

安全技术防范系统

智能系统工程师培训讲义

编制：杨守权

ysq1937@gmail.com

兰州 2010.5

安全防范概述

1. 安全防范及安全防范系统定义（GB50384-2004）

（现代汉语词典）安全-没有危险、不受侵害、不出事故

防范-防备、戒备

安全是目的，防范是手段

安全防范系统SPS(Security and Protection System): 以维护社会公共安全为目的，运用安全防范产品和其它相关产品所构成的入侵报警系统(Intruder Alarm System)、视频安防监控系统(Video Surveillance and Control System)、出入口控制系统(Access Control System)、防爆安全检查系统 (Security Inspection System for Anti-Explosion) 等；或由这些系统为子系统组合或集成的电子系统或网络。

2. 安全防范的基本手段和基本要素

■ **三种基本手段**：**PPT**人力防范；实体（物理）防范（门窗柜锁）；技术防范。

■ **三种基本要素**：**DDR**探测Detection；延迟Delay；反应Response。

3. 安全防范技术的专业体系与安全防范行业的标准体系

■ **专业体系**：**PEB**物理防范技术（实体防范）、电子防范技术、生物防范技术

①实体②防爆查毒③入侵探测防盗④视频探测⑤出入口（门禁、生物识别、可视对讲）⑥信息传输、控制、显示、存储⑦移动目标反劫防盗⑧智能建筑社区安防⑨系统集成社会救助应急报警⑩安防工程设计、施工与系统检测技术

■ **标准体系**：基础标准、专业标准、门类标准、产品（工程、服务）标准

PPT Personnel、Physical、Technical/Protection

PEB Physical、Electric-Electronic、Biometric/protection

■ 三种基本手段PPT：人力防范；实体（物理）防范（门窗柜锁）；技术防范。

人力防范：人身传感器（眼耳鼻）探测，反应（声音、恐吓、设障、武器还击、求援）

实体（物理）防范（**物防**）：推迟危险发生，为反应提供足够的时间，增加探测和反应的功能

技术防范：人防和物防的延伸和加强

■ 三种基本要素 DDR：探测 Detection；延迟 Delay；反应 Response。

- **探测 (Detection)**

是指感知显形和隐性风险事件发生并发出报警的**手段**; **Way**

- **延迟 (Delay)**

是指延长和推延风险事件发生进程的**措施**;
Method

- **反应 (Response) **Action****

为制止风险事件的发生所采取的快速**行动**。

- **DDR**探测、延迟和反应三个基本要素**WMA**之间是相互联系、缺一不可的关系。
- 探测要准确无误、延迟时间长短要合适，反应要迅速；
- 反应的总时间应小于（至多等于）探测加延迟的总时间。

$$T_{\text{反 应}} \leq T_{\text{探 测}} + T_{\text{延 迟}}$$

安全技术防范系统标准体系

基于民用建筑中高风险对象不多及高风险对象的安防工程国家已另有规范的事实，仅对通用型公共建筑安全技术防范系统做出规定。即应符合国家现行标准《安全防范工程技术规范》**GB 50348** 和《入侵报警系统工程设计规范》**GB 50394**、《视频安防监控系统工程设计规范》**GB 50395**、《出入口控制系统工程设计规范》**GB 50396**的相关规定。公安部《联网型可视对讲系统技术要求》**GA/T 678-2007** 现已正式实施。为目前唯一的联网型可视对讲的行业标准。

Safety与Security

- **Safety**指自然属性的安全，**Life Safety**即指火灾报警系统；防火、防目标被非人为因素伤害、破坏是“**Safety**”涉及的问题
- **Security**是指社会人文性的安全，即有明显人为属性的安全：**Securities** 证卷。以防入侵、防盗窃、防抢劫、防破坏、防爆炸等为目的的安全技术防范系统主要针对的是“**Security**”；
- 系统的设计，应充分考虑“安全”因素，当同时出现这两种安全问题时，在大多数情况下应优先解决“**Safety**”问题。这是设计系统与产品的基本原则。

安全防范系统是指用于安全防范目的，将具有防入侵、防盗窃、防抢劫、防破坏、防爆炸功能的专用设备、软件有效的组合成一个有机的整体，构造成一个具有探测、延迟、反应综合功能的信息技术网络，简称安防系统。

其目的是维护社会公共安全和预防灾害事故，基本特征是具有高安全性、高可靠性和高性价比。

安全技术防范系统不等同于安全防范系统，它只涵盖安全防范（人力防范、实体防范和技术防范）中的技术防范；它也不不同于一般的电子系统工程，它要求必须安全、可靠，设计时不能盲目追求先进、时髦，而应采用经实践证明是先进、稳定、成熟的产品和技术。

■ 高安全性（safety/security）

安防产品或系统是用来保护人员和财产安全的，首先产品自身必须安全，高安全性一方面是指产品和系统的自然属性方面的运行安全和操作者的安全，例如：防高温、低温、烟雾、电磁干扰、防火、防雷击等等。另一方面，安防产品或系统还应具有防人为破坏的功能，具有防拆报警，防短路、开路、防病毒软件（360安全卫士防木马程序）等等。

安防系统7个子系统

安全技术防范系统宜由SMS(Security Management System)安全管理系统和若干个相关子系统组成。相关子系统宜包括入侵报警系统、视频安防监控系统、出入口控制系统、电子巡查系统、停车库（场）管理系统、防爆安全检查系统等（GB50348-2004）。

安防系统7个子系统内在关系

- 最高层——安全管理系统
- 最重要——入侵报警系统
- 最直观——视频监控系统
- 最有效——出入口控制系统
- 最简单——电子巡查系统
- 最复杂——停车库（场）管理系统
- 最关键——防爆安全检查系统

安防系统设计7个化

GB 50348-2004 3.1.2

- 结构化
- 规范化
- 模块化
- 集成化
- 数字化
- 网络化
- 智能化

安防系统工程7个设计原则

GB 50348-2004

3.1.4

1. 风险等级**Level of Risk**（存在于防护对象本身及其周围的、对其构成安全威胁的程度，由建筑物的使用功能、性质、安全防范管理要求及建设标准决定）与系统防护级别**Level of Protection**（为保障防护对象的安全是采取的防范措施的水平，由投资规模决定）的**一致性**。
2. **PPE**结合性（人防、物防、技防）和**DDR****协调性**。
3. 防护纵深性、均衡性、**抗易损性**。
4. **安全性**、电磁兼容性（**EMC** Electric Magnetic Compatibility）。
5. **可靠性****MTBF**、可维修性**MTTR**、维护保障性。
6. **先进性**、兼容性、可扩展性。
7. **经济性**、实用性。

安防系统7类联动 (Interlock)

GB 50348-2004

3.3.3

1. 入侵报警 联动 声光报警设备
2. 入侵报警 联动 摄像机图像
3. 视频安防 联动 声光报警
4. 电子巡查 联动 声光报警
5. 出入口控制 联动 声光报警
6. 出入口控制 联动 摄像机图像
7. 火灾报警 联动 出入口控制

安全管理系统平台7个功能 (SMS)

GB 50348-2004

3.4.1

1. 多媒体平台：中央站视频流/音频流/数据流
2. 中文简体界面，操作无死机
3. 集中监视/分散控制；中央站不影响分站工作独立进行
4. 系统状态显示（声光/文字/图形）：系统自检；出入口人员通行情况（姓名、时间、地点、行为）；设防/撤防区域；报警；故障。
5. 系统控制：图像切换/处理/存贮/检索/回放；云台/镜头预置遥控；设防/撤防；执行机构及其它设备控制
6. 处警预案：入侵部位/图像/声音；对策显示；处警预案
7. 事件记录/查询；生成报表

GB 50348-2004

安全防范工程技术规范

一、内容简介

本章是《规范》中所用到的基本术语, 共有33条, 无强制性条款。

二、条文、条文说明及解释

2.0.1 2.0.2

【解释说明】

【条文】2.0.1 安全防范产品 security & protection products

用于防入侵、防盗窃、防抢劫、防破坏、防爆安全检查等领域的特种器材或设备。

【条文】2.0.2 安全防范系统 (SPS) security & protection system

2.0.2 2.0.3

以维护社会公共安全为目的，运用安全防范产品和其它相关产品所构成的入侵报警系统、视频安防监控系统、出入口控制系统、防爆安全检查系统等；或由这些系统为子系统组合或集成的电子系统或网络。

【条文】2.0.3 安全防范（系统）工程（ESPS）
engineering of security & protection system

以维护社会公共安全为目的，综合运用安全防范技术和其他科学技术，为建立具有防入侵、防盗窃、防抢劫、防破坏、防爆安全检查等功能（或其组合）的系统而实施的工程。通常也称为技防工程。

2.0.4 2.0.5

【条文】2.0.4 入侵报警系统(IAS) intruder 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。

【条文】2.0.5 视频安防监控系统(VSCS) video surveillance & control system

利用视频技术探测、监视设防区域并实时显示、记录现场图像的电子系统或网络。

2.0.5 2.0.6 2.0.7

【条文说明】2.0.5 本规范所指的视频安防监控系统，不同于一般的工业电视或民用闭路电视（CCTV）系统。它是特指用于安全防范的目的，通过对监视区域进行视频探测、视频监视、控制、图像显示、记录和回放的视频信息系统或网络。

【条文】2.0.6 出入口控制系统（ACS）
access
control system

利用自定义符识别或/和模式识别技术对出入口目标进行识别并控制出入口执行机构启闭的电子系统或网络。

【条文】2.0.7 电子巡查系统 guard tour system

2.0.7 2.0.8

对保安巡查人员的巡查路线、方式及过程进行管理和控制的电子系统。

【条文说明】2.0.7 在安防技术界和智能建筑界，通常将该系统称为“巡更系统”。“巡更”是一个古老而传统的用语，随着社会文明的进步，应赋予其新的内容。根据该系统的本质特征，本规范将其称为“电子巡查系统”。

【条文】2.0.8 停车库（场）管理系统 parking
lots management system

对进、出停车库（场）的车辆进行自动登录、监控和管理的电子系统或网络。

2.0.8 2.0.9

【条文说明】2.0.8 将停车库（场）管理系统作为安全防范系统的一个子系统，是安防技术界和智能建筑界在多年实践中达成的一种共识。“车辆”作为移动目标的一个代表，其安全防范工作已纳入“技术防范”的对象之中。这样做有利于社会治安的稳定和公民人身财产的安全。

【条文】2.0.9 防爆安全检查系统 security
inspection system for anti-explosion

检查有关人员、行李、货物是否携带爆炸物、武器和/或其他违禁品的电子设备系统或网络。

2.0.10

【条文】 2.0.10 安全管理系统 (SMS) security management system

对入侵报警、视频安防监控、出入口控制等子系统进行组合或集成, 实现对各子系统的有效联动、管理和/或监控的电子系统。

【条文说明】 2.0.10 在建筑智能化系统中, 综合管理系统习惯上称为IBMS, 其中的安全防范系统的管理系统, 通常称为SMS (security management system)。这里的安全管理系统也可称为综合报警安全管理系统 (generic security management system), 它是指在安全防范系统中, 对其各子系统进行管理和控制的集成系统 (包括硬件和软件), 它除提供报警信息服务外, 还可利用网络的信息资助提供其它的综合信息服务 (如物业管理、社区医疗、网上购物等) 平台。

2.0.11 2.0.12 2.0.13

【条文】2.0.11 风险等级 level of risk

存在于防护对象本身及其周围的、对其构成安全威胁的程度。

【条文】2.0.12 防护级别 level of protection
为保障防护对象的安全所采取的防范措施的水平。

【条文】2.0.13 安全防护水平 level of security
风险等级被防护级别所覆盖的程度。

【条文说明】2.0.13 安全防护水平，是一个定性概念。需要在系统运行一定时期后（例如一年、两年），对其防范效果做出综合评价。由于它所涉及的因素较多（包括人防、物防、技防及其它方面），需要建立一个比较科学、比较完备的评价体系。

2.0.14 2.0.15 2.0.16 2.0.17

【条文】2.0.14 探测 detection

感知显性风险事件或/和隐性风险事件发生并发出报警的手段。

【条文】2.0.15 延迟 delay

延长或/和推迟风险事件发生进程的措施。

【条文】2.0.16 反应 response

为制止风险事件的发生所采取的快速行动。

【条文】2.0.17 误报警 false alarm

2.0.17 2.0.18 2.0.19

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。

【条文】2.0.18 漏报警 leakage alarm

风险事件已经发生，而系统未能做出报警响应或指示。

【条文】2.0.19 人力防范（人防） personnel protection

执行安全防范任务的具有相应素质人员和/或人员群体的一种有组织的防范行为（包括人、组织和管理等）。

2.0.19 2.0.20

【条文说明】2.0.19 人力防范(人防)是安全防范的基础。传统的“人防”是指在安全防范工作中人的自然能力的展现。即：利用人体感官进行探测并做出反应，通过人体体能的发挥推迟和制止风险事件发生。现代的“人防”是指执行安全防范任务的具有相应素质的人员和/或人员群体的一种有组织的防范行为，包括高素质人员的培养、先进自卫设备的配置、以及人员的组织与管理等。因此，本规范所称的“人防”与“人民防空工程”所说的“人防”不是一个概念。

【条文】2.0.20 实体防范(物防)physical protection
用于安全防范目的、能延迟风险事件发生的各种实体防护手段（包括建（构）筑物、屏障、器具、设备、系统等）。

2.0.21 2.0.22

【条文】2.0.21 技术防范（技防）technical protection

利用各种电子信息设备组成系统和/或网络以提高探测、延迟、反应能力和防护功能的安全防范手段。

【条文】2.0.22 防护对象（单位、部位、目标）protection object

由于面临风险而需对其进行保护的對象，通常包括某个单位、某个建（构）筑物或建（构）筑物群，或其内外的某个局部范围以及某个具体的实际目标。

2.0.23 2.0.24 2.0.25 2.0.26

【条文】2.0.23 周界 perimeter

需要进行实体防护或/和电子防护的某区域的边界。

【条文】2.0.24 监视区 surveillance area

实体周界防护系统或/和电子周界防护系统所组成的周界警戒线与防护区边界之间的区域。

【条文】2.0.25 防护区 protection area

允许公众出入的、防护目标所在的区域或部位。

【条文】2.0.26 禁区 restricted area

不允许未授权人员出入（或窥视）的防护区域或部位。

2.0.27 2.0.28 2.0.29

【条文】2.0.27 盲区 blind zone

在警戒范围内，安全防范手段未能覆盖的区域。

【条文】2.0.28 纵深防护 longitudinal-depth protection

根据被防护对象所处的环境条件和安全管理的要求，对整个防范区域实施由外到里或由里到外层层设防的防护措施。纵深防护分为整体纵深防护和局部纵深防护两种类型。

【条文】2.0.29 均衡防护 balanced protection

2.0.29 2.0.30

安全防范系统各部分的安全防护水平基本一致，无明显薄弱环节或“瓶颈”。

【条文】2.0.30 抗易损防护 anti-damageable protection

保证安全防范系统安全、可靠、持久运行并便于维修和维护的技术措施。

【条文说明】2.0.30 抗易损防护，即防护的抗易损性。它是系统及其所用设备的可靠性、安全性、耐久性和抗破坏性等的综合体现。本规范将其作为系统设计的一项原则提出，意在提醒设计人员进行系统设计和设备选型时，要注意抗易损防护。

2.0.31 2.0.32

【条文】2.0.31 纵深防护体系 longitudinal-depth protection systems

兼有周界、监视区、防护区和禁区的防护体系。

【条文】2.0.32 监控中心 surveillance & control centre;

安全防范系统的中央控制室。安全管理系统在此接收、处理各子系统发来的报警信息、状态信息等，并将处理后的报警信息、监控指令分别发往报警接收中心和相关子系统。

2.0.33

【条文】 2.0.33 报警接收中心 alarm receiving centre

接收一个或多个监控中心的报警信息并处理警情的处所。通常也称为接处警中心(如公安机关的接警中心)。

【条文说明】 2.0.32、2.0.33 监控中心、报警接收中心

在社会公众看来，凡是能够接收报警信息并做出某种反应的“机构”都可称为报警接收中心。但在法律层面上，只有公安机关接警中心才具有法定的接处警执法功能。本规范根据我国国情，将不具有执法职能的各类“接处警机构”，一律称为“监控中心”（可能有多级）；而将公安机关这样的接警中心，定义为报警接收中心或接处警中心。

3.1.1 3.1.2 3.1.3

【条文】3.1.1 安全防范工程的设计应根据被防护对象的使用功能、建设投资及安全防范管理工作的要求，综合运用安全防范技术、电子信息技术、计算机网络技术等，构成先进、可靠、经济、适用、配套的安全防范应用系统。

【条文】3.1.2 安全防范工程的设计应以结构化、规范化、模块化、集成化的方式实现，应能适应系统维护和技术发展的需要。

【条文】3.1.3 安全防范系统的配置应采用先进而成熟的技术、可靠而适用的设备。

3.1.3 3.1.4

【条文说明】3.1.3 由于通信技术、电子信息技术和计算机网络技术的发展十分迅速，经常会推出一些新产品（包括硬件、软件）和新技术，而安全防范系统设备不同于一般的家用电器和信息设备，它必须安全、可靠。因此，安全防范系统的设计不能盲目追求先进、时髦，而应采用那些经过实践考验证明是先进而成熟的技术，经过严格的质量检验或认证，证明是性能可靠且性能价格比较高的产品或设备，以保证安全防范系统全天候、24小时的正常运行。

【条文】3.1.4 安全防范系统中使用的设备必须符合国家法规和现行相关标准的要求，并经检验或认证合格。

3.1.4 3.1.5

【条文说明】3.1.4 我国加入WTO以后，国家对符合WTO/TBT五项正当目标的产品推行强制性认证制度，大多数安防产品列在其中。因此，本规范规定，安全防范系统使用的设备，必须符合国家现行相关标准和法规的要求，属于强制性认证的产品必须经认证机构认证合格，不属于强制性认证的产品也应经相关检验机构检验合格。

【条文】3.1.5 安全防范工程的设计应遵循下列原则：

- 1 系统的防护级别与被防护对象的风险等级相适应。
- 2 技防、物防、人防相结合，探测、延迟、反应相协调。

3.1.5 3.1.6

- 3 满足防护的纵深性、均衡性、抗易损性要求。
- 4 满足系统的安全性、电磁兼容性要求。
- 5 满足系统的可靠性、维修性与维护保障性要求。
- 6 满足系统的先进性、兼容性、可扩展性要求。
- 7 满足系统的经济性、适用性要求。

【条文】3.1.6 安全防范工程程序与要求应符合《安全防范工程程序与要求》GA/T75的有关规定。

3. 1. 6

【条文说明】3. 1. 6 保证安全防范工程的质量，责任重于泰山。安全防范工程具有与一般工程不同的特点和要求，根据20多年来我国安防工程建设的实践，本规范认为执行以下程序对保证工程质量是极为有益的。

1 工程程序

安全防范工程的建设应符合国家法律、法规的规定及《安全防范工程程序与要求》GA/T75的相关要求。基本程序见图3. 1. 5（图中带*号者为重点）。（图3. 1. 6 安全防范工程程序表，请详见《安全防范工程技术规范》标准宣贯培训教材第25页）

3.1.6

2 工程主要环节要求

1) 工程立项与可行性研究。

安全防范工程申请立项前，须进行可行性研究。可行性研究报告经批准后，工程正式立项。可行性研究报告由建设单位（或委托单位）编制。

2) 工程设计任务书的编制。

建设单位根据经批准的可行性研究报告，编制工程设计任务书，并按照“工程招标法”进行工程招标与合同签约。

设计任务书的主要内容应包括：

- 任务来源；
- 政府部门的有关规定和管理要求；
- 应执行的国家现行标准；
- 被防护对象的风险等级与防护级别；

3. 1. 6

- 工程项目的内容和要求(包括设计、施工、调试、检验、验收、培训和维修服务);
- 建设工期;
- 工程投资控制数额;
- 工程建成后应达到的预期效果;
- 工程设计应遵循的原则;
- 系统构成;
- 系统功能要求(含各子系统的功能要求);
- 监控中心要求;
- 建设单位的安全保卫管理制度;
- 接处警反应速度;
- 建筑物平面图。

3.1.6

3) 现场勘察。具体要求见3.2节。

4) 方案论证

工程设计单位应根据工程设计任务书和现场勘察报告进行初步设计。初步设计完成后必须组织方案论证。方案论证由建设单位主持，业务主管部门、行业主管部门、设计单位及一定数量的技术专家参加，对初步设计的各项内容进行审查，对其技术、质量、费用、工期、服务和预期效果做出评价并提出整改措施。整改措施由设计单位和建设单位落实后，方可进行正式设计。

5) 工程检验。具体要求见本规范第7章。

6) 工程验收。具体要求见本规范第8章。

3.3.1

【条文】3.3.1 安全防范系统构成包括下列内容：

1 安全防范系统一般由安全管理系统和若干个相关子系统组成。

2 安全防范系统的结构模式按其规模大小、复杂程度可有多种构建模式。按照系统集成度的高低, 安全防范系统分为集成式、组合式、分散式三种类型。

3 各相关子系统的基本配置, 包括前端、传输、信息处理/控制/管理、显示/记录四大单元。不同（功能）的子系统, 其各单元的具体内容有所不同。

3.3.1

4 现阶段较常用的子系统主要包括：入侵报警系统、视频安防监控系统、出入口控制系统、电子巡查系统、停车库（场）管理系统以及以防爆安全检查系统为代表的特殊子系统等。

【条文说明】3.3.1 安全防范系统的三种组建模式的划分，旨在为设计者提供系统集成设计时三种不同模式的参考。随着信息技术和网络技术的不断发展，安全防范系统的规模、集成深度和广度也在不断变化。“一体化集成”的模式，将会是未来安全防范系统发展的方向。

3.3.2

【条文】3.3.2 安全防范系统中安全管理系统的設計要素包括下列内容：

- 1 集成式安全防范系统的安全管理系统。
 - 1) 安全管理系统应设置在禁区内(监控中心)，应能通过统一的通信平台和管理软件将监控中心设备与各子系统设备联网，实现由监控中心对各子系统的自动化管理与监控。安全管理系统的故障应不影响各子系统的运行；某一子系统的故障应不影响其它子系统的运行。

3.3.2

- 2) 应能对各子系统的运行状态进行监测和控制，应能对系统运行状况和报警信息数据等进行记录和显示。应设置足够容量的数据库。
- 3) 应建立以有线传输为主、无线传输为辅的信息传输系统。应能对信息传输系统进行检验，并能与所有重要部位进行有线和/或无线通信联络。
- 4) 应设置紧急报警装置。应留有向接处警中心联网的通信接口。
- 5) 应留有多个数据输入、输出接口，应能连接各子系统的主机，应能连接上位管理计算机，以实现更大规模的系统集成。

3.3.2

- 2 组合式安全防范系统的安全管理系统。
 - 1) 安全管理系统应设置在禁区内(监控中心)。应能通过统一的管理软件实现监控中心对各子系统的联动管理与控制。安全管理系统的故障应不影响各子系统的运行;某一子系统的故障应不影响其它子系统的运行。
 - 2) 应能对各子系统的运行状态进行监测和控制,应能对系统运行状况和报警信息数据等进行记录和显示。可设置必要的数据库。

3.3.2

- 3) 应能对信息传输系统进行检验, 并能与所有重要部位进行有线和/或无线通信联络。
 - 4) 应设置紧急报警装置。应留有向接处警中心联网的通信接口。
 - 5) 应留有多个数据输入、输出接口, 应能连接各子系统的主机。
- 3 分散式安全防范系统的安全管理系统。
- 1) 相关子系统独立设置, 独立运行。系统主机应设置在禁区内(值班室), 系统应设置联动接口, 以实现与其它子系统的联动。

3.3.2

- 3) 应能对信息传输系统进行检验, 并能与所有重要部位进行有线和/或无线通信联络。
 - 4) 应设置紧急报警装置。应留有向接处警中心联网的通信接口。
 - 5) 应留有多个数据输入、输出接口, 应能连接各子系统的主机。
- 3 分散式安全防范系统的安全管理系统。
- 1) 相关子系统独立设置, 独立运行。系统主机应设置在禁区内(值班室), 系统应设置联动接口, 以实现与其它子系统的联动。

3.3.3

入侵报警系统：系统应能根据被防护对象的使用功能及安全防范管理的要求，对设防区域的非法入侵、盗窃、破坏和抢劫等，进行实时有效的探测与报警。高风险防护对象的入侵报警系统应有报警复核（声音）功能。系统不得有漏报警，误报警率应符合工程合同书的要求。

入侵报警系统的设计应符合《入侵报警系统技术要求》GA/T368等相关标准的要求。

3.3.3

2 视频安防监控系统:系统应能根据建筑物的使用功能及安全防范管理的要求,对必须进行视频安防监控的场所、部位、通道等进行实时、有效的视频探测、视频监视,图像显示、记录与回放,宜具有视频入侵报警功能。与入侵报警系统联合设置的视频安防监控系统,应有图像复核功能,宜有图像复核加声音复核功能。

视频安防监控系统的设计应符合《视频安防监控系统技术要求》GA/T367等相关标准的要求。

3. 3. 3

3 出入口控制系统:系统应能根据建筑物的使用功能和安全防范管理的要求,对需要控制的各类出入口,按各种不同的通行对象及其准入级别,对其进、出实施实时控制与管理,并应具有报警功能。

出入口控制系统的设计应符合《出入口控制系统技术要求》GA/T394等相关标准的要求。

人员安全疏散口,应符合国家现行标准《建筑设计防火规范》GBJ16的要求。

3.3.3

防盗安全门、访客对讲系统、可视对讲系统作为一种民用出入口控制系统，其设计应符合国家现行标准《防盗安全门通用技术条件》GB 17565、《楼寓对讲电控防盗门通用技术条件》GA/T 72、《黑白可视对讲系统》GA/T 269的技术要求。

4 电子巡查系统：系统应根据建筑物的使用功能和安全防范管理的要求，按照预先编制的保安人员巡查程序，通过信息识读者或其他方式对保安人员巡逻的工作状态（是否准时、是否遵守顺序等）进行监督、记录，并能对意外情况及时报警。

3.3.3

5 停车库（场）管理系统：系统应能根据建筑物的使用功能和安全防范管理的需要，对停车库（场）的车辆通行道口实施出入控制、监视、行车信号指示、停车管理及车辆防盗报警等综合管理。

【条文说明】5 停车库（场）管理系统，作为安全防范系统的一个子系统来设计，主要是考虑到智能大厦、智能小区在安全防范管理工作上的需要。因为车辆的安全也是社会公众普遍关注的一个社会热点问题，把车辆存放时的安全问题纳入安全防范系统的设计之中，有利于维护社会治安的稳定。

3.3.3

6 其它子系统:应根据安全防范管理工作对各类建筑物、构筑物的防护要求或对建筑物、构筑物内特殊部位的防护要求,设置其他特殊的安全防范子系统,如防爆安全检查系统、专用的高安全实体防护系统、各类周界防护系统等。这些子系统(设备)均应遵照本规范和相关规范进行设计。

【条文说明】6 安全防范系统的其它子系统,是指根据实际需要,在特定场所或特殊情况下,设立的某些直接或间接用于安全防范目的的防范系统。比如机场、车站、码头,大型集会和活动场所需要设立的防爆安全检查系统、人员识别系统、特殊物品识别系统、应急疏散广播系统等。

安全技术防范系统的设计

- 应根据建筑物的使用功能、性质、安全防范管理要求及建设标准，构成技术先进、安全可靠、经济适用、灵活有效的安全技术防范体系。
 - 系统设计所采用的产品必须是经过国家授权认可的检验机构检测合格的产品。
 - 安全防范工程规模按风险等级或工程投资额划分为三级。
 - 1 一级工程：**一级风险或投资额**100**万元以上的工程。
 - 2 二级工程：**二级风险或投资额超过**30**万元不足**100**万元的工程。
 - 3 三级工程：**三级风险或投资额**30**万元以下的工程。
 - 系统的防护级别应与被保护对象的风险等级相适应，满足整体纵深防护和局部纵深防护的设计要求。
 - 系统设计应以用户提出的安全防范要求为主要依据，有条件时应进行现场进行勘查。
- 一、二级工程必须进行初步设计和方案论证，待相应主管部门批准后，方可进行正式设计。

入侵报警系统

GB50394-2007

入侵报警系统工程设计规范

2术语

2.0.1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非法进入或试图非法进入设防区域(包括主观判断面临被劫持或遭抢劫或其他譬急情况时，故意触发紧急报警装置)的行为、处理报警信息、发出报警信息的电子系统或网络。

2.0.2报警状态alarm condition系统因探测到风险而作出响应并发出报警的状态。

2.0.3故障状态fault condition系统不能按照设计要求进行正常工作的状态。

2.0.4防拆报警tamper alarm.因触发防拆探测装置而导致的报警。

2.0.5防拆装置tamper device用来探测拆卸或打开报警系统的部件、组件或其部分的装置。

2.0.6设防**set condition**使系统的部分或全部防区处于警戒状态的操作。

2.0.7撤防**unset condition**使系统的部分或全部防区处于解除警戒状态的操作。

2.0.8防区**defence area**利用探测器(包括紧急报警装置)对防护对象实施防护,并在控制设备上能明确显示报警部位的区域。

2.0.9周界**perimeter**需要进行实体防护或 / 和电子防护的某区域的边界。

2.0.10监视区**surveillance area**实体周界防护系统或 / 和电子周界防护系统所组成的周界警戒线与防护区边界之间的区域。

2.0.11防护区**protection area**允许公众出入的、防护目标所在的区域或部位。

2.0.12禁区**restricted area**不允许未授权人员出入(或窥视)的防护区域或部位。

2.0.14漏报警leakage alarm入侵行为已经发生，而系统未能做出报警响应或指示。

2.0.15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。

2.0.16报警复核check to alarm利用声音和 / 或图像信息对现场报警的真实性进行核实的手段。

2.0.17紧急报警emergency alarm用户主观判断面临被劫持或遭抢劫或其他危急情况时，故意触发的报警。

2.0.18紧急报警装置emergency alarm switch用于紧急情况下，由人工故意触发报警信号的开关装置。

2.0.19探测器detector对入侵或企图入侵行为进行探测做出响应并产生报警状态的装置。

2.0.20报警控制设备controller在入侵报警系统中，实施设防、撤防、测试、判断、传送报警信息，并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。

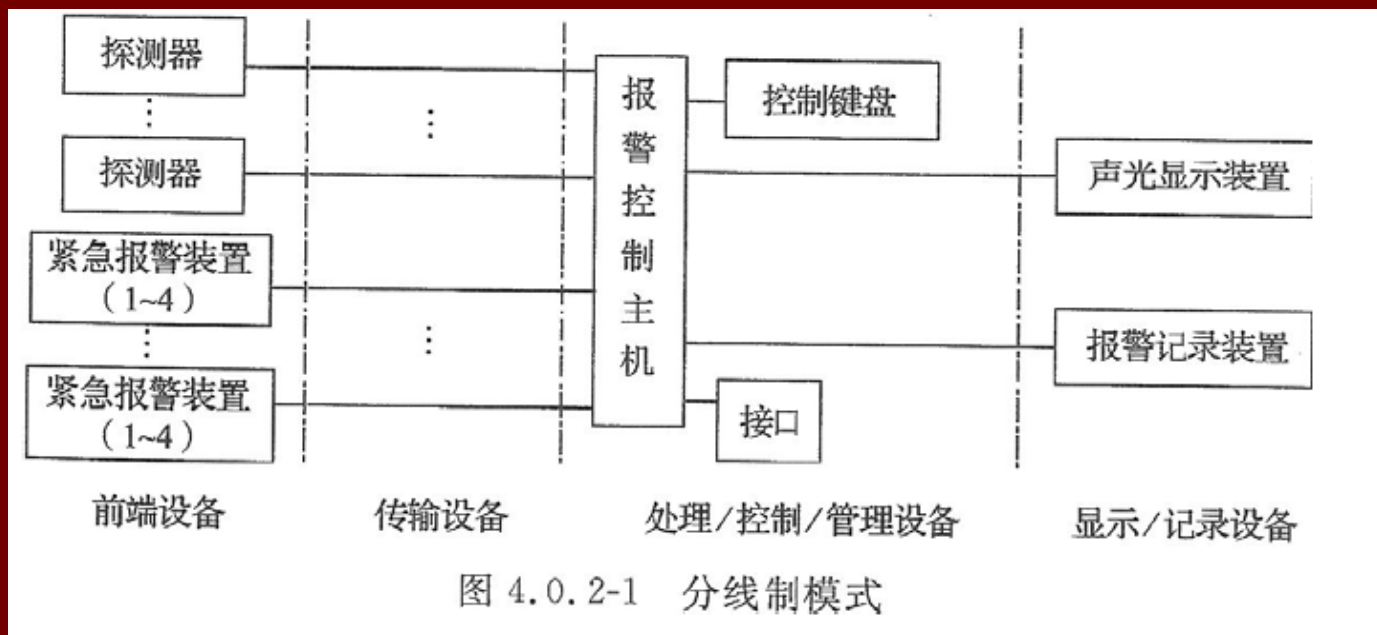
2.0.21报警响应时间response time从探测器(包括紧急报警装置)探测到目标后产生报警状态信息到控制设备接收到该信息并发出报警信号所需的时间。

4系统构成

4.0.1入侵报警系统通常由前端设备(包括探测器和紧急报警装置)、传输设备、处理 / 控制 / 管理设备和显示 / 记录设备四个部分构成。

4.0.2根据信号传输方式的不同，入侵报警系统组建模式宜分为以下模式：

1分线制：探测器、紧急报警装置通过多芯电缆与报警控制主机之间采用一对一专线相连(图4.0.2—1)。



2总线制：探测器、紧急报警装置通过其相应的编址模块与报警控制主机之间采用报警总线(专线)相连(图4.0.2-2)。

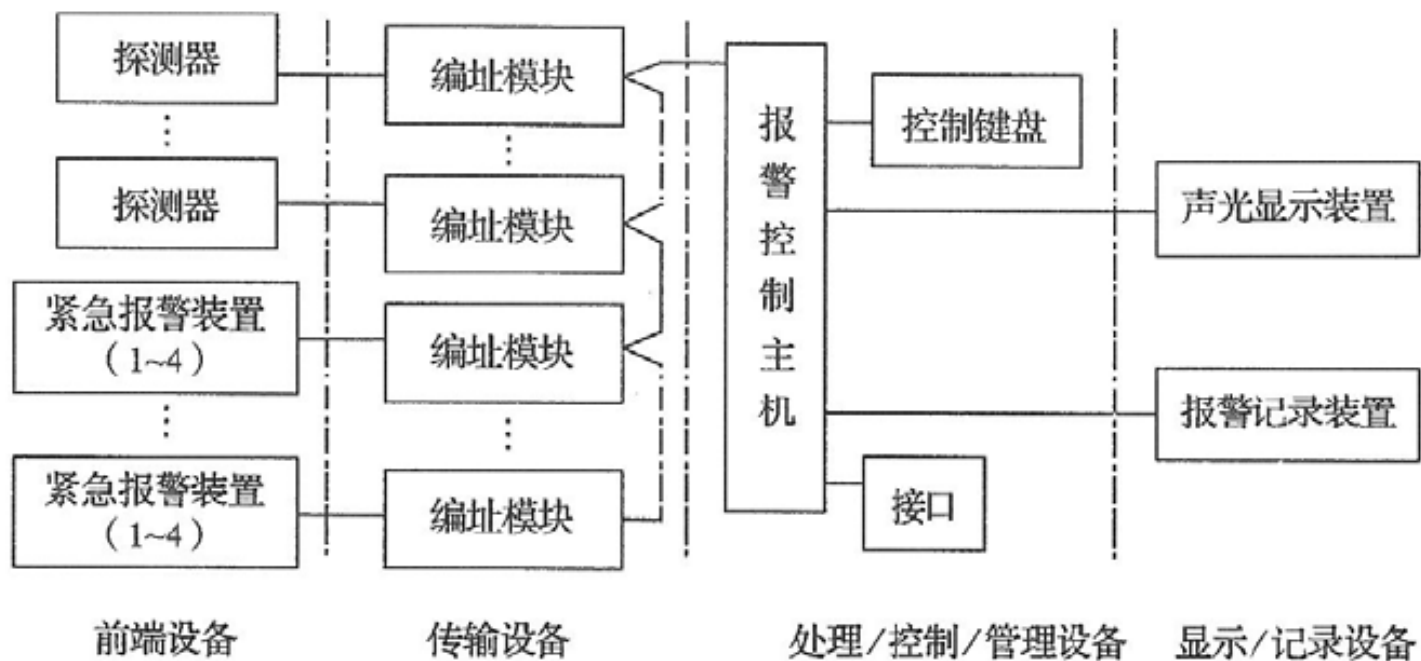


图 4.0.2-2 总线制模式

3无线制：探测器、紧急报警装置通过其相应的无线设备与报警控制主机通讯，其中一个防区内的紧急报警装置不得大于4个(图4.0.2-3)。

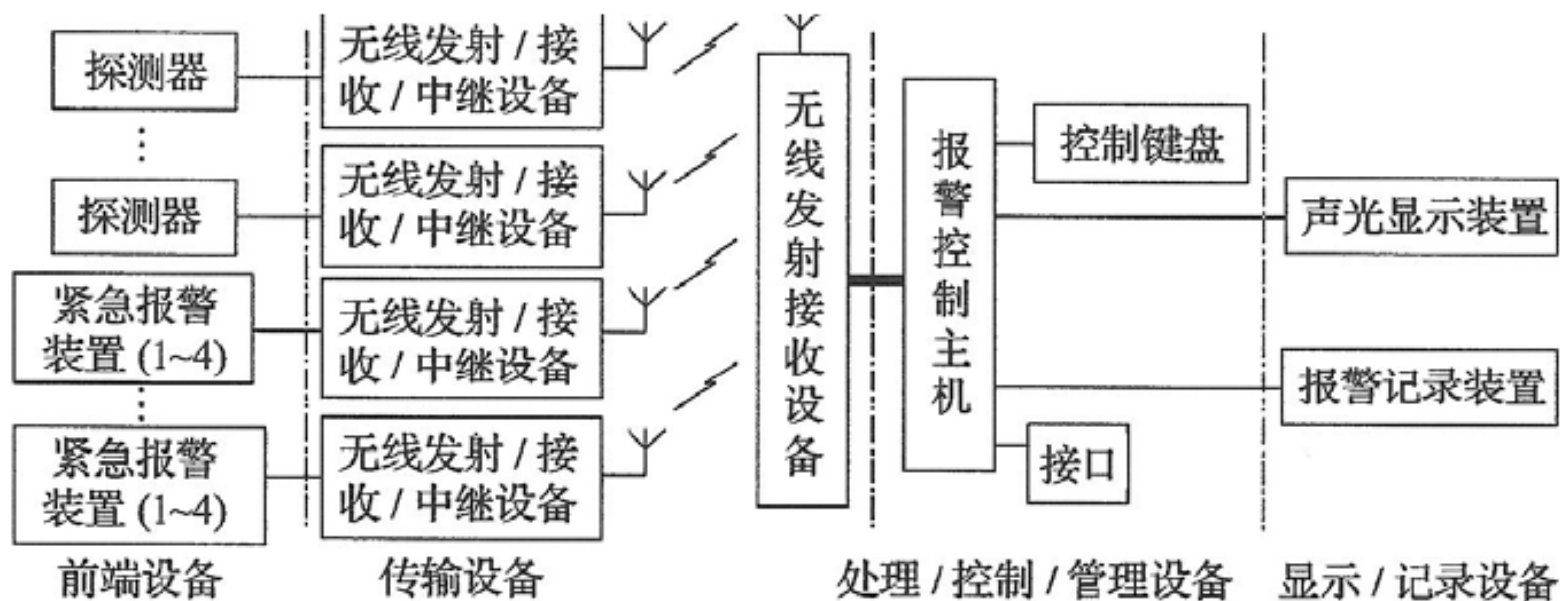


图 4.0.2-3 无线制模式

4公共网络：探测器、紧急报警装置通过现场报警控制设备和 / 或网络传输接入设备与报警控制主机之间采用公共网络相连。公共网络可以有线网络，也可以是有线-无线-有线网络(图4.0.2-4)。

注：以上四种模式可以单独使用，也可以组合使用；可单级使用，也可多级使用。

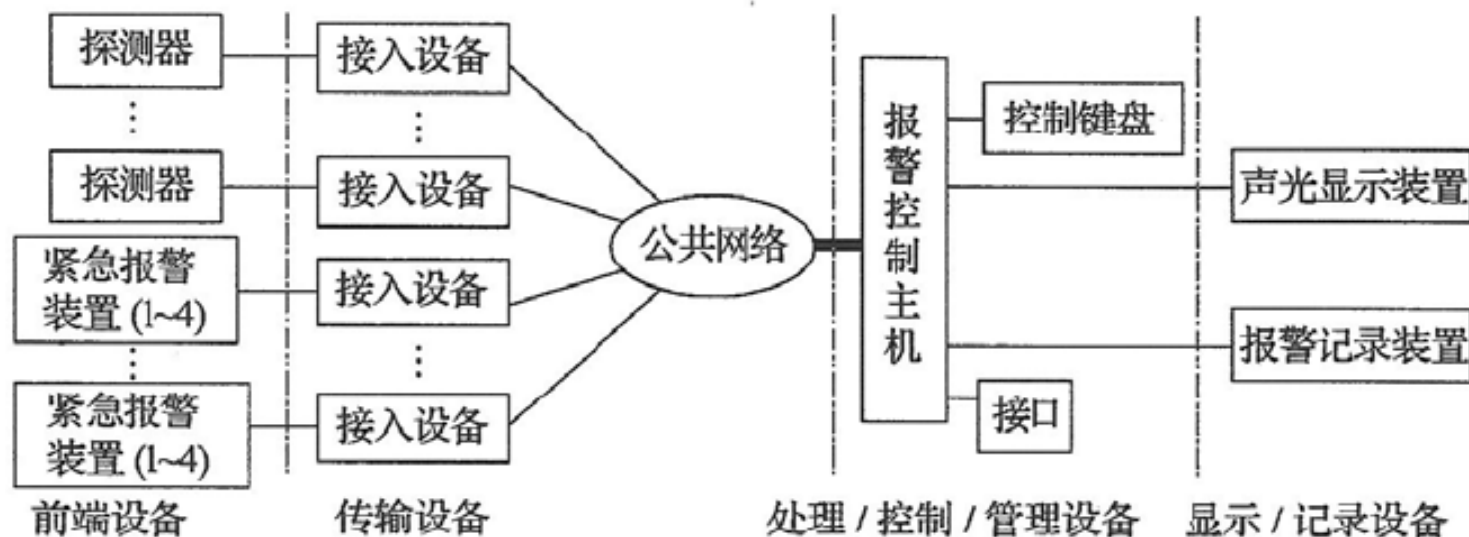


图 4.0.2-4 公共网络模式

5、系统设计

5.1纵深防护体系设计

5.1.1入侵报警系统的设计应符合整体纵深防护和局部纵深防护的要求，纵深防护体系包括周界、监视区、防护区和禁区。

5.1.2周界可根据整体纵深防护和局部纵深防护的要求分为外周界和内周界。周界应构成连续无间断的警戒线(面)。周界防护应采用实体防护或 / 和电子防护措施；采用电子防护时，需设置探测器；当周界有出入口时，应采取相应的防护措施。

5.1.3监视区可设置警戒线(面)，宜设置视频安防监控系统。

5.1.4防护区应设置紧急报警装置、探测器，宜设置声光显示装置，利用探测器和其他防护装置实现多重防护。

5.1.5禁区应设置不同探测原理的探测器，应设置紧急报警装置和声音复核装置，通向禁区的出入口、通道、通风口、天窗等应设置探测器和其他防护装置，实现立体交叉防护。

5.1.6被防护对象的设防部位应符合现行国家标准《安全防范工程技术规范》GB 50348的相关要求。

5.2系统功能性能设计

5.2.1入侵报警系统的误报警率应符合设计任务书和 / 或工程合同书的要求。

5.2.2入侵报警系统不得有漏报警。

5.2.3入侵报警功能设计应符合下列规定：

1紧急报警装置应设置为不可撤防状态，应有防误触发措施，被触发后应自锁。

2当下列任何情况发生时，报警控制设备应发出声、光报警信息，报警信息应能保持到手动复位，报警信号应无丢失：

1)在设防状态下，当探测器探测到有入侵发生或触动紧急报警装置时，报警控制设备应显示出报警发生的区域或地址；

2)在设防状态下，当多路探测器同时报警(含紧急报警装置报警)时，报警控制设备应依次显示出报警发生的区域或地址。

3报警发生后，系统应能手动复位，不应自动复位。

4在撤防状态下，系统不对探测器的报警状态做出响应。

5.2.4防破坏及故障报警功能设计应符合下列规定：

当下列任何情况发生时，报警控制设备上应发出声、光报警信息，报警信息应能保持到手动复位，报警信号应无丢失：

- 1在设防或撤防状态下，当入侵探测器机壳被打开时。
- 2在设防或撤防状态下，当报警控制器机盖被打开时。
- 3在有线传输系统中，当报警信号传输线被断路、短路时。
- 4在有线传输系统中，当探测器电源线被切断时。
- 5当报警控制器主电源 / 备用电源发生故障时。
- 6在利用公共网络传输报警信号的系统中，当网络传输发生故障或信息连续阻塞超过30s时。

5.2.5记录显示功能设计应符合下列规定：

- 1系统应具有报警、故障、被破坏、操作(包括开机、关机、设防、撤防、更改等)等信息的显示记录功能。
- 2系统记录信息应包括事件发生时间、地点、性质等，记录的信息应不能更改。

5.2.6系统应具有自检功能。

5.2.7系统应能手动 / 自动设防 / 撤防，应能按时间在全部及部分区域任意设防和撤防；设防、撤防状态应有明显不同的显示。

5.2.8系统报警响应时间应符合下列规定：

- 1分线制、总线制和无线制入侵报警系统：不大于2s；
- 2基于局域网、电力网和广电网的入侵报警系统：不大于2s。
- 3基于市话网电话线入侵报警系统：不大于20s。

5.2.9系统报警复核功能应符合下列规定：

- 1当报警发生时，系统宜能对报警现场进行声音复核。
- 2重要区域和重要部位应有报警声音复核。

5.2.10无线入侵报警系统的功能设计，除应符合本规范第5.2.1～5.2.9条的要求外，尚应符合下列规定：

- 1当探测器进入报警状态时，发射机应立即发出报警信号，并应具有重复发射报警信号的功能。
- 2控制器的无线收发设备宜具有同时接收处理多路报警信号的功能。
- 3当出现信道连续阻塞或干扰信号超过30s时，监控中心应有故障信号显示。
- 4探测器的无线报警发射机，应有电源欠压本地指示，监控。

6设备选型与设置

6.1探测设备

6.1.1探测器的选型除应符合本规范第3.0.3条的规定外，尚应符合下列规定：

- 1根据防护要求和设防特点选择不同探测原理、不同技术性能的探测器。多技术复合探测器应视为一种技术的探测器。
- 2所选用的探测器应能避免各种可能的干扰，减少误报，杜绝漏报。
- 3探测器的灵敏度、作用距离、覆盖面积应能满足使用要求。

6.1.2周界用入侵探测器的选型应符合下列规定：

- 1规则的外周界可选用主动式红外入侵探测器、遮挡式微波入侵探测器、振动入侵探测器、激光式探测器、光纤式周界探测器、振动电缆探测器、泄漏电缆探测器、电场感应式探测器、高压电子脉冲式探测器等。
- 2不规则的外周界可选用振动入侵探测器、室外用被动红外探测器、室外用双技术探测器、光纤式周界探测器、振动电缆探测器、泄漏电缆探测器、电场感应式探测器、高压电子脉冲式探测器等。
- 3无围墙 / 栏的外周界可选用主动式红外入侵探测器、遮挡式微波入侵探测器、激光式探测器、泄漏电缆探测器、电场感应式探测器、高压电子脉冲式探测器等。
- 4内周界可选用室内用超声波多普勒探测器、被动红外探测器、振动入侵探测器、室内用被动式玻璃破碎探测器、声控振动双技术玻璃破碎探测器等。

6.1.3出入口部位用入侵探测器的选型应符合下列规定:

1外周界出入口可选用主动式红外入侵探测器、遮挡式微波入侵探测器、激光式探测器、泄漏电缆探测器等。

2建筑物内对人员、车辆等有通行时间界定的正常出入口(如大厅、车库出入口等)可选用室内用多普勒微波探测器、室内用被动红外探测器、微波和被动红外复合入侵探测器、磁开关入侵探测器等。

3建筑物内非正常出入口(如窗户、天窗等)可选用室内用多普勒微波探测器、室内用被动红外探测器、室内用超声波多普勒探测器、微波和被动红外复合入侵探测器、磁开关入侵探测器、室内用被动式玻璃破碎探测器、振动入侵探测器等。

6.1.4室内用入侵探测器的选型应符合下列规定:

1室内通道可选用室内用多普勒微波探测器、室内用被动红外探测器、室内用超声波多普勒探测器、微波和被动红外复合入侵探测器等。

2室内公共区域可选用室内用多普勒微波探测器、室内用被动红外探测器、室内用超声波多普勒探测器、微波和被动红外复合入侵探测器、室内用被动式玻璃破碎探测器、振动入侵探测器、紧急报警装置等。宜设置两种以上不同探测原理的探测器。

3室内重要部位可选用室内用多普勒微波探测器、室内用被动红外探测器、室内用超声波多普勒探测器、微波和被动红外复合入侵探测器、磁开关入侵探测器、室内用被动式玻璃破碎探测器、振动入侵探测器、紧急报警装置等。宜设置两种以上不同探测原理的探测器。

6.1.5探测器的设置应符合下列规定：

1每个 / 对探测器应设为一个独立防区。

2周界的每一个独立防区长度不宜大于**200m**。

3需设置紧急报警装置的部位宜不少于**2**个独立防区，每一个独立防区的紧急报警装置数量不应大于**4**个，且不同单元空间不得作为一个独立防区。

4防护对象应在入侵探测器的有效探测范围内，入侵探测器覆盖范围内应无盲区，覆盖范围边缘与防护对象间的距离宜大于**5m**。

6.1.6常用入侵探测器的选型要求宜符合附录**B**的规定。

6.2控制设备

6.2.1控制设备的选型除应符合本规范第3.0.3条的规定外，尚应符合下列规定：

- 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报警控制设备的类型。
- 2宜具有可编程和联网功能。
- 3接入公共网络的报警控制设备应满足相应网络的入网接口要求。
- 4应具有与其他系统联动或集成的输入、输出接口。

6.2.2控制设备的设置应符合下列规定：

- 1现场报警控制设备和传输设备应采取防拆、防破坏措施，并应设置在安全可*的场所。
- 2不需要人员操作的现场报警控制设备和传输设备宜采取电子 / 实体防护措施。
- 3壁挂式报警控制设备在墙上的安装位置，其底边距地面的高度不应小于1.5m，如*门安装时，宜安装在门轴的另一侧；如*近门轴安装时，*近其门轴的侧面距离不应小于0.5m。
- 4台式报警控制设备的操作、显示面板和管理计算机的显示器屏幕应避开阳光直射。

6.3无线设备

6.3.1无线报警的设备选型除应符合本规范第**3.0.3**条的规定外，尚应符合下列规定：

1载波频率和发射功率应符合国家相关管理规定。

2探测器的无线发射机使用的电池应保证有效使用时间不少于**6**个月，在发出欠压报警信号后，电源应能支持发射机正常工作**7d**。

3无线紧急报警装置应能在整个防范区域内触发报警。

4无线报警发射机应有防拆报警和防破坏报警功能。

6.3.2接收机的位置应由现场试验确定，保证能接收到防范区域内任意发射机发出的报警信号。

6.4管理软件

6.4.1系统管理软件的选型应符合《安全防范工程技术规范》**GB50348**等国家现行相关标准的规定，尚应具有以下功能：

1电子地图显示，能局部放大报警部位，并发出声、光报警提示。

2实时记录系统开机、关机、操作、报警、故障等信息，并具有查询、打印、防篡改功能。

3设定操作权限，对操作(管理)员的登录、交接进行管理。

6.4.2系统管理软件应汉化。

6.4.3系统管理软件应有较强的容错能力，应有备份和维护保障能力。

6.4.4系统管理软件发生异常后，应能在**3s**内发出故障报警。

7传输方式、线缆选型与布线

7.1传输方式

7•1•1传输方式应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定。

7•1•2传输方式的确定应取决于前端设备分布、传输距离、环境条件、系统性能要求及信息容量等，宜采用有线传输为主、无线传输为辅的传输方式。

7•1•3防区较少，且报警控制设备与各探测器之间的距离不大于**100m**的场所，宜选用分线制模式。

7.1.4防区数量较多，且报警控制设备与所有探测器之间的连线总长度不大于**1500m**的场所，宜选用总线制模式。

7•1.5布线困难的场所，宜选用无线制模式。

7.1.6防区数量很多，且现场与监控中心距离大于**1500m**，或现场要求具有设防、撤防等分控功能的场所，宜选用公共网络模式。

7•1•7当出现无法独立构成系统时，传输方式可采用分线制模式、总线制模式、无线制模式、公共网络模式等方式的组合。

7.2 线缆选型

7.2.1 线缆选型应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定。

7.2.2 系统应根据信号传输方式、传输距离、系统安全性、电磁兼容性等要求，选择传输介质。

7.2.3 当系统采用分线制时，宜采用不少于5芯的通信电缆，每芯截面不宜小于0.5mm²。

7.2.4 当系统采用总线制时，总线电缆宜采用不少于6芯的通信电缆，每芯截面积不宜小于1.0mm²。

7.2.5 当现场与监控中心距离较远或电磁环境较恶劣时，可选用光缆。

7.2.6 采用集中供电时，前端设备的供电传输线路宜采用耐压不低于交流500V的铜芯绝缘多股电线或电缆，线径的选择应满足供电距离和前端设备总功率的要求。

7.3布线设计

7.3.1布线设计除应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定外，尚应符合以下规定：

- 1应与区域内其他弱电系统线缆的敷设综合考虑，合理设计。
- 2报警信号线应与220V交流电源线分开敷设。
- 3隐蔽敷设的线缆和 / 或芯线应做永久性标记。

7.3.2室内管线敷设设计应符合下列规定：

- 1.室内线路应优先采用金属管，可采用阻燃硬质或半硬质塑料管、塑料线槽及附件等。
- 2.竖井内布线时，应设置在弱电竖井内。如受条件限制强弱竖井必须合用时，报警系统线路和强电线路应分别布置在竖井

7.3.3 室外管线敷设设计应满足下列规定：

1 线缆防潮性及施工工艺应满足国家现行标准的要求。

2 线缆敷设路径上有可利用的线杆时可采用架空方式。当碍于架空敷设时，与杆架设的电力线(1kv I?2T)高高矗某二示-1.5m，与广播线的间距不应小于1m，与通信线的间距不应小于0.6m，线缆最低点的高度应符合有关规定。

3 线缆敷设路径上有可利用的管道时可优先采用管道敷设

4 线缆敷设路径上有可利用建筑物时可优先采用墙壁固定敷设方式。

5 线缆敷设路径上没有管道和建筑物可利用，也不便立杆时，可采用直埋敷设方式。引出地面的出线I=I，宜选在相对隐蔽地点，并宜在出口处设置从地面计算高度不低于3m的出线防护钢管，且周围5m内不应有易攀登的物体。

6 线缆由建筑物引出时，宜避开避雷针引下线，不能避开处两者平行距离应不小于1.5m，交*间距应不小于1m，并宜防止长距离平行走线。在间距不能满足上述要求时，可对电缆加缠铜皮屏蔽，屏蔽层要有良好的就近接地装置。

8 供电、防雷与接地

8.0.1 供电设计除应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定外，尚应符合下列规定：

- 1 系统供电宜由监控中心集中供电，供电宜采用TN—S制式。
- 2 入侵报警系统的供电回路不宜与启动电流较大设备的供电同回路。
- 3 应有备用电源，并应能自动切换，切换时不应改变系统工作状态，其容量应能保证系统连续正常工作不小于8h。备用电源可以是免维护电池和 / 或UPS电源。

8.0.2 防雷与接地除应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定外，尚应符合下列规定：

- 1 置于室外的入侵报警系统设备宜具有防雷保护措施。
- 2 置于室外的报警信号线输入、输出端口宜设置信号线路浪涌保护器。
- 3 室外的交流供电线路、信号线路宜采用有金属屏蔽层并穿钢管埋地敷设，屏蔽层及钢管两端应接地。

9 系统安全性、可靠性、电磁兼容性、环境适应性

9.0.1 系统安全性设计除应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定外，尚应符合下列规定：

1 系统选用的设备，不应引入安全隐患，不应对被防护目标造成损害。

2 系统的主电源宜直接与供电线路物理连接，并对电源连接端子进行防护设计，保证系统通电使用后无法人为断电关机。

3 系统供电暂时中断，恢复供电后，系统应不需设置即能恢复原有工作状态。

4 系统中所用设备若与其他系统的设备组合或集成在一起时，其入侵报警单元的功能要求、性能指标必须符合本规范和《防盗报警控制器通用技术条件》GB12663等国家现行标准的相关规定。

9.0.2 系统可靠性设计应符合现行国家标准《安全防范工程技术规范》GB50348的相关规定。

9.0.3 系统电磁兼容性设计应符合现行国家标准《安全防范工程技术规范》GB50348的相关规定。系统所选用的主要设备应符合电磁兼容试验系列标准的规定，其严酷等级应满足现场电磁环境的要求。

9.0.4系统环境适应性除应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定外，尚应符合下列规定：

1系统所选用的主要设备应符合现行国家标准《报警系统环境试验》>GB / T 15211的相关规定，其严酷等级应符合系统所在地域环境的要求。

2设置在室外的设备、部件、材料，应根据现场环境要求做防晒、防淋、防冻、防尘、防浸泡等设计。

10 监控中心

10.0.1监控中心的设计应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定。

10.0.2当入侵报警系统与安全防范系统的其他子系统联合设置时，中心控制设备应设置在安全防范系统的监控中心。

10.0.3独立设置的入侵报警系统，其监控中心的门、窗应采取防护措施。

B.0.1常用入侵探测器的选型要求宜符合表B.0.1的规定。

名称	适应场所与安装方式	主要特点	安装设计要点	适宜工作环境和条件	不适宜工作环境和条件	附加功能
----	-----------	------	--------	-----------	------------	------

超声波多普勒探测器	室内空间型	吸顶	没有死角且成本低	水平安装，距地宜小于3.6m	警戒空间要有较好密封性 简易或密封性不好的室内；有活动物和可能活动物；环境嘈杂，附近有金属打击声、汽笛声、电铃等高频声响	智能鉴别技术
------------------	-------	----	----------	----------------	---	--------

壁挂 距地2.2m左右，透镜的法线方向宜与可能入侵方向成180°角

微波多普勒探测器	室内空间型：壁挂式	不受声、光、热的影响	距地1.5~2.2m左右，严禁对着房间的外墙、外窗。透镜的法线方向宜与可能入侵方向成180°角	可在环境噪声较强、光变化、热变化较大的条件下工作	有活动物和可能活动物；微波段高频电磁场环境；防护区域内有过大、过厚的物体	平面天线技术；智能鉴别技术
-----------------	-----------	------------	---	--------------------------	--------------------------------------	---------------

被动红外入侵探测器 室内空间型 吸顶 被动式(多台交*使用互不干扰), 功耗低, 可靠性较好 水平安装, 距地宜小于**3.6m** 日常环境噪声, 温度在**15~25℃**时探测效果最佳背景有热冷变化, 如: 冷热气流, 强光间歇照射等; 背景温度接近人体温度; 强电磁场干扰; 小动物频繁出没场合等 自动温度补偿技术; 抗小动物干扰技术; 防遮挡技术; 抗强光干扰技术; 智能鉴别技术
壁挂距地**2.2m**左右, 透镜的法线方向宜与可能入侵方向成**90°**角
楼道 距地**2.2m**左右, 视场面对楼道
幕帘 在顶棚与立墙拐角处, 透镜的法线方向宜与窗户平行 窗户内窗台较大或与窗户平行的墙面无遮挡; 其他与上同 窗户内窗台较小或与窗户平行的墙面有遮挡或紧贴窗帘安装; 其他与上同

微波和被动红外复合入侵探测器 室内空间型 吸顶 误报警少(与被动红外探测器相比); 可靠性较好 水平安装, 距地宜小于**4.5m** 日常环境噪声, 温度在**15~25℃**时探测效果最佳 背景温度接近人体温度; 小动物频繁出没场合等双—单转换型; 自动温度补偿技术; 抗小动物干扰技术; 防遮挡技术; 智能鉴别技术
壁挂 距地**2.2m**左右, 透镜的法线方向宜与可能入侵方向成**135°**角
楼道 距地**2.2m**左右, 视场面对楼道

被动式玻璃破碎探测器 室内空间型：有吸顶、壁挂等 被动式；仅对玻璃破碎等高频声响敏感 所要保护的玻璃应在探测器保护范围之内，并应尽量靠近所要保护玻璃附近的墙壁或天花板上，具体按说明书的安装要求进行 日常环境噪声环境嘈杂，附近有金属打击声、汽笛声、电铃等高频声响 智能鉴别技术

振动入侵探测器 室内、室外被动式 墙壁、天花板、玻璃；室外地面表层物下面、保护栏网或桩柱，最好与防护对象实现刚性连接 远离振源 地质板结的冻土或土质松软的泥土地，时常引起振动或环境过于嘈杂的场合 智能鉴别技术

主动红外入侵探测器 室内、室外(一般室内机不能用于室外) 红外脉冲、便于隐蔽 红外光路不能有阻挡物；严禁阳光直射接收机透镜内；防止入侵者从光路下方或上方侵入 室内周界控制；室外“静态”干燥气候 室外恶劣气候，特别是经常有浓雾、毛毛雨的地域或动物出没的场所、灌木丛、杂草、树叶树枝多的地方

遮挡式微波入侵探测器 室内、室外周界控制 受气候影响 高度应一致，一般为设备垂直作用高度的一生 无高频电磁场存在场所；收发机间无遮挡物 高频电磁场存在的场所；收发机间有可能有遮挡物 报警控制设备宜有智能鉴别技术

振动电缆入侵探测器 室内、室外均可 可与室内外各种实体周界配合使用 在围栏、房屋墙体、围墙内侧或外侧高度的2 / 3处。网状围栏上安装应满足产品安装要求 非嘈杂振动环境 嘈杂振动环境 报警控制设备宜有智能鉴别技术

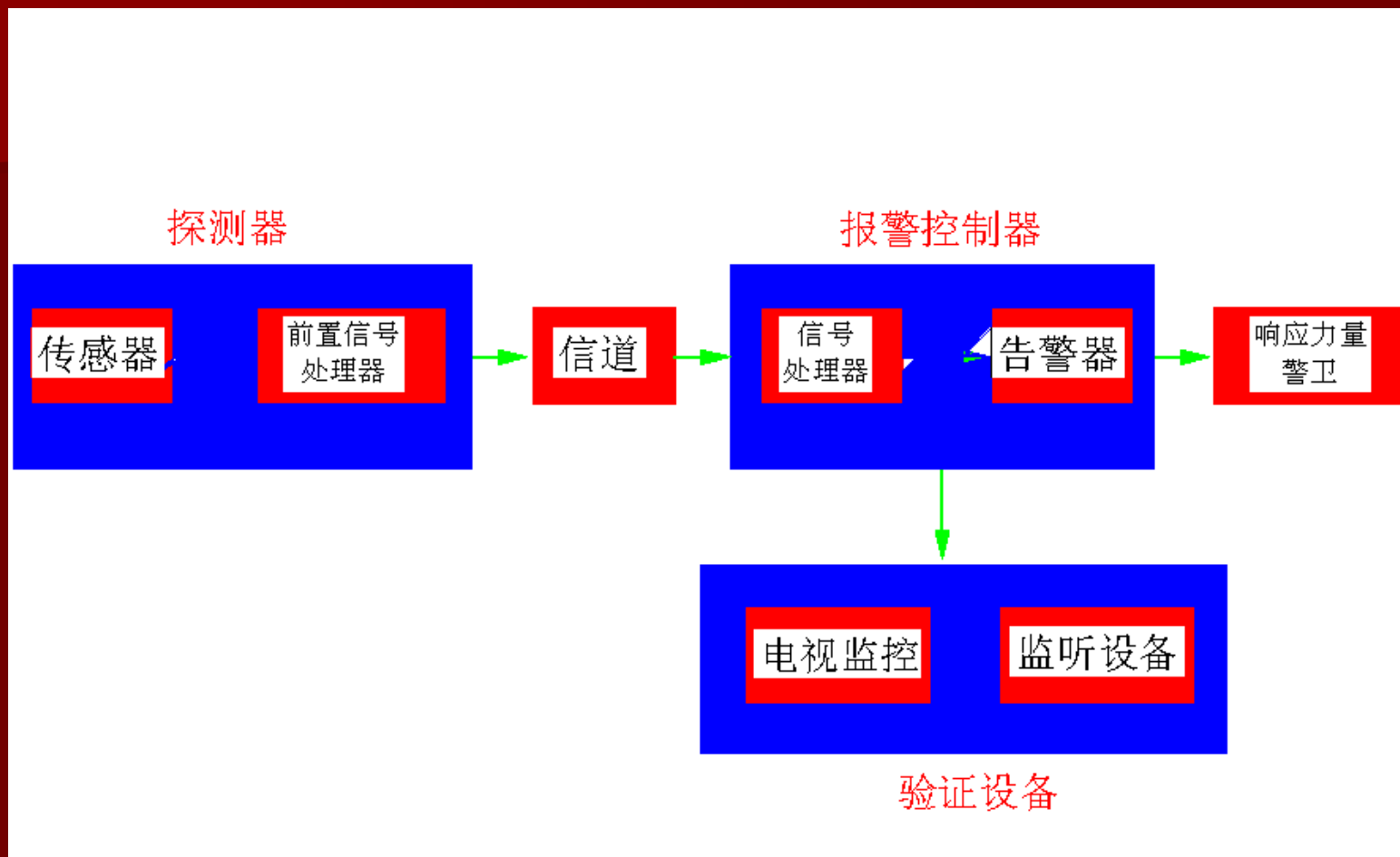
泄漏电缆入侵探测器 室内、室外均可 可随地形埋设、可埋入墙体 埋入地域应尽量避免金属堆积物 两探测电缆间无活动物体；无高频电磁场存在场所 高频电磁场存在场所；两探测电缆间有易活动物体(如灌木丛等) 报警控制设备宜有智能鉴别技术

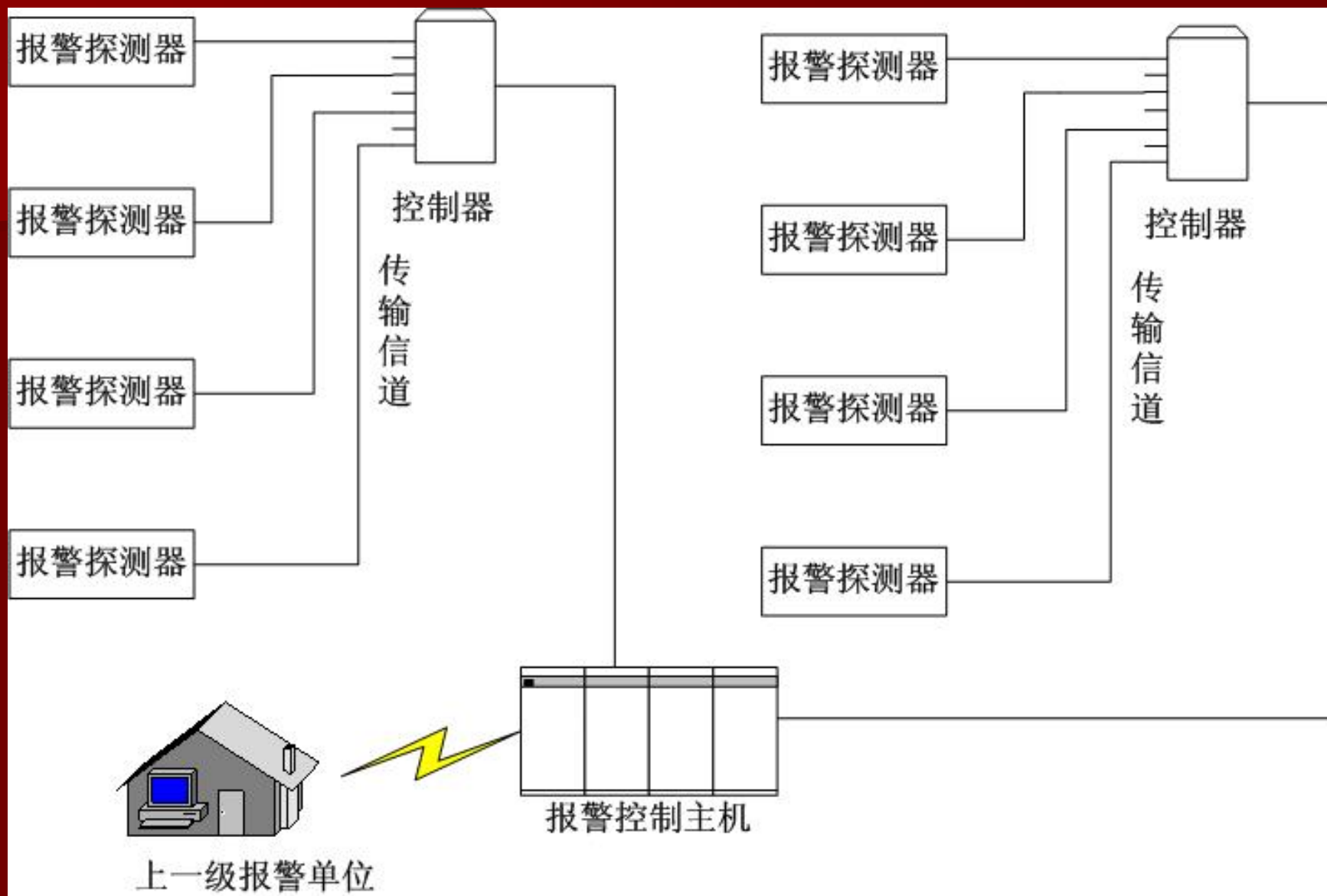
磁开关入侵探测器 各种门、窗、抽屉等 体积小、可靠性好 舌簧管宜置于固定框上，磁铁置于门窗等的活动部位上，两者宜安装在产生位移最大的位置，其间距应满足产品安装要求 非强磁场存在情况 强磁场存在情况 在特制门窗使用时宜选用特制门窗专用门磁开关紧急报警装置 用于可能发生直接威胁生命的场所(如金融营业场所、值班室、收银台等) 利用人工启动(手动报警开关、脚踢报警开关等)发出报警信号 要隐蔽安装，一般安装在紧急情况下人员易可靠触发的部位 日常工作环境防误触发措施，触发报警后能自锁，复位需采用人工再操作方式

入侵报警系统

入侵报警系统设计应符合下列原则

- 1** 入侵报警系统应由探测前端、传输、声光显示与（或）记录、控制四个主要部分组成。
- 2** 根据总体纵深防护和局部纵深防护的原则，分别设置或综合设置建筑物（群）周界防护、建筑物内区域防护、空间防护、实物目标防护系统。
- 3** 系统应自成网络，可独立运行；应能与视频监控系统、出入口控制系统等联动；应具有网络接口、扩展接口等。
- 4** 根据需要，系统除应具有本地报警功能外，还应具有异地报警功能。具有异地报警功能的系统，还应具有报警模式识别功能。
- 5** 系统前端的选择要根据安防需要、安装环境，设置不同类型、不同警戒范围的入侵探测设备，构成点、线、面、空间或其组合的综合防护系统。





入侵探测器的选择应符合下列规定：

- 1** 各类入侵探测器的设置原则是防范区内不得有盲区，探测器之间应有至少**20%**以上的交叉覆盖面，探测器的作用距离应有**30%**裕量。在交叉覆盖时，应避免相互干扰。
- 2** 探测器的设置应远离影响其工作的电磁辐射、热辐射、光辐射、噪声、气象条件等环境，或采取防护措施。
- 3** 探测器的灵敏度应满足设防要求，并可进行调节。
- 4** 复合入侵探测器，应视为一种探测技术的探测装置。
- 5** 入侵探测器盲区边缘与防护目标间的距离不得小于**5m**。
- 6** 玻璃破碎探测器应安装在被保护对象附近的墙壁或天花板上。
- 7** 被动红外探测器的防护区内不应有障碍物。
- 8** 采用室外双束或四束主动红外探测器时，探测器最远警戒距离，不应大于其最大射束距离的**2/3**。

点控制式的入侵探测器

磁开关入侵探测器

玻璃破碎入侵探测器

视频画面入侵探测器

触摸--感应式入侵探测器

出入口控制及门禁系统常用的
点控产品

其他常见的点控报警产品

警戒线控制式入侵探测器

主动红外入侵探测器

激光入侵探测器

反射式被动红外入侵探测器

收发分体式微波（微波墙）入侵探测器

感应式入侵探测器

移动防范

空间控制式入侵探测器

声控入侵探测器

超声波入侵探测器

微波入侵探测器

被动红外入侵探测器

双鉴入侵探测器

移动防范

周界控制式入侵探测器

主动红外入侵探测器

微波墙式入侵探测器

脉冲式高压电网

微波泄露电缆入侵探测器

振动式地音入侵探测器

振动电缆

●几种常见的入侵报警探测器



门窗磁开关



报警按钮



主动红外探测器



被动红外探测器



双鉴入侵探测器



吸顶式红外传感器

- 探测率：探测率 = 因出现危险情况而报警的次数 / 出现危险情况的次数 * **100 %**。
- 漏报率：漏报率 = 出现危险情况应报警而未报警的次数 / 出现危险情况的次数 * **100 %**。
- 误报率：误报率 = 误报次数 / 报警总数。
- 探测灵敏度。
- 报警传送方式，最大传输距离。
- 警戒范围。
- 功耗及工作电压和工作电流。
- 环境温度

报警主机也叫入侵报警控制器，用于连接报警探测器，判断报警情况，管理报警事件的专用设备。报警主机具有对报警主机防区分区进行设置与管理的能力，可以根据报警探测器的信号进行分析，产生报警事件并根据在报警主机上的参数设置进行处理。可以对设防区域进行撤 / 布防操作，是整个安全系统的核心。一般情况下通过专门的键盘对报警主机进行管理和编程，设置参数工作。

- 布防和撤防功能
- 布防后的延时功能
- 防破坏功能
- 联网功能
- 应有较高的稳定性
- 应能接受各种性能的报警输入

■ **1、小型报警主机**

■ **2、区域入侵报警主机**

■ **3、集中入侵报警主机**

1、小型报警主机

小型报警控制器适用于银行的储蓄所，学校的财务部门、档案室和仓库。其功能如下。

a) 提供4—8路报警信号、4—8路声控复核信号、2—4路电视复核信号，还可以在线接收无线传输的报警信号。

b) 在信号报警时，发出声光报警信号，并能显示报警部位、时间。

c) 有自动/手动、声音复核和电视、录像复核。

d) 对系统有自查能力。

e) 具有5—10MIN延迟报警功能。

f) 能向区域报警中心发出报警信号。

g) 能够存入2—4个紧急报警电话，一旦报警时，能自动依次向紧急报警电话发报警信号。

h) 断电时能自动切换到备用电源上，以保证系统正常工作。

2、区域入侵报警主机

区域入侵报警主机适用于防范要求较高的高层写字楼、住宅小区、大型仓库等场所。区域入侵报警器除了具有小型控制器的全部功能外，还有以下更多的输入控制端。

a)16路、24路、32、128路报警输入控制端。

b)24路声控复核输入控制端。

c)8—16路电视摄像复核输入控制端，并具有良好的并网能力。

d)区域入侵报警主机有效地利用了计算机技术，实现了输入信号的总线制。例如，探测器根据安置地点，实现统一编码，探测器的地址码、信号以及供电由总线完成，大大简化了工程安装。每路输入总线上可挂接128个探测器，而且每路总线上有短防接口。当某路电路发生故障时，控制中心的CPU，在报警显示板上，由发光二极管显示报警部位，同时驱动声光报警电路，及时把报警信号送到外设备通信接口，按原先存储的报警电话，向更高一级的报警中心报警。

3、集中入侵报警主机

集中入侵报警主机适用于大型和特大型报警系统。它能接收各个区域控制器送来的信息，同时向各区域控制器发送控制指令。集中入侵控制器能够直接切换出任何一个区域控制器送来的声音和图像复核信号。由于集中入侵控制器和多个区域控制联网，具有存储量大和更先进的联网功能

报警主机：

与PC连接的报警主机，不同的主机具有不同的唯一主机编号，主机名称由软件操作员定义，便于主机管理，允许相同，但建议主机名应该有所区别，每台主机对应的串行接口必须不同，接口的通讯参数如波特率，校验方式允许用户设置。

主机防区：

每台报警主机对应的报警点(传感器)。在每台主机上具有唯一的编号，主机编号与主机防区编号对应一个唯一的防区。

主机分区：

每台报警主机撤布防管理的基本单位，是主机防区的集合。

防区：

防区是管理系统的基本单位，是整个系统的核心,对应一个报警传感器，由主机编号和主机防区编号唯一决定，其工作方式由防区参数决定。

撤/布防：

对防区进行的撤布防，它与报警主机的撤布防状态无关，CMS7000根据防区的布防状态与防区类型来决定是否对收到的符合条件的主机报警消息作为报警处理。

地图：

用于监控防区，用户的地图，可以为每个防区或用户指定其所属的地图文件名称，定义它们在地图上的位置，显示地图时如果选择的是用户方式，则所有被定义在指定地图上的用户被显示，如果是显示防区，则指定地图上所有防区被显示，有报警事件发生的用户或防区将动态显示在地图上，系统定义有一张主监控地图，在规定时间内系统可以自动将监控地图切换到主监控地图上进行用户监控。

用户组：

为了便于管理还可以将用户分类成不同用户组进行管理，所有用户必须属于某一用户组。

入侵报警系统的显示、记录及控制应符合下列要求：

- 1** 现场报警控制器宜安装在具有自身防护设施的弱电间内，应配备可靠电源，断电时应能保存以往的运行数据。
- 2** 系统应能显示和记录发生的入侵事件、时间和地点。重要部位报警时，系统应能对报警现场进行声音和（或）图像的复核，复核手段不宜少于**2**种。
- 3** 系统应能按时间、区域、部位任意编程设防和撤防。
- 4** 系统设计要有业主认可的冗余量。
- 5** 在探测器防范区内，发生入侵事件时，系统不应产生漏报警，平时宜避免误报警。
- 6** 系统应具有设备防拆功能、系统自检功能及故障报警功能。

入侵报警系统声音（复核）探测器的选择应符合下列规定：

- 1** 设计应根据现场环境条件考虑。在背景噪声不大于**45dB**（**A**）的情况下，灵敏度调到最大值**90%**时所能探测的最大范围，应能满足现场保护的需要。
- 2** 声音探测器安装时应考虑声音的方向性。不应将其设计安装在墙角、拐弯处或能产生声响的物体附近。
- 3** 当要求与图像同步切换时，一台摄像机应配一个声音探测器。

按普通人的听觉

0—20 分贝 很静、几乎感觉不到；
20—40 分贝 安静、犹如轻声絮语；
40—60 分贝 一般。普通室内谈话；
60—70 分贝 吵闹、有损神经；
70—90 分贝 很吵、神经细胞受到破坏。
90—100 分贝 吵闹加剧、听力受损；
100—120 分贝 难以忍受、呆一分钟即暂时致聋。
120分贝以上：极度聋或全聋

0分贝 勉强可听见的声音：微风吹动的树叶声
20分贝 低微的呢喃：安静办公室的声音
40分贝 钟摆的声音：一般办公室谈话
80分贝 隔音汽车里的声音、热闹街道上的声音
100分贝 火车的噪音、铁桥下尖锐的警笛声
120分贝 飞机的引擎声：会令耳朵疼痛的声音

在分贝计前大叫得震耳欲聋，可能也不够轻轻对准探测器一吹的分贝读数来得大。这可能是因为尖叫只带来空气中能量的传送，但吹风带动空气粒子直接撞击分贝计的探测器，引起额外的“零距离”声波，取得更大的正增长参数数值。

《中华人民共和国城市区域环境噪声标准》规定，居住、文教机关为主的区域以及乡村居住环境的噪声标准值，白天等效噪声值为**55分贝**，夜间为**45分贝**；商业、工业混杂区的等效噪声值为**60分贝**，夜间为**50分贝**；城市中交通干线两侧，白天噪声的等效噪声值为**70分贝**，夜间不超过**55分贝**。

医学专家介绍，一般情况下，噪声如果超过**50分贝**，长时间处在这种环境里，人的神经系统就会受到影响。噪声平均每提高**3分贝**，噪声能量就会增强一倍。噪声污染严重，甚至会破坏人体的听觉系统。经常处于噪声困扰之中，会出现记忆力减退、失眠等症状。有研究显示，长期在机场、铁道附近生活或者工作的女性怀孕后，**婴儿智力低下和畸形的比例要明显高于其它地区**。

这里每项施工活动的最高噪音都有规定，如木工为**92分贝**，粉碎机为**85分贝**等。当工地噪音超过**140分贝**时，必须让一部分机器停工。在一些发展中国家的城市，噪音污染问题也越来越严重，有些地区全天的噪音达到**75-80分贝**。

噪音污染和大气污染、水污染并列为三大污染，但是噪音污染却不如后两者那样受到重视，相反，如果噪音污染不造成像上述两个案例那样大的恶果，往往被人们忽略。以至这些年来，噪音污染在全球范围内都是有增无减。世界卫生组织去年曾就全世界的噪音污染情况进行了调查，结果显示，美国及发达国家的噪音污染问题越来越严重，在美国，生活在**85分贝**以上噪音污染环境中的居民人数**20**年来上升了数倍；在欧盟国家，**40%**的居民几乎全天受到交通运输噪音污染的干扰，这些居民相当于每天生活在**55分贝**的噪音环境中，其中**20%**的人受到的交通噪音污染超过**65分贝**。此外，在发展中国家的一些城市，噪音污染问题也已相当严重，有些地区全天**24**小时的噪音达到**75至80分贝**……世界卫生组织认为，全球噪音污染已经成为影响人们身体健康和生活质量的严重问题，呼吁各国积极采取有效措施予以控制减少噪音。

据科学家测定，电视机、家庭影院、组合音响等所产生的噪音，可达**60至80**分贝；洗衣机为**42至70**分贝；电冰箱为**32至50**分贝。

噪音有损人体的听觉器官。医学专家认为，家庭噪音是造成儿童聋哑的病因之一。据临床医学资料统计，若在**80**分贝以上噪音环境中生活，造成聋哑的可能性达**50%**。同时，噪音是影响儿童智力和身体发育的大敌。据研究资料表明，处在吵闹环境中生活的儿童，其智力发育要比在安静环境中低**20%**；营养学家研究发现，噪音不仅会使人体的免疫功能下降，还能使人体中的维生素**C、B1、B2、B6**、氨基酸、谷氨酸、赖氨酸等营养物质的消耗量增加，这对儿童的生长发育造成恶劣影响。

按普通人的听觉

0—20 分贝 很静、几乎感觉不到；
20—40 分贝 安静、犹如轻声絮语；
40—60 分贝 一般。普通室内谈话；
60—70 分贝 吵闹、有损神经；
70—90 分贝 很吵、神经细胞受到破坏。
90—100 分贝 吵闹加剧、听力受损；
100—120 分贝 难以忍受、呆一分钟即暂时致聋。
120分贝以上：极度聋或全聋

0分贝 勉强可听见的声音：微风吹动的树叶声
20分贝 低微的呢喃：安静办公室的声音
40分贝 钟摆的声音：一般办公室谈话
80分贝 隔音汽车里的声音、热闹街道上的声音
100分贝 火车的噪音、铁桥下尖锐的警笛声
120分贝 飞机的引擎声：会令耳朵疼痛的声音

在分贝计前大叫得震耳欲聋，可能也不够轻轻对准探测器一吹的分贝读数来得大。这可能是因为尖叫只带来空气中能量的传送，但吹风带动空气粒子直接撞击分贝计的探测器，引起额外的“零距离”声波，取得更大的正增长参数数值。

入侵探测器分类

1按传传感器：开关、震动、声音、超声波、次声（频率极低信号，例如**1Hz**次声，源于开门、碎窗、凿墙开洞引起室内外气压差产生气流扰动次声，经低通滤波器放大报警）、主动被动红外、微波、激光、视频运动、多技术复合

2按工作方式：主动（发出能量）；被动（不发能量）

3按警戒方式：点、线、面、空间

4按报警信号传输方式：有线、无线

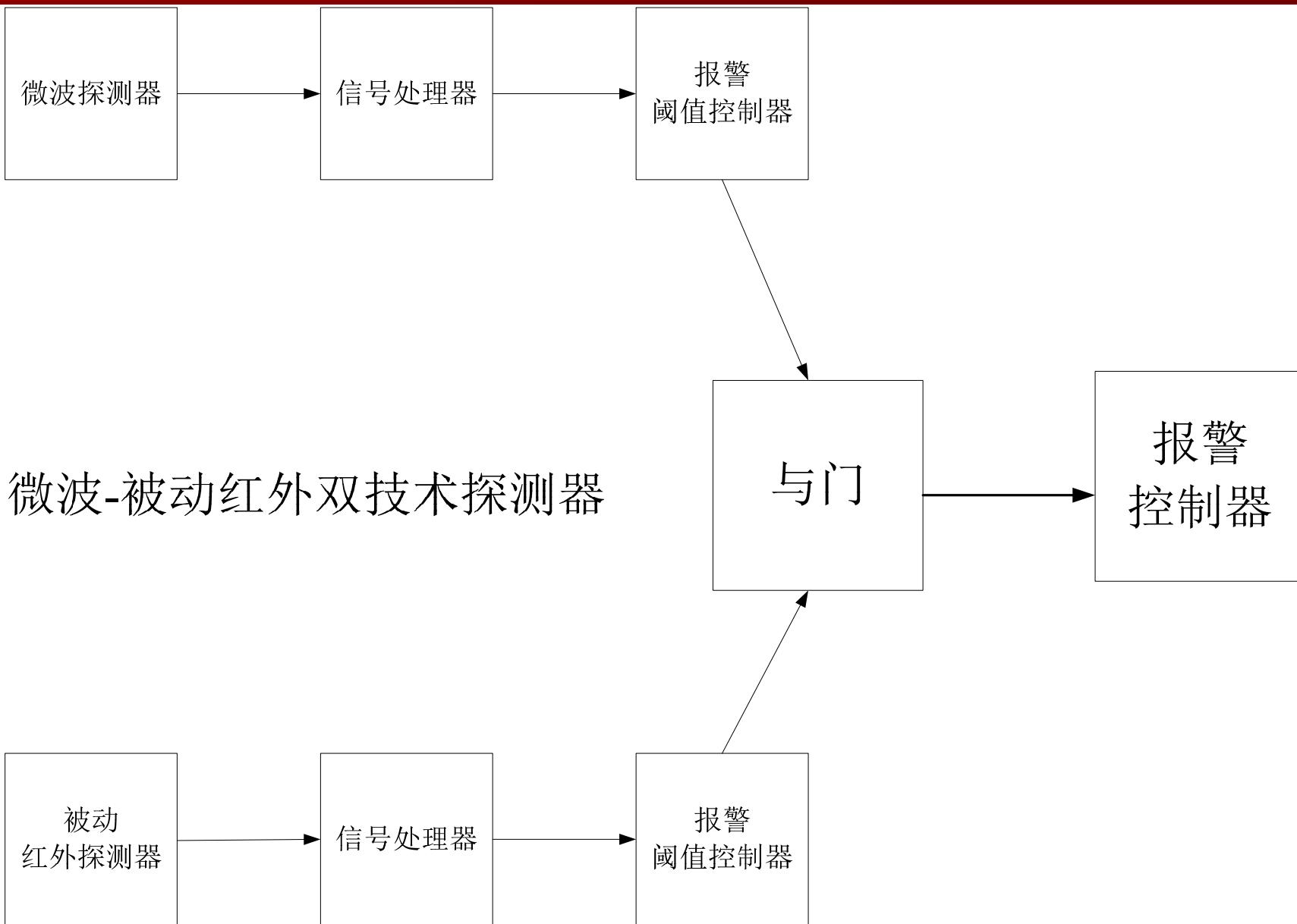
5按使用环境：室内、室外

6按探测模式：空间型（声音、次声、微波、**被动红外**）、幕帘型

红外探测器

10	红外辐射波长 (微米)
573K (300°C)	5
373K (100°C)	7.8
人体 (37°C)	10
273K (0°C)	10.5

	单技术探测器				双技术探测器			
种类	超声波	微波	声控	被动红外	超声+被动红外	主动+被动红外	超声+微波	微波+被动红外
误报率	4.21%				2.7%			1%
可信度	差				中			好





视频安防监控系统

视频监控系统构成

系统由以下四部分组成：

- 产生图像的摄像机或成像装置（前端设备）
- 图像的传输与转换设备（传输设备）
- 图像的处理与控制装置（主控设备）
- 终端图像显示记录装置（显示记录设备）

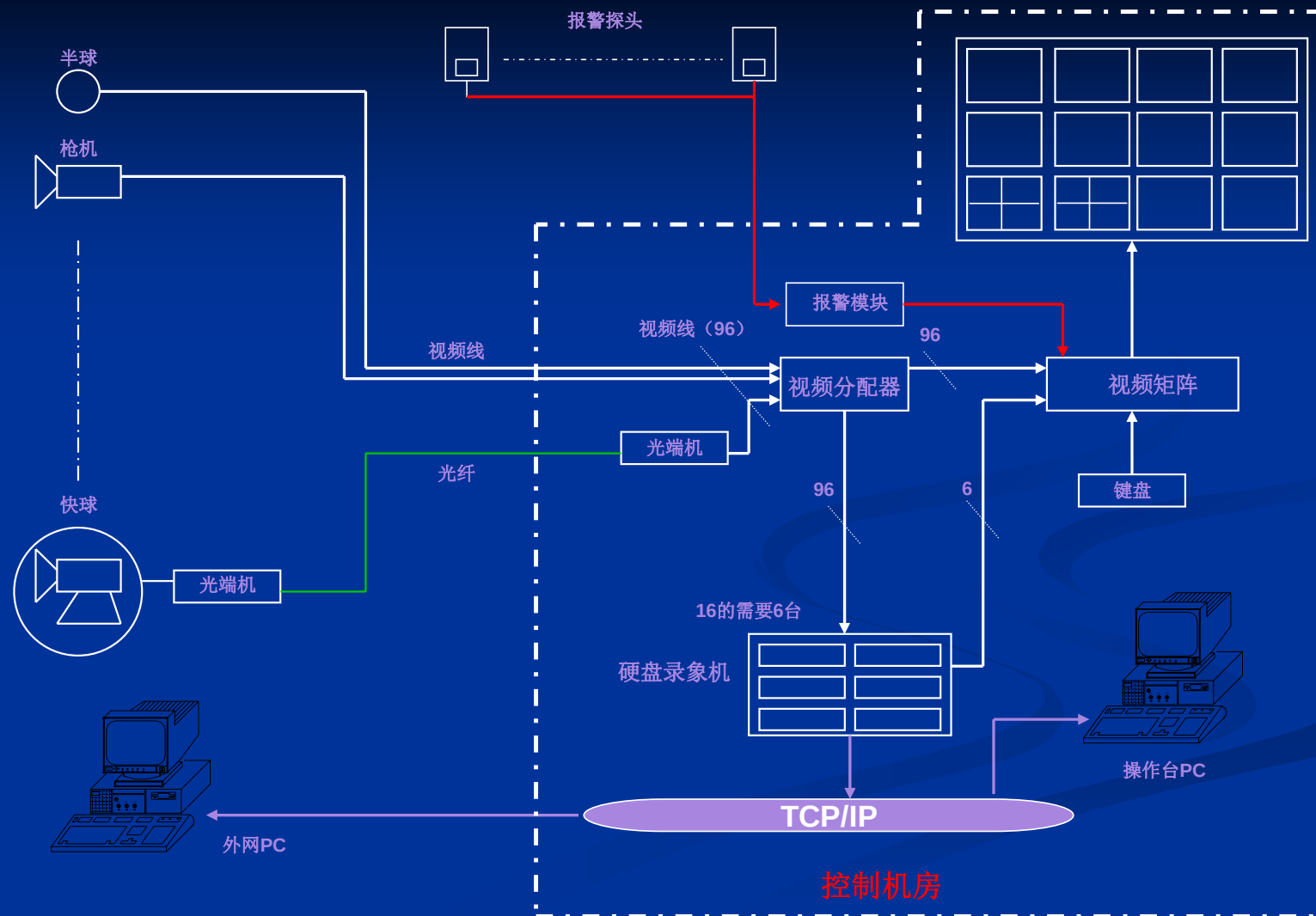
视频监控系统设计应符合下列原则：

- 1** 视频监控系统应由摄像、传输、显示与图像记录、控制四个主要部分组成，并具有对图像信号的分配、切换、存储、还原等功能。
- 2** 系统设计应满足监控区域有效覆盖、布局合理、图像清晰、控制有效的基本要求。
- 3** 视频监控电视图像质量的主观评价可采用五级损伤制评定(参见表**14.3.1**)。系统在正常工作条件下，图像质量应不低于**4**级的要求；在允许的最恶劣工作条件下或应急照明情况下，图像质量应不低于**3**级的要求。

图像等级图像质量损伤主观评价**5**不觉察损伤或干扰**4**稍有觉察损伤或干扰，但不令人讨厌**3**有明显损伤或干扰，令人感到讨厌**2**损伤或干扰较严重，令人相当讨厌**1**损伤或干扰极严重，不能观看

- 4** 视频监控系统的制式应采用与通用的电视制式一致，选用设备、部件的视频输入和输出阻抗以及电缆的特性阻抗均应为**75Ω**；音频设备的输入、输出阻抗宜为高阻抗。
- 5** 沿警戒线设置的视频监控系统，宜对沿警戒线**5m**宽的警戒范围实现无盲区监控。
- 6** 系统应自成网络独立运行。并能与防盗报警、出入口控制、火灾自动报警及辅助照明装置联动；性质重要场所，在有报警信号时，系统应能对报警现场进行声音及（或）图像复核。
- 7** 规模大、智能化程度要求高的项目，可采用多媒体视频监控系统，构成集成式安全防范自动化管理系统。

结构框图



GB 50395-2007

《视频安防监控系统设计规范》

1 总则.....	1
2 术语.....	1
3 基本规定.....	4
4 系统构成.....	5
5 系统功能、性能设计.....	6
6 设备选型与设置.....	8
7 传输方式、线缆选型与布线.....	13
8 供电、防雷与接地.....	13
9 系统安全性、可靠性、电磁兼容性、环境适应性.....	14
10 监控中心.....	14

2.0.1 视频安防监控系统**video surveillance & control system (VSCS)**

- 利用视频探测技术、监视设防区域并实时显示、记录现场图像的电子系统或网络。

2.0.2 模拟视频信号**video signal**

- 基于目前的模拟电视模式，所需的大约为**6MHz** 或更高带宽的基带图像信号。

2.0.3 数字视频**digital video**

- 利用数字化技术将模拟视频信号经过处理，或从光学图像直接经数字转换获得的具有严格时间顺序的数字信号，表示为特定数据结构的能够表征原始图像信息的数据。

2.0.4 视频探测**video detection**

- 采用光电成像技术（从近红外到可见光谱范围内）对目标进行感知并生成视频图像信号的一种探测手段。

2.0.5 视频监控**video monitoring**

- 利用视频手段对目标进行监视和信息记录。

2.0.6 视频传输**video transport**

- 利用有线或无线传输介质，直接或通过调制解调等手段，将视频图像信号从一处传到另一处，从一台设备传到另一台设备的过程。

2.0.7 前端设备**front-end device**

- 在本规范中，指摄像机以及与之配套的相关设备（如镜头、云台、解码驱动器、防护罩等）。

2.0.8 视频主机**video controller/switcher**

- 通常指视频控制主机，它是视频系统操作控制的核心设备，通常可以完成对图像的切换、云台和镜头的控制等。

2.0.9 数字录像设备**digital video recorder (DVR)**

- 利用标准接口的数字存储介质，采用数字压缩算法，实现视（音）频信息的数字记录、监视与回放的视频设备。
- 数字录像设备俗称数字录像机，又因记录介质以硬盘为主，故又称硬盘录像机。

基带信号

基带信号(Baseband Signal)

信源（信息源，也称发终端）发出的没有经过调制（进行频谱搬移和变换）的原始电信号，其特点是 频率较低，信号频谱从零频附近开始，具有低通形式。根据原始电信号的特征，基带信号可分为数字基带信号和模拟基带信号（相应地，信源也分为数字信源和模拟信源。）其由信源决定。说的通俗一点,基带信号就是发出的直接表达了要传输的信息的信号，比如我们说话的声波就是基带信号。（如果一个信号包含了频率达到 无穷大的交流成份和可能的直流成份，则这个信号就是基带信号。）

由于在近距离范围内基带信号的衰减不大，从而信号内容不会发生变化。因此在传输距离较近时，计 算机网络都采用基带传输方式。如从计算机到监视器、打印机等外设的信号就是基带传输的。大多数的局域网使用基带传输，如以太网、令牌环网。常见的网络设计 标准**10BaseT**使用的就是基带信号。

2.0.10 分控branch console

- 在监控中心以外设立的控制终端设备。

2.0.11 模拟视频监控系统analog video surveillance system

- 除显示设备外的视频设备之间以端对端模拟视频信号传输方式的监控系统。

2.0.12 数字视频监控系统digital video surveillance system

- 除显示设备外的视频设备之间以数字视频方式进行传输的监控系统。
- 由于使用数字网络传输，所以又称网络视频监控系统。

2.0.13 环境照度environmental illumination

- 反映目标所处环境明暗（可见光谱范围内）的物理量，数值上等于垂直通过单位面积的光通量。

2.0.14 图像质量picture quality

- 是指图像信息的完整性，包括图像帧内对原始信息记录的完整性和图像帧连续关联的完整性。它通常按照如下的指标进行描述：像素构成、分辨率、信噪比、原始完整性等。

2.0.15 原始完整性original integrity

- 在本规范中，专指图像信息和声音信息保持原始场景特征的特性，即无论中间过程如何处理，最后显示 / 记录 / 回放的图像和声音与原始场景保持一致，即在色彩还原性、灰度级还原性、现场目标图像轮廓还原性（灰度级）、事件后继顺序、声音特征等方面均与现场场景保持最大相似性（主观评价）的程度。

2.0.16 实时性real time

- 一般指图像记录或显示的连续性（通常指帧率不低于**25fps**的图像为实时图像）；在视频传输中，指终端图像显示与现场发生的同时性或者及时性，它通常由延迟时间表征。

2.0.17 图像分辨率picture resolution

- 人眼对电视图像细节辨认清晰程度的量度，在数值上等于在显示平面水平扫描方向上，能够分辨的最多的目标图像的电视线数。

2.0.18 图像数据格式video data format

- 指数字视频图像的表示方法，用像素点阵序列来表征。

2.0.19 数字图像压缩digital compression for video

- 利用图像空间域、时间域和变换域等分布特点，采用特殊的算法，减少表征图像信息冗余数据的处理过程。

2.0.20 视频音频同步synchronization of video and audio

- 视频显示的动作信息与音频的对应的动作信息具有一致性。

2.0.21 报警图像复核video check to alarm

- 当报警事件发生时，视频监控系统调用与报警区域相关图像的功能。

2.0.22 报警联动action with alarm

- 报警事件发生时，引发报警设备以外的相关设备进行动作（如报警图像复核、照明控制等）。

2.0.23 视频移动报警video moving detection

- 利用视频技术探测现场图像变化，一旦达到设定阈值即发出报警信息的一种报警手段。

2.0.24 视频信号丢失报警video loss alarm

- 当接收到视频信号的峰峰值小于设定阈值（视频信号丢失）时给出报警信息的功能。

4 系统构成

4.0.1 视频安防监控系统包括前端设备、传输设备、处理 / 控制设备和记录 / 显示设备四部分。

4.0.2 根据对视频图像信号处理 / 控制方式的不同，视频安防监控系统结构宜分为以下模式：

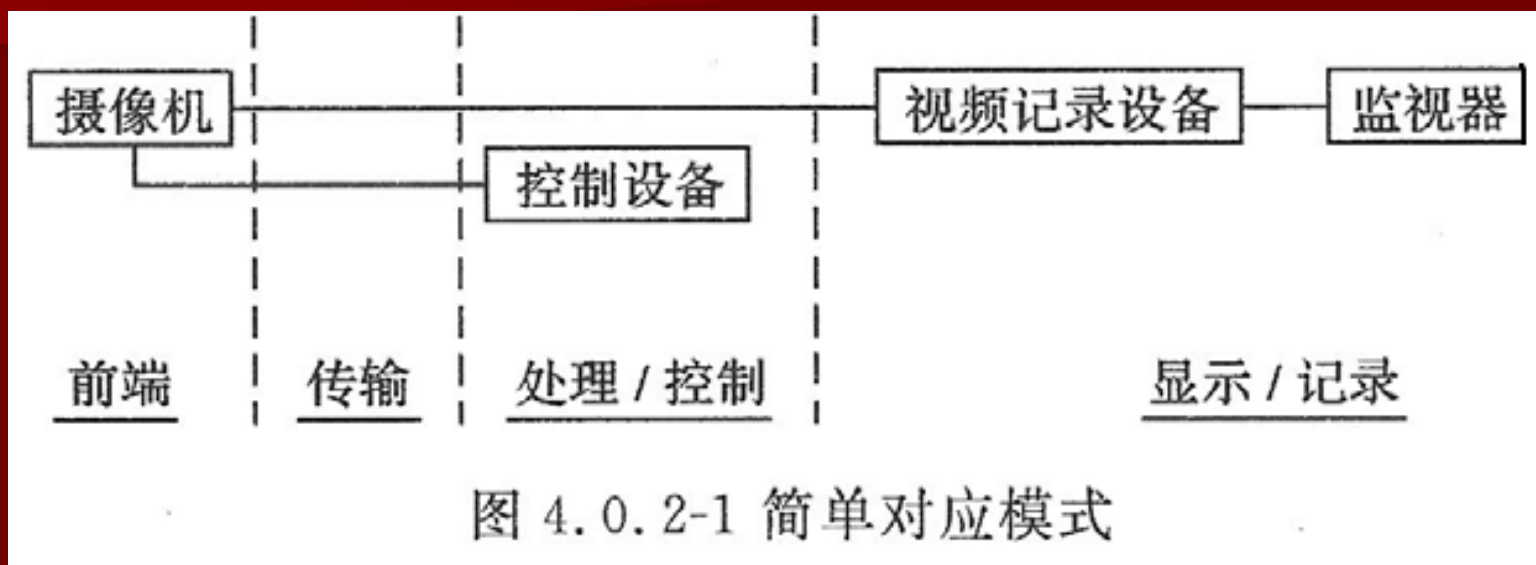
静止的画面称为图像Picture

利用视觉暂留原理，人在每秒24帧frame以上时，人们无法区别静态画面而成为平滑连续视觉效果，这样的画面称为视频。

低于24帧时，有不连续的感觉，称为动画，Catoon。

电影、电视、录像已经成为传统，现在是计算机网络和多媒体技术时代，，视频信息技术深入到我们生活中。

1、简单对应模式：监视器和摄像机简单对应（图4.0.2-1）。



2、时序切换模式：视频输出中至少有一路可进行视频图像的时序切换（图4.0.2-2）

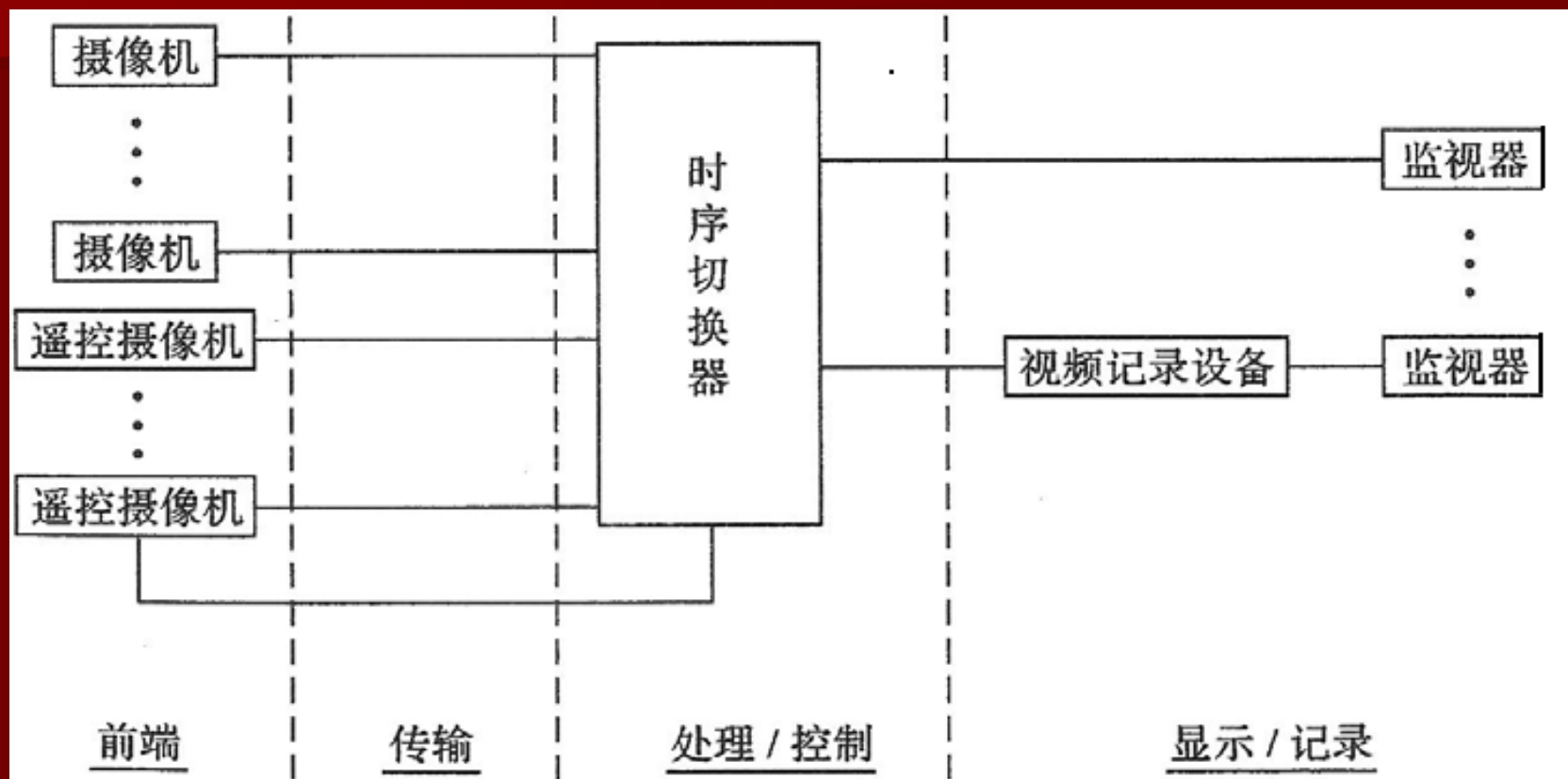


图 4.0.2-2 时序切换模式

3、矩阵切换模式：可以通过任一控制键盘，将任意一路前端视频输入信号切换到任意一路输出的监视器上，并可编制各种时序切换程序（图4.0.2-3）。

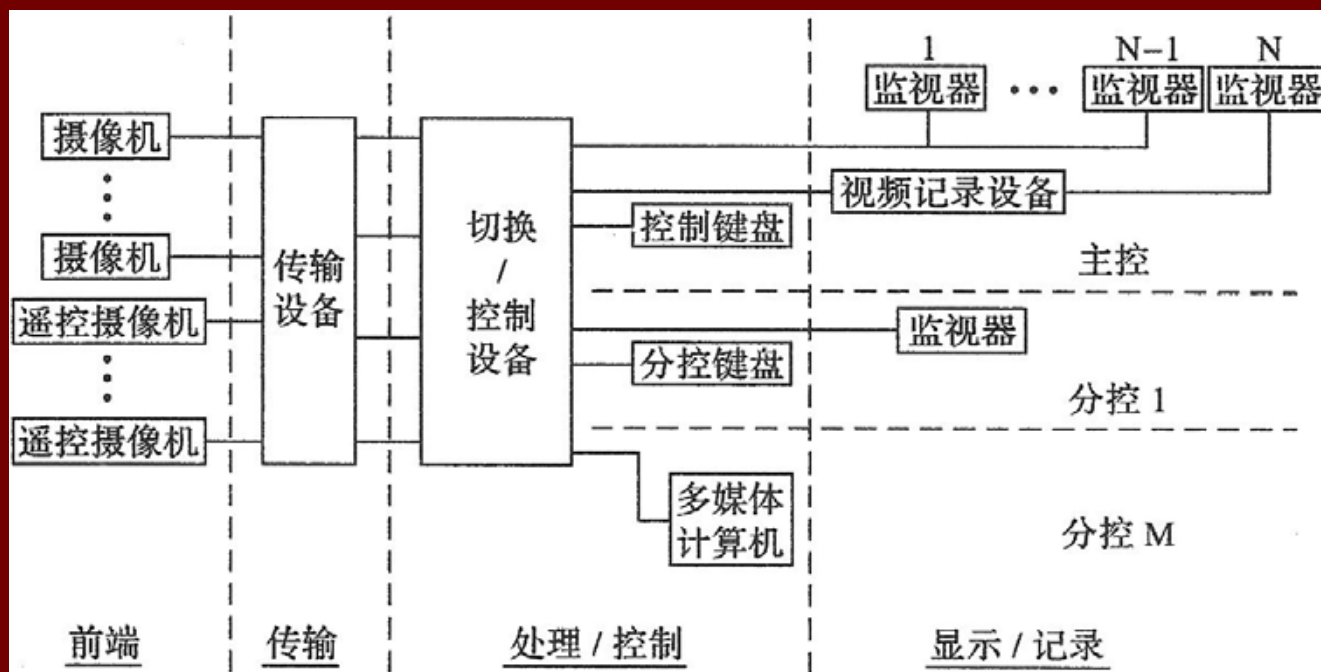


图 4.0.2-3 矩阵切换模式

4、数字视频网络虚拟交换/切换模式：模拟摄像机增加数字编码功能，被称作网络摄像机，数字视频前端也可以是别的数字摄像机。数字交换传输网络可以是以太网和**DDN**、**SDH**等传输网络。数字编码设备可采用具有记录功能的**DVR**或视频服务器，数字视频的处理、控制和记录措施可以在前端、传输和显示的任何环节实施（图**4.0.2-4**）。

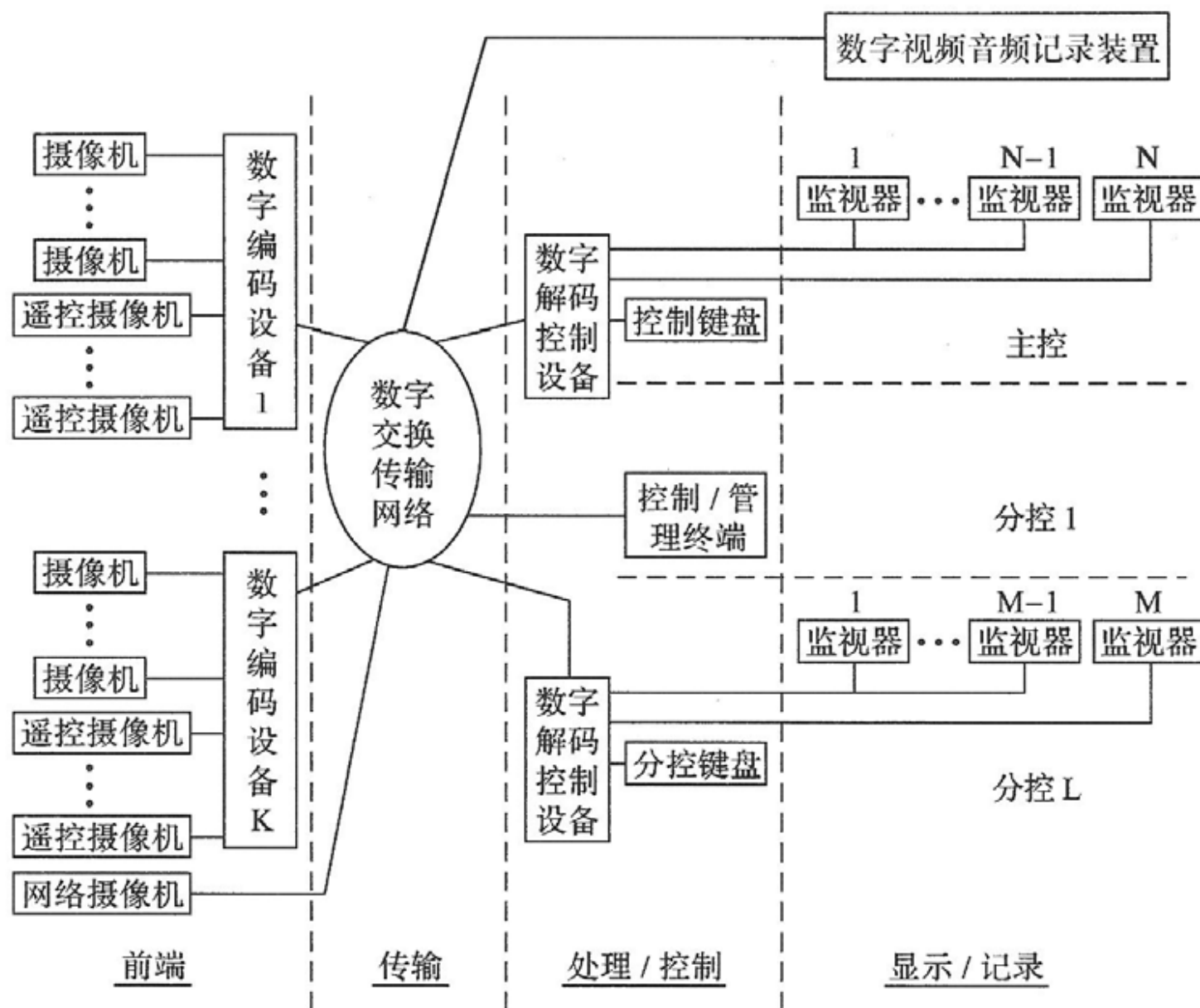


图 4.0.2-4 数字视频网络虚拟交换/切换模式

5 系统功能、性能设计

- 5.0.1 视频安防监控系统应对需要进行监控的建筑物内（外）的主要公共活动场所、通道、电梯（厅）、重要部位和区域等进行有效的视频探测与监视，图像显示、记录与回放。
- 5.0.2 前端设备的最大视频（音频）探测范围应满足现场监视覆盖范围的要求，摄像机灵敏度应与环境照度相适应，监视和记录图像效果应满足有效识别目标的要求，安装效果宜与环境相协调。
- 5.0.3 系统的信号传输应保证图像质量、数据的安全性和控制信号的准确性。

5.0.4 系统控制功能应符合下列规定：

- 1、系统应能手动或自动操作，对摄像机、云台、镜头、防护罩等的各种功能进行遥控，控制效果平稳、可靠。
- 2、系统应能手动切换或编程自动切换，对视频输入信号在指定的监视器上进行固定或时序显示，切换图像显示重建时间应能在可接受的范围内。
- 3、矩阵切换和数字视频网络虚拟交换/切换模式的系统应具有系统信息存储功能，在供电中断或关机后，对所有编程信息和时间信息均应保持。
- 4、系统应具有与其他系统联动的接口。当其他系统向视频系统给出联动信号时，系统能按照预定工作模式，切换出相应部位的图像至指定监视器上，并能启动视频记录设备，其联动响应时间不大于4s。
- 5、辅助照明联动应与相应联动摄像机的图像显示协调同步。
- 6、同时具有音频监控能力的系统宜具有视频音频同步切换的能力。
- 7、需要多级或异地控制的系统应支持分控的功能。
- 8、前端设备对控制终端的控制响应和图像传输的实时性应满足安全管理要求。

5.0.5 监视图像信息和声音信息应具有原始完整性。

5.0.6 系统应保证对现场发生的图像、声音信息的及时响应，并满足管理要求。

5.0.7 图像记录功能应符合下列规定：

1、记录图像的回放效果应满足资料的原始完整性，视频存储容量和记录 / 回放带宽与检索能力应满足管理要求。

2、系统应能记录下列图像信息：

1) 发生事件的现场及其全过程的图像信息；

2) 预定地点发生报警时的图像信息；

3) 用户需要掌握的其他现场动态图像信息。

3、系统记录的图像信息应包含图像编号 / 地址、记录时的时间和日期。

4、对于重要的固定区域的报警录像宜提供报警前的图像记录。

5、根据安全管理需要，系统应能记录现场声音信息。

5.0.8 系统监视或回放的图像应清晰、稳定，显示方式应满足安全管理要求。显示画面上应有图像编号/地址、时间、日期等。文字显示应采用简体中文。电梯轿厢内的图像显示宜包含电梯轿厢所在楼层信息和运行状态的信息。

5.0.9 具有视频移动报警的系统，应能任意设置视频警戒区域和报警触发条件。

5.0.10 在正常工作照明条件下系统图像质量的性能指标应符合以下规定：

1、模拟复合视频信号应符合以下规定：

- 视频信号输出幅度：1Vp-p， $\pm 3\text{dB}$ VBS
- 实时显示黑白电视水平清晰度： $\geq 400\text{TVL}$
- 实时显示彩色电视水平清晰度： $\geq 270\text{TVL}$
- 回放图像中心水平清晰度： $\geq 220\text{TVL}$
- 黑白电视灰度等级： ≥ 8
- 随机信噪比： $\geq 36\text{dB}$

2、数字视频信号应符合以下规定：

- 单路画面像素数量： $\geq 352 \times 288$ (CIF)
- 单路显示基本帧率： $\geq 25\text{fps}$
- 数字视频的最终显示清晰度应满足本条第1款的要求。

3、监视图像质量不应低于《民用闭路监视电视系统工程技术规范》GB50198-1994中表4.3.1-1规定的四级，回放图像质量不应低于表4.3.1-1规定的三级；在显示屏上应能有效识别目标。

CIF : common intermediate format

DCIF: double intermediate format

QCIF:quarter common intermediate format

分辨率数字监控产品中一项重要的技术指标，它在很大程度上决定了产品的性能（清晰度、存储量、带宽）和价格。能够在不增加成本和数据容量的情况下，提高录像的回放图像画质，这样的分辨率是我们所需要的。

目前监控行业中主要使用Qcif（176*144）、CIF（352*288）、HALF D1（704*288）、D1（704*576）等几种分辨率，

6 设备选型与设置

6.0.1 摄像机的选型与设置应符合以下规定：

- 1、为确保系统总体功能和总体技术指标，摄像机选型要充分满足监视目标的环境照度、安装条件、传输、控制和安全需求等因素的要求
- 2、监视目标的最低环境照度不应低于摄像机靶面最低照度的50 倍。
- 3、监视目标的环境照度不高，而要求图像清晰度较高时，宜选用黑白摄像机；监视目标的环境照度不高，且需安装彩色摄像机时，需设置附加照明装置。附加照明装置的光源光线宜避免直射摄像机镜头，以免产生晕光，并力求环境照度分布均匀，附加照明装置可由监控中心控制。
- 4、在监视目标的环境中可见光照明不足或摄像机隐蔽安装监视时，宜选用红外灯作光源。

- 5、应根据现场环境照度变化情况，选择适合的宽动态范围的摄像机；监视目标的照度变化范围大或必须逆光摄像时，宜选用具有自动电子快门的摄像机。
- 6、摄像机镜头安装宜顺光源方向对准监视目标，并宜避免逆光安装；当必须逆光安装时，宜降低监视区域的光照对比度或选用具有帘栅作用等具有逆光补偿的摄像机。
- 7、摄像机的工作温度、湿度应适应现场气候条件的变化，必要时可采用适应环境条件的防护罩。
- 8、选择数字型摄像机应符合本规范第3.0.5条，第5.0.2条，第5.0.3条，第5.0.4条第2、8款，第5.0.5条，第5.0.6条，第5.0.10条的规定。

6.0.2 镜头的选型与设置应符合以下规定（图6.0.2）：

- 1、镜头像面尺寸应与摄像机靶面尺寸相适应，镜头的接口与摄像机的接口配套。
- 2、用于固定目标监视的摄像机，可选用固定焦距镜头，监视目标离摄像机距离较大时可选用长焦镜头；在需要改变监视目标的观察视角或视场范围较大时应选用变焦距镜头；监视目标离摄像机距离近且视角较大时可选用广角镜头。

3、镜头焦距的选择根据视场大小和镜头到监视目标的距离等来确定，可参照如下公式计算：

$$f = A \times L / H \quad \text{公式 6.0.2}$$

式中：f——焦距（mm）；

A——像场高/宽（mm）；

L——镜头到监视目标的距离（mm）；

H——视场高/宽（mm）。

4、监视目标环境照度恒定或变化较小时宜选用手动可变光圈镜头。

5、监视目标环境照度变化范围高低相差达到100 倍以上，或昼夜使用的摄像机应选用自动光圈或遥控电动光圈镜头。

6、变焦镜头应满足最大距离的特写与最大视场角观察需求，并宜选用具有自动光圈、自动聚焦功能的变焦镜头。变焦镜头的变焦和聚焦响应速度应与移动目标的活动速度和云台的移动速度相适应。

7、摄像机需要隐蔽安装时应采取隐蔽措施，镜头宜采用小孔镜头或棱镜镜头。

6.0.3 云台/支架的选型与设置应符合以下规定：

- 1、根据使用要求选用云台 / 支架，并与现场环境相协调。
- 2、监视对象为固定目标时，摄像机宜配置手动云台即万向支架。
- 3、监视场景范围较大时，摄像机应配置电动遥控云台，所选云台的负荷能力应大于实际负荷的1.2 倍；云台的工作温度、湿度范围应满足现场环境要求。
- 4、云台转动停止时应具有良好的自锁性能，水平和垂直转角回差不应大于1°。
- 5、云台的运行速度（转动角速度）和转动的角度范围，应与跟踪的移动目标和搜索范围相适应。
- 6、室内型电动云台在承受最大负载时，机械噪声声强级不应大于50dB。
- 7、根据需要可配置快速云台或一体化遥控摄像机（含内置云台等）。

6.0.4 防护罩的选型与设置应符合以下规定：

- 1、根据使用要求选用防护罩，并应与现场环境相协调。
- 2、防护罩尺寸规格应与摄像机、镜头等相配套。

6.0.5 传输设备的选型与设置除应符合现行国家标准《安全防范工程技术规范》GB 50348 的相关规定外，还要符合下列规定：

- 1、传输设备应确保传输带宽、载噪比和传输时延满足系统整体指标的要求，接口应适应前后端设备的连接要求。
- 2、传输设备应有自身的安全防护措施，并宜具有防拆报警功能；对于需要保密传输的信号，设备应支持加/解密功能。
- 3、传输设备应设置于易于检修和保护的区域，并宜靠近前/后端的视频设备。

6.0.6 视频切换控制设备的选型应符合以下规定：

- 1、视频切换控制设备的功能配置应满足使用和冗余要求。
- 2、视频输入接口的最低路数应留有一定的冗余量。
- 3、视频输出接口的最低路数应根据安全管理需求和显示、记录设备的配置数量确定。
- 4、视频切换控制设备应能手动或自动操作，对镜头、电动云台等的各种动作（如转向、变焦、聚焦、光圈等动作）进行遥控。
- 5、视频切换控制设备应能手动或自动编程切换，对所有输入视频信号在指定的监视器上进行固定或时序显示。
- 6、视频切换控制设备应具有配置信息存储功能，在供电中断或关机后，对所有编程设置、摄像机号、地址、时间等均可记忆，在开机或电源恢复供电后，系统应恢复正常工作。
- 7、视频切换控制设备应具有与外部其他系统联动的接口。当与报警控制设备联动时应能切换出相应部位摄像机的图像，并显示记录。
- 8、具有系统操作密码权限设置和中文菜单显示。
- 9、具有视频信号丢失报警功能。
- 10、当系统有分控要求时，应根据实际情况分配控制终端如控制键盘及视频输出接口等，并根据需要确定操作权限功能。
- 11、大型综合安防系统宜采用多媒体技术，做到文字、动态报警信息、图表、图像、系统操作在同一套计算机上完成。

6.0.7 记录与回放设备的选型与设置应符合以下规定：

1、宜选用数字录像设备，并宜具备防篡改功能；其存储容量和回放的图像

（和声音）质量应满足相关标准和管理使用要求。

2、在同一系统中，对于磁带录像机和记录介质的规格应一致。

3、录像设备应具有联动接口。

4、在录像的同时需要记录声音时，记录设备应能同步记录图像和声音，并可同步回放。

5、图像记录与查询检索设备宜设置在易于操作的位置。

6.0.8 数字视频音频设备的选型与设置应符合以下规定：

- 1、视频探测、传输、显示和记录等数字视频设备符合本规范第3.0.5条，第5.0.2条，第5.0.3条，第5.0.4条第2、8款，第5.0.5条，第5.0.6条，第5.0.10条的规定。
- 2、宜具有联网和远程操作、调用的能力。
- 3、数字视频音频处理设备，其分析处理的结果应与原有视频音频信号对应特征保持一致。其误判率应在可接受的范围内。

6.0.8 数字视频音频设备的选型与设置应符合以下规定：

- 1、视频探测、传输、显示和记录等数字视频设备符合本规范第3.0.5条，第5.0.2条，第5.0.3条，第5.0.4条第2、8款，第5.0.5条，第5.0.6条，第5.0.10条的规定。
- 2、宜具有联网和远程操作、调用的能力。
- 3、数字视频音频处理设备，其分析处理的结果应与原有视频音频信号对应特征保持一致。其误判率应在可接受的范围内。

6.0.9 显示设备的选型与设置应符合以下规定：

- 1、选用满足现场条件和使用要求的显示设备。
- 2、显示设备的清晰度不应低于摄像机的清晰度，宜高出100TVL。
- 3、操作者与显示设备屏幕之间的距离宜为屏幕对角线的4~6倍，显示设备的屏幕尺寸宜为230mm 到635mm。根据使用要求可选用大屏幕显示设备等。
- 4、显示设备的数量，由实际配置的摄像机数量和管理要求来确定。
- 5、在满足管理需要和保证图像质量的情况下，可进行多画面显示。多台显示设备同时显示时，宜安装在显示设备柜或电视墙内，以获取较好的观察效果。
- 6、显示设备的设置位置应使屏幕不受外界强光直射。当有不可避免的强光入射时，应采取相应避光措施。
- 7、显示设备的外部调节旋钮/按键应方便操作。
- 8、显示设备的设置应与监控中心的设计统一考虑，合理布局，方便操作，易于维修。

6.0.10 控制台的选型与设置应符合以下规定：

- 1、根据现场条件和使用要求，选用适合形式的控制台。**
- 2、控制台的设计应满足人机工程学要求；控制台的布局、尺寸、台面及座椅的高度应符合现行国家标准《电子设备控制台的布局、形式和基本尺寸》GB7269 的规定。**

7 传输方式、线缆选型与布线

7.0.1 传输方式除应符合现行国家标准《安全防范工程技术规范》GB 50348 的相关规定外，对有安全保密要求的传输方式还应采取信号加密措施。

7.0.2 线缆选择除应符合现行国家标准《安全防范工程技术规范》GB 50348 的相关规定外，还应符合下列规定：

- 1、模拟视频信号宜采用同轴电缆，根据视频信号的传输距离、端接设备的信号适应范围和电缆本身的衰耗指标等确定同轴电缆的型号、规格；信号经差分处理，也可采用不劣于五类线性能的双绞线传输。
- 2、数字视频信号的传输按照数字系统的要求选择线缆。
- 3、根据线缆的敷设方式和途经环境的条件确定线缆型号、规格。

7.0.3 布线设计应符合现行国家标准《安全防范工程技术规范》GB 50348 的相关规定。

8 供电、防雷与接地

8.0.1 系统供电除应符合现行国家标准《安全防范工程技术规范》GB 50348 的相关规定外，还应符合以下规定：

- 1、摄像机供电宜由监控中心统一供电或由监控中心控制的电源供电。
- 2、异地的本地供电，摄像机和视频切换控制设备的供电宜为同相电源，或采取措施以保证图像同步。
- 3、电源供电方式应采用TN-S 制式。

8.0.2 系统防雷与接地除应符合现行国家标准《安全防范工程技术规范》GB50348 的相关规定外，还应符合下列规定：

- 1、采取相应隔离措施，防止地电位不等引起图像干扰。
- 2、室外安装的摄像机连接电缆宜采取防雷措施。

9 系统安全性、可靠性、电磁兼容性、环境适应性

9.0.1 系统安全性除应符合现行国家标准《安全防范工程技术规范》GB 50348 的相关规定外，还应符合以下规定：

- 1、具有视频丢失检测示警能力。
- 2、系统选用的设备不应引入安全隐患和对防护对象造成损害。

9.0.2 系统可靠性应符合现行国家标准《安全防范工程技术规范》GB 50348 的相关规定。

9.0.3 系统电磁兼容性应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定，选用的控制、显示、记录、传输等主要设备的电磁兼容性应符合电磁兼容试验和测量技术系列标准的规定，其严酷等级应满足现场电磁环境的要求。

9.0.4 系统环境适应性应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定。

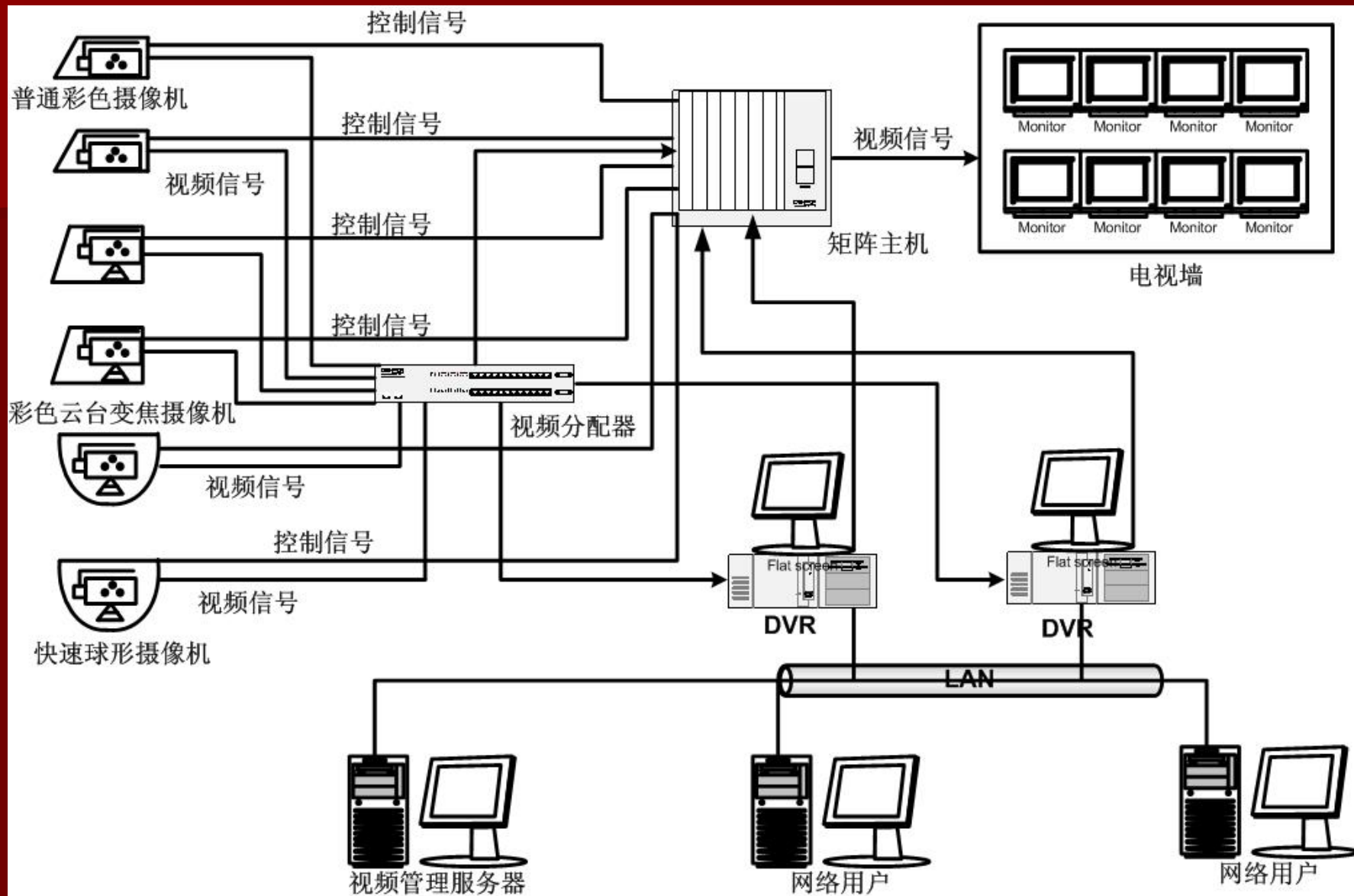
1 0 监控中心

10.0.1 监控中心的设置应符合现行国家标准《安全防范工程技术规范》GB 50348的相关规定。

10.0.2 对监控中心的门窗应采取防护措施。

10.0.3 监控中心宜设置独立设备间，保证监控中心的散热、降噪。

10.0.4 监控中心宜设置视频监控装置和出入口控制装置。



●今后的发展方向

1、数字化

2、网络化

3、视频行为分析技术

4、视频图像识别技术

出入口控制系统

GB50396-2007

2术语

2.0.1出入口控制系统access control system(ACS)利用自定义符识别或 / 和模式识别技术对出入口目标进行识别并控制出入口执行机构启闭的电子系统或网络。

2.0.2目标object通过出入口且需要加以控制的人员和 / 或物品。

2.0.3目标信息object information赋予目标或目标特有的、能够识别的特征信息。数字、字符、图形图像、人体生物特征、物品特征、时间等均可成为目标信息。

2.0.4钥匙key用于操作出入口控制系统、取得出入权的信息和 / 或其载体。钥匙所表征的信息可以具有表示人和 / 或物的身份、通行的权限、对系统的操作权限等单项或多项功能。

2.0.5自定义特征信息识别

1人员编码识别human coding identification通过编码识别(输入)装置获取目标人员的个人编码信息的一种识别。

2物品编码识别article coding identification通过编码识别(输入)装置读取目标物品附属的编码载体而对该物品信息的一种识别。

2.0.6模式特征信息识别

1人体生物特征信息human body biologic chamcteristic目标人员个体与生俱有的、不可模仿或极难模仿的那些体态特征信息或行为，且可以被转变为目标独有特征的信息。

2人体生物特征信息识别human body biologic chamcteristic identi±ication采用生物测定(统计)学方法，获取目标人员的生物特征信息并对该信息进行的识别。

3物品特征信息article chamcteristic目标物品特有的物理、化学等特性且可被转变为目标独有特征的信息。

4物品特征信息识别article chamcteristic identification通过辨识装置对预定物品特征信息进行的识别。

2.0.7密钥、密钥量与密钥差异key-code, amount of key-code, difference of key-code

可以构成单个钥匙的目标信息即为密钥。系统理论上可具有的所有钥匙所表征的全体密钥数量即为系统密钥量。如果某系统具有不同种类的、权限并重的钥匙，则分别计算各类钥匙的密钥量，取其中密钥量最低的作为系统的密钥量。构成单个钥匙的目标信息之间的差别即为密钥差异。

2.0.8钥匙的授权**key authorization**准许某系统中某种或某个、某些钥匙的操作。

2.0.9误识**false identification**系统将某个钥匙识别为该系统其他钥匙，包括误识进入和误识拒绝，通常以误识率表示。

2.0.10拒认**refuse identification**系统对某个经正常操作的本系统钥匙未做出识别响应，通常以拒认率表示。

2.0.11识读现场**identification locale**对钥匙进行识读的场所和 / 或环境。

2.0.12识读现场设备**locale identify equipment**在识读现场的、出入目标可以接触到的、有防护面的设备(装置)。

2.0.13防护面**protection surface**设备完成安装后，在识读现场可能受到人为被破坏或被实施技术开启，因而需加以防护的设备的结构面。

2.0.14防破坏能力**anti destroyed ability**在系统完成安装后，具有防护面的设备(装置)抵御专业技术人员使用规定工具实施破坏性攻击，即出入**13**不被开启的能力(以抵御出入口被开启所需要的净工作时间表示)。

2.0.15防技术开启能力**anti technical opened ability**在系统完成安装后，具有防护面的设备(装置)抵御专业技术人员使用规定工具实施技术开启(如各种试探、扫描、模仿、干扰等方法使系统误识或误动作而开启)，即出入**EI**不被开启的能力(以抵御出入口被开启所需要的净工作时间表示)。

2.0.16复合识别**combination identification**系统对某目标的出入行为采用两种或两种以上的信息识别方式并进行逻辑相与判断的一种识别方式。

2.0.17防目标重入**anti pass-back**能够限制经正常操作已通过某出入口的目标，未经正常通行轨迹而再次操作又通过该出入口的一种控制方式。

2.0.18多重识别控制multi-identification control系统采用某一种识别方式，需同时或在约定时间内对两个或两个以上目标信息进行识别后才能完成对某一出入口实施控制的一种控制方式。

2.0.19异地核准控制remote approve control系统操作人员(管理人员)在非识读现场(通常是控制中心)对虽能通过系统识别、允许出入的目标进行再次确认，并针对此目标遥控关闭或开启某出入口的一种控制方式。

2.0.20受控区、同级别受控区、高级别受控区controlled area, the same level controlled area, high level controlled area如果某一区域只有一个(或同等作用的多个)出入口，则该区域视为这一个(或这些)出入口的受控区，即：某一个(或同等作用的多个)出入口所限制出入的对应区域，就是它(它们)的受控区。具有相同出入限制的多个受控区，互为同级别受控区。具有比某受控区的出入限制更为严格的其他受控区，是相对于该受控区的高级别受控区。

3基本规定

3.0.1出入口控制系统工程的设计应符合国家现行标准《安全防范工程技术规范》GB50348和《出入口控制系统技术要求》GA / T394的相关规定。

3.0.2出入口控制系统的工程设计应综合应用编码与模式识别、有线 / 无线通讯、显示记录、机电一体化、计算机网络、系统集成等技术，构成先进、可靠、经济、适用、配套的出入口控制应用系统。

3.0.3出入口控制系统中使用的设备必须符合国家法律法规和现行强制性标准的要求，并经法定机构检验或认证合格。

3.0.4出入口控制系统工程的设计，应符合下列要求：

1根据防护对象的风险等级和防护级别、管理要求、环境条件和工程投资等因素，确定系统规模和构成；根据系统功能要求、出入目标数量、出人权限、出入时间段等因素来确定系统的设备选型与配置。

2出入口控制系统的设置必须满足消防规定的紧急逃生时人员疏散的相关要求。

3供电电源断电时系统闭锁装置的启闭状态应满足管理要求。

4执行机构的有效开启时间应满足出入口流量及人员、物品的安全要求。

5系统前端设备的选型与设置，应满足现场建筑环境条件和防破坏、防技术开启的要求。

6当系统与考勤、计费及目标引导(车库)等一卡通联合设置时，必须保证出入口控制系统的安全性要求。

3.0.5系统兼容性应满足设备互换的要求，系统可扩展性应满足简单扩容和集成的要求。

3.0.6出入口控制系统工程的设计流程与深度应符合附录A的规定。设计文件应准确、完整、规范。

4 系统构成

4.0.1 出入口控制系统主要由识读部分、传输部分、管理 / 控制部分和执行部分以及相应的系统软件组成。系统有多种构建模式，可根据系统规模、现场情况、安全管理要求等，合理选择。

4.0.2 出入口控制系统按其硬件构成模式可分为以下型式：

1 一体型：出入口控制系统的各个组成部分通过内部连接、组合或集成在一起，实现出入口控制的所有功能(图4.0.2—1)。

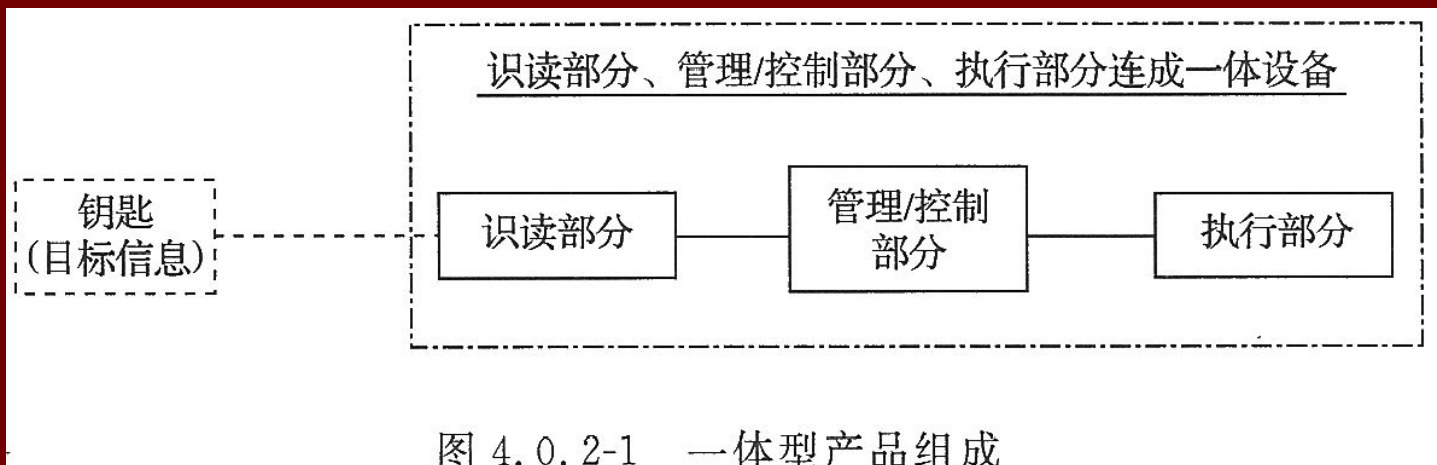
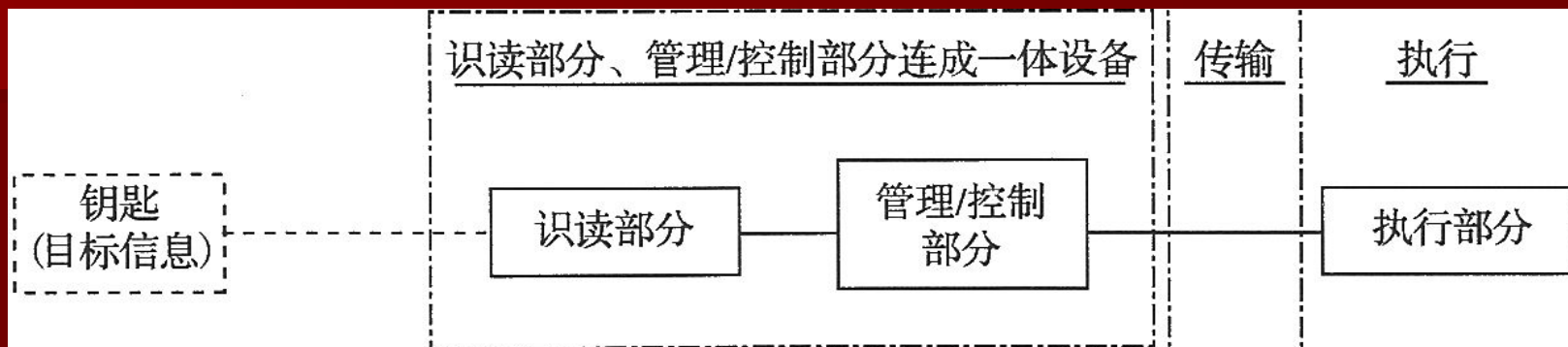
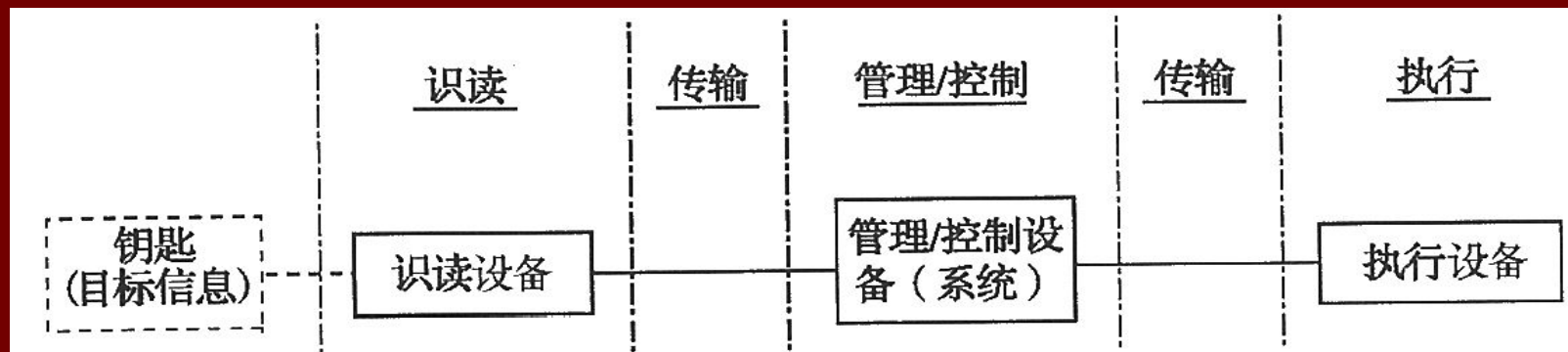


图 4.0.2-1 一体型产品组成

2分体型：出入口控制系统的各个组成部分，在结构上有分开的部分，也有通过不同方式组合的部分。分开部分与组合部分之间通过电子、机电等手段连成为一个系统，实现出入口控制的所有功能[图4.0.2-2(a)、(b)]。



(a)分体型结构组成之一



(b)分体型结构组成之二

图 4.0.2-2 分体型结构组成

4.0.3出入口控制系统按其管理 / 控制方式可分为以下型式:

1独立控制型: 出入口控制系统, 其管理与控制部分的全部显示 / 编程 / 管理 / 控制等功能均在一个设备(出入口控制器)内完成(图4.0.3-1)。

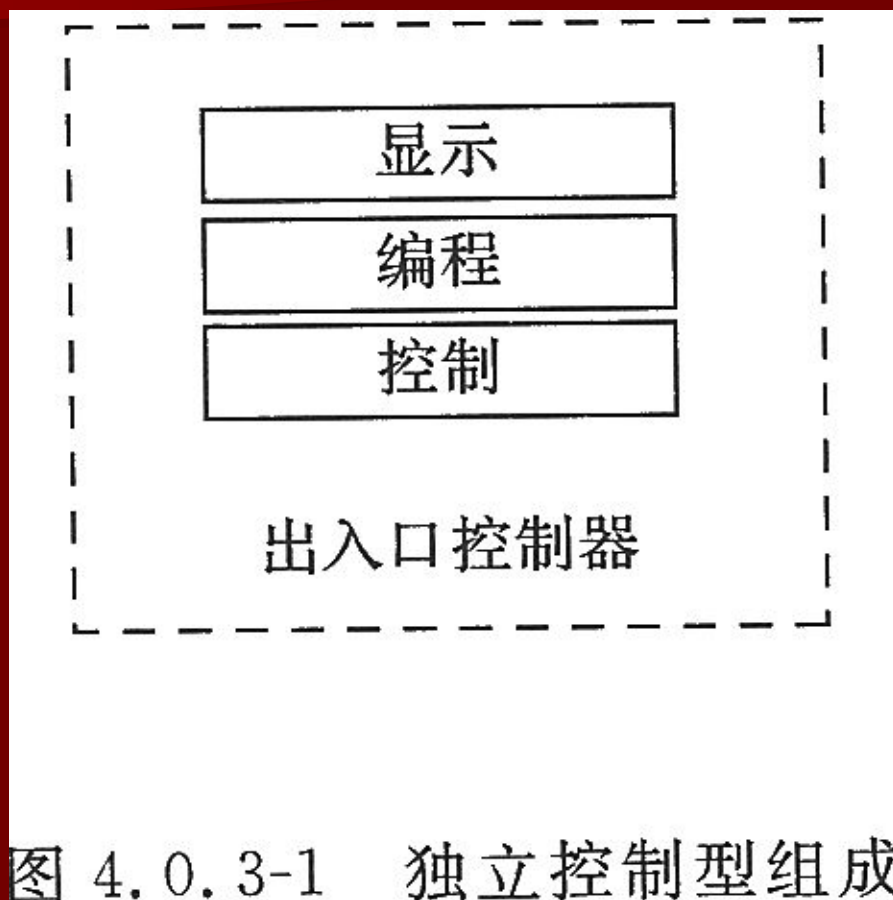
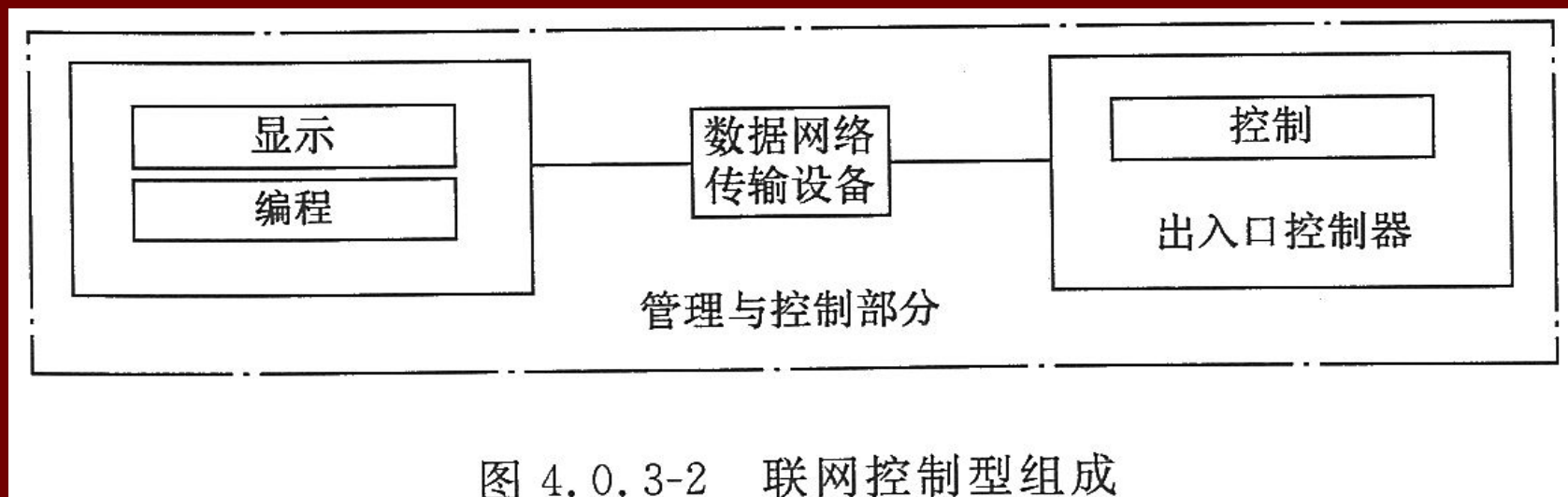


图 4.0.3-1 独立控制型组成

2联网控制型：出入口控制系统，其管理与控制部分的全部显示 / 编程 / 管理 / 控制功能不在一个设备(出入口控制器)内完成。其中，显示 / 编程功能由另外的设备完成。设备之间的数据传输通过有线和 / 或无线数据通道及网络设备实现(图4.0.3-2)。



3数据载体传输控制型：出入口控制系统与联网型出入口控制系统区别仅在于数据传输的方式不同，其管理与控制部分的全部显示 / 编程 / 管理 / 控制等功能不是在一个设备(出入口控制器)内完成。其中，显示 / 编程工作由另外的设备完成。设备之间的数据传输通过对可移动的、可读写的数据载体的输入 / 导出操作完成(图4.0.3-3)。

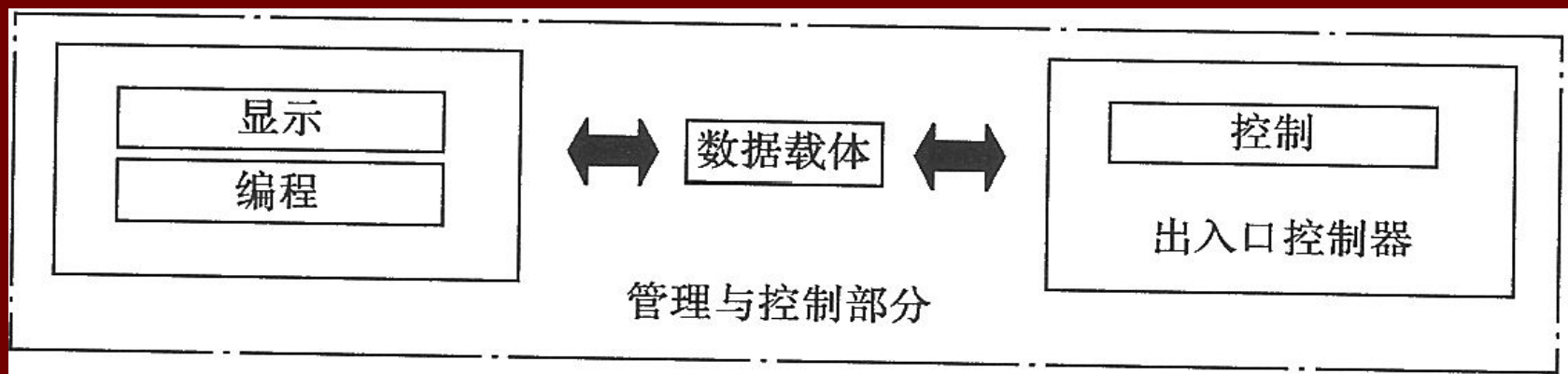
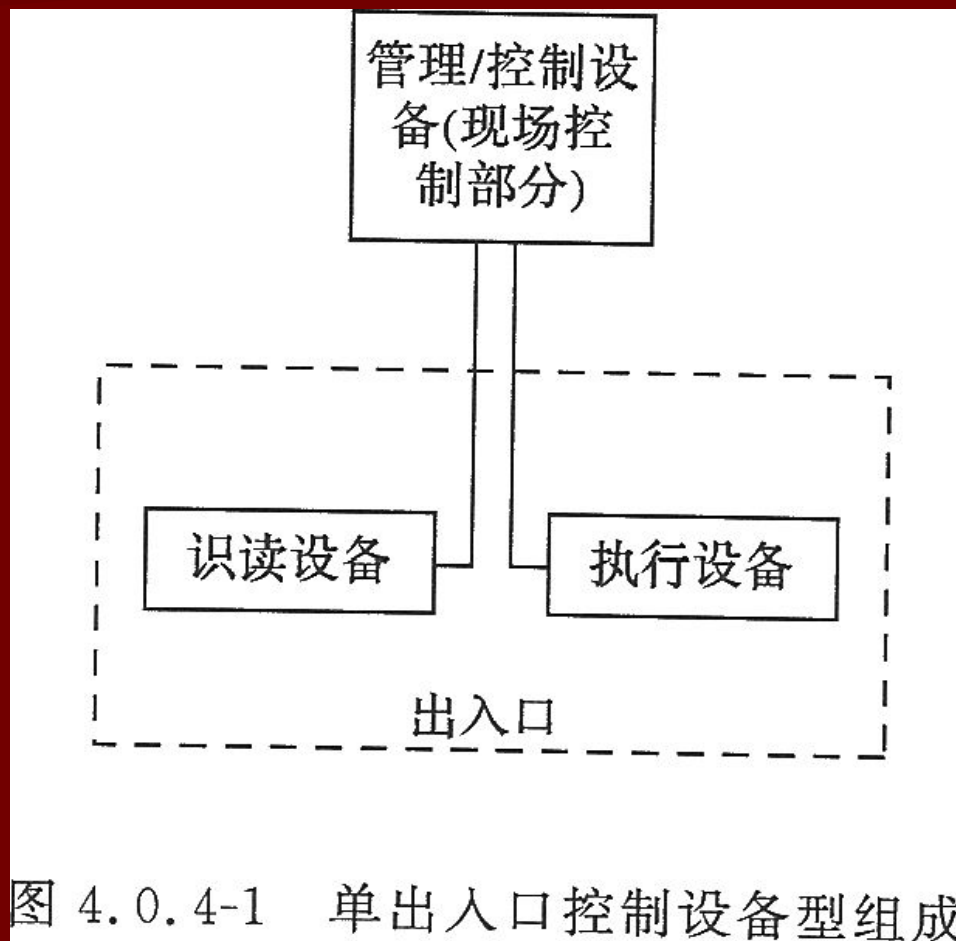


图 4.0.3-3 数据载体传输控制型组成

4.0.4出入口控制系统按现场设备连接方式可分为以下型式：

1单出入口控制设备：仅能对单个出入口实施控制的单个出入口控制器所构成的控制设备(图4.0.4-1)。



2多出入口控制设备：能同时对两个以上出入口实施控制的单个出入口控制器所构成的控制设备(图4.0.4-2)。

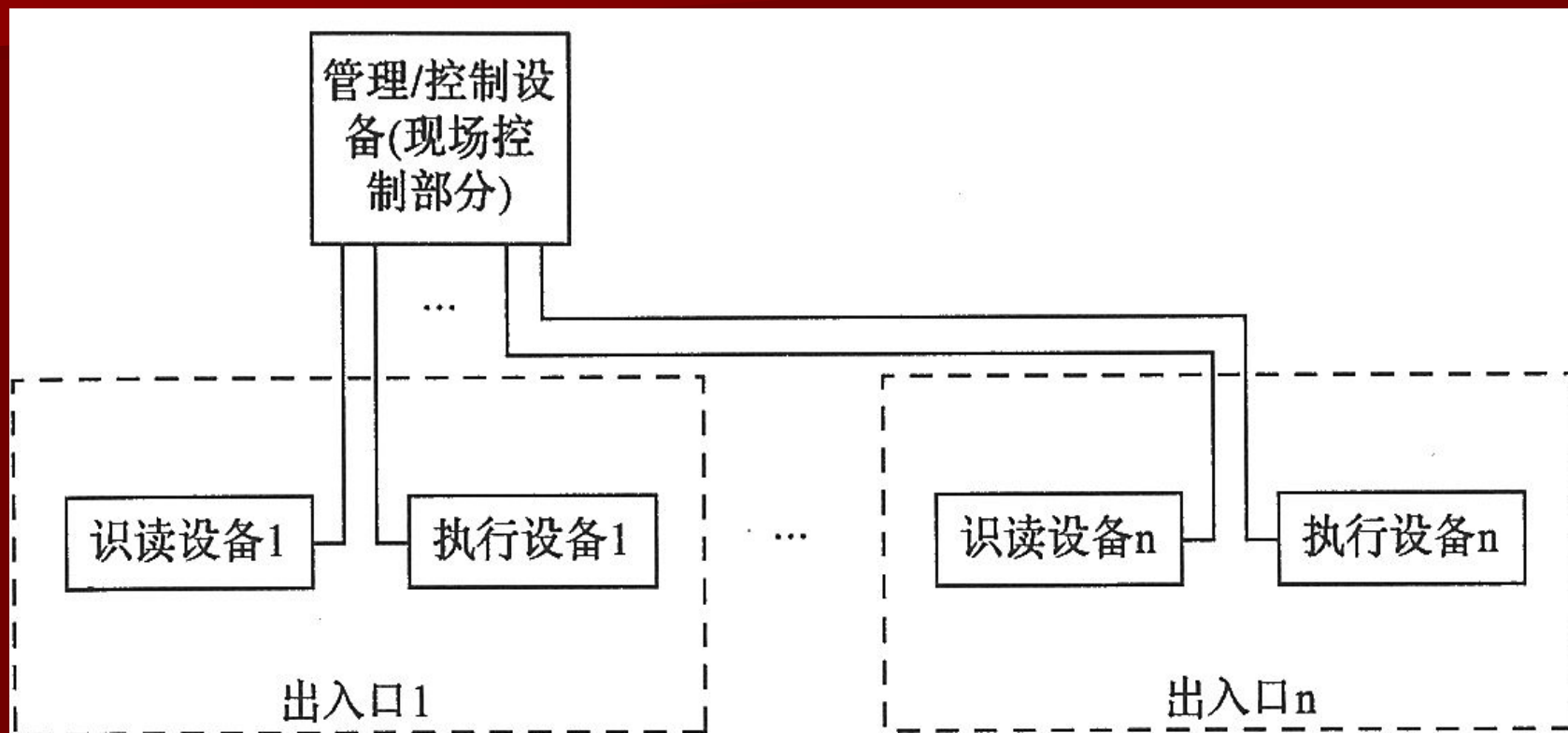


图 4.0.4-2 多出入口控制设备型组成

4.0.5 出入口控制系统按联网模式可分为以下型式:

1 总线制: 出入口控制系统的现场控制设备通过联网数据总线与出入口管理中心的显示、编程设备相连, 每条总线在出入口管理中心只有一个网络接口(图4.0.5-1)。

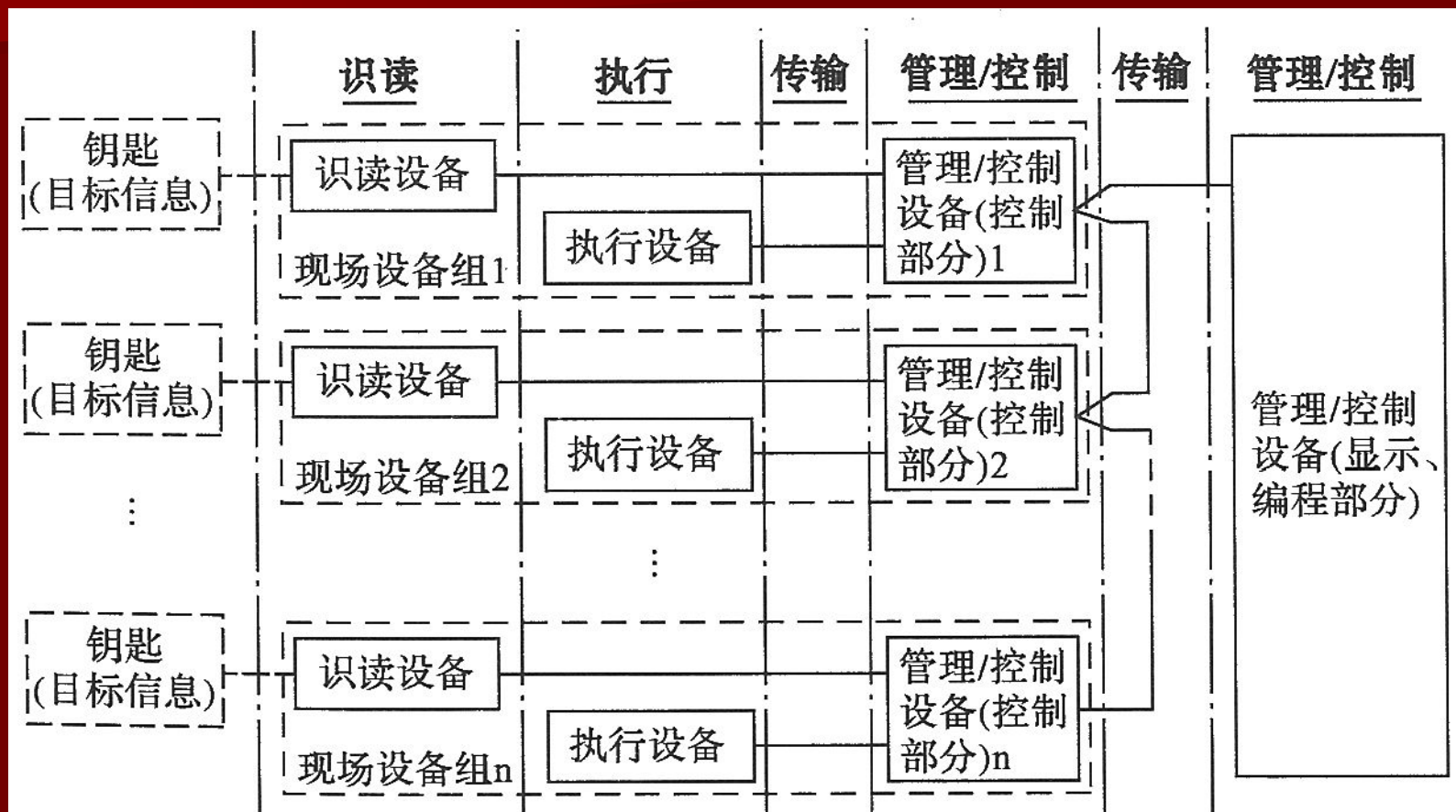


图 4.0.5-1 总线制系统组成

2环线制：出入口控制系统的现场控制设备通过联网数据总线与出入口管理中心的显示、编程设备相连，每条总线在出入口管理中心有两个网络接口，当总线有一处发生断线故障时，系统仍能正常工作，并可探测到故障的地点(图4.0.5-2)。

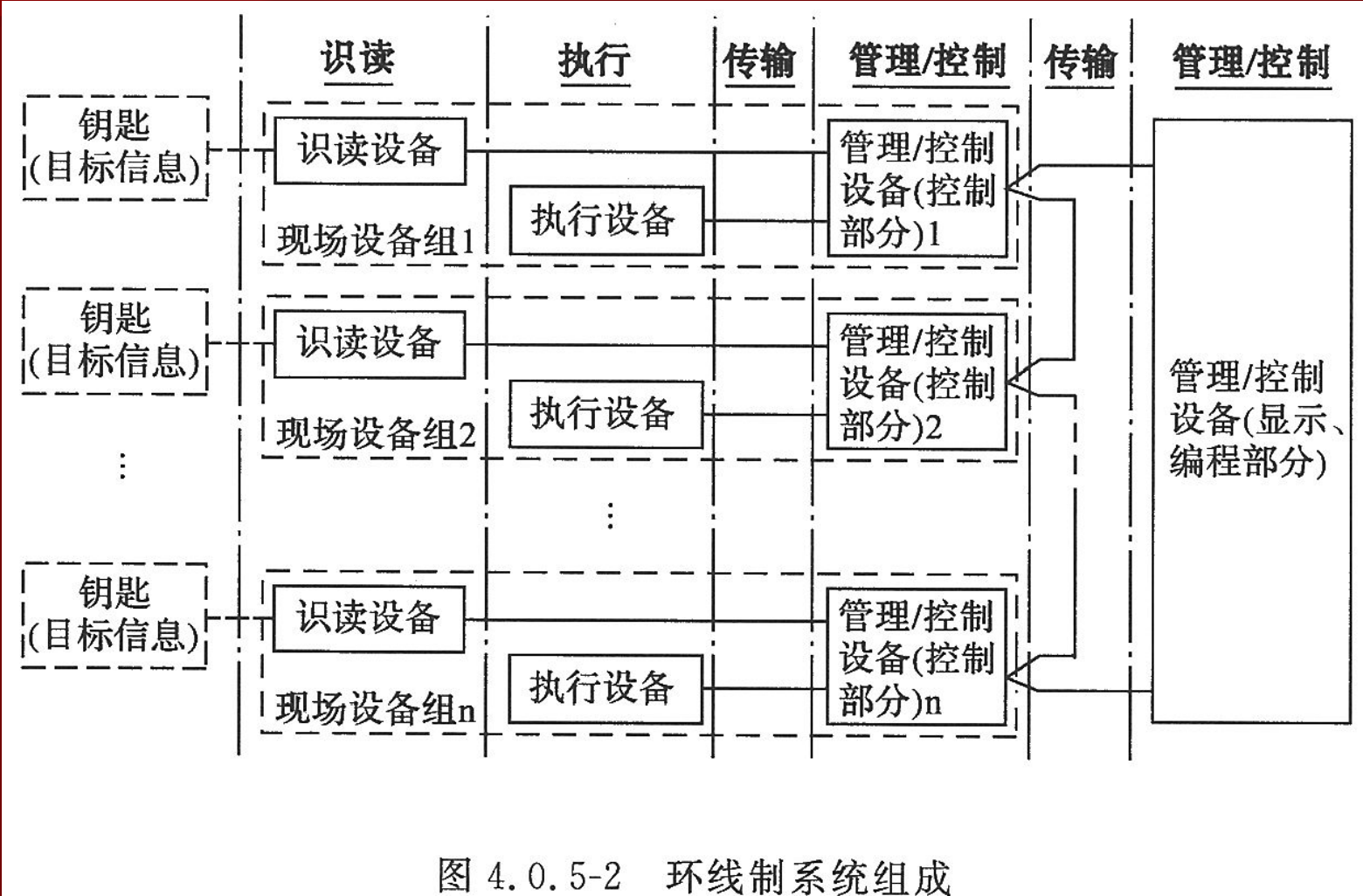


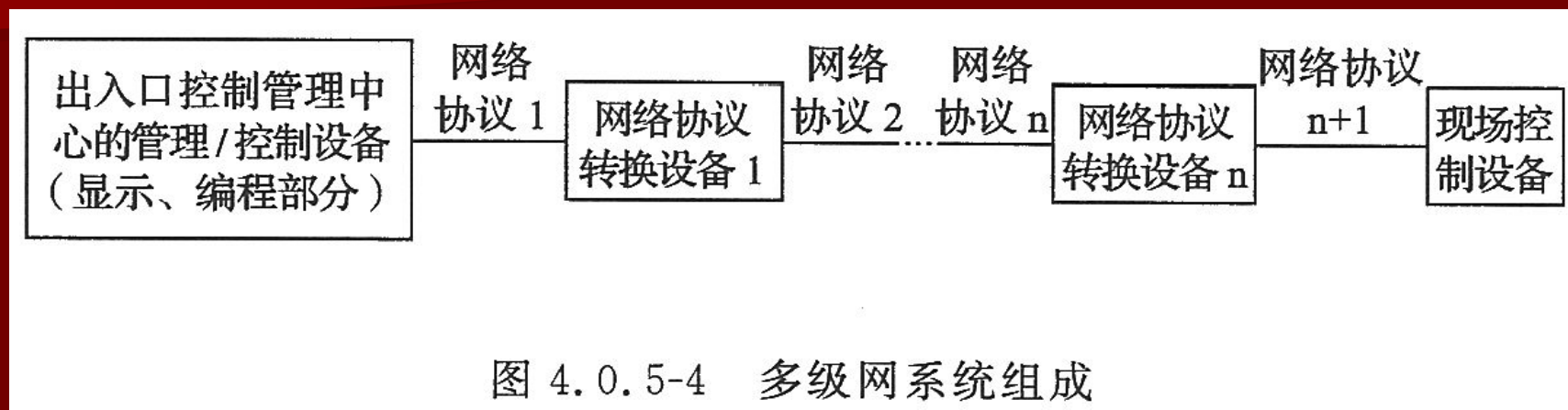
图 4.0.5-2 环线制系统组成

3单级网：出入口控制系统的现场控制设备与出入口管理中心的显示、编程设备的连接采用单一联网结构(图4.0.5-3)。



图 4.0.5-3 单级网系统组成示意图

4多级网：出入口控制系统的现场控制设备与出入口管理中心的显示、编程设备的连接采用两级以上串联的联网结构，且相邻两级网络采用不同的网络协议(图4.0.5-4)。



5 系统功能、性能设计

5.1 一般规定

5.1.1 系统的防护能力由所用设备的防护面外壳的防护能力、防破坏能力、防技术开启能力以及系统的控制能力、保密性等因素决定。系统设备的防护能力由低到高分A、B、C三个等级，分级方法宜符合附录B的规定。

5.1.2 系统响应时间应符合下列规定：

1 系统的下列主要操作响应时间应不大于2s。

1) 在单级网络的情况下，现场报警信息传输到出入口管理中心的响应时间。

2) 除工作在异地核准控制模式外，从识读部分获取一个钥匙的完整信息始至执行部分开始启闭出入口动作的时间。

3) 在单级网络的情况下，操作(管理)员从出入口管理中心发出启闭指令始至执行部分开始启闭出入口动作的时间。

4) 在单级网络的情况下，从执行异地核准控制后到执行部分开始启闭出入口动作的时间。

2 现场事件信息经非公共网络传输到出入口管理中心的响应时间应不大于5s。

5.1.3 系统计时、校时应符合下列规定：

1 非网络型系统的计时精度应小于 $5s / d$ ；网络型系统的中央管理主机的计时精度应小于 $5s / d$ ，其他的与事件记录、显示及识别信息有关的各计时部件的计时精度应小于 $10s / d$ 。

2 系统与事件记录、显示及识别信息有关的计时部件应有校时功能；在网络型系统中，运行于中央管理主机的系统管理软件每天宜设置向其他的与事件记录、显示及识别信息有关的各计时部件校时功能。

5.1.4系统报警功能分为现场报警、向操作(值班)员报警、异地传输报警等。报警信号应为声光提示。

5.1.5在发生以下情况时，系统应报警：

- 1当连续若干次(最多不超过5次，具体次数应在产品说明书中规定)在目标信息识读设备或管理与控制部分上实施错误操作时；
- 2当未使用授权的钥匙而强行通过出入口时；
- 3当未经正常操作而使出入口开启时；
- 4当强行拆除和 / 或打开B、C级的识读现场装置时；
- 5当B、C级的主电源被切断或短路时；
- 6当C级的网络型系统的网络传输发生故障时。

5.1.6系统应具有应急开启功能，可采用下列方法：

- 1使用制造厂特制工具采取特别方法局部破坏系统部件后，使出入口应急开启，且可迅即修复或更换被破坏部分。
- 2采取冗余设计，增加开启出入口通路(但不得降低系统的各项技术要求)以实现应急开启。

5.1.7软件及信息保存应符合下列规定：

- 1除网络型系统的中央管理机外，需要的所有软件均应保存到固态存储器中。
- 2具有文字界面的系统管理软件，其用于操作、提示、事件显示等的文字应采用简体中文。
- 3当供电不正常、断电时，系统的密钥(钥匙)信息及各记录信息不得丢失。
- 4当系统与考勤、计费及目标引导(车库)等一卡通联合设置时，软件必须确保出入口控制系统的安全管理要求。

5.1.8系统应能独立运行，并应能与电子巡查、入侵报警、视频安防监控等系统联动，宜与安全防范系统的监控中心联网。

5.2各部分功能、性能设计

5.2.1识读部分应符合下列规定：

- 1识读部分应能通过识读现场装置获取操作及钥匙信息并对目标进行识别，应能将信息传递给管理与控制部分处理，宜能接受管理与控制部分的指令。
- 2“误识率”、“识读响应时间”等指标，应满足管理要求。
- 3对识读装置的各种操作和接受管理 / 控制部分的指令等，识读装置应有相应的声和 / 或光提示。
- 4识读装置应操作简便，识读信息可靠。

5.2.2管理 / 控制部分应符合下列规定：

- 1系统应具有对钥匙的授权功能，使不同级别的目标对各个出入口有不同的出入权限。
- 2应能对系统操作(管理)员的授权、登录、交接进行管理，并设定操作权限，使不同级别的操作(管理)员对系统有不同的操作能力。
- 3事件记录：
 - 1)系统能将出入事件、操作事件、报警事件等记录存储于系统的相关载体中，并能形成报表以备查看。
 - 2)事件记录应包括时间、目标、位置、行为。其中时间信息应包含：年、月、日、时、分、秒，年应采用千年记法。
 - 3)现场控制设备中的每个出入口记录总数：A级不小于32条，B、C级不小于1000条。
 - 4)中央管理主机的事件存储载体，应至少能存储不少于180d的事件记录，存储的记录应保持最新的记录值。
 - 5)经授权的操作(管理)员可对授权范围内的事件记录、存储于系统相关载体中的事件信息，进行检索、显示和 / 或打印，并可生成报表。
- 4与视频安防监控系统联动的出入口控制系统，应在事件查询的同时，能回放与该出入口关联的视频图像。

5.2.3执行部分功能设计应符合下列规定：

- 1闭锁部件或阻挡部件在出入口关闭状态和拒绝放行时，其闭锁力、阻挡范围等性能指标应满足使用、管理要求。
- 2出入准许指示装置可采用声、光、文字、图形、物体位移等多种指示。其准许和拒绝两种状态应易于区分。
- 3出入口开启时出入目标通过的时限应满足使用、管理要求。

6设备选型与设置

6.0.1设备选型应符合以下要求：

- 1防护对象的风险等级、防护级别、现场的实际情况、通行流量等要求。
- 2安全管理要求和设备的防护能力要求。
- 3对管理 / 控制部分的控制能力、保密性的要求。
- 4信号传输条件的限制对传输方式的要求。
- 5出入目标的数量及出入口数量对系统容量的要求。
- 6与其他子系统集成的要求。

6.0.2设备的设置应符合下列规定：

- 1识读装置的设置应便于目标的识读操作。
- 2采用非编码信号控制和 / 或驱动执行部分的管理与控制设备，必须设置于该出入口的对应受控区、同级别受控区或高级别受控区内。

6.0.3设备选型宜符合附录B、附录C、附录D的要求。

7 传输方式、线缆选型与布线

7.0.1 传输方式除应符合现行国家标准《安全防范工程技术规范》GB 50348的有关规定外，还应考虑出入口控制点位分布、传输距离、环境条件、系统性能要求及信息容量等因素。

7.0.2 线缆的选型除应符合现行国家标准《安全防范工程技术规范》GB 50348的有关规定外，还应符合下列规定：

1 识读设备与控制器之间的通信用信号线宜采用多芯屏蔽双绞线。

2 门磁开关及出门按钮与控制器之间的通信用信号线，线芯最小截面积不宜小于 0.50mm^2 。

3 控制器与执行设备之间的绝缘导线，线芯最小截面积不宜小于 0.75mm^2 。

4 控制器与管理主机之间的通讯用信号线宜采用双绞铜芯绝缘导线，其线径根据传输距离而定，线芯最小截面积不宜小于 0.50mm^2 。

7.0.3 布线设计应符合现行国家标准《安全防范工程技术规范》GB50348的有关规定。

7.0.4 执行部分的输入电缆在该出入口的对应受控区、同级别受控区或高级别受控区外的部分，应封闭保护，其保护结构的抗拉伸、抗弯折强度应不低于镀锌钢管。

8供电、防雷与接地

8.0.1供电设计除应符合现行国家标准《安全防范工程技术规范》GB 50348的有关规定外，还应符合下列规定：

1主电源可使用市电或电池。备用电源可使用二次电池及充电器、UPS电源、发电机。如果系统的执行部分为闭锁装置，且该装置的工作模式为断电开启，B、C级的控制设备必须配置备用电源。

2当电池作为主电源时，其容量应保证系统正常开启10000次以上。

3备用电源应保证系统连续工作不少于48h，且执行设备能正常开启50次以上。

8.0.2防雷与接地除应符合现行国家标准《安全防范工程技术规范》GB50348的相关规定外，还应符合下列规定：

1置于室外的设备宜具有防雷保护措施。

2置于室外的设备输入、输出端口宜设置信号线路浪涌保护器。

3室外的交流供电线路、控制信号线路宜有金属屏蔽层并穿钢管埋地敷设，钢管两端应接地。

9.0.1 系统安全性设计除应符合现行国家标准《安全防范工程技术规范》GB 50348的有关规定外，还应符合下列规定：

1系统的任何部分、任何动作以及对系统的任何操作不应对出入目标及现场管理、操作人员的安全造成危害。

2系统必须满足紧急逃生时人员疏散的相关要求。当通向疏散通道方向为防护面时，系统必须与火灾报警系统及其他紧急疏散系统联动，当发生火灾或需紧急疏散时，人员不使用钥匙应能迅速安全通过。

9.0.2 系统可靠性设计应符合现行国家标准《安全防范工程技术规范》GB50348的有关规定。

9.0.3 系统电磁兼容性设计应符合现行国家标准《安全防范工程技术规范》GB50348的有关规定，并符合现场电磁环境的要求。

9.0.4 系统环境适应性设计应符合现行国家标准《安全防范工程技术规范》GB50348的有关规定，并符合现场地域环境的要求。

10 监控中心

10.0.1 监控中心应符合现行国家标准《安全防范工程技术规范》GB50348的有关规定。

10.0.2 当出入口控制系统与安全防范系统的其他子系统联合设置时，中心控制设备应设置在安全防范系统的监控中心。

10.0.3 当出入口控制系统的监控中心不是系统最高级别受控区时，应加强对管理主机、网络接口设备、网络线缆的保护，应有对监控中心的监控录像措施。

3.0.4出入口控制系统的设计，应充分考虑“安全”因素，英文“Security”和“Safety”翻译成中文都是“安全”，但它们的含义有所不同，“Security”是“安全”的社会属性，“Safety”是“安全”，的自然属性。以防入侵、防盗窃、防抢劫、防破坏、防爆炸等为目的的安全技术防范系统主要针对的是“Security”；而防火、防目标被非人为因素伤害等是“Safety”涉及的问题。当同时出现这两种“安全问题时，在大多数情况下应优先解决“Safety”问题。这是设计系统与产品的基本原则。

在出入EI控制系统中，识读部分与执行部分是出入目标最易接触的部分，也是最有可能对出入目标造成伤害的部分。但不同的产品类型，其对安全的影响也是不同的。

在生物特征识别中，指纹、掌形识别等需人体直接接触的识读装置就不如面部、眼虹膜识别这类不需人体直接接触的识读装置安全，因为直接接触的识读装置的接触面若不能及时清洁，就有可能成为某些传染性**疾病传播**的媒介。

另外，直接担负阻挡作用的执行机构，其启闭动作本身必须考虑出入目标的安全，如电动门的关闭动作必须等待出入目标安全离开时方可进行，挡车器必须等待车辆离开方可落下挡车臂等。

在安防系统中与紧急疏散及消防系统联系最为紧密的就是出入口控制系统。出入口控制系统强调的是对空间的隔离，以保证“Security”；而紧急疏散及消防系统强调的是能快速逃离，以保证“Safety”。

在“Safety”优先的原则指导下，出入口控制系统的设计必须满足紧急疏散及消防的需要，这并不是说出入口控制系统所管理与控制的每个出入口必须与消防联动。但在本标准9.0.1条第2款的条件下必须联动，保证在火灾等紧急情况发生时，用于闭锁或起到阻挡作用的出入口控制执行部件能自动释放疏散出口，不使用钥匙，人员应能迅速安全地疏散。

security

安全

safety



火



出入口控制系统

14.4.1 系统应根据安全技术防范管理的需要，在建筑物内（外）出入口、通道（门）、电梯、重要房间门等处设置。

14.4.2 出入口控制系统宜由出入对象识别装置，出入口信息处理、控制、通信装置及出入口执行机构等三部分组成。

14.4.3 不同的出入口，应设置不同的出入权限；系统应能对设防区域的位置、通行对象及通行时间等进行实时控制 and 多级程序控制。

14.4.4 系统的识别装置和执行机构应保证操作的有效性和可靠性。宜有防尾随、防潜入及防胁迫措施。

14.4.5 根据高风险对象特殊需要，可在出入口设置防爆安检系统（包括X射线安检设备、金属探测门、爆炸物检测仪等其它设备）。

14.4.6 系统管理主机（上位机）应能对系统中的有关信息自动记录、打印、存储，并有防篡改和防销毁等措施。

14.4.7 出入口控制系统的受控制方式、识别技术及设备装置的选择应根据实际控制需要、管理方式及投资情况等，灵活地加以选用。

1 受控制方式有：单向控制、双向控制、多重多级控制等。

2 识别技术有：密码输入式、卡片式、人体生物特征识别式、多种识别技术组合式。

3 设备装置有：普通设备装置、无线设备装置及对安防有特殊要求的特殊设备装置。

14.4.8 控制器宜安装在读卡机附近房间里、弱电间等隐蔽处，读卡机应安装在出入口、通道（门）旁，安装高度中心距地宜为**1.4m**。

14.4.9 控制管理主机（上位机）发生故障、检修或通信线路故障时，各出入口现场控制器应能脱机正常工作。现场控制器应具有后备电源，当正常供电电源失去时，应能可靠工作**24**小时左右，并保证信息数据长时间不丢失。

14.4.10 出入口控制系统应能独立组网运行，并应具有与入侵报警系统、火灾自动报警系统、视频监控系统、巡更管理系统等集成功能或联动功能。

14.4.11 出入口控制系统应具有非常情况（如强行开门、长时间门不关、通信中断、设备故障等）实时报警功能。

14.4.12 一卡通系统宜由“一卡”、“一库”、“一网”组成，宜同时具有、部分具有出入口控制、考勤管理、巡更管理、停车场管理、消费管理等功能，可根据建筑物（群）的具体管理需要确定。**14.4.13** 住宅（小区）访客对讲系统的设计见本规范第**25**章的有关规定。

14.5.5 在线式实时巡更系统宜独立设置，也可作为出入口控制系统或入侵报警系统的内置功能模块与其联合设置，配合识读者或钥匙开关，达到实时巡更目的。

14.5.6 独立设置的巡更系统应能与安全防范系统联网，实现安全防范系统对其的管理与控制。

14.5.7 离线式电子巡更系统应能用信息识读者或其它方式，对巡更人员的巡查行动、状态进行监督和记录。巡更人员应配备应急联络或报警装置。

14.5.8 巡更站点的安装高度宜为底边距地**1.4m**。

14.5.9 巡更管理主机应能利用软件实现对巡更路线的设置、更改等管理，并能对未巡更、未按规定路线巡更、未按时巡更等情况进行记录、报警。

电子巡查系统

14.5.1 应根据建筑物的使用性质、功能特点及防范要求设置实时在线式或离线式电子巡更系统。

14.5.2 一二级风险场所及对巡更实时性要求高的项目宜采用在线式实时巡更系统；其余可采用较为经济的离线式电子巡更系统。

14.5.3 巡更站点应设置在建筑物出入口、楼电梯前室、停车场、重点防范部门附近、主要通道及走廊等其它需要设置巡更站点的地方。同一层最近两巡更站点的直线距离不宜大于**30m**。

14.5.4 巡更路线的设置应根据建筑规模、性质、层数及巡更站点的设置特点，结合巡更人员的配备、行走的科学性来确定。

停车场管理系统

14.6.1 有车辆进出控制及收费管理要求的停车场（库）应设置停车场管理系统。

14.6.2 应根据安全技术防范管理的需要及用户的实际需求，设计或选择设计如下功能子系统并进行合理配置：

1 入口处车位信息显示、出口收费显示；**2** 自动控制出入挡车器；**3** 读卡识别；**4** 车牌和车型自动识别；**5** 出入口及场内通道行车指示；**6** 泊位显示与调度控制；**7** 保安对讲、报警；**8** 视频监控；**9** 自动计费与收费管理；**10** 多出入口的联网与综合管理；**11** 分层（区）停车场（库）的车辆统计与车位显示。

其中**1**，**2**，**3**，**9**款为基本配置，其它为可选款。

14.6.6 停车场（库）内所设置的视频监控或报警系统，除可在收费管理室控制外，还应能在安防控制中心（机房）进行集中管理、联网监控。

14.6.7 有快速进出停车场（库）要求时，应采用远距离感应读卡装置；有一卡通要求时应采取与一卡通系统联网设计。

14.6.8 停车场（库）综合管理系统应具备先进、灵活、高效等特点，可利用免费卡、计次卡、储值卡等实行全自动管理，亦可利用临时卡实行人工收费管理。识别卡的种类应包括现今及近期发展的各类成熟卡。

14.6.9 车辆检测器线圈宜为防水密封感应线圈，设计与施工时所有线路不得与地感线圈相交，并应与其保持至少**0.5m**的距离。

14.6.10 自动收费管理系统应具有对人工干预、手动开闸等违规行为记录和报警功能。

14.6.11 停车场（库）管理系统应能独立运行，亦可与安全技术防范系统联网，当联网运行时，应满足安防系统对该系统管理的相关要求。

系统控制中心（机房）

14.8.1 安全技术防范系统控制中心（机房）应设置为禁区。宜在建筑物或居住区一层中间位置，可与消防、**BAS**等控制室合用或毗邻。

14.8.2 控制中心（机房）的面积应与安防系统的规模相适应，一般不宜小于**20m²**，且应具有保证值班人员正常工作的相应辅助设施。一级工程或重要建筑的控制中心（机房）应设置值班人员卫生间和专用空调设备。

14.8.3 控制中心（机房）自身防范措施：应设置紧急报警装置；不应毗邻重要防范目标；宜设置对讲电话装置或其他出入口控制及复核装置。运用计算机管理时，应设有密码等阻止非授权者侵入的有效措施。

14.8.4 系统控制中心（机房）应具备有线及（或）无线通讯方式与外界联系，也可与公安机关**110**报警指挥中心联网。一级工程或重要建筑应具有两种以上的通讯手段与外界联络。

14.8.5 控制中心（机房）的选址、设备布置及环境条件应符合本规范第**23**章的有关规定。

14.8.6 电源及接地应符合下列要求：

1 安全技术防范系统的控制中心（机房）应设置专用配电箱，由专用线路直接供电，并宜采用双路电源末端自投方式，主电源容量应按系统额定功率的**1.5**倍计取。

2 安全技术防范系统的电源质量应符合本规范第**23.3.12**条**2**款的规定。

3 电源质量不能满足要求时，应采用交流净化稳压电源，其输出功率不应小于系统使用功率的**1.5**倍。

4 一、二级风险建筑的安防系统，应采用在线式不间断电源供电。不间断电源的后备支持能力应能保证系统正常工作**60—120min**或按实际要求确定。其他建筑的安防系统宜采用不间断电源供电。

5 系统控制（中心）机房的接地及等电位联结应符合本规范第**23.3.13**条的规定。

6 专用接地干线宜采用铜芯绝缘导线或电缆，其线芯截面积不应小于**25mm²**，接地电阻不大于**4Ω**。当采用共用接地时，其接地电阻不大于**1Ω**。

7 供电系统、信号传输线路、天线馈线，以及进入控制中心（机房）的架空电缆入室端均应采取防雷电波侵入措施及过电压保护措施。

14.8.6 电源及接地应符合下列要求：

1 安全技术防范系统的控制中心（机房）应设置专用配电箱，由专用线路直接供电，并宜采用双路电源末端自投方式，主电源容量应按系统额定功率的**1.5**倍计取。

2 安全技术防范系统的电源质量应符合本规范第**23.3.12**条**2**款的规定。

3 电源质量不能满足要求时，应采用交流净化稳压电源，其输出功率不应小于系统使用功率的**1.5**倍。

4 一、二级风险建筑的安防系统，应采用在线式不间断电源供电。不间断电源的后备支持能力应能保证系统正常工作**60—120min**或按实际要求确定。其他建筑的安防系统宜采用不间断电源供电。

5 系统控制（中心）机房的接地及等电位联结应符合本规范第**23.3.13**条的规定。

6 专用接地干线宜采用铜芯绝缘导线或电缆，其线芯截面积不应小于**25mm²**，接地电阻不大于**4Ω**。当采用共用接地时，其接地电阻不大于**1Ω**。

7 供电系统、信号传输线路、天线馈线，以及进入控制中心（机房）的架空电缆入室端均应采取防雷电波侵入措施及过电压保护措施。

14.8.7 联动控制和系统集成

- 1** 入侵报警系统应与视频监控系统联动，一旦发生报警，视频监控系统立即启动进行监视，同时自动进行实时录像状态。
- 2** 出入口控制系统应与火灾自动报警系统联动，在火灾等紧急情况下，打开相关疏散通道的安全门或预先设定的门；出入口控制系统还应与视频监控系统及入侵报警系统联动，警情发生时，系统可立即封锁相关通道。
- 3** 视频监控系统宜与火灾自动报警系统联动，在火灾情况下，可自动将监视画面切换至现场，监视火灾趋势，向消防人员提供必要信息。
- 4** 安全防范各子系统既可以自成垂直管理体系，即系统集成；同时通过开放通信协议网络互联、相应容量的数据库、应用软件等亦可组成一个相对完整的综合安全管理系统，即集成式安全防范系统。
- 5** 安全防范系统的集成应遵守行业管理的相关规定，在开放标准的软硬件平台上，适当地实现可互操作、资源共享及综合管理。
- 6** 集成式安全防范系统的应用软件应先进、成熟、具有中文友好界面。应使操作尽可能简化，不轻易出现宕机现象。
- 7** 集成式安全防范系统一旦发生故障，各子系统仍能单独运行；若某子系统出现故障，不应影响其它子系统的正常工作。
- 8** 集成式安全防范系统应具有与上一级管理系统(**BAS,IBMS**)实现更高层次应用集成的能力。

IC卡由PVC或耐高温材料层压线圈及芯片的多用途非接触智能IC卡，**IC卡**封装芯片可选择EM、4100、4102、4069、4550、S50、S70、ULtralight、ST175、T5557、RF256、TK4100、LEGIC等。可胶印、个性化处理图片、丝片、喷码、防尘、防水、抗震动。

非接触式**IC卡**又称射频卡,是世界上最最近几年发展起来的一项新技术,**IC卡**在卡片靠近读卡器表面时即可完成卡中的数据的数据的读写操作,它成功地将射频识别技术和IC卡技术结合起来,**IC卡**解决了无源(IC卡中无电源)和免接触这一难题,是电子器件领域的一大突破,与接触式IC卡相比较,非接触式IC卡具有以下优点:

1.可靠性高

2.操作方便,快捷、

读写器在10cm范围内就可以对IC卡进行读写,没有插拔卡的动作.非接触式IC卡使用时没有方向性,IC卡可以任意方向掠过读写器表面,读写时间不大于0.1秒,大大提高了每次使用的速度。

3.安全防冲突

非接触式IC卡的序列号是唯一的,制造厂家在产品出厂前 已将此序列号固化,不可更改.世界上没有任何两张卡的序列号会相同.非接触式IC卡与读写器之间采用双向验证机制,即读写器验证卡的合法性,同时IC卡也 验证读写器的合法性.非接触式IC卡在操作前要与读写器进行三次相互认证,而且在通讯过程中所有数据被加密.IC卡中各个扇区都有自己的操作密码和访问条 件。

应用范围

由于非接触式IC卡具有更加方便,快捷的特点,可广泛应用于电子钱包,通道收费控制,公交自动售票,停车自动收费,食堂售饭,考勤和门禁等多种场合。