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 物联网感知层接入信息网络的安全技术要求

Information security technology——Security requirements for IoT sensing layer access to the information network

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：2016/12/30）

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

`XXX－XX－XX 发布　　XXXX－XX－XX 实施

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》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提出并归口。

本标准起草单位：公安部第三研究所、公安部安全防范报警系统质量监督检验测试中心、中兴通讯股份有限公司、中国联通网络通信股份有限公司、北京天融信网络安全技术有限公司。

本标准主要起草人：胡传平、杨明、齐力、唐前进、张艳、陶源、刘泽坤、高峰、夏俊杰、李建清、陈书义、龚洁中。

信息安全技术 物联网感知层接入信息网络的安全要求

1 范围

本标准规定了物联网感知层接入信息网络的结构，提出了其分级安全要求。

本标准适用于物联网系统工程中的信息网络接入系统的信息安全设计、选型和系统集成。也适用于感知层网络及设备接入信息网络的安全功能设计、开发和选型。

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 18794.2-2002 信息技术 开放系统互连 开放系统安全框架 第2部分：鉴别框架

GB/T 25069-2010 信息安全技术 术语

GB/T 32905-2016 信息安全技术 SM3密码杂凑算法

GB/T 32907-2016 信息安全技术 SM4分组密码算法

GB/T 32918.2-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

3 术语和定义

GB/T 25069-2010和GB/T 18794.2-2002界定的以及下列术语和定义适用于本文件。

3.1

物联网感知层 sensing layer of IOT

在物联网三层架构中，通过有线、近距离（近场/短程）无线等通信技术实现感知终端与网络层互联的网络层次，它一般包含感知终端和网络设备等通信实体，并与网络层之间进行信息交互。

3.2

信息网络 information network

收集、融合和处理物联网感知信息数据，并形成相关应用的计算机设备和网络。

3.3

感知层接入信息网络 sensing layer access to the information network

物联网系统的感知设备、感知数据通过中间链路接入到专用信息化IP网络的过程。

3.4

物联网感知终端 sensing terminal of IoT

能够采集物理信息和/或接受控制信号，并通过有线/无线通信方式向信息网络发起数据传输的设备。

3.5

物联网(感知层)网关 sensing layer gateway of IoT

部署在物联网感知终端与感知信息传输网络之间的一种网络连接设备。

3.6

感知层实体 sensing layer entity

处于物联网感知层中，与信息网络进行数据通信的设备。

示例：感知终端、感知层网关等。

3.7

接入系统 access system

部署在物联网系统的信息网络与感知信息传输网络之间,用于实施感知信息接入信息网络的信息安全技术的设备和网络的集合体。

3.8

密钥材料 secrete material

指的是用于支撑加密算法运行和信息安全机制的预共享密钥，加密方式，加密参数等内容的统称。

3.9

数据新鲜性 freshness of data

保证数据发送和接收的时效性，确保数据的传输没有被重放。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control List）

ID：身份标识号码（Identity）

IP：互联网协议（Internet Protocol）

MAC：媒体访问控制（Media Access Control）

VPN：虚拟专用网络（Virtual Private Network）

5 概述

5.1 物联网感知层接入信息网络结构

物联网感知层接入信息网络的结构，如图 1 所示，其示例参见附录 A。结构包含从物联网感知终端到信息网络的通信链路，其中主要的实体对象包括：

a) 物联网感知终端；

b) 物联网（感知层）网关：

c) 感知信息传输网络（有线/无线）；

d) （信息网络）接入系统；

e) 信息网络。

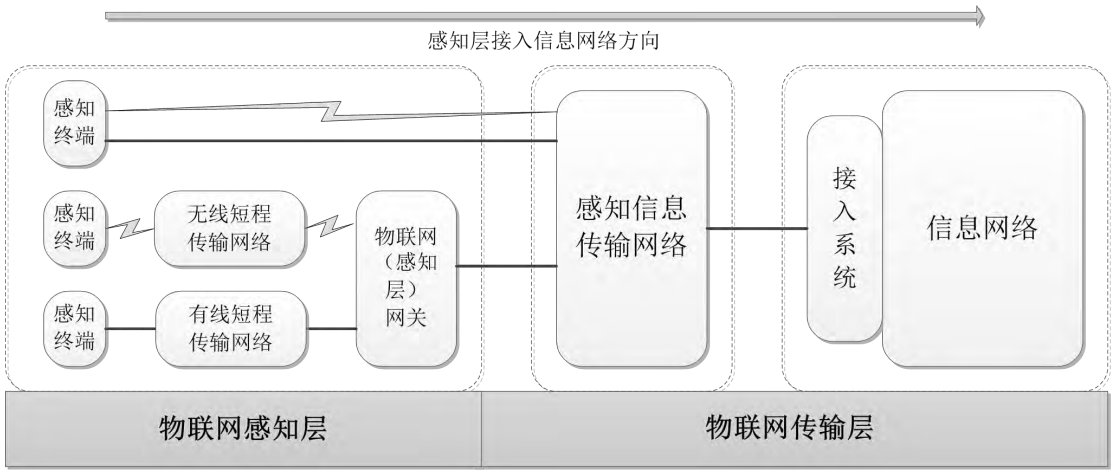

图 1 感知层接入信息网络结构

5.2 接入信息安全结构

物联网感知层接入信息网络的安全结构由感知层边界、信息网络边界和感知信息传输网络构成，如图2所示，包括以下要求：

a）信息网络接入系统安全技术要求；

b）感知信息传输网络安全技术要求；

c）感知层接入安全技术要求。

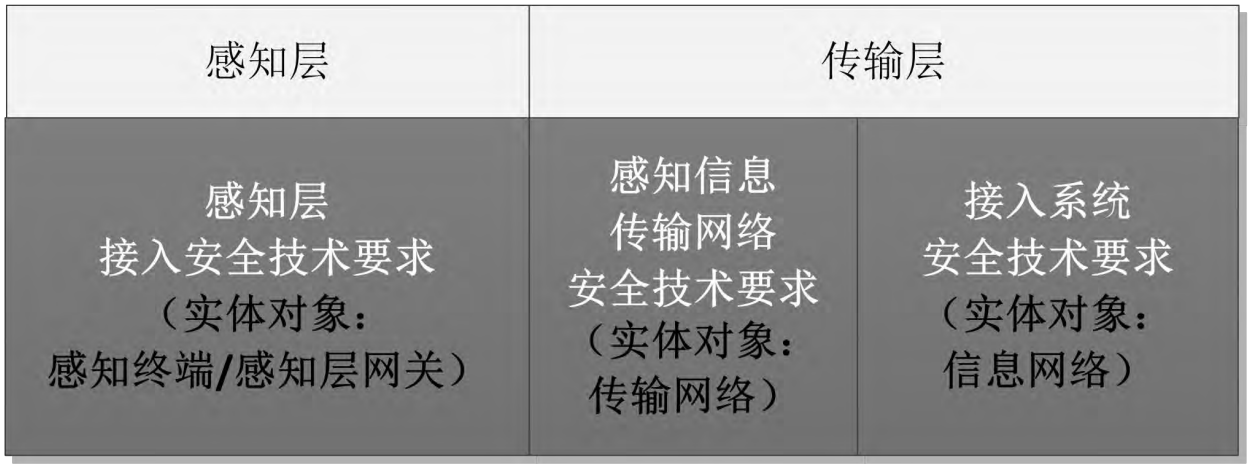

图 2 感知层接入信息网络的信息安全结构

5.3 安全要求分级说明

物联网感知层接入信息网络是连接感知终端和信息网络构成物联网应用的中间通路和环节。本标准按照感知层接入信息网络的安全功能强度，划分为基本级和增强级两个等级的技术要求。

注：本标准文本中，加粗字体表示基本级中没有出现且增强的技术要求。

6 信息网络接入系统安全技术要求

6.1 基本级要求

6.1.1 设备标识

信息网络接入系统（以下简称接入系统）中的设备应具备可用于通信识别的物联网系统中的唯一标识。

示例：设备ID、序列号、MAC地址等。

6.1.2 鉴别/认证

6.1.2.1 接入认证机制

接入系统应具备对感知层实体接入信息网络的鉴别/认证，并至少支持下列方式的一种：

a) 基于感知层实体标识和接入口令的单向认证；
b) 基于预共享密钥的单向或双向认证。

6.1.2.2 认证失败处理

接入系统应具备感知层实体接入认证失败的处理能力，并满足以下要求：

a) 当认证超时，接入系统应能终止与待接入感知层实体之间的当前会话；
b) 在经过一定次数的鉴别失败以后，接入系统应能终止由该感知层实体发起的建立会话的尝试，并在一定的安全时间间隔后才能恢复。

6.1.3 访问控制

接入系统宜支持感知层实体对信息网络的访问控制机制和安全策略，并满足以下要求：

a) 通过 ACL 方式控制感知层实体对信息网络的访问；
b) 支持制定和执行访问控制策略的功能，访问控制策略可以是基于 IP 地址、用户/用户组、读/写等操作的一种或多种的组合；
c) 支持黑名单制，阻断相关感知层实体对信息网络的访问。

6.1.4 路由安全支持要求

接入系统宜具备感知层实体接入路由的判别功能，并宜支持路由安全策略。

6.1.5 数据传输安全

接入系统应具备感知层实体与信息网络间的数据传输安全保障功能，并满足以下要求：

a) 数据完整性，支持数据完整性校验通信机制，宜采用国家规定的密码算法；
注：音视频数据除外。
b) 数据新鲜性，支持包含时间序列的数据信息，宜采用防篡改技术保护数据信息中的时间序列。

6.1.6 密钥管理

接入系统宜具备与感知层实体的通信密钥的管理功能，并满足以下要求：

a) 创建、存储、删除、更新接入和会话密钥及密钥材料；
b) 接入系统采用离线分发或旁路分发方式将预共享密钥和密钥材料分配至感知层接入实体。

6.1.7 隔离防护

接入系统宜具备感知层实体与信息网络之间的隔离防护功能。

6.1.8 入侵防护

接入系统应具备对感知层实体接入的防护能力，并满足以下要求：

a) 最小化开放应用指定的 IP 地址和端口；

b) 拒绝和丢弃不可鉴别的感知层实体发来的数据；

c) 支持通信协议和数据格式匹配的数据包过滤，并丢弃不符合过滤要求的数据包。

6.1.9 日志与审计

接入系统应对以下感知层实体接入安全事件进行日志和审计，日志内容应至少包含日期/时间、事件类型、事件主体、事件描述，成功/失败的信息，并满足以下要求：

a) 感知层实体的接入认证超时和失败；

b) 感知层实体的在线监测数据异常。

6.2 增强级要求

6.2.1 设备标识

接入系统中的设备应具备可用于通信识别的物联网系统中的唯一标识，**并且该标识具备硬件防篡改保护。**

6.2.2 鉴别/认证

6.2.2.1 接入认证机制

接入系统应具备对感知层实体接入信息网络的鉴别/认证，**并至少包括基于感知层实体标识和接入口令的单向认证，以及以下方式中的一种：**

a) 基于预共享密钥的双向认证；

b) 基于公钥基础设施的接入认证。

6.2.2.2 认证失败处理

同6.1.2.2

6.2.3 访问控制

接入系统**应**支持感知层实体对信息网络的访问控制机制和安全策略，并满足以下要求：

a) 通过 ACL 方式控制感知层实体对信息网络的访问；

b) 支持制定和执行访问控制策略的功能，访问控制策略可以是基于 IP 地址**及端口**、用户/用户组、读/写等操作、**有效时间周期、敏感标记等的两种以上构成的组合；**

c) 支持黑名单制，阻断相关感知层实体对信息网络的访问。

6.2.4 路由安全支持要求

接入系统**应**具备感知层实体接入路由的判别功能，并**应**支持路由安全策略。

6.2.5 数据传输安全

接入系统应具备感知层实体与信息网络间的数据传输安全保障功能，并满足以下要求：

a) **数据保密性，支持数据加密，应采用国家规定的对称密码算法；**

示例：sm1、sm4等算法[GB/T 32907-2016]。

b) 数据完整性，支持数据的完整性校验通信机制，**应采用国家规定的摘要、签名等密码算法及组合算法；**

示例：sm3等算法[GB/T 32905-2016]。

c) **数据真实性，支持数据的来源鉴别，应采用国家规定的签名密码算法及组合算法；**
示例：sm2等算法[GB/T 32918.2-2016]。

d) 数据新鲜性，支持包含时间序列的数据信息和**信息验证，应采用加密方式保护数据信息中的时间序列。**

6.2.6 密钥管理

接入系统**应**具备与感知层实体的接入和会话密钥的管理功能，并满足以下要求：

a) 创建、存储、删除、更新接入和会话密钥及密钥材料，**密钥存储应具备访问控制和基于可信计算的加密保护；**

b) 接入系统**应采用离线分发方式**将预共享密钥和密钥材料分配至感知层接入实体；

c) 密钥管理支持多级生成和更新机制，主密钥的管理应支持密钥更新和注销安全策略。
注：多级密钥指的是包含由一种密钥生成另一种密钥的安全机制，如：主密钥-会话密钥-临时密钥之间可由一个生成另一个。

6.2.7 隔离防护

接入系统应具备实体与信息网络之间的隔离防护功能，**应支持协议隔离或物理隔离，并采用网闸设备**对位于高等级安全域的信息网络进行防护。

6.2.8 入侵防护

接入系统应具备对感知层实体接入的防护能力，并满足以下要求：

a) 最小化开放应用指定的 IP 地址和端口；

b) 拒绝和丢弃不可鉴别的感知层实体发来的数据；

c) 支持通信协议和数据格式匹配的数据包过滤，并丢弃不符合过滤要求的数据包；

d) 支持对恶意攻击和异常行为的检测，并具备入侵报警功能；

e) 支持病毒/木马的防护功能。

6.2.9 日志与审计

接入系统应对以下感知层实体接入安全事件进行日志和审计，日志内容应至少包含日期/时间、事件类型、事件主体、事件描述，成功/失败的信息，并满足以下要求：

a) 感知层实体的接入认证的超时和失败；

b) 感知层实体的在线监测数据异常；

c) 恶意、异常数据、病毒、木马程序的入侵警报事件。

7 感知信息传输网络安全技术要求

7.1 基本级要求

感知信息传输网络应满足以下安全要求：

a) 使用有线连接的传输网络时，宜采用网络逻辑隔离技术或专用通道；

b) 使用无线连接的传输网络时，宜使用信道加密技术。

7.2 增强级要求

感知信息传输网络应满足以下安全要求：

a) 使用有线连接的传输网络时，**应采用 VPN 信道加密技术或专用通道；**

b) 使用无线连接的传输网络时，**应使用信道加密技术。**

8 感知层接入安全技术要求

8.1 基本级要求

8.1.1 感知层实体标识

感知层实体应具备可用于通信识别的物联网系统中的唯一标识。

8.1.2 接入鉴别/认证支持功能

感知层实体接入信息网络，应满足以下对应接入系统的鉴别/认证支持功能：

a) 应支持符合 6.1.2.1 a)要求的实体标识、口令等的存储和管理功能；

b) 应支持符合 6.1.2.1 b)要求的预共享密钥的存储和管理功能；

c) 应支持符合 6.1.2.2 要求的认证失败处理机制。

8.1.3 感知层实体访问控制

感知层实体应具备访问控制机制，并满足以下要求：

a) 支持 ACL 列表实现访问控制；

b) 支持基于感知层实体用户/用户组的访问控制，支持用户访问控制策略。

8.1.4 感知数据传输安全支持

感知层实体应支持感知数据传输安全功能，并满足以下要求：

a) 支持符合 6.1.5 a)要求的数据完整性校验；

b) 支持符合 6.1.5 b)要求的时间序列信息生成和传输机制。

8.1.5 接入密钥管理支持

感知层实体宜支持接入密钥管理安全机制，并满足以下要求：

a) 支持生成、存储、更新接入和会话密钥及密钥材料；

b) 支持存储、更新预共享密钥和密钥材料的功能，并支持密钥离线接收和旁路接收。

8.1.6 感知层入侵防护

感知层实体应具备接入应用的入侵防护功能，并满足以下要求：

a) 仅开放应用相关的通信端口；

b) 拒绝和丢弃不可鉴别的信息网络通信数据。

8.1.7 感知层实体日志与审计

感知层实体应对以下接入信息网络的安全事件进行日志和审计，日志内容应至少包含日期/时间、事件类型、事件主体、事件描述，成功/失败的信息，并满足以下要求：

a) 感知层实体的接入认证失败；

b) 感知层实体的访问用户登录失败。

8.2 增强级要求

8.2.1 感知层实体标识

感知层实体应具备可用于通信识别的物联网系统中的唯一标识，**并且该标识具备硬件防篡改保护。**

8.2.2 接入鉴别/认证支持功能

感知层实体接入信息网络，应满足以下对应接入系统的鉴别/认证支持功能：

a) 应支持实体标识和接入口令等的存储和管理功能；

b) 应支持符合 6.2.2.1 a)要求的预共享密钥的存储和管理功能；

c) 应支持符合 6.2.2.1 b)要求的基于公钥基础设施的证书、密钥等的存储和管理功能；

d) 应支持符合 6.1.2.2 要求的认证失败处理机制。

8.2.3 感知层实体访问控制

同8.1.3要求。

8.2.4 感知数据传输安全支持

感知层实体应支持感知数据传输安全功能，并满足以下要求：

a) 支持符合 6.2.5 a)要求的数据加密功能；

b) 支持符合 6.2.5 b)要求的数据完整性验证功能；

c) 支持符合 6.2.5 c)要求的数据真实性验证功能；

d) 支持符合 6.2.5 d)要求的时间序列信息生成和传输加密机制。

8.2.5 接入密钥管理支持

感知层实体应支持接入密钥管理安全机制，并满足以下要求：

a) 支持生成、存储、更新接入和会话密钥及密钥材料；

b) 支持存储、更新预共享密钥和密钥材料的功能，并支持密钥离线接收；

c) 支持多级密钥的生成和更新安全机制，主密钥的管理应支持密钥更新和注销安全策略。

d) 密钥的存储应具备访问控制和基于可信计算的加密保护。

8.2.6 感知层入侵防护

感知层实体应具备接入应用的入侵防护功能，并满足以下要求：

a) 仅开放应用相关的通信端口；

b) 拒绝和丢弃不可鉴别的信息网络通信数据；

c) 支持通信协议和数据格式匹配的数据包过滤，丢弃不符合过滤要求的数据包；

d) 支持终端的恶意攻击、病毒/木马入侵检测，并具备报警功能；

e) 支持物理拆卸报警功能。

8.2.7 感知层实体日志与审计

感知层实体应对以下接入信息网络的安全事件进行日志和审计，日志内容应至少包含日期/时间、事件类型、事件主体、事件描述，成功/失败的信息，并满足以下要求：

a) 感知层实体的接入认证失败；

b) 感知层实体的访问用户登录失败。

c) 感知层实体入侵、拆卸等报警。

附 录 A
（资料性附录）
典型应用示例

A.1 有线网络接入类应用案例

A.1.1 概述

有线网络接入类应用是指物联网感知层网络主要以有线或总线方式连接传感器终端或控制设备，再由感知层网关或管理计算机接入通信网的应用模式。其典型系统图如图 A.1 所示。

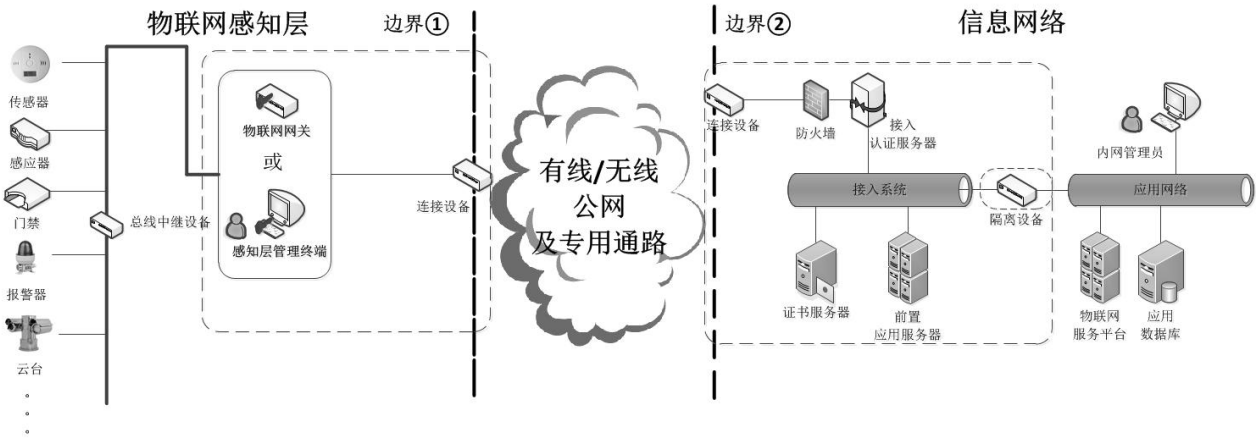

图 A.1 总线类感知应用安全接入系统示意图

有线总线接入类的典型应用包括：安防系统 485 总线控制的各类安防传感器，工业总线控制的各种机械自动化系统传感器应用等。这些总线控制类感知层网络大多处于较长距离总线或环路内，远程应用系统通过 IP 网络和连接总线的物联网网关或计算机（控制总线的设备），获取终端感知信息或执行控制。

总线连接的感知层网络，一般使用特定的数据传输/控制协议与终端设备进行通信，由于入侵设备可以通过挂载/接入总线的方式探测总线数据，并对其他设备进行控制和干扰，所以存在感知层安全问题；又由于其物联网应用主要通过 IP 网络来远程控制总线终端的工作模式存在接入安全问题。因此，其接入通信网的安全性有必要遵循本标准进行设计和管理。

A.1.2 安全接入应用模式

总线类感知应用系统的安全接入，分别在边界①和边界②的物联网网关和信息网络接入系统上部署实现，边界①部署满足本文件第 8 章要求的感知层实体支持功能，边界②部署满足本文件第 6 章要求的安全接入系统安全功能。

实际应用中可以根据基本级或增强级要求，通过分别在边界①部署物联网网关或感知层管理计算机，边界②中部署包含防火墙、接入认证服务器、证书服务器、前置应用服务器、隔离设备等，并在增强级要求时在两个边界的中间采用二层公网专用通道，如：VPDN、APN 等实现感知层与通信网的安全接入。

A.2 短程无线网络类应用案例

A.2.1 概述

短程无线网络类应用是指物联网感知层网络主要以短程无线通信方式互联形成自组织传感/控制网

络，再由感知层网关接入通信网的应用模式。其典型系统图如图 A.2 所示。

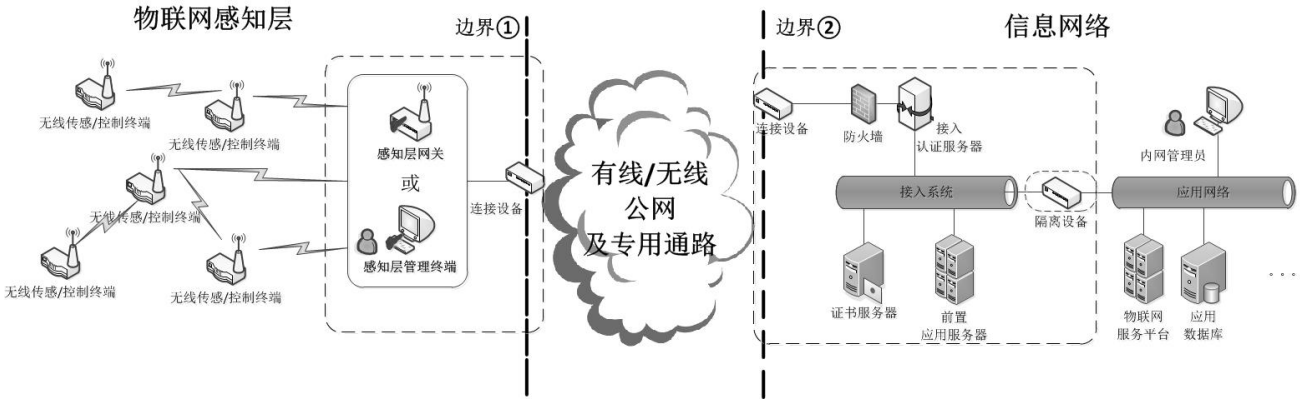

图 A.2 短程无线通信网络安全接入系统示意图

短程无线通信类的典型应用包括：用于监测、监控的无线传感网，无线工业自动化传感和控制、无线抄表等。这些应用的感知层环境都属于开放式的，在通信网内可以利用远程应用系统通过 IP 网络和感知层数据汇聚网关，获取终端感知信息或执行控制。

短程无线通信类感知层网络，一般使用自组织的无线组网和通信协议，入侵设备可以通过开放式的无线环境进行窃听、伪造数据，劫持终端等攻击方式来威胁基础设施的运行安全。因此，其接入通信网的安全性有必要遵循本标准进行设计和管理。一方面保障通信网内应用系统的安全，另一方面保障感知层网络的通信安全。

A.2.2 安全接入应用模式

短程无线通信类应用系统的安全接入，分别在边界①和边界②的物联网网关和信息网络接入系统上部署实现，边界①部署满足本文件第 8 章要求的感知层实体支持功能，边界②部署满足本文件第 6 章要求的安全接入系统安全功能。

实际应用中可以根据基本级或增强级要求，通过分别在边界①部署物联网网关或感知层管理计算机，边界②中部署包含防火墙、接入认证服务器、证书服务器、前置应用服务器、隔离设备等，并在增强级要求时在两个边界的中间采用二层公网专用通道，如：VPDN、APN 等实现感知层与通信网的安全接入。

A.3 有线/无线宽带接入类应用案例

A.3.1 概述

有线/无线宽带接入类应用是指物联网感知层终端主要通过互联网、宽带移动互联网、特定频段无线专网等接入通信网的应用模式。其典型系统图如图 A.3 所示。

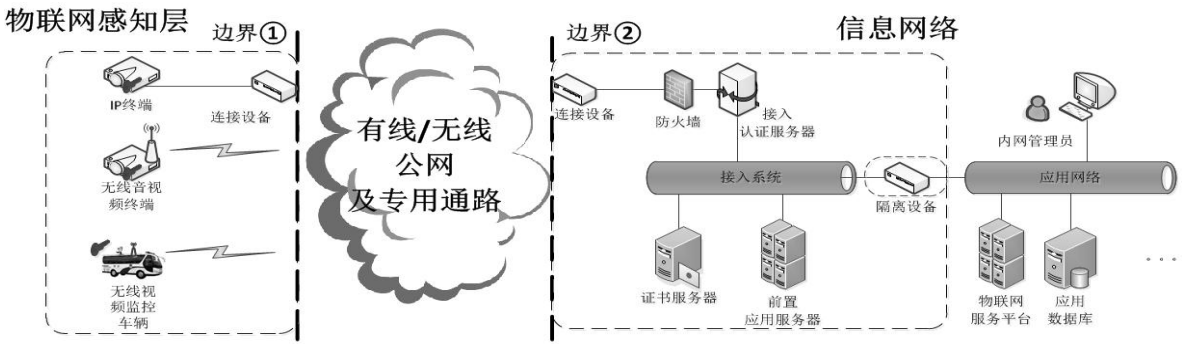

图 A.3 有线/无线终端宽带安全接入系统示意图

有线/无线宽带接入类典型应用包括：有线/无线音视频监控、现场事件应急反馈、车联网信息交互、区域安防等。利用有线/无线公网或专用宽带网络是展开这些应用的基础，在通信网内一般利用远程应用系统通过有线/无线公网或专用网络直接访问感知层终端，从而获取感知数据信息或进行通信和控制。

有线/无线宽带接入类应用网络，一般使用有线/无线公网，应用系统容易受到来自公网的威胁，从而使得敏感数据信息泄露。因此，其接入通信网的安全性应遵循本标准进行设计和管理。保障通信网应用系统的安全和感知终端的应用安全。

A.3.2 安全接入应用模式

有线/无线宽带接入类应用系统的安全接入，分别在边界①和边界②的物联网网关和信息网络接入系统上部署实现，边界①部署满足本文件第 8 章要求的感知层实体支持功能，边界②部署满足本文件第 6 章要求的安全接入系统安全功能。

实际应用中可以根据基本级或增强级要求，通过分别在边界①部署物联网网关或感知层管理计算机，边界②中部署包含防火墙、接入认证服务器、证书服务器、前置应用服务器、隔离设备等，并在增强级要求时在两个边界的中间采用二层公网专用通道，如：VPDN、APN 等实现感知层与通信网的安全接入。

A.4 RFID 通信接入类应用案例

A.4.1 概述

RFID 通信类接入应用是指由 RFID 读卡设备通过感知层网关接入通信网或（移动）终端式读写设备直接接入通信网的应用模式。其典型系统图如图 A.4 所示。

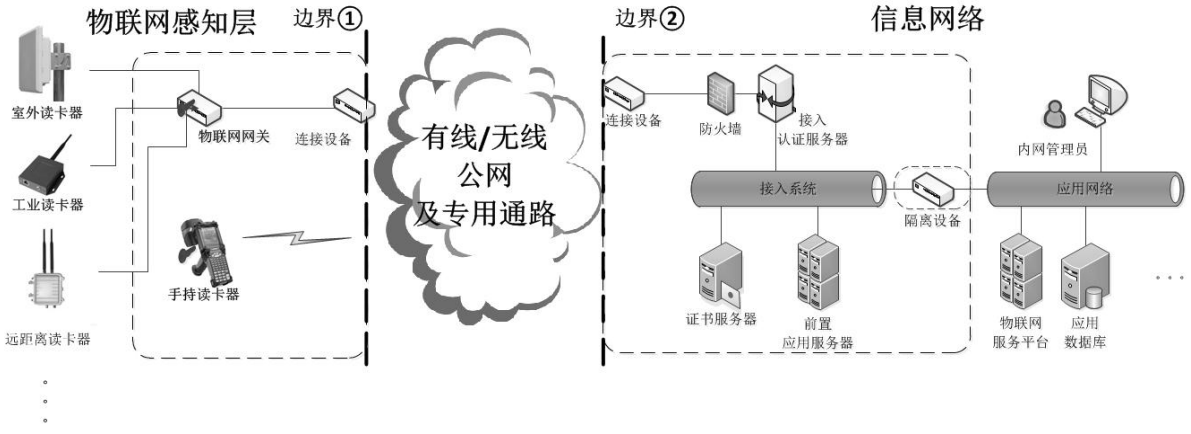

图 A.4 RFID 通信类安全接入应用系统示意图

RFID 通信类的典型应用包括：票证查询、物资管理、电子车牌，小区巡更等。这些应用分为两种感知层接入通信网的模式，一种是读写终端通过连接到感知层网关接入通信网，另一种是读卡终端直接接入通信网。RFID 读写终端的数据可靠性将影响整个应用系统的安全性，RFID 读写终端在感知层开放网络中容易被控制或假冒。因此，其接入通信网的安全性有必要遵循本标准进行设计和管理。

A.4.2 安全接入应用模式

RFID 通信接入类应用系统的安全接入，分别在边界①和边界②的物联网网关和信息网络接入系统上部署实现，边界①部署满足本文件第 8 章要求的感知层实体支持功能，边界②部署满足本文件第 6 章要求的安全接入系统安全功能。

实际应用中可以根据基本级或增强级要求，通过分别在边界①部署物联网网关或感知层管理计算机，边界②中部署包含防火墙、接入认证服务器、证书服务器、前置应用服务器、隔离设备等，并在增强级要求时在两个边界的中间采用二层公网专用通道，如：VPDN、APN 等实现感知层与通信网的安全接入。

A.5 个域网/终端接入类应用案例

A.5.1 概述

个域网/终端接入类应用是指是由个人智能终端为代表的通信网接入应用模式。其中个人智能终端是接入的主要终端设备，而其连接的有线/无线读卡器、打印机、摄像头、传感器等是感知/控制终端。其典型系统图如图 A.5 所示。

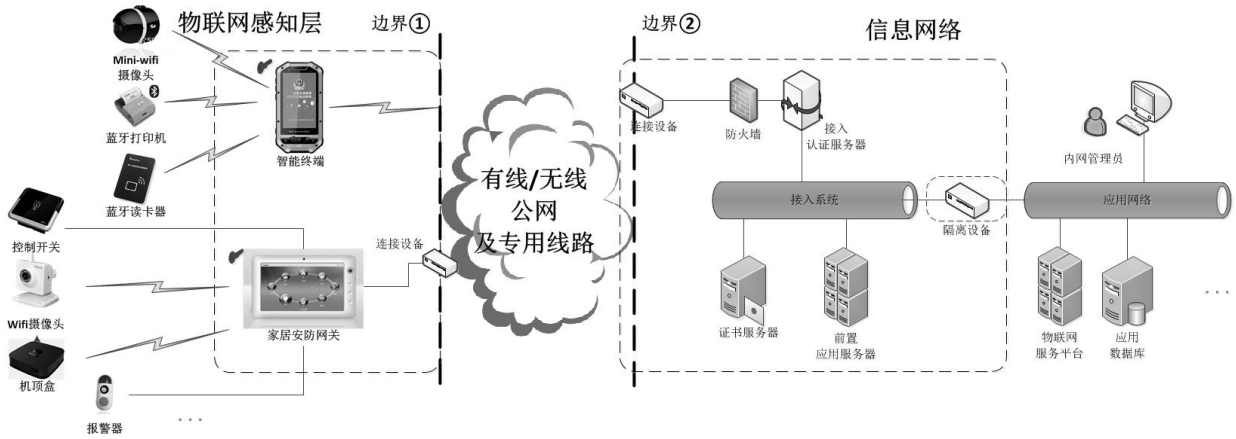

图 A.5 个域网终端安全接入应用系统示意图

个域网终端接入的典型应用包括：数字化单兵/单警系统、智能家居等。其个域网网关或终端是系统应用安全接入的关键点，容易被仿冒、伪造及受到未授权的远程控制，从而造成严重的应用系统安全威胁。因此，其接入通信网的安全性有必要遵循本标准进行设计和管理。

A.5.2 安全接入应用模式

个域网终端的安全接入，分别在边界①和边界②的物联网网关和信息网络接入系统上部署实现，边界①部署满足本文件第 8 章要求的感知层实体支持功能，边界②部署满足本文件第 6 章要求的安全接入系统安全功能。

实际应用中可以根据基本级或增强级要求，通过分别在边界①部署物联网网关或感知层管理计算机，边界②中部署包含防火墙、接入认证服务器、证书服务器、前置应用服务器、隔离设备等，并在增强级要求时在两个边界的中间采用二层公网专用通道，如：VPDN、APN 等实现感知层与通信网的安全接入。

参 考 文 献

[1] GB/T 20269-2006 信息安全技术 信息系统安全管理要求

[2] GB/T 20270-2006 信息安全技术 网络基础安全技术要求

[3] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

[4] GB/T 22239-2008 信息系统安全等级保护基本要求

[5] GB/T 22240-2008 信息系统安全等级保护定级指南

[6] GB/T 25068.1-2012 信息技术 安全技术 IT网络安全 第1部分：网络安全管理

[7] GB/T 25068.2-2012 信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构

[8] GB/T 25068.3-2010 信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护

[9] GB/T 25068.4-2010 信息技术 安全技术 IT网络安全 第4部分：远程接入的安全保护

[10] GB/T 25068.5-2010 信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护

[11] GB/T 29240-2012 信息安全技术 终端计算机系统安全等级技术要求

[12] 《商用密码产品使用管理规定》（国家密码管理局 2007年5月）