ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术
物联网安全参考模型及通用要求

Information security technology -

Security reference model and generic requirements 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）

2016 年 12 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：中国电子技术标准化研究院、北京工业大学、国家信息技术安全研究中心、国家网络与信息系统安全产品质量监督检验中心、无锡物联网产业研究院。

本标准主要起草人：范科峰、杨震、李京春、龚洁中、李琳、赵章界、姚相振、周睿康、顾健、齐力、杨明、陈书义。

引 言

随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统，包括分布式控制系统（DCS）、监控与数据采集（SCADA）系统和可编程逻辑控制器（PLC）等产品广泛应用于核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等国家重要领域。工业控制系统（ICS）由单机走向互联、从封闭走向开放、从自动化走向智能化进程的加快，使得工业控制系统的信息安全问题日益突出，工业控制系统一旦遭受攻击，将严重威胁人民生命财产安全和国家政权稳定。对此，全国信息安全标准化技术委员会（SAC/TC 260）立项研制了工业控制系统信息安全分级、管理要求、控制应用指南等多项标准。

本标准针对各行业工业控制系统的安全管理活动的共性特点，提出了工业控制系统安全管理基本框架，从领导、规划、支持、运行、绩效评价和持续改进等方面为工业控制系统安全管理活动提出了规范性要求，并给出了为实现该安全管理基本框架所需的安全管理基本控制措施和各级工业控制系统安全管理基本控制措施对应表，以满足组织对各级工业控制系统的安全管理需求，为实现对工业控制系统适度、有效的安全管理控制提供参考。

信息安全技术 物联网安全参考模型及通用要求

1 范围

本标准规定了物联网安全参考模型，包括物联网安全对象、物联网安全架构和物联网安全措施，并针对物联网系统提出了安全通用要求。

本标准适用于物联网系统的建设、运行、维护和管理，并对其中的安全性提供基础性指导。

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 7665-2005 传感器通用术语

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

感知终端 perception terminal

物联网信息系统中能对物进行信息采集和/或执行操作，并能联网进行通信的装置。感知终端根据是否具有操作系统，可分为具有操作系统的感知终端和不具有操作系统的感知终端。

3.2

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。

4 物联网安全参考模型

4.1 参考模型

物联网安全参考模型从物联网安全对象、物联网安全架构和物联网安全措施三个维度描述物联网安全保护方法。物联网安全对象规范了物联网最终达到的安全目标，物联安全架构规范了安全技术防护体系，物联网安全措施规范了具体实施环节的安全要素。图1给出了物联网安全参考模型。

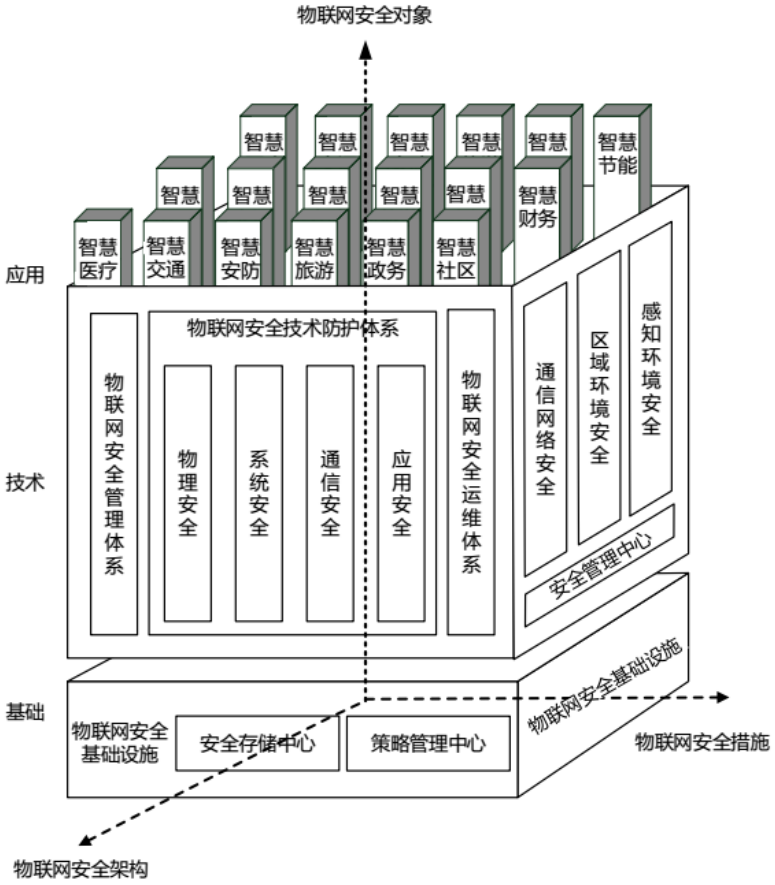

图1　物联网安全参考模型

4.2　物联网安全对象

物联网安全对象指物联网中所有实际应用，包括但不限于智慧医疗，智慧交通，智慧安防，智慧旅游，智慧政府，智慧社区，智慧家庭等。

4.3　物联网安全架构

物联网安全架构是从安全防护需求角度描绘物联网系统安全功能。物联网通过感知-传输-应用形成一个完整系统，并且在整个系统中包括多次数据预处理过程，通过满足基础设施安全和建立完善的防护体系来达到安全目标。

1）基础

物联网安全架构基础类指物联网安全基础设施，包括安全存储中心和策略管理中心。提供物联网系统需要的数据存储、数据处理、数据管理功能。

2）技术

安全架构中的技术指物联网安全防护体系。安全防护体系依照物联网系统模型，分为物理安全、系统安全、通信安全、应用安全、安全管理体系、安全运维体系。

4.4　物联网安全措施

物联网安全措施是从实际实施的角度描述物联网系统安全因素。在物联网系统实施过程中主要可分为几个环节，如图1“安全措施”维度所示。分为安全感知控制基础和各个环节的安全。

1）基础

安全基础主要指物联网安全基础措施，该措施具有基本的保护环境，能实现基本的安全功能。

2）技术

安全措施中的技术指在满足安全感知基础的前提下，在物联网实施的几个环节中，感知环境安全，感知边界安全，网络通信安全、应用环境安全和安全管理。

5 物联网安全通用要求

5.1 物理安全

物联网感知延伸层、网络/业务层和应用层由传感器等各类感知终端、路由器、交换机、计算机等物理设备组成，其物理安全是物联网安全的重要方面。

主要包括：

a）应制定物理设备的物理访问授权、控制等制度；

b）应具备可靠稳定的供电要求；

c）应具备防火、防盗、防潮、防雷和电磁防护等物理防护措施。

5.2 网络安全

物联网的网络部分包含通信网、互联网、行业专网等，具有网络异构化、多样化等特点，其安全要求主要包含接入安全和通信安全。

接入安全包括：

a）各类感知终端和接入设备在接入网络时应具备唯一标识；

b）对各类感知终端接入行为具有身份鉴别机制；

c）对于网络的访问控制采取禁用闲置端口、设置访问控制策略等防护手段

d）对于网关、防火墙等网络边界设备，需配置安全策略，具备加密功能和访问控制等防护措施；

通信安全包括：

a）物联网中的数据传输协议需有数据校验功能以确保数据传输的完整性

b）应采用标准化时间戳机制等技术确保数据传输的可用性

c）应采用技术手段对数据传输的隐私性进行保护；

d）在网络数据交互前，可采用认证等方式为交互双方身份的可信性提供证明；

e）可采用国家政策允许的加密算法对网络传输数据进行加密，确保信息的保密性；

f）物联网应具备防伪基站攻击、网络接力攻击的能力。

5.3 系统安全

对于物联网中存在的主机，应具备安全要求，包括：

a）对登录物联网中各系统的用户进行身份标识和鉴别；

b）应启用访问控制功能并制定相应安全策略；

c）应限制默认帐户的访问权限并及时更改默认账户及口令；

d）应对系统中多余、过期的账户，制定定期删除等管理制度；

e）物联网中的操作系统，应遵循最小安全原则；

f）及时更新补丁程序，应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

g）在使用中间件技术时，应确保其安全性。

5.4 应用安全

物联网的安全对象包括智慧医疗、智慧交通、智慧安防、智慧旅游等，在实际应用需要大量应用软件，采集大量数据，其安全要求包括：

a）应提供数据有效性检验功能，保证通过人机交互输入或通信接口输入的数据格式或长度符合系统设定要求；

b）应对涉及国家安全、社会公共秩序、公民个人隐私等的重要数据进行异地备份，以确保其安全。

5.5 运维安全

物联网是由多个子系统组成的复杂系统，其运行和维护通常由不同责任方负责开展，其安全要求包括：

a）物联网中不同责任方应根据其职责，在物联网系统建设时，对物联网设备和系统的获取做出规定，如规定设备和系统提供方的资质要求、可信赖性等、提供系统文档的详细程度，供应链的安全要求等；

b）对于物联网系统运行维护中的相关参与人员，应提出人员资质、身份审核、可信证明、诚信承诺等要求，以确保其在物联网系统维护过程中的安全可信；

c）应对物联网系统运维的时效性、维护工具等提出安全要求，对于远程维护设备的，应对远程维护制定安全守则。

5.6 安全管理

安全要求包括：

a）物联网系统在运行过程中，各子系统责任方应结合自身要求，制定安全管理策略规程；

b）应明确物联网系统不同设备责任人安全职责及其行为准则；

c）根据实际情况制定应急计划和配置管理策略；

d）必要时，可对物联网系统定期开展安全评估等工作。

附 录 A
（资料性附录）
物联网总体架构各层安全问题分析

A.1 物联网感知延伸层

物联网感知延伸层作为物联网和物理世界交互的边界，该层中的各种信息通信节点具有信息处理和通信能力。 物联网感知延伸层中各种信息通信节点的信息处理能力和安全能力强弱依赖于节点类型，如信息采集、标识读取、信息存储、根据网络指示执行特定动作等。需要建立对通信节点本身的安全机制，防止身份假冒，信息截取等常见攻击。保护物联网感知延伸层中各种信息通信节点所支持的通信手段可以有多种形式，如有线、无线、移动通信等方式，通常基于近距离通信技术，安全方面多采用轻量级安全手段。 物联网感知延伸层中各种信息通信节点之间可以直接交互，也可以连接到物联网网络/业务层，和物联网网络设备、应用服务器、其他感知延伸层节点设备进行所需的交互，每一次交互都需要不同的信息安全技术来保证整个感知延伸层的安全。

A.2 物联网网络/业务层

物联网网络/业务层主要提供消息的路由寻址和传送功能，可以基于现有或未来的各种网络技术，并可以有各种消息传送方式，如IP方式、短消息方式等。物联网可以是新构建的网络，或者是对现有网络进行功能扩展和能力增强。安全方面与现有网络类似。

物联网网络/业务层应能够获知物联网感知延伸层节点的通信状态。如果需要，物联网网络/业务层 可以提供到物联网感知延伸层节点的管理功能。

对于对消息传送的安全、可靠性、服务质量等有特殊的应用场景，物联网的网络核心应能够提供相应的机制满足要求。

如果需要，物联网网络/业务层可以向应用层提供必要和所需的能力支持，如网络能力开放、终端能力适配等。 物联网应支持与其他物联网之间的互联互通。 由于不同物联网应用对移动性、通信模式、鉴权、处理模式、数据速率、安全性、可靠性、交互性等业务交互特征和需求也存在很大差异，因此，物联网架构应具有智能和弹性，应能够通过充分利用各 种网络资源或通过能力增强，来满足不同物联网应用的服务需求，同时应能够实现网络资源和能力的共用。

物联网应具有扩展性，适应物联终端数量和业务种类的增加。

A.3 物联网应用层

典型的物联网应用包括：监控报警类、数据收集类、信息推送类、视频监控类、远程控制执行器类。从服务范围来看，物联网应用包括：公众服务、行业公众服务、行业专用服务。在应用层上，各自的软件系统，通信系统，数据库系统，管理系统等均需要一定安全手段进行保护，与现有方法类型。

参 考 文 献

[1] NIST SP 800-53 推荐的联邦信息系统和组织的安全控制措施