ICS 35.040
L 80

T/CCSCIOT

无锡“感知中国”物联网商会 团体标准

T/CCSCIOT 0002—2020

物联网 智慧社区安防系统安全要求

Security and protection system requirements for IoT smart communities

2020－11－26 发布　　2020－12－01 实施

无锡“感知中国”物联网商会　　发布

目　次

前　言

本标准按照GB/T　1.1-2020给出的规则起草。

本标准由无锡“感知中国”物联网商会提出并归口。

本标准起草单位：无锡市物联网产业协会、公安部第三研究所、无锡可信智慧安全技术研究院有限公司、无锡物联网产业研究院、江南大学、江苏西维斯信息技术有限公司、中兴智能交通股份有限公司、阿里云计算有限公司。

本标准主要起草人：杨明、谈伟中、许晓晨、周文宇、姚健、钱鹏江、蒋亦樟、费钧、夏朝彬、孙万源。

物联网　智慧社区安防系统安全要求

1　范围

本文件确立了智慧社区安防系统的感知终端、感知层网关、感知通信网络、安防信息平台等的安全技术要求。

本文件适用于社区物联网安防系统的设计、集成、运维和管理。

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/T　25069-2010　信息安全技术　术语

GB/T　36951-2018　信息安全技术　物联网感知终端应用安全技术要求

GB/T　37093-2018　信息安全技术　物联网感知层接入通信网的安全要求

3　术语和定义

3.1

安防感知终端　Sensor terminals of security and protection systems

用于采集智慧社区安防信息的物联网感知终端。

示例：监控摄像头、电子围栏、烟雾传感器、温湿度传感器、红外探测器、车位感应器、出入门禁等。

3.2

物联网安防系统　IoT security and protection systems

由物联网感知终端、通信网络和信息平台等所组成的安防信息系统。

3.3

安防信息平台　Security and protection information platform

用于社区安防信息汇聚、处理、可视化展现，以及安防终端管理和维护的软硬件平台。

3.4

安防感知层网关　Security and protection sensor layer gateway

用于智慧社区安防短程通信网络内数据汇聚和向安防信息平台转发的感知层网络设备。

3.5

网络报警　Network alarm

通过网络实现安防系统与公共安全报警系统连接，并产生和发送告警信息的过程。

3.6

敏感信息 Sensitive information

需要保护的信息，该信息的泄漏、修改、破坏或丢失都会对用户产生不可预知的损害。敏感信息包含但不限于安防系统用户口令、通信密钥、个人隐私信息等。

3.7

安全通信机制 Secure communication mechanisms

包含有实体鉴别、数据加解密、完整性验证、防篡改等技术保障措施的通信协议体。

3.8

物联网卡 IoT SIM cards

由物联网通信运营商发售，装置在物联网终端或网关上，用于物联网通信标识和网络流量计费的安全芯片卡。

3.9

物联网安全管控平台 IoT security management and control platform

以数据服务为基础的，用于管理和控制物联网应用安全的综合性信息业务平台。

4 缩略语

下列缩略语适用于本文件。

ID：身份标识（Identity）
IP：互联网协议（Internet Protocol）
MAC：媒体访问控制（Media Access Control）
SIM：用户识别模块（Subscriber Identity Module）
VPN：虚拟专用网络（Visual Private Network）
IoT：物联网技术（Internet of Things）
ACL：访问控制列表（Access Control List）

5 概述

5.1 社区安防系统结构

本标准规范的对象为智慧社区安防系统，其系统结构见图1。系统中的实体包括：

a） 安防感知终端（短程或公网感知终端），以下简称终端；
b） 短程感知通信网络（有线或无线短程网络）；
c） 安防感知层网关，以下简称感知层网关；
d） 通信网络（有线或无线公网/专网）；
d） 智慧社区安防信息平台，以下简称安防信息平台；
e） 管控通信网络（有线或无线公网/专网）；
f） 外部安防管控信息平台，以下简称管控信息平台。

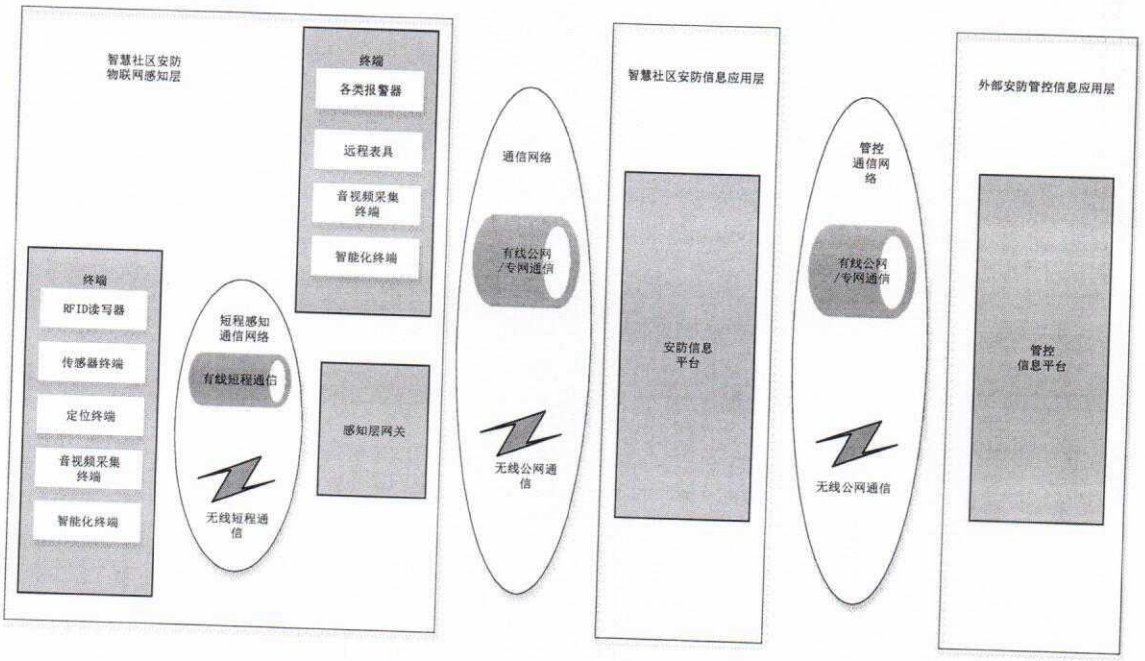

图1　智慧社区安防系统结构图

5.2　安全要求依据

本文件根据社区安防系统中涉及的感知终端、通信网络和信息平台相关联的人员隐私、人员财产、人身安全、国家基础设施等的威胁程度，提出安全要求依据。

6　安防感知终端安全要求

6.1　物理安全要求

6.1.1　选型

应符合GB/T　36951-2018　5.1.1章节规定的内容。

6.1.2　选址

应符合GB/T　36951-2018　5.1.2章节规定的内容，并应具备明确可查的位置信息。

6.1.3　供电

应符合GB/T　36951-2018　5.1.3章节规定的内容。

6.1.4　防拆

应符合GB/T　36951-2018　5.1.4章节规定的内容。

6.1.5　硬件设备要求

应满足以下要求：

a）具备自检和故障指示功能；

b）仅保留应用必需的通信接口，并标注接口信息；

c）应去除硬件和固件调试接口或将接口封闭在保护壳中；

d）存有敏感信息的芯片应进行去印刷防护或采用安全芯片存储敏感信息。

6.1.6 印刷标识

印刷标识应不易被涂改，宜采用二维码标识。

6.2 软件安全要求

6.2.1 标识

标识应满足以下要求：

a）系统内唯一标识；

b）标识包含3位以上随机数，防止批量猜测；

c）标识信息防篡改。

6.2.2 鉴别

鉴别应满足以下要求中的一项或多项：

a）支持基于系统内唯一标识的鉴别；

b）支持基于网卡地址、通信协议和通信端口的鉴别；

c）支持基于口令的鉴别，口令复杂度应不小于6个字符，包含中英文大小写和数字，避免使用默认口令；

d）支持基于预分配密钥的对称加密信息鉴别；

e）支持基于公钥密码机制的双向鉴别。

6.2.3 鉴别失败处理

鉴别失败处理应符合GB/T 37093-2018 6.2.2.2章节规定的内容。

6.2.4 接入鉴别机制

终端接入安防信息平台的鉴别机制应满足以下要求：

a）短程通信终端，支持网关的间接接入鉴别机制；

b）公网/专网终端，支持信息平台的直接接入鉴别机制。

6.2.5 访问控制

访问控制应满足以下要求：

a）支持基于ACL列表的访问控制；

b）有操作系统的终端，支持多用户访问控制，并最小化用户权限，避免使用默认用户名和口令访问终端；

c）有操作系统的终端，不向非管理员用户开放操作系统配置和软件的更改操作权限。

6.2.6 入侵防护

入侵防护应满足以下要求：

a）支持基于安全通信协议的数据过滤；

b）支持基于ID、IP、MAC、通信端口等限制条件的数据过滤；
c）有操作系统的终端，支持恶意程序和病毒代码的入侵防护；
d）有操作系统的终端，支持通信异常监测机制。

6.2.7 数据安全

数据安全应满足以下要求：
a）支持时间戳信息，支持数据传输和存储的时效记录；
b）支持数据摘要和校验等机制，保障数据传输和本地存储的完整；
c）敏感信息数据的传输和存储应采用加密和签名等防护机制，保障数据保密性和防篡改。

6.2.8 软件更新

软件安装或更新应满足以下要求：
a）支持本地基于管理员用户登录的软件更新；
b）支持基于安全通信机制下的远程更新；
c）支持软件更新包的完整性和防篡改机制验证；
d）不支持安装应用软件。

6.2.9 日志和审计

日志和审计应满足以下要求：
a）有操作系统的终端，支持鉴别失败、软件更新操作、入侵告警、恶意/病毒发现、设备重启等的安全日志，日志内容包括日期时间、事件类型、操作用户等；
b）有操作系统的终端，支持安全日志的审计。

6.2.10 自检和故障处理

自检和故障处理应满足以下要求：
a）支持基于软件的终端功能自检；
b）软件自检失败，支持根据安全策略执行设备重启或设备关闭等自动操作，并自动留存日志。

6.2.11 运行维护要求

6.2.12 终端生命周期管理

生命周期管理应满足以下要求：
a）终端存储终端版本信息、有效使用期限信息和当前运行状态，并定期发送至接入设备；
b）终端唯一标识随其生命周期生效和失效，失效标识不重复使用。

6.2.13 维护管理

维护管理应满足以下要求：
a）指定专人定期检查终端，并进行可用性维护；
b）对于使用移动通信物联网卡的终端，要定期检查其可靠性和机卡状态，发现异常应形成安全日志并上传安防信息平台。

7 短程感知通信安全要求

7.1 有线短程通信网络

整体系统中存在有线短程通信网络或总线时，应至少满足以下一项要求：

a）采用物理隔离的专用线路、专用协议组网通信；

b）采用逻辑隔离或信道加密技术的组网通信。

7.2 无线短程通信网络

整体系统中存在有线短程通信网络或总线时，应至少满足以下一项要求：

a）采用专用通信频段或专用通信方式、通信协议的组网通信；

b）采用逻辑隔离或信道加密技术的组网通信。

8 安防感知层网关安全要求

8.1 物理安全要求

8.1.1 选型

同6.1.1。

8.1.2 选址

同6.1.2。

8.1.3 供电

应采用持续型供电方式供电。

8.1.4 防拆

同6.1.4。

8.1.5 硬件设备要求

同6.1.5。

8.1.6 印刷标识

同6.1.6。

8.2 软件安全要求

8.2.1 标识

同6.2.1。

8.2.2 鉴别

同6.2.2。

8.2.3 感知终端接入鉴别机制

面向感知终端的接入鉴别机制应满足以下要求：

a）支持对其管理网络的所有接入短程感知通信终端进行接入鉴别；

b）有效管理通信网络的接入鉴别机制，终端接入密钥和接入安全策略；
c）接入安全策略包括终端、网络白名单和黑名单、接入鉴别响应处理等。

8.2.4 接入安防信息平台鉴别机制

面向安防信息平台的接入鉴别机制应满足以下要求：
a）支持接入安防信息平台的鉴别；
b）支持鉴别失败处理，符合GB/T 37093-2018 6.2.2.2章节规定的内容。

8.2.5 访问控制

访问控制应满足以下要求：
a）本地访问控制，采用网关管理员口令鉴别机制；
b）支持基于ACL列表的访问控制；
c）支持多用户访问控制，并最小化用户权限，禁止使用默认用户名和口令访问网关；
d）不向非管理员用户开放操作系统配置和软件的更改操作权限。

8.2.6 入侵防护

入侵防护应满足以下要求：
a）支持基于安全通信协议的数据过滤；
b）支持基于ID、IP、网络地址、通信端口等限制条件的数据过滤；
c）支持恶意程序和病毒代码的入侵防护；
d）支持通信异常监测机制。

8.2.7 数据安全

同6.2.7。

8.2.8 软件更新

软件安装或更新应满足以下要求：
a）支持本地基于管理员用户登录的软件更新；
b）支持基于安全通信机制下的远程更新；
c）支持软件更新包的完整性和防篡改机制验证。

8.2.9 日志和审计

日志和审计应满足以下要求：
a）支持鉴别失败、软件更新操作、入侵告警、恶意/病毒发现、设备重启、感知层网络异常事件等的安全日志，日志内容包括日期时间、事件类型、操作用户等；
b）支持感知终端安全日志数据的读取、存储和转发；
c）支持安全日志的审计。

8.2.10 自检和故障处理

自检和故障处理应满足以下要求：
a）支持基于软件的网关功能自检；
b）软件自检失败，支持根据安全策略执行设备重启操作，并自动留存日志。

8.3 运行维护要求

8.3.1 生命周期管理

感知层网络生命周期管理应满足以下要求：

a）网关存储网关版本信息、有效使用期限信息和当前运行状态，并定期发送至安防信息平台；

b）网关采集、存储、并转发接入终端的标识信息、版本信息、有效使用期限信息和当前运行状态；

b）网关唯一标识随其生命周期生效和失效，失效标识不重复使用。

8.3.2 维护管理

维护管理应满足以下要求；

a）指定管理员定期检查网关，并进行可用性维护；

b）对于使用移动通信物联网卡和插卡式硬件数字证书的网关，要定期检查其可靠性和机卡状态，发现异常应形成安全日志并转发安防信息平台。

9 感知通信网络安全要求

应符合GB/T 37093-2018第7.1章节的要求。

10 安防信息平台安全要求

10.1 安防信息平台接入要求

应符合GB/T 37093-2018第6.1章节的要求。

10.2 安防信息平台用户管理要求

信息平台的用户管理应满足以下要求：

a）具备多角色用户注册和管理功能，角色至少包括：平台管理员、普通用户；

b）支持多类型用户的账号、口令和权限分配的管理；

c）支持用户管理安全策略，包括：黑名单、白名单管理。

10.3 安防信息平台感知层安全信息采集要求

信息平台应接收经鉴别接入的网关和终端的以下信息内容：

a）网关和终端的联网报警信息；

b）网关和终端的安全告警信息；

c）网关和终端的安全日志数据信息；

d）网关和终端的设备生命周期管理信息；

e）使用移动通信物联网卡、数字证书卡的网关和终端的机卡维护管理信息。

10.4 安防信息平台感知层安全信息可视化要求

信息平台的安全信息可视化应满足以下要求：

a）支持联网报警信息可视化；

b）支持安全告警信息可视化；

c）支持安全日志统计分析信息可视化；

d）支持设备生命周期统计信息可视化；

e）支持使用移动通信物联网卡、数字证书卡的网关和终端的机卡维护管理统计分析信息可视化。

10.5 安防信息平台对接管控平台要求

10.5.1 对接设备鉴别要求

对接设备应支持基于安全数字证书的PKI鉴权，鉴权采用的非对称加密算法应符合国家密码管理局的相关规定。

10.5.2 数据传输要求

数据传输应满足以下要求：

a）数据传输安全性符合GB/T 37093-2018第6.2.4章节的要求；

b）数据传输内容包括：10.3章节的内容。

11 管控通信网络安全要求

应符合GB/T 37093-2018第7.2章节的要求。

附 录 A
（资料性附录）
安防系统设备安全标准化评测样例

依据《物联网 智慧社区安防系统安全要求》文件，以某厂商提供的社区物联网安防系统设备为样例，进行了标准化评测，评测结果按照符合项、部分符合项以及不符合项进行分类记录，具体列表如下：

表A.1 社区物联网安防系统安全标准化评测说明

设备类型	设备名称型号	符合项	部分符合项	不符合项	备注
摄像机	130W 网络枪机（DS-2CDJS66-SEV1CE）	6.1.1 选型 6.1.3 供电 6.1.4 防拆 6.1.5 硬件电路 6.1.6 印刷标识 6.2.1 标识 6.2.3 鉴别失败处理 6.2.4 接入鉴别机制 6.2.7 数据安全 6.2.9 日志和审计 6.2.10 自检和故障处理 6.3.2 维护管理	6.1.2 选址 6.2.2 鉴别 6.2.5 访问控制 6.2.6 入侵防护 6.3.1 终端生命周期管理	6.2.8 软件更新	安防感知终端
水压探测器	室外消防栓采集终端（XFP-WO1PN）	6.1.1 选型 6.1.3 供电 6.1.4 防拆 6.1.5 硬件电路 6.1.6 印刷标识 6.2.1 标识 6.2.3 鉴别失败处理 6.2.4 接入鉴别机制 6.2.7 数据安全 6.2.9 日志和审计 6.2.10 自检和故障处理 6.3.2 维护管理	6.1.2 选址 6.2.2 鉴别 6.2.5 访问控制 6.2.6 入侵防护 6.3.1 终端生命周期管理	6.2.8 软件更新	
无线	LORA	7.1 有线短程通信网络	7.2 无线短程通信网络	/	短程通信网络

表 A.1　社区物联网安防系统安全标准化评测说明（续）

设备类型	设备名称型号	符合项	部分符合项	不符合项	备注
数据采集网关	LORA 中继转发器（XFS-ZJ01）	8.1.1 选型 8.1.2 选址 8.1.3 供电 8.1.4 防拆 8.1.5 硬件电路 8.1.6 印刷标识 8.2.1 标识 8.2.2 鉴别 8.2.3 感知终端接入鉴别机制 8.2.4 接入安防信息平台鉴别机制 8.2.7 数据安全 8.2.9 日志和审计 8.2.10 自检和故障处理 8.3.1 生命周期管理 8.3.2 维护管理	8.2.5 访问控制 8.2.6 入侵防护	8.2.8 软件更新	安防感知层网关
无线	NB-IoT	/	11.1 增强级要求	9.1 基本级要求	安防通信网络
小区平台	燃气监控报警系统管理平台	10.1.1 设备标识 10.1.2 鉴别 10.1.3 访问控制 10.1.4 数据传输安全 10.1.5 密钥管理 10.1.6 入侵防护 10.1.7 日志审计 10.2 用户管理要求 10.3 感知层安全信息采集要求 10.4 感知层安全信息可视化要求 10.5.1 对接设备鉴别要求 10.5.2 数据传输要求	/	/	安防信息平台

依据《物联网　智慧社区安防系统安全要求》文件，以某厂商提供的智慧停车系统设备为样例，进行了标准化评测，评测结果按照符合项、部分符合项以及不符合项进行分类记录，具体列表如下：

表A.2　智慧停车系统安全标准化评测说明表

设备类型	设备名称型号	符合项	部分符合项	不符合项	备注
道闸	车辆识别终端 ZTEITS2.0	6.1.2 选址 6.1.3 供电 6.1.4 防拆 6.1.5 硬件电路 6.1.6 印刷标识 6.2.1 标识 6.2.7 数据安全 6.2.9 日志和审计 6.3.1 终端生命周期管理	6.1.1 选型 6.2.3 鉴别失败处理 6.2.5 访问控制 6.2.6 入侵防护 6.2.8 软件更新	6.2.2 鉴别 6.2.4 接入鉴别机制 6.2.10 自检和故障处理 6.3.2 维护管理	安防感知终端
智慧停车管理系统	ZTEITS2.5	10.1.1 设备标识 10.1.2 鉴别 10.1.3 访问控制 10.1.4 数据传输安全 10.1.6 入侵防护 10.1.7 日志审计 10.2 用户管理要求 10.3 感知层安全信息采集要求	10.1.5 密钥管理 10.5.2 数据传输要求	10.4 感知层安全信息可视化要求 10.5.1 对接设备鉴别要求	安防信息平台
智慧停车管理系统	ZTEITS2.5	12.1.1 设备标识 12.1.2 鉴别 12.1.3 访问控制 12.1.4 数据传输安全 12.1.5 密钥管理 12.1.6 隔离防护 12.1.7 入侵防护 12.1.8 日志审计 12.3 物联网系统安全信息采集要求 12.2 用户管理要求 12.4 感知层安全信息可视化要求	/	/	安防信息平台

参 考 文 献

[1] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[2] GB/T 35318-2017 公安物联网感知终端安全防护技术要求

[3] GB/T 35592-2017 公安物联网感知终端接入安全技术要求

[4] GB/T 37024-2018 信息安全技术 物联网感知层网关安全技术要求