ICS：13.320

A 90

DB31

上　海　市　地　方　标　准

DB 31/ T 1086—2018

入侵报警系统应用基本技术要求

Basic requirements of applications for Intrusion alarm system

2018－05－21 发布　　2018－08－01 实施

上海市质量技术监督局　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规格起草。

本标准由上海市公安局技术防范办公室提出并组织实施。

本标准由上海市社会公共安全技术防范标准化技术委员会归口。

本标准起草单位：上海市公安局技术防范办公室、上海傲兰杰信息科技有限公司、上海德梁安全技术咨询服务有限公司、国家安全防范报警系统产品质量监督检验中心、上海界安信息科技有限公司、上海能泰智能科技有限公司、上海润德科技发展有限公司、上海宝学电子信息技术有限公司、上海复栋智能科技有限公司、上海炎荣电子科技有限公司、博世（上海）保安系统有限公司、上海明力电子科技有限公司、上海灏广电子科技有限公司。

本标准起草人：陶焱升、孙亮、顾忠平、王喆、沈晔、雷智雄、陈军、刘晓新、施天明、王雷、梁晶、汪华、郭善勇、缪璇、杨军、黄郁人、吴家辉、瞿帅。

入侵报警系统应用基本技术要求

1 范围

本标准规定了入侵报警系统应用的基本要求，技术要求，评审、验收、维护。

本标准适用于入侵报警系统的设计、评审、施工、检验、验收和维护过程的应用。其他具有入侵报警功能的安防子系统适用于本标准。

在建和已投入使用的入侵报警系统应按照本标准进行改（扩）建。

2 规范性引用文件

下列文件中对于本标准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标准。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本标准。

GB 4208-2008 外壳防护等级（IP 代码）

GB/T 7946 脉冲电子围栏及其安装和安全运行

GB 10408.1 入侵探测器 第 1 部分：通用要求

GB 10408.2 超声入侵探测器

GB 10408.3 入侵探测器 第 3 部分：室内用微波多普勒探测器

GB 10408.4 入侵探测器 第 4 部分：主动红外入侵探测器

GB 10408.5 入侵探测器 第 5 部分：室内用被动红外入侵探测器

GB 10408.6 微波和被动红外复合入侵探测器

GB/T 10408.8 振动入侵探测器

GB 12663 防盗报警控制器通用技术条件

GB 15209 磁开关入侵探测器

GB/T 15211-2013 安全防范报警设备 环境适应性要求和试验方法

GB 15407 遮挡入侵探测器

GB/T 15408 安全防范系统供电技术要求

GB/T 16796 安全防范报警设备 安全要求和试验方法

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB 25287 高压电网式装置

GB/T 30147 安防监控视频实时智能分析设备技术要求

GB/T 30148 安全防范报警系统 电磁兼容抗扰度要求和试验方法

GB/T 31132　入侵报警系统 无线（射频）设备互联技术要求

GB/T 32581　入侵和紧急报警系统技术要求

GB 50311　综合布线系统工程设计规范

GB 50312　综合布线工程验收规范

GB 50348　安全防范工程技术规范

GB 50394-2007　入侵报警系统工程设计规范

GA/T 75　安全防范工程程序与要求

GA 308　安全技术防范系统验收规则

GA/T 368　入侵报警系统技术要求

GA/T 394　出入口控制系统技术要求

GA/T 1031　泄漏电缆探测器

GA/T 1032　张力式电子围栏通用技术要求

GA/T 1158　激光对射入侵探测器技术要求

GA/T 1217　光纤振动入侵探测器技术要求

YD/T 1099　以太网交换机技术要求

YD/T 1141　以太网交换机测试方法

3　术语和定义

GB 50348、GB 50394-2007 中界定的，以及下列术语与定义适用于本标准。

3.1

入侵报警系统 intrusion alarm system

利用传感器技术和电子信息技术探测并指示非法进入或试图非法进入设防区域的行为、处理报警信息、发出报警信息的电子系统或网络。

3.2

入侵报警系统应用 applications of intrusion alarm system

对利用一种或多种传感器技术和电子信息技术，探测并指示非法进入或试图非法进入设防区域的行为、处理报警信息、发出报警信息的电子系统或网络的应用。

3.3

设备间 electronic equipment room

建筑内集中放置技术防范设备主机、网络设备及其他电子设备的物理区域。

3.4

远程联网报警中心（remote）alarm processing center

以维护安全为目的，基于本地入侵报警系统，利用通讯及网络技术构建的具有报警信息采集/传输/控制/显示/存储/管理等功能，可对管辖范围内需要防范的目标实施报警接收和安全管理的处所。

4 基本要求

4.1 系统设计要求

4.1.1 入侵报警系统的设计应基于现场勘察，根据环境条件、防范对象、投资规模、维护保养以及接处警方式等因素进行设计。系统的设计应符合有关风险等级和防护级别标准的要求，符合有关设计规范、设计任务书及建设方的管理和使用要求。

4.1.2 入侵报警系统的设计、施工程序应符合 GA/T 75 的规定。入侵报警系统的设计原则、设计要素、功能设计、安全性设计、电磁兼容性设计、可靠性设计、环境适应性设计、防雷接地设计、集成设计、设备选型与安装设计、供电设计、监控中心设计，以及传输方式、传输线缆、传输设备的选择与布线设计等，应符合 GB 50311、GB 50312、GB 50348、GB 50394、GB/T 15408、GB/T 32581 的相关规定。

4.1.3 入侵报警系统中使用的设备和产品应符合国家法律法规、现行标准和安全防范管理的要求，并经检验或认证合格。

4.1.4 入侵报警系统的设计应具备与上一级管理系统联网功能，终端接口及通信协议应符合国家现行有关标准规定。系统应与本市技防工程监督管理系统／平台联网，系统直接与“本市技防工程监督管理平台”联网的，还应安装专用上传加密模块。

4.1.5 入侵报警系统的设计宜同本市监控报警联网系统的建设相协调、配套，作为社会监控报警接入资源时，其接口、性能应符合相关标准要求。

4.1.6 入侵报警系统工程的建设，除执行本标准外，还应符合国家工程建设标准及有关技术标准、规范和规定。

4.2 应用设计原则

4.2.1 入侵报警系统应用设计在技术上应有适度超前性和互换性，为系统的整体和／或局部升级、扩容留有余地。

4.2.2 入侵报警系统应用设计应能准确及时地探测入侵行为、发出报警信号；对入侵报警信号、防拆报警信号、各类故障信号的来源应有清楚和明显的指示。系统误报警率应控制在可接受的限度内，不允许有漏报警。

4.2.3 入侵报警系统应用设计应充分考虑与视频安防监控系统、出入口控制系统等安防子系统的联动。当与其他安防子系统联合设计时，应进行系统集成设计，各系统之间应相互兼容又能独立工作。

4.3 系统基本组成

4.3.1 入侵报警系统通常由前端探测设备、前端传输设备、区域控制设备、区域传输设备及中心控制设备等组成，如图 1 所示。

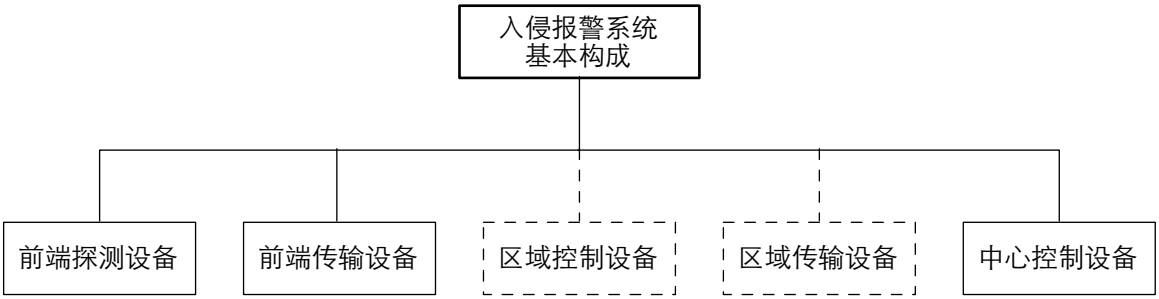


图 1 入侵报警系统基本组成

4.3.2 前端探测设备可包括一种或多种紧急报警装置、被动探测设备、主动探测设备、电子围栏探测系统、感应线缆探测系统、视频入侵探测系统等，前端探测设备可自带地址编码及专用传输等接口。

4.3.3 前端传输设备及区域传输设备包括传输线缆及系统传输设备，其中系统传输设备可包括地址编码设备、网络交换设备、有线 / 无线传输辅助设备、联动输入 / 输出设备等。

4.3.4 区域控制设备应为信息接收及处理、内置信息存储的报警集成控制设备，可集成包括报警显示、信息存储、操作控制及状态监测等功能模块，区域控制设备可自带报警输出、地址编码、有线和 / 或无线 IP 网络等接口。区域控制设备包括区域报警集成控制设备、区域报警控制扩展设备等，也可将区域报警集成控制、区域报警控制扩展等功能集成。区域报警集成控制设备内置事件记录信息存储容量应不小于 256 条。

4.3.5 中心控制设备的控制主机应为信息接收及处理、内置信息存储的报警集成控制设备，应集成包括报警显示、信息存储、操作控制、报警输出等控制接口，公共电话网、有线和 / 或无线、IP 网络等通讯接口，应具有状态监测等功能。中心控制设备包括中心报警集成控制设备、中心报警控制扩展设备、中心报警集中管理设备等，也可将中心报警集成控制、中心报警控制扩展、中心报警集成管理等功能集成。中心报警集成控制设备内置事件记录信息存储容量应不小于 512 条。

4.4 系统应用分级

4.4.1 入侵报警系统根据不同应用方式和报警响应时间，分为一级、二级、三级。

4.4.2 入侵报警系统应用方式分级应符合以下要求：

a） 一级：前端入侵探测设备通过前端传输设备直接与中心控制设备相连的；

b） 二级：前端入侵探测设备通过前端传输设备—区域控制设备—区域传输设备与中心控制设备相连的；

c） 三级：前端入侵探测设备通过前端传输设备—区域控制设备—区域传输设备与中心控制设备相连，再通过专用传输接口与远程报警控制设备相连的。

4.4.3 入侵报警系统各应用分级报警响应时间应符合以下要求：

a） 一级：报警响应时间应不大于 2s；

b） 二级：报警响应时间应不大于 5s；

c） 三级：使用公共电话网的，报警响应时间应不大于 20s；使用 IP 网络方式的，至远程报警控制设备报警响应时间应不大于 6s。

4.5 系统应用类型

4.5.1 入侵报警系统的应用根据信号传输方式的不同可分为分线制、总线制和网络型三种类型。各种类型可单独使用，也可组合使用。

4.5.2 入侵报警系统的应用分类应符合以下要求：

a） 分线制：前端探测设备与中心控制设备之间，采用传输线缆直接相连所构成入侵报警系统的应用类型，如图 2 所示。

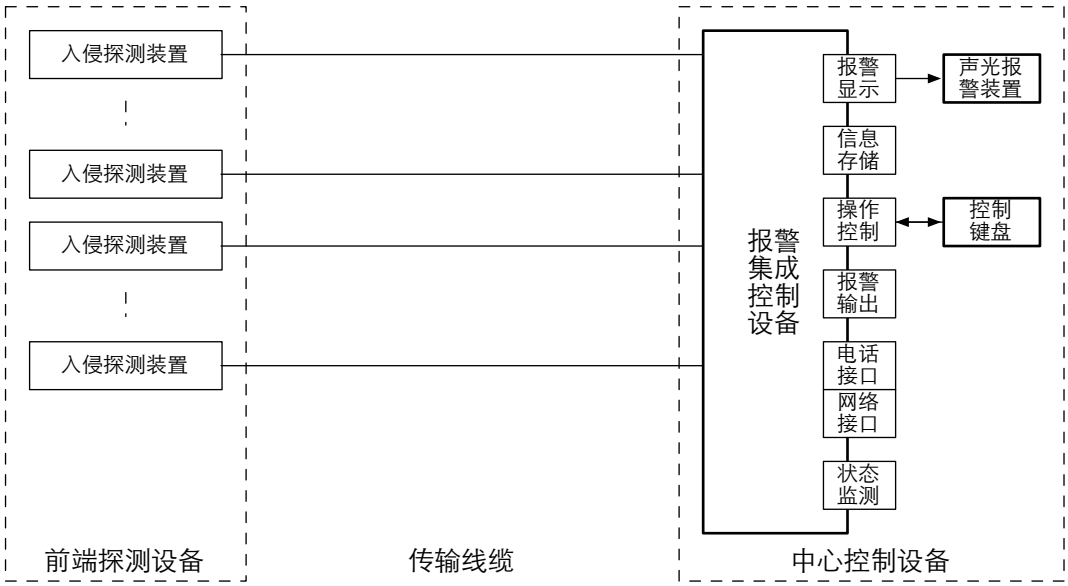


图 2 应用类型为分线制的入侵报警系统

b） 总线制：前端探测设备、前端传输设备或区域控制设备与中心控制设备之间，采用传输线缆并以地址编码方式总线相连所构成入侵报警系统的应用类型，如图 3 所示。

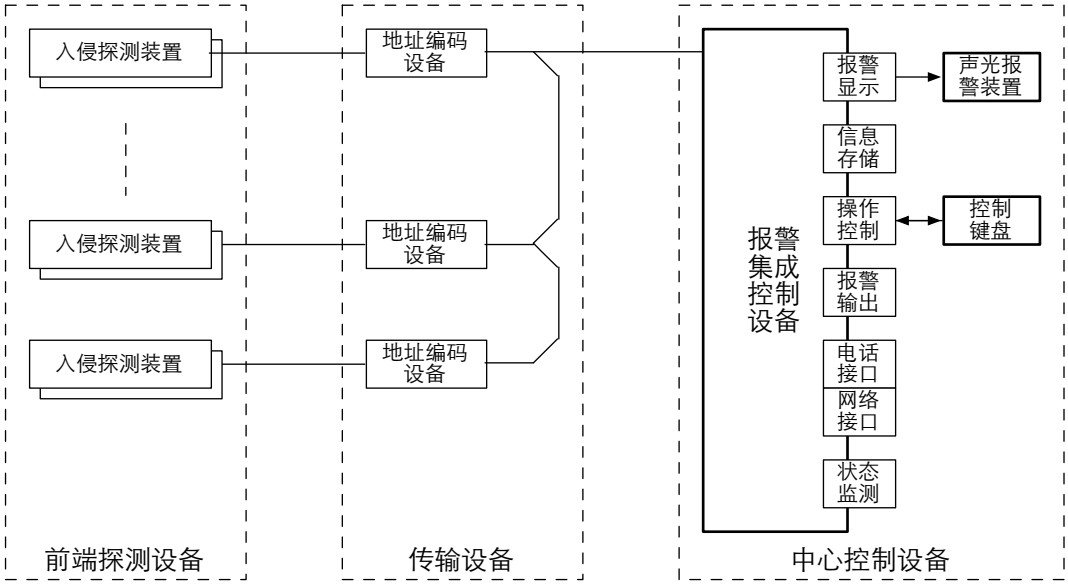
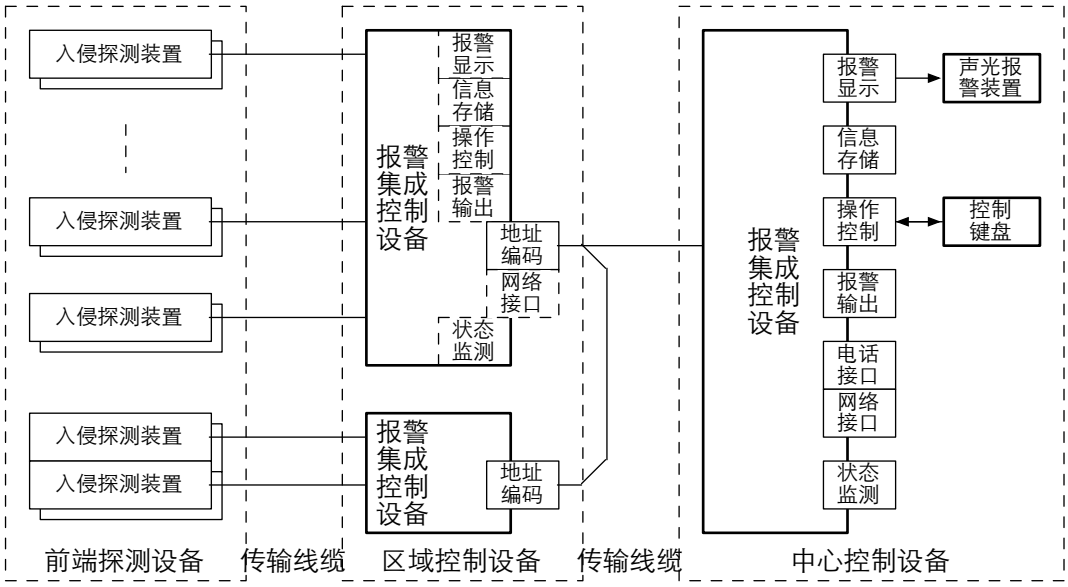


图 3 应用类型为总线制的入侵报警系统



续图 3 应用类型为总线制的入侵报警系统

c） 网络型：前端探测设备、前端传输设备或区域控制设备与中心控制设备之间，采用传输线缆并以网络交换方式网线相连所构成入侵报警系统的应用类型，如图 4 所示。

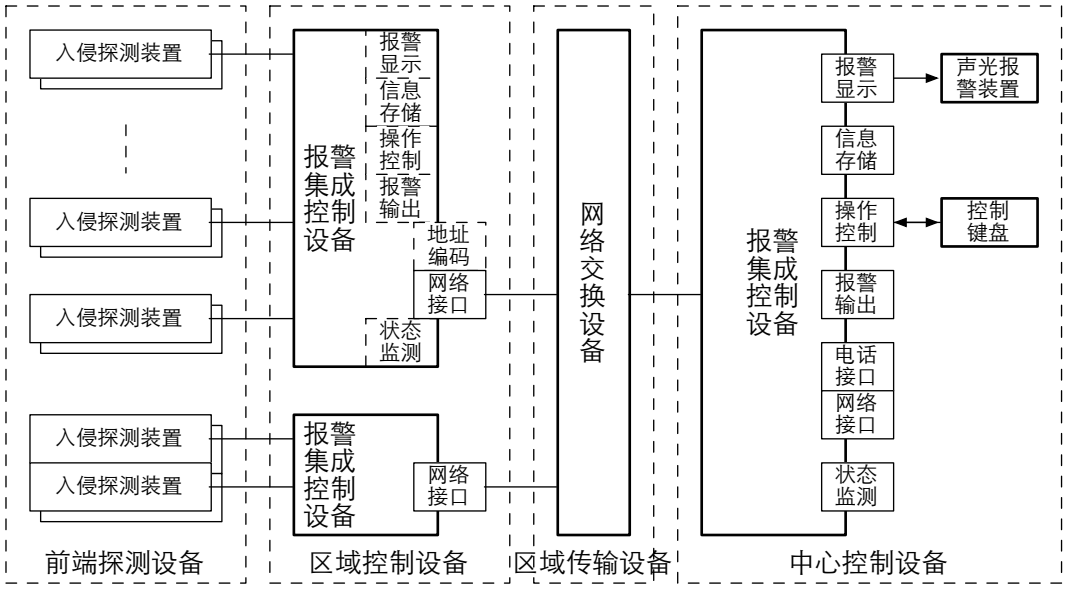


图 4 应用类型为网络型的入侵报警系统

5 技术要求

5.1 前端探测设备

5.1.1 前端探测设备的选用和安装应能构成点、线、面、空间或其组合的综合防护系统，确保对非法入侵行为及时发出报警响应，探测范围应有效覆盖防护区域，但同时应避免或减少因防护区域以外正常活动而引起误报的情发生。

5.1.2 应分别或综合设置周界、区域和目标防护系统，对被保护对象采取不同的防护措施。各防区的灵敏度、探测距离、覆盖区域应按国家、地方及产品相关技术要求设置并应符合以下要求：

a） 室外防护的应用：有实体围墙无需具有阻挡作用的周界防护宜配置室外被动探测设备、室外主动探测设备、感应线缆（包括振动电缆、振动光纤、泄漏电缆等）探测系统；室外有实体围墙需要具有阻挡作用的周界防护可配置电子围栏探测系统，加装辅助设施后可配置感应线缆（包括振动电缆、振动光纤、泄漏电缆等）探测系统；实体围墙需要具有防凿功能的周界防护宜在加装辅助设施后配置感应线缆（包括振动电缆、振动光纤、泄漏电缆等）探测系统；室外无实体围墙无需具有阻挡作用的周界防护可配置室外被动探测设备、室外主动探测设备、感应线缆（包括振动电缆、振动光纤、泄漏电缆等）探测系统;室外无实体围墙需要具有阻挡作用的周界防护可配置电子围栏探测系统,也可配置感应线缆(包括振动光纤、泄漏电缆等）探测系统；室内周界防护宜配置被动探测设备、主动探测设备。

b） 室外出入口防护的应用：宜配置室外被动探测设备、室外主动探测设备、感应线缆（包括振动光纤、泄漏电缆等）探测系统；室内出入口宜配置被动探测设备、主动探测设备。

c） 室内外区域防护及目标防护的应用：宜配置被动探测设备、主动探测设备、感应线缆（包括振动电缆、振动光纤、泄漏电缆等）探测系统；重要目标应配置两种或以上不同探测原理的探测设备进行防护。

d） 无实体围墙和／或无阻挡作用周界防护的应用：应采用与视频安防监控系统联动的方式，对防范区域的入侵报警进行复核；防护区域地理、环境等情况较为复杂以及防护区域范围较大的，宜采用与视频安防监控系统或出入口控制系统联动的方式，对防范区域的入侵报警进行复核。

e） 智能探测防护的应用：宜采用具有智能分析功能的探测系统作为入侵探测应用，并应采用与视频安防监控系统或出入口控制系统联动的方式，对防范区域的入侵报警进行复核。

5.1.3 应符合整体纵深防护和局部纵深防护的要求，根据被保护区域、目标所处的风险等级和防护级别，对整个防范区域实施分区域、分层次的设防，防区划分应有利于报警时准确定位，并应符合以下要求：

a） 紧急报警装置每路防区的数量应不大于 4 个，同一空间相邻安装的紧急报警装置不应作为同一防区，不同空间的紧急报警装置不应作为同一防区。

b） 同一空间区域防护的被动探测设备每路防区的串联数量应不大于 3 个，不同空间区域防护、目标防护的被动探测设备防区应独立。区域防护、目标防护的覆盖范围内应无盲区，覆盖范围边缘与防护对象间的距离应不少于 5m。

c） 周界防护每路独立防区的长度或距离（无障碍物遮挡时）应不大于 70m。

5.1.4 紧急报警装置应安装在隐蔽、便于操作的部位，应设置为 24h 不可撤防模式，并具有防误触发措施。触发报警后应能立即发出紧急报警信号并自锁，复位应采用人工操作方式。

5.1.5 常用被动探测设备的要求除符合产品技术说明书的规定外，还应符合以下要求：

a） 壁挂式被动探测设备的安装高度距地面宜不大于 2.2m，入侵探测设备与墙壁的倾角视防护区域覆盖要求确定。幕帘防护被动探测设备透镜的法线方向应与入侵目标方向垂直；通道防护被动探测设备透镜的法线方向应正对通道；被动红外探测设备透镜的法线方向与可能入侵目标方向之间的夹角宜为 $90^0 \pm 5^0$；微波和被动红外复合式入侵探测设备透镜的法线方向与可能入侵目标方向之间的夹角宜为 $45^0 \pm 5^0$；

b） 吸顶式被动探测设备应水平安装在需要防护部位的上方，被动红外探测设备的安装高度宜不大于 3.6m，微波和被动红外复合式入侵探测设备的安装高度宜不大于 4.5m，入侵探测设备与地面的倾角视防护区域覆盖要求确定；

c） 被动红外入侵探测设备及微波和被动红外复合式入侵探测设备的视窗应避开正对强光源，附近及视场内不应有温度快速变化的热源，防护区域内不应有障碍物；

d） 被动振动探测设备应牢固安装在被探测部位的表面，在探测范围内受到大于 100N 外力敲击时应能感应并输出报警信号，并应设置为 24h 不可撤防模式；被动玻破探测装置应尽量靠近所要保护玻璃

附近的墙壁或天花板上，在探测范围内对玻璃破碎等高频声响应敏感并输出报警信号，并应设置为 24h 不可撤防模式；

e） 磁开关入侵探测设备应安装在门、窗开合处，舌簧管应安装在门、窗固定框上，磁铁应安装在门、窗活动部位上，两者间应对准，间距应保证能可靠工作；

5.1.6 主动探测设备、电子围栏探测系统、感应线缆（包括振动电缆、振动光纤、泄漏电缆等）探测系统的要求除符合产品技术说明书的规定外，还应符合以下要求：

a） 张力式电子围栏前端的测控杆、承力杆、轴承杆应具攀爬报警功能，并能根据外界环境、气候等变化自动调整警戒张力值；脉冲式电子围栏前端任意一根金属导体应具有旁路（等电位跨接）报警及触网报警功能。

b） 前端探测设备及系统的防区不应有盲区和死角，周界防护的应设置为 24h 不可撤防模式。

c） 前端探测设备及系统与附近的绿化带应保持合适距离，及时对可能触碰、缠绕、遮挡前端探测设备及系统的枝条进行修剪。

5.1.7 前端探测设备应具有防拆、防破坏报警功能，并应启用。

5.1.8 采用电流环探测原理的独立型探测设备（如紧急报警按钮、被动探测设备、主动探测设备等），环路电阻应安装在前端探测设备内；采用电流环探测原理的复合型探测设备及探测系统（如主动探测设备、电子围栏探测系统、感应线缆探测系统等），环路电阻应根据产品的探测原理，安装在前端探测设备、前端传输设备或区域控制设备内。采用非电流环探测原理的前端探测设备信息传输应采用加密措施。

5.1.9 前端探测设备其他技术要求还应符合 GB 10408.1、GB 10408.2、GB 10408.3、GB 10408.4、GB 10408.5、GB 10408.6、GB 15209、GB 15407、GB 25287、GB/T 7946、GB/T 10408.8、GB/T 30147、GB/T 31132、GA/T 394、GA/T 1031、GA/T 1032、GA/T 1158、GA/T 1217 的要求。

5.2 系统传输设备

5.2.1 应根据前端探测设备、区域控制设备及中心控制设备的应用类型选择前端传输设备及区域传输设备。

5.2.2 传输线缆的敷设应符合 GB 50394-2007 第 7 章的相关规定。在运行过程中，系统对传输线缆的任何异变（含开路、短路、串接、并接等）应能发出报警信号。

5.2.3 系统传输设备的要求除符合产品技术说明书的规定外，还应符合以下要求：

a） 无线传输设备的载波频率和发射功率应符合国家相关管理规定，无线发射机使用的电池应保证有效使用时间不少于 180d，发出欠压报警信号后，电源应能支持发射机正常工作时间不少于 7d，接收机的安装位置应由现场试验确定，应能保证接收到防范区域内任意发射机发出的报警信号；

b） 网络型应用类型的系统，网络交换设备应达到线速标准、无阻塞，并具有网络管理功能，接入端口设计应不超过网络交换设备端口的80%，网络交换层不应超过三个层级，应对所有接入网络交换设备端口予以管理和绑定，且不应采用桌面型网络交换设备。

5.2.4 系统传输设备应放置在隐蔽、通风、安全又便于检修的位置，应有物理实体防护安全措施。

5.2.5 室内使用的系统传输设备应符合 GB/T 15211-2013 中 II，外壳防护等级应达到 GB 4208-2008 中 IP50 的要求；室外系统传输设备应符合 GB/T 15211-2013 中 III，外壳防护等级应达到 GB 4208-2008 中 IP65 的要求。

5.2.6 系统传输设备应具有防拆、防破坏报警功能，并应启用。

5.2.7 非电流环探测原理的前端传输设备 / 区域传输设备信息传输应采用安全加密措施。

5.2.8 系统传输设备其他技术要求还应符合 GB 50311、GB 50312、GB/T 16796、GB/T 22239、GB/T 30148、GB/T 31132、YD/T 1099、YD/T 1141 的要求。

5.3 报警控制设备

5.3.1 应根据系统规模、系统功能、信号传输方式及安全管理要求等选择区域控制设备及中心控制设备的类型。

5.3.2 报警集成控制设备应为嵌入式操作系统或软硬件固化的专用控制设备，应无需外置设备能与前端探测设备、前端传输设备、区域传输设备组成独立运行的入侵报警系统，实现报警接收及处理、内置信息存储等基本功能。应具有防拆、防破坏报警功能，并应启用。

5.3.3 区域控制设备应至少包括区域报警集成控制设备，中心控制设备应至少包括中心报警集成控制设备、中心报警控制扩展设备、中心报警集中管理设备等，或至少包括中心报警集成控制、中心报警控制扩展、中心报警集中管理等功能的集成设备。

5.3.4 中心控制设备应配置能与其他安防子系统联动或集成的输入、输出接口。

5.3.5 无操作控制功能的区域控制设备应放置在弱电箱、设备间等隐蔽、通风、安全又便于检修的位置，应有物理实体防护安全措施；有操作控制功能的区域控制设备应放置在受控对象的附近，并在受控区域内便于操作的位置。区域控制设备应具有防拆、防破坏报警功能，并应启用。

5.3.6 中心控制设备应能接收前端探测设备发出的报警及故障信号，并应具有布防和撤防、不可撤防模式、外出与进入延迟的设置和编程，以及自检、防破坏、声光报警、报警记录与储存、打印输出、密码操作保护等功能，能准确地识别报警区域，实时显示发生报警的区域、日期、时间及报警类型等信息。

5.3.7 系统布防、撤防、报警、故障等信息的存储应不少于 30d。

5.3.8 系统应有备用电源,应能保证在市电断电后系统供电时间不少于 8h。

5.3.9 报警集成控制设备其他技术要求应符合 GB 12663 的要求。

5.3.10 系统其他技术要求还应符合 GB 50394-2007、GB/T 32581、GA/T 368 的要求。

5.4 状态监测要求

5.4.1 应能自动监测入侵报警系统探测、传输、控制等设备及系统的运行状态。

5.4.2 自动状态监测应至少包括入侵报警系统运行进程的心跳测试、操作日志、故障报警、故障恢复等定时上传的状态监测应用内容，如图 5 所示。

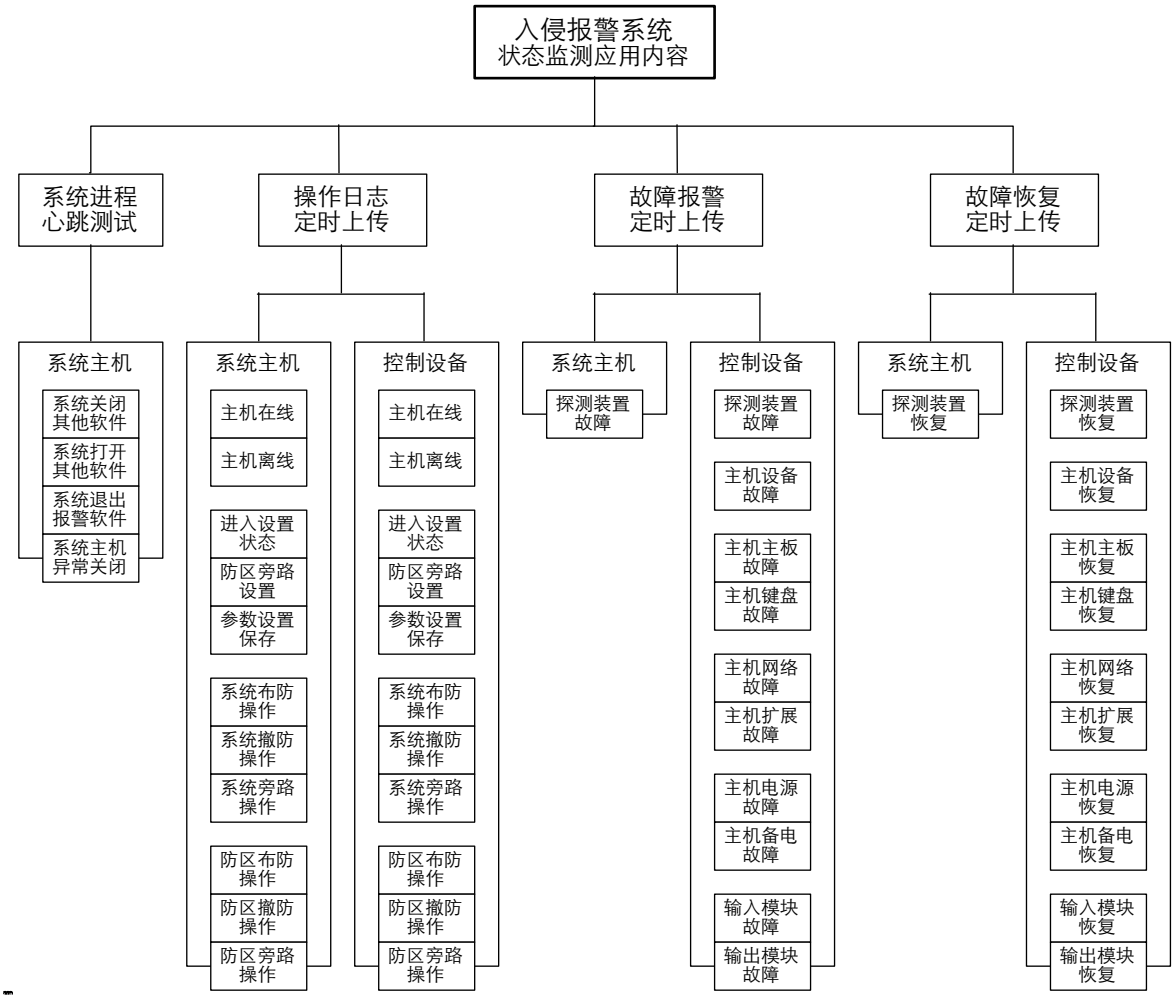


图 5 入侵报警系统状态监测应用内容

5.4.3 应能根据状态监测情况对入侵报警系统资源、系统设备、软件运行、参数设置等运行信息，心跳超时、操作异常、系统故障、设备故障等故障信息进行自动分类。

5.4.4 应能直接与“本市技防工程监督管理平台”联网，并通过技防监督管理系统查询所接入技防项目基本信息、设备运行信息、设备故障信息、维护保养信息等，生成相应的报表，反映接入技防设施实际运行和维护情况等信息。

5.5 远程联网报警中心

5.5.1 应能接收本地所有接入入侵报警系统各类紧急报警、入侵报警等警情报告和设备状态、通讯状态等状态报告。

5.5.2 所有接收、处置、操作、监测、运行等信息均应自动保存，不可更改，信息保存时间应不小于180d。

5.5.3 应具有双路由、双报告的联网接入功能，并能同时接收通过公共电话网和有线或无线、IP 网络传送的报警信号。报警响应时间应符合 4.4.3 的规定。

5.5.4 应具有自动监测系统运行和传输线路工作状况的功能。

5.6 远程联网传输要求

5.6.1 与远程联网报警中心的传输网络应物理独立。传输网络应能自动检测线路在线、断线、故障以及在线设备数量变更等状态，并应具有自动监测报警和故障提示等功能。

5.6.2 远程联网的传输网络带宽应满足联网报警接收及处理、报警显示、信息存储、操作控制、报警输出、状态监测等上传应用，并留有足够的冗余。采用有线方式连接时，网络带宽应不少于 2M；采用无线方式连接时，应采用电信运营商提供的专用无线网络。

5.6.3 远程联网报警中心总传输节点实用带宽应不大于进网总传输带宽的 75%，所有本地传输节点实用带宽应不大于传输带宽的 45%。

6 评审、检验、验收、维护

6.1 入侵报警系统应按 GA/T 75、GA 308 的规定进行技术方案评审并合格。经修改完善设计、安装调试、试运行、初验合格后，应根据 GB 50348 有关要求进行系统检测。检测合格后，应根据 GB 50348 有关要求进行系统验收。

6.2 入侵报警系统的维护、检测、保养应由取得相应资质的单位承担，并应建立有效的运行保障体系和安全评估机制。入侵报警系统应每年定期进行检测、维护、保养，及时排除故障，淘汰、更换过期和损坏的设备器材，保持各系统处于良好的运行状态。

6.3 入侵报警系统设施出现故障时，应按安全保卫工作管理规定的时间要求及时修理或调整，并恢复正常使用功能。在修理或调整期间应采用有效的应急保卫方案，确保安全。