ICS 03.240
T 36
备案号:87926—2022

YZ

中华人民共和国邮政行业标准

YZ/T 0186—2022

邮政业智能视频监控系统采集设备技术要求

Technical requirements for acquisition device of intelligent video surveillance system for postal industry

2022-11-17 发布　　2023-02-01 实施

国家邮政局　发布

目　　次

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》的规定起草。

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。

本文件由国家邮政局提出。

本文件由全国邮政业标准化技术委员会(SAC/TC 462)归口。

本文件起草单位：华为技术有限公司、杭州海康威视数字技术股份有限公司、浙江大华技术股份有限公司、上海锐承通讯技术有限公司、国家安全防范报警系统产品质量监督检验中心(北京)。

本文件主要起草人：戴列峰、王雯、方贵明、赵青、刘军、张楠、徐朝辉、何学文、李连威、卢雅鹏、林勉嵩。

邮政业智能视频监控系统采集设备技术要求

1 范围

本文件规定了邮政业智能视频监控系统采集设备的应用场景要求、技术要求和试验方法。

本文件适用于邮政业智能视频监控系统中使用的采集设备的选型和验收,以及采集设备生产厂家的规划和研发。

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 16796 安全防范报警设备安全要求和试验方法

GB 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB 35114—2017 公共安全视频监控联网信息安全技术要求

GA/T 1127—2013 安全防范视频监控摄像机通用技术要求

GA/T 1128—2013 安全防范视频监控高清晰度摄像机测量方法

GA/T 1399.2—2017 公安视频图像分析系统 第2部分:视频图像内容分析及描述技术要求

GA/T 1400.4 公安视频图像信息应用系统 第4部分:接口协议要求

YZ/T 0187—2022 邮政业智能视频监控系统接口要求

YZ/T 0188—2022 邮政业寄递车辆智能视频监控系统技术规范

3 术语和定义

GA/T 1127—2013 界定的以及下列术语和定义适用于本文件。

3.1

邮政业智能视频监控系统 intelligent video surveillance system for postal industry

具备邮政业视频图像信息采集、智能分析、存储、传输,以及违规事件报警及处理等功能的信息系统,包括前端设备、寄递企业智能视频监控平台和邮政管理智能视频监控平台。

[来源:YZ/T 0187—2022,3.1]

3.2

前端设备 front-end device

安装于寄递企业监控现场或寄递车辆,用于视频图像信息采集、编/解码、存储、智能分析、传输、安全控制等的设备,包括采集设备、前端智能分析设备、车载终端等。

[来源:YZ/T 0187—2022,3.2]

3.3

采集设备 acquisition device

安装于寄递企业监控现场或寄递车辆,主要实现视频图像信息采集、编/解码等功能的前端设备,包括固定场所摄像机和车载摄像机。

3.4

枪型摄像机　box camera

外形结构为长方体或圆柱体的摄像机。

3.5

球型摄像机　speed dome camera

外形结构为球型,具有镜头、云台(含解码)和球型防护罩的一体化摄像机。

3.6

半球型摄像机　dome camera

外形结构为半球型,具有镜头、云台(含解码)和半球型防护罩的一体化摄像机。

3.7

正检　true positive

视频图像中出现应被检测的目标或事件,且检测输出了正确的检测结果。

[来源:GA/T 1399.2—2017,3.1.1,有修改]

3.8

漏检　false negative

视频图像中出现应被检测的目标或事件,但未检测输出正确的检测结果。

[来源:GA/T 1399.2—2017,3.1.2,有修改]

3.9

误检　false positive

视频图像中未出现应被检测的目标或事件,但检测输出了检测结果。

[来源:GA/T 1399.2—2017,3.1.3,有修改]

3.10

检测率　true positive rate

检测出的正确目标数或正确事件数与视频图像中应被检测的目标数或事件数的百分比,见式(1)。

$$检测率 = \frac{正检数}{漏检数 + 正检数} \times 100\% \quad \cdots\cdots(1)$$

[来源:GA/T 1399.2—2017,3.1.4,有修改]

3.11

误检率　false positive rate

检测出的目标或事件中,错误目标数或事件数所占的百分比,见式(2)。

$$误检率 = \frac{误检数}{误检数 + 正检数} \times 100\% \quad \cdots\cdots(2)$$

[来源:GA/T 1399.2—2017,3.1.5,有修改]

3.12

识别准确率　recognition accuracy

正确识别的目标数与应被正确识别的目标总数的百分比,见式(3)。

$$识别准确率 = \frac{正确识别的目标数}{应被正确识别的目标总数} \times 100\% \quad \cdots\cdots(3)$$

[来源:GA/T 1399.2—2017,3.1.6,有修改]

3.13

水平分辨力　horizontal resolution

在图像高度相等的水平尺寸内可分辨的垂直黑白条数(TV 线)。

[来源:GA/T 1127—2013,3.1.14]

4 缩略语

下列缩略语适用于本文件。

AES:高级加密标准(Advanced Encryption Standard)
ARP:地址解析协议(Address Resolution Protocol)
DES:数据加密标准(Data Encryption Standard)
HTTPS:超文本传输安全协议(Hyper Text Transfer Protocol Secure)
ICMP:互联网控制报文协议(Internet Control Message Protocol)
IP:网际互连协议(Internet Protocol)
MAC:媒体介入控制(Media Access Control)
MD5:消息摘要算法 5(Message Digest Algorithm 5)
MJPEG:移动式连续图像压缩技术(Motion Joint Photographic Experts Group)
NAT:网络地址转换(Network Address Translation)
RC4:RC4 加密算法(Rivest Cipher 4)
SFTP:安全文件传输协议(Secure File Transfer Protocol)
SHA-1:安全散列算法 1(Secure Hash Algorithm 1)
SQL:结构化查询语言(Structured Query Language)
SSH:安全外壳协议(Secure Shell)
SYN:同步序列编号(Synchronize Sequence Numbers)
TVL:电视行(TV Line)
XML:可扩展标记语言(Extensible Markup Language)
XSS:跨站脚本攻击(Cross Site Scripting)

5 应用场景要求

5.1 应用场景分类

邮政业智能视频监控系统通过采集设备检测监控邮件快件、寄递车辆及工作人员等的实时状态,并对异常情况进行报警,包括如下应用场景:

——营业场所:包括停车及装卸区、暂存区、业务接待区、操作区、邮筒(箱)区、特定人员授权区、消防通道和充电区等区域;
——处理场所:主要针对邮件快件的分拣和运送,具体场景包括处理场所出入口、安检区、分拣区、卸载/装载区、异常邮件快件处理区、物料存放区等区域;
——运输:运输场景包括车辆前后左右区域、车辆驾驶室内区域和驾驶员驾驶区域。

5.2 应用场景采集要求

5.2.1 营业场所

5.2.1.1 停车及装卸区

应对停车及装卸区的暴力分拣行为、邮件快件着地状态、车辆装载率等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式安装枪型摄像机;
b) 采集设备安装高度满足检测监控要求,根据安装区域空间条件,宜为 3 m~5 m,俯仰角度为 10°~

40°,正对车厢门,监控画面应能透视整个车厢底面、后面;

c) 监控画面中工作人员至少上半身无遮挡,清晰可见,完整监控工作人员动作和作业过程。

5.2.1.2 暂存区

应对暂存区仓库内外的邮件快件堆积状态、是否产生烟火等进行采集监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装或顶装方式,安装半球型摄像机或枪型摄像机;

b) 采集设备安装高度满足检测监控要求,根据安装区域空间条件,宜为4 m~6 m,俯仰角度为10°~40°,采集区域覆盖整个邮件快件堆积区域;

c) 监控画面内无明显遮挡。

5.2.1.3 操作区

应对操作区的邮件快件破损状态、邮件快件堆积状态等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装或顶装方式,安装枪型摄像机、半球型摄像机或球型摄像机;

b) 采集设备安装高度满足检测监控要求,根据安装区域空间条件,宜为3 m~6 m,俯仰角度为10°~40°,采集区域覆盖整个操作区;

c) 监控画面内无明显遮挡。

5.2.1.4 业务接待区

5.2.1.4.1 柜台及寄递区

应对柜台及寄递区的营业状态、人证比对、开箱验视行为和佩戴口罩状态等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用顶装方式,安装半球型摄像机或球型摄像机;

b) 采集设备安装高度满足检测监控要求,根据安装区域空间条件,宜为3 m~5 m,俯仰角度为10°~40°,采集区域覆盖整个营业柜台或工作人员的工位;

c) 监控画面中工作人员至少上半身无遮挡,清晰可见,完整监控工作人员动作和作业过程。

5.2.1.4.2 收寄验视区

应对收寄验视区的开箱验视行为、邮件快件破损状态等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式,安装枪型摄像机;

b) 采集设备安装满足检测监控要求,根据安装区域空间条件,宜为高度4 m~6 m,俯仰角度为10°~40°,摄像机正对收寄验视区,监控画面覆盖整个收寄验视区;

c) 监控画面中工作人员至少上半身无遮挡,能够看清工作人员的收寄验视动作,工作人员的半身高度占画面高度1/4以上。

5.2.1.5 邮筒(箱)区

应对邮政邮筒(箱)开箱频次进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装方式,安装枪型摄像机;

b) 采集区域能覆盖整个工作人员及邮筒(箱);

c) 工作人员图像直立完整,全身无遮挡,开箱过程可见;

d) 监控画面内无明显遮挡。

5.2.1.6 授权人员区

应对授权人员区的人员进行人脸识别抓拍和佩戴口罩检测,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式,安装人脸识别摄像机;

b) 采集设备安装高度满足检测监控要求,根据安装区域空间条件,宜为2 m~2.5 m,镜头倾斜10°~

15°,左右偏角25°以内,视频图像采集画面正对人流行进方向;

c) 监控画面中工作人员至少上半身无遮挡,清晰可见,完整监控工作人员的动作和作业过程。

5.2.1.7 消防通道

应对消防通道的消防器械数量及消防通道拥堵状态等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装、横杆装、立杆装等方式,安装枪型摄像机;

b) 采集设备安装高度满足检测监控要求,根据安装区域空间条件,宜为3 m~5 m,俯仰角度为10°~40°,采集区域覆盖整个消防通道区域。

5.2.1.8 充电区

应对充电区的消防器械放置状态、是否产生烟火等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式,安装枪型摄像机;

b) 摄像机安装高度满足检测监控要求,根据安装区域空间条件,宜为2 m~3.5 m,镜头倾斜10°~15°,正对充电区,监控画面覆盖整个充电区;

c) 视频画面中,可看清充电装置及消防器械的位置。

5.2.2 处理场所

5.2.2.1 处理场所出入口

应对处理场所出入口的人员进行人脸识别抓拍,并对其进出状态及佩戴口罩行为等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式,安装枪型摄像机;

b) 摄像机安装高度满足检测监控要求,根据安装区域空间条件,宜为2 m~3.5 m,镜头倾斜10°~15°,正对场所出入口,覆盖整个出入口;

c) 视频画面中,能够看清进出人员的脸部,人员的全身高度宜占画面高度的1/3以上。

5.2.2.2 安检区

应对安检区的未佩戴口罩行为、人员离岗行为、安检机作业合规等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式,安装枪型摄像机、半球型摄像机或球型摄像机;

b) 摄像机安装在安检机斜前/后方30°~60°范围内,或正对安检机邮件快件出口;

c) 视频画面中,安检机占画面面积1/6~1/4为宜,安检机及防辐射铅帘、安检机工位及工位上的安检人员无遮挡,清晰可见。

5.2.2.3 分拣区

应对分拣区的工作人员未佩戴口罩行为、暴力分拣行为、传送带作业违规行为等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式,安装枪型摄像机、半球型摄像机或球型摄像机;

b) 摄像机安装在工作人员正面45°~135°范围内;

c) 视频画面中,工作人员的全身高度占画面高度1/4以上或半身高度占画面高度1/6以上。

5.2.2.4 卸载/装载区

应对卸载/装载区的暴力分拣行为、传送带作业违规行为、车辆装载率等进行检测监控,视频采集设备安装和采集应符合如下要求:

a) 采用壁装、吊装方式,安装枪型摄像机、半球型摄像机或球型摄像机;

b) 对于暴力分拣行为检测,摄像机安装在工作人员正面45°~135°范围内,视频画面中,工作人员的全身高度占画面高度1/4以上或半身高度占画面高度1/6以上;

c） 对于传送带作业违规行为检测，摄像机安装在传送带作业区，视频画面中，传送带宽度占视频宽度1/6以上，工作人员的全身高度占画面高度1/8以上；

d） 对于车辆装载率检测，摄像机安装正对车厢门，俯仰角度为10°～40°，监控画面能透视整个车厢底面、后面；

e） 监控画面中工作人员至少上半身无遮挡，清晰可见，完整监控工作人员动作和作业过程。

5.2.2.5 异常邮件快件处理区

应对异常邮件快件处理区的邮件快件堆积状态等进行检测监控，视频采集设备安装和采集应符合如下要求：

a） 采用壁装、吊装方式，安装枪型摄像机、半球型摄像机或球型摄像机；

b） 采集设备安装高度满足检测监控要求，根据安装区域空间条件，宜为4 m～6 m，俯仰角度为10°～40°，采集区域覆盖整个异常邮件快件处理区域；

c） 视频画面中异常邮件快件处理区位于画面中心，且工作人员处理异常邮件快件的活动范围占整个画面面积不低于60%；

d） 监控画面内无明显遮挡。

5.2.2.6 物料存放区

应对物料存放区的邮件快件堆积状态、场地是否漏水、是否产生烟火等进行检测监控，视频采集设备安装和采集应符合如下要求：

a） 采用壁装、吊装方式，安装变焦枪型摄像机、半球型摄像机或球型摄像机；

b） 采集设备安装高度满足检测监控要求，根据安装区域空间条件，宜为4 m～6 m，俯仰角度为10°～40°，摄像机正对物料存放区，监控画面覆盖整个物料存放区。

5.2.2.7 人车分流区

应在处理场所出入口、卸载/装载区等需对人车进行分流或隔离的区域进行人车混行检测，视频采集设备安装和采集应符合如下要求：

a） 采用壁装、吊装方式，安装变焦枪型摄像机、半球型摄像机或球型摄像机；

b） 采集设备安装高度满足检测监控要求，根据安装区域空间条件，宜为4 m～6 m，俯仰角度为0°～45°，摄像机正对人车分流区，监控画面覆盖整个人车分流区。

5.2.3 运输

应对运输场景的车辆前后左右区域、车辆驾驶室内区域、驾驶员驾驶区域等进行检测监控，车载摄像机的配置要求、采集要求和安装要求应符合YZ/T 0188—2022中6.1.2、6.1.3.2、6.5.2的规定。

5.3 应用场景功能配置

采集设备的智能分析功能应按不同应用场景进行配置，具体要求见表1。

表1 应用场景功能配置表

序号	智能分析功能	应用场景		
		营业场所	处理场所	运输
1	暴力分拣行为检测	●	●	
2	邮件快件堆积状态检测	●	●	
3	安检机作业合规检测	●	●	
4	人员离岗检测	○	○	

表1　应用场景功能配置表(续)

序号	智能分析功能	应用场景		
		营业场所	处理场所	运输
5	传送带作业违规行为检测		●	
6	画面质量检测	○	○	○
7	烟火识别	●	●	
8	作业越界检测		○	
9	消防器械数量检测	●	●	
10	车辆装载率检测	○	○	
11	邮件快件着地检测	●	●	
12	人脸识别	○	○	○
13	邮件快件破损检测	○	○	
14	传送带掉货检测		●	
15	场地漏水检测	○	○	
16	人员着装检测	●	●	
17	人证比对	●		
18	邮政邮筒(箱)开箱频次检测	●		
19	营业状态检测	●		
20	开箱验视检测	●	○	
21	消防通道拥堵检测	●	●	
22	人车混行检测		●	
23	口罩佩戴检测	●	●	
24	驾驶员状态监测与报警			●
25	车辆盲区监测			●
26	车辆烟火监测与报警功能			●
27	高级驾驶辅助			○
注：●表示必备功能；○表示可选功能				

6　技术要求

6.1　固定场所摄像机技术要求

6.1.1　一般要求

6.1.1.1　外观、结构和外壳防护能力

应符合 GA/T 1127—2013 中 5.1.1 的要求。

6.1.1.2 接口

电气接口应符合 GA/T 1127—2013 中 5.1.2 的要求,系统接口应符合 GB/T 28181 规定的音视频接口协议要求、GA/T 1400.4 规定的数据接口协议要求和 YZ/T 0187—2022 规定的邮政业智能视频监控系统接口要求。

6.1.1.3 电源、环境适应性和电磁兼容性

应符合 GA/T 1127—2013 中 5.1.3、5.1.4、5.1.5 的要求。

6.1.1.4 电气安全性

应符合 GB 16796 的规定。

6.1.2 功能要求

6.1.2.1 基本功能

6.1.2.1.1 应符合 GA/T 1127—2013 中 5.2.1 规定的自动增益、自动白平衡调整、逆光补偿、日夜模式、电子快门等功能要求。

6.1.2.1.2 视频编码应支持 H.264、H.265 和 MJPEG 格式。

6.1.2.1.3 应符合 GA/T 1127—2013 中 5.2.2 规定的时钟同步、音视频参数调节、在线升级、配置保存获取、恢复出厂设置和重启、字符叠加、多码流、主动注册、本机存储、Web 服务、报警、日志记录、NAT 穿越、动态域名解析等功能要求。

6.1.2.1.4 应支持断网续传,当网络断开后能自动重连,并自动续传网络断开期间的视频等信息。

6.1.2.1.5 宜具备宽动态能力。

6.1.2.2 抓拍功能

应支持定时、手动、事件触发抓拍图片。

6.1.2.3 防抖功能

宜支持防抖功能,减轻摄像机晃动产生的图像画面抖动。

6.1.2.4 智能分析功能

6.1.2.4.1 概述

智能分析功能宜通过采集设备实现,也可通过企业前端智能分析设备或寄递企业智能视频监控平台实现。通过采集设备实现的,应符合表 1 的配置要求和 6.1.2.4.2 ~ 6.1.2.4.24 的要求。

6.1.2.4.2 暴力分拣行为检测

应能检测出视频图像中工作人员用抛、甩、丢、扔、倒等动作使邮件快件脱离原有接触点(起始点)至新接触点(终点)距离超过 30 cm 的行为,包括但不限于工作人员手部抬起过高及抬起速度过快、工作人员不转身直接向后投掷邮件快件、工作人员使用脚踢邮件快件等,并输出报警事件。

视频图像中工作人员至少上半身无遮挡,人员所占区域面积不小于整个画面的 10%,人员高度不小于 100 像素,宽度不小于 40 像素。在此条件下检测率≥80%、误检率≤10%。

6.1.2.4.3 邮件快件堆积状态检测

应能检测出视频图像中邮件快件画面覆盖率超过设定值(占整个拍摄画面的比例)且持续时间超过设定时间的状态,并输出报警事件。包括以下场景:

a) 运行中的传送带,邮件快件在平面上的覆盖率超过设定值;

b) 在设定的区域内,静止邮件快件在平面上的覆盖率超过设定值。

视频图像中单件邮件快件大于(80×80)像素,在此条件下检测率≥90%、误检率≤10%。

6.1.2.4.4 安检机作业合规检测

在工作时间内,应能检测出视频图像中的安检机及工作人员的以下状态,并输出报警事件:

a) 安检机不运转状态超过设定时间;

b) 工作人员离岗行为:工作人员数量少于设定数量且持续时间超过设定时间,智能安检机除外;

c） 工作人员玩手机行为：工作人员手持手机状态且持续时间超过设定时间。

视频图像中安检机及安检机工作台大小超过画面1/6，工作人员头肩大于(60×60)像素，在此条件下检测率≥90%、误检率≤10%。

6.1.2.4.5 人员离岗检测

应能检测出视频图像中设定区域内的工作人员数量少于设定数量且持续时间超过设定时间的行为并输出报警事件。

视频图像中目标人员头肩面积大于(60×60)像素，在此条件下检测率≥90%、误检率≤10%。

6.1.2.4.6 传送带作业违规行为检测

应能检测出视频图像中工作人员翻越传送带、在传送带上行走或着装不规范的行为，并输出报警事件。

视频图像中工作人员占画面高度1/6以上，在此条件下检测率≥80%、误检率≤10%。

6.1.2.4.7 画面质量检测

应能对采集的视频图像质量进行检测诊断并告警，且满足如下要求：

a） 对环境光线变化原因引起的视频图像过亮或过暗的亮度异常现象进行检测并告警；

b） 对视频图像中出现的雪花噪声干扰，混有呈带状、波纹、网状等带有周期性的叠加噪声干扰进行检测并告警；

c） 对视频图像中出现模糊或抖动情况进行检测并告警；

d） 对视频图像在某一范围颜色值分布过多而导致图像整体偏色的现象进行检测并告警；

e） 对采集设备镜头被物体遮挡的情况进行检测并告警；

f） 对采集设备被移动或转动等更换场景的情况进行检测并告警。

6.1.2.4.8 烟火识别

应能检测出视频图像中的火焰、烟雾，并输出报警事件。

对于视频图像中大于80像素且持续时间不低于10 s的烟火目标，在此条件下检测率≥90%、误检率≤10%、检测时间≤5 s。

6.1.2.4.9 作业越界检测

应能检测出视频图像中人员越过或进入设定的警戒区域的行为，并输出报警事件。

视频图像中目标人员上半身及中部可辨识，高度不小于100像素，宽度不小于40像素，在此条件下检测率≥80%、误检率≤10%。

6.1.2.4.10 消防器械数量检测

应能检测出视频图像中设定区域内灭火器数量，当灭火器数量少于设定数量时，输出报警事件。

视频图像中灭火器尺寸大于(80×80)像素，露出部分占灭火器整体2/3以上，在此条件下检测率≥80%、误检率≤10%。

6.1.2.4.11 车辆装载率检测

应能检测出视频图像中车厢内邮件快件所占图像面积与车厢所占图像面积的占比，输出相应装载率。

视频图像中邮件快件目标尺寸大于(60×60)像素，在此条件下检测率≥80%、误检率≤10%。

6.1.2.4.12 邮件快件着地检测

应能检测出视频图像中邮件快件与地面之间无其他介质(如托盘)而直接接触地面的情形，并输出报警事件。

视频图像中目标像素大于(60×60)像素，在此条件下检测率≥70%、误检率≤10%。

6.1.2.4.13 人脸识别

应能对视频采集区域内出现的人脸进行检测，并与指定人脸库中的人脸进行比对和识别。

视频图像中的人脸两眼之间像素大于60像素，上下偏转不超过30°，左右偏转不超过45°，在此条件

下识别准确率≥95%。

6.1.2.4.14 邮件快件破损检测

应能检测出视频图像中处于静止状态的邮件快件,其破损区图像面积与邮件快件图像面积的占比,邮件快件破损区面积占比超过设定值时,输出报警事件。宜支持破损类型分类,包括穿透性损坏、压痕/皱褶、湿损、裸露包装等。

视频图像中邮件快件占画面的1/10以上,在此条件下检测率≥70%、误检率≤10%。

6.1.2.4.15 传送带掉货检测

应能检测出视频图像中设定检测区域内的邮件快件从传送带或高处掉落至地面或其他介质上的行为,并输出报警事件。

视频图像中邮件快件占画面的1/20以上,在此条件下检测率≥70%、误检率≤10%。

6.1.2.4.16 场地漏水检测

应能检测出视频图像中场地上的水渍目标并输出报警事件。

视频图像中水渍大于(80×80)像素,在此条件下检测率≥70%、误检率≤10%。

6.1.2.4.17 人员着装检测

应能检测出视频图像中工作人员头发未包扎、着装与指定工作服相似性比对分析不符合设定值的行为,并输出报警事件。

视频图像中工作人员图像完整且宽度大于60像素,在此条件下检测率≥70%、误检率≤10%。

6.1.2.4.18 人证比对

应能采集人脸图像,将采集的人脸图像与采集的身份证进行相似性比对分析,输出身份比对结果(匹配相似度等)。

视频图像中人脸转动角、偏转角、转动角小于15°,人脸两眼之间像素不小于50像素或人脸宽度大于100像素,在此条件下识别准确率≥99%。

6.1.2.4.19 邮政邮筒(箱)开箱频次检测

应能检测出视频图像中进入设定的邮政邮筒(箱)监测区域且符合着装要求的工作人员进行开邮筒(箱)的动作行为,且停留时间满足设定时间则为一次邮筒(箱)开箱,统计输出工作人员的开箱次数。

视频图像中目标人员图像完整且宽度大于32像素,在此条件下识别准确率应≥80%。

6.1.2.4.20 营业状态检测

应能检测出视频图像中设定的营业监测区域和营业时间内有无工作人员,无工作人员情况持续时间超过设定时间,输出营业状态结果。

视频图像中工作人员头肩面积大于(50×50)像素,在此条件下检测率≥90%、误检率≤10%。

6.1.2.4.21 开箱验视检测

应能检测出视频图像中工作人员的开箱动作,对未检测出开箱动作的行为输出报警事件。

视频图像中被开箱的邮件快件占画面的1/10以上,在此条件下检测率≥70%、误检率≤10%。

6.1.2.4.22 消防通道拥堵检测

应能检测出视频图像中设定的消防通道监测区域内的人员、机动车、非机动车、物体等目标,对于监测区域内存在机动车、非机动车或物体目标而无人员目标且持续时间超过设定时间的情形,输出报警事件。

视频图像中占用目标大于(120×120)像素,在此条件下检测率≥80%、误检率≤10%。

6.1.2.4.23 人车混行检测

应能在设置人车分流围栏和标线的场景检测出人车混行的行为,当工作人员进入机动车区域或机动车侵占行人区域时,输出报警事件。

视频图像中标线和围栏清晰可辨,人员目标高度大于100像素,车辆目标宽度大于100像素,在此条件下检测率≥80%、误检率≤10%。

6.1.2.4.24　口罩佩戴检测

应能检测出视频图像中工作人员未正确佩戴口罩的行为,并输出报警事件。

视频图像中工作人员人脸图像完整且人脸宽度大于60像素,在此条件下检测率≥90%、误检率≤10%。

6.1.2.4.25　智能扩展功能要求

具备智能检测功能在线升级、扩展和多算法的运行管理维护能力,且满足如下要求:

a)　应支持智能检测算法在线更新和升级;

b)　应支持远程部署新的智能检测算法;

c)　宜支持多种算法应用并行运行,算法应用之间资源和故障隔离,单一算法的管理操作应不影响其他算法应用;

d)　宜支持接入其他视频采集设备的视频流进行智能检测分析。

6.1.3　性能要求

性能指标应符合表2的要求。

表2　性能指标要求

序　号	性能名称	指标要求
1	水平分辨力(TVL)	≥1 000
2	水平分辨率(像素)	≥1 920
3	帧速率(fps)	≥25
4	最低照度(lx)	≤0.01/F1.2
5	最大亮度鉴别等级(级)	≥11
6	信噪比(dB)	≥45
7	延时(ms)	≤500
8	几何失真	≤5%
9	平均色彩还原误差	≤15(色温6 500K)
		≤20(其他色温)

6.2　车载摄像机技术要求

6.2.1　一般要求

应符合YZ/T 0188—2022中6.1.3.2的规定。

6.2.2　功能要求

应符合YZ/T 0188—2022中6.2.2.1的规定。

6.2.3　性能要求

应符合YZ/T 0188—2022中6.4的规定。

6.3 安全要求

6.3.1 网络安全

6.3.1.1 通信安全

应符合如下要求：

a) 能防范 ICMP、SYN 泛洪与畸形报文、ARP 欺骗等常见的网络攻击；

b) 采集设备接入网络获得 IP 之前应通过口令机制验证设备身份，防范设备仿冒、网络私接。

6.3.1.2 安全防护

应符合如下要求：

a) 支持安全启动功能，在启动过程中，校验引导程序、操作系统、应用软件的完整性，阻止非法程序在设备上运行；

b) 应支持检测病毒/木马的防护功能；

c) 宜具备对恶意攻击和异常行为的检测和报警功能。

6.3.2 Web 安全

6.3.2.1 身份鉴别

应符合如下要求：

a) 支持对登录用户进行身份标识和鉴别，身份标识具有唯一性，并保障身份鉴别机制不可被绕过；

b) 支持基于账号口令进行用户身份鉴别，支持账号口令的有效期设置；

c) 具备登录失败处理功能，如限制非法登录次数、要求输入验证码等机制；

d) 符合 GB 35114—2017 中 6.3.2 的规定，支持基于数字证书与管理平台双向身份认证，数字证书格式应符合 GB 35114—2017 附录 A 的规定。

6.3.2.2 访问控制

应符合如下要求：

a) 支持用户配置 IP 地址、协议类型等访问控制策略，控制采集设备请求或相应的通信方；

b) 支持仅允许经过身份鉴别的用户主体执行权限范围内的操作。

6.3.2.3 Web 攻击防范

应符合如下要求：

a) 默认启用 SFTP、HTTPS、SSH 等安全协议进行上传、下载、请求和响应等，保障 Web 通信安全；

b) 对自身可控组件以外的数据进行检验，拒绝没有通过校验的数据，以防范 SQL/XML 注入、XSS 等攻击；

c) 支持使用 Web 验证码等机制防范 Web 攻击；

d) 支持设置会话超时机制，会话超时后，用户如需继续操作，应再次经过身份鉴别；

e) Web 通信过程中，当检测到用户的 IP、UserAgent 等信息发生了变化，强制销毁当前会话，并要求用户重新登录。

6.3.3 日志记录和审计

应符合如下要求：

a) 支持日志记录功能，日志记录覆盖每个用户，对重要的用户行为和重要的安全事件进行审计；

b) 支持对系统启动、关闭、升级等记录日志；

c) 审计日志包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

d) 对日志记录进行保护，避免受到非预期的删除、修改或覆盖等；

e） 对日志进程进行保护,防止未经授权的中断;
f） 支持将审计日志上传至寄递企业智能视频监控平台。

6.3.4 数据安全

应符合如下要求:
a） 采用校验技术或密码技术保证数据在传输过程中的完整性和保密性;
b） 支持对采集设备关键数据(包括但不限于 Boot 文件、配置文件、密钥文件等)进行备份与恢复处理;
c） 支持对敏感数据如密钥文件等进行完整性校验;
d） 支持数据彻底删除。

6.3.5 个人信息安全

应符合国家个人信息保护相关法律法规规定和 GB 22239 关于个人信息保护的相应要求。

6.3.6 运维管理安全

6.3.6.1 账号口令安全

应符合如下要求:
a） 用户首次登录时,强制用户修改出厂默认口令;
b） 所有口令支持用户自主修改,不使用硬编码口令;
c） 口令具有复杂度要求,密码长度应不低于 8 位,包含数字、大小写字母、特殊字符中的两种或两种以上组合。

6.3.6.2 密码管理

应优先采用国家商用密码算法,禁止在密钥协商、数字签名、数据加密等高敏感场景中使用不安全密码算法,如 SHA-1、MD5、DES、RC4 等。

7 试验方法

7.1 测试条件

按照 GA/T 1128—2013 中第 5 章规定的测试条件进行测试。

7.2 固定场所摄像机试验方法

7.2.1 一般要求检验

按照 GA/T 1127—2013 中 6.2.1 规定的试验方法进行。

7.2.2 功能要求检验

7.2.2.1 基本功能检验

按照 GA/T 1127—2013 中 6.3.1 和 6.3.2 规定的试验方法进行。

7.2.2.2 抓拍功能检验

按照厂家提供的产品说明手册,通过测试平台或采集设备客户端对采集设备进行定时、手动、事件触发的抓拍图片操作,检查是否符合 6.1.2.2 的要求。

7.2.2.3 防抖功能检验

将采集设备安装在防抖试验台上,根据厂家声明的防抖角度和频率配置防抖试验台参数,将采集设

备对准分辨力测试卡进行拍摄。分别开启/关闭防抖功能,查看采集设备在开启防抖功能后拍摄的测试卡的分辨力和清晰度读数是否提高。

7.2.2.4 智能分析功能检验

智能分析功能的测试方法和样本集按照相关测试规范执行。

7.2.3 性能要求检验

按照 GA/T 1127—2013 中 6.4.1.6 规定的试验方法进行几何失真性能检验,按照 GA/T 1128—2013 中第 6 章规定的试验方法进行其他性能指标检验。

7.3 车载摄像机技术要求试验方法

按照 YZ/T 0188—2022 中第 11 章规定的试验方法进行。

7.4 安全要求试验方法

7.4.1 网络安全检验

7.4.1.1 通信安全检验

通过软件工具(如 Xcap)等向采集设备高频次发送 ICMP、SYN 数据包,模拟泛洪攻击,发送源、目的 IP 相同的畸形报文攻击,检查采集设备播放画面的状态。通过软件工具向采集设备高频次发送需求 ARP 响应包,欺骗摄像机建立错误的 IP、MAC 映射,查看采集设备中是否存有虚假 ARP 响应包中的 IP、MAC 映射信息。

通过查阅厂家提供的产品说明手册、访谈技术人员、抓包分析等方法,查证采集设备是否支持类似 802.1x 的链路层认证机制。

7.4.1.2 安全防护检验

通过采集设备 Web 客户端,使用 Root 登录采集设备操作系统,修改系统配置文件,重新启动采集设备,检查采集设备是否能正常启动,并且具有相关安全启动日志记录。

通过采集设备 Web 客户端,使用 Root 登录采集设备操作系统,修改系统敏感文件或提升进程权限,或创建用户名非 Root 账号。重新启动采集设备,检查摄像机是否能够对相应情况产生告警信息。

通过测试平台(安装测试软件、采集设备客户端的 PC 机或服务器)向采集设备中传入典型僵尸网络代码、典型挖矿程序、典型恶意 Rootkit 等恶意代码模拟网络攻击,检查采集设备是否产生告警信息。

7.4.2 Web 安全检验

7.4.2.1 身份鉴别检验

通过默认的管理员身份登录摄像机管理界面,访问摄像机账号列表,并进行创建、删除、口令修改等账号管理操作,检查是否成功。

使用相应的账号和口令登录摄像机,检测摄像机的账号和口令的校验功能:是否允许正确的账号和口令登录摄像机;是否拒绝错误的账号和口令以及不存在的账号登录摄像机;是否具备非法登录次数的限制、提醒和验证码机制。

通过管理员身份设置某个账户的口令有效期,在有效期内和有效期外分别登录该账户,检测该账户口令的有效期是否生效。

通过查阅厂家提供的符合 GB 35114—2017 中 A 级要求的检测报告,验证是否满足相应的身份认证规则。

7.4.2.2 访问控制检验

测试平台配置为采集设备不接受的 IP 地址或不接受的封禁协议,向采集设备发送数据包,检测采集

设备是否接受该数据包。

通过管理员身份设置采集设备的用户及权限,通过不同的用户账号登录,执行权限内和权限外的操作,检测采集设备的防控控制策略是否生效。

7.4.2.3 Web 攻击防范检验

通过测试平台登录采集设备,进行交互访问并进行抓拍,分析数据包的协议类型是否满足安全协议的要求。

访问一个可以提交来自不可信数据源的数据并对提交的数据格式有限制的界面(如添加用户),并启用代理工具(如 BurpSuite、FIDDLER),通过代理工具拦截并修改提交的数据为不符合要求的数据或非当前采集设备的地址,检查数据是否提交成功。

通过采集设备 Web 客户端与采集设备通信,检查 SessionID 的生成机制、长度,判断遭暴力破解的可能性。

通过采集设备 Web 客户端登录采集设备,打开页面后长时间不操作,检查采集设备的会话超时机制是否生效。通过不同测试平台的客户端用相同账号登录采集设备,检查先登录的测试平台客户端是否退出。

7.4.3 日志记录和审计检验

使用不同账号登录采集设备,执行各种操作,模拟采集设备的软件安装、升级、卸载等,通过管理员账号登录采集设备,打开采集设备日志信息,检查日志记录信息是否正确。

按照厂家提供的产品说明手册中对日志权限控制和保护措施的说明,对日志文件进行删除、修改、覆盖等操作,验证日志保护措施是否生效。

配置测试平台作为日志服务器与采集设备相连,检查日志文件是否上传至测试平台。

7.4.4 数据安全检验

对采集设备的传输数据进行抓包分析,检查是否支持数据完整性校验和加密保护。访问采集设备关键数据备份目录,检查是否对关键数据进行备份。

使用管理员账号对采集设备存储的数据进行格式化操作,检查格式化是否成功。

7.4.5 运维管理安全检验

7.4.5.1 账号口令安全检验

使用新建账号登录采集设备,检查是否有强制修改口令的提示,并检查是否具备口令复杂度要求及提示。

7.4.5.2 密码管理检验

检查采集设备中各场景使用的密码算法是否为国家商用密码算法,不得存在使用不安全密码算法、自创或未公开密码算法的情况。