ICS
点击此处添加中国标准文献分类号

T/CPPC

团　　体　　标　　准

T/CPPC ××××—××××

营运车辆联网数据安全通用技术要求

Commercial Vehicles Data&information Security Technology Requirement

点击此处添加与国际标准一致性程度的标识

文稿版次选择

××××－××－××发布　　××××－××－××实施

中国生产力促进中心协会　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由交通运输通信信息工程质量检测中心提出。

本文件由全国资产管理标准化技术委员会（SAC/TC 583）归口。

本文件起草单位：交通运输通信信息工程质量检测中心、长春吉大正元信息技术股份有限公司、北京诺君安信息技术股份有限公司，一汽解放，中寰卫星，T3出行，有为科技。

本文件主要起草人：×××、×××、×××。

本文件为首次发布。

引　　言

本标准规定了营运车辆服务过程中数据全生命周期内保护的总体要求，主要包括数据采集、分类分级、数据传输、数据存储、数据处理、数据交换和数据备份、销毁等方面的安全保护要求。本标准规定的数据，涵盖道路运输车辆服务过程中的除了用户信息以外的所有数据，包括但不限于来自车辆、移动智能终端、路边基础设施和车联网服务平台等载体相关的数据。

营运车辆联网数据安全通用技术要求

1 范围

本标准适用于道路运输车辆信息服务数据提供者或数据使用者的信息服务系统，包括但不限于汽车厂商、零部件供应商、第三方供应商、车联网服务提供商、4S店和维修厂等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

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
GB/T 22239信息安全技术信息系统安全等级保护基本要求
GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求
GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
GB/T35276——2017信息安全技术SM2密码算法使用规范
GB/T 17964信息安全技术分组密码算法的工作模式
GB/T 32905信息安全技术SM3密码杂凑算法
GB/T 32907信息安全技术SM4分组密码算法
JT/T 415—2006道路运输电子政务平台 编目编码规则
JT/T 697.7—2014 交通信息基础数据元 第7部分：道路运输信息基础数据元
JT/T 808-2011道路运输车辆卫星定位系统终端通讯协议及数据格式
JT/T 1049.1-2016道路运政管理信息系统 第1部分：总体技术要求
JT/T 1049.2-2016道路运政管理信息系统 第2部分：数据资源采集接口
JT/T 1049.3-2016道路运政管理信息系统 第3部分：数据资源目录服务接口
YD/T 3746-2020车联网信息服务 用户个人信息保护要求
YD/T 3751-2020车联网信息服务 数据安全技术要求

3 术语和定义

GB/T 40856-2021界定的以及下列术语和定义适用于本文件。

3.1 车载信息交互系统 on-board information interactive system

安装在车辆上的通信系统，具备下列至少一项功能：

a)对外可通过蜂窝网络、短距离通信等通信技术建立连接并进行数据交换等功能，对内可通过汽

车总线与电子电气系统进行信息采集、数据传递与指令下发等功能；

b)实现通话、录音、导航和娱乐等相关服务功能。

3.2 数据全生命周期：data life cycle

数据采集、传输、存储、使用、迁移、销毁、备份恢复过程。

3.3 车联网信息服务数据安全： data security of Internet of vehicle information service

对车联网信息服务活动过程中相关的数据及数据处理环节（采集、传输、存储、使用、共享、销毁、备份与恢复等）实施安全保护。

3.4 用户数据 user data

由用户产生或为用户服务的数据。（注：该数据不影响安全功能的运行。）

4 营运车辆网联数据安全架构

4.1 营运车辆网联数据交互范围

营运车辆网联数据，是指交通运输部门及企业在开展运输业务和进行经营管理的过程中，对进行采集、传输、存储、使用、删除、销毁的各类网联数据。其数据范围包括：路侧计算终端、交通运输网联车载终端设备所采集的数据；自动驾驶示范区运营平台，运输车辆运营平台，政府交通管理平台运行过程中产生的数据。其数据交互范围包括：终端与平台，终端与终端，平台与平台。如图1所示。

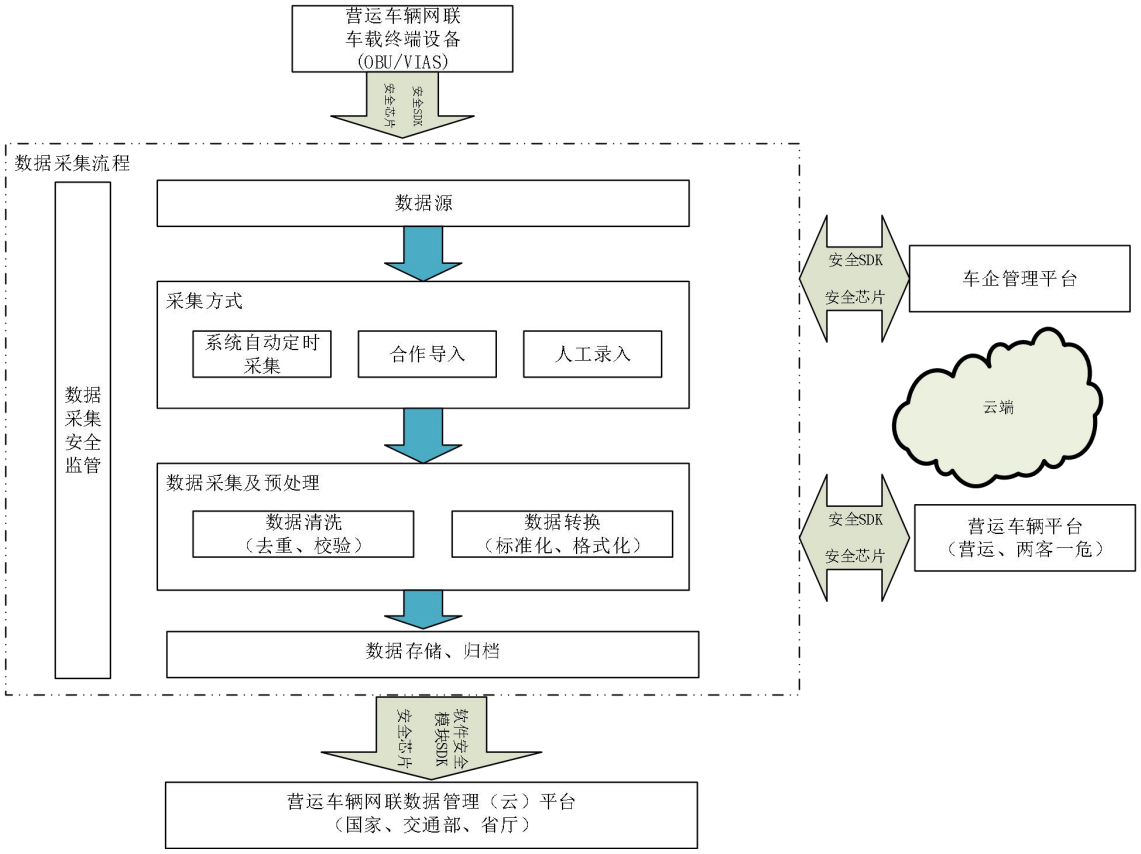

图1 营运车辆网联数据交互示意图

4.2 营运车辆网联数据安全生命周期管理

营运车辆网联数据安全生命周期管理是指交通运输部门及企业在开展业务和进行经营管理的过程中，对运输车辆网联数据进行采集、传输、存储、使用、删除、销毁的整个过程。数据生命周期安全框架（见图 1）遵循数据安全原则，以数据安全分级为基础，建立覆盖数据生命周期全过程的安全防护体系，并通过建立健全数据安全组织架构和明确信息系统运维环节中的数据安全需求，实现数据安全、密码安全、通信安全、网络安全的规范管理，全面加强营运车辆网联数据安全保护能力。如图2所示。

图 2 营运车辆网联数据安全生命周期示意图

5 营运车辆网联数据分类

参考JT/T 697.7—2014相关分类要求，根据营运车辆网联数据特点进行分类。

5.1 基础数据

包括但不限于：车辆数据、车载终端数据、云平台服务数据等

a）车辆数据：

车辆基础属性数据：包括但不局限于车牌号、发动机号、车架号、车辆品牌和型号、标识、车辆颜色、车身长度和宽度外观等数据。

b）车载终端数据：指车联网移动终端中与车联网信息服务相关的应用软件的属性类数据，包括但不限于应用软件的开发商、类别、版本、大小等相关的数据。

c）云平台服务数据：

这里指与车联网服务平台在规划设计、建设运维等阶段相关 ， 包括但不限于车联网服务平台的开发商或运营商、平台服务器和操作系统等的品牌和版本、平台主机及软件的配置信息等。

d）平台业务数据：

包括但不限于业务管理等数据。

e）管理终端数据：

指管理终端和车机联网通过互联网进行数据共享，包括但不限于用户信息、购买信息、用户行为、车辆操控数据、通讯录、通话记录、行驶轨迹等。

5.2 营运数据

a）营运类数据主要是与车辆所处运营状态相关，包括车联网信息服务中与车辆进行通信或交互的外部设备、终端、行人等相关的数据信息。

b）包括但不局限于车-车通信中的车辆位置、行驶速度，红绿灯信息、道路基础设施相关的测速雷达、摄像头等采集的信息，道路行人的具体位置、行驶和运动的方向、行驶和运动状态、速度、距离、有无发生碰撞的可能相关的状态数据，以及针对电动汽车获取的充电桩等设备相关的数据。

5.3 控制指令数据

车控类数据包括但不限于：对车辆操控直接相关的指令数据，主要包括两类：智能决策车控类数据、车辆远程操控类数据。

a)智能决策车控类数据：是与车辆自动驾驶或智能辅助驾驶行为相关，基于环境感知和智能决策等系统处理之后，实现的对车辆的智能控制行为数据，包括但不限于线控制动与驱动、线控转向、自动变速、底盘一体化控制等相关的数据。

b)车辆远程操控类数据： 主要是指借助于车联网 APP、车联网服务平台等载体， 对车辆实施的远程操作和控制类指令数据，包括但不仅限于远程开关门锁、远程开关空调、远程开关车窗、 远程开关车灯、远程开关车喇叭、远程开关车辆后备箱、远程启动或制动车辆、远程控制车辆熄火、远程诊断等。

5.4 应用类数据

应用类数据包括但不限于，支撑道路运输业务运行的各类信息系统数据、运营平台业务及应用程序的安全数据等。

6 营运车辆网联数据分级

营运车辆网联数据安全级别按照YD/T 3751-2020相关要求，根据安全性遭到破坏后的影响范围和影响程度，将数据安全级别由高到低划分为隐私数据、重要数据、普通数据。

6.1 普通数据

普通数据包含但不限于：车牌号、车辆品牌等数据；

6.2 重要数据

重要数据包含但不限于：发动机号、vin码等数据；

6.3 敏感隐私数据

敏感隐私数据包含但不限于：车辆操控类数据、车辆权益人数据等；

7 营运车辆网联数据基础安全要求

7.1 数据采集

数据采集是指交通运输部门和企业开展服务及经营管理等活动中，直接或间接从各类车载终端、路侧计算终端，以及企业客户、外部数据供应方等外部平台获取数据的过程。数据采集过程存在数据泄露、数据源伪造、特权账户滥用、数据篡改等安全风险。参考《信息安全技术 汽车采集数据的安全要求》（GB/T XXXX-2021），并根据营运车辆特殊性加以规范。

数据采集应满足以下要求：

a)采集用户数据时，应告知用户采集目的和范围等方式得到用户的授权同意，并提供关闭数据采集的功能；

b)采集个人敏感信息时，需测试是否通过主动点击“同意”等方式得到用户的明示同意，并确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的意愿表示；

c)采集远程控制、远程诊断等功能场景下所发送的指令数据时，需测试是否通过明确告知等方式得到用户的授权同意，应取得用户授权同意；

d)启动一项服务，需检查是否在服务启动之后才启动数据采集、终止服务时停止数据采集。宜在提供相应服务的同时进行用户数据采集。

7.2 数据传输

数据传输应满足以下：

需通过使用篡改、伪造等方法进行模拟攻击，检查对于数据完整性、保密性和可用性的防护措施是否有效。即：车载信息交互系统应采取管理措施和技术手段，保护所传输用户数据的保密性、完整性和可用性。

7.3 数据存储

数据存储应满足以下要求：

a)需通过尝试读取存储包含个人敏感信息的文件，检查个人敏感信息是否进行了加密存储。即：应采用SM2、SM3、SM4、长度不低于2048位的RSA、长度不低于128位的AES、哈希（Hash）摘要等加密算法存储个人敏感信息，宜采用硬件安全存储方式；

b)通过查看车载信息交互系统设计文档，需检查是否有效实现重要安全参数的安全存储和运算。即：应实现安全重要参数的安全存储和运算，可采用硬件防护方式；

c)存储用户数据时，需测试“使用非授权身份访问存储用户数据的文件，检查是否无法访问文件信息”。即：应防止非授权访问；

d)需检查存储在车载信息交互系统中的个人生物识别信息，是否使用了仅存摘要等技术措施。即：应采用技术措施处理后再进行存储个人生物识别信息，例如：仅存储个人生物识别信息的摘要等方式；

e)需测试：“存储的用户数据，在被车载信息交互系统尝试修改或删除时，是否经用户同意才能操作成功”。即：未经用户授权不应修改、删除用户数据；

f)需检查：“车载信息交互系统是否支持采集、传输、存储、销毁等数据操作日志的存储功能”。即：应对用户数据采集、传输、存储、销毁等操作进行日志存储。

7.4 数据使用

数据使用是指交通运输部门和企业在提供服务、开展经营管理等活动中，进行运输车辆网联数据的访问、导出、加工、展示、开发测试、汇聚融合、公开披露、数据转让、委托处理、数据共享等活动。数据使用不应超出数据采集时所声明的目的和范围，数据使用过程存在数据非授权访问、窃取、泄漏、篡改、损毁等安全风险。

数据访问控制安全要求如下：

a) 应综合考虑数据使用主体、信用等级、业务需要、时效性等因素，按最小化原则确定数据的访问权限规则。

b)敏感隐私数据访问应建立访问权限申请和审核批准机制，并宜通过访问控制组件或访问控制代理技术对访问的终端设备、系统进行控制，以及实际操作和申请操作进行验证，保证实际操作与申请并审批的操作是一致的。

c) 应根据数据的不同安全级别，制定和明确数据访问控制过程中的相关安全措施，保障在被访问过程中的机密性和完整性，包括但不限于：

1) 重要、敏感隐私数据访问应进行身份认证，对访问者实名认证，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问。

2) 重要、敏感隐私数据访问过程应留存相关操作日志，操作日志应至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等。

3)敏感隐私数据访问应实现多因素认证或二次授权，并应结合业务需要对数据采取脱敏和控制访问数据行数的技术措施，以满足最小化原则要求。

d) 应对数据的访问权限和实际访问控制情况进行定期审计，至少每半年 1 次对访问权限规则和已授权清单进行复核，及时清理已失效的账号和授权。

e) 应通过访问控制等措施限制频繁查询数据人员的数据访问频率，如平台、数据库管理员等确需批量查询的应通过相应审批并留存相关记录，并宜提供访问控制组件与审批结果的自动联动能力。

7.5 数据交换

数据交换应满足以下要求：

a) 应进行数据交换前的网络安全能力评估，保证数据交换的安全实施；

b) 应保证数据在不同数据设备之间交换不影响业务应用的连续性：

c)数据交换中应做好数据备份及恢复相关工作，确保数据防泄漏、保密性要求。

7.6 数据销毁

数据销毁应满足以下要求：

a)需测试：“更换零部件或删除应用后，检查车载信息交互系统是否具备数据销毁的功能”，需测试“尝试修复销毁的数据，检查是否能够恢复”。即：应预备数据销毁功能，且销毁后数据不能恢复；

b)对共享类应用，需测试：“启动共享应用程序，执行用户退出后再次登录，检查是否可以获取到个人敏感信息”。例如：营运车辆状态等应用场景，在当前用户退出后，应清空个人敏感信息。

7.7 数据备份

数据备份应满足以下要求:

a)提供本地数据备份功能，进行定期备份，或提供多副本备份机制;

b)备份数据应与原数据具有相同的访问控制权限和安全存储要求。

8 营运车辆网联通信安全要求

8.1 联网安全

营运车辆网联通信安全主要用权限管理与配置加以实现。提供用户分级管理的功能。原则上用户权限可分为系统管理级、操作配置级和监控查看级等三个级别。

1)系统管理级:拥有所有权限。

2)操作配置级:具备修改配置权限，但不具备用户管理权限。

3)监控查看级:具备查看系统配置文件和设备运行状态的权限。

用户权限的设置应遵循：

1)特权分散原则:维护管理的重要操作权力分散给若干个程序、节点或用户，必须由规定的若干个具有特权的程序、节点或用户到齐后才能实现该操作。

2)最小授权原则:仅将那些用户进行操作时必需的权限分配给用户，而不要为其分配无关的或更大的权限。

8.2 远程升级安全

1)应通过设定终端接入方式或网络地址范围对通过无线(有线)网络进行管理的管理终端进行限制，确保车辆OTA升级安全；

2)应保障运输车辆关键设备具有系统升级功能；

3)应保障运输车辆升级操作的安全，如更新时机和权限；

4)应能检测升级软件的真实性和完整性。

9 营运车辆网联密码安全

9.1 密码应用

结合信息系统现状、GB/T 39786中对不同等级的信息系统提出的密码应用要求，分别针对计算平台层、业务应用层进行安全风险分析，确定风险控制措施、密码应用基本需求分析和密码应用特殊需求分析。通过风险控制措缓解信息系统存在的高风险。

GB/T 39786-2021规定的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据等四方面适用。

9.2 加密方式

1）终端应支持软件密码模块功能，为应用提供更强的数据加密，数字签名，身份认证等功能。为应用提供防克隆，防逆向调试等软件攻击的能力。密码模块应符合GB/T 37092-2018安全等级第二级认证，宜符合GB/T 39786-2021三级要求。

2）终端可支持安全芯片对生物识别等敏感数据进行加解密以保障安全。安全芯片应符合以下要求：

a)安全芯片密码算法应符合国家法律法规的规定和相关国家标准和行业标准的要求。推荐优先采用国家商用密码算法。

b)安全芯片应满足GM/T 0008安全等级2级及以上要求，且应具备商用密码产品认证证书。

c)安全芯片应具备在内部生成并存储密钥的能力。并对不同类型的密钥进行管理，公钥可以读取，私钥不可读，防止密钥泄露

10 营运车辆网联平台网络安全

10.1 平台架构安全

确保平台架构符合营运车辆网联数据交互需要。满足信息交互安全,确保业务应用过程的安全防护、身份识别和管理。

a)技术要求包括但不限于：网络安金、主机安全、应用安全和数据安全等。

b)管理要求包括但不限于：管理制度、人员安全管理、系统建设管理和系统运维管理等。

10.2 平台网络边界

a)网络边界隔离

平台内部网络与平台外部网络之间应划分为两个区域，区域间应采用技术隔离手段。

b)网络边界访问控制

1)应在网络边界根据访问控制策略设置访问控制规则,保证跨越网络边界的访问和数据流通过边界防护设备提供的受控网关进行通信，默认情况下受控网关拒绝所有通信；

2)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

3)应根据网络边界访问控制规则，通过检查数据包的源地址、目的地址、源端口、目的端口、协议等，确定是否允许该数据包通过该区域边界；

4)平台内部网络与平台外部网络之间应采用访问控制机制，禁止穿越区域边界的通用网络服务；

5)应能根据会话状态信息为输入/输出数据流提供明确的允许 / 拒绝访问的能力；

6)禁止平台内部网络的重要控制节点在无安全防护指施的情况下直接与外部网络建立连接。

10.3 平台网络环境安全

a)数据传输完整性保护

应采用常规校验机制检验网络数据传输的完整性，并能发现其完整性被破坏的情况。

b)数据传输保密性保护

应采用密码技术支持的数据保密机制，实现对网络中传输数据的保密性保护。

c)网络入侵防范

应在关键网络节点处部署入侵防范措施，对针对这些节点的入侵行为进行检测，并在发生严重入侵事件时提供报警。

11 营运车辆网联数据安全管理要求

11.1 数据安全合规评估

a）数据安全合规性评估的对象涵盖涉及存储、处理数据的交通运输网联汽车管理及运营单位、平台等;

b）基础数据安全合规性评估的对象涵盖涉及对外提供业务或服务的交通运输网联汽车管理各级管理平台、自动驾驶示范区平台、第三方运营平台等；

其他数据安全合规性评估的对象涵盖拥有涉及存储、处理用户个人信息相关系统的交通运输车辆主管部门、专业公司及运营单位、直属分支机构（平台）等。

c）评估组织实施阶段，采用包括文档查验、人员访谈、系统演示、测评验证等方式对管理措施和技术措施进行评信，对不合规项现项提出针对性整改建议。数据安全评估团队评估实践过程中，应当对评估佐证材料进行收集、整理，做好评估过程记录。

d) 应建立数据安全检查评估机制，定期制定数据安全检查评估计划。

e) 在业务功能发生重大变化时，应及时做好数据安全评估。

f) 在国家及交通运输主管部门的相关要求发生变化时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，应进行数据安全评估。

g) 应形成数据安全评估报告，并以此采取措施降低风险及可能带来的损失。

h) 每年至少应开展 1 次全面的数据安全检查评估，评估方式包括但不限于自评估、外部第三方机构评估等。

i) 数据安全检查宜采取多种形式，如自查、内部检查和外部检查等，执行管理和技术并重的检查原则，并通过技术工具对相关管理检查内容进行验证和确认。

j) 针对检查评估过程中发现的问题，应指定责任部门，制定适宜的整改计划，并跟踪落实。

k) 应妥善留存有关安全评估报告，确保可供相关方查阅，并以适宜的形式对外公开。

l) 应采取技术措施确保检查评估记录和检查报告的安全留存。

11.2 设备监控管理能力

设备监控管理包括但不限于：

a)应指定人员定期巡视车辆内部、道路、监管平台部署环境，对可能影响道路运输车辆及路网正常工作的环境异常进行记录和维护；

b)应记录设施的状态，根据需要进行维护；

c)应对设施部署环境的评估方法作出明确规定；

d)应对道路运输车辆车载设施及道路设施部署、维修、丢失和报废等过程作出明确规定 ，并进行全程管理；

e)安全审计

1) 应对控制系统、路网信息系统、标识解析系统、管理平台以及具备日志审计功能的道路运输车辆相关设备等启用安全审计功能 ，审计覆盖到进行运维的每个用户，对重要的用户行为和重要安全事件进行审计；

2)审计记录应包括事件的日朔和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3)应对审计记录进行保护 ，定期备份，避免受到未预期的删除、修改或覆盖等：

4)审计记录中应避免明文记录敏感数据，如用户口令等；

5)审计记录的留存时间应不少于 十二个月。

11.3 安全策略自适应能力

安全策略自适应能力基于警报的会审和修复，围绕全面数据风险修复自动重构系统，可以节省时间和资源，大大减轻安全团队的负担，也可以全面加强基于零信任、纵深防御方法的安全态势。

数据泄漏溯源能力

数据泄露溯源基于数据映射的判定方法及系统。通过原始交通运输网联数据集的子集作为交付数据集;对被引用的数据集中的每一条数据进行数据标记以标识交付对象并建立数据识别标签;将待溯源数据集中的每--条数据,与原始数据集中的各个子集进行匹配,得到匹配数据集:统计匹配数据集中所有子集数据的数据标记的分布,结合识别标签,判定待溯源数据集所指向的交付对象。在发现数据泄露后的追责阶段,可以根据泄露的数据对应的识别标签找到具体的数据持有用户。

参 考 文 献

[1] 姚相振,张骁,郝春亮,胡影,罗璎珞.汽车数据安全政策与标准化研究[J].中国信息安全,2022(03):82-85.

[2] 吴海燕,陈朴,陈亚亮,米昂,戴沁芸.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(09):27-33.

[3]张雪莹,陈雪鸿,杨帅锋.工业互联网数据安全标准体系研究[J].网络空间安全,2019,10(10):86-92.

[4] 乔雅. 陕西省道路交通信息服务系统框架体系设计[D].长安大学,2014.

索　　引