ICS 13.310
A 91

中华人民共和国国家标准

GB/T 32581—2016

入侵和紧急报警系统技术要求

Specifications for intrusion and hold-up alarm systems

(IEC 62642-1:2010,Alarm systems—Intrusion and hold-up systems—Part 1:System requirements,NEQ)

2016-04-25 发布　　2016-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准与 IEC 62642-1:2010《报警系统　入侵和紧急系统　第 1 部分:系统要求》的一致性程度为非等效。

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这些专利的责任。

本标准由全国安全防范报警系统标准化技术委员会(SAC/TC 100)提出并归口。

本标准负责起草单位:公安部第一研究所、北京声迅电子股份有限公司、西安北方信息产业有限公司、国家安全防范报警系统产品质量监督检验中心(北京)、国家安全防范报警系统产品质量监督检验中心(上海)、陕西省公安厅、陕西省计量科学研究院、博世(珠海)安保系统有限公司、霍尼韦尔安防(中国)有限公司、深圳市豪恩安全科技有限公司。

本标准主要起草人:李天銮、施巨岭、周群、聂蓉、卢玉华、韩峰、解桂秋、张文弘、黄瑾、胡大为、宁文生、罗宗正、钱志雄、杨捷、季景林。

入侵和紧急报警系统技术要求

1 范围

本标准规定了入侵和紧急报警系统的构成与应用模式、安全等级、功能及性能要求、安全性要求、电磁兼容性要求、可靠性要求、环境适应性要求等，是设计、检测和验收入侵和紧急报警系统的基本依据。

本标准适用于建筑物内、外部的入侵和紧急报警系统、单独的入侵报警系统以及单独的紧急报警系统；也适用于其他电子系统中所包含的入侵报警系统、紧急报警系统、入侵和紧急报警系统。

2 规范性引用文件

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

GB 4208—2008 外壳防护等级(IP 代码)

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/T 15408 安全防范系统供电技术要求

GB 16796 安全防范报警设备 安全要求和试验方法

GB/T 30148—2013 安全防范报警系统 电磁兼容抗扰度要求和试验方法

GB 50343 建筑物电子信息系统防雷技术规范

GB 50348 安全防范工程技术规范

GA/T 670 安全防范系统雷电浪涌防护技术要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

报警 alarm

生命、财产或环境面临危险时发出的警告。

3.1.2

报警系统 alarm system

对面临生命、财产或环境的危险进行人工判别或自动探测并做出响应的电子系统或网络。

3.1.3

入侵报警系统 intruder alarm system；IAS

利用传感器技术和电子信息技术探测并指示进入或试图进入防护范围的报警系统。

3.1.4

紧急报警系统 hold-up alarm system；HAS

由用户主动触发紧急报警装置的报警系统。

3.1.5

入侵和紧急报警系统　intrusion and hold-up alarm system;I&HAS

兼有入侵报警和紧急报警的报警系统。

3.1.6

防护范围　supervised premises

入侵和/或紧急报警系统所防护的建筑物和/或场所或其部分。

3.1.7

防区　zone

在防护区域内,入侵和紧急报警系统可以探测到入侵或人为触发紧急报警装置的区域。

3.1.8

报警状态　alarm condition

报警系统因对面临的危险做出响应而产生的状态。

3.1.9

入侵报警状态　intruder alarm condition

报警系统对存在入侵行为做出响应的状态。

3.1.10

紧急报警状态　hold-up alarm condition

报警系统对人为触发紧急报警装置做出响应的状态。

3.1.11

正常状态　normal condition

不存在阻碍入侵和紧急报警系统设防的状态。

3.1.12

故障状态　fault condition

报警系统处于非正常工作状态。

3.1.13

入侵信号　intruder signal

入侵信息　intruder message

由入侵探测器产生的信号(信息)。

3.1.14

故障信号　fault signal

故障信息　fault message

出现故障情况下产生的信号(信息)。

3.1.15

防拆信号　tamper signal

防拆信息　tamper message

由防拆探测装置发出的信号(信息)。

3.1.16

遮挡　masked

移动探测器视场被阻挡的状态。

注:移动探测器是指因探测到人体移动而产生报警信号的入侵探测器。

3.1.17

探测范围明显减少　significant reduction of range

在探测器的探测范围中心轴上测量,探测器探测范围的减小超过指定范围的50%。

3.1.18

拆改 tamper

对报警系统的故意改动、蓄意干扰等行为。

注：俗称防拆。

3.1.19

防拆状态 tamper condition

报警系统探测到被拆改的一种状态。

3.1.20

防拆报警 tamper alarm

由防拆状态发出的报警。

3.1.21

防拆探测 tamper detection

探测报警系统是否受到拆改。

3.1.22

防拆保护 tamper protection

保护报警系统以免受到拆改的方式或方法。

3.1.23

互连 interconnection

报警系统部件之间传送信息和/或信号的方式。

3.1.24

互连有效性 availability of interconnection

能够传输信号或信息的互连状态。

3.1.25

周期性通信 periodic communication

周期性发送和/或应答的通信。

3.1.26

系统部件 system component

构成报警系统的单个部件。

3.1.27

部件替换 component substitution

使用其他装置替换报警系统部件，阻碍报警系统按原设计运行。

3.1.28

信息替换 message substitution

有意或无意地在报警系统部件之间建立替代的信息，妨碍报警系统正常运行。

3.1.29

入侵探测器 intrusion detector

对入侵或企图入侵行为进行探测、作出响应并产生入侵报警状态的装置。

3.1.30

紧急报警装置 hold-up device

由人工故意触发并产生紧急报警状态的装置。

3.1.31

互连媒介 interconnection media

传输信号或信息的介质。

3.1.32

控制指示设备 control and indicating equipment

具有信号接收、处理、控制、指示、记录和向上一级进行信息传输等功能的设备。

注：俗称防盗报警控制器。

3.1.33

告警装置 warning device

对通告给出声音报警的设备。

3.1.34

指示 indication

由报警系统产生的可听、可视或者其他可感知形式的信息。

3.1.35

告警指示 alert indication

听觉和/或视觉指示。

3.1.36

等待指示 pending indication

当不能同时显示所有信息时，对未显示信息的指示。

3.1.37

通告 notification

将报警、防拆或故障状态传递给告警装置和/或报警传输系统的过程。

3.1.38

事件 event

报警系统运行与操作所产生的状态。

3.1.39

事件记录 event recording

对报警系统的操作(如设防/撤防)或运行所产生的可事后分析事件的存储。

3.1.40

电源 power supply

为报警系统供电的报警系统组件。

3.1.41

主电源 prime power source

在正常工作条件下，为报警系统供电的电源。

3.1.42

辅助主电源 supplementary prime power source

独立于主电源，能够支持报警系统在一段时间内工作的电源，且不会影响备用电源的备用供电时间。

3.1.43

备用电源 alternative power source

当主电源不可用时，可以为报警系统提供预定时间电量的电源。

3.1.44

备用供电时间 standby period

备用电源能为报警系统供电的时间。

3.1.45

辅助控制设备 ancillary control equipment

执行辅助控制功能的设备。

3.1.46

防护区域收发器 supervised premises transceiver

防护区域内具有与报警系统、报警传输网络进行信息交互的接口设备。

3.1.47

传输路径 transmission path

报警系统和与其相关的报警接收中心之间的传输路径。

3.1.48

报警传输系统 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。

注：报警传输系统不包括本地直连，即报警系统部件之间的互连，他不需要通过接口把报警信息转换成适合传输的形式。

3.1.49

用户 user

经授权操作报警系统的人员。

3.1.50

操作人员 operator

获得授权使用报警系统的个人(用户)。

3.1.51

授权 authorisation

报警系统不同控制功能的使用许可。

3.1.52

授权代码 authorisation codes

允许使用报警系统功能的机械或逻辑密钥。

3.1.53

权限类别 access level

访问报警系统特定功能的权限。

3.1.54

设防 set

使系统或其一部分处于能通告报警状态的操作，也称为布防。

3.1.55

强制设防 override

允许用户在报警系统处于非正常状态时进行设防。

3.1.56

部分设防 part set

使系统的部分防区处于通告报警状态，其他防区处于撤防状态的操作。

3.1.57

撤防 unset

使系统或其一部分处于不能通告报警状态的操作。

3.1.58

旁路 isolation

报警系统的部分报警状态不能被通告的状态。此状态会一直保持到手动复位。也称为隔离。

3.1.59

暂时旁路 inhibit

报警系统的部分报警状态不能被通告的状态。此状态在撤防时自动复位。也称为暂时隔离。

3.1.60

恢复 restore

取消报警、防拆、故障或其他状态并将报警系统返回上一个状态的程序。

3.1.61

进入/退出路径 entry/exit route

通过授权进入或退出防护区域的路径。

3.1.62

报警响应时间 response time

从探测器探测到目标或人为触发紧急报警装置后产生报警状态信息，控制指示设备或远程报警接收中心接收到该信息并发出报警信号所需的时间。

3.1.63

报警接收中心 alarm receiving center

一直有人值守的、能接收或向前传输报警系统信息的场所。

3.2 缩略语

下列缩略语适用于本文件。

ACE：辅助控制设备(ancillary control equipment)

ARC：报警接收中心(alarm receiving centre)

ATS：报警传输系统(alarm transmission system)

CIE：控制指示设备(control and indicating equipment)

HAS：紧急报警系统(hold-up alarm system(s))

IAS：入侵报警系统(intruder alarm system(s))

I&HAS：入侵和紧急报警系统(intrusion and hold-up alarm system(s))

PS：电源(power supply)

SPT：防护区域收发器(supervised premises transceiver)

WD：告警装置(warning device)

4 系统构成与应用模式

4.1 系统基本构成

入侵和紧急报警系统(I&HAS)通常由前端设备、互连媒介、控制指示设备和告警装置等组成。

I&HAS 前端设备可以包括一个或多个探测器和紧急报警装置；互连媒介一般包括电缆、有线或无线数据采集和处理装置(或地址编解码器/发射接收装置)；控制指示设备一般包含控制主板、操作输入装置、指示/记录装置以及通信接口等。

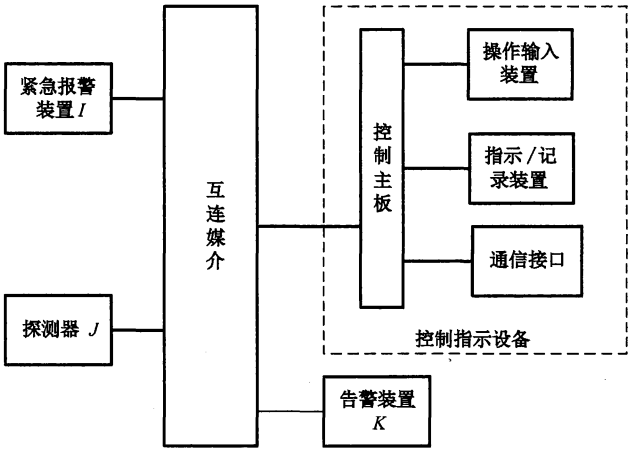
4.2 系统应用模式

4.2.1 系统应用模式分类

按系统的组成方式不同，I&HAS 可分为单一控制指示设备模式(简称单控制器模式)、多控制指示设备本地联网模式(简称本地联网模式)、远程联网模式和集成模式。

4.2.2 单控制器模式

该模式具有一个控制指示设备，其组成如图 1 所示。



说明：

I ——紧急报警装置的数量，$I \geqslant 0$；

J ——入侵探测器的数量，$J \geqslant 0$，I 与 J 不能同时为 0；

K——告警装置的数量，$K \geqslant 1$。

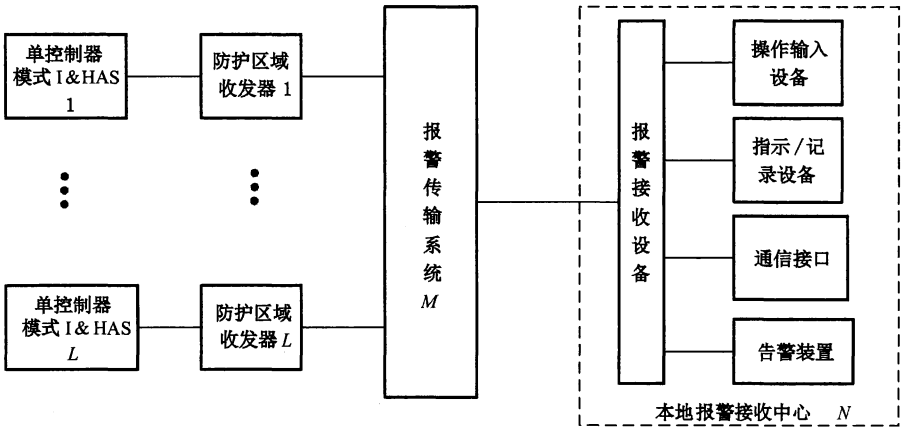
注 1：图中虚框内的功能部件，可以是分立的设备，也可以是组合或集成的一体化设备。

注 2：图中通信接口能提供与其他应用系统实现联动的信号或信息。

图 1 单控制器模式 I&HAS 结构图

4.2.3 本地联网模式

系统由一个或多个 I&HAS 和 1 个本地报警接收中心组成。其结构如图 2 所示。



说明：

L ——单控制器模式 I&HAS 及其防护区域收发器(SPT)的数量，$L \geqslant 1$；

M——报警传输系统(ATS)的数量，$M \geqslant 1$；

N——本地报警接收中心(ARC)的数量，$N \geqslant 1$。

注 1：本地报警接收中心位于防护区域内，与所设置的 I&HAS 防护区域均属于对该区域具有行政管理权的单位或部门。

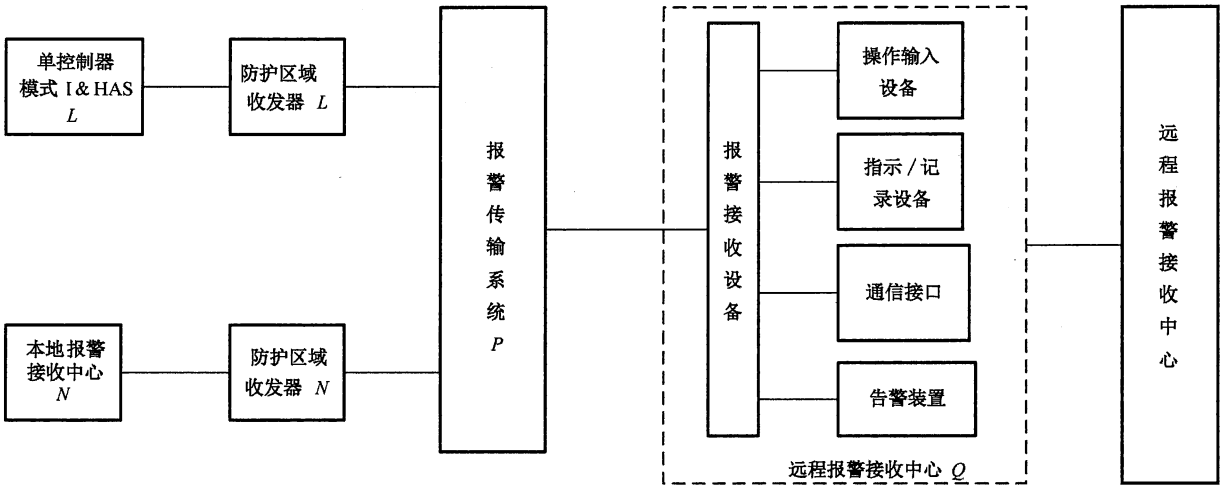
注 2：图中操作输入设备可以是控制键盘，也可以是计算机。

注 3：指示/记录设备可以是分立的单独设备，也可以是与报警接收设备集成的一体化设备，或计算机的硬盘等。

图 2 本地联网模式 I&HAS 结构图

4.2.4 远程联网模式

系统由一个或多个 I&HAS 和一个或多个报警接收中心组成，至少具有一个远程报警接收中心。其结构如图 3 所示。



说明：

L ——单控制器模式 I&HAS 及其防护区域收发器(SPT)的数量，$L \geqslant 1$；

N ——本地报警接收中心(ARC)及其防护区域收发器(SPT)的数量，$N \geqslant 1$；

P ——报警传输系统(ATS)的数量，$P \geqslant 1$；

Q ——远程报警接收中心(ARC)的数量，$Q \geqslant 1$。

注 1：远程报警接收中心位于防护区域外，其地理位置相对独立，与所设置的 I&HAS 防护区域不具有行政管理权的单位或部门。

注 2：远程报警接收中心可以是多级的。

图 3 远程联网模式 I&HAS 结构图

4.2.5 集成模式

当 I&HAS 与视频监控系统、出入口控制系统等安防子系统集成时，I&HAS 的功能性能应满足本标准的要求，其他安防子系统的故障不应影响 I&HAS 的正常工作。

5 安全等级

5.1 一般要求

5.1.1 I&HAS 应按其性能分为四个安全等级，1 级为最低等级，4 级为最高等级。I&HAS 的安全等级取决于系统中安全等级最低的部件等级。

5.1.2 单控制器模式 I&HAS 的安全等级取决于单控制器模式 I&HAS 中安全等级最低的部件。

5.1.3 本地联网模式 I&HAS 共享的部件安全等级应与其中安全等级最高的单控制器模式 I&HAS 一致。

5.2 安全等级的划分

5.2.1 等级 1:低安全等级

入侵者或抢劫者基本不具备 I&HAS 知识,且仅使用常见、有限的工具。

注:该等级通常可用于风险低、资产价值有限的防护对象。

5.2.2 等级 2:中低安全等级

入侵者或抢劫者仅具备少量 I&HAS 知识,懂得使用常规工具和便携式工具(如万用表)。

注:该等级通常用于风险较高、资产价值较高的防护对象。

5.2.3 等级 3:中高安全等级

入侵者或抢劫者熟悉 I&HAS,可以使用复杂工具和便携式电子设备。

注:该等级通常用于风险高、资产价值高的防护对象。

5.2.4 等级 4:高安全等级

入侵者或抢劫者具备实施入侵或抢劫的详细计划和所需的能力或资源,具有所有可获得的设备,且懂得替换 I&HAS 部件的方法。

注 1:本等级的安全性优先于其他所有要求。

注 2:在所有等级中,"入侵者"的定义也包含其他威胁类型(如抢劫或人身暴力的威胁,这些会影响 I&HAS 的设计)。

注 3:该等级通常用于风险很高、资产价值很高的防护对象。

6 功能及性能要求

6.1 探测

6.1.1 入侵探测

6.1.1.1 当入侵探测器被激活时,应能产生入侵信号或信息,其持续时间应能确保信息发送通信成功。

6.1.1.2 入侵探测器应能最大限度地探测到实际的入侵和将误报的风险降到最低。

注:入侵行为可能包括但不限于下列情况:

1) 翻越、爬越建筑载体、边界、孔洞等;
2) 打开门、窗、空调百叶窗等;
3) 用暴力、工具通过门、窗、天花板、墙及其他建筑结构;
4) 破碎玻璃;
5) 在建筑物内部移动;
6) 接触或接近保险柜或重要物品。

6.1.2 人为触发

6.1.2.1 当紧急报警装置被人为触发时,应能产生紧急报警信号或信息,其持续时间应能确保信息发送通信成功。

6.1.2.2 紧急报警装置应具有避免意外人为触发的措施。

6.1.3 防拆探测

当防拆探测被触发时，应能产生防拆探测信号或信息，其持续时间应能确保信息发送通信成功。

6.1.4 故障识别

6.1.4.1 I&HAS应能识别探测器、紧急报警装置、主电源、备用电源、互连、报警传输系统、告警装置等故障。

注：要求I&HAS能识别探测器故障、紧急报警设备故障、ATS故障和WD故障，并不要求此类设备需要提供专用的故障输出，例如WD故障可通过周期性通信失败获知。

6.1.4.2 当出现故障时，应产生故障信号或信息，其持续时间应能确保信息发送通信成功。

6.1.5 其他

6.1.5.1 在安全等级3和等级4中，I&HAS移动目标探测器应具有探测遮挡的功能。

6.1.5.2 在安全等级4中，I&HAS移动目标探测器应具有检测探测范围明显减少的功能。

6.1.5.3 在安全等级3和等级4中，室外周界入侵探测器（如泄漏电缆入侵探测器、光纤振动入侵探测器等）宜具有信号自分析处理、调节和设置等功能。

注：信号自分析处理是指通过提取出信号的特征值，与预存的数据进行分析、计算、比较、判断等，从而判别是否发出报警信号。

6.2 操作

6.2.1 一般要求

I&HAS的设计应将因操作人员错误操作产生报警的可能性降到最低。应对用于I&HAS操作的控制设备进行清楚无误的标记和合理布局，以将误操作的可能性降到最低。

6.2.2 权限类别

6.2.2.1 用户访问系统部件和控制功能有下列四种权限类别：

a) 类别1：操作访问无任何权限限制。

注：该类别指任何人均可访问，但只能进行简单的设防操作，一般通过按钮（开关）对部分或局部I&HAS进行设防。

b) 类别2：在不改变I&HAS配置情况下，操作访问能影响系统运行状态的功能。操作访问应受密钥、编码开关、锁或者其他等同方法限制，其密钥或编码不能访问权限类别3或4。

注：该类别通常适用于具有通行相应防护区域的使用、操作人和系统管理员。

c) 类别3：在不更改系统设备设计的情况下，操作访问能影响I&HAS配置的所有功能。操作访问应受密钥、编码开关、锁或者其他等同方法限制，其密钥或编码不能访问权限类别4。如需访问权限类别2，需获得权限类别2用户的许可，并在本地访问。

注：该类别通常适用于专业安装、维修人员。

d) 类别4：操作访问部件会改变设备的设计。操作访问应受密钥、编码开关、锁或者其他等效方法限制，其密钥或编码不能访问权限类别2和3。除非权限类别2和权限类别3的用户授权，否则不允许使用权限类别4。

注1：该类别通常适用于设备制造商或代理商。

注2：权限类别4只适用于在不触发CIE或ACE上的防拆装置时更改操作程序软件。

6.2.2.2 权限类别2、3和4满足表2中的要求时可通过远程获得授权。

6.2.2.3 每种权限类别可用的功能应满足表1的要求。

表 1　权限类别

功　　能	权限类别			
	1	2	3[a]	4[b]
设防	NP[e]	P	P	NP
撤防	NP	P	P	NP
I&HAS 恢复	NP	P	P	NP
验证 I&HAS 功能	NP	P	P	NP
查询事件日志	NP	P	P	NP
暂时旁路/旁路/强制[c]	NP	P	P	NP
添加/更改个人授权代码	NP	P[d]	P[d]	P[d]
添加/删除权限类别 2 用户和代码	NP	P	P	NP
添加/更改现场特定数据	NP	NP	P	NP
更改/更换基本程序	NP	NP	NP	P

注 1：P 表示允许、NP 表示不允许。

注 2：本表所列功能并不代表 I&HAS 提供的这些功能是强制性的。

注 3：本表列出了每项功能的权限类别；适用于每项功能的更多条件将在本标准的其他部分规定。

注 4：与用户权限相关的要求不会限制在 CIE 首次通电时初始化用户访问权限的方法(如，存在默认或一次性使用访问代码)。

注 5：现场特定数据是指与 I&HAS 架构相关的信息，如运行参数。

[a] 仅在获得权限类别 2 授权时。

[b] 仅在获得权限类别 2 和权限类别 3 授权时。

[c] 取决于 I&HAS 安全等级。

[d] 个人仅允许更改其自己的用户代码。

[e] 仅 I&HAS 安全等级 1 允许，参见 6.2.5。

6.2.3　授权

访问 I&HAS 功能的用户权限应满足表 2 中要求的授权代码或同等方法。

表 2　授权代码要求

权限类别	安全等级 1 组合	安全等级 2 组合	安全等级 3 组合	安全等级 4 组合
逻辑密钥量	1 000	10 000	100 000	1 000 000
机械密钥量	300	3 000	15 000	50 000

注：除本表所列的机械钥匙和逻辑密钥外，还可使用其他授权方法，如生物特征密钥。

6.2.4　设防和撤防

对于各权限类别用户，应具有对 IAS、HAS、I&HAS 或其部分进行设防和撤防的不同权限和相应

方法。

6.2.5 设防

6.2.5.1 当系统处于正常状态时，应由授权用户进行设防，在设防期间，宜具有设防指示。

6.2.5.2 权限类别 2 或 3 的用户应按表 2 中安全等级指定的授权代码或等同方法，在 I&HAS 的相应安全等级中设防。

6.2.5.3 在 I&HAS 安全等级 1 中，任何权限类别用户在防护区域内均可开始设防(如通过按钮设防)，且在完成设置前可取消设防。

注：权限类别 1 的用户启动系统设防时宜谨慎。

6.2.6 禁止设防

除 6.2.7 允许的强制设防的情况外，当存在表 3 中显示的一个或多个状态时，应禁止 I&HAS 或其部分设防。

表 3 禁止设防

禁止设防状态	安全等级 1	安全等级 2	安全等级 3	安全等级 4
入侵探测器处于激活状态[a]	M	M	M	M
紧急报警装置处于激活状态	M	M	M	M
移动目标探测器被遮挡	Op	Op	M	M
移动目标探测器距离明显减小	Op	Op	Op	M
入侵探测器故障	M	M	M	M
拆改状态	M	M	M	M
互连故障	M	M	M	M
主电源故障	M	M	M	M
备用电源故障	M	M	M	M
报警传输系统故障	M	M	M	M
告警装置故障	M	M	M	M
ATS 和 WD 故障[b]	M	M	M	M
其他故障	Op	M	M	M

注 1：M 表示强制、Op 表示可选。

注 2：本表所列状态并不代表在 I&HAS 中包括相关功能。

[a] 可不包括设定退出路径上的入侵探测器。

[b] 所有现有的 ATS 和 WD 出现的不能发出通告的故障。

6.2.7 强制设防

6.2.7.1 强制设防的状态可通过表 4 中权限类别用户操作。

6.2.7.2 强制设防应在事件日志中记录。

6.2.7.3 如果强制设防会导致出现报警状态，则不应该强制设防。

表 4　强制设防状态

强制设防状态	安全等级 1	安全等级 2	安全等级 3	安全等级 4
入侵探测器处于激活状态[a]	权限类别 2	权限类别 2	权限类别 2	权限类别 2
紧急报警设备处于激活状态	权限类别 2	权限类别 2	权限类别 2	权限类别 2
移动目标探测器被遮挡	权限类别 2	权限类别 2	权限类别 2	权限类别 2
移动目标探测器范围减小	权限类别 2	权限类别 2	权限类别 2	权限类别 2
入侵探测器故障	权限类别 2	权限类别 2	权限类别 2	权限类别 2
拆改状态	权限类别 2	权限类别 2	权限类别 2 或 3	权限类别 2 或 3
互连故障	权限类别 2	权限类别 2	权限类别 2 或 3	权限类别 2 或 3
主电源故障	权限类别 2	权限类别 2	权限类别 2	权限类别 2
备用电源故障	权限类别 2	权限类别 2	权限类别 2	权限类别 2 或 3
报警传输系统故障	权限类别 2	权限类别 2	权限类别 2 或 3	权限类别 2 或 3
告警装置故障	权限类别 2	权限类别 2	权限类别 2 或 3	权限类别 2 或 3
ATS 和 WD 故障[b]	权限类别 2	权限类别 2	权限类别 2 或 3	权限类别 2 或 3
其他故障	权限类别 2	权限类别 2	权限类别 2	权限类别 2 或 3
注：本表所列状态并不代表在 I&HAS 中包括相关功能。				
[a] 可不包括设定退出路径上的入侵探测器。 [b] 所有现有的 ATS 和 WD 出现的不能发出通告的故障。				

6.2.8　设防状态

6.2.8.1　当设防程序成功完成后，在一定时间内应有设防完成指示，显示系统或其中一部分已改变为设防状态。

6.2.8.2　当 I&HAS 或其中一部分处于设防状态时：

a)　进入防护区域及部分防护区域时应发出报警；

b)　当通过进入/退出路径时，应启动进入程序；

c)　对于 I&HAS 安全等级 1 和等级 2，可提供设防/撤防状态的指示。

6.2.9　撤防

6.2.9.1　在所有安全等级中，I&HAS 或其部分撤防应通过授权获得。

6.2.9.2　当对 I&HAS 或其部分按 6.2.8.2b)撤防时：

a)　应设定从进入位置到撤防设备间的路径。如果按正确路径进入防护区域撤防成功，则已设定路径上的探测器报警信息应被忽略。

注：通过进入/退出路径进入防护区域撤防是撤防的一种方法。也可不进入防护区域撤防，即从防护区域外部撤防。

b)　完成撤防最长时间应不大于 45 s 或在 1 s～300 s 内可调，在此期间，应提供进入指示。如果在规定的时间内未完成撤防，在超出时间后应发出报警状态。当成功完成撤防时，应有指示(见表 6)。

c)　如果在撤防期间出现入侵报警状态，应给出指示或由告警装置发出通告。当 IAS 具备远程通知功能时，指示设备或告警装置应运行不少于 30 s 且超出进入延时时间后，才可进行远程

报警。

6.2.10 恢复

在I&HAS或其中一部分出现入侵报警、紧急报警、拆改、故障、遮挡、探测范围明显减小等状态之后，应有恢复的必要方法，恢复操作仅限于权限类别2或3的用户。

6.2.11 暂时旁路

I&HAS宜具有暂时旁路的方法，暂时旁路操作仅限于权限类别2或3的用户。

6.2.12 旁路

I&HAS宜具有旁路的方法。对于远程联网模式的I&HAS，旁路操作仅限于权限类别2或3的用户；对于本地联网模式的I&HAS，旁路操作仅限于权限类别2的用户。

6.2.13 测试

应给权限类别2的用户提供对I&HAS入侵探测器和紧急报警装置进行无损坏性功能测试的方法。

6.3 信号/信息处理

6.3.1 一般要求

6.3.1.1 信号或信息的处理应包括其状态、类型以及I&HAS的配置。

6.3.1.2 入侵、紧急报警、拆改和故障等信号和/或信息的处理应满足表5的要求。

6.3.1.3 宜将多个独立探测器进行逻辑分组，以便根据需要产生入侵报警状态的一条或多条报警信号或信息。

6.3.1.4 单个探测器可设置为需多次激活方能产生一个入侵报警信号或信息。

6.3.2 入侵信号或信息

6.3.2.1 来自入侵探测器的信号和/或信息应按照表5中的要求进行处理。

6.3.2.2 外接告警装置的报警声音运行最长时间应满足管理要求。

6.3.2.3 单次报警状态通告时间截止后，I&HAS应具有继续通告报警状态的能力。

注：报警接收中心收到多个入侵报警、拆改或故障状态通告时，ARC宜进行处理以避免无效响应。

6.3.3 紧急报警信号或信息

6.3.3.1 来自紧急报警装置的信号和/或信息应按表5中的要求进行处理。

6.3.3.2 通告紧急报警状态以后，来自其他紧急报警装置的信号和/或信息应继续按表5中的要求进行处理。

6.3.3.3 在之前的紧急报警信号和信息发出后180 s以内，来自同一个紧急报警装置的多个信号和/或信息不必按表5中的要求进行处理。

6.3.4 防拆报警信号或信息

根据I&HAS的安全等级，防拆报警信号或信息应按照表5中的要求进行处理。

6.3.5 故障信号或信息

根据I&HAS的安全等级，故障信号或信息应按照表5中的要求进行处理。

6.3.6 遮挡报警信号或信息

遮挡报警信号或信息应根据表5中的入侵或者故障信号或信息进行处理。

6.3.7 探测范围明显减少信号或信息

探测范围明显减少的信号或信息应根据表5中的入侵或者故障信号或信息进行处理。

表5 入侵、紧急、防拆报警和故障信号和/或信息处理

I&HAS状态[a]	输出	安全等级1				安全等级2				安全等级3				安全等级4			
		输入				输入				输入				输入			
		紧急信号/信息	入侵信号/信息	防拆信号/信息	故障信号/信息	紧急信号/信息	入侵信号/信息	防拆信号/信息	故障信号/信息	紧急信号/信息	入侵信号/信息	防拆信号/信息	故障信号/信息	紧急信号/信息	入侵信号/信息	防拆信号/信息	故障信号/信息
设防	指示	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	外部声音报警	Op	M	M	NP	Op	M	M	NP	Op	M	Op	NP	Op	M	Op	NP
	内部声音报警	Op	M	M	Op	Op	M	M	Op	Op	M	M	Op	Op	M	M	Op
	ATS信息类型	紧急	入侵	入侵或防拆	入侵或故障	紧急[b]	入侵	入侵或防拆	故障	紧急[b]	入侵	防拆	故障	紧急[b]	入侵	防拆	故障
撤防	指示	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	外部声音报警	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP	Op	NP	NP	NP
	内部声音报警	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP	Op	NP
	ATS信息类型	紧急时Op	NP	防拆时Op	故障时Op	紧急时Op	NP	防拆时Op	故障时Op	紧急	NP	防拆	故障	紧急	NP	防拆	故障

注1：M表示强制、Op表示可选、NP表示不允许。

注2：如果I&HAS不包括告警装置以及报警传输系统，则此表格的相关要求不适用。但是，如果I&HAS包括此类设备或系统，则应满足此表格的要求。

注3：包括Op、M或NP的单元格表示指示设备、告警装置和ATS的输出结果，其运行取决于这些功能在相关章节中指定的要求。

注4：对于每一项内容，尽管技术规格显示为强制，如果未提供通告选项(参见表8)，则不需要相应的输出。

注5：指示要求应与6.4结合使用，且指示的运行状态取决于6.4的要求。

注6：撤防状态下，外部WD不应由CIE激活。但是若WD防拆探测被激活或与CIE互连失败，外部WD可以自行激活。

[a] 应根据I&HAS、IAS或HAS或者其中一部分的状态处理信号和/或信息。

[b] 与紧急报警相关的防区信息应包括在传输至ARC的信息中。

6.4 指示

6.4.1 一般要求

6.4.1.1 应按表6中的要求指示。当I&HAS不具有某种功能时，与其相关的指示要求不适用。

注1：例如：当I&HAS不使用紧急报警功能时，与紧急报警相关的指示不作要求。

注2：在特定情况下可不给出指示，例如：在某种紧急报警装置被触发时，不宜给出本地报警指示。

6.4.1.2 当系统无法同时显示所有的信息时，应有待显示信息指示。

6.4.1.3 当I&HAS在撤防状态时，如有待显示信息，应能向用户给出提示。

6.4.1.4 本节所要求的所有强制性指示应至少在一个CIE或ACE中，也可在其他位置指示。

6.4.1.5 在I&HAS具备多个报警传输系统的情况下，当探测到任意一个传输系统故障时，应向系统操作人员给出指示。

表6 指示

指示	安全等级1	安全等级2	安全等级3	安全等级4
I&HAS设防/部分设防状态	M	M	M	M
I&HAS撤防状态	M	M	M	M
紧急报警状态	M	M	M	M
紧急防区识别	M	M	M	M
入侵报警状态	M	M	M	M
入侵防区识别	M	M	M	M
独立入侵探测器指示(参见6.4.4)[a]	Op	Op	M	M
探测器报警状态指示装置(参见6.4.4)	M	M	M	M
暂时旁路	M	M	M	M
旁路	M	M	M	M
故障状态	M	M	M	M
防拆状态	M	M	M	M
遮挡(参见6.1.5)	Op	Op	M	M
探测范围明显减小(参见6.1.5)[d]	Op	Op	Op	M
等待指示	M	M	M	M
告警指示	M	M	M	M
设防(参见6.2.5)[b]	Op	Op	Op	Op
完成设防(参见6.2.8)[b]	M	M	M	M
进入指示(参见6.2.9.2)[b,c]	M	M	M	M
完成撤防(参见6.2.9.2)[c]	M	M	M	M

注1：M表示强制、Op表示可选。

注2：当某种功能，如紧急报警未提供时，则不要求提供相关指示。

[a] 独立探测器识别仅适用于具有处理能力的探测器，参见6.4.4。

[b] 这些指示受时间限制。

[c] 仅当使用6.2.9.2中描述的可选撤防程序时为必选指示。

[d] 可与“遮挡”指示相同。

6.4.2 权限类别的指示

应按表7中的指示对权限类别1的用户提供指示。表6中的其他指示只能提供给权限类别2、3或4的用户。

表 7　权限类别 1 用户在设防和撤防期间的指示

指　示	安全等级 1	安全等级 2	安全等级 3	安全等级 4
I&HAS 设防/部分设防状态[参见 6.2.8.2c)]	Op	Op	NP	NP
I&HAS 撤防状态[参见 6.2.8.2c)]	Op	Op	NP	NP
撤防期间告警指示	M	M	M	M
设防期间撤防操作指示(参见 6.2.5)[a]	Op	Op	Op	Op
设防完成(参见 6.2.8)[a]	M	M	M	M
设防状态下的进入指示(参见 6.2.9.2)[a, b]	M	M	M	M
撤防完成(参见 6.2.9.2)[a, b]	M	M	M	M
注 1：Op 表示可选、NP 表示不允许、M 表示强制。 注 2：在 I&HAS 安全等级 3 和安全等级 4 下，不可对权限类别 1 的用户显示 I&HAS 的设防/撤防状态。 注 3：当某种功能未提供时，则不要求提供相关指示。				
[a] 这些指示受时间限制。 [b] 仅当使用 6.2.9.2 中描述的可选撤防程序时为必选指示。				

6.4.3　取消指示

表 6 中要求的指示(受时间限制的指示除外)在用户取消前应保持有效状态。

6.4.4　探测器指示

6.4.4.1　具备有处理能力的入侵探测器应按表 6 所规定的独立的报警状态指示。

6.4.4.2　不具备处理能力(如门磁开关，专门的指示装置)的入侵探测器可共享同一指示装置，但共享同一指示装置的探测器不多于 10 个。

6.5　通告

6.5.1　入侵报警、紧急报警、防拆、故障以及其他状态应由 ATS 和/或声音 WD 按表 8 中的要求进行通告。I&HAS 应满足表 8 中至少一个安全等级某个选项组合的通告。

6.5.2　告警装置的运行应具有可被禁止的功能。

注：如，在发生抢劫，且紧急报警装置被触发时，宜避免现场告警装置运行。

6.5.3　根据 I&HAS 的安全等级，当 I&HAS 包含报警传输系统时，报警传输系统应满足附录 A 和附录 B 中的性能要求。

6.5.4　当 I&HAS 同时具有 ATS 和 WD 时，告警装置可延迟运行，但延时时间应不大于 10 min。在延时时间段内，报警接收中心或其他接收设备通过报警传输系统接收通告并确认，则应禁止告警装置运行。

6.5.5　当探测到报警传输系统的传输路径有一个或多个故障时，应自动取消告警装置延迟运行。

6.5.6　告警装置的发声运行时间应满足当地的相关规定。运行时间宜不小于 90 s、不大于 15 min。

6.5.7　主电源故障的通告延迟时间不应大于 1 h。

表 8 通告要求

通告设备		安全等级 1			安全等级 2				安全等级 3				安全等级 4			
		选项			选项				选项				选项			
		A	B	C	A	B	C	D	A	B	C	D	A	B	C	D
远程供电的发声告警装置		2	Op	Op	2	Op	Op	Op	2	Op	Op	Op	2	Op	Op	Op
自供电的发声告警装置		Op	1	Op	Op	1	Op	Op	Op	1	Op	Op	Op	1	Op	Op
PSTN 传输	主 ATS	Op	Op	ATS 1	ATS 2	ATS 2	ATS 2	ATS 3	ATS 4	ATS 4	ATS 4	ATS 5	ATS 5	ATS 5	ATS 5	ATS 6
	附加 ATS	Op	Op	Op	Op	Op	ATS 1	Op	Op	Op	ATS 3	Op	Op	Op	ATS 4	Op
IP 传输	主 ATS	Op	Op	ATS I1	ATS I2	ATS I2	ATS I2	ATS I3	ATS I4	ATS I4	ATS I4	ATS I5	ATS I5	ATS I5	ATS I5	ATS I6
	附加 ATS	Op	Op	Op	Op	Op	ATS I1	Op	Op	Op	ATS I3	Op	Op	Op	ATS I4	Op

注 1：Op 表示可选。

注 2：单元格中的数字的代表相应发声告警装置数量。

注 3：ATS 1，ATS 2，…，ATS 6 参考附录 A 中规定的性能要求，ATS I1，ATS I2，…，ATS I6 参考附录 B 中规定的性能要求。

注 4：本表中 A、B、C、D 各列代表各类安全等级下的不同配置选项。PSTN 传输与 IP 传输为和/或的关系。

注 5：当有 2 个 ATS 时，建议各自使用独立的传输路径，且使用不同的技术，典型的应用是有线和无线传输技术。

注 6：多个 ATS 可以共享一个 SPT。

注 7：在工作正常状态下，主 ATS 和附加的 ATS 应能达到所规定的性能要求。本标准并不要求在主 ATS 出现故障时改变附加 ATS 的性能。

6.6 防拆

6.6.1 防拆保护

6.6.1.1 I&HAS 部件应提供阻止访问内部元件的方法，以便将被拆改风险降到最小。防拆保护的要求应根据 I&HAS 部件的位置（防护区域内部或外部）和安全等级变化。

6.6.1.2 所有端子以及机械和电气调试方法应置于部件外壳内部。

6.6.1.3 外壳应足够坚固，以防止进入设备内部对元件造成看不见的损坏。

6.6.1.4 开启 I&HAS 部件的方法应安全可靠，应使用合适的工具。

6.6.2 防拆探测

6.6.2.1 表 9 中规定了 I&HAS 部件的防拆探测要求。表 10 规定了要探测的拆改类型。防拆探测应能在所有等级的设防和撤防状态下工作。

6.6.2.2 应具有防止防护区域外部的辅助控制设备被替换的方法，和/或防止辅助控制设备与控制指示设备之间的信号或信息被替换的方法。当此类替换不会影响 I&HAS 的正常运行时，本要求不适用。

表 9 防拆探测的部件

部件	安全等级 1	安全等级 2	安全等级 3	安全等级 4
CIE/ACE[a]/SPT/WD/PS	M	M	M	M
紧急报警装置[a]	Op	M	M	M
入侵探测器[b]	Op	M	M	M
接线盒[c]	Op	Op	M	M
注：Op 表示可选、M 表示强制。				
[a] 便携式 ACE 和紧急报警装置不要求满足此表中的要求。 [b] 磁驱动或机械驱动开关在实际应用上是可以不提供防拆探测。但是，在某些安全等级中，可能需要对磁性启动开关进行保护，以防止受到外部磁性或电磁源的破坏。 [c] 在安全等级 3 中，当 I&HAS 包括信号或信息替换防护时，不必对接线盒提供防拆探测。				

表 10 防拆探测的方法

方法	安全等级 1	安全等级 2	安全等级 3	安全等级 4
正常方法开启	M	M	M	M
从底座拆卸——无线 I&HAS 部件	Op	M	M	M
从底座拆卸——有线 I&HAS 部件	Op	Op	M[c]	M
侵入声音 WD	Op	Op	Op	M[a]
侵入 CIE/ACE/SPT	Op	Op	Op	M[a]
探测器方向调节	Op	Op	M[b]	M[b]
注：Op 表示可选、M 表示强制。				
[a] 适用于在防护区域外部的 CIE、ACE、SPT 或 WD。 [b] 当方向调节可用时。 [c] 本要求对于接线盒和常开开关(磁性)为可选项。				

6.6.3 替换监测

安全等级 4 的 I&HAS 应对部件替换进行监测。当 I&HAS 处于设防或撤防状态，且探测到被替换时，应产生防拆信号或信息。

6.6.4 替换监测时间

I&HAS 部件的替换应在表 11 中指定的时间内被探测。

表 11 替换监测时间

监测要求	安全等级 1 s	安全等级 2 s	安全等级 3 s	安全等级 4 s
I&HAS 部件被替换	Op	Op	100[a]	10
注：Op 表示可选。				
[a] 当 I&HAS 的等级包含替换探测。				

6.7 互连

6.7.1 一般要求

6.7.1.1 互连应根据其用途和设计要求，为I&HAS部件之间的通信提供可靠方法。

6.7.1.2 互连的设计应将信号或信息的延迟、修改、替换或丢失的可能性降到最低。

6.7.1.3 I&HAS应具有验证I&HAS部件之间正常通信的功能。

6.7.1.4 应可通过对互连监测，探测以下两种情况：

a) 不能满足6.7.2和6.7.3中有效性要求；

b) 6.7.5中关于对信号或信息的延迟、更改、替换或丢失的要求。

6.7.1.5 当互连功能正常时，信号或信息从源部件传输到目标部件的时间应满足6.7.2的要求。

6.7.1.6 当互连媒介受到来自防护区域外部的影响时，安全等级4的I&HAS应采取特殊措施以确保信号或信息不能被延迟、修改、替换或丢失。

6.7.2 互连有效性

6.7.2.1 互连应有效地为传输信号或信息提供一种可靠的手段。

6.7.2.2 当互连与其他安防子系统共享时，I&HAS的有效互连应满足本标准的要求。

6.7.3 互连监测

6.7.3.1 表12规定了允许互连的最大无效时间。当超出该最大允许时间时，应产生防拆或故障信号或信息。本条规定的要求不适用于便携式紧急报警装置和便携式ACE。

表12 互连的最大无效时间

监测要求	安全等级1 s	安全等级2 s	安全等级3 s	安全等级4 s
允许最大无效时间	100	100	100	10
注：以上要求旨在通过对监控通信媒介来建立通信，以确定是否可以传输信号或信息。可通过以下方法进行监测：当采用无线电射频技术时，监测是否受干扰；或者I&HAS与其他安防子系统共享总线时，检测其他安防子系统是否永久控制总线。				

6.7.3.2 对于I&HAS安全等级1和安全等级2，当周期性通信的时间(见6.7.4.1)大于100 s时，应对互连媒介进行监测，以建立其传输信号或信息的有效性。

6.7.4 验证

6.7.4.1 互连完整性——周期性通信

应对互连的完整性进行反复验证，验证的时间间隔不应大于表13的规定。对于按照表13的规定而无法验证通信事件，应生成如下信号或信息：

a) 当识别到故障状态且通信无法验证时，则应生成故障信号或信息；

b) 当无法识别的原因存在且通信无法验证时，则应生成防拆或故障信号或信息。

表 13 验证间隔

监测要求	安全等级 1 min	安全等级 2 min	安全等级 3 s	安全等级 4 s
周期性通信信号或信息之间最大允许间隔	240	120	100	10

6.7.4.2 设防期间的验证

当进行设防操作时，如果任何系统部件上的最后一个验证信号或信息大于表 14 中指定的时间间隔，I&HAS 应立即进行一次验证，验证成功后，方可设防。

表 14 距离最后一个信号或信息的最大时间间隔

监测要求	安全等级 1 min	安全等级 2 min	安全等级 3 s	安全等级 4 s
接收到上个信号或信息的最大时间间隔	60	20	60	10

6.7.5 通信安全性

6.7.5.1 安全等级 4 的 I&HAS 应具有探测任何信号或信息的延迟、修改、替换或丢失的方法。

6.7.5.2 探测任何信号或信息的延迟、修改、替换或丢失允许的最大时间周期不得大于表 13 中指定的值加上 10 s。

6.7.5.3 如果探测到任何信号或信息延迟、修改、替换或丢失等事件，应产生故障或防拆信号或信息。

6.8 响应

6.8.1 激发保持时间超过 400 ms 的入侵探测、紧急报警和防拆信号应被处理。故障信号保持时间超过 10 s 应被处理。

注：仅在确保通信成功的时间时期内，发出紧急报警、入侵、防拆和故障信息。

6.8.2 入侵、紧急、防拆以及故障信号和/或信息的报警响应时间应满足以下要求：

a) 单控制器模式：不大于 2 s。

b) 本地联网模式：

1) 安全等级 1：不大于 10 s；

2) 安全等级 2、3：不大于 5 s；

3) 安全等级 4：不大于 2 s。

c) 远程联网模式：

1) 安全等级 1、2：不大于 20 s；

2) 安全等级 3、4：不大于 10 s。

6.9 记录

6.9.1 应根据 I&HAS 的安全等级对表 16 中规定的事件进行记录。

6.9.2 应具有事件记录的防篡改措施。

6.9.3 事件记录应不低于表 15 中要求的容量。当记录的容量有限且事件记录达到最大容量时，应能自动循环覆盖原有记录。

6.9.4 除事件记录外，第 2、3 和 4 安全等级的 I&HAS 还应记录事件发生的时间和日期。I&HAS 应

具有自动和/或手动校时的接口，联网模式的I&HAS时钟与北京时间的误差应不大于±5 s。I&HAS宜具有自动和/或手动校时的功能。

6.9.5 事件可记录在I&HAS部件或报警接收中心，应具有远程传输失败提示功能，安全等级2、3和4的I&HAS应具有记录等待传输事件的功能，远程事件记录应符合表15的要求。

注：当事件记录在报警接收中心完成时，在I&HAS中应提供必要的通告方法。在报警接收中心记录事件的方法应满足本条的要求。

6.9.6 对于安全等级3和等级4，应具有事件记录永久保存的设备。

6.9.7 在设防或撤防期间，任何单一来源事件的记录数量应不小于3个、不大于10个。

表15 事件存储

容量和持续时间	安全等级1	安全等级2	安全等级3	安全等级4
存储容量——最低存储事件数量	Op	250个事件	500个事件	1 000个事件
I&HAS电源丢失后，存储功能的最低持续时间	Op	30 d	30 d	30 d
注：Op表示可选。				

表16 事件记录

事件	安全等级1	安全等级2	安全等级3	安全等级4
设防/撤防时的用户身份(如果可能)	Op	Op	M	M
设防/分区设防	Op	M	M	M
撤防	Op	M	M	M
紧急报警状态	Op	M	M	M
紧急防区识别	Op	Op	M	M
入侵报警状态	Op	M	M	M
入侵防区识别	Op	Op	M	M
防拆状态	Op	M	M	M
独立入侵探测器识别(参见6.4.4)	Op	Op	M	M
防区/入侵探测器/紧急报警装置暂时旁路	Op	M	M	M
防区/入侵探测器/紧急报警装置旁路	Op	M	M	M
探测器故障	Op	Op	M	M
紧急报警装置故障	Op	Op	M	M
主电源故障	Op	Op	M	M
备用电源故障	Op	Op	M	M
互连故障	Op	M	M	M
ATS故障	Op	M	M	M
告警装置故障	Op	M	M	M
其他故障	Op	Op	Op	Op
强制设防状态	Op	M	M	M
探测器首次报警	Op	M	M	M

表 16（续）

事件	安全等级 1	安全等级 2	安全等级 3	安全等级 4
需要更换电池[a]	Op	Op	M	M
防区/探测器强制设置	Op	M	M	M
更改时间和日期	Op	Op	M	M
更改现场特定数据	Op	Op	M	M
权限类别 2 用户被权限类别 3 用户添加/删除	Op	M	M	M
替换探测（6.6.3）	Op	Op	Op	M
注 1：Op 表示可选、M 表示强制。 注 2：此表中要求的事件记录并不代表需要提供相关的功能；但是，当存在与事件记录相关的功能时，则应按照本表的要求进行记录。				
[a] 仅适用于一次性电池。				

6.10 供电

6.10.1 电源类型

I&HAS 中所包含的电源应满足 GB/T 15408 的相关要求。用于 I&HAS 的电源类型如下：

a) 类型 A：主电源（如市电），和由 I&HAS 进行充电的备用电源（如可由 I&HAS 自动充电的电池）。

b) 类型 B：主电源，和不由 I&HAS 充电的备用电源（如不能由 I&HAS 自动充电的电池）。

c) 类型 C：容量有限的主电源，如电池（如不可充电的电池或一次性电池）。

6.10.2 要求

6.10.2.1 电源应能支持 I&HAS 在所有状态下运行，储能设备的充电时间不应超出表 18 中的要求。电源可置于一个或多个 I&HAS 部件或独立的外壳中。

6.10.2.2 主电源和备用电源之间的转换和恢复不应产生报警信号或其他会影响 I&HAS 的状态。

6.10.2.3 在所有 I&HAS 安全等级中，如果类型 C 电源作为主电源，则主电源应能够在所有使用状态下为 I&HAS 供电至少一年。在电压降到低于能维持 I&HAS 正常运行所要求的水平之前，类型 C 电源应产生故障信号或信息。

6.10.2.4 对于所有 I&HAS，在使用类型 A 或 B 电源时，如果主电源出现故障，备用电源应向 I&HAS 供电，且其供电时间应满足表 17 的要求。

6.10.2.5 在表 17 中要求的时间内，电源应能提供 I&HAS 正常运行所需的电能，包括有足够的电能对由两个独立的入侵报警信号或信息进行处理，并能确保产生所有强制性的指示和通告。

表 17 备用电源最短持续时间

电源的类型	安全等级 1 h	安全等级 2 h	安全等级 3 h	安全等级 4 h
类型 A	8	8	12	12
类型 B	24	24	120	120

6.10.2.6 在安全等级3和4的I&HAS，当主电源故障通知到报警接收中心或其他远程中心时，备用电源的持续时间可减半。

注：如6.5中规定，主电源故障的通告时间可最多延迟1 h。

6.10.2.7 对于类型A和B电源，当有提供辅助主电源时，且具有主电源和辅助主电源之间能自动进行切换，则备用电源对I&HAS供电的时间可降至4 h。

6.10.2.8 所有安全等级的I&HAS应按6.4的要求，在备用电源可用电压降到低于I&HAS正常运行所要求的水平时，应发出指示。

注：发出的实际电压指示与备用电源能够为I&HAS供电的持续时间是没有直接关系。

6.10.2.9 在包括类型A电源的I&HAS，备用电源应能按照表18中指定时间内充电至最大容量的80%。

表18 备用电源——充电时间

类型A电源	安全等级1 h	安全等级2 h	安全等级3 h	安全等级4 h
充电最长时间	72	72	24	24

6.11 防雷接地要求

6.11.1 I&HAS应满足GB 50348、GB 50343和GA/T 670等现行国家标准的相关要求。

6.11.2 I&HAS选用的设备应满足电子设备的雷电防护要求。

6.11.3 I&HAS应有雷电防护措施。应设置电源浪涌保护器，宜设置信号浪涌保护器。

6.11.4 I&HAS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 mm^2。

7 安全性要求

7.1 应满足GB 50348等现行国家标准的相关要求。

7.2 I&HAS所使用的设备应满足GB 16796和相关产品标准规定的安全性要求。

7.3 在具有易燃易爆物质的特殊区域，I&HAS应有防爆措施并满足有关规定。

7.4 I&HAS的室外有线线路宜具有抗干扰措施。

7.5 I&HAS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。

7.6 系统运行的密钥或编码不应是弱口令。

注：弱口令一般指设备出厂默认的密钥或编码、顺序升序或降序的数字、相邻相同数字使用两次以上，或与操作人员相关的生日、电话号码等具有一定规律、易被破解的编码。

7.7 安全等级为2、3、4的I&HAS，操作人员的用户名和操作密码组合应不同。

8 电磁兼容性要求

I&HAS的所有部件都应适用于相应环境和应用条件的电磁兼容性要求，并符合GB/T 30148—2013的相关规定。

9 可靠性要求

9.1 操作可靠性

9.1.1 通用要求

应提供I&HAS的正确操作方法，以避免操作人员的误操作。

9.1.2 部件要求

I&HAS功能操作部件的标记应明确、清晰无误，排列应整齐，以减少误操作。不同权限类别的用户具有不同的操作功能。

9.2 功能可靠性

I&HAS部件应满足相关标准要求。I&HAS的设计和配置应确保I&HAS功能满足本标准的要求，要达到系统功能要求应通过以下实现：

a) 明确的设计和安装说明书；
b) 明确的调试和维护说明书；
c) 合适的产品；
d) 定期维护；
e) 高信噪比的设计；
f) 设计优良的软件；
g) 部件工作在设计范围内(如电压，温度)；
h) 功能可测(由用户，安装人员操作)；
i) 功能监测，如看门狗电路。

9.3 系统可靠性

9.3.1 I&HAS应满足GB 50348等现行国家标准的相关要求。

9.3.2 I&HAS所使用的设备，在正常工作条件下其平均无故障间隔时间(MTBF)不应小于5 000 h。

9.3.3 周界入侵探测器在正常工作条件下平均无故障工作时间(MTTF)应能达到(6×10^4)h。

9.3.4 I&HAS验收后的首次故障时间应大于3个月。

10 环境适应性要求

10.1 环境类别

10.1.1 一般要求

I&HAS各部件暴露在10.1.2～10.1.5规定的环境类别之一时，应能够正常运行。类别Ⅰ、类别Ⅱ、类别Ⅲ和类别Ⅳ的严酷程度依次增加，适用于类别Ⅳ环境的部件可用于类别Ⅲ的环境中。

10.1.2 环境类别Ⅰ

能够良好保持温度的室内环境(如在住宅或商业楼内)。

注：温度可在+5 ℃～+40 ℃之间变化，平均相对湿度约为75%，无凝结。

10.1.3 环境类别Ⅱ

无法良好保持温度的室内环境(如走廊、大厅、楼梯、可能产生冷凝的窗户和无供热的存放区或间歇性供暖的仓库等)。

注：温度可在－10 ℃～＋40 ℃之间变化，平均相对湿度约为75%，无凝结。

10.1.4 环境类别Ⅲ

I&HAS部件未完全暴露于室外(有遮蔽)或室内极端环境状态下经历的环境变化。

注：温度可在－25 ℃～＋50 ℃之间变化，平均相对湿度约为75%，无凝结。每年有30 d，相对湿度在85%～95%之间变化，无冷凝。

10.1.5 环境类别Ⅳ

当I&HAS部件完全暴露于露天环境下，环境因素受室外环境变化影响。

注1：温度可在－25 ℃～＋60 ℃之间变化，平均相对湿度约为75%，无凝结。每年有30 d，相对湿度在85%～95%之间变化，无凝结。

注2：对于东北、西北、西南的部分特殊地区(是指气候条件、电气接地条件经常性地有别于注1的要求)，应按下列条件：温度可在－40 ℃～＋60 ℃之间变化，平均相对湿度约为75%，无凝结。每年有30 d，相对湿度在85%～95%之间变化，无凝结。

10.2 适应性要求

10.2.1 I&HAS的所有部件都应适用于相应环境和应用条件。

10.2.2 I&HAS部件的环境试验方法应满足GB/T 15211—2013的要求。

10.2.3 在有腐蚀性气体和易燃易爆环境中工作的入侵报警系统设备，应有相应的保护措施。

10.2.4 室外设备的外壳防护等级应不低于GB 4208—2008规定的IP52。

10.2.5 地埋设备的外壳防护等级应不低于GB 4208—2008规定的IP65。

10.2.6 高压脉冲电子类周界产品还应满足国家或行业的相关要求。

11 标志

11.1 I&HAS所使用设备应该在其上清晰而耐久地标出下列资料：

a) 制造商和/或供应商的名称；

b) 类型；

c) 生产日期或批次号或序列号；

d) 供电额定值，例如标称电压、电流和频率；

e) 申明部件应满足的标准；

f) 标明部件的强制性认证标识；

g) 安全等级；

h) 环境类别。

11.2 端子和引线应该加以编号，加上颜色或者用别的办法来识别。

11.3 标记应耐久和易读，标牌不应被容易取下且不卷曲。

11.4 对于脉冲电网应配置警示标识，同时还应满足现行国家标准规范的相关要求。

12 文件提供

12.1 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。

12.2 系统文件

12.2.1 与I&HAS有关的文件应简洁、完整、明确。应提供足够的信息，用于I&HAS的安装、运行、操作和维护。

12.2.2 I&HAS操作指南(说明书)应将错误操作的可能性降到最低，且其结构设计编排应反映用户的权限级别权限类别。

12.3 部件文件

12.3.1 与I&HAS部件有关的文件应简洁、完整、明确。文件应确保对I&HAS部件进行正确安装、操作和维护。应提供足够的信息以确保每个部件和其他I&HAS部件的集成。

12.3.2 部件文件应包括以下内容：

a) 制造商或供应商的名称；
b) 设备描述；
c) 申明部件应满足的标准；
d) 认证机构的名称(如被认证)或标记；
e) 安全等级；
f) 环境类别。

附 录 A
（资料性附录）
报警传输系统性能条件

A.1 安全类别

报警传输系统的安全类别可以定义为5个参数的组合：

——D，传输时间-分类；

——T，报告时间；

——M，传输时间-最大值；

——S，替换安全性；

——I，信息安全性。

这些参数的值由表A.1、表A.2、表A.3以及A.2中的内容定义。

表 A.1 传输时间分类

类别	D0 s	D1 s	D2 s	D3 s	D4 s
所有传输的平均数计算	—	120	60	20	10
所有传输超过95%以上的部分	240	240	80	30	15

表 A.2 传输时间-最大值

类别	M0 s	M1 s	M2 s	M3 s	M4 s
可接受的最长传输时间	—	480	120	60	20

表 A.3 报告时间分类

类别/周期	报告时间					
类别	T1 d	T2 h	T3 m	T4 s	T5 s	T6 s
最大周期	32	25	300	180	90	20

A.2 信号安全

A.2.1 报警传输系统应提供措施，以防止或探测下列任一阻断或替换方式，对报警信息或其他信息在I&HAS及其相关报警接收中心之间的传输进行有意干扰。

表A.4规定了ATS性能要求。

表 A.4 报警传输系统性能标准

性能标准	传输时间分类	传输时间最大值	报告时间分类	替换安全性	信息安全性
ATS 1	D1	M1	T2	S0	I0
ATS 2	D2	M2	T2	S0	I0
ATS 3	D2	M2	T2	S1	I1
ATS 4	D2	M2	T3	S1	I2
ATS 5	D3	M3	T4	S2	I3
ATS 6	D4	M4	T6	S2	I3

A.2.2 替换安全，应以以下任一方式，防止未经授权的类似设备沿着传输路径对报警系统收发器进行替换：

——S0，无措施；

——S1，通过在报警信号传输路径上传输的所有信息中加入认证码或地址码，对防护区域收发器的替换进行探测；

——S2，通过以下方式对防护区域收发器的替换进行探测：

a) 通过对报警信号传输路径上传输的所有信息中的认证码或地址码加密；

b) 通过为每个连接的收发器添加不同的秘密代码以对防护区域收发器进行验证；

c) 制造商指定的其他措施。

验证始终需要足够的密钥以便为每个相连的接发器提供唯一代码。S2 的标识范围应不能少于 250 个独有的地址。

A.2.3 信息安全，应提供以下任一方式以保护报警传输系统传输的信息：

——I0，无措施；

——I1，防止擅自读取发送信息的措施；

注 1：此项可通过加密完成。

——I2，防止擅自修改发送信息的措施；

注 2：此项可通过加密或密码识别方法完成。

——I3，防止擅自读取和修改发送信息的措施。

A.2.4 加密算法应如下：

——对同步报警传输系统，数据模式在 10 000 000 连续位比特得有重复的任何连续的 100 比特；

——对非同步系统，数据模式在 1 000 000 连续比特不得有重复的任何连续的 100 位元。

附 录 B
（资料性附录）
基于 IP 网络的报警传输系统性能条件

B.1 IP 报警传输系统的安全类别

——IP，报警传输系统的安全类别可以定义为 6 参数的组合；
——D，传输时间-分类；
——M，传输时间-最大值；
——T，报告时间；
——H，攻击安全性；
——S，替换安全性；
——I，信息安全性。
这些参数的值由表 B.1、表 B.2、表 B.3 以及 B.2 中的内容定义。

表 B.1 传输时间分类

类别	D0 s	D1 s	D2 s	D3 s	D4 s
所有传输的平均数计算	—	12	8	4	2
所有传输超过 95%以上的部分	24	24	16	8	3

表 B.2 传输时间-最大值

类别	M0 s	M1 s	M2 s	M3 s	M4 s
可接受的最长传输时间	—	48	12	6	4

表 B.3 报告时间分类

类别/周期	报告时间					
类别	T1 d	T2 h	T3 m	T4 s	T5 s	T6 s
最大周期	1	12	30	180	90	4

B.2 信号安全

B.2.1 报警传输系统应提供措施，以防止或探测下列任一阻断或替换方式，对报警信息或其他信息在 I&HAS 及其相关报警接收中心之间的传输进行有意干扰。

表 B.4 规定了 ATS 性能要求。

表 B.4 报警传输系统性能标准

性能标准	传输时间分类	传输时间最大值	报告时间分类	攻击安全性	替换安全性	信息安全性
ATS 1	D1	M1	T2	H0	S0	I0
ATS 2	D2	M2	T2	H0	S0	I0
ATS 3	D2	M2	T2	H1	S1	I1
ATS 4	D2	M2	T3	H1	S1	I2
ATS 5	D3	M3	T4	H2	S2	I3
ATS 6	D4	M4	T6	H2	S2	I3

B.2.2 攻击安全，应以以下一种方式，防止未经授权的设备进行攻击：

——H0，无措施；

——H1，通过在报警信号传输途径上添加防火墙的措施，防止攻击；

——H2，通过以下方式进行防攻击的保护：

a) 身份认证；

b) 数据加密；

c) 采用 VPN 隧道网络和专用 AAA 认证。

B.2.3 替换安全，应以以下任一方式，防止未经授权的类似设备沿着传输路径对报警系统收发器进行替换：

——S0，无措施；

——S1，通过在报警信号传输路径上传输的所有信息中加入认证码或地址码，对防护区域收发器的替换进行探测；

——S2，通过以下方式对防护区域收发器的替换进行探测：

a) 通过对报警信号传输路径上传输的所有信息中的认证码或地址码加密；

b) 通过为每个连接的收发器添加不同的秘密代码以对防护区域收发器进行验证；

c) 制造商指定的其他措施。

验证始终需要足够的密钥以便为每个相连的接发器提供唯一代码。S2 的标识范围应不能少于 2^8 个独有的地址。

B.2.4 信息安全，应提供以下任一方式以保护报警传输系统传输的信息：

——I0，无措施；

——I1，防止擅自读取发送信息的措施；

注 1：此项可通过加密完成。

——I2，防止擅自修改发送信息的措施；

注 2：此项可通过加密或密码识别方法完成。

——I3，防止擅自读取和修改发送信息的措施。

B.2.5 加密算法应如下：

——对同步报警传输系统，数据模式在 10 000 000 连续位比特得有重复的任何连续的 100 比特；

——对非同步系统，数据模式在 1 000 000 连续比特不得有重复的任何连续的 100 位元。

中 华 人 民 共 和 国
国 家 标 准
入侵和紧急报警系统技术要求
GB/T 32581—2016
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.5 字数 63 千字
2016年6月第一版 2016年6月第一次印刷
*
书号:155066·1-53849 定价 36.00 元

GB/T 32581-2016

打印日期:2016年8月16日 F009B