安全防范工程技术

主审　孙廷华　　主编　孙国强

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

安全防范工程技术

主审　孙廷华
主编　孙国强
参编　陶焱升　刘晓新　茹文彪
　　戴伟民　邱全中　王冠群

上海交通大学出版社

内 容 提 要

本书从安防工程的视频安防监控、入侵报警和出入口控制三个最基本组成部分介绍了安防工程建设技术，书中侧重技能知识，注意反映数字化、网络化技术的新发展。全书共7章，主要包括三大部分：工程设计、工程施工、工程管理。

书中各章节的内容安排合理、文字简明、内容翔实、图文并茂，具有较强的针对性和实用性，是当前安防工程建设和管理不可多得的参考书。

本书可作为高等职业技术学院或各类大专院校的技防专业教材，也可作为技防从业人员职业培训教材，对于安防工程的建设单位和监管部门也能起到较好的参考作用。

图书在版编目(CIP)数据

安全防范工程技术/孙国强主编. —上海：上海交通大学出版社，2013

ISBN 978-7-313-10175-4

Ⅰ. 安... Ⅱ. 孙... Ⅲ. 安全装置—电子设备—系统工程 Ⅳ. TM925.91

中国版本图书馆CIP数据核字(2013)第191549号

安全防范工程技术

孙国强 **主编**

上海交通大学出版社出版发行

(上海市番禺路951号 邮政编码200030)

电话：64071208 出版人：韩建民

上海景条印刷有限公司 印刷 全国新华书店经销

开本：787mm×1092mm 1/16 印张：20.75 字数：510千字

2013年8月第1版 2013年8月第1次印刷

印数：1～3 030

ISBN 978-7-313-10175-4/TM 定价：48.00元

前　言

“安防工程”是指以维护公共安全为目的，以科学技术为手段，综合运用安全防范产品和其他相关产品，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。本书“安全防范工程技术”主要介绍安防工程建设和维护过程中所应用的技能和相关知识。

近年来，我国的安防工程建设无论从规模还是技术上都得到了空前的发展。加强安防工程建设已经成为各地、各单位提高安全防范能力和水平的主要特征和重要举措。但是，当前安防工程的建设质量以及工程建成后系统的维护保养状况令人担忧，设计不贯彻标准和要求，施工不讲究工艺和流程，工程建设不注重质量和效果，维护保养未建立长效机制等现象时有发生，导致不少的安防工程起不到应有的安全防范作用，有的甚至是形同虚设。本书宗旨是，试图通过规范和统一安防工程建设和维护过程中每个阶段和各个环节的工作标准和具体做法，来达到提高安防工程的建设质量和实际效果。

本书的编者都是长期从事技防工程管理或是技防工程从业单位的专业技术人员，他们将自己长期工作在第一线的实际经验和体会贡献给读者。此外，本书还引用了近年来国家、行业、地方技术标准及地方一些技术性管理文件的相关要求，参考了有关教材和书籍，使本书对安防工程建设和维护工作的介绍内容更丰富，且更具有针对性和实用性。

本书共分7章，从安全防范的工程程序、工程设计、工程施工、工程检验、工程管理、工程维护保养和工程技术标准要求等多方面阐述了安防工程技术。

第1章“安全防范工程概述”，主要介绍了工程建设的基本要求、安防系统的组成与功能和安防工程的基本程序与主要环节。

第2章“工程设计”，主要介绍了安防工程的系统设计、系统前端设计和系统设计方案的编制。

第3章“工程施工”，主要介绍了安防工程的施工准备、现场施工、监控中心施工和系统调试。

第4章“工程检验”，主要介绍了安防工程检验的一般规定、检验项目、检验要求与方法，以及相关工序与质量的检验。

第5章“维护与保养”，主要介绍了安防工程的维护保养守则、预防性维护和故障性维护。

第6章“质量管理”，主要介绍了安防产品的质量管理和安防工程的质量管理。

第7章“安防标准”，主要介绍了安全防范标准化的基本概念、标准种类及分级与编号、主要标准的目录及概要，以及各地技术和管理性文件的摘要。

本书在编写过程中得到了上海科学技术职业技术学院、上海安全防范报警协会、上海市公安局安全技术防范办公室、公安部第三研究所、上海保安服务总公司、上海慧谷多高信息工程

有限公司、上海中电电子系统有限公司、上海能泰智能科技有限公司、上海汇迪电子有限公司、广州市伟昊科技电子有限公司等单位或部门的大力支持和帮助，在此表示感谢！

安防工程涉及面广，技术复杂。本书存在的不妥之处，敬请业内专家和广大读者批评指正。

编者

2012年12月

目　录

第 1 章　安全防范工程概述

1.1　工程建设的基本要求

安全防范工程是指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。安全防范工程建设应遵守以下基本要求：

1. 安全防范工程的建设

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、实用、配套的安全防范系统。

2. 安全防范工程的设计

应以结构化、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。

3. 安全防范系统中使用的设备

必须符合国家法规和现行相应标准的要求，并经检验或认证合格。

4. 安全防范工程建设应遵循的原则

（1）安全防范工程的防护级别与被防护对象的风险等级相适应。

被防护对象的风险等级是指存在于被防护对象本身及其周围的、对其构成安全威胁的程度。不同的被防护对象由于自身的性质与特点不同，所具有的风险等级自然就不同。被防护对象的风险等级越高，遭受攻击的可能性就越大。被保护对象的风险等级主要依据其人员、财产、物品的重要价值、日常业务数量、所处地理环境、受害的可能性以及公安业务主管部门对其安全水平的要求等因素，一般分为三级：一级风险为最高风险，二级风险为高风险，三级风险为一般风险。

安全防范工程的防护级别是指为保障被防护对象的安全所采取的防范措施的水平。被保护对象的防护级别，主要由所采取的综合安全防范措施（技防、物防、人防）的硬件、软件水平来确定。一般也分为三级：一级防护为最高安全防护，二级防护为高安全防护，三级防护为一般安全防护。

被保护对象的风险等级和安全技术防范工程的防护等级的划分是相对的，主要由管理工作的需要而定。一般说来，风险等级与防护的划分应有一定的对应关系：高风险的对象应采取高级别的防护措施，才能获得高水平的安全防护。如果低风险的对象采用高级别的防护，安全水平提高了，但这种安防防范工程的性能价格比一定会降低，不可取。首先安防工程的防护级别与被防护对象的风险等级相适应是所有安全技术防范工程设计与建设必须遵守的最基本的原则。

（2）技防、物防、人防相结合，探测、延迟、反应相协调。

“人防、物防、技防相结合”“打防并举、以防为主”是我国社会治安综合治理的总方针，基于

这一方针，在安全技术防范工程中，必须坚持“探测、延迟、反应相协调”的原则，过分强调某一种手段的重要性而贬低或忽视其他手段的作用，都会影响安全防范工程的持续稳定运行。

(3) 满足防护的纵深性、均衡性、抗易损性要求。

① 防护的纵深性。

所谓防护的纵深性，简而言之就是层层设防，即根据被保护对象所处的风险等级和所确定的防护级别，对整个防范区域实施分区域的分层次设防。一般而言，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性质的防区，对它们应实施不同的防护措施。

防护的纵深性通常分为整体纵深防护和局部纵深防护两种类型。整体纵深防护是对这个防区实施纵深防护；局部纵深防护是对防区的某个局部区域，按照纵深防护的设计思想进行分层次防护。

纵深防护的四种分区界定，一般由建设方与设计方共同商定，建设方有最终决定权。四种分防区的设置也不是绝对的，要视被保护对象所处的地理环境、被保护对象内部的具体配置而定。

② 防护的均衡性。

所谓防护的均衡性，有两方面的含义。一是指这个安全防范工程(或体系)在整体布局上不能存在明显的设计缺陷和防范误区，如各分区之间安装设置是否合理、各子工程(系统)的组合或集成是否有效等；二是指防区内同层防护(或系统)的防护水平应保持基本一致，不能存在薄弱环节或防护盲区。

在系统工程领域，系统的有效性遵从“水桶效应”原则或“瓶颈效应”原则。那一个安全技术防范工程(系统)，其总体防护水平的高低不由高防护部位决定，往往由系统的最薄弱环节来决定。

③ 防护的抗易损性。

所谓的抗易损性是指系统的可靠性和耐久性。系统的可靠性越高，抗易损性就越强。当然，还与系统的维修性、保障性以及组织管理工作有密切联系。

安全防范工程(系统)防护的纵深性、均衡性、抗易损性要求是相互联系的。抗易损性主要是对设备、器材的要求，均衡性主要是对各层防护或系统的要求，纵深性则是对整个系统的总要求，只有以上三者统筹考虑，全面规划，才能实现系统的高防护水平。

安全防范工程(系统)防护的纵深性、均衡性和抗易损性要求是安全防范三个基本防范要素在工程技术中的具体体现。之所以要求系统具有防范的纵深性、均衡性和抗易损性，都是为了保证探测、延迟和反应的有效性，只有这样，系统工程才能防范相应的风险，实现安全的目的。

(4) 满足系统的安全性、电磁兼容性要求。

① 系统的安全性。

安全防范工程(系统)的安全性包含自然属性的安全和社会人文属性的安全两个层面的意义。自然属性的安全一般是指系统包括所使用的产品在运行过程中能够保证人员健康、安全和设备本身安全的技术要求。人文属性的安全通常是指设备和系统的防人为破坏，信息的防人为窃取和篡改等技术要求。

因此在进行安全防范工程(系统)设计时，必须要采取专门的措施保障自然属性和人文属性的安全。保证所采用设备及安装部件具有足够的机械强度，安全防范工程(系统)的设计还

应保障系统的供电安全可靠以防对人员造成伤害。系统所用设备所产生的气体、射线辐射、电磁辐射等应符合国家相关标准的要求，不能损害人体健康，系统和设备应有防火、防过热、防人身触电的保护措施。在信息安全方面，对系统的操作权限、登录认证进行有效管理。专线传输应有防信号泄漏或加密措施，公网传输或无线传输也应有加密措施。系统应设置防病毒和防网络入侵的措施。

安全防范工程（系统）设计要格外重视系统自身的防破坏能力，安全技术防范系统的设计应具备防拆、开路、短路等报警功能，传输系统线路应隐蔽铺设并加有相应的保护措施，系统设计时最好具备系统自检和故障报警等功能。

② 系统的电磁兼容性。

安全防范工程（系统）的电磁兼容性设计要求包括电磁干扰和抗电磁干扰两方面内容，涉及设备选型和设计、传输介质选择和传输路由设计等多个环节。安全防范工程（系统）所使用的设备及电缆的电磁兼容性设计应符合相关的标准和规范；传输线路的抗干扰设计应注意做到电力系统与信号传输系统线路应分开铺设；信号电缆的屏蔽性能、铺设方式、接头工艺、接地要求等应符合相关标准规定；安全防范工程（系统）的防电磁干扰设计应注意系统所用设备外壳开口尽可能小，开口数量尽可能少；系统中所采用的无线发射设备的电磁辐射频率、功率，非无线发射设备对外的杂散电磁辐射功率均应符合国家现行有关法规和有关技术水平标准。

（5）满足系统的可靠性、维修性与维护保障性要求。

① 系统的可靠性。

系统的可靠性是指在规定条件、规定时间内系统的保持有效工作的能力，它反映了系统性能的耐久性。安全技术防范工程（系统）常用的可靠性设计有降额设计、简化设计、冗余设计等方式。定量表示可靠性的数学特征量有可靠度、累计失效概率、失效率、平均无故障时间（MTBF：mintime between failures）、有效度等。衡量安全技术防范工程（系统）可靠性最常用的指标是 MTBF。

② 系统的维修性与维护保障性。

维修性是指在规定的条件下并按规定的程序和手段对系统实施维修时，系统在规定的使用条件下，保持或恢复执行规定功能状态的能力，它表示为保持或增强系统性能而进行维修和改进的难易程度。

维修保障性是为达到可用性目标而提供的后勤保障和资源分配情况，也就是系统的设计特性和计划的保障资源能满足系统使用要求的能力。

系统的维修性和保障性是系统的可信性的重要组成部分，维修性技术、保证性技术与可靠性技术一起形成了可信性技术。对于可修复产品而言，维修性和保障性是两项重要技术特性，它们对产品的使用寿命有重大影响。

（6）满足系统的先进性、兼容性、可扩展性要求。

系统的先进性是指采用产品、技术要成熟、可靠，并且具有一定的先进性，既满足系统目前的工作需要，又能适应未来一段时期内业务增长的需求。

系统兼容性是指系统设计采用国际标准，具有开放式体系结构，便于将来系统升级；硬件产品要兼容多种操作系统平台和软件平台。

可扩展性是指基于标准技术的基础上，系统能够随着信息技术的进步不断实现升级，并且有一定的扩展能力满足业务不断增长的需求。

(7) 满足系统的经济性、适用性要求。

经济性是指系统具有较高的性能价格比，即产品质量、性能质量好，同时具有较低的价格。安全防范工程(系统)的设计和建设，要考虑到被防护对象的风险等级与防护级别，要在保证一定防护水平的前提下，争取最高的性能价格比。

安全防范工程(系统)的适用性是指安全技术防范工程(系统)的设计要围绕着被保护对象的特点来进行，要有针对性，根据防护对象的性质，如其周边环境、地形地貌条件、防护等级等，判断是否能够满足安全技术防范的要求。

安全防范工程(系统)的设计和建设既不是设备价格档次越高越好，价格越贵越好，也不是功能越多越好，而是要适合要求，根据具体情况作出设计，应该要求做到一个工程一设计，一个点位一设计，这是对设计师的最基本的要求。

1.2 系统的组成与功能

据使用场所和要求不同，安防防范工程从技术层面上所涉及的安全技术防范系统可分为入侵报警系统、视频安防监控系统、防爆系统、出入口控制系统、监听系统、安全检查系统和通信系统等多项安防子系统。在实际应用中，为了提高防范系统的防范能力和工作可靠性，各安防子系统往往是相互配合使用，而其中的入侵报警系统、视频安防监控系统和出入口控制系统又往往是安全技术防范系统的最基本组成部分(见图 1-1)。

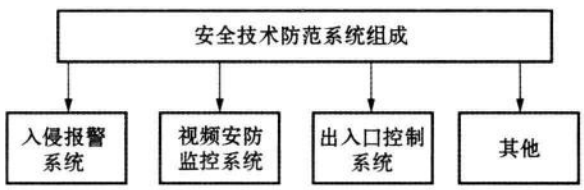

图 1-1 安全技术防范系统的基本组成

所有安防子系统的结构，概括起来，都由系统的前端、传输和终端三大单元组成。但不同的系统，其具体设备和架构也不相同。以下就各主要分系统的组成部分和基本功能进行介绍。

1.2.1 入侵报警系统的组成与基本功能

入侵报警系统是利用传感器及电子信息等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。

1. 入侵报警系统的组成

经典的入侵报警系统的组成如图 1-2 所示。由图可知，系统由前端设备、传输设备、处理/控制/管理设备和显示/记录设备四部分组成。

1) 前端设备

前端设备是入侵报警系统的触觉部分，相当于人的眼睛、鼻子、耳朵、皮肤等，是指安装在防护现场的，对各种入侵行为进行探测的探测器，它们不能独立工作，而仅仅是将探测信息传输至处理/控制/管理设备。

2) 传输设备

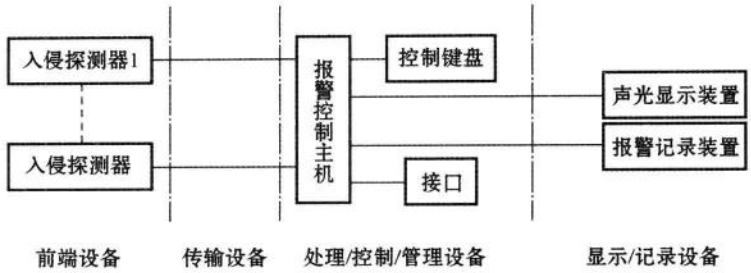

图 1-2　入侵报警系统的组成

传输设备相当于人的神经系统，其主要任务是保证前端设备与报警控制器之间的正确连接与通信，并将前端设备的探测信号和状态信号上传至报警控制器。

3）处理/控制/管理设备

处理/控制/管理设备中关键是报警控制主机，主要负责控制、管理入侵报警系统的工作状态；监测前端设备是否已正常连接；收集探测器发出的信号，按照探测器所在防区的类型与主机的工作状态（布防/撤防）做出逻辑分析，进而发出本地报警信号；同时输出特定的报警信息至指定的报警中心。鉴于报警控制主机在系统中所起的作用，又把它称作报警控制器、报警控制/通讯器。入侵报警系统的功能主要由报警控制主机的功能决定。

报警控制主机有很多的输入输出接口，控制键盘的主要功能是完成指令的编写与输入并对系统实施控制与管理。

4）显示/记录设备

显示/记录设备主要完成入侵报警系统各种操作指令、工作状态的显示与记录功能。显示装置可以是控制键盘自带的显示屏幕，也可以是计算机显示器；各种信息的记录可以保存在报警控制主机内存中，也可以保存在硬盘中，但无论保存在何处，信息都应不能更改。

2. 入侵报警系统的基本功能

入侵报警系统的基本功能主要包括：前端探测、报警（本地报警和警情传输）控制与管理、状态指示与记录、自身安全监测与防护等。

1）探测功能

入侵报警系统最基本的功能是探测，系统应能对需防护现场可能的入侵行为进行准确、实时的探测。可能的入侵行为包括：非法打开门、窗；通过暴力手段破坏天花板、墙体及建筑结构体；破碎玻璃；接触或接近保险柜或重要物品等。

2）报警控制与管理

（1）报警控制。报警控制功能主要体现在编程控制上。入侵报警系统应能通过灵活的编程设置对系统实施控制，使之能够更广泛地适应各种环境。例如，瞬时防区和延时防区的设置，由于两种类型的防区其触发后的报警过程不同，需要根据现场的具体情况对防区类型进行合理定义，一般紧急按钮是发生紧急事件时人为触发的紧急报警设备，无论它连接到哪个防区都一定要将此防区定义为瞬时防区，保证一旦触发立即报警；延时防区为在该防区的探测器已被布防的情况下，只要在设定的延时时间内探测器被触发，该防区不报警，但超过此延时时间，一旦被触发则报警。入侵报警系统的编程控制功能还表现在对全部或部分探测回路设置警戒（布防）与解除警戒（撤防），向远程中心传输信息或取消信息传输，向辅助装置发激励信号等。

(2) 报警响应。入侵报警系统的报警响应功能体现在响应时间上,即报警应及时迅速。所谓报警响应时间是指从探测器触发到控制设备接收到该信息并发出报警信号所需的时间。

(3) 报警传输。入侵报警系统能够用有线或无线传输方式传输报警信号;应能对传输线路自检、巡检;应有与远程中心进行有线或无线通信的接口,并能对通信线路的故障进行监控。

3) 状态指示与记录

作为入侵报警系统应能够对系统内所有的工作状态有所指示,这些工作状态包括:试验状态、报警状态、故障状态及布撤防状态等,以便使用者(维护者)能够清楚地了解当前入侵报警系统的运行状况,及时采取相应措施。

系统内的所有技术参数及其改变情况,系统各设备的运行维修状况,各事件发生的时间、地点、处理结果都将是破案或解决争端的法律依据,所以系统应对发生的所有事件以及编程设置的所有参数进行记录并能查询,包括操作人员的姓名、开关机时间、警情的处理及维修等。

4) 自身安全监测与防护

入侵报警系统是确保一方平安所实施的技术手段,其自身的安全最为重要,应具备自身的安全监测与防护,如系统所连设备的状态监测、防破坏措施等。

1.2.2 视频安防监控系统的组成与基本功能

视频安防监控系统是安全技术防范系统的重要组成部分,是利用视频技术监视控制区域并实时显示、记录与回放现场图像的电子信息系统或网络。

1. 视频安防监控系统的组成

从实现的功能上看,一个完整的视频安防监控系统通常由前端采集、信号传输、控制、显示与存储五个主要部分组成,如图 1-3 所示。

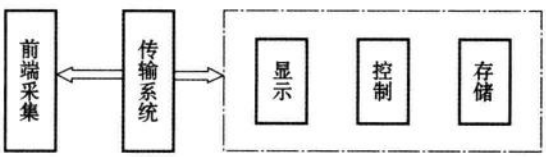

图 1-3 视频安防监控系统的组成

1) 前端采集

前端采集部分完成对视频信号的获取,它包括一台或多台摄像机以及与之配套的镜头、云台、防护罩、云镜解码器、红外灯、拾音器等设备,完成图像信息、语音信息、报警信息和状态信息的采集。摄像机通过内置图像传感器及辅助电路将现场情况摄制成为模拟/数字视频信号,传输到监控系统中。电动变焦镜头可将拍摄场景拉近、推远,并实现光圈、调焦等光学调整。云台、防护罩为摄像机和镜头提供适宜的工作环境,并可实现拍摄角度的水平和垂直调整。云镜解码器是在对云台、镜头实施控制时必不可少的设备,通过它可把由监控中心发出的代表控制命令的编码信号解码还原为对云台、镜头的具体控制信号。

2) 信号传输

信号传输部分完成对前端音视频、控制与状态信号的传送。按照传输信号的类型,可分为数字和模拟两大类。常用的模拟传输媒介包括同轴电缆、光缆、微波等线路类型;数字传输系统主要包括熟知的 TCP/IP 网络,常用的传输媒介包括双绞线、光缆、无线网络等。不论是数

字或模拟传输系统，不同传输媒介的成本、传输距离、传输能力各有不同，在实际应用中，要根据各自的应用需求和特点来进行合理地选择和组合。

3）控制

控制部分完成对音视频信号的显示切换、云台和镜头的控制（简称云镜控制—PTZ）及资源的分配，是视频安防监控系统的核心。它包括音视频信号切换与分配、云镜控制、操作键盘、各类控制通信接口转换等设备，还包括配套的电源、控制台等设备。在数字化系统中，控制上升到了一个更广义的层面，除显示切换和云镜控制外，还包括设备管理、权限管理、码流调整、带宽控制、区域管理、网管控制等，这是监控技术与计算机技术相结合的产物。随着这些新的控制手段引入，视频安防监控系统已经不单纯只是录像、回放的工具，而成为了能够覆盖广泛区域的管理手段。

4）显示

显示部分完成对视频信号终端设备的输出。视频图像显示设备种类繁多，从传统的监视器、液晶监视器、投影仪，到如今的DLP、LCD大屏幕拼接等设备。视频信号的显示分为数字方式与模拟方式两种。对于数字方式显示又分为两种，一种是YUV数字信号预览显示，通常用在数字硬盘录像机的预览显示上；另一种是压缩数字信号的解压还原显示，通常用在数字硬盘录像机或网络硬盘录像机的录像回放和远程查看上。

5）录像存储

录像存储部分主要完成数字视频信号存储和回放，主要目标是在保证回放图像质量的前提下，确保存储周期、数据的完整与安全。视频安防监控系统存储设备主要有数字硬盘录像机（DVR）、网络硬盘录像机（NVR）及网络存储等。DVR/NVR主要用于小型系统，网络存储则主要用于大中型集中系统，如NAS、IFSAN、IPSAN。

2. 视频安防监控系统的基本功能

1）多路监控功能

多路监控功能具有简单的和复杂的两种方式，简单的方式是采用视频切换器完成多路视频图像的时序性切换，每路视频图像依据时间顺序自动切换，并在监视器上停留固定时间。复杂的方式是采用矩阵，编制各种时序切换程序，实现多路同时时序性切换。在复杂的多路监控中也可以通过操作键盘完成对前端云台及镜头的控制；如果前端有快速球，那么也可以通过操作键盘完成对快速球预置位的设置与操控。

2）视频录像

系统能够实时记录全部的视频监控信号，并能按照指定编码模式（JPEG，MJPEG，MPEG-1，MPEG-2，MPEG-4，H.264，SVAC等）将压缩后的数字视频信号保存到磁盘上。

3）录像检索与回放

每台DVR/NVR均可启用录像检索功能完成录像回放；另外还可以建立一台录像资料集中管理的媒体浏览服务器，通过媒体浏览服务软件来完成整个视频安防监控系统资料的远程查询与回放任务。

4）报警联动

视频安防监控系统的报警联动功能一般都是通过矩阵的接口来完成，这种接口一般有两种：一是矩阵报警控制箱；二是串口通信协议。矩阵报警控制箱是通过若干个独立的开关量接口端子来接入其他系统的报警信号，如开启照明设备、启闭出入口执行设备、改变快球监控

方位等。串口通信协议是利用串口总线及特殊编制的通信协议来接入其他系统的报警信号。报警联动功能包括：报警联动音视频图像自动切换显示和报警联动视频自动录像。

5）视频移动侦测与识别

视频移动侦测与识别属于视频信号分析的范畴，一般是通过两种方式完成：一种是专门的微电子技术设备；一种是专门的分析软件模块。

通常复杂的视频信号分析都是在中心端完成，视频移动侦测就是从图像序列中将变化区域从背景图像中提取出来。移动区域的有效分割将大大减少后继过程的运算量。然而，背景图像的不稳定性，如阴影、光照、慢移动、静移动（树叶的摆动）等，也使得移动检测非常困难。

1.2.3 出入口控制系统的组成与基本功能

为完成对进出对象出入的监控，出入口控制系统的首要目的是识别进出对象的身份或特征信息，进而根据存储于系统中的信息，最后判断是否已授权该对象具有进出的权利并完成控制命令的传送和执行，其次对非法异常操作、强行闯入行为予以报警。

1. 出入口控制系统的组成

出入口控制系统的组成可以归纳为：中央管理、识读、控制、执行等四大部分，如图 1-4 所示。中央管理部分主要起到业务决策、设备设置、数据查询、统计、维护等作用；识读部分就是采集人、车或物的生物特征或代表其身份编码的信息；控制部分主要采集检测输入信号，或接收中央管理部分的指令，或接收反馈信息，结合控制规则进行核实、分析和处理，然后向执行部分输出相应的指令，或通知其他设备；执行部分主要在接收到控制执行指令时完成允许或禁止通行动作或指示。

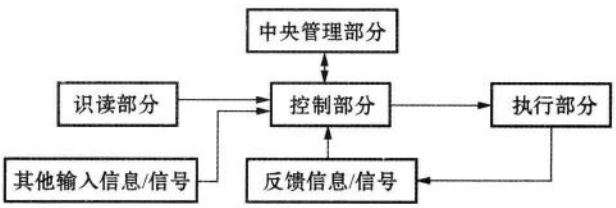

图 1-4　出入口控制系统的组成

1）中央管理部分

中央管理部分是出入控制系统的神经中枢，其作用是：根据业务需要确定授权形式与内容，担负卡（特征）管理任务，并协调监控整个控制系统的运行。通常情况下，中央管理部分由计算机、授权设备、UPS 电源、打印机、网络控制器或传输设备等组成。

（1）计算机主要安装管理软件和数据库等，数据库除服务于本身系统的需求外，也可服务于整个大厦智能系统的集成。

（2）授权设备主要是完成卡管理中的卡识别、授权等任务。

（3）UPS 电源是后备电源，以应对停电、突然掉电的特殊情况发生时，保证系统能正常保存相关数据，甚至保证系统能正常运行一段时间。

（4）打印机设备主要是为了输出报表、系统制卡等情况下使用。

（5）网络控制器或传输设备主要包含 RS485 通信设备、通信级联控制器、中央数据处理设备、网络交换机等，其主要是起到数据交互、传输、特殊数据处理等一种或多种作用。

2）识读部分

被授权允许进出的人员、车辆或物品，凭借其代表的特征信息介质/载体表明其身份和权限。在同一系统中，尽管目标识别的特性相同，但因授权的内容不同，目标被授权出入的区域范围与权限也就不同。

识读设备的主要任务是识别目标在出入区域的权限，当允许进入时，识读部分向对应的控制部分发出开启指令，否则不授权“放行”。识读部分通过识读设备获取目标的操作及编码、特征信息并对其进行识别，应能将识别信息传递给控制部分处理，也可接受控制部分的指令。

在停车场、高速公路进出口等特殊场合，若需要远距离读取卡的信息，则可选用主动式射频卡及配套的射频读卡器。

3）控制部分

根据识读部分的信息，向能控制出入口与通道启闭的执行机构发出操作命令，是控制部分的主要任务。实施和完成这些任务的设备统称为出入控制器。

出入控制器应将出入事件信息发送至中央管理部分，可连接多个报警输入与报警输出设备，兼有防盗报警等功能。出入控制器需要通过连接线路，向上连接中央管理部分，向下连接识读与执行等部分的设备，通过标准通信协议将全部出入控制器构成一个网络。

在突然断电、掉电时为保证系统能正常工作，控制部分应配备备用电源（内置后备电源或电池），以保证数据的安全性。

需要说明的是：各类出入控制系统的控制方案是不一样的，需要与实际业务结合进行设计。

4）执行部分

执行部分是实现出入控制功能最后一个关键部分。门禁管理系统利用电信号控制电子锁以实现门的启闭动作；停车场管理系统则是利用电动栏杆、路障机与红绿灯等设备的动作或指示实现“禁行”与“放行”；人行通道管理系统利用通道闸的辊杆、挡板等设备来控制人员的通行。

执行部分接收控制部分发来的出入控制命令，在出入口做出拒绝与放行操作的指示。执行部分分为闭锁部件、阻挡部件、出入准许指示装置三类产品。常见的闭锁部件或阻挡部件有：各种电子锁、各种电动门、电磁吸铁、电动栅栏、电动栏杆等；出入准许指示装置主要是发出声响和/或可见光信号的装置，可采用声、光、文字、图形、物体位移等多种指示。出入准许指示装置的准许和拒绝两种状态应易于区分，出入口开启时，对通过人员和/或物品的通过的时限和/或数量可以做出限制或明示。

2. 出入口控制系统的基本功能

1）权限控制管理

中央管理部分首先要赋予操作人员登录的权限，并且使不同级别的操作人员对系统有不同的操作权力。一般情况下操作人员分为管理员、操作员。

由于管理者会要求不同的对象在不同的时间里，具有进出不同的区域的权限，因此系统应能针对不同的对象设定相应的权限。例如，卡的权限可根据实际需要，设置为一卡开一门/通道、一卡开多门/通道、多卡开一门/通道，同时附加以时间限制，如按小时、按天、按月授权。故而，系统应对不同对象身份信息的录入、授权、变更、注销、充值、延期、挂失等进行管理。

2）数据管理