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。

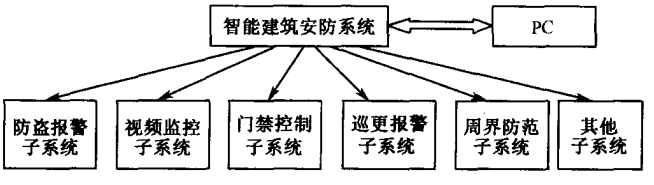

图 1-1　智能建筑安防系统组成框图

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。

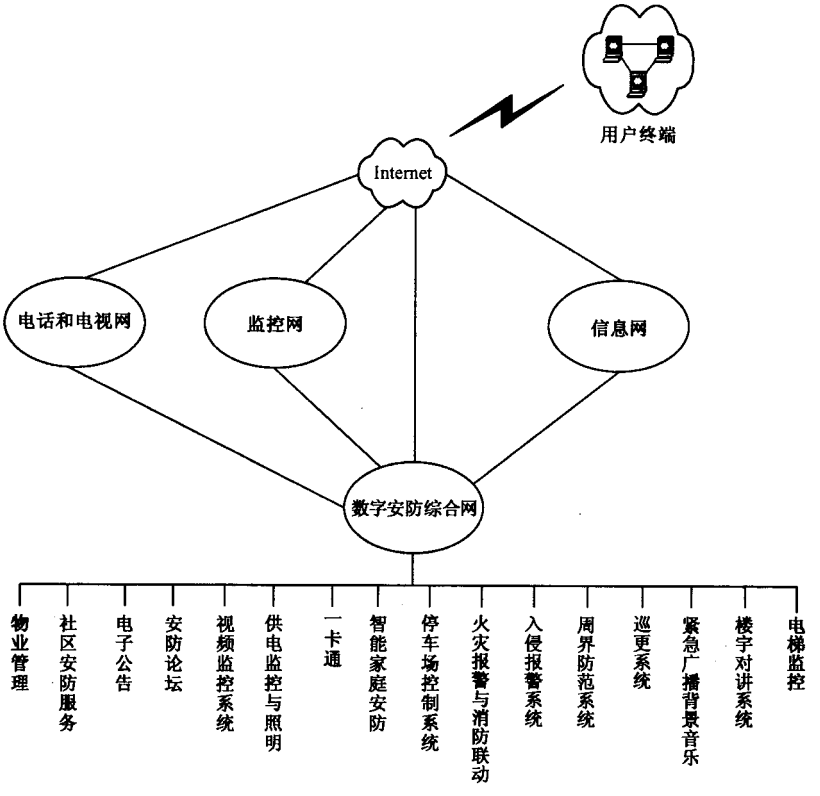

图 1-2　数字安防网络结构图

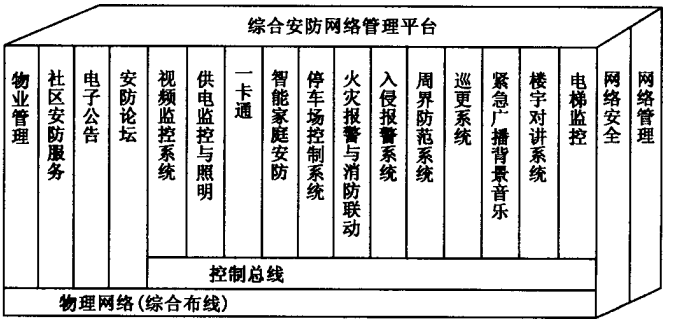

图 1-3　数字安防网络层次图

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。

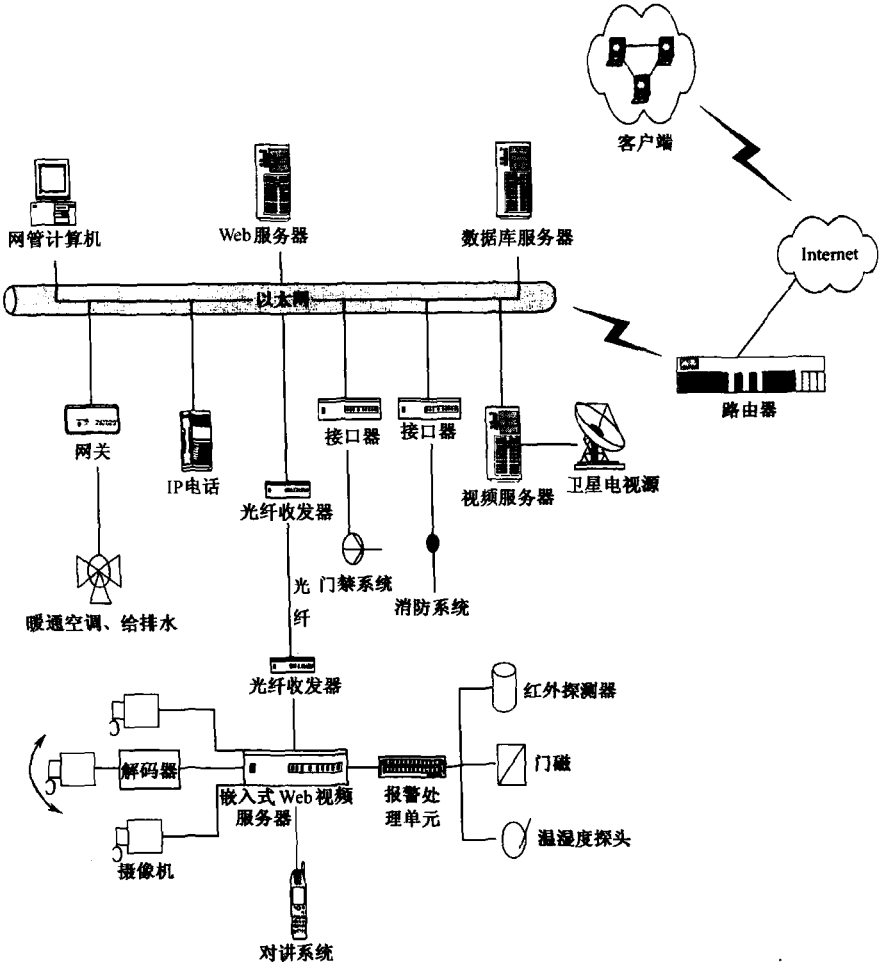

图 1-4　数字安防的物理拓扑图

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：

（1）社区数字安防网计算机具有与社区服务中心数据处理和数据通信能力。

（2）社区数字安防的综合布线系统能与外部通信网及因特网连接，进行数据通信交换。

（3）布线系统可连接语音与图像传输设备，如电话交换设备、视频会议、紧急广播和背景音乐设备等。

数字安防综合布线系统由下列子系统组成：

- 工作区子系统
- 水平子系统
- 管理子系统
  干线子系统
- 设备间子系统（主配线架）及楼群子系统

2．数字安防综合管理

数字安防是数字社区的一部分，是以网络为中心构建的。综合管理既是数字安防的理想结果，又是建立网络化的统一管理平台。数字安防综合管理网实质是与信息网、监控网、电话和电视网融为一体而形成的局域网。为了与因特网连接，该网络应采用 TCP/IP 协议，通常可由以太网来实现。局域网通过防火墙与因特网连接，具有良好的网络安全功能。

3．数字安防子系统

社区的安全防范通过数字安防综合管理网来实现，应具有一体化、联动综合防范功能，这些功能主要有：

- 视频监控
- 入侵报警
- 周界防范
- 出入口控制
- 巡更系统
- 楼宇对讲
- 智能家庭安防系统
- 电力供应监控
- 公共区照明
- 背景音乐与紧急广播
- 停车场管理
- 一卡通系统
- 社区安防服务

- 社区安防论坛

4. 消防系统

数字安防通过数字安防综合管理网实现社区的火灾自动报警和消防联动，可对消防态势进行实时监控。

5. 社区信息网功能

社区信息网、监控网、电话、电视网与社区数字安防综合管理网融为一体，对社区的安全防范起着重要作用。

1）社区网络服务

数字安防的社区服务通过社区网络实现，应具有以下基本功能：

- 社区安防论坛
- 社区安防网络教育
- 社区网络图书馆
- 社区电子政务
- 网络医疗保健服务
- 视频点播
- 网络（IP）电话

2）因特网服务

数字安防享有充分便利的因特网服务，这些服务应具有以下功能：

- 因特网带宽接入
- 远程监控
- 网上购物
- 远程教育
- 电子政务
- 网络信息服务
- GIS, RS, GPS 服务

3）电话、电视网功能

数字安防的电话、电视网是社区局域网的一部分，人员可通过电话、电视网实现社区现代化的电话、电视服务。

4 语音通信

人员可通过电话网实现社区普通语音通信和数字语音通信（IP 电话),完善的数字安防应提供社区内廉价的数字电话服务。

5)电视服务

数字安防通过电视网可提供完善的电视服务，包括：

- 有线电视服务
- 卫星电视服务
- 数字电视服务

6. 数字安防的物业管理

1）物业管理功能

数字安防的物业管理通过网络实现，具有以下基本功能：

（1）安防设施维修与管理

安防设施维修与管理包括小区、大楼、房间的安防设施的维修与管理，以及信息管理。

（2）住户登记与管理

住户登记与管理包括业主、租户、单位、家庭资料、家庭成员等信息的管理及业主满意度调查。

（3）电子公告

电子公告是社区内安防信息发布的平台，可显示、查询有关公共安防信息和安防管理信息。

（4）物业综合服务

物业综合服务用于协调管理各个安防子系统，使之处于良好运行状态。

2）社区安防管理的现状

社区安防管理与社区的物业管理紧密相连，但目前国内的物业管理尚未进入专业化、集约化的经营方式，多为一家物业管理公司管理一个楼盘。通常物业管理公司不成规模，造成其技术与管理的层次与能力不高。长期以来物业管理主要依赖于手工方式进行操作，随着数字化时代的到来，计算机、网络技术长足发展，物业管理中出现了手工、自动化并存的局面，加之社会对物业管理的认识尚未从“房管所”的概念转变过来，从业人员的地位不高，以及对专业人才的吸引力弱，所以，尽管国内的物业管理市场正不断地迅速发展及膨胀，需求日益扩大，但国内目前的物业管理服务水平，均与专业的物业管理服务有一定差距，这种状况影响了社区的安防。因此，大胆借鉴一些发达国家及地区的物业管理和安防管理的经验，探索符合国际惯例并适合中国国情的安防管理体系，建立社会化、专业化、企业化的安防管理新思路，是目前中国安防管理和物业管理行业发展的迫切需要。

3）数字安防管理和物业管理的要求

数字安防管理和物业管理急需解决的主要问题是：

（1）管理观念的改变

（2）管理制度的建立

（3）管理队伍的建设和人员培训

7. 数字安防的验收和评价

1）数字安防的分级

从目前我国的国情出发，数字安防可分为两个级别，即基本型与增强型。基本型与增强型的划分根据社区的需求和服务对象而定，数字安防的级别仅代表社区数字化安防程度的高低，并不能说明设计的先进水平的高低和工程质量的优劣。

2）数字安防的验收

数字安防全面、严格的验收应根据有关标准，由法定的机构进行严格测试，写出条目详细的测试报告，由有关部门组织专家进行评审验收。鉴于目前我国部分条件尚不成熟，验收过程可按功能验收的要求进行，即由有关部门组织专家对数字安防的各种系统、设备和网络构件，从功能上进行考察，给出相应的评价，进行验收。

3）数字安防全面验收

（1）数字安防全面验收报告的范围

- 关键产品检测报告
- 子系统检测报告
- 子系统接口检测报告
- 子系统、系统运行报告
- 网络运行检测报告

（2）数字安防全面验收的技术文档的范围

- 数字安防用户需求说明
- 各子系统工程设计文件
- 隐蔽工程检查记录
- 阶段验收报告
- 招标文件
- 投标文件
- 合同书
- 竣工图纸
- 工程变更说明
- 系统使用手册
- 用户使用报告

（3）数字安防功能验收要求

功能验收可分为基本型验收和增强型验收。

基本型和增强型都应达到技术的成熟性和设备的商品化、标准化的要求。具体要

求略。

1.4 门禁系统

由上一节的讲述可知，门禁系统属于智能建筑楼宇自动化系统（BAS）中的安防系统。作为一种新型现代化安全管理系统，门禁系统集自动识别技术和现代安全管理措施为一体，涉及电子、机械、光学、计算机技术、通信技术、生物技术等诸多新技术。门禁系统在建筑物内的主要管理区、出／入口、电梯厅、设备控制中心机房、贵重物品的库房等重要部位的通道口安装门磁、电控锁或控制器、读卡器等控制装置，由管理人员在中心控制室监控，能够对各通道口的位置、通行对象及通行时间、方向等进行实时控制或设定程序控制，从而实现对出／入口的安全控制。授权人员在其授权范围内通行无阻，在非授权范围禁止通行。门禁系统使任何人在任何时间段内通过任何出／入口进行事先设置、实时监视和事后检查成为现实。它能对所有人员的出入事件进行详细的记录，并有丰富的扩展功能。扩展功能主要包括实时巡更、身份核实、考勤管理和人员定位等。门禁系统是解决重要部门出／入口安全防范管理的有效措施。适用于银行、宾馆、机房、仓库、机要室、办公室、智能化小区、工厂等各种场合。

1. 门禁系统的组成

门禁系统通常由出入凭证、识别仪、门禁控制器、电控锁、其他设备和门禁软件组成。

1)出入凭证

出入凭证是门禁系统开门的“钥匙”，这个“钥匙”在不同的门禁系统中可以是磁卡、IC 卡等各种卡片，密码，或者是指纹、掌纹、虹膜、视网膜、脸面、声音等各种人体生物特征。

2 识别仪

识别仪负责读取出入凭证中的数据信息（或生物特征信息），并将这些信息传输到门禁控制器。

3 门禁控制器

门禁控制器是门禁系统的核心部分，相当于计算机的 CPU，它负责整个系统输入、输出信息的处理、储存和控制等。它验证识别仪输入信息的可靠性，并根据出入法则和管理规则判断其有效性，若有效则对执行部件发出动作信号。

4 电控锁

电控锁是门禁系统中的执行部件。根据门的材料、出门要求等不同可选取不同的锁具。主要有以下几种类型：

（1）电磁锁：电磁锁属断电开门型锁具，适用于单向的木门、玻璃门、防火门、对开的电动门。

（2）阳极锁：阳极锁属断电开门型锁具，适用于双向的木门、玻璃门、防火门，它本身带有门磁检测器，可随时检测门的安全状态。

（3）阴极锁：一般的阴极锁属通电开门型锁具。适用于单向木门。因为停电时阴极锁是锁门的，所以安装阴极锁一定要配备 UPS 电源。

其他设备：包括对出门无限制的情况下安装在门内侧的出门按钮，检测门的开／关状态的门磁，负责对整个门禁系统供电的电源等部分。

门禁软件：门禁软件负责门禁系统的监控、管理、查询等工作，监控人员通过门禁软件可对出／入口的状态、门禁控制器的工作状态进行监控管理，并可扩展完成巡更、考勤、人员定位等功能。

简单的系统信号框图如图 1-5 所示。

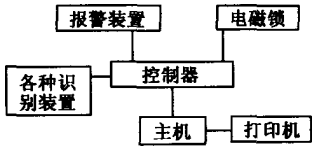

图 1-5　简单的系统信号框图

在图 1-5 中，出入人员首先在前端输入设备上进行身份识别，如：通过按键输入密码、在读卡器上划卡或出示指纹、掌纹等生物特征。识别设备再将读到的信息送到控制器，由控制器根据系统所存储的数据进行比较处理，发出各种控制命令：对合法出入，控制自动开门器开门；对非法出入，发出报警信号（或与其他报警监控系统联动）。每一次的出入都作为一个事件存储起来，以便进行处理或有选择地输出。对系统参数、人员授权的设置，可通过控制器按钮或系统主机实现。

2. 门禁系统的发展

门禁系统是在传统的门锁基础上发展而来的。现在，许多场合还在使用传统的门锁。传统的门锁是一种单纯的机械装置，虽然经过不断改进，安全性有所提高，但无论其结构设计多么合理，材料多么坚固，总能通过某种非正常手段把它打开，因此其安全性较差。对每个使用者来说，一把锁配一把钥匙，多把锁就需要配多把钥匙，使用起来不方便。在出入人较多的通道（办公室，酒店客房等），钥匙的管理也相当麻烦，遇到钥匙丢失或人员更换都要把锁和钥匙一起更换。

为了解决这些问题，出现了电子磁卡锁和电子密码锁，这两种锁的出现从一定程度上提高了人们对出入口通道的管理效率，使通道管理进入了电子时代。但随着这两种电子锁的不断应用，它们本身的缺陷就逐渐暴露出来：磁卡锁的信息容易复制，卡片与读卡机具之间磨损大，故障率高，安全系数低；密码锁的密码容易泄露，又无事件记录，安全系数很低；同时这个时期的产品由于大多采用识别仪与控制器一体设

计，必须安装在门外，很容易被人在室外打开门锁。因此这个时期的门禁系统还属早期不成熟阶段，被称为电子锁。

最近几年，随着自动识别技术的发展，门禁系统得到了飞跃式的发展，进入了成熟期，出现了乱序键盘门禁系统、 IC 卡式门禁系统、感应式门禁系统、各种生物识别门禁系统等应用各种技术的系统，这些门禁系统应用的自识别技术更为先进（感应技术、生物识别技术等），设计也趋于更合理，控制器与识别仪分体设计，识别仪安装在门外，控制器安装在门内，即只有识别仪对控制器的输入线露在门外，其他所有控制线均在门内，因此在安全性方面有很大提高，系统的可靠性、管理和使用的方便性等方面也有很大进步。

在与微机的通信方面，较早的门禁系统多为单机控制型。这种类型的门禁系统通常采用 RS485 通信方式，投资小，通信线路专用。但是一旦安装好就不能方便地更换管理中心的位置，不易实现网络控制和异地控制，适用于小系统或安装位置集中的单位。随着网络的普及应用，出现了网络型门禁系统。这种类型的门禁系统中门禁控制器与管理中心是通过局域网传递数据的，通信方式采用的是网络常用的 TCP/IP 协议，技术含量高，管理中心位置可以随时变更，不需重新布线，很容易实现网络控制或异地控制。适用于大系统或安装位置分散的单位，但是系统通信部分的稳定需要依赖于局域网的稳定。

随着人们对门禁系统各方面要求的不断提高，门禁系统的发展主要呈现出两种趋势：

1 门禁系统的应用范围越来越广泛

门禁系统的应用已不局限在单一的出／入口控制。它不仅可应用于智能大厦或智能小区的门禁控制，还可以应用在远程控制、停车场控制、电梯控制、交通管理或与其他系统联动控制等多种控制场合。

感应式门禁系统和生物辨识门禁系统成为门禁发展的两大热点。感应式门禁系统由于价格较低，使用简单，维护方便等诸多优点成为目前和今后研究使用的一大方向。随着技术的日渐成熟，生物辨识门禁系统成本将逐步降低，实用性不断提高，成为门禁系统发展的另一方向。

2 门禁系统的集成应用趋势

门禁系统可兼容多种读卡技术，同时具备先进的联网功能，通过联网组成智能大厦、智能小区等大型系统进行统一管理和监控。

3. 门禁系统的工作原理

门禁系统应用自识别技术，对进出人员的出入凭证与门的锁具开闭实现逻辑控制关系。根据出入凭证与识别方式，目前门禁系统工作方式可分为密码识别方式、卡片

识别方式、生物识别方式三种。

1）密码识别方式的门禁系统原理

这种门禁系统通过检验输入密码是否正确来识别进出权限，在系统前端有一个键盘（通常为 12 键或 16 键），门禁控制器中存储有主管码、主用码、客户码三类密码。不同类型的密码有不同的权限。使用者在进门前需要从键盘上输入密码，门禁控制器通过对键盘传输来的密码与存储的密码比较后判断是否开门。这种方式的门禁系统操作方便，无需携带卡片，成本低，但同时也存在着只能容纳三组密码、密码容易泄露、没有进出记录、口能单向控制等明显的缺陷。

为了提高密码识别方式门禁系统的安全性，出现了乱序键盘型门禁系统。这种门禁系统的工作原理与上述普通密码门禁系统一样，但它前端的键盘不是普通键盘，而是一种乱序键盘，键盘上的数字不固定，可以根据设置不定期自动变化键盘上数字排序，或者在用户键入一组密码后自动随机变换一次数字排序。每个数字的视锥角约为 10°，因此仅供一人可视，可以确保用户密码保密。这种门禁系统除了安全性稍高，成本较高外，其他特点与普通密码门禁系统类似。

2）卡片识别方式的门禁系统原理

卡片识别方式的门禁系统通过读卡或读卡加密码方式来管理进出权限。这种门禁系统的出入凭证为各类卡片（包括磁卡、接触式 IC 卡、非接触式 IC 卡等），识别仪为相应的读卡器。

如图 1-6 所示，磁卡是在符合国际标准的非磁性基片上用树脂粘贴磁条，贴在磁卡背面的磁条是一层薄薄的由定向排列的铁性氧化粒子组成的材料（也称为涂料），磁条上共有 3 个磁道，磁道 1、磁道 2 都是只读磁道，磁道 3 是读写磁道。磁条上记录的信息采用调频制编码技术，具有自同步能力。如图 1-7 所示，简单地说调频制编码技术就是在每个时钟周期 τ 内，磁通至少变化一次。如在每个周期中间产生磁通变化表示逻辑“ 1”，无磁通变化表示逻辑“ 0 ”。在磁卡插入读卡器中时，读卡器将读出的磁条中的信息送入门禁控制器，门禁控制器根据出入法则进行判断、执行、事件记录等功能。磁卡门禁系统成本较低，一人一卡，使用方便，可联微机，可记录开门事件，但磁卡与读卡器之间有磨损，寿命较短，而且磁卡容易被复制，卡内的信息容易因外界磁场而丢失，使卡片无效，因此安全性一般。

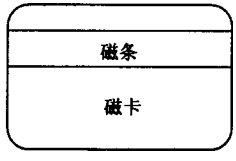

图 1-6　磁卡示意图

接触式 IC 卡是将一个集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。卡片内没有电源，但有存储器，可记录卡片号码、发行商信息，也可记录持卡人的信息，卡片表面有从 C1 到 C8 共 8 个触点。这 8 个触点的功能