ICS 35.020
CCS L 70

DB33

浙 江 省 地 方 标 准

DB33/T 1416—2025

人民防空固定式警报设施运行监测系统技术规范

Technical specification for civil air defense fixed alarm facility operational monitoring system

2025－01－22 发布　　2025－02－22 实施

浙江省市场监督管理局　发布

目　　次

前　言

本标准按照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》的规定起草。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本标准由浙江省国防动员办公室提出、归口并组织实施。

本标准起草单位：湖州市国防动员办公室、浙江大学湖州研究院、浙江臻善科技股份有限公司、杭州科骏电子科技有限公司。

本标准主要起草人：张志宏、杨郑成、李欣未、房胜、褚晓剑、柏垚伊、费婷婷、姚应财、顾兴月、袁恒、项圆圆、黄宇飞、方卿、陈炜波、周新林、段小兵、方欣、邓建飞、葛予晴。

人民防空固定式警报设施运行监测系统技术规范

1 范围

本标准规定了人民防空固定式警报设施运行监测系统的系统架构、警报设施层、物联感知层、传输层、应用层、安全、试验方法、系统维护等内容。

本标准适用于人民防空固定式警报设施运行监测系统的设计、建设、测试和运行。

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标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 5080.7—1986 设备可靠性试验 恒定失效率假设下的失效率与平均无故障时间的验证试验方案

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

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 37025—2018 信息安全技术 物联网数据传输安全技术要求

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

GB/T 39786 信息安全技术 信息系统密码应用基本要求

DB33/T 2207—2019 人民防空固定式警报设施建设管理规范

3 术语和定义

DB33/T 2207—2019界定的以及下列术语和定义适用于本标准。

3.1

人民防空固定式警报设施 civil air defense fixed alarm facility

用于战时防空、平时防灾鸣放警报信号的固定设备设施，包括警报器、控制终端、后备电源及相关的通信、供电线路和构筑物等附属设施。

[来源：DB33/T 2207—2019，2.1]

3.2

人民防空固定式警报设施运行监测系统 civil air defense fixed alarm facility operation monitoring system

对人民防空固定式警报设施的运行状态和运行环境进行连续或周期性监测、分析与辅助诊断的系统。

4 缩略语

下列缩略语适用于本文件。

CoAP：物联网应用协议（Constrained Application Protocol）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

IP：网际互连协议（Internet Protocol）
JSON：对象简谱（JavaScript Object Notation）
LoRa：远距离无线电（Long Range Radio）
MODBUS：串行通信协议（Modelbus）
MQTT：消息队列遥测传输协议（Message Queuing Telemetry Transport）
SDI-12：传输速度为1 200波特率的串行数据接口（Serial Digital Interface）
TCP：传输控制协议（Transmission Control Protocol）
UDP：开放系统互连（Open Systems Interconnection）
WiFi：无线通信技术（Wireless Fidelity）

5 系统架构

人民防空固定式警报设施运行监测系统（以下简称运行监测系统）采用分层、分布式结构，由警报设备层、物联感知层、传输层、应用层构成，总体架构见图1。

——警报设施层，是运行监测系统的监测对象，包括供电电源、警报器、警报控制器、后备电源、扬声器等；
——物联感知层，由传感设备和边缘处理器构成，传感设备负责警报设施运行数据的监测与采集，边缘处理器负责警报设施运行数据的协议封装、加密上传、存储以及供电电源开关控制指令的接收、执行与回复等；
——传输层，是运行监测系统的通信链路，负责边缘处理器与管理平台间的数据和指令传输等；
——应用层：由管理平台运作实现，负责警报设施运行数据的接收与存储、分析、查询以及供电电源开关控制指令下发、维保/巡检任务生成与管理等。

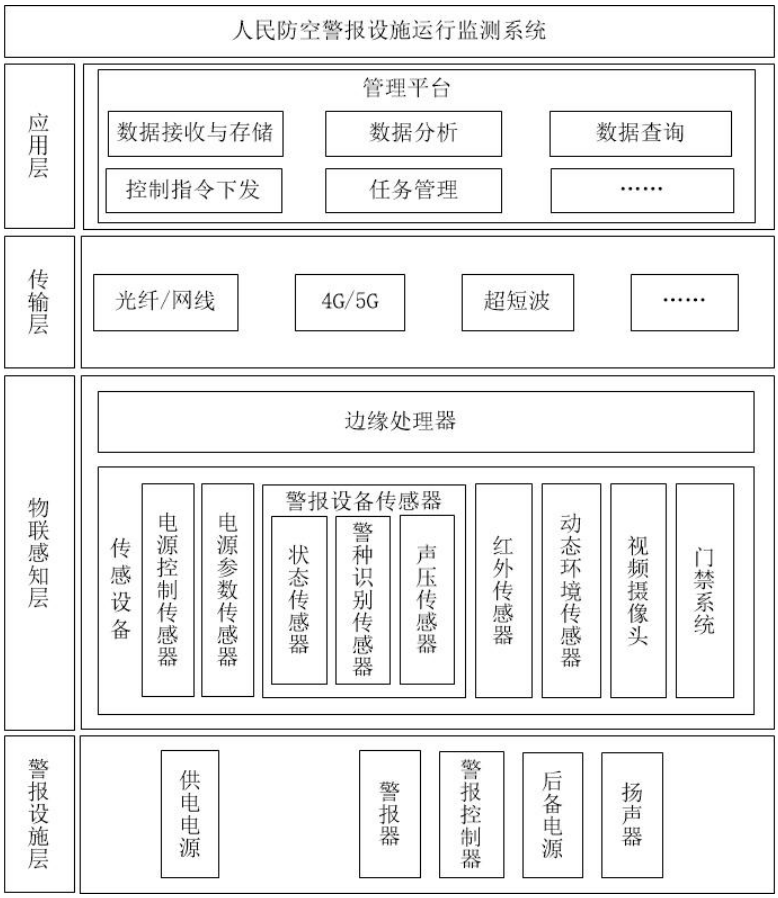

图 1　总体架构图

6　警报设施层

应符合DB33/T 2207的相关规定。

7　物联感知层

7.1　传感设备配置

7.1.1　应综合考虑警报设施的新旧程度、监测环境等因素，根据实际需求配置传感设备。应配的传感设备包括电源参数传感器、状态传感器、警种识别传感器、声压传感器等，宜配的传感设备包括电源控制传感器、红外传感器、动态环境传感器、视频摄像头、门禁系统等。

7.1.2　传感设备的安装应按表 1 的规定。

表 1　传感设备安装要求

序号	设备名称	安装位置	通用要求
1	电源控制传感器	室内，警报设施配电箱输出端	安装位置周边应留有接线、维护和调校的足够空间； 安装处应不受阳光和强热源直射； 传感器的架设应安全可靠且不妨碍维保人员工作，不易被碰撞、损坏； 传感器信号传输线不应与其他电源线一同穿过线管或线槽。
2	电源参数传感器	室内，警报设施配电箱输入端	
3	状态传感器	室内，警报设施运行维护接口处	
4	警种识别传感器	室外，警报器音头5m音源45°处	
5	声压传感器	室外，警报器音头5m音源45°处	
6	红外传感器	室内，警报器正向方	
7	动态环境传感器	室内，警报器四音头中心上方1.5m	
8	视频摄像头	室内，警报器设备正前方1.5m至3m处	
9	门禁系统	警报机房出入口	

7.2　接口要求

7.2.1　传感设备与边缘处理器间的接口

7.2.1.1　传感设备与边缘处理器间的接口要求如下：

——边缘处理器应能通过该接口获取传感设备采集上报的警报设施运行数据，并能通过该接口向传感设备发送控制指令；

——边缘处理器应能通过该接口实现对传感设备的通信状态管理、设备管理、协议适配等。

7.2.1.2　电源控制传感器、电源参数传感器、状态传感器、警种识别传感器、声压传感器、红外传感器、动态环境传感器等可采用 MODBUS、SDI-12、MODBUS-TCP/IP 等有线通信接口协议或 WiFi、LoRa、ZigBee、MQTT、CoAP 等无线通信接口协议。

7.2.1.3　视频摄像头、门禁系统等应采用 TCP、UDP 等网络协议。

7.2.2　边缘处理器与管理平台间的接口

7.2.2.1　边缘处理器与管理平台间的接口要求如下：

——边缘处理器应能通过该接口将采集到的和分析形成的警报设施运行数据发送至管理平台；

——管理平台应能通过该接口实现对边缘处理器的设备管理、控制指令下发等。

7.2.2.2　通信协议应采用 HTTPS、MQTT 等应用协议。

7.3　功能要求

7.3.1　数据监测与采集

7.3.1.1　传感设备应能对警报设施的运行数据开展实时、自动、连续监测与采集，监测与采集的数据项目及频次要求按表 2 的规定。

表 2　监测与采集的数据项目及频次要求

监测节点	采集项目		采集频次
电源控制传感器	警报器、警报控制器的通电状态		实时采集
电源参数传感器	电源参数数据（含电压、电流、功率）		实时采集
状态传感器	警报控制器	电台单元、接口单元、电源单元状态数据	按需求设定
	警报器	功放单元、电源单元、喇叭单元状态数据	

表 2　监测与采集的数据项目及频次要求（续）

监测节点	采集项目		采集频次
状态传感器	后备电源	工作状态、开启状态、维护状态、电量状态、供电状态、充电状态、电量显示等数据	按需求设定
警种识别传感器	警报音频率		触发后采集
声压传感器	周边环境瞬时噪声值		实时采集
红外传感器	移动热源数据		实时采集
动态环境传感器	环境温度、湿度数据		实时采集
视频摄像头	监控视频或抓拍照片		实时采集
门禁系统	人员进出数据		实时采集

7.3.1.2　传感设备采集的数据内容按表 3 的规定。

表 3　传感设备采集的数据内容

一级字段名称	一级字段代码	二级字段名称	二级字段代码	数据类型	字段长度	小数位	值域	备注
电源控制	dykz	警报器通电状态	jbqtdzt	numeric	1	0	0：关电 1：通电	—
		警报控制器通电状态	jbkzqtdzt	numeric	1	0	0：关电 1：通电	—
电源参数	dycs	电流	dl	numeric	5	3	—	—
		电压	dy	numeric	4	1	—	—
		功率	gl	numeric	5	1	—	—
警报器状态	jbqzt	工作状态	gzzt	numeric	1	0	0：正常 1：故障	—
		电源单元	dydy	numeric	1	0	0：正常 1：故障	—
		功放单元	gfdy	numeric	1	0	0：正常 1：故障	—
		喇叭单元	lbdy	numeric	1	0	0：正常 1：故障	—
警报控制器状态	jbkzqzt	工作状态	gzzt	numeric	1	0	0：正常 1：故障	—
		接口单元	jkdy	numeric	1	0	0：正常 1：故障	—
		电台单元	dtdy	numeric	1	0	0：正常 1：故障	—
		电源单元	dydy	numeric	1	0	0：正常 1：故障	—
后备电源状态	hbdyzt	充电状态	cdzt	numeric	1	0	0：充电 1：浮充 11：放电	—

表 3　传感设备采集的数据内容（续）

一级字段名称	一级字段代码	二级字段名称	二级字段代码	数据类型	字段长度	小数位	值域	备注
后备电源状态	hbdyzt	电流	dl	numeric	5	3	—	—
		电量状态	dlzt	numeric	1	0	0：充电完成 1：正在充电	—
		电压	dy	numeric	4	1	—	—
		供电状态	gdzt	numeric	2	0	0：交流 1：直流 11：交直	—
		工作状态	gzzt	numeric	1	0	0：正常 1：故障	—
		开启状态	kqzt	numeric	1	0	0：关闭 1：开启	—
		维护状态	whzt	numeric	1	0	0：关闭 1：开启	—
警种识别	jzsb	警种	jz	numeric	3	0	1：预先警报音 2：空袭警报音 3：解除警报音 4：防灾警报音 5：防灾解除警报音 6：其他警报信号	将电参数功率变化、警报声压变化与预先警报音、空袭警报音、解除警报音、防灾警报音、防灾解除警报音、测试警报6类警种频率特征进行分析比对，得出具体警种类型
红外	hw	移动热源	ydry	numeric	1	0	0：有移动热源 1：无移动热源	—
环境感知	hjgz	声压	sy	numeric	4	4	—	—
		温度	wd	numeric	3	1	—	单位为℃，温度均匀度为0.3 ℃、温度波动度为±0.2 ℃
		湿度	sd	numeric	4	1	—	单位为RH，湿度均匀度为1.0%RH、湿度波动度为±0.8%RH

表 3　传感设备采集的数据内容（续）

一级字段名称	一级字段代码	二级字段名称	二级字段代码	数据类型	字段长度	小数位	值域	备注
视频监控	spjk	状态	zt	numeric	1	0	1：在线 2：离线	—
门禁	mj	状态	zt	numeric	1	0	0：开启 1：闭合	实时采集
		出入目标	crmb	numeric	2	0	—	触发后采集，根据出入授权信息识别显示出入目标身份信息
		出入时间	crsj	timestamp	6	0	—	触发后采集，按字节依次表示时、分、秒，精确到1 s/d
		出入口	crk	varchar	255	0	—	触发后采集，目标具体的出入口信息
		抓拍照片	zpzp	text	—	—	—	触发后采集，目标具体出入的照片
采集时间	time	—	—	timestamp	6	0	—	—

7.3.2　协议封装

7.3.2.1　边缘处理器应能对警报设施运行数据进行协议封装，形成常态报文和事件报文。

7.3.2.2　常态报文应包括电源控制、电源参数、警报器状态、警报控制器状态、后备电源状态、环境感知等数据内容，具体要求按表 3 的相关规定，报文结构见示例。

示例：

```
{
  "dykz":{"jbqtdzt":0,"jbkzqtdzt":0},
  "dycs":{"dl":1.35,"dy":224.3,"gl":45.5},
  "jbqzt":{"gzzt":0,"dydy":0,"gfdy":0,"lbdy":0},
  "jbkzqzt":{"gzzt":0,"jkdy":0,"dtdy":0,"dydy":0},
  "hbdyzt":{"cdzt":0,"dl":1.12,"dlzt":0,"dy":4.8,"gdzt":0,"gzzt":0,"kqzt":0,"whzt":0},
  "hjgz":{"sy":51.2,"wd":26.5,"sd":57.2},
  "time":"2022-06-28 10:00:00"
}
```

7.3.2.3　事件报文应包括警报鸣响、红外检测入侵告警、门禁入侵告警、电源告警、警报点维护等，触发条件按表 4 的规定，报文数据内容按表 5～表 9 的相关规定，报文结构见示例 1～示例 5。

表 4　事件报文触发条件

事件	触发条件
警报鸣响	将采集到的电参数功率变化、警报声压变化与预先警报音、空袭警报音、解除警报音、防灾警报音、防灾解除警报音、测试警报6类警种频率特征进行分析比对，得出具体警种类型和鸣放状态。
入侵告警（含红外检测和门禁）	对进入人员的身份、进入时间、进入口等信息的识别分析，若进入人员与录入人员信息未匹配，则判定为入侵告警。
电源告警	采集到的电参数功率与平时相比，显示为过高或过低。
警报点维护	警报点现场需进行设备维护等情况时。

表 5　警报鸣响事件报文数据内容

序号	字段名称	字段代码	字段类型	字段长度	小数位	值域	备注
1	事件类型	type	varchar	10	0	e01	鸣响警报类型
2	声压	sy	numeric	5	1	—	—
3	警报类型代码	vtype	numeric	1	0	1：预先警报音 2：空袭警报音 3：解除警报音 4：防灾警报音 5：防灾解除警报音 6：其他警报信号	—
4	鸣放状态	status	numeric	1	0	0：正常鸣放 1：误鸣	—
5	鸣放开始时间	starttime	timestamp	6	0	—	—
6	鸣放结束时间	endtime	timestamp	6	0	—	—
7	采集时间	time	timestamp	6	0	—	—

示例 1：

```
{
"type":"e01",
"sy":57.2,
"vtype": 1,
"status": 1,
"starttime": "2022-06-28 9:40:00",
"endtime": "2022-06-28 9:43:00",
"time":"2022-06-28 10:00:00"
}
```

表 6　红外检测入侵告警事件报文数据内容

序号	字段名称	字段代码	字段类型	字段长度	小数位	值域	备注
1	事件类型	type	varchar	10	0	e02	红外检测类型
2	状态	status	numeric	1	0	0：有移动热源 1：无移动热源	—
3	采集时间	time	timestamp	6	0	—	—

示例 2：

```
{
  "type":"e02",
  "status":1,
  "time":"2022-06-28 10:00:00"
}
```

表 7　门禁入侵告警事件报文数据内容

序号	字段名称	字段代码	字段类型	字段长度	小数位	值域	备注
1	事件类型	type	varchar	10	0	e03	门禁检测类型
2	状态	status	numeric	1	0	0：开启 1：闭合	—
3	出入目标	target	varchar	255	0	—	—
4	抓拍图片	images	text	0	0	—	值为图片数组[{"img":""},{"img":""}...]
5	出入口	door	varchar	255	0	—	目标具体的出入口信息
6	采集时间	time	timestamp	6	0	—	—

示例 3：

```
{
  "type":"e03",
  "status":0,
  "target":"出入人标识（姓名等）",
  "images":[
    {"img":"抓拍图片 base64 编码"},
    {"img":"抓拍图片 base64 编码"},
    {"img":"抓拍图片 base64 编码"}
    ……
  ],
  "door":"前门",
  "time":"2022-06-28 10:00:00"
}
```

表 8　电源告警事件报文数据内容

序号	字段名称	字段代码	字段类型	字段长度	小数位	值域	备注
1	事件类型	type	varchar	10	0	e04	电源告警类型
2	告警等级	rank	numeric	5	1	1：一级 2：二级	—
3	告警内容	content	numeric	1	0	—	—
4	功率	gl	numeric	5	3	—	—
5	采集时间	time	timestamp	—	—	—	—

示例4：

```
{
  "type":"e04",
  "rank":"1",
  "content":"报警内容说明",
  "gl":3.4,
   "time":"2022-06-28 10:00:00"
}
```

表9　警报点维护事件报文数据内容

序号	字段名称	字段代码	字段类型	字段长度	小数位	值域	备注
1	事件类型	type	varchar	10	0	e99	维护事件类型
2	维护标识	whbz	numeric	1	0	1：开始维护 2：结束维护	—
3	维护事件唯一编码	whid	varchar	64	0	—	维护事件唯一编码
4	采集时间	time	timestamp	—	—	—	—

示例5：

```
{
  "type":"e99",
  "whbz":"1",
  "whid":"维护事件唯一编码",
  "time":"2022-06-28 10:00:00"
}
```

7.3.3　加密上传

7.3.3.1　边缘处理器在进行报文上传时应采用加密操作，传输密文为加密后的密文字节数组转16进制字符串。

7.3.3.2　加密报文内容按表10的规定，报文结构见示例。

表10　加密传输报文内容

一级结构内容	代码	值含义	备注
初始化向量	iv	—	初始化向量，长度固定16位，内容为“英文字母+数字”
数据阶段	stage	0：调试 1：正式	数据阶段
报文内容是否加密	insecret	true：加密； false：未加密。	—
ID编码	idbm	—	外键，引用警报点ID编码
密文内容	data	—	密文内容根据表3和表5～表8规定的内容进行组织，解密后即为相应密文的JSON内容 未采集到的参数用默认值“999”代替

示例：

```
{
"iv":"",     //初始化向量，长度固定 16 位，内容为英文字母+数字。
 "stage":"1", //阶段:0 测试 1 正式
"insecret":true,       //报文内容是否加密，true 加密，false 未加密。
"idbm":"",
 "data":"密文内容"       //密文内容根据不同报文类型格式进行组织,解密后即为响应密
文的 json 内容。详见【报文格式】。
}
```

7.3.4 数据存储

边缘处理器应具备数据本地存储功能，数据存储应符合 GB/T 39786 相关规定。

7.3.5 控制指令接收、执行与回复

边缘处理器应能对管理平台下发的供电电源开启与关闭控制指令进行接收、执行与回复。控制回复报文数据内容按表11的规定，报文结构见示例。

表 11 控制回复报文数据内容

序号	二级字段名称	二级字段代码	三级字段名称	三级字段代码	数据类型	字段长度	小数位	值域
1	指令唯一识别码	ccode	—	—	varchar	64	0	—
2	指令内容	devices	响应设备类型	device	varchar	64	0	gddykz：供电电源控制
			执行结果	status	varchar	10	0	true：执行成功 false：执行失败
			控制设备类型	tagcode	varchar	255	0	jbp：警报器 jbkzq：警报控制器
			开启/关闭指令	value	numeric	1	0	0：关闭 1：开启
3	采集时间	time	—	—	timestamp	6	0	—
4	读写类型	type	—	—	varchar	255	0	write：写入
注：一条控制报文若同时控制多个操作，则有多个回复报文，一个回复报文对应一次设备操作。								

示例：

```
{
  "ccode":"7099099322322",
  "devices":
  {
    "device":"gddykz",
    "status":"true",
    "tagcode":"jbq",
    "value":"0"
  },
  "time":"2022-06-28 10:00:00",
  "type":"write"
}
```

7.4 性能要求

7.4.1 实时性

在网络运行正常、接口数据传输通畅的情况下，边缘处理器处理传感设备上报的数据或管理平台下发的控制指令的时间应≤10秒。

7.4.2 容量

边缘处理器应能存储≥60天的业务数据量，数据存储容量应有一定裕度，存储单元应具有可扩充能力。

8 传输层

8.1 组网架构

边缘处理器与管理平台间的组网方式可包括光纤/网线、4G/5G等运营商网络或自组网方式，组网架构见图2。

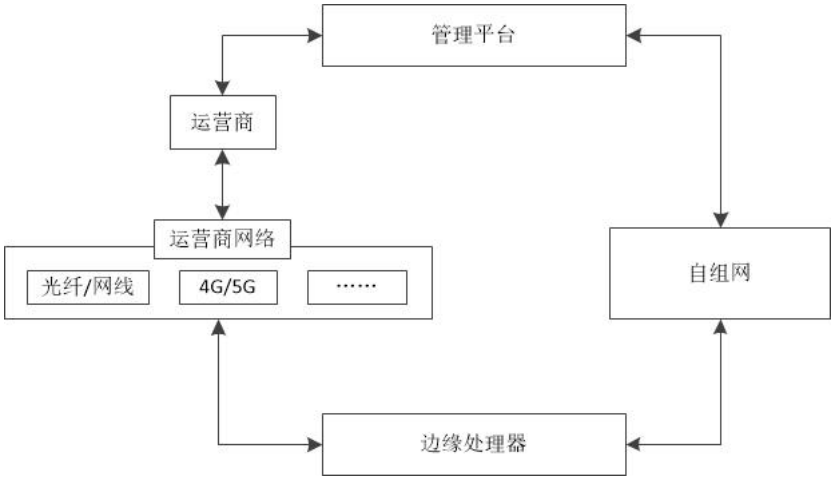

图 2 边缘处理器与管理平台间的组网架构图

8.2 通信协议

边缘处理器与管理平台间的通信方式采用无线通信和有线通信，通信协议采用MQTT、HTTPS等。

8.3 接入要求

8.3.1 管理平台应能以警报点为整体单元，录入登记该警报点内所有警报设施和传感设备的基础信息。

8.3.2 管理平台应向警报点发放唯一接入授权码，边缘处理器应通过该授权码接入管理平台。

8.3.3 接入授权码应为16位，由“阿拉伯数字+字母”组成。

8.4 传输性能

8.4.1 传输速率

采用运营商网络传输方式的，数据传输速率应不低于10 Mbps；采用自组网传输方式的，数据传输速率应不低于1 Mbps。

8.4.2 误码率

所有传输方式的误码率不应高于1×10^{-4}。

9 应用层

9.1 功能要求

9.1.1 数据接收与存储

9.1.1.1 管理平台应能接收边缘处理器上传的警报设施运行数据，并在符合安全要求的前提下进行数据解密运算。

9.1.1.2 管理平台应能对接收到的警报设施运行数据进行管理与存储。

9.1.2 数据分析

9.1.2.1 管理平台应能将边缘处理器上传的警种识别数据进行分析比对，若存在实际鸣放的警报类型、时间与任务规定要求不一致的情况，则判定该警报点存在警报误鸣事件。

9.1.2.2 管理平台应能根据接收到的警报设施运行数据，对区域内警报设施的完好率、统控率、覆盖率、鸣响率进行统计与分析，各指标的分析算法按附录 A 的规定。

9.1.3 数据查询

管理平台应设置省、市、县三级权限，并根据权限要求提供区域内警报设施的基础信息、运行数据、分析统计数据等的查询与显示功能。

9.1.4 控制指令下发

管理平台宜通过自动或人工方式向边缘处理器下发供电电源开启或关闭的下行控制指令。指令报文内容按表12的规定，报文结构见示例。

表 12 控制请求指令报文内容

二级字段名称	二级字段代码	三级字段名称	三级字段代码	数据类型	字段长度	小数位	值域
指令唯一识别码	ccode	—	—	varchar	64	0	—
指令内容	devices	响应设备类型	device	varchar	64	0	gddykz：供电电源控制【固定值】
		控制设备类型	tagcode	varchar	255	0	jbp：警报器 jbkzq：警报控制器
		开启/关闭指令	value	numeric	1	0	0：关闭 1：开启
请求时间	time	—	—	timestamp	6	0	—
读写类型	type	—	—	varchar	255	0	write：写入

示例：

```
{
  "ccode":"7099099322322",
  "devices":
  {
    "device":"gddykz",
    "tagcode":"jbq",
    "value":"0"
  },
  "time":"2022-06-28 10:00:00",
  "type":"write"
}
```

9.1.5 任务生成与管理

管理平台应能对工作状态显示为故障的警报器、警报控制器、后备电源，生成相对应的维修/巡检任务，并结合表9规定的维护事件报文内容，对警报管理员、维保单位的执行情况进行管理。

9.2 性能要求

9.2.1 可靠性

管理平台的平均故障间隔时间应≥4 500小时。

9.2.2 开放性

管理平台应能允许不同厂家的终端接入。

9.2.3 容量

管理平台应能存储≥3年的业务数据量。

10 安全

10.1 一般要求

管理平台应符合 GB/T 22239—2019 中 8.1 条规定的安全通用要求和 8.4 条规定的物联网安全扩展要求。

10.2 物联感知安全

10.2.1 传感设备的物联接口安全应符合 GB/T 36951—2018 中 6.4.7 条的要求。

10.2.2 台站设备（含警报器、警报控制器、后备电源）提供给边缘处理器的数据应通过对应接口拓展板或串口读取，不应开放鸣放控制指令通道。

10.3 传输安全

传输完整性应符合GB/T 37025—2018中7.1条的要求，传输保密性应符合GB/T 37025—2018中7.8条的要求。

10.4 系统应用安全

10.4.1 访问控制应符合 GB/T 37093—2018 中 6.2.3 条的要求。

10.4.2 日志审计应符合 GB/T 37093—2018 中 6.2.8 条的要求。

11 试验方法

11.1 功能试验

11.1.1 功能试验项目包括 7.3 条规定的物联感知层功能要求和 9.1 条规定的应用层功能要求。

11.1.2 功能试验步骤为：

a) 按第 8 章的要求实现组网互联后，保证管理平台、边缘处理器、传感设备、警报设施处于运转工作；

b) 对照功能要求逐条检查，核实管理平台、边缘处理器和传感设备是否具备规定的功能。

11.2 性能试验

11.2.1 物联感知层

11.2.1.1 实时性

实时性试验方法如下：

——常态报文实时性测试，设定边缘处理器的常态报文上传频率为 10 秒，查看管理平台是否可以在 1 分钟内正常显示 6 条常态报文；

——接收控制指令实时性测试，管理平台下发控制指令，查看是否可以在 10 秒内接收到边缘处理器返回的数据报文；

——事件报文实时性测试，使用工具或测试设备，触发告警阈值，查看管理平台是否可以在 10 秒内接收并显示告警报文。

11.2.1.2 容量

查询边缘处理器60天以内的常态报文历史数据，核对试验结果是否符合7.4.2条的规定。

11.2.2 传输层

11.2.2.1 传输速率

运行网络测试工具，进行数据传输操作，观察并记录网络测试工具上显示的传输速率。测试重复执行多次，计算平均传输速率，核对试验结果是否符合8.4.1条的规定。

11.2.2.2 误码率

设置边缘处理器以10秒的间隔主动上传数据，且上传不少于50次，记录管理平台收到的数据，核对试验结果是否符合8.4.2条的规定。

11.2.3 应用层

11.2.3.1 可靠性

按照GB/T 5080.7—1986中第5章的规定进行试验，核对试验结果是否符合9.2.1条的规定。

11.2.3.2 开放性

将3家以上不同厂商生产的边缘处理器接入管理平台，核对试验结果是否符合9.2.2条的规定。

11.2.3.3 容量

模拟插入3年的业务数据量，检查确认管理平台存储的3年间的业务数据内容、数据顺序等，核对试验结果是否符合9.2.3条的规定。

11.3 安全试验

11.3.1 一般安全试验

检查确认管理平台是否已通过网络安全等级保护三级以上测评，并取得相应备案证书，核对备案证书测评指标是否符合10.1条的规定。

11.3.2 物联感知安全

传感设备和边缘处理器的物理接口安全试验流程如下：

a) 检查确认传感设备和边缘处理器是否有闲置的物理接口；
b) 若存在闲置物理接口的，对所有闲置接口进行接线尝试读写等操作，确认闲置接口被禁用；
c) 审查传感设备和边缘处理器制造商提交的文件，验证确认无法通过外部存储设备自启动。

11.3.3 传输安全

数据传输安全试验要求如下：

a) 检查数据传输信任能力，确认边缘处理器与传感设备、管理平台间传输管理、鉴别等敏感信息是否建立可信路径，此路径在逻辑上应与其他通信传输路径隔离；
b) 检查数据传输策略和程序，确认可明文传输的信息类别和范围，对于敏感数据，例如口令、私钥、对称密钥等，是否采用加密传输策略和程序。

11.3.4 系统应用安全

11.3.4.1 检查管理平台是否制定和执行访问控制策略。

11.3.4.2 检查管理平台是否对边缘处理器和终端设备接入安全检查进行日记审计，日志内容是否包含日期/时间、时间类型、事件主体、事件描述、成功/失败的信息。

12 系统维护

12.1 常规维护

12.1.1 传感设备及边缘处理器的常规维护频次宜根据实际情况确定，维护内容包括传感器配件维护、软件升级等。

12.1.2 管理平台的常规维护频次宜根据系统运行状况确定，维护内容包括网络及网络设备、服务器、存储、数据库、中间件等的检查与维护。

12.2 年度检修

12.2.1 应每年进行 1 次全系统检修，年度检修时间可结合警报年度维修时间确定。

12.2.2 年度检修内容包括警报点传感设备、边缘处理器以及管理平台的全面检查，必要时应更换受损

件。

12.3 应急维护

出现警报点传感设备、边缘处理器损坏或管理平台通讯故障、数据异常等情况时，应进行应急维护。

12.4 记录留档

12.4.1 应采用电子或纸质形式留档常规维护、年度检修、应急维护记录。

12.4.2 常规维护和年度检修的留档记录应包括检查或检修的人员、时间、地点、内容、设备状态、结果等。

12.4.3 应急维护的留档记录应包括维修时间、人员以及故障设备、故障原因、维修情况、维修结果等。

附 录 A
（规范性）
警报设施完好率、统控率、覆盖率、鸣响率分析算法

A.1 完好率

区域内警报设施完好率的分析算法按式（A.1）。

$$B = \frac{d}{e} \times 100\% \cdots\cdots (A.1)$$

式中：

B——警报设施完好率；

d——运行数据中未出现工作状态为故障的警报设施数量；

e——录入登记的警报设施总数。

A.2 统控率

区域内警报设施统控率的分析算法按式（A.2）。

$$D = \frac{r}{e} \cdots\cdots (A.2)$$

式中：

D——警报设施统控率；

r——警报控制器与警报器数据关联且运行数据均正常的警报设施数量；

e——录入登记的警报设施总数。

A.3 覆盖率

区域内警报设施覆盖率的分析算法按式（A.3）。

$$X = \frac{S_1 - S_2 - S_3}{S_0} \cdots\cdots (A.3)$$

式中：

X——警报设施覆盖率；

S_1——警报设施鸣响覆盖面积；

S_2——警报设施鸣响重叠面积；

S_3——区域内非建成区面积；

S_0——区域内建成区总面积。

A.4 鸣响率

区域内警报设施鸣响率的分析算法按式（A.4）。

$$Z = \frac{v}{e} \cdots\cdots (A.4)$$

式中：

Z——警报设施鸣响率；

v——正常鸣放的警报设施数量；

e——录入登记的警报设施总数。