国际电信联盟
电信标准化部门

建议书

ITU-T X.1383 (03/2023)

X系列：数据网、开放系统通信和安全性

安全应用和服务（2）– 智能交通系统（ITS）安全

车联网（V2X）通信中分类数据的安全要求

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	**X.1370–X.1389**
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1383建议书

车联网（V2X）通信中分类数据的安全要求

摘要

数据安全性是车联网（V2X）通信最重要的考虑因素之一。但在车载通信等资源受限的环境中，由于需要加密功能，数据保护会消耗大量的资源。

ITU-T X.1383建议书将V2X通信中使用的数据分为几种类型，如对象属性数据、车辆状态数据、环境感知数据、车辆控制数据，应用服务数据和用户个人数据，并为分类数据类型确定了三个安全保护等级。本建议书根据这些分类数据类型和确定的数据安全等级，规定了V2X通信中分类数据的安全要求。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T X.1383	2023-03-03	17	11.1002/1000/15108

关键词

分类数据、数据安全性、V2X通信

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1383建议书

车联网（V2X）通信中分类数据的安全要求

1 范围

本建议书将车辆网（V2X）通信中使用的数据分为几种类型，并定义了每种分类数据类型的安全保护等级。本建议书根据每个安全等级中的分类数据类型，规定了V2X通信中分类数据的安全要求。

2 参考文件

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指示的版本有效。所有的建议书和其他参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。ITU-T建议书的现行有效版本清单定期发布。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.1641] ITU-T X.1641建议书（2016年），*云服务客户数据安全导则*。

[ITU-T X.1603] ITU-T X.1603建议书（2018年），*云计算监测业务的数据安全性要求*。

[ITU-T X.1372] ITU-T X.1372建议书（2020年），*车联网（V2X）通信的安全导则*。

3 定义

3.1 他处定义的术语

本建议书采用下列他处定义的术语：

3.1.1 数据脱敏（data desensitization）[b-ITU-T X.1217]：隐藏敏感数据的过程。

3.1.2 数据生命周期（data lifecycle）[b-ITU-T X.1751]：数据生成后的整个生存过程，包括数据收集、数据传输、数据存储、数据使用（涵盖数据分析和可视化）、数据共享和数据销毁。

4 缩写词和首字母缩略语

本建议书定义了如下术语：

ABS 防滑制动系统

BSM 基本安全消息

CAM 协同感知消息

DoS 拒绝服务

GDPR 《通用数据保护条例》

ICV 智能网联汽车

TLS 传输层安全协议

V2I 车对基础设施

V2D 车对移动便携设备

V2P 车对行人

V2V 车对车

V2X 车联网

5 惯例

本建议书采用以下惯例：

关键词“**要求（is required to）**”表示必须严格遵守的要求，如果宣称符合本文件，就不得偏离该要求。

关键词“**应（should）**”表示建议性的并非需绝对遵守的要求，因此宣称符合本文件时不一定按照该要求行事。

关键词“**可以（can）**”表示允许的可选要求，不含有建议的意思。

关键词“**不应（should not）**”表示必须严格遵守的要求，如果宣称符合本建议书，就不得偏离该要求。

6 V2X通信中的数据生命周期

6.1 数据生命周期

数据生命周期是根据车辆网（V2X）通信环境中相关组织业务的数据流定义的。根据V2X通信的实际情况，数据安全生命周期与[ITU-T X.1641]中的内容类似，包括下述的数据收集、数据传输、数据存储、数据使用、数据迁移、数据销毁以及数据备份和恢复阶段：

– **数据收集：**在组织内部的系统中生成新数据并从外部收集数据的过程。V2X通信中的数据收集有两种形式，一种是各种V2X通信业务流程中产生的数据，另一种是从相关用户、合作伙伴和其他第三方收集的数据。

– **数据传输：**数据在组织内部从一个实体流向另一个实体的过程。V2X通信中的数据传输主要涉及在V2X通信服务相关系统和设备之间实现数据流。

– **数据存储：**以任何数字格式对数据进行物理存储或云存储的过程。这一阶段通常与数据收集几乎同时发生。

– **数据使用：**各组织对V2X通信中的动态数据进行的一系列活动，如数据查询、分析和处理。在这一阶段，将涉及数据更新和新数据的生成。

– **数据迁移：**向外部第三方传输数据的过程，包括在V2X通信中向用户显示和提供数据，亦包括在V2X通信中各企业和机构之间合作的双方相互提供数据的过程。

– **数据销毁：**通过物理或技术手段使数据永久或暂时不可用的过程。数据销毁可出于企业的成本考虑以及外部合规性或业务要求。特别是，如果有相关的数据保留规定，应考虑服务提供商应对所收集的数据进行适当的删除或匿名化处理，使已达到保留期限或用户不再给予同意的数据无法恢复。

– **数据备份和恢复：**将全部或部分数据复制到其他存储介质以防止数据丢失并在数据丢失的情况下用备份数据恢复原始数据的过程。

6.2 威胁分析

V2X通信中的数据也面临着与[ITU-T X.1603]和[ITU-T X.1641]中定义的威胁和挑战类似的安全威胁和挑战。V2X通信中的数据所面临的一些安全威胁和挑战包括但不限于表6-1中列出的内容。

表6-1 – 根据V2X通信中数据生命周期列出的威胁和挑战

数据生命周期	安全威胁和挑战
数据收集	a) 未经授权的数据采集 b) 采集接口漏洞 c) 欺骗 d) 篡改和拦截 e) 不安全的服务访问 f) 未经授权获取管理权限
数据传输	a) 拦截 b) 伪装 c) 窃听 d) 未授权访问 e) 拒绝服务（DoS）攻击
数据存储	a) 数据丢失和泄露 b) 服务不可用
数据使用	a) 数据滥用 b) 内部威胁 c) 系统漏洞 d) 窃听
数据迁移	a) 数据滥用 b) 系统漏洞 c) 错误的呈现 d) DoS攻击
数据销毁	a) 欺骗 b) 系统漏洞
数据备份和恢复	a) 系统漏洞

7 V2X通信中的分类数据

本节规定了V2X通信所处理的数据的分类策略。六个数据类别：对象属性数据、车辆状态数据、环境感知数据、车辆控制数据、应用服务数据和用户个人数据见第7.2节。

7.1 基于V2X通信场景的数据识别

V2X通信所处理的数据可根据实际通信场景进行识别。[ITU-T X.1372]将V2X通信场景分类如下：车对车（V2V）、车对基础设施（V2I）、车对移动便携设备（V2D）和车对行人（V2P）。本节描述了每个通信场景的相关通信过程和数据。

7.1.1 V2V通信中的数据

[ITU-T X.1372]确定了三种V2V通信场景：V2V预警传播、V2V队列通信和V2V信标。在V2V预警传播场景中，预警消息在车辆之间传播。在V2V队列通信场景中，车辆组相互交换车辆状态。在V2V信标场景中，每辆车都会发送其车辆状态信息。表7-1显示了V2V通信中的数据。

表7-1 – V2V通信中的数据

类别	场景	数据
车对车	V2V预警传播	• 预警消息 • 基本安全消息（BSM） • 协同感知消息（CAM）
	V2V队列通信	• BSM • CAM
	V2V信标	• BSM • CAM

BSM和CAM的技术规范分别见[b-SAE J2735]和[b-ETSI TS 102 637-2]。

7.1.2 V2I通信中的数据

[ITU-T X.1372]确定了两种V2I通信场景：V2I预警和V2I信息交换。在V2I预警场景中，车辆与基础设施之间能够交换预警消息。在V2I信息交换中，车辆与基础设施相互通信以更新交通信息和/或有关信息娱乐服务的信息。表7-2显示了V2I通信中的数据。

表7-2 – V2I通信中的数据

类别	场景	数据
车对基础设施	V2I预警	• 预警消息
	V2I信息交换	• 车载标识 • 车载信息 • 信号相位 • 交通信号灯的时间信息 • 路面状况 • 天气状况 • 可视距离状况 • 道路施工信息

7.1.3 V2D通信中的数据

在V2D通信场景中，车与车载移动便携设备进行通信，如智能手机、笔记本电脑和导航系统。[ITU-T X.1372]确定了两种V2D通信场景：通过间接链路进行的V2D通信和通过直接链路进行的V2D通信。两种场景的区别在于通信方式，两者处理的数据类型相同。在[ITU-T X.1372]中，V2P通信被认为是V2D通信的一种具体情况。表7-3显示了V2D通信中的数据。

表7-3 – V2D通信中的数据

类别	场景	数据
车对移动便携设备	通过间接/直接链路实现的V2D通信	• 车辆硬件数据 • 车辆软件数据 • 设备硬件数据 • 设备软件数据 • 服务平台数据 • 应用服务数据

7.2 数据分类

本节描述了V2X通信中处理的数据的分类。

考虑到V2X通信中的数据，以符合个人数据保护相关法律法规，如《通用数据保护条例》（GDPR），本建议书中所述数据不能指向具体或可识别的个人的信息。

7.2.1 对象属性数据

对象属性数据是指V2X通信中实体的属性，可细分为三种类型，即车辆、移动设备和云服务平台的属性：

– 车辆数据的属性与车辆的特性有关，如品牌、类型、标志、颜色。

– 移动设备的数据属性是指与移动设备相关的特性，如品牌、类型、颜色。

– 服务平台数据的属性是与服务平台相关的特性，如版本、制造等。

7.2.2 车辆状态数据

车辆状态数据是指车辆的状态，与V2X通信中的信息服务密切相关，包括汽车动力总成系统、底盘系统、汽车安全系统、车身系统、车辆舒适系统和汽车电气系统等这些系统的运行状态和参数。

更具体而言，车辆状态数据包括来自以下系统的数据信息：车辆控制器（如泵控制信号、气压传感器报警、发动机制动有线信号等）、变送器系统（如扭矩、油耗率等）、冷却系统（如冷却液温度）、变速箱系统（如车辆启动、加速等数据）、安全系统（如安全气囊状态、安全带使用状态等）、底盘系统（如反映车载网络、转向系统、防抱死制动（ABS）、胎压监测等状态的数据信息）、舒适系统（如空调开启、座椅调节、车窗系统、照明使用等数据）及其他辅助系统。

根据对车辆运行状态的描述，车辆状态数据可分为两类：车辆的动态状态数据和车辆的静态状态数据。

– 动态的车辆状态数据与车辆系统的运行状态有关。以空调系统的状态为例，包括车内的温度和湿度。

– 静态的车辆状态数据涉及空调系统的静态状态，如安全带使用状态和空调状态等。

7.2.3 环境感知数据

环境感知数据主要与车辆的外部环境有关，包括与V2X通信中车辆通信或信息服务交互相关的外部设备、终端、行人的数据信息，包括但不限于车对车通信中的车速、交通信号灯信息和道路基础设施。测速雷达和摄像头收集的与道路基础设施、驾驶和行驶方向、驾驶和行驶状态、速度、距离相关的信息，是否会发生碰撞的可能相关状态数据，与充电站（桩）及其他为电动汽车所购置的设备相关的数据亦属于环境数据的要素。

7.2.4 车辆控制数据

车辆控制数据涉及V2X通信中的车辆控制，主要包括三个子类型：自动驾驶/智能辅助驾驶车载控制数据和远程操作与远程驾驶：

– 自动驾驶/智能辅助驾驶车载控制数据是与自动驾驶或智能辅助驾驶相关的控制指令数据。此类数据基于环境感知和智能决策系统的处理，用于实现车辆智能控制行为的数据，如线控制动或驾驶、自动变速和底盘集成控制。

– 车辆远程操作控制数据是指通过应用、服务平台等向车辆下达的远程操作指令，包括有关远程车门锁止/解锁、远程控制空调、远程车窗操作和车灯等的数据。

– 用于远程驾驶的车辆控制数据，其中远程驾驶使用案例通过将人类分为远程驾驶员或将“云”作为可能的远程驾驶员，而将这些使用案例细分为几个子使用案例。用于远程驾驶的车辆控制数据指的是显示车辆周围车道情况的车外视频流，或传送给远程驾驶员作为其决策支持的车外音频流。此外，用于远程驾驶的数据可以指传送给远程驾驶员用于监控情况的车内视频流或车内音频流。此外，用于远程驾驶的车辆控制数据指的是关于从远程驾驶员到车辆的远程控制指令的数据，例如加速或操纵指令，当由控制事件触发时，例如可以产生和发送制动指令[b-ETSI TR 126 985]，[b-3GPP TR 22.886]。

7.2.5 应用服务数据

应用服务数据涉及信息交互在V2X通信中的应用，是指V2X通信中除对象属性数据、车辆状态数据、环境感知数据、车辆控制数据和用户个人数据之外与信息服务相关的数据，包括但不限于信息娱乐数据、交通安全管控类数据、车辆相关服务数据等：

– 信息和娱乐数据涉及V2X通信中提供的娱乐服务，如特定人群的多媒体下载、网站浏览和广播订阅，以及天气预报等。

– 交通安全管控类数据涉及交通安全和交通管理，如道路交通安全预警、应急救援、车辆远程监控和管理等。

– 车辆相关服务数据涉及V2X通信中的后市场服务，如车辆维修、二手车管理、金融保险和相关电子商务。例如，某汽车品牌下某类汽车零部件的维修频率就属于车辆相关服务数据。

7.2.6 用户个人数据

用户个人数据是指V2X通信中使用和/或产生的有关用户的个人信息。本节不讨论用户个人数据的分类和保护问题。

因此，如果表7-4中作为示例列出的数据与隐私相关法律和GDPR等法规中的用户个人数据相对应，那么该法规的效力优先于分类政策。

7.3 数据安全等级

结合数据安全目标、数据的重要性、可能发生的安全事件的影响等因素的综合考虑，每个数据类别可分为3个等级：

– **1级**（保护程度较低的数据）包含V2X通信中公开的数据，如V2X平台的软件版本。

– **2级**（中度保护数据）包含需要采取安全措施保护的数据，如V2V通信中获得的车辆数据、V2X通信的登录账号和密码。

– **3级**（高度保护数据）包含V2X通信中需要的保护力度比2级（中度保护数据）更强的数据，如V2D通信中的金融交易信息、车辆关键性能数据和V2X通信的身份认证信息。

保密数据仅指企业与V2X通信相关的机密数据，这里不涉及用户的个人信息。

表7-4提供了有关V2X通信中数据安全等级和示例的详细信息。

表7-4 – V2X通信中的数据安全等级示例

V2X通信中的数据类别		V2X通信中的数据安全等级	示例
对象属性数据	车辆属性数据	1级	车辆的品牌、类型、标志、颜色。
		2级	某类型车辆的性能参数。
		3级	某类型车辆的具体软硬件配置数据。
	移动设备属性数据	1级	移动终端的品牌、类型、标志、颜色。
		2级	V2X通信中与一些重要功能相关的设备状态数据。
		3级	一种移动设备的关键性能参数和配置信息。
	云服务平台属性数据	1级	云服务平台的类型和名称。
		2级	硬件、操作系统或应用软件的信息。
		3级	服务平台的关键性能参数和配置信息。
车辆状态数据	动态的车辆状态数据	1级	空调系统的状态。 车辆内部温度。
		2级	安全气囊和安全带等的运行状态。 车内传感器感知的数据，与重要的车辆操控密切相关，如轮胎压力。
		3级	车辆的核心运行技术指标。 车内传感器接收到的与关键车辆操控密切相关的数据，如碰撞传感器的数据。
	静态的车辆状态数据	1级	一定时间内空调系统的使用频率。
		2级	车辆的平均油耗。
		3级	车辆系统的保密数据。
环境感知数据	车辆外部环境感知数据	1级	道路类型（高速公路或乡村道路或人行道）、道路状况（完好或湿滑）、道路限速、信号灯分布和状态信息、信号灯状态信息、道路拥堵、交通事故等。
		2级	在车对车通信场景中，脱敏后附近车辆的信息，如物理位置、经纬度、更新时间、行驶速度、前进方向、变道信息。 在车对行人通信场景中，脱敏后的数据，如正在接近的行人的位置、距离、速度和运动状态，以及碰撞的可能性。

表7-4 – V2X通信中的数据安全等级示例

V2X通信中的数据类别		V2X通信中的数据安全等级	示例
		3级	在车对车通信场景中，脱敏后相邻车辆一定时间段内的数据信息，如行驶路线、位置、时间、停车信息等。
车辆控制数据	自动驾驶/智能辅助驾驶车载控制数据	1级	倒车辅助中倒车提示的声音数据。
		2级	在智能辅助驾驶系统的车道保持应用中，当车辆趋于偏离行驶车道时，发送方向盘抖动、仪表盘红灯或绿灯指示等提醒指令数据。
		3级	自动泊车中智能泊车系统的确认指令。
	车辆远程操作控制数据	1级	与V2X通信远程监控相关的一般读取类数据。
		2级	远程启动车辆或启动车辆转向的指令。
		3级	通过V2X通信服务平台实现对车队规模的多辆汽车进行远程操控相关的指令。
	用于远程驾驶的车辆控制数据	1级	远程驾驶员可以使用延迟要求比车外视频和音频更宽松的车内视频流和车内音频流监控车内状态。
		2级	车外音频流可以传送给远程驾驶员，用于传送来自其他车辆的噪声和喇叭声。
		3级	传感器、显示或声音系统等再现设备用于接收来自远程驾驶员的操纵指令。指令应具有高可靠性和低延迟并且需要得到确认，尤其是与报警事件相关的指令（例如制动指令）。 记录外部声音或影像的视频（摄像机）和音频（麦克风）传感器数据（也可能是雷达或激光雷达传感器数据），用于路线中障碍物的早期和非视觉识别，例如紧急车辆、行人等。 车辆状态传感器（加速度、速度、方向、位置等）数据可以以固定的间隔从车辆高可靠性地发送给远程驾驶员，因为某些传感器流对于正确的驾驶操作或许是必不可少的。
应用服务数据	信息和娱乐数据	1级	无线电广播数据
		2级	脱敏后的网购浏览记录
		3级	信息服务应用中脱敏后的语音和视频记录
	交通安全管控类数据	1级	道路交通拥堵提醒、交通事故实时提醒数据等。
		2级	车辆列队行驶中因前方车辆急停而产生的车辆碰撞预警数据。
		3级	道路交通车辆远程监控数据。
	车辆相关服务数据	1级	脱敏后，记录与车载娱乐系统的使用、操作等信息相关的娱乐系统使用行为数据。
		2级	脱敏后，与车辆驾驶行为相关的车辆行为数据。

表7-4 – V2X通信中的数据安全等级示例

V2X通信中的数据类别		V2X通信中的数据安全等级	示例
		3级	脱敏后的数据，如基于车辆出行时间、路线、位置以及信息娱乐系统使用行为数据等分析出的车主个人喜好和行为习惯，或基于车辆自身状态和环境感知数据的车辆核心参数。
用户个人数据	N/A	N/A	N/A
表7-4的内容说明如下： 1) N/A：不适用 2) 经匿名模糊等技术手段处理后，表7-4中所述的脱敏后的数据无法直接或间接识别或表明个人信息。数据脱敏方法包括但不限于匿名、去标识化、多样化、数据抑制、数据扰动、差异化隐私等。V2X通信相关组织应在综合考虑数据主体特征、数据敏感度等级和数据操作要求的基础上，采取适当的数据脱敏措施。			

8 安全要求

本节规定了基本安全要求、中级安全要求和高级安全要求，这些要求与1-3级数据严格对应。

8.1 安全要求等级

根据对分类数据的分类，规定了每个等级的安全保护方法或措施。安全要求有三个安全等级：基本安全要求、中级安全要求和高级安全要求。一般而言，对1级（保护程度较低的数据）采用基本安全要求，对2级（中度保护数据）采用中级安全要求，对3级（高度保护数据）采用高级安全要求。表8-1基于V2X通信数据安全等级的安全保护要求。

企业也可根据自身情况或数据的机密性选择安全保护措施。

表8-1 – 基于V2X通信数据安全等级的安全保护要求

V2X通信数据的安全等级	安全要求等级		
	基本	中级	高级
1级 （保护程度较低的数据）	*	N/A	N/A
2级 （中度保护数据）	*	*	N/A
3级 （高度保护数据）	*	*	*
*：适用； N/A：不适用。			

8.2 基本安全要求

1) 数据收集

- 应根据数据安全保护目标、数据的重要性和可能发生的安全事件的影响等综合因素对V2X通信中的数据进行分类。
- 在数据收集过程中应遵循最小化原则。仅收集与业务功能相关的数据。
- 应按照第6节和第7节所述的数据分类和分类方法对所收集的数据进行分类和管理。应针对不同的数据等级制定和实施不同的安全保护措施。

2) 数据传输

- V2X通信中数据传输的总体安全要求不应低于一般通信网络。
- 应根据V2X通信场景的不同数据分类、业务流程和安全风险，采取不同的数据传输安全策略和措施。
- 应采用传输层安全协议（TLS）等安全协定，以确保各通信场景中车辆与其他实体之间数据传输的安全性。
- 应能够检测到数据在传输过程中被损坏。

3) 数据存储

- 对于车载终端和服务平台中存储的数据，V2X通信相关设备和系统应采用数据加密机制。加密的算法、强度和模式等参数应通过可选的配置来支持。
- 应能够确保服务平台或车载系统中缓存数据的安全性。应对存储在缓存系统中的数据进行加密。
- 对于车载终端和服务平台存储的数据，应采用数据访问控制机制，以防止未经授权的访问、修改和删除以及跨域信息访问。
- 应能够在存储过程中验证数据的完整性，以防止数据被篡改、删除和插入。如数据的完整性被破坏，应提供用户预警信息。

4) 数据使用

- 应在授权范围内对数据进行处理，仅限于业务需求的最小范围。
- 数据的使用应得到授权和验证。
- 数据使用的目的和范围应符合相关国内法律法规的要求。
- 在数据分析和挖掘过程中，应对源数据和挖掘结果进行签识，以防止数据被恶意删除、随意篡改或无约束的滥用。
- 对于车联网设备、系统和平台之间的数据传送或导出，应采取管理和技术措施以确保安全性。

5) 数据迁移

- 数据迁移前应进行安全能力评估，以确保数据迁移的安全性。
- 数据在不同数据设备之间迁移时，应确保业务和应用的连续性。
- 在准备数据迁移时，应制定迁移方案，评估其可行性及相关风险，而后制定相应的风险控制措施。

6) 数据销毁

- 应建立数据销毁策略和管理制度，明确销毁对象和流程。建立数据销毁审批机制，设立相关的销毁监督职能，对销毁过程进行监督。

- 应提供措施，清除已达到留存期限的数据，或用户不再给予同意时，应立即销毁数据。
- 应提供措施，帮助清除数据迁移或业务遗留的数据。
- 应提供措施，删除备份数据的所有副本。

7) 数据备份和恢复

- 应在数据迁移前建立数据备份和恢复机制。
- 应提供本地数据备份和恢复。
- 应建立定期全量数据备份机制，建议时间周期不少于每周一次。
- 备份数据应具有与原始数据相同的访问控制权限和安全存储要求。

8.3 中级安全要求

中级安全要求是基本安全要求的一组超集。在数据生命周期各阶段的基本安全要求基础上，增加以下要求：

1) 数据收集

除满足基本安全要求外，还应符合以下要求：

- 在收集2级数据的过程中，应对原始数据进行备份，以避免数据遗漏和丢失。
- 应采用识别机制，确保数据收集的真实性。
- 应采用数据验证机制，确保数据收集的完整性。

2) 数据传输

除满足基本安全要求外，还应符合以下要求：

- 汽车与车联网核心服务平台的数据传输应采用专用网或虚拟专用网通信，以实现与互联网的隔离。
- 在V2V/V2I通信中，应有可信的身份证书，从而验证数据传输节点的身份，认证信息不应泄露隐私信息。
- 车辆应能够识别来自蜂窝网络的非法连接请求，以过滤恶意数据包。
- 对于2级数据，如远程控制指令数据，应验证数据源的可靠性，以确保数据不是伪造的。

3) 数据存储

除满足基本安全要求外，还应符合以下要求：

- 应能够在存储过程中验证数据的完整性，以防止数据被篡改、删除和插入，并在数据完整性被破坏时提供必要的恢复措施。
- 应为智能网联汽车（ICV）、服务平台和应用中存储的数据文件设置识别信息，以避免未经授权的设备和系统使用此类文件。
- 对于V2X通信中服务平台的缓存系统，应保留具体的操作记录，以保护缓存的2级数据。
- 应建立数据日志管理全过程，以防止数据否认威胁。

4) 数据使用

除满足基本安全要求外，还应符合以下要求：

- 对于2级数据的数据查询，应进行查询、外部显示和统计、模糊化处理等操作。

- 应对2级数据的使用进行审计，并形成审计日志。

5) 数据迁移

除满足基本安全要求外，还应符合以下要求：

- 应制定迁移计划，评估其可行性和相关风险，而后制定相应的风险控制措施，为数据迁移做好准备。

6) 数据销毁

除满足基本安全要求外，还应符合以下要求：

- 应确保V2X通信相关资源（如文件、目录和数据库记录）的存储空间被完全清除之前，不会释放或重新分配给其他用户。
- 对于车载终端，为防止因更换车辆部件而造成数据泄露，应能够提供车载终端数据擦除功能，以确保被擦除的车载终端数据不会被恢复。

7) 数据备份和恢复

除满足基本安全要求外，还应符合以下要求：

- 对于本地或远程备份数据，全量数据备份应至少每周一次，增量备份至少每天一次。此外，还应建立多副本备份机制。
- 备份数据应加密并存储。

8.4 高级安全要求

高级安全要求是中级安全要求的一组超集。应在数据生命周期各阶段的中级安全要求基础上，采用以下所有要求。

1) 数据收集

- 保护要求与中级安全要求相同。

2) 数据传输

除满足中级安全要求外，还应符合以下要求：

- 应能够检测到数据在传输过程中完整性受到破坏，并在检测到完整性受到破坏时采取必要的措施恢复数据。
- 对于3级保密数据，应采用相互认证的方式来应对外部实体的身份冒充造成的篡改和数据泄露威胁。

3) 数据存储

除满足中级安全要求外，还应符合以下要求：

- 应采用硬件安全加密存储方案，以确保车辆、服务平台、智能移动终端应用和路侧基础设施的机密数据的保密性。
- 应能够在存储过程中验证数据的完整性，以防止数据被篡改、删除和插入，并在数据完整性受到破坏时提供必要的恢复措施。

4) 数据使用

除满足中级安全要求外，还应符合以下要求：

- 二级操作权限的审批应采用多人授权模式。
- 应进行数据关联性隔离，防止因对不同系统、平台或应用中的数据进行数据关联分析而导致数据泄露。

- 应支持保密数据使用过程中的动态脱敏。

5) 数据迁移

保护要求与中级安全要求相同。

6) 数据销毁

除满足中级安全要求外，还应符合以下要求：

- 应提供手段禁止被销毁数据的恢复。

7) 数据备份和恢复

除满足中级安全要求外，还应符合以下要求：

- 应提供安全认证措施，如身份认证，以确保本地和远程的数据备份和恢复操作仅在授权用户知情或控制下进行。

参考文献

[b-ITU-T X.1217] Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation*.

[b-ITU-T X.1751] Recommendation ITU-T X.1751 (2020), *Security guidelines for big data lifecycle management by telecommunication operators*.

[b-3GPP TR 22.886] 3GPP TR 22.886 V16.2.0 (2018), *Study on enhancement of 3GPP Support for 5G V2X Services (Release 16).*

[b-ETSI TR 126 985] ETSI TR 126 985 V16.0.0 (2020), *5G Vehicle-to-everything (V2X) Media handling and interaction (3GPP TR 26.985 version 16.0.0 Release 16).*

[b-ETSI TS 102 637-2] ETSI TS 102 637-2 (2011), *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*.

[b-SAE J2735] *V2X Communications Message Set Dictionary*, (July 2020).

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦