[智能建筑系列]

智能门禁控制系统

王汝琳 编著

http: //www.phei.com.cn

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

智能建筑系列

智能门禁控制系统

王汝琳　编著

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

本书在对当前门禁控制系统的现状进行全面调研的基础上，从整体方案、软硬件设计、系统控制、单片机应用、通信接口、功能集成等方面介绍了一种新型的感应式（RF）智能门禁控制系统，不仅实现了对出/入口的安全控制，而且具有联网、巡更和考勤功能。最后给出了几种国内外典型门禁控制系统的设计实例。

本书适合于从事门禁控制系统和智能建筑技术研究、设计和工程施工的工程技术人员、物业管理人员学习和参考，也可作为相关专业本科生、研究生的参考书。

图书在版编目（CIP）数据

智能门禁控制系统/王汝琳编著. —北京：电子工业出版社，2004.9
（智能建筑系列）
ISBN 7-121-00262-0

Ⅰ. 智… Ⅱ. 王… Ⅲ. 智能建筑—保险装置—控制系统 Ⅳ. TS914.211.7

中国版本图书馆 CIP 数据核字（2004）第 085208 号

责任编辑：张 榕（zr@phei.com.cn）
特约编辑：刘汉斌
印 刷：北京天竺颖华印刷厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
经 销：各地新华书店
开 本：787×980 1/16 印张：18.25 字数：467.2 千字
印 次：2004 年 9 月第 1 次印刷
印 数：5 000 册 定价：28.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前 言

智能建筑集多种先进技术和多种系统于一体，向人们提供高质量、安全、舒适、方便的综合性服务，同时体现了高效管理、节省能源等现代都市生活理念。本书主要介绍楼宇自动化系统中的安防系统的门禁子系统。

门禁控制系统在安全防范中具有重要作用，但目前缺乏系统的讨论和总结。本书在对当前门禁控制系统现状进行全面调研的基础上，总结作者近年的研究成果，介绍了一种新型的感应式（RF）智能门禁控制系统。这种新型的感应式门禁控制系统的读卡器和卡片之间通过射频方式交换信息，不需接触。其控制器采用 I^2C 串行总线，以 PHILIPS87LPC764 为中央处理器，硬件主要由 CPU、EEPROM、实时日历/时钟、通信接口、读卡器接口及其他外围电路构成，软件采用 C 语言与汇编语言混合编程，不仅实现了对出/入口的安全控制，还可以联网，具有巡更和考勤功能。本着安全性、先进性、时效性、便捷性的要求，对功能更加完备的高级网络型智能门禁控制系统进行了详细的规划和设计。同时，还详细讨论了串行通信的特点，比较了 RS232 与 RS485 的特性，在此基础上设计了光电隔离型 RS232/RS485 转换器，为上位机与控制器之间通信的可靠性提供了保障。书中首次讨论了用于智能建筑的通用型直接数字控制器（DDC），提出了以通用型 DDC 为基础的新型集成方案，并编写了门禁系统的控制软件。本书所给出的设计方案先进合理、结构简单、功能完善、成本低、安全性和可靠性高，具有较高的性能价格比，有很强的实用价值。最后，本书以三种国内外典型的门禁控制系统为例说明门禁控制系统的结构和功能。

本书适合于从事门禁控制系统研究、设计和工程施工的工程技术人员、物业管理人员学习和参考，也可作为相关专业本科生、研究生的参考书。

研究生叶本耀、王燕妮、张爱华、刘慧明和梁琼参加了项目的研究和本书的编写工作，深圳视得安公司、北京吉高公司和美国 HIRSCH 公司提供了产品资料，在此一并表示感谢。由于作者水平所限，书中缺点和错误在所难免，希望广大读者批评指正。

作 者

目　录

第1章 综 述

1.1 安全防范

随着我国经济的快速发展，城市人口数量的急速上升，对建筑的安防系统要求越来越高。同时，大量的电气设备在使用中也存在着不安全因素，这些因素对人民的生命和财产安全构成了很大的威胁，这就对社会公共安全科学提出了更高的要求。社会公共安全科学是预防、控制、处理各种社会违法犯罪活动和灾害事故，维护社会治安，保障人民正常工作、生活秩序，保障国家和人民生命财产安全的综合性应用科学。它包括安全防范、计算机安全、侦查、物证鉴定、治安管理、道路交通管理、消防、信息管理、警用通信指挥、警用武器、防护装备等专业领域。

安全防范是社会公共安全科学技术的一个分支，包括人力防范、技术防范和实体（物理）防范三个范畴。本书中所说的安全防范主要是指安全技术防范。安全技术防范以安全技术防范产品和基础防护设施为手段，以人力防范为基础，是预防入侵、盗窃、抢劫、破坏、爆炸等违法犯罪活动和重大政治事故，维护社会治安的技术防范措施。其技术领域主要有：防爆炸、安全检查、防盗报警、门禁控制、电视监控、周界防范、电子巡更，以及相应的联动防范系统等。目前，利用计算机技术、自动化技术和通信技术建立高效、完善的安全技术防范系统已成为现代生活的必然要求。安全技术防范系统的微机化和网络化是其今后的主要发展方向。

用于安全防范工作的专门技术被称为安全防范技术。在国外，安全防范技术通常分为三大类：物理防护技术（Physical Protection）、电子防护技术（Electronic Protection）、生物统计学防护技术（Bio-Metrics Protection）。在我国，安全防范技术是指安全技术防范行业所采用的防爆安检技术、实体防护技术、入侵报警技术、门禁控制技术、电视监控技术及其相应的工程设计、施工技术等。

1.1.1 安全防范系统的基本特征和技术要求

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、软件有效地组合成一个有机整体，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、高可靠性和高性能价格比。

1. 高安全性（Safety/Security）

安防产品或系统是用来保护人员和财产的安全，首先自身必须安全，因此这里所说的高安全性一方面是指产品或系统的自然属性或准自然属性应确保证设备、系统运行和操作者的安全，例如：设备和系统本身要能防高温、低温、烟雾、霉菌、潮湿、（宇宙）射线辐射、电磁干扰（电磁兼容性）、冲击、碰撞等，设备、系统的运行安全还包括防火、防雷击、防爆、防触电等；另一方面，安防产品或系统还应具有防人为破坏的功能，如具有防破坏的保护壳体，具有防拆报警，防短路、开路、并接假负载，防内部人员作案软件等。为此，安防产品与系统应满足有关的产品标准和系统的技术要求，以及气候环境适应性要求、电磁兼容性要求和防人为破坏的技术要求。

2. 高可靠性（Reliability）

安防产品或系统以预防损失、扼制犯罪为主要目的，应是常备不懈的哨兵。俗话说“养兵千日，用兵一时”，“不怕一万，就怕万一”，这两句话可以形象地说明安防产品或系统高可靠性的重要意义。一个报警系统在其有效寿命期的大多数时间内可能没有警情发生，报警的概率很小，但是若在这样很小的概率内报警系统失灵，则意味着灾难的降临。因此，安防产品或系统在设计、施工、使用的各个阶段，必须实施可靠性设计（冗余设计）和管理，以保证产品或系统的高可靠性。

在理论上，可靠性就是指产品或系统在规定使用条件（使用条件＝工作条件＋环境条件）下和规定时间内完成规定功能的能力。定量表示可靠性的数学特征量有可靠度、累积失效概率、失效率、平均无故障工作时间（MTBF：Mean Time Between Failures）、有效度等。对电子设备和系统（安防产品和系统也基本上是电子产品与系统）而言，衡量可靠性最常用的指标就是 MTBF——产品或系统的无故障工作时间的平均值。它实际上表示产品或系统的可修复性技术指标。

保证系统的可靠性，必须首先提高系统所用设备的可靠性，这是因为系统的可靠度公式为 $R=\sum R_i \times \rho_i$，其中：R_i 是系统所用第 i 种设备的可靠度，ρ_i 是其对应的加权因子。因此，理论上讲，系统越复杂，它所用的设备越多，则系统的可靠性就越低，所以在设计安防系统时，为保证系统的高可靠性，通常采取以下措施：

（1）提高设备（或系统）的平均无故障工作时间（MTBF 值）。

（2）提高设备（或系统）的易维修性（组件、插板的易更换）。

（3）提高设备（或系统）的冗余度：关键设备要有备份（热备份），在设备真正出问题时能做到自动转接。

一般的产品或系统，也要求高可靠性。但对于安防产品或系统来说，如果在规定条件和时间内，不能完成规定的功能，即该报警时不报警（漏报）或者误报警，就会

导致财产和生命的损失。所以安防产品或系统必须做到具有很高的可靠性。

3. 高性能价格比（Cost Performance Ratio）

安防产品或系统要根据被保护对象的风险等级和防护级别的要求综合考虑，使风险等级和防护级别相互适应，具有高性能价格比。

（1）风险等级是指存在于人或财产周围的对他（它）们构成威胁的严重程度（Level of Risk）。

（2）防护级别是指对人和财产安全所采取的防范（包括技术方面和组织方面）措施的水平（Level of Protection）。

（3）安全防护水平是指风险等级被防护级别所覆盖的程度（Level of Security）。

风险等级和防护级别的划分不是绝对的，一般来说风险等级与防护级别的划分有一定的对应关系：高风险的对象应采取高级别的防护措施，以获得高水平的安全防护。如果高风险的对象采取低级别的防护，安全性必然降低，容易发生事故，但如果低风险的对象采用高级别的防护，则这种系统的性能价格比降低，造成浪费。因此，在保证系统安全防护水平的前提下，保证高性能价格比是考核系统经济性、实用性的重要指标。

1.1.2 智能建筑安防系统

1. 智能建筑

智能建筑以目前国际上先进成熟的分布式系统理论和控制理论为基础，综合利用了现代计算机技术（Computer）、现代控制技术（Control）、现代通信技术（Communication）和现代图形显示技术（CRT），即 4C 技术。智能建筑适应了社会信息化和经济国际化的需要，向人们提供高质量、安全、舒适和快捷的综合服务功能。同时，它采用科学、高效的综合管理，最大限度地节约能源，按照用户要求灵活变动，具有极强的适应性。

智能建筑由集成管理系统通过综合布线系统，将楼宇自动化系统（Building Automation System，BAS）、通信自动化系统（Communication Automation System，CAS）和办公自动化系统（Office Automation System，OAS）连接起来并予以管理和控制，即通常所说的 3A 智能建筑。在智能建筑内，这三个子系统都是建立在综合布线系统物理连接的基础之上，同时又统一于智能大厦集成管理系统。

楼宇自动化系统（BAS）通常包括暖通空调、给排水、供配电、照明、电梯、消防、安全防范等子系统。根据我国行业标准，BAS 又可分为设备运行管理与监控子系统、消防子系统和安全防范子系统。

通信自动化系统（CAS）由各种通信设备、通信线路和相关计算软件组成，用来保证大厦内、外各种通信联系畅通无阻，并提供网络支持能力。实现对语音、数据、文本、图像、电视及控制信号的收集、传输、控制、处理与利用。借助这些通信网络可以实现大厦内外、国内外的信息互通、资料查询和资源共享。

办公自动化系统（OAS）是服务于具体办公业务的人机交互信息系统。办公自动化系统由多功能电话机、高性能传真机、各类终端、PC、文字处理机、主计算机、声像存储装置等各种办公设备、信息传输与网络设备和相应配套的系统软件、工具软件、应用软件等组成。

2. 智能建筑安防系统

智能建筑安防系统的结构模式大致可分为组合式和集成式两大类。组合式的特点是系统的各子系统分别单独设置，集中管理；集成式的特点是通过统一的通信平台和管理软件将各子系统联网，从而实现对全系统的集中管理、监视和控制。

智能建筑安防系统组成框图如图 1-1 所示，包括的主要子系统为：防盗报警子系统、视频监控子系统、门禁控制子系统、巡更报警子系统、周界防范子系统和其他子系统。这些子系统可以单独设置、独立运行，也可以由中央控制室进行集中监控，还可以与其他综合系统进行系统集成和集中监控。智能建筑安防系统的各主要子系统简介如下所述。

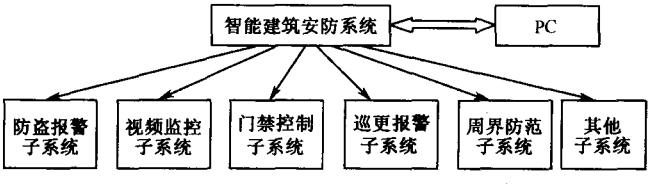

图 1-1　智能建筑安防系统组成框图

防盗报警子系统一般分为建筑物内防护、空间防护和对实物目标的防护。系统的前端设备为各种类型的报警探测器（传感器），传输方式可采用有线和无线，有线传输又可采用专线传输和电话线传输等方式。系统的终端是显示/控制/通信设备，可采用独立的报警控制器，也可以采用报警中心控制台。不管采用何种方式，都要求实现对设防区域的非法入侵进行实时、可靠和正确无误的报警和复核。漏报警是绝对不允许的，误报警应降低到可以接受的限度。为预防抢劫或人员受到威胁，系统应设置紧急报警装置和留有与 110 报警中心联网的接口。

视频监控子系统一般用于对建筑物内的主要公共场所和重要部位进行实时监视、录像和报警时的图像复核。系统的前端设备是各种类型的摄像机（或视频报警器）及其附属设备，传输方式一般采用同轴电缆或光缆传输，系统的终端是显示/记录/控制设

备，一般采用独立的视频监控中心控制台或监控报警中心控制台。安防用视频监控系统一般与防盗报警系统、门禁控制系统等联动，由智能建筑安防系统中央控制室进行集中管理和监控。当报警发生时，系统应能对报警现场进行图像（和声音）的复核，这是对安全防范视频监控系统的一项基本要求，不管是独立运行的系统，还是联动的系统，或是与其他系统联网实施集中管理、集中监控的系统，都要求做到这一点，才能保证不发生漏报警和误报警。

门禁控制子系统是指采用现代电子与信息技术，在建筑物内外的出/入口对人（或物）的进、出，实施放行、拒绝、记录和报警等操作的一种电子自动化系统，通常又叫出/入口控制系统。系统的前端设备为各种出/入口目标的识别装置和门锁启闭装置（执行机构），传输方式一般采用专线或网络传输，系统的终端为显示/控制/通信设备，可采用独立的控制器，也可以通过计算机网络对各控制器实施集中监控。门禁系统一般要与防盗报警系统、视频监控监视系统和消防系统联动，才能有效地实现安全防范。

巡更报警子系统通过预先编制的保安巡逻软件，应用通行卡读卡器对保安人员巡逻的运动状态（是否准时、遵守顺序等）进行监督和记录，并对意外情况及时报警。

智能建筑安防系统除了上述主要子系统外，通常还包括保安访客报警子系统及其他安防子系统。访客报警子系统使建筑物内部人员与访客可双向通话或可视通话，内部人员可对建筑物入口门或单元门实施遥控开启或关闭，并在意外情况发生时能向保安中心报警。其他安防子系统可根据安全防范管理的需要而设置。如汽车库综合管理系统，要对车库（场）内车辆通行道口实施出入控制、监视、行车信号的指示，以及停车计费等综合管理。重要仓储库安防系统，要对建筑物内的重要仓储库实施有效的门禁控制、防盗、监视控制和管理等。

1.2 数字安防

1. 数字安防的基本概念

随着自动控制技术、计算机技术和通信技术的发展，建筑与社区智能化建设获得了长足的发展，近十年来，我国大规模兴建的建筑和社区都配备了不同水平的智能化弱电系统。随着数字化理念逐步深入人心，社区的弱电系统开始走向数字化。为了促进科技创新，适应信息技术在社区中应用发展的需要，以及今后一段时期数字安防规划、建设的需要，数字安防理念和实现方法的讨论具有十分重要的意义。

数字安防是利用现代传感技术、数字信息处理技术、数字通信技术、计算机技术、多媒体技术和网络技术，实现社区各种安防信息的采集、处理、传输、显示和高

度集成共享，实现社区和家庭各种安防设备的自动化、智能化监控，营造高度安全、舒适的城市生活与工作社区。

数字安防是传统安防的进一步发展，数字安防除具有传统安防的主要功能外，还具有某些重要的数字化功能。传统安防建立在各种安防子系统结构的基础上，而数字安防则以网络结构为基础。数字安防更充分地实现了信息的数字化采集、处理、传输和显示，在更高水平上实现了信息的集成与共享。

社区数字安防是城市数字安防的单元节点，社区数字安防的建设是城市数字安防建设的基础。本文将重点讨论社区数字安防建设。

2. 数字安防的发展与现状

数字安防的提出和实施依赖于信息技术的发展及其产品性能价格比的迅速提高。随着微处理器和网络技术的普及，国外于 20 世纪 80 年代提出了智能化安防的基本框架，以建筑物内的数字通信设施为核心，配置面向商务用户的安防系统和资源控制系统，并逐渐增加了计算机网络和相应设施，出现了商住融合的概念。随着我国经济的发展，智能化安防在国内也有了广泛的应用。20 世纪 90 年代以后，因特网的普及和电子商务的应用迎来了信息社会的实用阶段，出现了大规模的信息基础建设和电子政务的实施，形成了有利于数字安防建设的良好外部环境，使数字安防建设不仅有了坚实的技术基础，而且进入了规范性发展的实用阶段。

随着信息技术发展和人民生活水平的提高，智能安防系统获得了长足的发展，为了适应信息技术的发展和数字城市的建设，数字安防的理念和建设数字安防有了更高的要求。数字安防是智能小区和智能社区安防系统发展的新阶段，它们之间既有紧密的联系又有区别。数字安防的主要特点表现在以下几个方面：

首先，数字安防进一步加强了网络的功能，能够接入局域网、广域网及因特网。通过完备的网络可以实现社区机电设备和家用电器的自动化、智能化远程监控，实现数字化安防系统的自动化、智能化监控。

其次，数字安防应用现代数字技术，包括现代传感技术、数字信息处理技术、数字通信技术、计算机技术、多媒体技术和网络技术，加快了信息传播的速度，提高了信息采集、传播、处理、显示的性能，增强了监控系统的安全性。

第三，数字安防提高了安防系统的集成程度，实现了信息和资源的充分共享，提高了系统的优化程度。

第四，数字安防是数字城市的基本单元，数字安防的建设为数字城市的建设创造了有利条件。

3. 数字安防的规划和设计应遵守下列主要原则

（1）需求导向原则：社区安防的基本需求和社区在城市总体规划中的定位是数字

安防设计的出发点。按需出发，实事求是，追求最大的性能价格比是社区规划设计的指针。当前应着重反对贪大求洋的做法。

（2）优化配置原则：数字安防应通过采用先进技术、利用集成和共享实现各种资源和配置的优化。

（3）国际化原则：数字安防的规划设计要采用国际化的有关标准，应具有充分的可兼容性、开放性和可扩张性。网络结构与协议要与因特网和国际主流网络技术兼容。

（4）技术创新原则：由于各地情况千差万别，各种技术、工艺日新月异，数字安防的建设与工程施工要充分发挥创造性，结合具体条件，提高数字安防的设计和施工建设水平。

数字安防的总体设计应整体规划，分阶段实施，以开放性互连网络体系为核心、以与社区密切相关的设施为重点、以用户的需求和承受能力及性能价格比为依据，逐步建立完善实施、验收的规范与标准。

数字安防的数字化设施及设备的配置原则应适合技术的发展趋势和标准化进程，适合用户的需求和承受能力。设施及设备可分为两个层次：基本配置与增强配置。基本配置是指与社区关联性较强，具有预留、预埋的要求，能保证数字安防的功能要求，以及具有目前和未来一段时期的先进性、示范性。增强配置是保证数字安防中公用建筑和会馆及高档住宅安防的功能要求，具有相当的前瞻性。两者都应具有技术的成熟性和设备标准化的要求。

4．数字安防的网络结构

1）数字安防的网络结构

社区安防数字化建设的核心是建设以信息网、监控网、电话和电视网为中心的社区网络系统，数字安防通过高效、便捷、安全的网络系统实现信息的高度集成与共享，实现安防设备的自动化、智能化监控。数字安防网络结构如图1-2所示。

社区数字安防建设是一个不断改进和完善的过程，随着技术的进步、我国体制和行政管理改革的不断深化，目前，由监控网、信息网、电话和电视网组成的社区数字化综合网可逐步融合为一个统一的社区网络。融合统一后的网络将进一步提高社区数字安防的水平，实现资源、信息的共享和设备、配置的优化。

2）数字安防网络的层次

数字安防网络层次如图1-3所示。

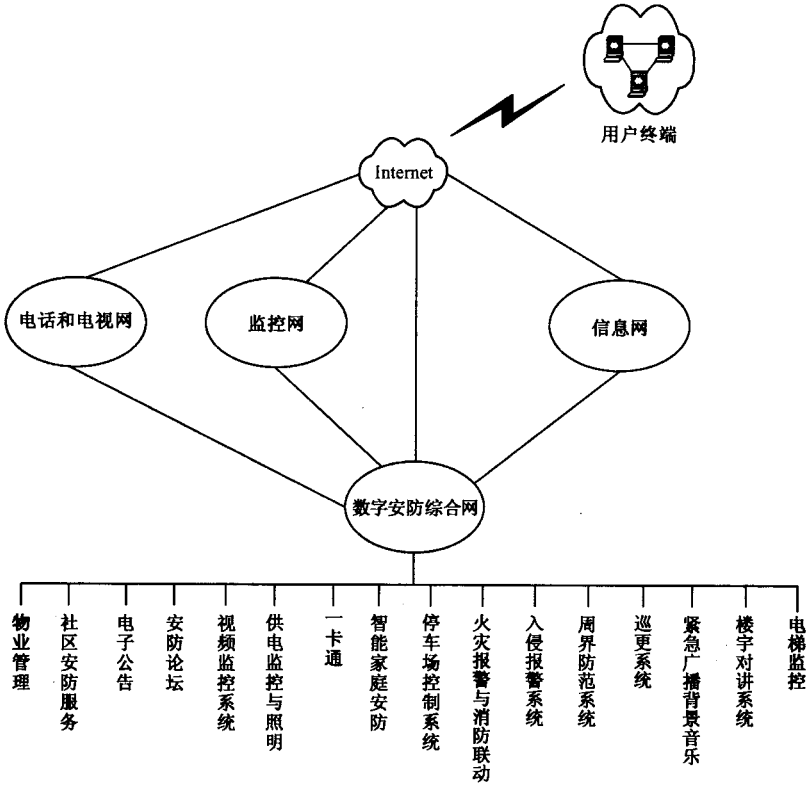

图 1-2　数字安防网络结构图

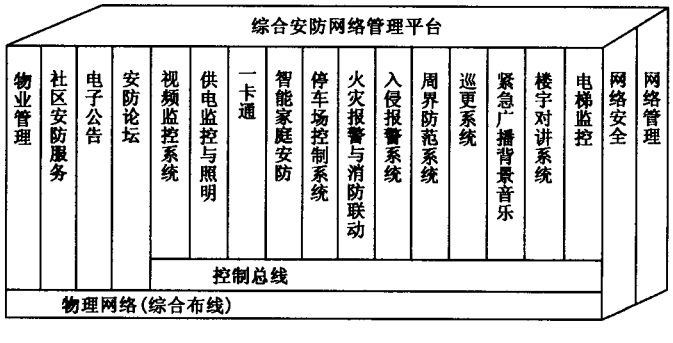

图 1-3　数字安防网络层次图

3）数字安防的物理拓扑

数字安防的物理拓扑图如图 1-4 所示。

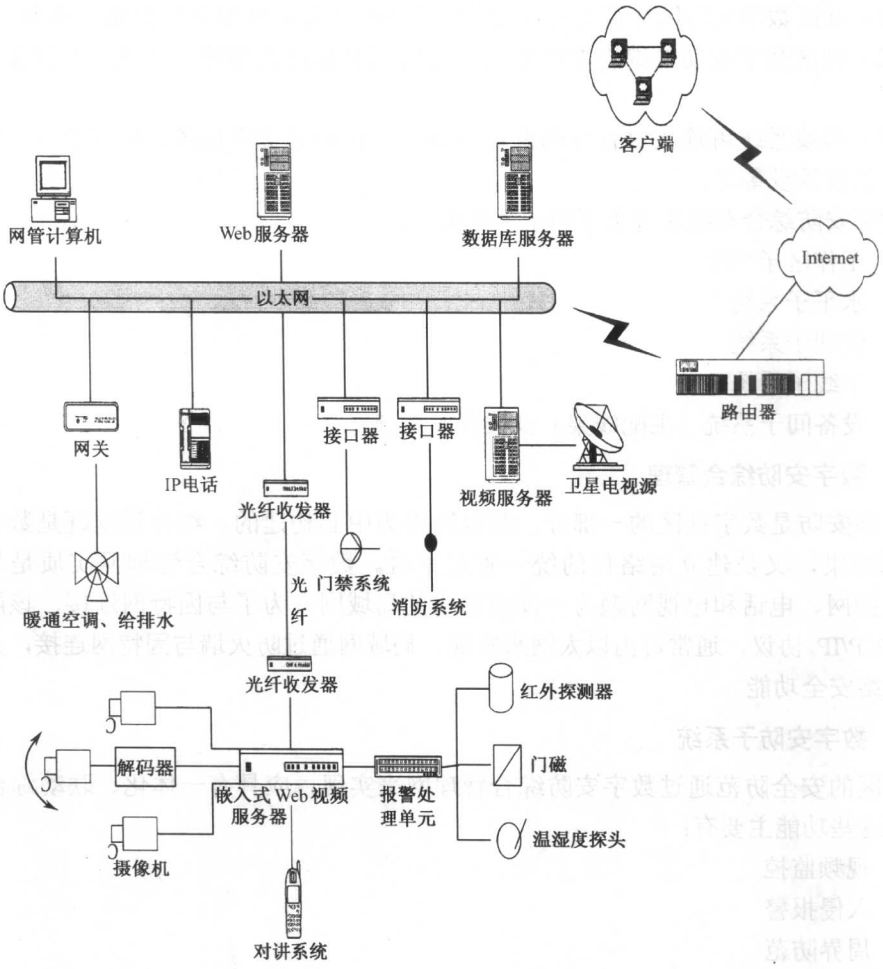

图 1-4 数字安防的物理拓扑图

1.3 数字安防的功能

1. 结构化综合布线

社区通信网络应采用结构化综合布线系统，实现社区数字安防建设的一体化、标准化和模块化，同时又满足现在应用要求，建成适应未来发展的开放式网络基础架构。

综合布线系统是数字安防的网络传输平台。使音、视频和数据通信设备、交换设备和其他信息管理系统彼此相连，同时又使这些设备能与外部通信网络连接。

综合布线系统应能满足下列主要应用要求：