ICS 43.020
CCS T 40

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T XXX—XXXX

智能网联汽车数据安全要求

Intelligent and connected vehicle Requirements for data security

（送审稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

深圳市市场监督管理局　　发布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件以推荐性国家标准《智能网联汽车 数据通用要求》（征求意见稿）（计划号：20213606-T-339）（2022年10月版本）为基础制定，主要用于支持深圳市智能网联汽车准入管理工作的实施。

本文件由深圳市工业和信息化局提出并归口。

本文件起草单位：深圳市工业和信息化局。

智能网联汽车数据安全要求

1 范围

本文件规定了智能网联汽车数据的一般要求、个人信息保护要求、重要数据保护要求、审核评估要求等。

本文件适用于智能网联汽车及其数据处理者。

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 14886 道路交通信号灯设置与安装规范

GB 14887 道路交通信号灯

GB/T 38636—2021 信息安全技术 传输层密码协议（TLCP）

DB4403/T XXX—XXXX 智能网联汽车整车信息安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能网联汽车 intelligent and connected vehicle

具备环境感知、智能决策和自动控制，或与外界信息交互，乃至协同控制功能的汽车。

3.2

汽车数据 vehicle data

汽车设计、生产、销售、使用、运维、报废等过程中涉及的个人信息和重要数据。

[来源：汽车数据安全管理若干规定（试行）,第三条,有修改]

3.3

汽车数据处理 vehicle data processing

汽车数据收集、存储、使用、加工、传输、提供、公开、删除等过程。

[来源：汽车数据安全管理若干规定（试行）,第三条,有修改]

3.4

汽车数据处理者 vehicle data processor

开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

[来源：汽车数据安全管理若干规定（试行）,第三条]

3.5

汽车数据安全管理体系 vehicle data security management system

一种与汽车数据安全相关的要素集合，包括组织内部建立的汽车数据安全方针和目标、完成目标

使用的方法和系统、确立的汽车安全组织架构和角色责任以及形成文件化管理体系的过程。

3.6

审计 audit

获取审核证据并对其进行客观评价以确定满足审核准则程度的，系统的、独立的和文档化的过程。

[来源：GB/T 25069—2022,3.515]

3.7

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

示例：自然人包括车主、驾驶人、乘车人、车外人员等。

注：个人信息包括敏感个人信息和一般个人信息。

[来源：中华人民共和国个人信息保护法,第四条]

3.8

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

[来源：汽车数据安全管理若干规定（试行）,第三条]

3.9

一般个人信息 general personal information

除敏感个人信息外的其他个人信息。

3.10

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

[来源：中华人民共和国个人信息保护法,第七十三条]

3.11

个人信息主体 personal information subject

个人信息所标识的自然人。

[来源：GB/T 35273-2020,3.3,有修改]

3.12

人脸目标 human face object

自然人的头部正面眉毛最上端至颏底线之间、左耳到右耳（不包括耳朵）之间的部分。

3.13

人脸边界框 human face boundary frame

覆盖人脸目标范围的最小矩形或旋转矩形。

示例：人脸范围示意图见图1。

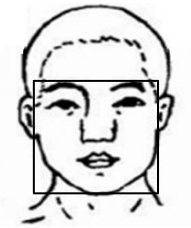

图1 人脸范围示意图

3.14

汽车号牌目标　vehicle license plate object

基材为金属的准予汽车在中华人民共和国境内道路上行驶的法定标志，其号码是机动车登记编号。

[来源：GA 36-2018,3.1,有修改]

注：本文所指汽车号牌目标均指基材为金属的正式机动车号牌，不包含喷涂的放大号牌、纸质临时机动车号牌。

3.15

汽车号牌边界框　vehicle license plate boundary frame

汽车号牌外延组成的矩形或旋转矩形。

3.16

交并比　intersection-over-union, IoU

对于符合本文件5.6.2.1要求的单个匿名化对象，应进行匿名化处理的区域与已进行匿名化处理的区域的交集与并集的比值，如图2所示。

注1：应进行匿名化处理的区域与已进行匿名化处理的区域完全重叠时，交并比为1。

注2：应进行匿名化处理但未进行匿名化处理的目标，交并比为0。

图 2　交并比示意图

3.17

检出率　recall rate

某类目标的正检数与真实目标数（正检数＋漏检数）的比值。

注：漏检数是未被检出为真实目标，但实际为真实目标的数量。

3.18

误检率　false detection rate

某类目标的误检数与检出目标数的比值。

注：误检数是被检出来为真实目标，但实际为虚假目标的数量。

3.19

重要数据　important data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

a) 军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；
b) 车辆流量、物流等反映经济运行情况的数据；
c) 汽车充电网的运行数据；
d) 包含人脸信息、车牌信息等的车外视频、图像数据；
e) 涉及个人信息主体超过 10 万人的个人信息；
f) 国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

[来源：汽车数据安全管理若干规定（试行）,第三条]

4 一般要求

4.1 汽车数据安全管理体系要求

4.1.1 汽车数据处理者应建立汽车数据安全管理体系。

4.1.2 汽车数据处理者应执行必要活动，以支持汽车数据安全管理体系的建立，必要活动包括：

a) 制定汽车数据安全方针，以明确汽车数据处理者的汽车数据安全方向和目标；
b) 分析汽车数据安全管理体系建立环境，以确定与汽车数据安全管理体系目的以及影响达成预期效果的内外部问题；
c) 确定汽车数据安全管理体系的边界及其适用范围；
d) 建立汽车数据安全组织机构并确定相关人员职责，以确保汽车数据安全管理的决策、管理和执行活动的完成；
e) 建立并维护汽车数据安全文化，以提升相关人员汽车数据安全保护意识与能力。

4.1.3 汽车数据处理者应建立汽车数据分类分级制度，形成数据资产管理台账，可参考附录 A。

4.1.4 汽车数据安全管理体系应覆盖数据全生命周期，应制定数据收集、存储、使用、加工、传输、提供、公开、删除等过程的具体分级防护要求和操作规程，并确保数据全生命周期可追溯。

4.1.5 汽车数据处理者应制定车辆全生命周期数据安全流程管理制度。

注：车辆全生命周期包括车辆的开发阶段、生产阶段及后生产阶段。

4.1.6 汽车数据处理者应建立汽车数据安全风险管理和事件处置制度，及时排查安全隐患，发生数据安全事件时，应立即采取处置措施，有效降低影响。

4.1.7 汽车数据处理者应建立与合同供应商、服务提供商、车辆生产企业子组织之间数据安全依赖关系的流程管理制度。

4.1.8 汽车数据处理者应建立投诉举报处理机制，建立数据安全投诉举报渠道并及时受理、处置数据安全投诉举报。

4.1.9 汽车数据处理者应建立数据安全审计制度，以持续改进汽车数据安全管理体系。

4.2 个人信息和重要数据的一般要求

4.2.1 汽车数据处理者处理个人信息应符合第 5 章的要求，法律法规及具有强制效力的标准另有规定的除外。

4.2.2 汽车数据处理者处理重要数据应符合第 6 章的要求，法律法规及具有强制效力的标准另有规定的除外。

4.2.3 汽车数据处理者处理的数据既属于个人信息也属于重要数据，应同时符合第 5 章和第 6 章的要求。

5 个人信息保护要求

5.1 个人信息处理通用要求

5.1.1 汽车数据处理者应只处理满足处理目的所必需的个人信息。

5.1.2 处理汽车个人信息的系统应符合相关法律法规的要求。

5.2 个人同意的取得

5.2.1 显著告知

处理个人信息的汽车数据处理者应在处理个人信息前以显著方式告知个人，具体要求如下：

——告知方式可选取弹窗、文字说明、提示条、提示音、产品说明书、合同书、个人信息保护政策等；

——告知内容应至少包含：

a) 处理个人信息的种类、处理各类个人信息的目的、用途、方式；
b) 收集各类个人信息的具体情境以及停止收集的方式和途径；
c) 个人信息存储地点、存储期限，或者确定存储地点、存储期限的规则；
d) 查阅、复制其个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径；
e) 汽车数据处理者的名称或者用户权益事务联系人的姓名和联系方式；
f) 法律、行政法规规定的应当告知的其他事项。

5.2.2 取得个人同意的选项设置

向个人进行符合本文件5.2.1要求的显著告知后，汽车数据处理者应取得个人同意并按如下要求设置取得个人同意的选项：

——提供同意和拒绝同意的选项；

——处理敏感个人信息，应取得单独同意，并提供自主设定同意期限的途径；

——不应仅依赖于个人生物识别特征信息保障车辆基础功能的正常使用。

5.2.3 取得个人同意的例外

5.2.3.1 满足以下例外情形时，汽车数据处理者处理个人信息可不取得个人同意：

——提高车辆行驶安全性且不向车外传输个人信息的功能，例如驾驶员注意力监测功能等；

——用于事故或紧急救援的服务功能，例如车载事故紧急呼叫系统等；

——处理个人自行公开或者其他已经合法公开的个人信息；

——无法通过有效的技术手段取得个人同意的情形；

——其他为了满足法律、行政法规、地方性法规、部门规章、规范性文件、具有强制效力的国家标准要求处理个人信息的情形。

5.2.3.2 汽车数据处理者应通过产品说明书、合同书、个人信息保护政策等形式提供取得个人同意例外的功能清单及例外理由。

5.2.4 个人同意范围和时效性要求

5.2.4.1 汽车数据处理者应依据取得的同意范围处理个人信息，若超出同意范围，应重新取得个人同意。

5.2.4.2 当个人同意期限届满时，若汽车数据处理者仍有必要继续进行除删除外的个人信息处理活动，应重新取得个人同意。

5.2.5 个人同意的撤回

5.2.5.1 汽车数据处理者应提供个人撤回同意的途径并告知撤回同意所带来的影响。

5.2.5.2 个人撤回同意后，若汽车数据处理者仍需要继续进行除删除外的个人信息处理活动，应重新取得个人同意。

5.3 个人信息收集

5.3.1 收集个人信息时，汽车数据处理者应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。

5.3.2 因同一数据收集设备支持多个功能服务且所需数据精度要求不同，至少应有一个功能服务符合5.3.1要求，针对其他不符合5.3.1要求的功能服务，汽车数据处理者应在个人信息处理相关文档中当作出合理说明。

5.4 个人信息存储

5.4.1 汽车数据处理者存储个人信息的期限应与取得同意的个人信息存储时间一致。

5.4.2 存储个人信息时，汽车数据处理者应制定数据访问控制策略并实施访问控制机制。

5.4.3 采用非易失性存储介质在车内存储个人信息时，汽车数据处理者应进行加密，使用的密码技术应满足以下要求：

a）汽车数据处理者应使用公开的、已发布的、有效的密码算法，并选择适当的参数和选项；应根据不同密码算法和场景，选择适当长度和有效的密钥。

注：有效的密码算法指安全有效且未被破解的算法，如MD5已被破解，此类算法相对不安全。

b）汽车数据处理者应将密钥及密钥相关信息存放在可控且专用的存储区域，防止通过软硬件接口的非法访问以及物理攻击等手段获取密钥及密钥相关信息。

注：专用指该存储区域仅用于存储密钥及密钥相关信息；可控是指密钥及相关信息不被非法访问并且得到安全应用。

5.5 个人信息使用

使用个人信息时，汽车数据处理者应制定数据访问控制策略并实施访问控制机制。

5.6 个人信息传输

5.6.1 车外传输要求

5.6.1.1 向车外传输敏感个人信息过程中，汽车数据处理者应对敏感个人信息进行真实性、完整性、保密性和抗抵赖保护。

5.6.1.2 向车外传输敏感个人信息过程中，汽车数据处理者使用的密码技术应满足以下要求：

a）汽车数据处理者应使用公开的、已发布的、有效的密码算法，并选择适当的参数和选项；应根据不同密码算法和场景，选择适当长度和有效的密钥。

注：有效的密码算法指安全有效且未被破解的算法，如MD5已被破解，此类算法相对不安全。

b）汽车数据处理者应将密钥及密钥相关信息存放在可控且专用的存储区域，防止通过软硬件接口的非法访问以及物理攻击等手段获取密钥及密钥相关信息。

注：专用指该存储区域仅用于存储密钥及密钥相关信息；可控是指密钥及相关信息不被非法访问并且得到安全应用。

5.6.1.3 向车外传输敏感个人信息过程中，汽车数据处理者使用的数据传输通道应满足以下要求：

a）应至少对个人信息接收方进行身份认证；

b）应采用符合GB/T 38636-2020或等级不低于TLS1.2的安全协议。

5.6.1.4 对于汽车数据处理者无法获得个人信息传输授权同意的情形，应于车端进行匿名化处理后再向车外传输。其中，对于车外的人脸目标及汽车号牌目标的匿名化处理应满足5.6.2要求。

5.6.2 匿名化要求

5.6.2.1 匿名化对象

5.6.2.1.1 人脸匿名化对象

汽车数据处理者至少应对图像或视频中满足以下要求的人脸目标进行匿名化处理：

——人脸目标对应的人脸边界框最小边长像素大于等于 32 像素；

——人脸目标对应的头部姿态水平偏转角绝对值小于等于 45°、俯仰角绝对值小于等于 30°且倾斜角绝对值小于等于 45°。

5.6.2.1.2 汽车号牌匿名化对象

汽车数据处理者至少应对图像或视频中汽车号牌边界框高度像素大于等于图像或视频有效像素高度的六十分之一的汽车号牌目标进行匿名化处理。

注：标识框高度指汽车号牌标识框上沿至下沿的距离。

5.6.2.2 匿名化处理性能要求

5.6.2.2.1 检出率要求

根据附录C.5进行试验并按照C.6进行试验结果处理，人脸目标和汽车号牌目标的检出率均应不低于90%。

5.6.2.2.2 误检率要求

根据附录C.5进行试验并按照C.6进行试验结果处理，人脸目标和汽车号牌目标的误检率均应不高于10%。

5.6.2.3 匿名化效果要求

根据附录C.8.1进行试验，已进行匿名化处理的人脸目标和汽车号牌目标应无法被识别。

5.7 个人信息删除

5.7.1 删除条件

5.7.1.1 汽车数据处理者应提供个人请求的删除个人信息的途径。

5.7.1.2 有下列情形之一的，汽车数据处理者应当主动删除个人信息或匿名化处理：

a) 处理目的已实现、无法实现或者为实现处理目的不再必要；

b) 汽车数据处理者停止提供产品或者服务，或者保存期限已届满；

c) 个人撤回同意；

d) 汽车数据处理者违反法律、行政法规或者违反约定处理个人信息；

e) 法律、行政法规规定的其他情形。

5.7.1.3 若法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，汽车数据处理者应当停止除存储和采取必要的安全保护措施之外的处理。

5.7.2 删除要求

5.7.2.1 个人信息主体主动发起删除个人信息请求的，汽车数据处理者应在删除个人信息前告知删除个人信息可能会造成的影响。

5.7.2.2 个人请求删除敏感个人信息的，汽车数据处理者应在 10 个工作日内完成删除；其他情形，汽车数据处理者应在 15 个工作日内完成删除；法律、行政法规另有规定的按照其规定执行。

5.7.2.3 被删除的个人信息应不可检索、不可访问且不被任何汽车数据处理者处理。

5.8 个人信息出境

个人信息通过车辆出境应符合DB4403/T XXX—XXXX《智能网联汽车整车信息安全技术要求》的要求。

个人信息通过其他方式确需向境外提供的，应当符合法律法规的有关规定。

5.9 个人信息的处理记录

5.9.1 有下列情形之一时，汽车数据处理者应对处理情况进行记录：

a） 处理敏感个人信息；

b） 利用个人信息进行自动化决策；

c） 委托处理个人信息、向其他汽车数据处理者提供个人信息、公开个人信息；

d） 向境外提供个人信息；

e） 其他对个人权益有重大影响的个人信息处理活动。

5.9.2 记录内容应该包括但不限于处理的个人信息种类、数据量、处理方式、处理时间。

6 重要数据保护要求

6.1 重要数据处理通用要求

6.1.1 汽车数据处理者应只处理满足处理目的所必需的重要数据。

6.1.2 处理汽车重要数据的系统应符合相关法律法规的要求。

6.2 重要数据收集

6.2.1 收集重要数据时，汽车数据处理者应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。

6.2.2 因同一数据收集设备支持多个功能服务且所需数据精度要求不同，至少应有一个功能服务符合6.2.1要求，针对其他不符合6.2.1要求的功能服务，汽车数据处理者应在重要数据处理相关文档中当作出合理说明。

6.3 重要数据存储

6.3.1 存储重要数据时，汽车数据处理者应制定数据访问控制策略并实施访问控制机制。

6.3.2 采用非易失性存储介质在车内存储重要数据时，汽车数据处理者应进行加密，使用的密码技术应满足以下要求：

a）汽车数据处理者应使用公开的、已发布的、有效的密码算法，并选择适当的参数和选项；应根据不同密码算法和场景，选择适当长度和有效的密钥；

注：有效的密码算法指安全有效且未被破解的算法，如MD5已被破解，此类算法相对不安全。

b）汽车数据处理者应将密钥及密钥相关信息存放在可控且专用的存储区域，防止通过软硬件接口的非法访问以及物理攻击等手段获取密钥及密钥相关信息。

注：专用指该存储区域仅用于存储密钥及密钥相关信息；可控是指密钥及相关信息不被非法访问并且得到安全应用。

6.4 重要数据使用

使用重要数据时，汽车数据处理者应制定数据访问控制策略并实施访问控制机制。

6.5 重要数据传输

6.5.1 向车外传输重要数据过程中，汽车数据处理者应对重要数据进行真实性保护、完整性保护、保密性保护和抗抵赖保护。

6.5.2 汽车数据处理者应使用公开的、已发布的、有效的密码算法，并选择适当的参数和选项；应根据不同密码算法和场景，选择适当长度和有效的密钥。

注：有效的密码算法指安全有效且未被破解的算法，如MD5已被破解，此类算法相对不安全。

6.5.3 汽车数据处理者应将密钥及密钥相关信息存放在可控且专用的存储区域，防止通过软硬件接口的非法访问以及物理攻击等手段获取密钥及密钥相关信息。

注：专用指该存储区域仅用于存储密钥及密钥相关信息；可控是指密钥及相关信息不被非法访问并且得到安全应用。

6.5.4 向车外传输重要数据过程使用的数据传输通道应满足以下要求中：

a）应至少对重要数据接收方进行身份认证；

b）应采用符合GB/T 38636-2020或不低于TLS1.2的安全协议。

6.6 重要数据删除

被删除的重要数据应不可检索、不可访问且不被任何汽车数据处理者处理。

6.7 重要数据出境

重要数据通过车辆出境应符合DB4403/T XXX—XXXX《智能网联汽车整车信息安全技术要求》的要求。

重要数据通过其他方式确需向境外提供的，应当符合法律法规的有关规定。

6.8 重要数据的处理记录

6.8.1 当出现下列情形之一时，汽车数据处理者应对处理情况进行记录：

a） 处理重要数据；

b） 越权访问、篡改重要数据等行为；

c） 向境外提供重要数据。

6.8.2 记录内容应该应包括但不限于处理的个人信息种类、数据量、处理方式、处理时间。

7 审核评估要求

依据本标准开展个人信息及重要数据保护要求试验前，汽车数据处理者应通过4.1的符合性评估。

依据本标准开展个人信息及重要数据传输和存储试验前，汽车数据处理者应通过针对5.1、5.2、5.3、5.5、5.7、5.8、5.9、6.1、6.2、6.4、6.6、6.7、6.8要求的符合性评估。

按照附录B进行个人信息和重要数据的存储及传输试验，应满足5.4、5.6、6.3和6.5的要求。

审核评估方法可参考附录E。

附 录 A
（资料性）
智能网联汽车数据分类分级要求

A.1 数据分类分级原则

智能网联汽车数据分类分级应遵循以下原则：

a) 科学性：按照智能网联汽车数据的多维特征以及相互间客观存在的逻辑关联进行科学和系统化的分类分级；
b) 实用性：智能网联汽车数据的分类分级要确保每个类目下要有数据，不设没有意义的类目；
c) 扩展性：智能网联汽车数据分类分级方案在总体上应具有概括性和包容性，能够实现各种类型数据的分类，以及满足将来可能出现的数据类型；
d) 合法合规性：数据分类分级应遵循国家法律法规及行业主管部门有关规定；
e) 可执行性：数据分类分级规则应避免过于复杂以保证数据分类分级的可行性；
f) 时效性：数据分级应具有一定的有效期限，超过有效期限数据级别应按照级别变更策略及时调整；
g) 稳定性：分类分级要基于智能网联汽车数据最稳定的特征和属性，以保持分类分级结果稳定，并在总体上利于对同一类别或级别的数据适用相同的安全要求；
h) 显著性：根据数据在产生、采集、使用等方面的成果或内容上的显著特征确定智能网联汽车的分类方案。

A.2 数据分类

根据智能网联汽车数据的类型、特性及业务使用场景等因素，并综合数据安全管理的总体目标和安全策略要求，对数据资产进行梳理、归类和细分后形成的智能网联汽车数据分类见表A.1。

表 A.1 数据分类表

一级分类名称	二级分类名称	定义	示例
车辆基本数据	车辆标识数据	能识别或关联出特定车辆的数据	如汽车号牌、车辆识别号VIN、车辆厂商、商标、品牌、车辆产品型号等
	车辆属性数据	车辆静态属性数据（不能识别或关联出特定车辆的数据）	如车辆外廓尺寸、传动比、轴距、轮距等
	核心零部件标识数据	影响车辆感知、决策、数据记录的核心零部件数据	车载传感器、域控制器、EDR、DSSAD 软硬件型号、版本号
	车辆鉴别数据	用于验证车辆及零部件身份的信息	如密码和证书等
	车辆维保数据	车辆的诊断、维修、检查、定期监测、维修、重新编程或重新初始化或远程诊断支持所需的所有信息，这些信息是制造商为其授权经销商和维修商提供的，包括对此类信息的所有后续修订和补充。该信息包括将零件或设备安装到车辆上所需的所有信息	如车辆保险信息、车辆维护信息、车辆保养信息等
感知数据	激光雷达数据	通过车载激光雷达获取到的原始数据	点云数据信息

表A.1 数据分类表（续）

一级分类名称	二级分类名称	定义	示例
感知数据	毫米波雷达数据	通过车载毫米波雷达获取到的原始数据	点云数据或目标物信息
	摄像头数据	通过车载摄像头获取到的原始数据	视频、图片等信息
	超声波雷达数据	通过车载超声波雷达获取到的原始数据	障碍物信息（如与障碍物的相对距离）
	IMU数据	通过车载IMU获取到的原始数据	角速度和加速度等信息
	高精地图数据	相比传统导航地图，能提供精度更高、内容更丰富的道路拓扑、拓扑关系、位置、几何、交通标识、交通信号设施等地图属性，为智能网联汽车提供环境信息的地图的数据	道路信息、车道信息、道路附属设施信息等静态信息， 实时路况、交通事件等动态信息
	GNSS数据	通过卫星或基准站获取到的定位数据	载波，伪距（用于计算车的位置）
	V2X数据	通过C-V2X获取到的相关数据	红绿灯、标识、目标物等信息（BSM，RSM，SPAT 等消息集）
	语音	通过车载麦克风采集的车内乘员与车机进行语音交互的数据	——
	融合后的目标（机动车及其他道路交通参与者）数据	各感知模块融合后的输出数据	目标物的类型、相对位置、相对速度等
	融合后的交通信息数据	通过车载部件获取到的交通信息数据	交通标志、信号灯、路况信息、限速信息等
	融合后的自然条件数据	通过车载部件获取到的自然条件数据	白天、黑夜、晴天、雨天、雪天、车外温度等
	融合后的道路属性数据	通过车载部件获取到的道路属性数据	道路类别（高速公路、城市道路、乡村路等）
	融合后的自车车身姿态	通过车载部件获取到的车身姿态数据	航向角，横摆角速度，侧倾角速度等
	融合后的自车位置数据	通过车载部件获取到的绝对或相对位置数据	绝对位置信息，相对位置信息
	语义	通过采集到的语音解析得出的与车机交互的一类数据	如用来唤醒车载语音交互系统的特定关键语句等
	声纹	用来识别特定用户身份的声波频段数据	用来完成说话人辨认和确认过程的信息
	其他感知部件采集的数据	以上未能涵盖的车辆感知数据	——
	其他的感知融合数据	以上未能涵盖的车辆感知融合数据	——
决策数据	人类驾驶员操作数据	由人类驾驶员进行的操作类数据，包含非驾驶控制类数据	如档位信息、加速踏板开度、刹车踏板开度、转向角度、用户操作指令等
	远程操作数据	通过远程控制指令对车辆进行操作的数据	如车辆远程开关门锁、远程开关空调、远程鸣笛和闪灯等远程启动或泊车等
	系统决策数据	由车辆系统进行的驾驶决策控制类数据	如系统请求的档位、横向加速度、转向角、转向力矩、纵向加速度、灯光状态、雨刮状态等
运行数据	整车状态数据	车辆在运行工况下的状态数据	如上电状态、控制模式、动力模式、充电状态、挡位、制动状态、剩余油量/电量、车辆控制模式等 如实时车速、横或纵向加速度、航向角、横摆角速度、侧倾角速度、俯仰角速度等

表A.1　数据分类表（续）

一级分类名称	二级分类名称	定义	示例
运行数据	系统及部件运行状态数据	表征部件及系统运行状态的数据	如安全气囊状态、GNSS 运行状态、IMU运行状态、驾驶自动化系统运行状态、高精地图运行状态、OBU运行状态、摄像头运行状态、激光雷达运行状态、超声波雷达运行状态、毫米波雷达运行状态、夜视系统运行状态等（正常、异常、表示异常、无效）
	安全日志数据	与安全相关的日志数据	——
	其他日志数据	与安全相关性较低的日志数据	——
	汽车充电网运行数据	——	充电量、充电桩类别、编号等
其他数据	用户行为汇聚分析数据	经过处理后的用户数据，无法单独或者与其他信息结合识别特定用户的各种数据	——
	用户身份标识数据	用于标识用户身份的数据	如用户账号、密码等
	用户与座舱交互数据（非操控类数据）	用于描述用户与座舱交互产生的相关数据	如用户通讯录、通讯记录和内容、上网记录等

A.3　重要数据识别参考

A.3.1　分级要素

A.3.1.1　智能网联汽车数据分级应评估危害程度和重要程度两个方面，评估要素应至少包括影响对象和影响程度。若数据分级过程中出现多个影响对象，应按照程度的较高等级进行判定。

A.3.1.2　评估数据遭到篡改、破坏、泄露或者非法获取、非法利用后对国家安全、公共利益、个人权益和企业权益的危害程度的方法见表 A.2。

表 A.2　危害程度评估表

危害程度	影响对象	影响程度	数据一般特征
严重	国家安全	任何	影响国家的安全保卫工作、经济竞争力、科技实力、涉及国家安全的其他事项。 对国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益造成影响。
严重	公共利益	严重	影响社会公众接受公共服务的活动、使用公共设施的活动、涉及公共利益的其他事项。 对经济运行、社会稳定、公共健康和安全和其他重要社会公共利益造成影响。
中等	个人权益	中等/严重影响	个人敏感信息，一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害。
中等	企业权益	中等	对企业的科研、生产秩序、经济活动、涉及企业权益的其他事项造成严重影响。
轻度	个人权益	轻度	个人非敏感信息，个人信息主体可被识别，一旦泄露或者非法使用，可能会给个人信息主体合法权益带来负面影响。
轻度	企业权益	轻度	对企业的科研、生产秩序、经济活动、涉及企业权益的其他事项造成有限影响。
无影响	个人权益	无影响	相关数据在任何场景下均无法关联或识别到个人信息主体；或个人信息主体可主动公开或经授权公开的数据。
无影响	企业权益	无影响	对企业权益不造成影响；或数据处理者可主动公开或经授权公开的数据。

A.3.1.3 评估汽车数据处理者为处理数据所投入的各项成本、对达成预设目标及可能带来的利益的重要程度方法见表 A.3。

表 A.3 重要程度评估表

重要程度	影响对象	影响程度	数据一般特征
极高	数据处理者所投入的成本	极高	数据处理需在软硬件、技术、人力、经济等方面投入巨大成本。
极高	对数据处理者达成预设目标的关键程度	极高	达成预设目标对数据的依赖程度非常高，没有数据支撑无法完成，或者数据起到决定性作用，没有可替代方案。
极高	给数据处理者可能带来的利益	极高	数据处理可以给数据处理者在技术进步、业务发展、社会影响、经济收入等方面带来巨大利益，显著地促进技术进步、开拓新的业务模式、提升业务规模、增加业务营收。
高	数据处理者所投入的成本	高	数据处理需在软硬件、技术、人力、经济等方面投入较高成本。
高	对数据处理者达成预设目标的关键程度	高	达成预设目标对数据的依赖程度较高，数据起到关键性作用，没有可替代方案或者可替代方案成本较高。
高	给数据处理者可能带来的利益	高	数据可能给数据处理者在业务发展、技术进步、社会影响、经济收入等方面带来较大利益，有效地促进技术进步、提升业务规模、增加业务营收。
中	数据处理者所投入的成本	中	数据处理需在软硬件、技术、人力、经济等方面投入一定成本。
中	对数据处理者达成预设目标的关键程度	中	达成预设目标对数据处理有一定依赖，但有可替代方案。
中	给数据处理者可能带来的利益	中	数据可能给数据处理者在业务发展、技术进步、社会影响、经济收入等方面带来有限利益。
低	数据处理者所投入的成本	低	数据处理几乎无额外成本。
低	对数据处理者达成预设目标的关键程度	低	数据对达成预设目标无影响。
低	给数据处理者可能带来的利益	低	数据无法带来利益。

A.3.2 分级要求

智能网联汽车数据分级应按照表A.2和表A.3的要求评估数据遭到篡改、破坏、泄露或者非法获取、非法利用后的危害程度和对汽车数据处理者的重要程度，形成的数据分级应符合表A.4的要求。

若数据定级要素出现不同程度，应按照程度对应的较高数据级别进行判定。

表 A.4 数据分级表

数据级别	定级要素
S3	危害程度：严重，或 重要程度：极高
S2	危害程度：中等，或 重要程度：高
S1	危害程度：轻度，或 重要程度：中
S0	危害程度：无影响，或 重要程度：低

A.3.3 数据定级规则参考

数据定级要素主要从影响对象和影响程度两方面进行考虑，具体如下：

a) 智能网联汽车重要数据安全等级不低于 S2；

b) 同一数据由于数据量的增加可能会造成数据级别上升；

c) 不同种类数据的组合可能会造成数据级别上升。

A.3.4 数据分类分级映射参考

数据分类分级的映射关系可参考附录 D。

A.4 个人信息识别参考

以下列举汽车数据处理者处理较为广泛的个人信息作为示例，若存在表中未列举的个人信息类型可参考3.7和3.8进行判定。

表A.5 个人信息分类分级示例表

分类	分级	
	一般个人信息	敏感个人信息
个人基本资料	个人姓名、出生日期、电子邮箱地址、住址、个人电话号码、年龄、性别、家庭关系	——
个人身份信息	个人账户的系统账号（不包含密码）	身份证、驾驶证、个人账户的系统账号（包含密码）
个人车辆标识	车辆VIN、车牌号、行驶证	
个人生物识别信息	——	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等数据，数据能够识别或确定自然人的独特标识
个人财产信息	——	银行账号、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等、虚拟货币、虚拟交易、游戏类兑换码等虚拟财产、风评记录、资产信息 、信用记录
个人通信信息	短信、彩信、电子邮件以及个人通信的数据（元数据）	通信记录和内容
联系人信息	电子邮箱地址列表	通讯录、好友列表、群组列表
个人应用操作信息	通过日志存储的个人信息主体操作记录，如应用或软件使用记录、点击记录、收藏列表	网站浏览记录
个人常用设备信息	描述个人常用设备基本情况的信息，如硬件序列号、设备MAC地址、软件列表、唯一设备识别码 （如IMEI/CCID/ANDROIDID/IDFA/OPENUDID//GUID/SIM卡IMSI信息	——
个人位置信息	——	行踪轨迹、精准定位信息、住宿信息、经纬度
其他信息	——	个人音频、视频、图像数据
注1：直连通信范围较小且车辆持续移动，导致数据接收者难以持续获得车辆的行驶路线，车辆行踪泄露风险较低，因此，通过直连通信发送的车辆位置和车辆历史位置信息均可不视为敏感个人信息。 注2：通过将标识车辆的信息（如标识和/或假名证书）频繁随机变化使得直连通信范围内的数据接收者凭借自身资源和技术手段无法识别特定自然人，属于一种匿名化技术。		

附 录 B
（规范性）
个人信息和重要数据试验方法及要求

B.1 试验车辆

进行个人信息和重要数据传输和存储试验的车辆应满足以下要求：
——具备向车外传输和车内存储的能力；
——具备明确的向车外传输和车内存储相关功能开启条件。

B.2 数据车外传输试验

B.2.1 试验方法

B.2.1.1 试验前，送检厂商应提供密码算法等相关信息说明和密钥及密钥相关信息存储区域安全机制说明。

B.2.1.2 打开数据车外传输功能，通过抓包工具或者流量监测工具，获取传输的数据包，解析通信报文数据：

a) 通过检验传输的敏感个人信息和重要数据电子签名情况等方式，检验是否进行真实性和抗抵赖保护；
b) 通过对比哈希值或篡改攻击等方式，检验是否进行完整性保护；
c) 检验是否存在明文传输敏感个人信息和重要数据；
d) 检验向车外传输敏感个人信息和重要数据时是否采用了双向身份认证；
e) 检验向车外传输敏感个人信息和重要数据时是否采用了安全传输协议。

B.2.1.3 依据提供的密码算法等相关信息说明，通过分析数据包的内容：

a) 查看说明的密码算法是否是公开的、已发布的、有效的密码算法；
b) 检验使用的密码算法是否与说明的密码算法一致；
c) 查看是否使用了适当长度和有效的密钥。

B.2.1.4 依据提供的密钥及密钥相关信息存储区域安全机制说明，对存储区域进行安全分析，检查是否有安全漏洞：

a) 查看存储区域安全机制是否合理；
b) 查是存储区域仅用于存储密钥及密钥相关信息；
c) 尝试对软硬件接口进行非法访问攻击，对存储区域进行物理攻击，检查是否可以获取密钥及密钥相关信息。

B.2.1.5 依据附录 C 进行个人信息匿名化处理试验。

B.2.2 通过要求

按照B.2.1进行试验后，个人信息传输保护应符合5.6的要求；
按照B.2.1进行试验后，重要数据传输保护应符合6.5的要求。

B.3 车内数据存储试验

B.3.1 试验方法

B.3.1.1 试验前，送检厂商应提供个人信息和重要数据在车内存储的地址、数据访问控制规则说明、数据读取方式、密码算法等相关信息说明和密钥及密钥相关信息存储区域安全机制说明。

注：密钥及密钥相关信息存储区域安全机制说明包含密钥及密钥相关信息存储方式和安全存储采用的技术手段等

B.3.1.2 按照访问控制规则创建一个未添加访问控制权限的用户，尝试访问和读取存储的个人信息和重要数据，检验是否可访问和读取。

B.3.1.3 依据提供的密码算法等相关信息说明，分析数据包的内容：

a) 查看说明的密码算法是否是公开的、已发布的、有效的密码算法；
b) 检验使用的密码算法是否与说明的密码算法一致；
c) 查看是否使用了适当长度和有效的密钥。

B.3.1.4 依据提供的密钥及密钥相关信息存储区域安全机制说明，对存储区域进行安全分析，检查是否有安全漏洞：

a) 查看存储区域安全机制是否合理；
b) 查是存储区域仅用于存储密钥及密钥相关信息；
c) 尝试对软硬件接口进行非法访问攻击，对存储区域进行物理攻击，检查是否可以获取密钥及密钥相关信息。

B.3.1.5 通过修改车端系统时间设置等方式，检验个人信息车端存储时间是否与取得同意的个人信息存储时间一致。

B.3.2 通过要求

按照B.3.1进行试验后，个人信息存储保护应符合5.4的要求；
按照B.3.1进行试验后，重要数据存储保护应符合6.3的要求。

附 录 C
（规范性）
个人信息匿名化处理试验方法

C.1 试验车辆

C.1.1 进行个人信息匿名化处理的试验车辆应满足以下要求：

——具备对包含车外人脸目标及汽车号牌目标的图像或视频数据进行匿名化处理及向车外传输的能力；

——具备明确的匿名化处理及向车外传输相关功能开启条件。

C.1.2 可提供具备提供匿名化区域范围文件的能力，匿名化范围文件至少包括矩形、椭圆形或旋转矩形等匿名化标注区域、匿名化对象性质（人脸、汽车号牌目标）和记录时间。

C.2 试验设备

C.2.1 试验记录内容

试验过程中应通过试验记录设备至少记录以下内容：

——试验时间轴；

——试验车辆纵向速度；

——记录试验车辆的试验里程和试验时长；

——试验车辆周边环境视频信息。

C.2.2 试验记录设备精度

试验记录设备应满足以下要求：

——运动状态采集和存储的频率至少为 50 Hz；

——视频采集设备分辨率不小于(1920×1080) 像素，视频采样帧率至少为 30 fps；

——试验车辆速度采集精度至少为 0.1 km/h。

C.2.3 试验记录设备安装及运行

试验设备的安装、运行不应影响试验车辆原有配置及其个人信息收集和传输功能的正常运行。

C.2.4 试验结果标注能力要求

在开展 C.6.1 的图片标注处理前，应对匿名化目标标注能力进行评估且满足以下要求：

——若人脸或汽车号牌边界框的范围可覆盖匿名化区域，有无原始图片的交并比偏差不应大于 5%；

——若人脸或汽车号牌边界框的范围不完全覆盖匿名化区域，有无原始图片的交并比偏差不应大于 10%。

其中，用于评估标注能力的人脸和汽车号牌目标数量应分别不少于 500 个。

注：用于评估标注能力的图片来源于试验开始前已收集的包含原始图片和匿名化处理后图片的图片集，非试验过程采集的图片。

C.3 试验环境及道路要求

试验环境及道路应满足以下条件：

——试验道路具有良好附着能力的混凝土或沥青路面的道路；

——道路及基础设施符合 GB 14886 和 GB 14887 的要求。

C.4 匿名化处理性能要求试验过程

C.4.1 试验车辆启动车外人脸及汽车号牌图像或视频数据匿名化处理和车外传输，且功能正常。

C.4.2 试验过程中，试验车辆正常行驶于满足C.3要求的试验道路，试验记录设备开启。

C.4.3 试验过程可分单次完成或多次完成。

C.5 匿名化处理性能要求试验结束条件

C.5.1 总体要求

匿名化处理性能要求试验应在满足以下条件后结束：

——采集速度满足 C.5.2，并满足各关键速度点的图像和视频采集要求；

——匿名化对象数量满足 C.5.3 的要求。

C.5.2 试验速度

C.5.2.1 除 C.5.2.2 和 C.5.2.3 情形外，根据匿名化处理及向车外传输相关功能的开启条件中最大开启速度 T_1和最小开启速度 T_2选取采集的速度范围，试验过程应至少在以下关键速度范围内采集匿名化结果：

——大于等于 T_2且小于等于 T_2+10%（T_1-T_2）；

——大于等于 T_2+30%（T_1-T_2）且小于等于 T_2+40%（T_1-T_2）；

——大于等于 T_2+50%（T_1-T_2）。

若速度范围上限大于 120 km/h 时，则按照 120 km/h 最大开启速度进行上述计算。

C.5.2.2 若功能启动的最大速度小于 30 km/h 且不等于 0 km/h 内，可选取 C.5.2.1 中 2 个关键速度范围进行试验。

C.5.2.3 若功能仅可在静止状态下启动，可在静止状态下进行试验。

C.5.2.4 各关键速度范围采集图片不应少于 10 张或采集视频时长不应少于 10 s 且该速度范围内采集结果中至少包含已进行匿名化处理的 1 个人脸目标或 1 个汽车号牌目标。

示例：某车型匿名化相关功能开启的速度范围是 0 km/h 至 120 km/h，则采集结果至少包括：

——0 km/h至12 km/h的速度内至少采集10张图片或10 s视频，可包括静止采集的结果；

——36 km/h至48 km/h的速度内至少采集10张图片或10 s视频；

——大于等于60 km/h的速度内至少采集10张图片或10 s视频。

每个速度范围内采集的所有图片或视频中至少有1张图片或1 s视频中包含1个进行过匿名化的人脸目标或1个汽车号牌目标。

C.5.3 匿名化对象数量要求

匿名化对象数量应满足以下要求：

——若试验车辆输出图片，采集间隔大于等于 1 s 的图片数量不小于 1000 张；

——若试验车辆输出视频，每段视频不少于 10 s，总长度不小于 1000 s；

——经过匿名化处理的人脸目标数量不少于 200 个，其中相同人脸目标在不同图片内分别计数；

——经过匿名化处理的汽车号牌目标数量不少于 200 个，其中相同汽车号牌目标在不同图片内分别计数。

C.6 匿名化处理性能要求试验结果处理

C.6.1 试验结果后处理

C.6.1.1　试验过程中或试验结束后，读取已进行匿名化处理的图像、视频及匿名化区域范围文件（若有）。

C.6.1.2　完成 C.4 后，应对试验结果进行以下后处理：

——若试验车辆输出的文件包含匿名化处理后的视频，相隔固定帧数或相隔固定时间间隔进行抽帧处理且每秒提取图片不大于1张、提取图片数量应不少于1000张。

——在直接输出或抽帧后的图片中标注人脸边界框、汽车号牌边界框和已进行匿名化区域。

C.6.1.3　在读取匿名化处理的图像、视频和对视频进行抽帧处理过程中，不应改变匿名化处理后图片的尺寸和分辨率。

C.6.2　交并比计算过程

根据C.6.1.1处理的试验结果计算交并比。

C.6.3　检出率计算过程

C.6.3.1　人脸目标正检数计算方式

当人脸目标满足以下要求时，应记入人脸目标的正检数：

——满足5.6.2.1.1要求并进行匿名化处理；

——交并比大于等于50%。

C.6.3.2　人脸目标漏检数计算方式

当人脸目标满足以下要求时，应记入人脸目标的漏检数：

——满足5.6.2.1.1要求；

——交并比小于50%；

——人脸目标可见范围大于50%；

——可准确定位可见范围内的眉毛、眼睛、鼻子或嘴。

示例：图片中存在已佩戴口罩的人脸目标如图 C.1 所示，人脸目标未进行匿名化处理，根据人脸目标边界框比对，可见范围大于 50%，可见范围内包括眉毛和眼睛，可清晰定位，该目标计入漏检数。

图 C.1 匿名化漏检数结果示例

C.6.3.3　人脸误检数计算方式

当匿名化目标满足以下要求时，应记入人脸目标的误检数：

——被标记为人脸目标；

——进行匿名化处理；

——与任一人脸目标不存在交集。

其中，若匿名化目标中包含广告牌、光滑表面倒影中出现的具有人脸目标特征的图像，应不计入误检数。

示例1：动物面部进行匿名化处理且标记为人脸目标，记入误检数；

示例2：匿名化区域出现于头部上方、与人脸目标无交集且标记为人脸目标，记入误检数；

示例3：匿名化区域与人脸目标有交集，不计入误检数。

C.6.3.4 人脸检出数计算方式

被标记为人脸的匿名化对象的总数量。

C.6.3.5 汽车号牌检出数计算方式

当汽车号牌目标满足以下要求时，应记入汽车号牌目标的正检数：

——满足5.6.2.1.2要求且进行匿名化处理；

——交并比大于等于50%。

C.6.3.6 汽车号牌漏检数计算方式

当汽车号牌目标满足以下要求时，应记入汽车号牌目标的漏检数：

——满足5.6.2.1.2要求；

——交并比小于50%；

——可见范围不小于汽车号牌目标总面积的80%；

——全部数字及文字内容无遮挡且可识别。

C.6.3.7 汽车号牌误检数计算方式

C.6.3.7.1 当匿名化目标满足以下要求时，应记入汽车号牌目标的误检数：

——被系统标记为汽车号牌；

——进行匿名化处理；

——与任一汽车号牌目标不存在交集。

C.6.3.7.2 若匿名化目标中包含电动自行车、摩托车号牌、机动车临时号牌并标记为汽车号牌目标，应不计入误检数。

C.6.3.7.3 若匿名化目标中包含喷涂的放大汽车号牌、广告牌、光滑表面倒影中出现的具有汽车号牌目标特征的图像，应不计入误检数。

示例1：电线杆、垃圾桶等区域出现匿名化区域且标记为汽车号牌目标，记入误检数；

示例2：匿名化区域与汽车号牌目标有交集，不计入误检数。

C.6.3.8 汽车号牌检出数计算方式

被标记为汽车号牌目标的匿名化对象的总数量。

C.7 通过条件

试验后，匿名化处理性能应符合5.6.2.2的要求。

C.8 匿名化处理效果试验

C.8.1 不可识别性试验

C.8.1.1 机器识别试验方法

C.8.1.1.1 人脸不可识别性试验方法

选择两种具备人脸识别功能的算法模型对计入人脸正检数的所有匿名化目标进行识别。例如开源模型（insightface）、公安模型。

C.8.1.1.2 汽车号牌不可识别性试验方法

选择两种具备数字、字母、文字识别功能的算法模型对计入汽车号牌正检数的匿名化目标进行识别，例如CRNN算法。

C.8.1.2 人工识别试验方法

C.8.1.2.1 分别随机挑选100张已经完成匿名化处理的图片，由人工对计入人脸和汽车号牌正检数的匿名化目标进行识别。

C.8.1.2.2 评估任一计入人脸正检数的匿名化目标双眼、鼻子、嘴巴是否均无法确定全部轮廓范围。

C.8.1.2.3 评估任一计入汽车号牌正检数的匿名化目标的汽车号牌内容是否可全部识别。

C.8.2 通过要求

按照C.8.1.1和C.8.1.2开展试验后，匿名化处理效果应符合5.6.2.3的要求。

附 录 D
（资料性）
数据分类与分级映射表

智能网联汽车数据分类与分级的映射关系参见表D.1。

表 D.1 数据分类与分级映射表

一级分类名称	二级分类名称	分级映射
车辆基本数据	车辆标识数据	S1/S0
	车辆属性数据	S0
	核心零部件标识数据	S1
	车辆鉴别数据	S1/S2
	车辆维保数据	S1/S2
感知数据	激光雷达数据	车外的个人生物特征数据S2 车外的个人非生物特征数据S1 其他车辆车牌S2 车牌以外的其他车辆信息S0 车内的个人生物特征（人脸、声纹、指纹等）S2 车流、人流等交通信息数据S3 自然条件数据S0 测绘数据S3 行踪轨迹数据S2 单点位置数据（不包含高程）S1/S2
	毫米波雷达数据	
	摄像头数据	
	超声波雷达数据	
	IMU数据	
	高精地图数据	
	GNSS数据	
	V2X数据	
	语音	
	融合后的目标（机动车及其他道路交通参与者）数据	
	融合后的交通信息数据	
	融合后的自然条件数据	
	融合后的道路属性数据	
	融合后的自车车身姿态	
	融合后的自车位置数据	
	语义	
	声纹	
	其他感知部件采集的数据	
	其他的感知融合数据	
决策数据	人类驾驶员操作数据	档位信息S2 加速踏板开度S2 刹车踏板开度S2 转向盘角度S2
	远程操作数据	S1/S2
	系统决策数据	AD系统请求挡位S2 AD系统请求横纵向加速度S2 AD系统请求转向角S2 AD系统请求转向力矩S2 AD系统请求纵向力矩S2 AD系统请求车辆灯光/雨刮状态S2

表D.1数据分类与分级映射表（续）

一级分类名称	二级分类名称	分级映射
运行数据	整车状态数据	上电、充电状态S2 控制、动力模式S2 挡位信息S2 制动状态S2 车灯、雨刮、安全带状态S2 电池SoH S2 当前油量、电量数据S2 累计里程数据S2
	系统及部件运行状态数据	实时车速S2 横纵向加速度S2 航向角S2 横摆、侧倾、俯仰角速度S2 平均和瞬时油耗/电耗S2等
	系统及部件运行状态数据	GNSS运行状态S2 IMU运行状态S2 AD系统运行状态S2 OBU运行状态S2 各类传感器运行状态S2 OBU、TBox运行状态S2
	安全日志数据	S2
	其他日志数据	S1
	汽车充电网运行数据	S2/S3
其他数据	用户行为汇聚分析数据	S1/S2
	用户身份标识数据	S1
	用户与座舱交互数据（非操控类数据）	S1

附 录 E
（资料性）
汽车数据安全管理体系符合性评估细则

E.1 汽车数据安全管理体系评估

E.1.1 评估细则

汽车数据处理者建立了包含4.1.2-4.1.9要求的管理体系，并以体系管理规范、流程制度等相关文件进行展示。

E.1.2 通过条件

按照E.1.1进行评估后，汽车数据安全管理体系符合4.1.2-4.1.9的要求。

E.2 必要活动评估

E.2.1 标准对应条款

汽车数据处理者应执行必要活动，以支持汽车数据安全管理体系的建立。

E.2.2 评估细则

E.2.2.1 评估汽车数据处理者在开展数据处理活动前是否结合国内外法规要求及企业情况，建立数据安全方针，且形成文件化信息。

E.2.2.2 评估汽车数据处理者在设计数据安全管理框架时，是否了解并确定与组织活动相关的，且影响其实现数据安全管理体系预期结果能力的内外部环境。

E.2.2.3 评估汽车数据处理者是否确定数据安全管理体系的边界及其适用范围，在确定范围时，汽车数据处理者应考虑内外部环境及相关方的要求。

E.2.2.4 评估汽车数据处理者是否明确数据安全管理责任部门及责任人，并明确管理责任部门职责以及责任人职责范围。最高管理层对数据安全管理体系的领导和承诺、最高管理层应与数据安全相关角色进行责任和权限的分配和沟通、确定相关人员职责。

E.2.2.5 评估汽车数据处理者是否建立数据安全文化，包括培训、沟通、意识的培养：采取措施确保相关人员具备履行数据安全职责所需的能力和意识，确定与数据安全管理体系相关的内部和外部的沟通需求。其中，汽车数据处理者每年至少开展一次数据安全管理培训工作，并具备相关数据安全教育培训记录。

E.2.3 通过条件

按照E.2.2进行评估后，汽车数据安全管理体系符合4.1.2的要求。

E.3 汽车数据分类分级制度及数据资产管理台账评估

E.3.1 标准原文

汽车数据处理者应建立汽车数据分类分级制度，形成数据资产管理台账。

E.3.2 评估细则

E.3.2.1 评估汽车数据处理者是否明确数据资产的安全管理目标和原则并建立数据资产台账，且具备

E.3.2.2 数据资产清单定期更新机制，对数据资产使用、留存及报废等状态进行登记，并定期更新。

E.3.2.3 评估汽车数据处理者是否建立数据分类分级制度；评估汽车数据处理者数据分类分级制度是否能够反应数据本身的真实属性、是否能够完整覆盖企业数据处理相关活动涉及的内容。

E.3.3 通过条件

按照E.3.2进行评估后，汽车数据安全管理体系符合4.1.3的要求。

E.4 汽车数据安全管理体系评估

E.4.1 标准原文

汽车数据安全管理体系应覆盖数据全生命周期，应制定数据收集、存储、使用、加工、传输、提供、公开、删除等过程的具体分级防护要求和操作规程，并确保数据全生命周期可追溯。

E.4.2 评估细则

评估汽车数据处理者是否针对不同级别数据提出数据在收集、存储、使用、加工、传输、提供、公开等环节的安全要求及操作规程，并以文档进行展示。如开发需求文档、开发设计文档、测试验证报告等。

E.4.3 通过条件

按照E.4.2进行评估后，汽车数据安全管理体系符合4.1.4的要求。

E.5 数据安全流程管理制度评估

E.5.1 标准原文

汽车数据处理者应制定车辆全生命周期数据安全流程管理制度。

E.5.2 评估细则

评估汽车数据处理者在车辆全生命周期项目执行过程中是否针对数据安全各项活动项进行项目管理，并以文档等文件化信息的形式记录数据安全流程管理制度，并在组织中进行沟通。

E.5.3 通过条件

按照E.5.2进行评估后，汽车数据安全管理体系符合4.1.5的要求。

E.6 汽车数据安全风险管理和事件处置制度

E.6.1 标准原文

汽车数据处理者应建立汽车数据安全风险管理和事件处置制度，及时排查安全隐患，发生数据安全事件时，应立即采取处置措施，有效降低影响。

E.6.2 评估细则

E.6.2.1 评估汽车数据处理者是否建立汽车数据安全风险管理制度，并形成文件化信息，包括但不限于：数据安全风险识别规范、数据安全风险评估规范、数据安全风险处置规范、数据安全事件管理规范。

E.6.2.2 评估汽车数据处理者是否建立数据安全事件处置制度，明确数据安全事件应急响应牵头部门及相关执行部门的其工作职责、数据安全事件发现及报告机制、安全事件等级及相关应急措施、溯源及处置流程、事件总结等要求。

E.6.3 通过条件

按照E.6.2进行评估后，汽车数据安全管理体系符合4.1.6的要求。

E.7 子组织数据安全管理制度评估

E.7.1 标准原文

汽车数据处理者应建立与合同供应商、服务提供商、车辆生产企业子组织之间数据安全依赖关系的流程管理制度。

E.7.2 评估细则

评估汽车数据处理者是否明确数据安全管理体系与合同供应商、服务提供商、车辆生产企业子组织之间安全流程相关的依赖关系并进行管理，并对以下内容进行评估：

a) 通过核查企业数据安全相关制度等，评估汽车数据处理者是否对供应链企业进行背景调查和安全资质审查，综合评估第三方的数据安全保障能力；
b) 通过核查企业数据安全相关制度等，评估汽车数据处理者是否明确供应链企业数据安全管理制度，是否通过签订数据安全合作承诺书，在协议中明确细化明确第三方的数据使用权限、安全保护责任、必要的安全保护措施以及违约责任和处罚条款等。

E.7.3 通过条件

按照E.7.2进行评估后，汽车数据安全管理体系符合4.1.7的要求。

E.8 举报处理机制评估

E.8.1 标准原文

汽车数据处理者应建立投诉举报处理机制，建立数据安全投诉举报渠道并及时受理、处置数据安全投诉举报。

E.8.2 评估细则

评估汽车数据处理者是否明确数据安全事件投诉、举报的受理、处置机制流程，并对以下内容进行评估：

a) 评估汽车数据处理者是否按照法律法规和相关标准要求，建立数据安全投诉处理制度，明确举报投诉处理的部门和人员、数据安全投诉类型和相关处理流程、要求等；
b) 评估汽车数据处理者是否面向用户提供数据安全举报投诉渠道和有效的联系方式，至少采用以下一种：电子邮件、电话、传真、在线客服、在线表格等；是否能够受理与用户个人信息保护相关的举报投诉，例如用户个人信息违规采集、使用、共享等。若通过官方网站设置投诉举报信息提交窗口，是否可提交投诉举报人、问题、建议等内容；
c) 评估汽车数据处理者数据安全投诉处理记录（若有），是否遵循数据安全投诉处理制度，针对有效举报线索依法依规组织开展处置和记录工作，并自接到投诉之日起十五日内答复投诉人。

E.8.3 通过条件

按照E.8.2进行评估后，汽车数据安全管理体系应符合4.1.8的要求。

E.9 审计制度评估

E.9.1 标准原文

汽车数据处理者应建立数据安全审计制度，以持续改进汽车数据安全管理体系。

E.9.2 评估细则

对以下内容进行评估：

a) 评估汽车数据处理者是否建立数据安全审计制度，数据安全审计方案和审计结果是否以文档等文件化信息的形式记录和存档，并在组织内部必要人员中进行沟通；
b) 评估数据安全审计制度是否完整覆盖企业相关汽车数据处理活动；
c) 评估汽车数据处理者是否对审计问题进行跟踪审核，并留存异常情况处置记录。

E.9.3 通过要求

按照E.9.2进行评估后，汽车数据安全管理体系符合4.1.9的要求。