ICS
L80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术
物联网数据传输安全要求

Information security technology -

Security requirements of data transmission for Internet of things

（在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上）

（征求意见稿）

2017 年 3 月

XXXX－XX－XX 发布　　XXXX－XX－XX

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目 次

前　言

本标准按照 GB/T 1.1-2009《标准化工作导则 第一部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准主要起草单位：北京工业大学、中国电子技术标准化研究院、中央财经大学、公安部第三研究所、中国科学院软件研究所、北京邮电大学、西安电子科技大学、无锡物联网产业研究院。

本标准主要起草人：杨震、范科峰、丁治明、李健、刘贤刚、龚洁中、李琳、黄剑、李怡德、赖英旭、段立娟、马占宇、丁丽萍、顾健、齐力、杨明、陈书义、裴庆琪、涂山山、何通海、魏欣、吴亚玺。

引　言

随着计算机和网络技术的发展，特别是感知与控制技术的深度融合，物联网产品的应用日益广泛。从家用摄像头、智能恒温器、可穿戴电子设备、烟雾感应器等生活环境用品，到温湿度感应器、光敏感应器、物料电子标签、PM2.5自动监测仪等生产环境用品，可以说我们的生产、生活都已经被物联网技术和产品深度渗透。物联网应用系统一旦遭受攻击，将严重影响人们生产、生活的安全稳定。对此，全国信息安全标准化技术委员会（SAC/TC 260）立项研制了物联网安全通用模型、感知设备安全、传输安全等多项国家标准。

本标准参考物联网概念模型、体系结构及安全参考模型，归纳物联网数据传输面临的安全威胁，规定物联网数据传输安全普通级和增强级技术要求。并制定数据传输安全属性，以便使用者自查。为物联网系统在设计、建设、运维、管理等活动中的安全保障提供规范性要求，也为各组织定制自身的安全标准提供基线参考。

信息安全技术 物联网数据传输安全要求

1 范围

本标准归纳了物联网数据传输面临的安全威胁，规定了物联网数据传输安全基础级和增强级技术要求。并制定数据传输安全属性，以便使用者自查。

本标准适用于物联网规划、建设、运行、管理等相关方，对物联网数据传输安全的规划和落实，也可为物联网数据传输安全检查和测评等工作的开展提供依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 25069-2010 《信息安全技术 术语》

GB/T 33474-2016 《物联网 参考体系结构》

GB/T AAAAA-AAAA 《信息安全技术 物联网安全参考模型及通用要求》

3 术语和定义

GB/T 25069-2010中界定的及下列术语和定义适用于本文件。

3.1 物联网 Internet of things

通过感知终端，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。

3.2 感知终端 perception terminal

能对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

3.3 传感器 transducer/sensor

能感受被测量并按照一定的规律转换成可用输出信号的器件或装置，通常由敏感元件和转换元件组成。

注1：GB/T 7665-2005定义了传感器的一般分类术语，其中从被测量角度定义了三类传感器，即物理量传感器、化学量传感器和生物量传感器。

3.4 传输安全 transmission security

保护网络中所传输信息的完整性、保密性、可用性及用户定制等特性。

3.5 完整性 integrity

保护资产准确性和完整的特征。

3.6 保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

3.7 可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

3.8 新鲜性 Freshness

对所接收的历史数据或超出时限的数据进行识别的特性。

3.9 隐私 privacy

个人所具有的控制或影响与之相关信息的权限，涉及由谁收集和存储、由谁披露

3.10 信任 trust

两个元素之间的一种关系：元素Z信任元素Y，当且仅当Z确信Y相对于一组活动，元素Y将以良好定义的方式实施，且不违反安全策略。

4 物联网数据传输安全概述

4.1 物联网数据传输安全模型

物联网安全参考模型从物联网系统参考安全区、系统生存周期、基本安全防护措施三个维度三个维度共同描述物联网安全保护方法。参考安全区是从物联网系统的逻辑空间维度出发，生存周期则是从物联网系统存续时间维度出发，配合相应的基本安全防护措施，在整体架构和全生命周期层面上为物联网系统提供了一套可参考的安全模型。物联网数据传输指在物联网获取信息及传输信息中使用到的数据传输技术集合，其传输安全涉及基本安全防护措施中的网络安全部分，物联网系统功能域的全部域间及域内数据传输，以及系统生命周期的全过程。本标准依据GB/T AAAAA-AAAA 中的物联网安全参考模型，给出了数据传输安全定位。

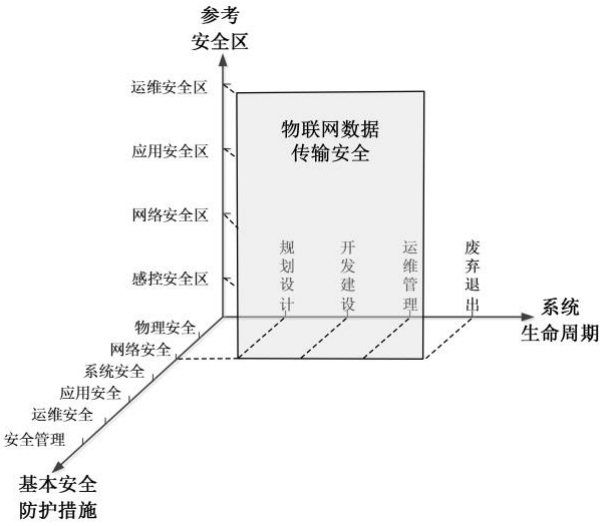

图1 物联网数据传输安全技术要求在物联网安全参考模型中的定位

4.2 安全防护范围

本标准提出的物联网安全防护范围主要是指在从设备采集数据开始到应用场景过程中，所使用的数据传输技术的集合，其用于向物联网数据传输提供安全保障以及安全性支持。

物联网数据传输安全防护范围具体包括：物联网系统功能域内、域间数据传输接口安全保障以及安全性支持，作用于系统全生命周期（规划设计、开发建设、运维管理、废弃退出）。依照物联网参考体系结构，涉及的通信接口包括CRAI-01—CRAI-24。将其分为通用网络接口、感知网域接口、感知网络接口三类（详见GB/T 33474-2016）。表1给出了物联网数据传输接口及其分类，图2给出了物联网数据传输接口的具体位置。

通用网络接口数据传输安全保障应满足通用网络安全要求，也可采纳本标准网络安全要求。

感知网域接口数据传输安全保障宜采纳本标准网络安全要求。

感知网络接口数据传输安全保障应满足本标准网络安全要求

表1 物联网数据传输接口及其分类

对象 / 对象	用户域	资源交换域	服务提供域	运维管控域	感知控制域	目标对象域
用户域	SRAI-24					
资源交换域	SRAI-20	--				
服务提供域	SRAI-19	SRAI-14 SRAI-15	SRAI-13			
运维管控域	SRAI-21	SRAI-16	SRAI-17 SRAI-18	SRAI-23		
感知控制域	SRAI-22	SRAI-12	SRAI-11	SRAI-10	SRAI-01 SRAI-02 SRAI-03 SRAI-04 SRAI-05 SRAI-06 SRAI-09	
目标对象域	--	--	--	--	SRAI-07 SRAI-08	--

注：白色方框表示通用网络接口，黄色方框表示感知网域接口，红色方框表示感知网络接口。

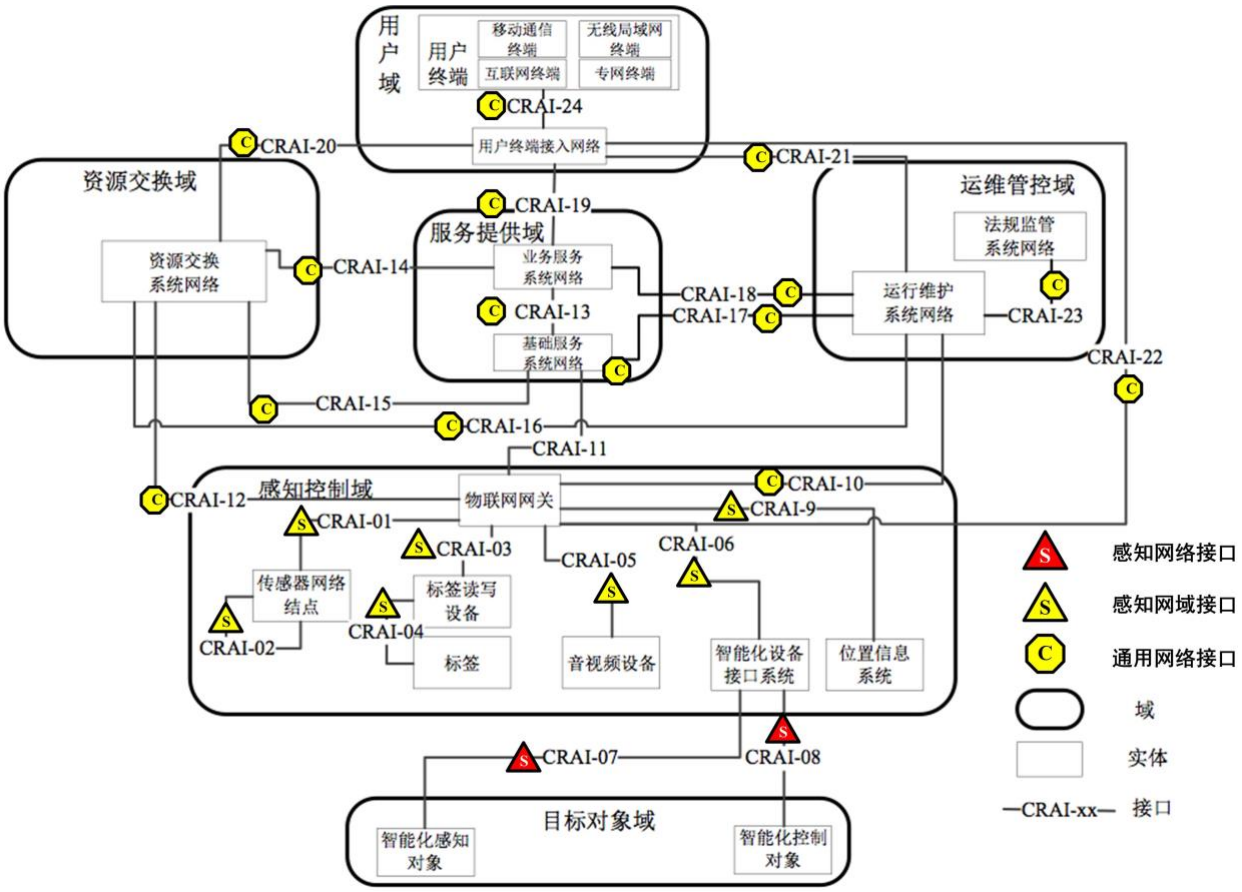

图2　物联网数据传输接口及其分类

4.3　安全分级原则

物联网数据传输安全技术要求分为基础级和增强级两类。处理一般性数据传输应满足基础级安全技术要求；处理重要数据、敏感数据，涉及重大安全问题的数据传输应满足增强级安全技术要求，或参考等级保护或其他相关标准中安全等级划分内容。

相对于基础级安全技术要求，增强级安全技术要求新增内容用宋体加粗字表示。

5　基础级安全技术要求

基础级主要针对着一般性数据传输场景下的应用，主要针对非加密环境下的安全问题。

5.1　数据传输完整性

数据传输共性要求如下：

a）传输时应支持信息完整性校验机制，实现管理数据、鉴别信息、隐私数据、重要业务数据等重要数据的传输完整性保护。（如：校验码、消息摘要、数字签名等）

b）应具有通信延时和中断处理功能，配合终端进行完整性保证。

5.2　数据传输可用性

宜保证数据传输时数据的新鲜性、准确性。具体包括：

1）新鲜性：数据来源与系统采用统一时间分配/矫正机制，数据中宜包含时间标识。
2）准确性：在数据存在可接受的误差时，可建立容错机制保障系统正常运行。

5.3 数据传输隐私

1）进行数据传输时，宜告知用户可能的隐私暴露环节，告知可能的隐私收集与存储部分。
2）需要时，对数据传输双方身份进行隐私保护。可采用数据脱敏算法等进行数据保护。

5.4 数据传输信任

宜保证对身份的信任，即在交互之前保证主体对客体的身份完全信任。

5.5 信息传输策略和程序

应建立正式的传输策略、程序和控制措施，以保护通过通讯设施传输的所有类型信息的安全。

5.6 信息传输协议

协议应解决组织外部方之间业务信息的安全传递。

5.7 保密或非扩散协议

应识别、定期评审并记录组织的保密或保密协议，该协议应反反映织对于信息保护的要求。

6 增强级安全技术要求

6.1 数据传输完整性

在满足5.1基础上，应满足如下要求：
1）对于重要数据来源，使用密码技术保证数据传输完整性。
2）在检测到完整性遭到破坏时采取措施用恢复或重新获取数据。

6.2 数据传输可用性

对于重要数据，在满足5.2基础上，应满足如下要求：
1）新鲜性：时间标识为加密字段。
2）准确性：在数据出现较大不可接受误差时，有重载机制保证数据正常获取。
3）对于重要数据，应使用部署的冗余感知终端通过专用传输通道进行采集，保证数据可用性。

6.3 数据传输保密性

1）对于重要数据、鉴别信息和重要业务数据应采用有一定强度的加密算法或其他有效措施对信息进行加密；
2）对发送方和接收方进行身份认证，在建立连接前，利用密码技术进行初始化会话验证；
3）必要时采用专用传输协议或安全传输协议服务，避免来自基于协议的攻击破坏保密性。

6.4 数据传输隐私

在满足 5.3 基础上，宜满足如下要求：
当需要时，允许用户进行隐私设置，按照用户自定义隐私，对其认为的隐私部分进行保护。

6.5 数据传输信任

在满足 5.4 基础上，宜满足如下要求：

对于重要环节，保证对行为的相对信任，即在交互过程中判断客体行为，保证主体对客体行为的相对信任。

6.6 信息传输策略和程序

在满足 5.5 基础上，宜满足如下要求：

1）策略和程序宜具有监控策略，监视非法连接。

2）策略和程序宜具有被管理员禁止的功能。

3）策略和程序应能够控制传输速率。

6.7 信息传输协议

在满足 5.6 基础上，宜满足如下要求：

1）协议应保证传输的机密性和完整性。

2）对于重要数据，协议应具有密码保护措施。

3）对于重要数据，宜使用隐蔽、随机化的传输协议。

6.8 保密或非扩散协议

在满足5.7基础上，宜满足如下要求：

对于重要数据、鉴别信息和重要业务数据应采用特殊的协议保护信息。

附　录　A
（规范性附录）
数据传输安全能力要求与自查表

A.1 数据传输安全能力要求

为实现基础级及增强级安全技术要求，如图3所示，可以根据身份、行为、能力三个属性做出等级评估及可能的属性划分。以方便使用者与普通、增强级做出对应并自查。

身份属性依据为身份完整性，具体包括硬件设备，引导程序，配置文件，操作系统。

行为依据为安全性（密钥信息、加密强度），可用性（资源占用率、带宽占用率、时间延迟），可靠性（丢包率、误码率、故障率）。

能力依据为安全能力，包括数据完整性保护能力，数据机密性能力，数据容错能力，数据泄露补救能力。

依据图3，表3给出了数据安全能力自查表。

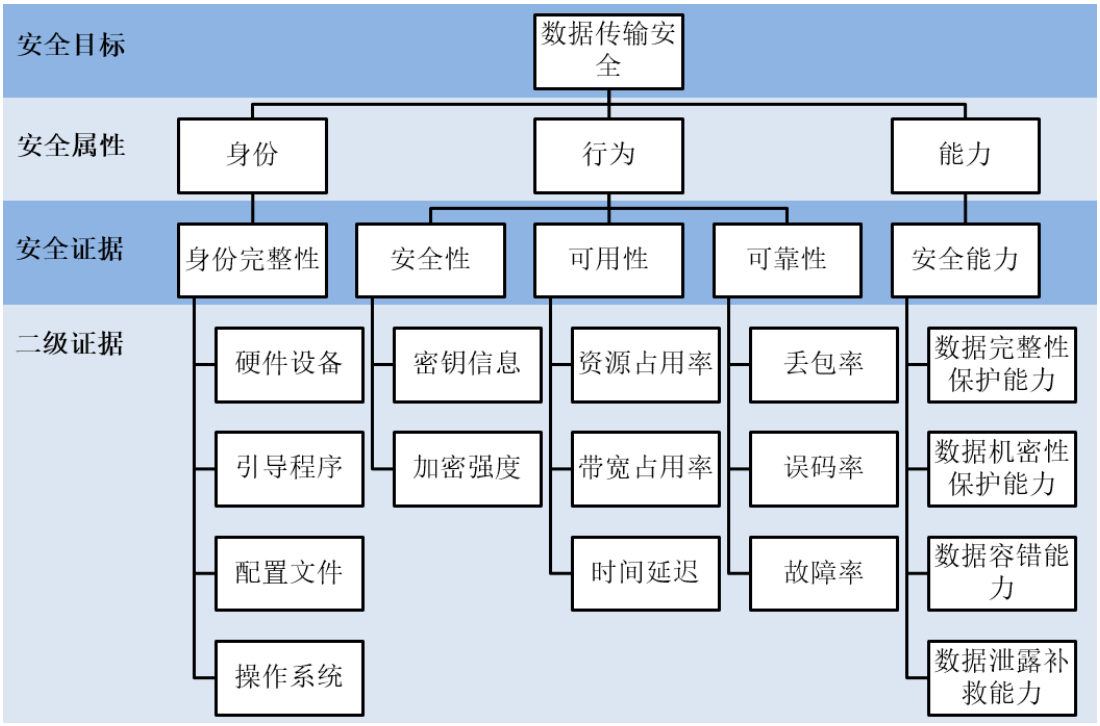

图3　安全属性参考图

A.2 数据传输安全能力自查表

表 2 数据传输安全能力要求与自查表

类	序号	安全能力要求	基础级	增强级
身份	1			
	2			
	3			
	4			
	注：“●”表示必须具备的功能项目；“○”表示不具备的功能项目。			
行为	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	注：“●”表示必须具备的功能项目；“○”表示不具备的功能项目。			
能力	1			
	2			
	3			
	4			
	注：“●”表示必须具备的功能项目；“○”表示可不具备的功能项目。			
综合评价				

附 录 B
（资料性附录）
物联网域模型与层模型的比较

物联网三层模型，如下图所示：

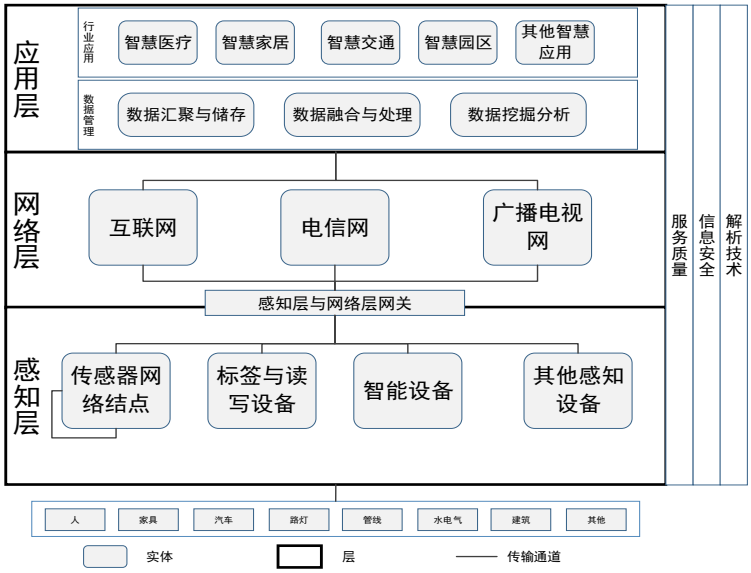

图4 物联网三层模型

三层传输模型与六域传输模型的简单对应关系如下图所示：

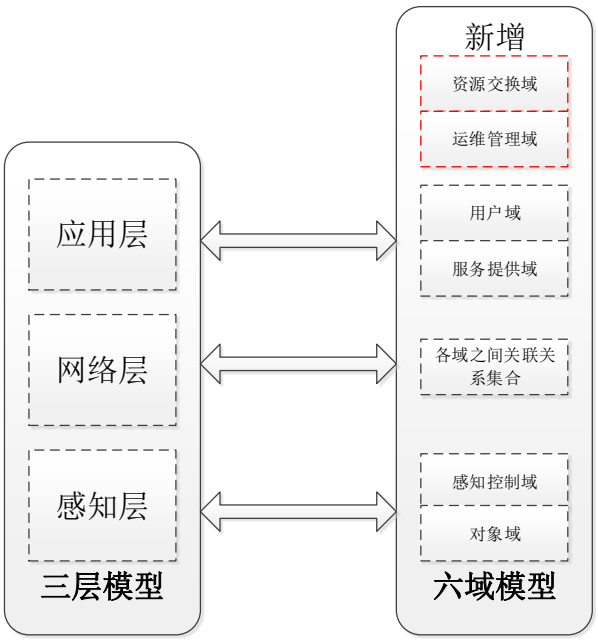

图5 三层模型及六域模型对应关系

参 考 文 献

[1]NIST SP 800-53R4 《Security and Privacy Controls for Federal Information Systems and Organizations》