



中华人民共和国公共安全行业标准

GA/T 368—2001

入侵报警系统技术要求

Specifications for intrusion alarm systems

(IEC 60839-1-1 Alarm systems Part 1, 1988,
General requirements—Section One—General, NEQ)

2001-12-14 发布

2002-06-01 实施

中华人民共和国公安部 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	2
4 技术要求	5
5 安全性要求	7
6 电磁兼容性要求	7
7 防雷接地要求	7
8 环境适应性要求	8
9 可靠性要求	8
10 标志	8
11 文件提供	8

前 言

本标准非等效采用 IEC 60839-1-1《报警系统 一般要求 总则》(1988)。

本标准与 IEC 60839-1-1(1988)的主要不同在于：

- 1) 根据我国安全技术防范行业的实际,对术语和定义进行了适当的增删。
- 2) 根据信息技术的发展和报警专业标准化的最新成果,在规范性引用文件中,除增加了 91 年出版的 IEC 60839-5 系列标准外,还增加了 2001 年出版的 IEC 60839-7 系列标准,这两个系列标准即将转化为我国标准。同时还引用了我国安防专业近年来制定的有关国家标准和行业标准。
- 3) 在原标准的基础上,更加强调系统的安全性、电磁兼容性和可靠性,增加了相关的技术要求。

本标准由公安部科技局提出。

本标准由全国安全防范报警系统标准化技术委员会(SACS/TC100)归口。

本标准由中国兵器工业集团第二一二研究所西安北方信息产业有限公司、陕西省公安厅科技处技防办、SACS/TC100 秘书处负责起草。

本标准主要起草人:李天奎、万军、金巍、周明锦、刁群、康凤琴。

入侵报警系统技术要求

1 范围

本标准规定了用于保护人、财产和环境的入侵报警系统(手动式和被动式)的通用技术要求,是设计、安装、验收入侵报警系统的基本依据。

本标准适用于建筑物内、外部的入侵报警系统。本标准不涉及远程中心,也不包括入侵报警系统与远程中心之间通信数据的加载和卸载。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

- GB 10408.1 入侵探测器 第1部分:通用要求(idt IEC 60839-2-2)
- GB 10408.2 入侵探测器 第2部分:室内用超声波多普勒探测器(idt IEC 60839-2-4)
- GB 10408.3 入侵探测器 第3部分:室内用微波多普勒探测器(idt IEC 60839-2-5)
- GB 10408.4 入侵探测器 第4部分:主动红外入侵探测器(mod IEC 60839-2-3)
- GB 10408.5 入侵探测器 第5部分:室内用被动红外探测器(idt IEC 60839-2-6)
- GB 10408.6 微波和被动红外复合入侵探测器
- GB 12663 防盗报警控制器通用技术条件
- GB 15207 视频入侵报警器
- GB 15209 磁开关入侵探测器
- GB/T 15211 报警系统环境试验
- GB 15407 遮挡式微波入侵探测器技术要求和试验方法
- GB/T 15408 报警系统电源装置、测试方法和性能规范(idt IEC 60839-1-2)
- GB/T 16572 防盗报警中心控制台
- GB 16796 安全防范报警设备 安全要求和试验方法
- GB/T 17626.2—1998 电磁兼容 试验与测量技术 静电放电抗扰度试验
- GB/T 17626.3—1998 电磁兼容 试验与测量技术 射频电磁场辐射抗扰度试验
- GB/T 17626.4—1998 电磁兼容 试验与测量技术 电快速瞬变脉冲群抗扰度试验
- GB/T 17626.5—1999 电磁兼容 试验与测量技术 浪涌抗扰度试验
- GB/T 17626.11—1999 电磁兼容 试验与测量技术 电压暂降、短时中断及电压变化抗扰度试验
- GA/T 74 安全防范系统通用图形符号
- GA/T 75 安全防范工程程序与要求
- IEC 60839-5 报警系统 第5部分:报警信号传输系统技术要求¹⁾
- IEC 60839-7 报警系统 第7部分:报警传输系统中串行数据接口信息格式和协议¹⁾

1) 该系列标准即将转化为我国标准(等同采用)。

3 术语和定义

下列术语和定义适用于本标准。

3.1

报警 alarm

生命、财产或环境面临严重威胁时的警告。

[IEC 60839-1-1]

3.2

入侵报警系统 intrusion alarm system

用于探测设防区域的非法入侵行为并发出报警信号的系统或网络。

3.3

正常状态 normal condition

报警系统处于完全可使用而不在任何其他限定情况下的状态。

[IEC 60839-1-1]

3.4

报警状态 alarm condition

报警系统或其部分因对面临的危险作出响应而产生的状态。

[IEC 60839-1-1]

3.5

故障状态 fault condition

使报警系统无法按照相关标准的技术要求进行工作的系统状态。

[IEC 60839-1-1]

3.6

试验状态 test condition

系统的正常功能被作试验用的报警系统状态。

[IEC 60839-1-1]

3.7

断线状态 disconnection condition

故意造成的报警系统状态,使得系统的一部分不能工作。

[IEC 60839-1-1]

3.8

报警信号 alarm signal

由处于报警状态中的报警系统发出的信号。

[IEC 60839-1-1]

3.9

故障信号 fault signal

由处于故障状态中的入侵报警系统发出的信号。

[IEC 60839-1-1]

3.10

防拆装置 tamper device

用来探测故意干扰(拆卸或打开)报警系统的部件或一部分的装置。

[IEC 60839-1-1]

3.11

防拆探测 tamper detection

使用防拆装置探测对报警系统或其部分的故意干扰。

[IEC 60839-1-1]

3.12

防拆保护 tamper protection

使用电气或机械方法防止对报警系统或其部分的故意干扰。

[IEC 60839-1-1]

3.13

防拆报警 tamper alarm

由防拆装置的动作而发出的报警。

[IEC 60839-1-1]

3.14

误报警 false alarm

由于意外触动手动装置、自动装置对未设计的报警状态做出响应、部件的错误动作或损坏、操作人员失误等而发出的报警信号。

[IEC 60839-1-1]

3.15

漏报警 leakage alarm

入侵行为已经发生,而系统没有作出报警响应或指示。

3.16

探测器 detector

用来辨别面临危险的不正常情况下而产生报警状态的装置。

[IEC 60839-1-1]

3.17

传感器 sensor

探测器中用来辨别状态变化的部分,这个状态变化能指示面临的危险性。

[IEC 60839-1-1]

3.18

处理器 processor

通过对一个或更多传感器输出的处理以断定是否应该产生报警状态的装置。

3.19

控制器 controller

对探测器的信号进行处理以断定是否应该产生报警状态以及完成某些显示、控制、记录和通信功能的装置。

[IEC 60839-1-1]

3.20

系统响应时间 response time

从探测器(包括人工启动开关、按钮或电键)探测到目标后产生报警状态信息到控制器接收到该信息并发出报警信号所需的时间。

3.21

中央控制设备(中心控制台) central control equipment

接收、处理、显示来自探测器、控制器的各种信息并发出控制指令的装置。

3.22

远程中心 remote centre

远离受保护场所、在此收集有关一个或多个报警系统的状态信息,或用作报告(就接收中心而言)或用作向前传输(就卫星站或收集点而言)。

[IEC 60839-1-1]

3.23

报警接收中心 alarm receiving centre

连续不断有人操纵的远程中心,有关一个或多个报警系统的信息向它做出报告。

[IEC 60839-1-1]

3.24

卫星站 satellite station

平常无人操纵但备有在紧急情况下供人操作的设备,有关若干报警系统状态的信息是在这里收集的,或是直接或是通过更远的卫星站向前传输到报警接收中心。

[IEC 60839-1-1]

3.25

收集点 collector point

无人操纵的远程中心,不具有供人在紧急情况下操作的设备,有若干报警系统状态的信息在这里收集,或是直接或是通过卫星站向前传输到报警接收中心。

[IEC 60839-1-1]

3.26

监控中心 monitoring centre

有人操纵的远程中心,报警信号传输系统的状态在此进行监控。

[IEC 60839-1-1]

3.27

组合系统 combined system

在探测、传输、控制、处理环节上,采用两种(含两种)技术以上的报警系统。

[IEC 60839-1-1]

3.28

报警信号传输系统 alarm transmission system

用来把一个或更多报警系统状态的信息传送到一个或更多接收中心的设备和网络。

[IEC 60839-1-1]

3.29

手动控制装置 manual controls

影响报警控制单元动作的手动操作开关、按钮或电键。

[IEC 60839-1-1]

3.30

实体防护 physical protection

防止部件受损坏的保护或防止人受到伤害的保护。

[IEC 60839-1-1]

3.31

设置警戒(设防状态) set condition

使报警状态能够指示出来的一种状态。

3.32

解除警戒(撤防状态) **unset condition**

使报警状态不能指示出来的一种状态。

4 技术要求

4.1 系统概述

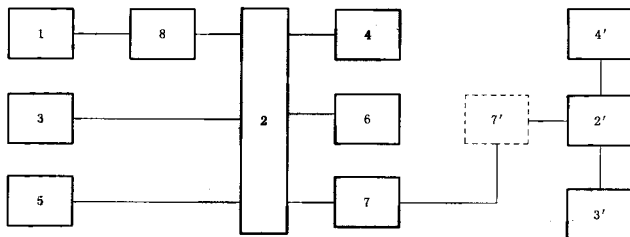
入侵报警系统应包括前端设备、传输设备和控制/显示/处理/记录设备。前端设备包括一个或多个探测器;传输设备包括电缆或数据采集和处理器(或地址编解码器/发射接收装置);控制设备包括控制器或中央控制台,控制器/中央控制台应包含控制主板、电源、声光指示、编程、记录装置以及信号通信接口等。入侵报警系统设备应分别符合 GB 10408 系列标准、IEC 60839-5 系列标准、IEC 60839-7 系列标准、GB 12663、GB 15207、GB 15209、GB 15407、GB/T 16572 等相关标准的技术要求。

入侵报警系统可有多种构成模式。各种不同入侵报警系统的共同部分的基本构成如图 1 所示。

注 1: 声光指示、编程装置、信号通信接口可为分离部件,也可为组合或集成部件。

注 2: 入侵报警系统中探测器与控制器之间、控制器与远程中心的信号传输可以采用有线或/和无线传输方式。

注 3: 入侵报警系统可以包括其他附加装置,但它们均应符合本标准的相关要求。



1—探测器、手动控制装置;

2、2'—控制设备;

3、3'—电源;

4、4'—可视和/或音响指示设备;

5—由控制设备激发的装置;

6—程序输入装置;

7、7'—信号通信接口(调制解调器);

8—传输设备。

图 1 各种入侵报警系统的共同部分

4.2 系统设计

4.2.1 规范性和实用性

入侵报警系统的设计应基于对现场的实际勘察,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。设备选型应符合有关国家标准、行业标准和相关管理规定的要求。

4.2.2 先进性和互换性

入侵报警系统的设计在技术上应有适度超前性和互换性,为系统的增容和/或改装留有余地。

4.2.3 准确性

入侵报警系统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、故障信号的来源应有清楚和明显的指示。

入侵报警系统应能进行声音复核,与电视监控系统联动的入侵报警系统应能同时进行声音复核和图像复核。

系统误报警率应控制在可接受的限度内。入侵报警系统不允许有漏报警。

4.2.4 完整性

应对入侵设防区域的所有路径采取防范措施,对入侵路径上可能存在的实体防护薄弱环节应有加强防范措施。所防护目标的5 m范围内应无盲区。

4.2.5 纵深防护性

入侵报警系统的设计应采用纵深防护体制,应根据被保护对象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。一个完整的防区,应包括周界、监视区、防护区和禁区四种不同类型的防区,对它们应采取不同的防护措施。

防护区内应设立控制中心,必要时还可设立一个或多个分控中心。控制中心宜设在禁区内,至少应设在防护区内。

4.2.6 联动兼容性

入侵报警系统应能与电视监控系统、出入口控制系统等联动。当与其他系统联合设计时,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。入侵报警的优先权仅次于火警。

4.3 系统基本功能

4.3.1 探测

入侵报警系统应对下列可能的入侵行为进行准确、实时的探测并产生报警状态:

- a) 打开门、窗、空调百叶窗等;
- b) 用暴力通过门、窗、天花板、墙及其他建筑结构;
- c) 破碎玻璃;
- d) 在建筑物内部移动;
- e) 接触或接近保险柜或重要物品;
- f) 紧急报警装置的触发。

4.3.2 响应

当一个或多个设防区域产生报警时,入侵报警系统的响应时间应符合下列要求:

- a) 分线制入侵报警系统:不大于2 s;
- b) 无线和总线制入侵报警系统的任一防区首次报警:不大于3 s;
其他防区后续报警:不大于20 s。

4.3.3 指示

入侵报警系统应对下列状态的事件来源和发生的时间给出指示:

- a) 正常状态;
- b) 试验状态;
- c) 入侵行为产生的报警状态;
- d) 防拆报警状态;
- e) 故障状态;
- f) 主电源掉电、备用电源欠压;
- g) 设置警戒(布防)/解除警戒(撤防)状态;
- h) 传输信息失败。

4.3.4 控制

入侵报警系统应对下列功能进行编程设置:

- a) 瞬时防区和延时防区;
- b) 全部或部分探测回路设置警戒(布防)与解除警戒(撤防);
- c) 向远程中心传输信息或取消;
- d) 向辅助装置发激励信号;
- e) 系统试验应在系统的正常运转受到最小中断的情况下进行。

4.3.5 记录和查询

入侵报警系统应对下列事件记录和事后查询：

- a) 4.3.3 所列事件、4.3.4 所列编程设置；
- b) 操作人员的姓名、开关机时间；
- c) 警情的处理；
- d) 维修。

4.3.6 传输

- a) 报警信号的传输可采用有线和/或无线传输方式；
- b) 报警传输系统应具有自检、巡检功能；
- c) 入侵报警系统应有与远程中心进行有线和/或无线通信的接口，并能对通信线路的故障进行监控；
- d) 报警信号传输系统的技术要求应符合 IEC 60839-5；
- e) 报警传输系统串行数据接口的信息格式和协议，应符合 IEC 60839-7 的要求。

4.4 设备安装要求

入侵报警系统设备的安装、线缆的敷设等应符合有关国家标准、行业标准的要求和相关管理规定的要求。

4.5 电源

入侵报警系统的电源装置，应符合 GB/T 15408 的要求。系统应有备用电源，其容量至少应能保证系统正常工作时间大于 8 h。备用电源可以是下列之一或其组合：

- a) 二次电池及充电器；
- b) UPS 电源；
- c) 发电机。

5 安全性要求

- 5.1 入侵报警系统所使用的设备应符合 GB 16796 和相关产品标准规定的安全性要求。
- 5.2 入侵报警系统的任何部分的机械结构应有足够的强度，能满足使用环境的要求，并能防止由于机械不稳定、移动、突出物和锐边造成对人员的伤害。
- 5.3 在具有易燃易爆物质的特殊区域，入侵报警系统应有防爆措施并符合有关规定。
- 5.4 室外有线入侵报警系统的线路宜屏蔽。

6 电磁兼容性要求

入侵报警系统所使用的设备应能承受下列电磁兼容性试验要求：

- a) GB/T 17626.2—1998 中，严酷等级 3 的静电放电干扰；
- b) GB/T 17626.3—1998 中，严酷等级 3 的射频电磁场干扰；
- c) GB/T 17626.4—1998 中，严酷等级 3 的电快速瞬变脉冲群干扰；
- d) GB/T 17626.5—1998 中，严酷等级：交流电源线不超过 3，信号线不超过 2 的浪涌干扰；
- e) GB/T 17626.11—1998 中，严酷等级：40% U_T 10 个周期的电压暂降，0% U_T 10 个周期的短暂中断干扰；

试验中系统工作正常，不应产生误报警和漏报警。

7 防雷接地要求

- 7.1 设计入侵报警系统时，选用的设备应符合电子设备的雷电防护要求。
- 7.2 入侵报警系统应有防雷击措施。应设置电源避雷装置，宜设置信号避雷装置。
- 7.3 系统应等电位接地；单独接地电阻不大于 4 Ω ，接地导线截面应大于 25 mm²。

7.4 室外装置和线路的防雷和接地设计应符合有关国家标准和行业标准。

8 环境适应性要求

入侵报警系统所使用的设备应符合 GB/T 15211 的要求。

在有腐蚀性气体和易燃易爆环境中工作的人侵报警系统设备,应有相应的保护措施。

9 可靠性要求

入侵报警系统所使用的设备,其平均无故障间隔时间(MTBF)不应小于 5 000 h。

系统验收后的首次故障时间应大于 3 个月。

10 标志

入侵报警系统所使用设备应该在其上清晰而耐久地标出下列资料:

- a) 厂家名称;
- b) 批号;
- c) 生产日期(可以用代号);
- d) 供电额定值,例如标称电压、电流和频率。

端子和引线应该加以编号,加上颜色或者用别的方法来识别。

标记必须耐久和易读,标牌不应被容易取下且不卷曲。

11 文件提供

11.1 同设备一起提供的资料

如果不能从设备上看清楚,应随设备给出正确安装的详细说明书。任何设备在输入极性接反时可能受损的情况,应在使用说明书中陈述清楚。

11.2 设计文件

承建方应按 GA/T 75 的要求,向建设方提供规定的全部设计文件;图纸应规范,图形符号应符合 GA/T 74 的要求。
