ICS35.040
L 80

团 体 标 准

T/SZSSIA XXX—20XX

物联网专网感知层设备接入控制与监测系统技术要求

Technical requirements for access control and monitoring systems for IoT private network sensing layer devices

征求意见稿

2020-05-26

20XX-XX-XX 发布 20XX-XX-XX 实施

深圳市智慧安防行业协会 发布

目　　次

前言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　设计原则 2
6　系统构成 2
6.1　概述 2
6.2　组件构成 3
6.3　功能配置 3
7　技术要求 4
7.1　功能要求 4
7.2　性能要求 7
7.3　自身安全要求 7
7.4　接口要求 8
8　安装部署 9
9　文件提供 9
9.1　安装部署手册 9
9.2　用户操作手册 9
9.3　系统接口手册 9
附　录　A　（资料性附录）　系统接入部署 10
参考文献 11

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由深圳市智慧安防行业协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

物联网专网感知层设备接入控制与监测系统技术要求

1 范围

本文件规定了物联网专网感知层设备接入控制与监测系统的设计原则、构成、技术要求、安装部署和文件提供。

本文件适用于以旁路方式部署的物联网专网感知层设备接入控制与监测系统，指导此类系统选型、部署、运行和维护。

注：在不引起混淆的情况下，本文件中的“物联网专网感知层设备接入控制与监测系统”简称为“系统”。

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 22239—2019 信息安全技术网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 33745—2017 物联网 术语

GB/T 37093 物联网感知层接入通信网的安全要求

3 术语和定义

GB/T 25069、GB/T 33745—2017、GB/T 37093界定的以及下列术语和定义适用于本文件。

3.1

物联网 Internet of Things

基于互联网、传统电信网等的信息承载体，通过信息传感设备按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。

3.2

物联网专网 IoT private network

具体行业或企业为特定应用搭建的专用物联网络，实时采集其需要监控、连接、互动的物体或过程，实现对业务或生产过程的智能化感知、识别和管理。具体行业或企业特定应用如：电力行业的电力采集网络、公安行业的视频监控网络。

3.3

物联网应用 IoT application

物联网在具体场景中的使用实例，向用户提供物联网服务的集合。

[来源：GB/T 33745—2017，2.1.6]

3.4

感知层设备 Sensing layer Devices

具备信息采集、传输、分析与处理功能的，以及具备执行指令和联网功能的电子设备。

4 缩略语

下列缩略语适用于本文件。

HTTPS：安全的超文本传输协议（Hypertext Transfer Protocol Secure）

IoT：物联网（Internet of Things）

IP:互联网协议（Internet Protocol）

JSON：对象标记语言（(JavaScript Object Notation）

MAC：媒体访问控制（Medica Access Control）

XML：可扩展标记语言（Extensible Markup Language）

5 设计原则

5.1 系统应以实际情况和现实问题为基础，遵照国家及地方相关的标准、政策、法律法规和规章，执行相应的安全标准和参照行业的最佳实践。

5.2 系统应以“可信”为基础，从终端到网络边界、从边界到行为、从行为到业务应用，确保可信设备才能入网、可信业务应用才能使用、可信网络流量才可通行。

5.3 系统应遵循最优最简原则、易用原则，以用户体验为基准，在保持客户原有网络结构，以及不对网络产生任何影响的原则下构建系统。

5.4 系统应针对专网内感知层设备进行资产梳理、状态监测、安全防护和行为监测，从感知层设备到网络边界、从网络边界到网络行为、从网络行为到业务应用，建立以感知层设备为核心，贯穿感知层、网络层、应用层、数据层形成立体监控和纵深防御体系，充分保障终端安全、应用安全、数据安全、系统与网络安全和操作合规。

5.5 系统以旁路方式为物联网专网感知层构建安全防护体系，具备为安全管理者和决策者展示安全运行态势的能力。

5.6 系统设计时，应根据安全功能的强弱将安全技术要求分为基本级和增强级两个等级。

5.7 系统设计时，应符合 GB/T 22239—2019 中第二级安全要求、第三级安全要求中的安全通用要求和物联网安全扩展要求。

6 系统构成

6.1 概述

系统由探测处置引擎、采集处理引擎两类物理设备组成，探测处置引擎用于发现和识别感知层设备，并将设备信息上报至采集处理引擎；采集处理引擎部署采集处理组件、大数据分析平台和安全应用平台，用于采集网络流量，构建行为模型，并进行网络行为分析。应用示例参见资料性附录A。

6.2 组件构成

系统组件主要包括探测、采集组件、大数据分析平台和安全应用平台，可以根据网络流量大小、网络可达性以及管理颗粒度等因素，选择集中式部署或分布式部署，并且可以根据业务流量的增长情况，灵活拆分、快速迁移。系统组件架构见图1。

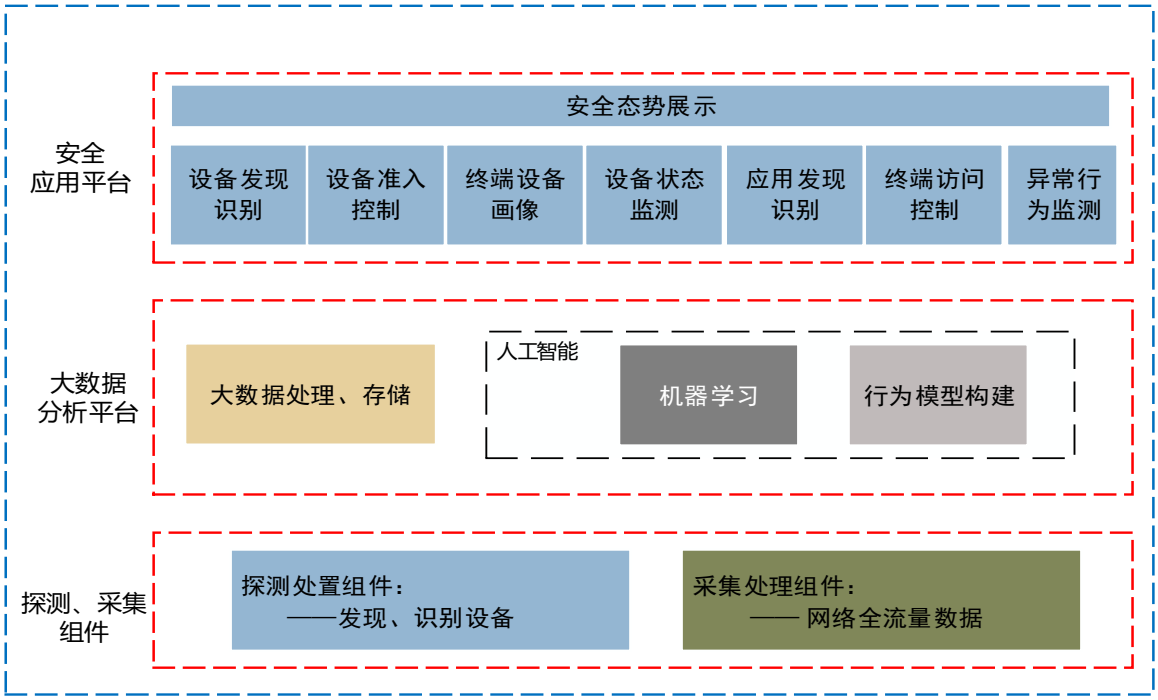

图1 系统组件架构图

a) 探测、采集组件包括探测处置组件和采集处理组件，基本功能配置如下：
   1) 探测处置组件用于发现和识别网络内物联终端、管理终端、服务器等设备，获取设备属性信息、采集设备及业务应用系统的运行状态数据，归一化处理后传输给大数据分析平台；
   2) 采集处理组件采集网络流量数据，在进行报文的初步解析、归一化、格式化等操作处理后，传输给大数据分析平台，用于后续的深度分析处理。
b) 大数据分析平台由大数据处理、存储和人工智能功能模块组成，基本功能配置如下：
   1) 用于存储探测处置组件和采集处理组件提交的设备信息和网络流量数据；
   2) 使用分布式存储以及并行计算等大数据技术，构建行为模型，分析网络数据，洞察异常行为；
   3) 为安全应用平台提供数据接口；
   4) 人工智能功能模块具备机器学习、行为模型构建等功能。
c) 安全应用平台为安全业务管理的功能集合，是用户使用系统的交互界面，将前台展现后台数据剥离，提高系统部署和项目实施效率。主要功能配置如下：设备发现识别、设备准入控制、终端设备画像、设备状态监测、应用发现识别、终端访问控制、异常行为监测、安全态势展示。

6.3 功能配置

系统应配置如下功能，设备发现识别、设备准入控制、设备状态监测、终端设备画像、应用发现识别、IP地址管理、终端访问控制、边界安全防护、网络拓扑绘制、异常行为监测、安全态势展示。系统功能要求应符合7.1中的相关规定。

7 技术要求

7.1 功能要求

7.1.1 设备发现识别

设备发现识别功能要求见表1。

表1

功能点	序号	要求	安全等级	
			基本	增强
设备发现识别	1	系统能够主动获取感知层设备的以下信息： a）IP 地址； b）设备唯一性标识信息（如：MAC 地址）； c）操作系统； d）生产厂商； e）设备类型； f）设备开放端口等信息； g）在线时长。	应	应
	2	系统能够对感知层设备以下信息进行识别或管理： a）识别通信协议信息； b）设备经纬度信息管理； c）符合 GB/T 22239—2019 中 8.4.3.1、8.4.3.2 的要求。	宜	应

7.1.2 设备准入控制

系统能够制定安全准入策略，对感知层设备进行准入控制，设备准入控制功能要求见表2。

表2

功能点	序号	要求	安全等级	
			基本	增强
设备准入控制	1	a）准入策略能够自定义配置，能按操作系统、设备类型、设备唯一性识别信息（如：MAC 地址）进行组合配置； b）准入策略能够加入安全检查项，包括弱口令检查、风险端口检查和风险漏洞检查； c）支持手工准入和规则自动准入两种方式； d）对于不符合准入策略的设备，能够实时阻断隔离； e）符合 GB/T 22239—2019 中 7.4.2.1 的要求。	应	应
	2	a）能够快速发现仿冒设备接入，并能阻止对接入设备的非法控制； b）能够识别感知层设备的通讯协议和信令，并进行合法性检测，对不符合格式的数据进行阻断和告警； c）符合 GB/T 22239—2019 中 8.4.2.1 的要求。	宜	应

7.1.3 设备状态监测

系统能够对感知层设备的运行、安全状态进行监测，对异常状态进行告警，设备状态监测功能要求见表3。

表3

功能点	序号	要求	安全等级	
			基本	增强
设备状态监测	1	a）能够实时监测感知层设备的离线、在线状态； b）能发现感知层设备是否存在弱口令； c）能够发现感知层设备的风险端口； d）针对离线设备、存在弱口令和风险端口的设备，具备告警功能； e）符合 GB/T 22239—2019 中 7.1.4.4 的要求。	应	应
	2	a）能够发现设备的风险漏洞，并具备告警功能； b）系统告警信息具备 XML 或 JSON 标准格式的对外接口； c）符合 GB/T 22239—2019 中 8.1.4.4 的要求。	宜	应

7.1.4 终端设备画像

系统能够对感知层设备进行画像绘制并可视化展示，终稿设备画像功能要求见表4。

表4

功能点	序号	要求	安全等级	
			基本	增强
设备终端画像	1	a）终端画像能够展示设备静态属性，包括：设备类型、IP 地址、操作系统等； b）终端画像能展示设备的历史分析事件信息。	应	应
	2	终端画像能够展示设备行为习惯，包括：连接习惯、流量习惯。	宜	应

7.1.5 应用发现识别

系统能够自动发现并识别物联网专网内运行的应用系统，应用发现识别功能要求见表5。

表5

功能点	序号	要求	安全等级	
			基本	增强
应用发现识别	1	a）自动发现识别物联网专网内运行的 B/S 架构应用系统，包括：系统名称、服务 IP、服务端口等； b）自动发现识别物联网专网内运行的 C/S 架构应用系统，包括：系统名称、服务 IP、服务端口等。	应	应
	2	自动发现识别物联网专网内运行的扫描类应用系统，包括：系统名称、服务 IP 等。	宜	应
注：扫描类应用指应用服务端主动发起请求的应用，比如漏洞扫描类应用。				

7.1.6 IP 地址管理

系统能够对物联网专网IP地址资源使用情况进行分析展示，IP地址管理功能要求见表6。

表6

功能点	序号	要求	安全等级	
			基本	增强

IP 地址管理	1	a) 准确展示专网内在线使用的 IP 地址； b) 准确展示专网内未分配使用的 IP 地址。	应	应
	2	准确展示专网内长时间（可设置）未在线的 IP 地址。	宜	应

7.1.7 终端访问控制

系统能够对感知层设备的访问范围进行控制和监测，终端访问控制功能要求见表7。

表7

功能点	序号	要求	安全等级	
			基本	增强
终端访问控制	1	a) 能够对感知层设备访问的目的安全域和目的地址进行控制和监测； b) 能够识别感知层设备开放的风险端口； c) 符合 GB/T 22239—2019 中 7.1.3.2 的要求。	应	应
	2	a) 能够对超出访问范围的感知层设备进行告警和阻断； b) 符合 GB/T 22239—2019 中 8.1.3.2 的要求。	宜	应

7.1.8 边界安全防护

系统能够对物联网专网中的网络边界进行防护，边界安全防护功能要求见表8。

表8

功能点	序号	要求	安全等级	
			基本	增强
边界安全防护	1	a) 能够依据网络流量，对网络边界的访问策略进行梳理，发现无效和冗余策略； b) 能够对跨越安全边界的非授权访问进行监测和告警； c) 符合 GB/T 22239—2019 中 7.1.3.1、7.1.3.2 的要求。	应	应
	2	a) 能够识别非法网络边界，并进行告警； b) 符合 GB/T 22239—2019 中 8.1.3.1、8.1.3.2 要求。	宜	应

7.1.9 网络拓扑绘制

系统能够生成物联网专网的网络拓扑关系图，网络拓扑绘制功能要求见表9。

表9

功能点	序号	要求	安全等级	
			基本	增强
网络拓扑绘制	1	a) 支持所有主流厂商可网管设备网络拓扑绘制，并能够以拓扑图的形式展现； b) 支持 SNMP 协议的 V1/V2/V3 版本。	应	应
	2	支持生成全网访问关系，形成业务访问拓扑图。	宜	应

7.1.10 异常行为监测

系统能够发现物联网专网中异常网络行为和非法攻击，异常行为监测功能要求见表10。

表10

功能点	序号	要求	安全等级	
			基本	增强
异常行为监测	1	a) 支持防范业务专网中的未授权访问、非法外联、违规运维等行为，保证业务应用和核心数据的安全，并具备告警功能； b) 具备对已知病毒、木马等恶意代码的检测和阻断能力； c) 支持安全域划分功能，实现所划分安全域间的访问控制和监测； d) 符合 GB/T 22239—2019 中 7.1.3.3、7.1.3.4、7.4.2.2 要求。	应	应
	2	a) 支持通过白名单策略识别非正常应用网络行为，具备对未知新型网络攻击行为的监测能力； b) 符合 GB/T 22239—2019 中 8.1.3.3、8.1.3.4、8.4.2.2 要求。	宜	应

7.1.11 安全态势展示

系统能够对物联网专网的整体安全态势进行可视化展示，要求如下：

a) 应集中动态展示专网内感知层设备的数量及类型分布；
b) 应集中动态展示专网内感知层设备安全和运行状态，部门分布情况；
c) 应实时展示产生非法行为的感知层设备；
d) 应集中展示非法网络行为的类型和趋势，展示攻击源和外联目标的详情；
e) 宜支持在监控大屏进行安全态势的展示。

7.2 性能要求

系统针对感知层设备的发现识别能力，符合以下要求：

a) 新设备接入时，系统发现速度应不大于 30s；
b) 系统的设备发现能力应不低于 5000 p/min；
c) 安全等级为基本级时，宜具备发现识别不同厂家的、主流的物联网感知层设备的能力。
d) 安全等级为增强级时，应具备发现识别不同厂家的、主流的物联网感知层设备的能力。

7.3 自身安全要求

7.3.1 系统健壮性

系统健壮性相关要求见表12。

表11

名称	序号	要求	安全等级	
			基本	增强
系统健壮性	1	a) 系统对自身的关键进程和资源使用情况，具备监控机制，并具备重新连接、重新启动等自愈机制； b) 系统采用旁路部署方式，系统故障不影响其他应用和网络的运行； c) 具备安全升级功能，使用安全通道传输系统升级文件，并对升级文件进行合法性校验。	应	应

	2	系统具备双系统或集群高可用能力，保证系统服务的连续性。	宜	应

7.3.2 数据安全性

数据安全性相关要求见表13。

表12

名称	序号	要求	安全等级	
			基本	增强
数据安全性	1	a) 系统关键数据采取加密方式存储和传输； b) 系统具备数据备份和恢复功能； c) 具备安全升级功能，使用安全通道传输系统升级文件，并对升级文件进行合法性校验。	应	应
	2	a) 系统具备双系统或集群高可用能力，保证系统服务的连续性； b) 系统支持关键数据（异常网络行为、风险事件、审计日志）的区块链存储，保证的数据可追踪、不可篡改。	宜	应

7.3.3 日志审计

日志审计相关要求见表14。

表13

名称	序号	要求	安全等级	
			基本	增强
日志审计	1	a) 系统能够记录操作用户的登录/登出，各模块的操作记录日志； b) 系统日志能够记录关键处理逻辑的处理结果，处理失败时需记录明确原因。	应	应

7.4 接口要求

系统对外的接口要求见表15。

表14

名称	序号	要求	安全等级	
			基本	增强
接口要求	1	a) 系统的对外接口基于 HTTPS 协议； b) 主动推送和等待请求的数据格式采用 JSON 格式； c) 第三方系统将请求报文以 GET 方式，发送到系统提供请求地址； d) 系统将推送报文以 POST 方式，发送至第三方系统提供的接收地址。	应	应
	2	系统支持与区块链类系统的接口。	宜	应

8 安装部署

符合以下要求：

a） 系统应以旁路方式部署，不改变原有网络架构，不影响原有系统运行；

b） 系统应采集汇聚交换机或核心交换机的镜像网络数据；

c） 系统组件应支持分布式部署，可灵活组合部署于实体机或虚拟机。

9 文件提供

9.1 安装部署手册

应包括以下内容：

a） 硬件部署步骤及方法；

b） 软件部署步骤及方法。

9.2 用户操作手册

应包括以下内容：

a） 描述系统功能及业务目标；

b） 描述功能点的操作流程和方法。

9.3 系统接口手册

应包括以下内容：

a） 描述所有接口的目的与使用方法；

b） 描述每个接口的输入、输出参数。

附 录 A
（资料性附录）
系统接入部署

接入控制与监测系统主要由探测处置引擎、采集处理引擎两类物理设备组成，探测处置引擎部署于感知层设备，采集处理引擎部署于网络层。系统接入部署拓扑图如图 A.1 所示。

探测处置引擎部署位置靠近感知层物联终端，能够快速发现识别设备，获取设备的运行和风险状态，及时完成违规处置；采集处理引擎作为“大脑中枢”，部署于核心网络层，集中数据，智能分析，统一管控；双引擎协调联动，能够有效提升物联专网安全的综合防御能力。

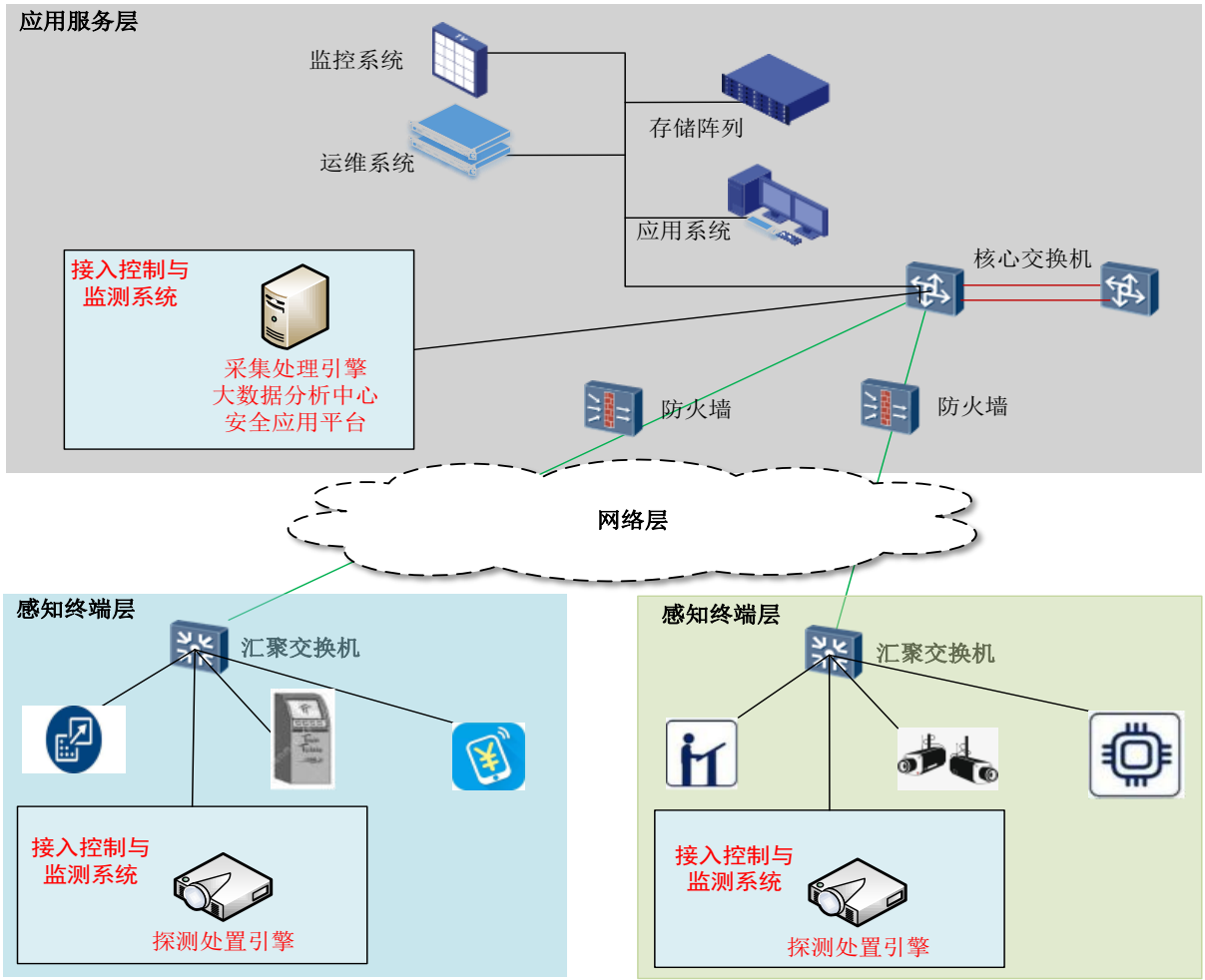

图 A. 1 系统接入部署拓扑图

参考文献

[1] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[2] GB/T 22239—2019 信息安全技术网络安全等级保护基本要求
[3] GB/T 36951—2018 物联网感知层终端应用技术要求
[4] GB/T 37093—2018 物联网感知层接入通信网的安全要求