance frameworkthat includes data security management，data security technology，data security operation and data processing scenario security management. This provides a systematic governance path for data security of intelligent connected vehicles.

Key words：intelligent connected vehicles；data security compliance；data governance；reference frame

0　引言

随着人工智能、车联网、智能汽车等新兴信息技术和交通工具不断发展，智能网联汽车从概念设计进入现实应用阶段，研发及商业化进程不断提速，将为交通运输领域转型升级带来重大变革。其中，各类智能终端以及数字场景的应用交互，产生海量“车、路、云、网、图”数据，面临多重数据安全风险[1]。数据安全治理是支撑智能网联汽车系统安全运行的基石，也是保障智能网联汽车产业健康发展的关键。为更好地开展智能网联汽车数据安全管理与保护，本文拟对智能网联汽车数据安全治理体系进行探讨。

1　智能网联汽车数据安全风险挑战

根据工信部统计显示[2]，2022 年我国搭载辅助自动驾驶系统的智能网联乘用车市场渗透率提升至 34.9%，至 2025 年仅乘用车部分新增产值将预计超 1 万亿元。与此同时，为有效降低驾驶失误、提高交通效率，智能汽

车集成大量感知、通信、控制等智能终端，使得相关数据应用规模呈爆发式增长。作为数字时代的关键生产要素，数据信息的有效利用对行业提质发展和个性化服务发挥重要作用。然而，数据安全因素不断跃入行业视野，智能网联汽车数据安全风险日益严峻，已成为监管部门和生产企业的关注焦点。

从数据生命周期来看，智能网联汽车数据面临多重安全风险叠加[3]。数据采集过程中，自动驾驶所需的核心高精地图技术，使得未授权违规采集、处理、销毁用户信息风险激增；数据传输过程中，“车、路、云、网、图”数据交互渠道增多，增加了数据在通信链路传输中被截获、篡改、破坏、伪造的风险，涉及合资汽车厂商的数据跨境流动也增加了数据恶意泄露威胁；数据存储中，车、云数据类型识别和分类分级存储在实践中仍缺乏统一规范，数据分级存储评估和责任界定复杂，国家重要公共安全数据泄露风险影响较大；数据处理过程中，人脸、车牌、隧道和桥梁属性等特殊敏感数据排查缺乏完善审计机制，潜在泄露隐患较多；数据交换过程中，智能网联汽车数据的多源异构特性，导致数据协同与共享漏洞难，系统脆弱性带来一系列安全风险；数据销毁中，过程缺乏监管，销毁不彻底、虚假销毁、恶意恢复等数据泄露风险难以觉察。面对复杂的安全风险挑战，智能网联汽车数据安全治理能力亟待提升。

2　智能网联汽车数据安全治理需求

2.1　智能网联汽车数据安全治理概述

数据安全治理是数据治理体系中的重要内容，是以确保数据“可用性、完整性和保密性”目标宗旨，依托顶层数据安全战略，由治理范围内外相关方在组织、制度、技术等方面协作实施的治理活动集合。这一个概念最早由国际 IT 调研与咨询服务公司高德纳（Gartner）倡导提出：“数据安全治理不仅是一套工具组合的产品级解决方案，也是一个从决策层到技术层，从管理制度到技术工具，自上而下贯穿整个组织架构的完整支撑链条”[4]。总体来说，数据安全治理旨在促进数据安全保护，从数据业务出发，基于数据全生命周期建立以数据为中心的安全架构体系，实现数据资产价值、业务效益、企业安全的最优化。

智能网联汽车数据安全治理是数据安全治理在智能网联汽车行业的扩展应用[5-6]，其治理对象包括智能网联汽车技术运用和行业发展过程中所采集、生产、使用及销毁的数据，涵盖数据类别包括个人、车辆、道路等交通信息，涉及的主要业务流程包括个人信息隐私保护、数据跨境流动监管、网络信息安全管理等，体现于数据采集、传输、存储、处理、使用、共享、销毁生命周期各个阶段。

2.2　智能网联汽车数据安全合规要求

近年来，全球各主要国家相继出台数据安全法律规章[6]，智能网联汽车数据应用与保护要求逐步完善。我国高度重视智能网联汽车数据安全制度建设，已在数据安全及其智能网联汽车细分领域发布多项国家法规和行业标准（如表 1 所示）。其中，《网络安全法》《数据安全法》和《个人信息保护法》分别从系统、数据本身以及个人信息层面提供了智能网联汽车数据安全保护总体原则与法律规定。《汽车数据安全管理若干规定（试行）》《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网网络安全和数据安全工作的通知》等部门规章和指导文件逐步推动智能网联汽车行业法律设计落地。《车联网信息服务用户个人信息保护要求》《信息安全技术汽车数据处理安全要求》等标准不断布局，加强对智能网联汽车数据安全管理实践的引导和规范。

通过对当前法律规范文件分析，目前我国智能网联汽车数据安全治理主要面临如下合规要求：

一是符合数据安全治理基本原则。日益完善的法规框架为智能网联汽车数据安全治理提供了总体原则目标。例如《网络安全法》提出了“维护网络数据的完整性、保密性和可用性”的数据安全治理总目标；《数据安全法》确定了保障数据安全与促进数据开发利用并重的数据安全治理思路；《个人信息保护法》明确了“最小必要、知情同意”的个人信息处理合规原则，划定了个人信息不得“随意收集、违法获取、过度使用、非法买卖”前提；《汽车数据安全管理若干规定（试行）》框定了汽车数据范围，规定了“车内处理、默认不收集、精度范围适用、脱敏处理”数据利用原则，并明确重要数据分类。

二是覆盖数据安全合规基本要素。我国法律法规及标准指南要求指出，智能网联汽车的数据安全治理要打造以数据分类分级为核心的数据安全制度，构建汽车数据安全管理体系，实施全生命周期数据安全保护，建立合理的数据安全风险评估、报告、信息共享、监测预警及应急处置机制，同时也规定了各要素建设的相关支持活动。对智能网联汽车数据处理活动主体而言，其数据安全治理框架必须相应涵盖数据分类分级、数据全生命周期保护、数据安全评估、数据安全监测应急、数据安全监督等基本要素及其支持活动，进而从组织、管理、技术等方面进行配套建设，形成有机融合的综合性数据安全治理体系。

表 1　智能网联汽车数据安全制度

类别	名称	日期
法律	《中华人民共和国网络安全法》	2017 年 6 月 1 日生效
	《中华人民共和国数据安全法》	2021 年 9 月 1 日生效
	《中华人民共和国个人信息保护法》	2021 年 11 月 1 日生效
部门规章	《交通运输政务数据共享管理办法》	2021 年 4 月 15 日生效
	《关于加强智能网联汽车生产企业及产品准入管理的意见》	2021 年 8 月 12 日发布
	《关于加强车联网网络安全和数据安全工作的通知》	2021 年 9 月 16 日发布
	《数据出境安全评估办法》	2022 年 9 月 1 日生效
	《汽车数据安全管理若干规定（试行）》	2021 年 10 月 1 日生效
国家标准	GB/T 35273—2020《信息安全技术 个人信息安全规范》	2020 年 10 月 1 日发布
	TC260—001《汽车采集数据处理安全指南》	2021 年 10 月 8 日发布
	GB/T 40855—2021《电动汽车远程服务与管理系统信息安全技术要求及试验方法》	2021 年 10 月 11 日发布
	GB/T 40856—2021《车载信息交互系统信息安全技术要求及试验方法》	2021 年 10 月 11 日发布
	GB/T 40857—2021《汽车网关信息安全技术要求及试验方法》	2021 年 10 月 11 日发布
	GB/T 40861—2021《汽车信息安全通用技术要求》	2021 年 10 月 11 日发布
	GB/T 41871—2022《信息安全技术 汽车数据处理安全要求》	2022 年 10 月 12 日发布
行业标准	YD/T 3746—2020《车联网信息服务 用户个人信息保护要求》	2020 年 10 月 1 日生效
	YD/T 3751—2020《车联网信息服务 数据安全技术要求》	2020 年 10 月 1 日生效
	YD/T 3752—2020《车联网信息服务 平台安全防护技术要求》	2020 年 10 月 1 日生效
	GB/T 41871—2022《信息安全技术 汽车数据处理安全要求》	2023 年 5 月 1 日生效
	T/TMAC 057—2023《智能网联汽车数据通用要求》	2023 年 5 月 19 日发布

三是满足数据安全合规具体规则。我国法律法规及标准指南针对部分智能网联汽车数据安全合规要素给出了遵循的具体规则和标准，包括数据分类分级和保护、数据全生命周期处理、敏感数据发现、隐私保护、用户个人信息主体权利保护、数据跨境传输、数据披露等，相关的技术细则、责任划分、授权与使用所需满足的要求和标准不断细化。智能网联汽车数据安全治理框架，必须对以上要素综合平衡考量，同时在规划组织、设计开发、实施交付、运行维护中同步推进，为保障组织、管理、技术、运营、监督评价等基本要素合规，提供相应的工具支撑。

2.3　智能网联汽车数据安全合规监管重点

2.3.1　数据分类分级监管

数据分类分级是实现智能网联汽车数据安全有效治理的核心基础，也是数据安全合规监管的重点[7]。

（1）数据分类

依据现有行业规范要求，智能网联汽车的重点数据主要包括个人信息、车辆数据和环境信息。个人信息主要包括个人车内活动数据，如乘车人基本信息、生物识别信息，图像与语音数据，驾驶行为数据（如驾驶速度、加速度和刹车数据，用户与座舱交互数据，人类驾驶员操作数据等）。其中，生物识别信息和位置轨迹信息与个人主体生活习惯及生理状态强相关，在处理和使用中应当严格遵守个人信息保护最小必要和知情同意原则。车辆数据包括车辆基础属性数据、车辆运行工况数据、车联网移动终端应用软件系统数据（如远程监测数据、预测规划数据、决策数据、驾驶辅助系统状态数据等）。车辆数据是否涉及重要数据应根据数据状态（静态、动态）及其与个人的关联度、与车辆驾驶功能展开的关联度来判断。环境信息是智能网联汽车实现安全自动驾驶的基础，包括交通数据、地图数据、周边环境感知数据等。其中，地图数据的采集、测绘、处理、管理，交通数据中个人信息的采集处理均涉及公共安全，属于应重点监管的数据类型。

（2）数据分级

根据已发布法规及标准中有关重要数据、敏感信息等概念定义，需要在数据分类的基础上进一步确定智能网联汽车数据的重要等级。数据分级可根据数据安全事件对国家、社会、组织、个人造成的影响程度划分，如一般级、敏感级、重要级和核心级等。一般数据指主体

之间信息交互使用时能从公开渠道获取的一般性信息。敏感数据指该信息经非授权操作后对个人隐私、企业利益等主体造成严重损害的数据。重要数据指一类对车辆安全驾驶、人身安全、企业经济效益等造成重大损害的数据。核心数据指关系到国家和社会安全稳定的数据。数据分级还可以根据不同主体类型（如车辆、个人、企业等）进行细分。同时，同类数据量的累积或场景的变化，不同类数据的组合、汇聚等，均可能造成数据级别变动，因此数据分级需根据实际情况进行动态调整。

2.3.2 数据生命周期安全监管

数据安全法律法规文件明确指出，企业应在数据生命周期内建立并尽可能系统化实施适当的控制流程，因此落实全生命周期数据合规监管是数据安全治理的重要基础，在加强监管的同时考虑减少其对业务效率的影响[8]。

（1）数据采集。智能网联汽车数据采集主要涉及用户信息、生物识别特征、环境信息等敏感数据采集，典型安全合规要求包括：遵循“知情同意”“最小必要”“目的限定”原则；已制定数据分类分级安全合规要求并在数据采集中严格遵守等。

（2）数据传输。智能网联汽车数据传输主要涉及车内传输和车外传输，典型安全合规要求包括：传输数据遵循“最小必要”原则；获得用户单独同意；进行必要脱敏、加密；进行传输信道技术保护；执行数据访问管控等。

（3）数据存储。智能网联汽车数据主要存储在汽车和车联网服务平台上，典型安全合规要求包括：仅存储必要数据；满足事故风险排查及事故数据还原要求；进行存储数据加密或脱敏；进行数据防篡改及删除等安全控制配置；合理配置存储期限等。

（4）数据使用。智能网联汽车数据使用包括对数据的统计、计算、应用等操作，面临多维场景的复杂环境，典型安全合规要求包括：依据数据分类分级进行数据使用授权和验证；进行数据去标识、匿名化、加密等脱敏处理；进行数据使用行为审计等。

（5）数据共享。智能网联汽车数据共享包括车辆与用户、其他车辆、交通基础设施之间的数据共享，典型安全合规要求包括：进行充分有效的数据共享评估，包括可行性评估、安全能力评估、风险评估等；制定数据共享风险控制措施；接收方承诺数据保护义务等。

（6）数据销毁。智能网联汽车数据销毁是数据生命周期的“最后一公里”，往往也是最易忽视数据安全风险的环节，典型安全合规要求包括：建立数据销毁策略和审批机制；确保应销毁数据及其相关副本、文件、数据库所在存储空间完全清除并释放；采用禁止销毁数据恢复技术保护手段等。

2.3.3 数据跨境安全监管

汽车行业具有全球性产业链特征，数据跨境流动一方面可以推动创新和经济增长[9]，另一方面也带来较大数据安全隐患。智能网联汽车数据跨境安全风险主要包括两方面：一是重要数据、敏感信息非法传输至境外。其中用户信息、车辆状态及行驶路径等可泄露国家敏感地区位置信息，影响国家安全。二是重要数据、敏感信息存储至境外平台被非法共享、利用和分析，损坏国家利益。我国合资车企数量众多，车联网数据境内外平台的互联、传输与共享需重点关注。对智能网联汽车数据进行跨境安全监管，需要严格判断用户、车辆、环境等相关数据的分类分级状态，做好重要数据与敏感信息存储、传输及共享方式监督，按有关规定对确需向境外提供的数据实施出境安全评估，明确跨境传输数据的目的、范围、方式、种类，采取技术措施实时监控数据出境状态等。

3 智能网联汽车数据安全治理框架

3.1 数据安全治理体系

依据上述智能网联汽车数据安全合规要求和监管重点，本文构建智能网联汽车数据安全治理框架的思路为：从数据安全战略出发，聚焦数据安全合规，以数据分类分级为基础，以数据生命周期安全管理为主线，构建数据安全管理体系、技术体系、运营体系，形成以愿景战略为中心，以管理体系为保障，以运营体系为驱动，以技术体系为支撑的有机融合数据安全治理框架（如图 1 所示），主要包括以下部分：数据安全战略、组织架构、数据分类分级、数据全生命周期安全管理体系、数据安全运营体系、数据安全技术体系、数据处理场景安全管理体系、基础环境等。

3.2 数据安全战略

数据安全战略是实施数据安全治理工作的总体要求，指导整个数据安全治理体系建设。智能网联汽车数据安全战略主要从数据安全顶层规划方面提出要求，设定智能网联汽车数据安全治理愿景、目标、领域、指导原则等，为健全数据安全治理体系锚定发展方向，提供统一指引。制定智能网联汽车数据安全战略首先要在全面贯彻国家数据安全战略，平衡安全合规约束与业务发展风险的基础上，明确数据安全治理目标、原则、对象与场景，梳理所需遵守的相关法律、法规及标准。同时，可对智能网联汽车数据安全重点领域及关键场景制定数据安全治理子目标，如数据跨境、个人隐私保护等，阐明实现目标的治理规划与任务。

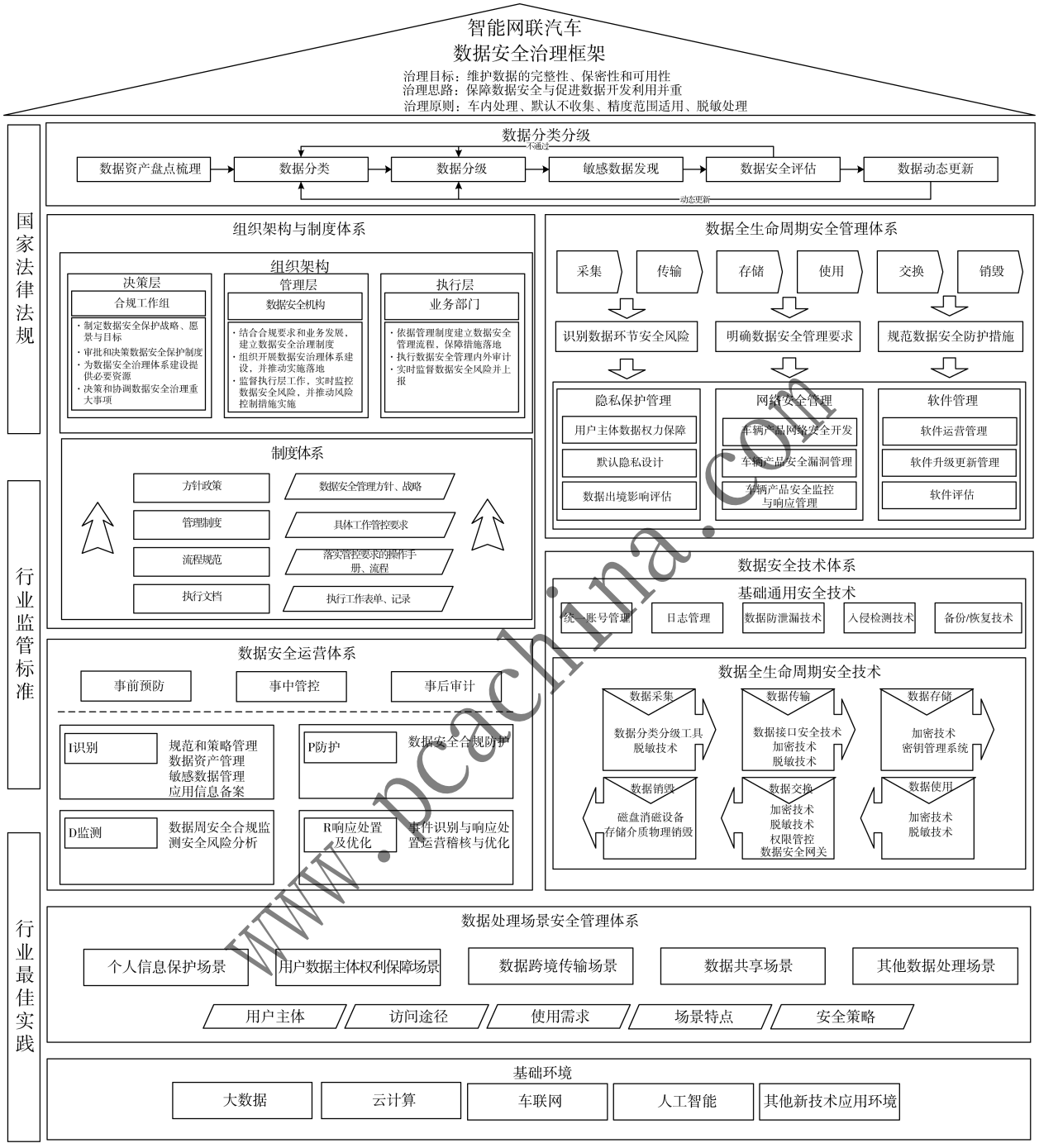

图 1　智能网联汽车数据安全治理参考框架

3.3　组织架构

数据安全治理组织架构是数据安全治理工作顺利开展的前提，是数据安全治理战略制定、落地并持续优化的组织保障。组织架构应面向智能网联汽车整体数据安全治理目标、方针，支撑覆盖数据安全决策、管理、执行与监督等多层级任务，落实人员管理和制度体系。在组织架构设计方面，决策层一般由负责智能网联汽车安全治理工作领导担任，负责制定数据安全战略、愿景与目标，审批和决策数据安全治理制度，提供必要的资源，协调重大事项；管理层一般为数据安全治理专门机构，负责建立数据安全治理制度及实施指南，建设数据安全管理体系并推动落地实施，监督执行层执行并推动实施风险控制措施；执行层一般为各业务部门，负责根据管理制度建立业务数据安全管理流程并推动落地，执行内

外审计要求，及时发现数据安全风险并上报管理层。监督层一般由公司内控审计部门担任，负责审计数据资产、数据安全风险，并监督管理制度落实情况，及时向决策层汇报问题及整改建议。在人员管理方面，应定岗定责，注重能力培养与提升，加强安全教育。在制度体系建设方面，需构建包含方针政策、管理制度、流程规范、执行文档的数据安全治理制度集合，并持续优化。随着智能网联汽车技术系统日趋复杂，数据安全治理面临更加专业化的挑战。作为智能网联汽车数据安全治理专门机构，资源整合、功能完备的管理层日益成为组织架构中的核心部门，并形成与其他部门密切协作的有效运作机制。具体来讲，管理层机构应包括功能安全团队、标准与规范团队、风险管理与评估团队，纳入专业工程师、安全专家和测试人员，负责整体数据安全治理体系的功能设计、验证和评估，相关标准和最佳实践的制定和推广，并进行全面的风险评估并制定相应的应对策略。

3.4 数据分类分级

数据分类分级是构建数据安全治理框架的基础工作。首先，需开展数据资产的盘点梳理，包括车辆基本数据、感知数据、决策数据、运行数据等。其次，应基于识别备案的数据资产，落实、审核、发布业务数据分类分级目录。再次，通过敏感数据识别技术，全面、准确、快速发现和定位敏感数据，形成敏感数据目录，明确数据保护对象，为构建完善的数据安全治理体系打造坚实基础[10]。智能网联汽车数据分类分级需要遵循合规合法（遵循有关法律、法规要求）、科学合理（充分考虑车、路、人、云的数据特征，合理设定数据类别和级别）、客观明确（数据分类分级方法应是客观且可校验的）、简单易用（数据分类分级方法应精炼且易于理解）等原则。智能网联汽车数据分类分级重点在于制定数据分类分级方法。为了确保智能网联汽车数据分类全面并界限明确，可基于数据来源对智能网联汽车数据进行分类，从“车、路、云、人”的角度与产业链主体（公司、机构、业务部门等）联动进行数据的盘点。同时，可基于定性指标判定智能网联汽车数据的重要性等级：一般级、严重级、特别重要级。智能网联汽车数据分类分级流程及示例如图 2 所示。

3.5 数据全生命周期安全管理体系

数据全生命周期安全管理体系可认为是数据安全治理框架的主体，主要针对现有数据安全合规要求，基于数据收集、存储、传输、使用、交换和销毁等数据全生命周期，从技术和管理角度，识别重要数据处理环节所存在的安全风险，明确数据安全管理要求，规范相应数据安全防护措施。智能网联汽车数据全生命周期安全管理体系主要涉及车辆内部数据安全管理，数据安全风险识别与处理，车辆数据安全测试，监测、响应、上报针对车辆数据的网络攻击和威胁，以及相关主体之间数据安全依赖关系等。同时，智能网联汽车数据全生命周期安全管理体系覆盖涉及众多管理功能，如与隐私保护管理、网络安全管理、软件管理等，并将具体安全管控要求在数据生命周期中落地。其中，隐私保护管理涉及用户主体数据权力保障、默认隐私设计、数据出境影响评估等；网络安全管理涉及车辆开发、生产、测试、运维中影响数据安全，包括车辆产品网络安全漏洞管理、安全监控与响应管理等；软件管理涉及软件运营、更新、销毁中的数据安全管理等。

3.6 数据安全运营体系

数据安全运营体系是实现数据安全事前预防、事中管控、事后审计的全面数据安全防护的组织运作规则及相应资源。数据安全运营体系目的是将数据全生命周期安全管理体系和数据安全技术体系以有效运营的方式持续推行下去，实现对其从制度指导与策略制定，到事件识别与风险处置，再回归到优化改进制度及策略的闭环持续化运营。数据安全运营体系以数据全生命周期安全管理体系和数据安全技术体系为基础，以持续性监控分析为核心，一般基于经典的 IPDR 理论，从识别（I）、防护（P）、监测（D）与响应处置及优化（R）四个维度出发，通过如数据安全策略优化、基于数据安全规范的业务持续改进、数据安全事件处理和数据安全风险评估及处置等运营措施，支撑闭环、持续化的数据安全运营。其中，“识别”主要涉及规范和策略管理、数据资产管理、敏感数据管理和应用信息备案等功能；“防护”主要涉及数据安全合规防护等功能；“监测”主要涉及数据安全合规监测、安全风险分析等功能；“响应处置及优化”主要涉及事件识别与响应处置、运营稽核与优化等功能。

3.7 数据安全技术体系

数据安全技术体系是基于数据分类分级成果构建的支持数据全生命周期安全及通用安全的技术防护体系，力图通过技术手段落实全面、系统的数据安全管控措施。数据安全技术体系可分为基础通用安全技术工具和全生命周期安全技术工具两个层级。基础通用安全技术主要用于支撑通用安全管理，多采用统一账号管理、日志管理、数据防泄漏技术、入侵检测技术、备份/恢复等技术；全生命周期安全支持技术是在部署通用技术工具保证通用安全的基础上，针对数据安全生命周期的各个阶段实施保障安全技术，多采用数字签名和身份认证技术、数据清洗技术、数据脱敏技术、数据溯源技术、密码使

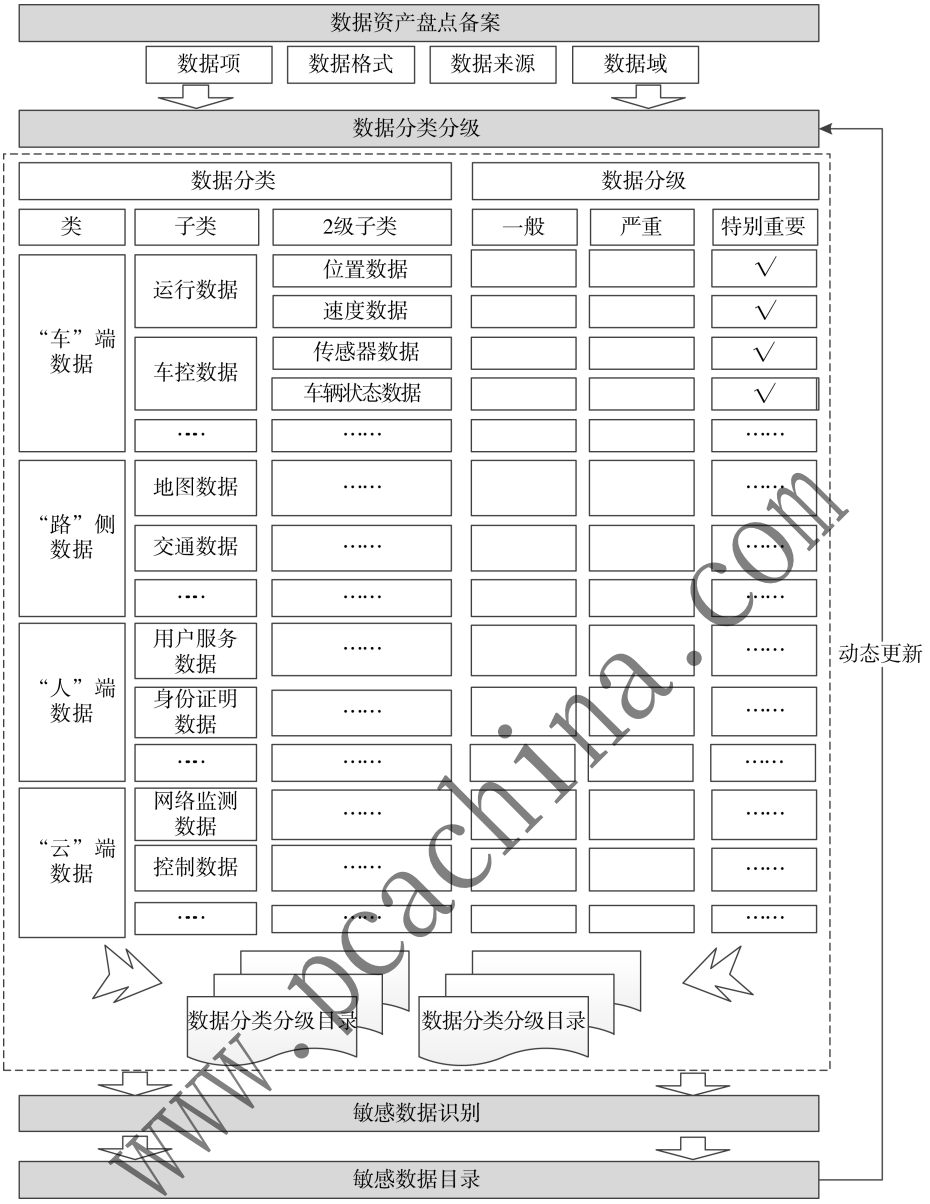

图 2　智能网联汽车数据分类分级示例

用和密钥管理技术等新技术应用，支持数据全生命周期安全管理实施。在智能网联场景下的功能实现过程中，数据安全技术体系需结合智能网联技术特性进行持续完善。一是加强区块链、轻量化密码等新安全技术与智能网联汽车技术融合，推动零知识证明、同态加密、可信多方计算等技术应用；二是加大传统数据安全技术创新，通过多层防护和多重检测技术结合，实现对智能网联汽车数据安全进行深度检测与防护。

3.8　数据处理场景安全管理体系

数据处理场景安全管理体系是在保证数据正常使用目标下，基于智能网联汽车不同使用场景特点及时发现数据风险，促进数据安全技术与数据场景业务深度融合，用于实现数据安全治理关注点的核心场景化安全。根据现有智能网联汽车合规要求，随着市场持续拓展和深化，个人信息保护、用户数据主体权利保障、数据跨境传输等场景愈来愈体现出独特的场景安全需求，迫切需要制定相应的数据安全策略，依法推动数据合理有效利用和依法有序流动。典型的数据使用场景，需要按照监管要求，从用户主体、访问途径、使用需求、场景特点、安全策略等方面，建立健全相关技术和管理措施，保证数据安全。例如，智能网联汽车跨境传输场景的安全管理体系，就需要全面审查数据跨境传输目的、数据类型、数据量、数据跨境方向，根据合规要求，明确数据跨境传输管理流程，并建立有针对性的场景化数据安全管理

体系并加以实施，包括数据跨境传输需求申请、数据跨境自评估、数据跨境风险评估、数据出境工具审查、跨境计划制定并执行、合规检查与考核等。又如，智能网联汽车个人隐私信息保护场景的安全管理体系，需要先就是否涉及个人敏感信息或对个人信息进行分析、监控、评估开展预评估，其次对数据处理活动进行分析，明确个人信息收集、处理、控制措施，制定相应风险应对措施，包括采用隐私政策、授权条款等方式告知个人信息处理方式、提供用户撤回授权渠道等，最后对风险进行识别与定级，开展风险整改。同时，全程应开展个人隐私信息保护风险审核与监控。

3.9 基础环境

基础环境是针对智能网联车涉及的大数据、云计算、车联网等复杂多元异构软硬件，采用区块链、联邦学习、多方安全计算等技术，搭建的统一规范、互联互通、安全可控的智能网联汽车数据流动基础设施环境，实现数据“可用不可见”“可控可计量”“可信可追溯”等，提供数据安全流通和共享协同。

4 结论

智能网联汽车时代，数据安全事关人身安全和隐私伦理，具有数据量庞大、安全风险大、经济价值高、数据关联复杂等特点，对智能网联汽车数据安全风险进行治理是智能网联汽车产业发展的首要任务。本文以数据安全合规为数据安全治理目标，从顶层设计的角度给出智能网联汽车数据安全风险的治理框架，在数据安全战略、数据分类分级、数据全生命周期安全管理体系、运营体系、技术体系、场景管理体系等方面，提出一套数据安全治理的可行路径，为智能网联汽车数据安全治理提供了参考。

参考文献

[1] 钟永超，杨波，杨浩男，等. 智能网联汽车安全综述 [J]. 信息安全研究，2021，6（6）：558.

[2] 工信部. 统筹推进智能网联汽车高质量发展 [EB/OL]. [2023 - 04 - 26]. http：//www. whwx. g ov. cn/xxh/hyfzyw/202304/t20230426_ 2192448. shtml.

[3] 郑霖豪，许漾方，任羽卓. 构建国家数据安全治理体系：理论、挑战与对策 [J]. 价格理论与实践，2023（9）：53 - 54.

[4] FRITSCH J, WONHAM M. How to successfully design and implement a data-centric security architecture [EB/OL]. [2021 - 12 - 20], https：//www. gartner. com/en/documents/3953491.

[5] 曾小松. 智能网联汽车数据安全治理框架研究 [J]. 智能网联汽车，2022（3）：22 - 23.

[6] 吴海燕，陈朴，陈亚亮，等. 智能网联汽车数据安全国内外治理机制及政策研究 [J]. 电信快报，2022（9）：28 - 33.

[7] 张敏，魏伟，谭天怡，等. 数据分类分级及其发展路径研究 [J]. 网络安全与数据治理，2022（1）：19 - 21.

[8] 郝艳丽. 大数据时代政府数据安全治理：文献综述与研究展望 [J]. 网络安全技术与应用，2023（8）：65 - 66.

[9] 赵高华，姜伟，王普. 数据跨境流动治理与对策研究 [J]. 网络安全与数据治理，2022（3）：23 - 27.

[10] 路特斯科技有限公司，普华永道会计师事务所（中国）. 智能网联汽车数据安全合规白皮书 [R/OL]. 2023.

（收稿日期：2024 - 01 - 29）

作者简介：

宋琦（1981 - ），男，博士，工程师，主要研究方向：人工智能融合应用与安全治理。

武波（1990 - ），男，硕士，工程师，主要研究方向：数据挖掘、数据分析、高校信息化。

刘永东（1973 - ），男，硕士，高级工程师，主要研究方向：人工智能融合应用与安全治理。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部