



中华人民共和国公共安全行业标准

GA/T 669.1—2008
代替 GA/T 669—2006

城市监控报警联网系统 技术标准 第 1 部分：通用技术要求

Technical standard of city area monitoring and alarming network system—
Part 1: General specification

2008-08-29 发布

2008-08-29 实施

中华人民共和国公安部 发布



目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	3
4 联网系统设计原则	3
4.1 互通性	3
4.2 实用性	3
4.3 扩展性	3
4.4 规范性	3
4.5 易操作性	4
4.6 安全性	4
4.7 可靠性	4
4.8 可维护性	4
4.9 可管理性	4
4.10 经济性	4
5 联网系统结构	4
5.1 总体结构	4
5.2 组网模式	6
5.3 软件结构和基本功能模块	6
6 联网系统功能及性能要求	7
6.1 功能要求	7
6.2 性能要求	9
7 联网系统设备要求	9
7.1 信息采集设备	9
7.2 传输设备	10
7.3 视频编/解码设备	10
7.4 存储设备	10
7.5 视频切换设备	11
7.6 图像显示设备	11
7.7 网络服务器设备	11
7.8 用户终端设备	11
8 联网系统信息传输要求	12
8.1 通信协议结构	12
8.2 基于 SIP 的监控网络内部信息传输	12
8.3 基于 SIP 的监控网络与非 SIP 监控网络之间的信息传输	13

8.4 视音频编解码要求	13
9 联网系统安全性要求	14
9.1 物理安全	14
9.2 运行安全	15
9.3 信息安全	15
9.4 通信和网络安全	16
10 联网系统电磁兼容性要求	16
11 联网系统电源要求	16
12 联网系统环境与环境适应性要求	16
13 联网系统可靠性要求	16
14 联网系统运行和维护要求	17
14.1 硬件系统监测及维护	17
14.2 软件系统维护	17
14.3 数据维护	17
14.4 维护机构	17
附录 A (资料性附录) 推荐采用的联网系统组网模式	18
附录 B (资料性附录) 联网系统互联结构参考实例	22
参考文献	24

前 言

请注意,本部分的基本内容有可能涉及专利,本部分的发布机构不应承担识别这些专利的责任。

GA/T 669《城市监控报警联网系统 技术标准》分为 11 个部分:

- 第 1 部分:通用技术要求;
- 第 2 部分:安全技术要求;
- 第 3 部分:前端信息采集技术要求;
- 第 4 部分:视音频编、解码技术要求;
- 第 5 部分:信息传输、交换、控制技术要求;
- 第 6 部分:视音频显示、存储、播放技术要求;
- 第 7 部分:管理平台技术要求;
- 第 8 部分:传输平台技术要求;
- 第 9 部分:卡口信息识别、比对、监测系统技术要求;
- 第 10 部分:无线视音频监控系统技术要求;
- 第 11 部分:关键设备通用技术要求。

本部分为 GA/T 669 的第 1 部分。

本部分自实施之日起代替 GA/T 669—2006《城市监控报警联网系统通用技术要求》。

本部分与 GA/T 669—2006 相比,有如下变化:

- 涉及到范围、规范性引用文件、术语、定义和缩略语以及条文中的“本标准”改为“本部分”。

本部分的附录 A、附录 B 为资料性附录。

本部分由公安部科技局提出。

本部分由全国安全防范报警系统标准化技术委员会(SAC/TC 100)归口。

本部分起草单位:公安部科技局、公安部第一研究所、北京中盾安全技术开发公司、浙江省公安厅科技处、广东省公安厅科技处、武汉大学国家多媒体软件工程技术研究中心、北京联视神盾安防技术有限公司、北京国通创安报警网络技术有限公司、辽宁道亨视讯科技有限公司、天津天地伟业数码科技有限公司、上海三盾智能科技有限公司、杭州恒生数字设备科技有限公司、杭州浙大信达数码科技有限公司。

本部分主要起草人:陈朝武、李明甫、刘希清、张俊业、房子河、何青林、赵惠芳、栗红梅、胡瑞敏、施巨岭、张跃、蒋乐中、黄伟群、刘建、戴林、沈伟斌、查敏中、赵问道、秦嘉黎、王建勇、张本锋、李荣、崔云红、苗祥珠、侯鸿川。

本部分所代替标准的历次版本发布情况为:

- GA/T 669—2006。

引 言

经过多年的努力,我国安全防范技术和安全防范系统的实际应用取得了长足的进步,区域监控报警系统已遍布全国各地,初步形成了社会治安技术防范的基础网络。但是,这些已建成的报警监控系统大都相互独立、自成体系,彼此间缺少统一的规划和技术协调,不能在更大范围内(如一个城市区域)有效实现网络的互联、互通和信息共享,尚未形成完善的面向公安业务需求和社会公共安全综合应用的系统集成平台,影响了安全防范技术在城市社会治安综合防控体系建设中作用的发挥,不利于安全防范报警服务业的专业化、社会化。

为了实现城市范围内由不同设备、异构网络组成的各类报警监控系统间的互联、互通、互操作,综合利用各种监控和报警的信息资源,首先在城市范围内实现监控报警系统的联网,进而实现全省、全国联网,以提高社会公共安全的综合防控能力,特制定本部分。

城市监控报警联网系统的建设,需要一系列技术标准和管理、服务标准的支撑,本部分是支持城市监控报警联网系统建设的通用(基础)标准之一,与之相关的标准将陆续制定,并在实际工作中配套使用。



城市监控报警联网系统 技术标准

第 1 部分:通用技术要求

1 范围

GA/T 669 的本部分规定了城市监控报警联网系统(简称联网系统)的设计原则、系统结构、系统功能及性能要求、系统设备要求、信息传输要求、安全性要求、电磁兼容性要求、电源要求、环境与环境适应性要求、可靠性要求、运行和维护要求等通用性技术要求,是进行城市监控报警联网系统建设规划、方案设计、工程实施、系统检测、竣工验收以及与之相关的系统设备研发、生产的依据。

本部分适用于城市社会公共安全领域的监控报警联网系统,其他领域的监控报警联网系统可参考采用。

2 规范性引用文件

下列文件中的条款通过 GA/T 669 的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB 50198—1994 民用闭路监控电视系统工程技术规范

GB 50348—2004 安全防范工程技术规范

GA/T 367—2001 视频安防监控系统技术要求

GA/T 379.1~379.10—2002 报警传输系统串行数据接口的信息格式和协议(IEC 60839-7-1~60839-7-10:2001, IDT)

YD/T 1171—2001 IP 网络技术要求 网络性能参数与指标

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本部分。

3.1 术语和定义

3.1.1

城市监控报警联网系统 city area monitoring and alarming network system

以维护社会公共安全为目的,综合运用安全防范、通信、计算机网络、系统集成等技术,在城市范围内构建的具有信息采集/传输/控制/显示/存储/处理等功能的能够实现不同设备及系统间互联/互通和互控的综合网络系统。利用该系统,可对城市范围内需要防范和监控的目标实施有效的视频监控、报警处置,并可为城市应急体系建设提供相应的信息平台。

3.1.2

前端设备 front end device

联网系统中安装于监控现场的信息采集、编码/处理、存储、传输、安全控制等设备。

3.1.3

监控点 monitoring site

前端设备安装或监控的地点或场所。

3.1.4

监控中心 monitoring center

联网系统内特定的信息汇集、处理、共享节点,监控管理人员在此对联网系统进行集中管理、控制,对监控信息进行使用、处置。

联网系统的监控中心分为公安监控中心和社会监控中心。公安监控中心是指公安部门管理和使用的、具有接处警能力的监控中心,社会监控中心是指非公安性质的其他社会单位管理和使用的监控中心。

3.1.5

监控报警管理平台 monitoring and alarming management platform

城市监控报警联网系统的核心系统软件,对联网系统内的视频、音频、报警等各种信息资源进行集成及处理,对联网系统的设备、用户、网络、安全、业务等进行综合管理,实现联网系统所规定的相关功能。

3.1.6

用户终端 user terminal

经联网系统注册并授权的、对系统内的数据和/或设备有操作需求的客户端设备。本部分将用户终端分为公安用户终端和社会用户终端。公安用户终端是指由公安监控中心注册并授权的用户终端,社会用户终端是指由社会监控中心注册并授权的用户终端。

3.1.7

视频编码设备 video coding device

具有对视频信号进行数字采集、编码、网络传输功能的设备,并可带有音频处理、设备控制、视频移动侦测、图像存储和回放等特定功能。

3.1.8

视频解码设备 video decoding device

具有对数字压缩视频进行解码还原功能的设备,并可带有音频处理、设备控制、数据交换、图像分割显示等特定功能。

3.1.9

报警联动 action with alarm

报警事件发生时,触发与报警设备相关的其他系统、设备实现预设动作(如报警图像复核、照明控制、信息服务等)的过程。

3.1.10

图像质量 image quality

能够为观察者分辨的光学图像质量,它通常包括像素数量、分辨率、色彩还原性、图像轮廓还原性、灰度级和信噪比,但主要表现为信噪比。

3.1.11

数字接入 digital access

前端设备或区域监控报警系统通过数字传输通道将数字视音频信号传送到监控中心的接入方式。

3.1.12

模拟接入 analog access

前端设备或区域监控报警系统通过模拟传输通道将模拟视音频信号传送到监控中心的接入方式。

3.1.13

模数混合型监控系统 analog-digital mixed monitoring system

监控中心中同时存在模拟、数字两种信号控制和处理方式的监控系统。

3.1.14

数字型监控系统 digital monitoring system

监控中心中只存在数字信号控制和处理方式的监控系统。

3.1.15

公安专网 private network for public security

公安信息网络或其他有明确安全管理要求的公安机关专用的计算机网络。

3.2 缩略语

AVS	Audio Video coding Standard	音视频编码标准
B/S	Browser/Server	浏览器/服务器
CA	Certification Authority	认证中心
CIF	Common Intermediate Format	通用中间格式
CPU	Central Processing Unit	中央处理器
GIS	Geographic Information System	地理信息系统
IP	Internet Protocol	因特网协议
MPEG	Moving Picture Experts Group	运动图像专家组
PKI	Public Key Infrastructure	公钥基础设施
RTCP	Real-time Transport Control Protocol	实时传输控制协议
RTP	Real-time Transport Protocol	实时传输协议
RTSP	Real-Time Streaming Protocol	实时流化协议
SDIO	Secure Digital Input/Output	安全数字输入输出
SIP	Session Initiation Protocol	会话初始协议
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
UUID	Universally Unique Identifier	全局唯一标识符
USB	Universal Serial Bus	通用串行总线
VCR	Video Cassette Recoder	磁带录像机
VPN	Virtual Private Network	虚拟专用网络

4 联网系统设计原则

联网系统设计除应满足 GB 50348—2004 中 3.1 的要求外,还应遵从以下原则:

4.1 互通性

联网系统内监控中心之间、监控中心与系统前端设备/用户终端之间均应能有效地进行通信和共享数据,应能够实现不同厂商、不同规格的设备或系统间的兼容和互操作。

4.2 实用性

联网系统应能满足当地环境条件、监视对象、监控方式、维护保养以及投资规模等因素。应按照“技防、物防、人防相结合”、“探测、延迟、反应相协调”的原则,合理设置系统功能、正确进行系统配置和设备选型,保证具有较高的性价比,满足公安业务和社会公共安全管理的需求。

4.3 扩展性

联网系统的设计应采用模块化设计,以适应系统规模扩展、功能扩充、配套软件升级的需求。

4.4 规范性

系统设计应符合防护对象风险等级与防护级别的要求。控制协议、传输协议、接口协议、视音频编解码、视音频文件格式等除应符合本部分及其他城市监控报警联网系统相关标准中的规定外,还应符合相应国家标准、行业标准的规定。

4.5 易操作性

联网系统的管理软件应提供清晰、简洁、友好的中文人机交互界面,操控应简便、灵活、易学易用,便于管理和维护。

4.6 安全性

联网系统应采取有效的安全保护措施,防止系统被非法接入、非法攻击和病毒感染;系统具有防雷击、过载、断电、电磁干扰和人为破坏等综合安全防护措施。

4.7 可靠性

联网系统应采用成熟的技术和可靠的设备,关键设备应有备份或冗余措施,系统软件应有备份和维护保障能力,并具有较强的容错和系统恢复能力。

4.8 可维护性

联网系统应具备自检、故障诊断及故障弱化功能,在出现故障时,应能快速地确定故障点,并及时恢复。

4.9 可管理性

联网系统内的设备、网络、用户、性能和安全应便于管理和配置。

4.10 经济性

联网系统在保证符合标准规范、满足使用要求的前提下,系统应尽量简化,降低运行维护成本,达到系统一次性投资和长期运行维护成本最优的要求。

5 联网系统结构

5.1 总体结构

5.1.1 应用结构

联网系统构成主体可分成监控资源、传输网络、监控中心和用户终端四个部分。联网系统应用结构见图1。

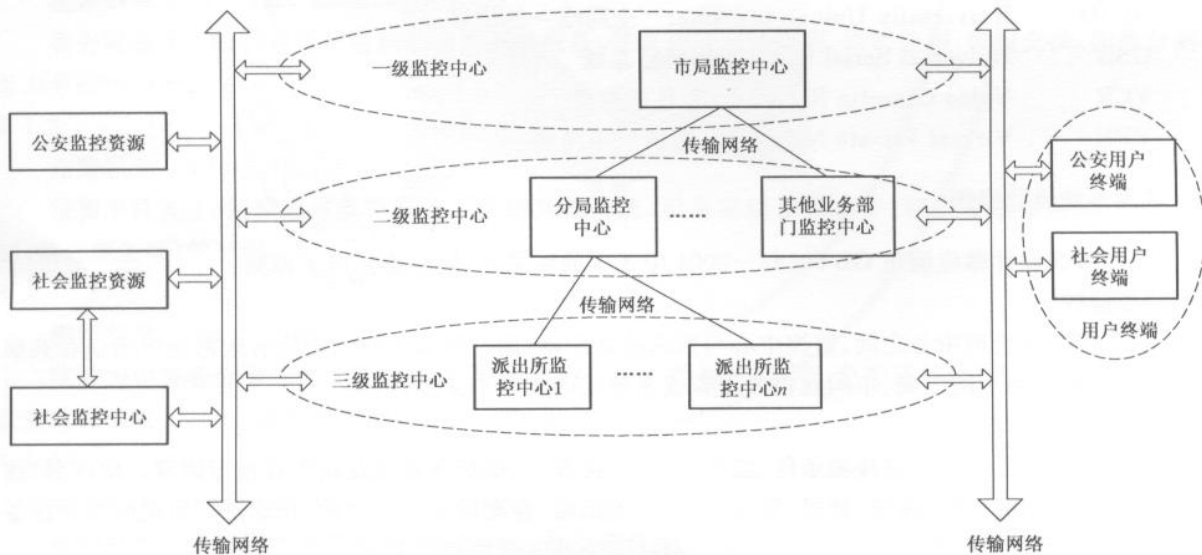


图1 联网系统应用结构

5.1.1.1 监控资源

监控资源指为联网系统提供监控信息的各种设备和系统,主要包括前端设备和区域监控报警系统。监控信息包括图像、声音、报警信号、业务数据等。监控资源分为公安监控资源和社会监控资源。社会监控资源可直接接入公安监控中心,也可先汇入社会监控中心后再接入公安监控中心。

区域监控报警系统由前端、传输/变换、控制/管理、显示/存储/处理四个基本部分组成,通常是一个

相对独立的系统,实际应用中可由入侵报警、视频安防监控、出入口控制、电子巡查、停车场安全管理等子系统根据需要进行组合或集成。区域监控报警系统输出的接口与信息格式应符合本部分的要求。

5.1.1.2 传输网络

传输网络可分为公安专网、公共通信网络和专为联网系统建设的独立网络等,其网络结构分为 IP 网络或/和非 IP 网络;传输方式由有线传输或/和无线传输构成。应根据实际情况选择传输方案。无论采用何种网络、何种传输方式,均应保证接入公安专网的安全。当公安专网资源满足需求时,应优先选择使用公安专网。

5.1.1.3 监控中心

公安监控中心宜分级设置:市局设置一级监控中心,分局和交警、消防等业务部门设置二级监控中心,派出所设置三级监控中心。公安监控中心的分级和数量宜根据实际需要设置,监控中心的建设重点宜设在派出所一级。

社会监控中心应提供相应接口,根据公安业务和社会公共安全管理的相关规定向公安监控中心提供本区域的特定的图像、报警及相关信息。

5.1.1.4 用户终端

用户终端包括公安用户终端和社会用户终端,可分为固定终端和移动终端。用户通过用户终端实现对监控资源的访问和控制,用户终端的行为受到监控中心的管理和授权。

5.1.2 互联结构

联网系统内的设备、系统(包括监控中心之间、监控中心与前端设备/用户终端之间)通过 IP 网络互联的结构见图 2。联网系统的互联结构参考实例参见附录 B。

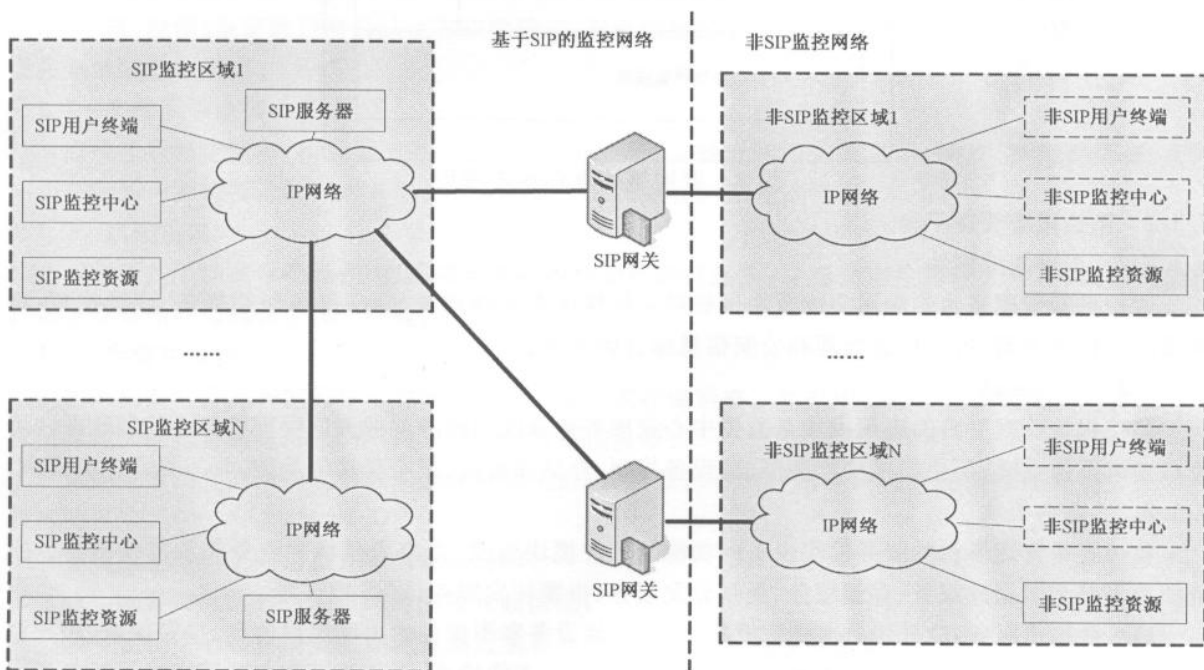


图 2 联网系统互联结构

联网系统的互联是基于 IP 网络、在应用层上实现的,包括对基于 SIP 的监控网络和非 SIP 监控网络的互联。基于 SIP 的监控网络可以直接连接到联网系统,非 SIP 监控网络则需通过 SIP 网关连接到联网系统。基于 SIP 的监控网络是指具有 SIP 服务器、且其中的监控资源、用户终端、监控中心等支持本部分及其他城市监控报警联网系统相关标准规定的 SIP 协议的监控网络;非 SIP 监控网络是指其中的监控资源、用户终端、监控中心等不支持本部分及其他城市监控报警联网系统相关标准规定的 SIP 协

议的监控网络；SIP 网关是指能实现本部分及其他城市监控报警联网系统相关标准规定的 SIP 协议与其他协议相互转换的设备。

5.2 组网模式

根据联网系统的功能需求，结合现有区域监控报警系统的结构模式和联网要求，联网系统的组网模式应能实现新建系统对原有系统的兼容。本部分推荐五种基本组网模式供参考。根据现场实际情况，可选择一种或综合其中几种模式进行组网，参见附录 A。

5.3 软件结构和基本功能模块

5.3.1 参考模型

监控报警管理平台是联网系统的核心系统软件。根据公安业务和社会公共安全管理的需求，推荐采用的联网系统软件参考模型见图 3。该模型在结构上包括应用集成模块、应用模块、服务模块、系统管理模块和系统协议模块。

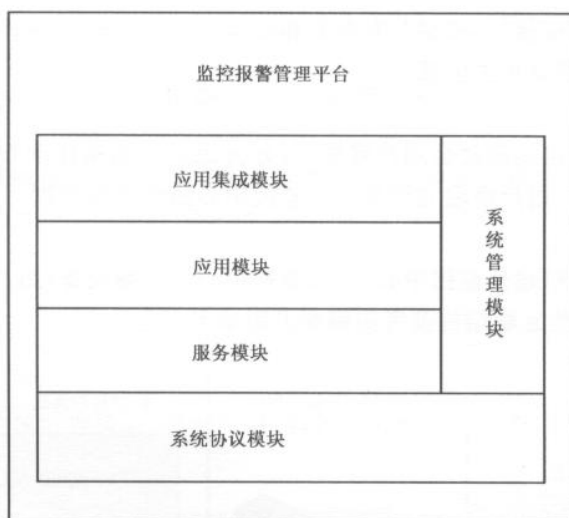


图 3 联网系统软件参考模型

5.3.2 监控报警管理平台

5.3.2.1 应用集成模块

监控报警管理平台的应用集成模块可根据实际情况有选择地实现，一般可包括报警、现场指挥、视频资料的快速查阅、报警信息处理和公安信息综合研判等。

5.3.2.2 应用模块

监控报警管理平台的应用模块是监控中心完成各种系统功能和图像调度管理的核心控制软件。可完成实时图像点播、历史图像检索和回放、设备控制、存储和备份、报警联动等功能，具体见 6.1 的要求。

5.3.2.3 服务模块

监控报警管理平台的服务模块由不同功能的软件模块组成，为应用模块和业务模块提供服务。服务模块可分为数据库服务、存储服务、视频分发服务、报警转发服务、Web 服务等。

- a) 数据库服务：应采用分布式数据库，应能存储设备和图像的索引和属性信息、报警信息、用户资料和权限、系统运行日志等，为设备管理、数据和图像检索、身份认证和权限管理提供服务。
- b) 存储服务：应能主要完成图像数据的存储、备份、管理。存储服务宜采用分布式存储和集中存储相结合的策略；应按照应用需求，选择适当的存储容量、存储带宽和响应时间的存储设备；按照数据的重要程度制定相应的备份策略。
- c) 视频分发服务：在多用户并发访问同一个图像资源时，应能提供视频分发服务。设定启动视频分发服务的触发条件（如并发连接数），当满足触发条件时，视频分发模块与视频编码设备建立单路连接，然后视频分发模块将图像分发给请求服务的设备。

- d) 报警转发服务:当报警发生时,报警转发服务模块应能实时接收来自报警设备的报警请求,并根据定制的处警策略将报警信息发送给具有处警能力的用户终端或相关系统。
- e) Web 服务:应能为远程用户登录系统、访问图像资源、控制前端设备等操作提供 B/S 方式的服务。

5.3.2.4 系统管理模块

系统管理模块应能负责对联网系统的用户和设备进行管理,具体要求如下:

- a) 用户和权限管理:设定管辖范围内用户、组的权限。用户管理可包括用户注册、用户查询、用户增加和删除、用户访问权限管理、用户锁定和解锁、用户分组、用户访问记录查看等;对系统的管理、视频浏览、前端设备控制、历史图像资料的删除、复制、浏览等操作行为的权限设定、权限收回等。
- b) 设备管理:软硬件的配置与查询;系统设备性能的实时监视;系统设备的故障报警、故障诊断与定位分析,报警日志的创建及维护等。
- c) 安全认证:验证用户的访问权限和优先级别,监测和记录用户的访问和操作;验证接入设备的合法性并注册合法设备等。

5.3.2.5 系统协议模块

系统协议模块应包括数据定义、通信协议和视音频编解码协议等,详见第 8 章的要求。

6 联网系统功能及性能要求

6.1 功能要求

联网系统应能实现不同设备及系统的互联、互通、互控,实现视音频及报警信息的采集、传输/变换、显示/存储、控制;应能进行身份认证和权限管理,保证信息的安全;应能实现报警联动;宜能提供与其他业务系统的数据接口。

6.1.1 实时图像点播

应能按照指定设备、指定通道进行图像的实时点播,支持点播图像的显示、缩放、抓拍和录像,支持多用户对同一图像资源的同时点播。宜支持基于 GIS 地图的图像点播。

6.1.2 远程控制

应能通过手动或自动操作,对前端设备的各种动作进行遥控;应能设定控制优先级,对级别高的用户请求应有相应措施保证优先响应。

6.1.3 存储和备份

宜采用前端存储和监控中心存储相结合的分布式存储策略。监控中心的数据库应能同时存储与录像资料相关的检索信息,如设备、通道、时间、报警信息等。

宜配置专用存储备份设备以长期保存相关信息,信息保存的时间应符合公安业务和社会公共安全管理的要

求。系统应能存储下列信息并保持相应时间:

- a) 报警发生前后一段时间内的视音频信息;
- b) 监控中心操作员人工指定或通过编程定时指定的现场视音频信息。

6.1.4 历史图像的检索和回放

应能按照指定设备、通道、时间、报警信息等要素检索历史图像资料并回放和下载;回放应支持正常播放、快速播放、慢速播放、逐帧进退、画面暂停、图像抓拍等;应能支持回放图像的缩放显示。

6.1.5 报警管理

6.1.5.1 报警信息的接收和分发

应能实时接收报警源发送来的报警信息,根据报警处置预案将报警信息及时分发给相应的用户终端或系统、设备。报警信号的信息格式和传输协议可参考 GA/T 379—2002 中的相关要求。

6.1.5.2 报警联动

若报警位置存在监控设备,当报警发生时系统应能通过预设方式自动触发图像复核和/或声音复核设备进行报警复核,并同时触发录像录音设备进行记录或存储。

系统宜支持与其他警用业务系统进行报警联动。

6.1.5.3 报警记录

当发生报警时,监控中心应记录报警的详细信息,如报警源地址、报警源所属组织、报警级别、报警类型、报警时间、处警时间、处警结果等。

6.1.6 与其他系统的数据接口

联网系统可提供与其他信息系统的互联接口。宜能与“三台合一”接处警系统、应急指挥系统、GIS地理信息系统、卡口监控管理、交通监控管理等各警务技术系统互联,实现更大规模的系统集成。

6.1.7 语音功能

根据应用需要(如声音复核、通信指挥等),监控中心之间宜能支持语音双向对讲功能,监控点和监控中心之间宜能支持语音双向对讲或语音广播功能。

6.1.8 人机交互

人机交互应满足如下要求:

- a) 具有直观、友好、简洁的中文人机交互界面;
- b) 具有视频画面分割显示、信息提示等处理功能;
- c) 能反映自身的运行情况,对正常、报警、故障等状态给出指示。

6.1.9 用户与权限管理

监控中心应具有对接入的用户进行授权和认证的功能。用户及权限管理可由各级监控中心独立执行,也可由指定的监控中心集中执行。用户及权限管理模块应定义用户对设备的操作权限、访问数据的权限和使用程序的权限。

监控中心的用户应有权限获取所辖范围内的历史图像和实时监视图像,当需要获取非管辖范围内的历史图像和实时图像时,应取得有效授权。

系统可提供对前端设备进行独占性控制的锁定及解锁功能,锁定和解锁方式可设定。

6.1.10 网络与设备管理

应能在监控管理平台管理范围内对系统设备、网络进行管理,收集、监测网络内的监控设备、报警设备、相关服务器的运行情况;对有权调用访问本级监控中心的用户应能进行监控;在联网系统内部应能实现实时工作时钟同步。

6.1.11 网络信息安全管理

联网系统应具备保证信息安全的功能,包括身份认证、设备认证、前端设备和社会监控中心的接入安全、移动监控系统的接入和传输安全、图像信息的防篡改等。具体要求见9.2、9.3、9.4和城市监控报警联网系统的其他相关标准。

6.1.12 日志管理

联网系统的日志包括运行日志和操作日志。运行日志应能记录系统内设备启动、自检、异常、故障、恢复、关闭等状态信息及发生时间;操作日志应能记录操作人员进入、退出系统的时间和主要操作情况。应具有支持日志信息查询和报表制作等功能。

6.1.13 监控智能化

根据应用需要宜在联网系统中采用智能化视频处理技术,如运动目标检测、轨迹跟踪、行为分析、目标识别、快速图像检索、多元信息融合分析等。系统中智能处理技术应用的位置宜尽量前移。

6.1.14 移动/无线监控

宜能支持前端设备的移动/无线接入和移动/无线用户终端的使用。

6.2 性能要求

6.2.1 网络带宽

联网系统网络带宽设计应能满足前端设备接入监控中心、监控中心互联、用户终端接入监控中心的带宽要求并留有余量。网络带宽的估算方法如下：

- a) 前端设备接入监控中心所需的网络带宽应不小于允许并发接入的视频路数×单路视频码率；
- b) 监控中心互联所需的网络带宽应不小于并发联接的视频路数×单路视频码率；
- c) 用户终端接入监控中心所需的网络带宽应不小于并发显示的视频路数×单路视频码率；
- d) 预留的网络带宽应根据联网系统的应用情况确定，一般应包括其他业务数据传输带宽、业务扩展所需带宽和网络正常运行需要的冗余带宽。

CIF 分辨率的单路视频码率可按 512 kbps 估算(25 帧/秒)，4CIF 分辨率的单路视频码率可按 1 536 kbps 估算(25 帧/秒)。

6.2.2 监控中心内部及监控中心间互联的 IP 网络性能指标

监控中心内部及监控中心间互联的网络性能指标应符合 YD/T 1171—2001 中规定的 1 级(交互式)或 1 级以上服务质量等级。具体指标如下：

- a) 网络时延上限值为 400 ms；
- b) 时延抖动上限值为 50 ms；
- c) 丢包率上限值为 1×10^{-3} 。

6.2.3 端到端的信息延迟时间

当信息(可包括视音频信息、控制信息及报警信息等)经由 IP 网络传输时，端到端的信息延迟时间(包括发送端信息采集、编码、网络传输、信息接收端解码、显示等过程所经历的时间)应满足下列要求：

- a) 前端设备与信号直接接入的监控中心相应设备间端到端的信息延迟时间应不大于 2 s；
- b) 前端设备与用户终端设备间端到端的信息延迟时间应不大于 4 s。

6.2.4 视频报警联动响应时间

报警触发后，在本监控中心内触发并启动视频显示和记录所需的直接联动响应时间应不大于 4 s；报警图像的预录时间不小于 10 s。

6.2.5 系统图像质量

应保证图像信息的原始完整性，即在色彩还原性、图像轮廓还原性、灰度级、事件后继性等方面均应与现场场景保持最大相似性(主观评价)。系统的最终显示图像(主观评价)应达到四级(含四级)以上图像质量等级，对于电磁环境特别恶劣的现场，图像质量应不低于三级。图像质量的主观评价见 GB 50198—1994 中的 4.3。

应保证对目标监视的有效性。重要监控点图像存储、回放的图像分辨率宜满足 GA/T 367—2001 中 4.4.7 系统分级规定的一级(甲级)要求。系统分级参见 GA/T 367—2001 的附录 B。

经智能化处理的图像，其质量不受上述等级划分要求的限制。但对指定目标的智能化处理，其处理前后的主要图像特征信息应保持一致。

7 联网系统设备要求

联网系统设备主要由信息采集、视频编/解码、传输、切换、显示、存储、网络服务器、用户终端等设备组成。

7.1 信息采集设备

信号采集的范围宜包括图像、声音、报警信号，应根据不同的组网模式(前端接入方式)选用相应的设备，并满足下列要求：

7.1.1 图像采集设备应能清晰有效地采集到现场的图像。图像采集设备应能适应现场的照明条件，环境照度不满足视频监控要求时，应配置辅助照明，或采用微光/红外类摄像设备。

- 7.1.2 声音采集设备的性能(灵敏度、探测范围)应与监测范围相适应。
- 7.1.3 报警设备均应符合现行国家标准、行业标准的要求,并经检验或认证合格。
- 7.1.4 信息采集及相关的前端设备应具有防破坏和抗易损防护措施,安装应符合现场环境要求,并满足相应防护等级的要求。
- 7.1.5 信息采集设备应提供开放的控制接口。

7.2 传输设备

- 7.2.1 模拟视频传输方式应适合 PAL 制式;数字视频传输通道应采用 IP 方式,传输协议见第 8 章。
- 7.2.2 信号传输可采用有线和/或无线传输方式,传输网络可选用公安专用网络、自建监控报警网络或公共通信网络。采用无线或公共通信网络传输时传输设备应有信息安全管理措施。具体传输方式的选择详见 GB 50348—2004 中 3.11.1 要求。传输设备的选型详见 GB 50348—2004 中 3.11.3 要求。
- 7.2.3 应优先保证报警信号和控制信号的传输。

7.3 视频编/解码设备

7.3.1 视频编码设备

- a) 宜采用本部分所引用的 H.264 或 MPEG-4 视频编码标准,图像分辨率应支持 CIF(352×288)和/或 4CIF(704×576)并可调。宜支持 G.711/G.723.1/G.729 音频编解码标准。在适用于安防领域的 AVS 标准发布后,宜优先采用 AVS 标准。
- b) 应具有以太网接口,支持 TCP/IP 协议,宜扩展支持 SIP、RTSP、RTP、RTCP 等网络协议。
- c) 应具有 RS-232/RS-485/RS-422 数据通道,可用于支持常用控制协议。
- d) 宜支持 IP 组播技术。
- e) 编码输出应具有可设定的点对点、点对多点传输能力;多路输入的设备应支持由输入到编码输出的多点对一点或多点对多点的切换控制功能。
- f) 应具有视频移动侦测能力,可根据设置策略实现相应的编码、传输、存储或视频报警。
- g) 在重要场所或特殊应用时,应具有设备认证功能、防篡改功能及加密传输能力。
- h) 应提供二次开发的软件接口。

7.3.2 视频解码设备

- a) 应支持符合本部分及其他城市监控报警联网系统相关标准规定的各种视频编码格式,宜支持 G.711/G.723.1/G.729 音频编解码标准。
- b) 解码通道可单路或多路,模拟视频输出应为符合 PAL 制视频标准的复合视频信号(1.0 V_{p-p}, 75 Ω)。
- c) 应具有以太网接口,支持 TCP/IP 协议,宜扩展支持 SIP、RTSP、RTP、RTCP 等网络协议。
- d) 应具有报警联动功能。多路传输的视频解码设备,在收到报警联动信息时能自动切换到对应的视频通道。
- e) 在重要场所或特殊应用时,应具有设备认证功能及数字加密图像的解码能力。
- f) 应提供二次开发的软件接口。

7.4 存储设备

- 7.4.1 各级监控中心应根据安全管理的要求和存储策略合理配置存储设备。配置的专用存储设备(如磁盘阵列、网络存储系统、光盘刻录机等)应能备份需要长期保留的信息。
- 7.4.2 图像存储设备应满足如下要求:
 - a) 宜采用本部分及其他城市监控报警联网系统相关标准所引用的 H.264 或 MPEG-4 视频编码格式和文件格式进行图像存储。宜支持 G.711/G.723.1/G.729 等音频编解码标准实现音频同步存储。在适用于安防领域的 AVS 标准发布后,宜优先考虑采用 AVS 标准。
 - b) 应具有足够的存储空间。存储的图像数据应保证具有 CIF 格式的图像分辨率,重要目标和报警图像应具有 4CIF(704×576)的图像分辨率。存储时可结合视频移动侦测等技术做帧率调

整。监控图像存储时间宜不小于 15 d, 经过复核后的报警图像应按相应的公安业务和社会公共安全防范管理的相关要求作长期保存。在重要应用场合, 应采取对录像文件防篡改或确保文件完整性的相关措施。

- c) 应支持按图像的来源、记录时间、报警事件类别等多种方式对存储的图像数据进行检索, 应能支持多用户同时访问同一数据资源。
- d) 应支持图像记录、回放同时工作的双工模式, 宜支持图像高码流记录、低码流传输的双码流模式。
- e) 应具有以太网接口, 支持 TCP/IP 协议, 宜扩展支持 SIP、RTSP、RTP、RTCP 等网络协议。
- f) 应提供二次开发的软件接口。

7.4.3 其他信息存储设备应满足如下要求:

- a) 存储系统配置参数、系统管理日志、用户管理数据、报警文件等重要信息的设备宜具有冗余、纠错及自动备份等功能。
- b) 存储图像索引、摘要等信息的设备, 其存储空间应与对应的图像数据量相适应, 并支持与对应图像数据的同步更新。

7.5 视频切换设备

监控中心视频切换设备应满足如下要求:

- a) 图像切换应能通过手动或编程实现, 图像信号应能在指定的显示设备上固定显示或时序显示;
- b) 宜采用模块式结构, 容量应按系统规模确定, 并留有冗余;
- c) 应具有视频丢失检测报警和系统自诊断功能;
- d) 应提供 RS-232 或 RS-485 数据通道, 可用于支持常用控制协议;
- e) 宜能支持键盘、网络计算机双重控制方式;
- f) 应具有报警联动功能。

7.6 图像显示设备

宜根据需要和可能选择合适的显示器或大屏设备。

显示设备应能清晰显示现场实时图像。显示设备的分辨率指标应高于系统对采集、传输过程规定的分辨率指标。

7.7 网络服务器设备

网络服务器设备是监控中心内部网络上运行特定服务程序的计算机主机, 为监控报警管理平台软件运行提供硬件支持。监控报警管理平台应支持的服务程序包括数据库、视频分发、视频存储、认证、注册、设备代理等。

- a) 网络服务器设备的基本功能和性能应符合国家和行业相关产品标准的规定, 并经检验或认证合格;
- b) 网络服务器设备的 CPU、硬盘、网络接口等部件的技术指标应符合本部分及城市监控报警联网系统的其他相关标准的要求;
- c) 数据库、视频分发、安全认证等重要服务器宜采用双机备份的方式。

7.8 用户终端设备

用户终端设备应满足如下要求:

- a) 应具有远程浏览、控制等功能;
- b) 固定用户终端主机应采用通用多任务操作系统, 操作系统应带有通用的 Web 浏览器, 操作应简单, 易学易用; 主机应有 USB 接口和 10 Mbps 以上的以太网端口; 主机显示分辨率不小于 1024×768, 颜色位数不少于 16 位;
- c) 移动用户终端有 USB 或 SDIO 接口; 显示分辨率宜不小于 352×288。

8 联网系统信息传输要求

8.1 通信协议结构

联网系统内部进行视频/音频/数据等信息传输时,传输的过程应遵循本部分及其他城市监控报警联网系统相关标准所规定的通信协议,通信协议的结构见图 4。

联网系统在进行视音频传输及控制时应建立两个传输通道:信令/控制通道和视音频流通道。信令和控制通道用于在设备之间建立会话并传输控制命令;视音频流通道用于传输视音频数据,经过压缩编码的视音频流采用流媒体协议 RTP/RTCP 传输。视音频编解码、信令协议等内容见本部分及其他城市监控报警联网系统相关标准中的规定。

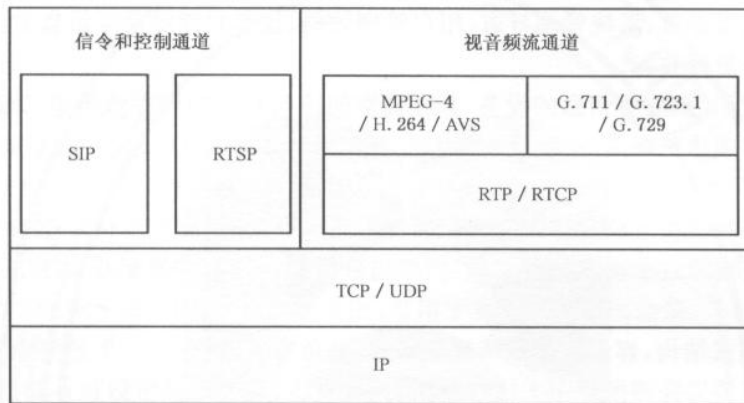


图 4 通信协议结构

8.2 基于 SIP 的监控网络内部信息传输

8.2.1 控制命令的传输

系统控制命令的传输应采用本部分及其他城市监控报警联网系统相关标准规定的 SIP 协议作会话控制,控制命令的定义见城市监控报警联网系统相关标准中的规定。控制命令的传输流程见图 5。

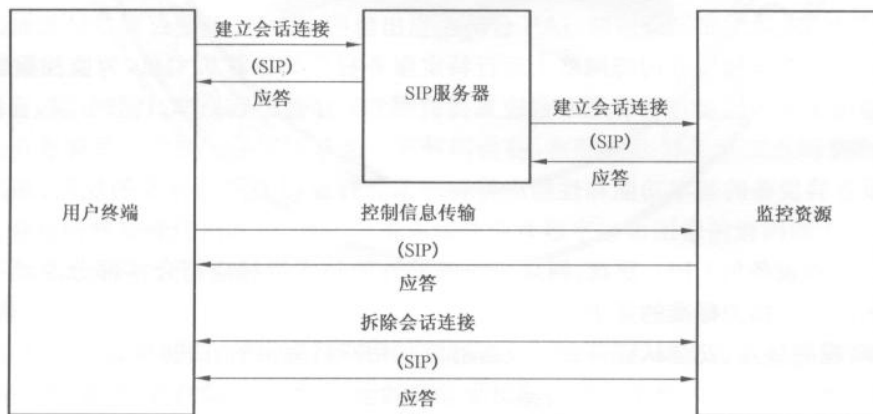


图 5 控制命令的传输

8.2.2 报警信息的传输

当报警发生时,服务器接收来自报警源的报警请求,根据处警策略将报警信息发送给具有处警能力的监控终端。报警源至服务器、服务器至监控终端的报警信息传输过程应采用本部分及其他城市监控报警联网系统相关标准规定的 SIP 协议作会话控制,报警信息的传输流程见图 6。

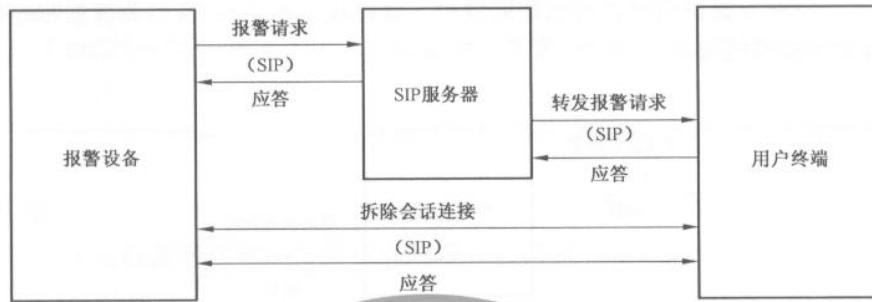


图 6 报警信息的传输

8.2.3 实时监控图像的传输

实时监控图像的传输应采用本部分及其他城市监控报警联网系统相关标准规定的 SIP 协议作会话控制, RTP/RTCP 协议传输视频流。实时监控图像的传输流程见图 7。

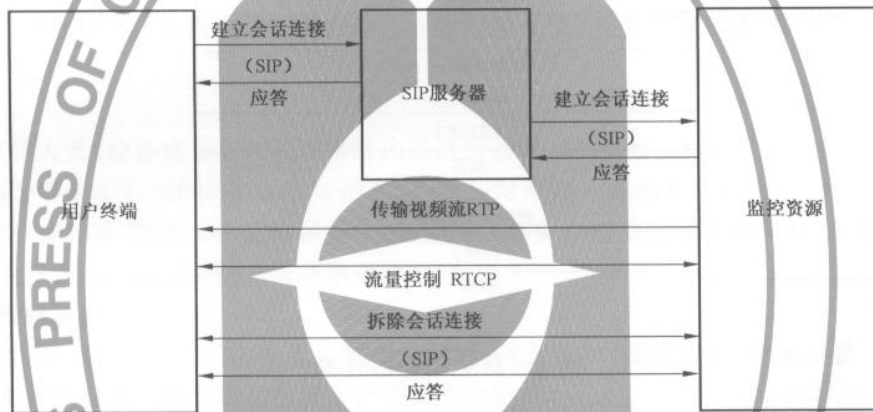


图 7 实时监控图像的传输

8.2.4 历史图像的传输

历史图像的传输应采用本部分及其他城市监控报警联网系统相关标准规定的 RTSP 协议作控制, RTP/RTCP 协议传输视频流。历史图像的传输流程见图 8。

8.3 基于 SIP 的监控网络与非 SIP 监控网络之间的信息传输

基于 SIP 的监控网络与非 SIP 监控网络之间通过 SIP 网关进行信息交换。其信息交换连接关系见图 9。

SIP 设备是指支持本部分及其他城市监控报警联网系统相关标准规定的 SIP 协议的设备;非 SIP 设备是指不支持本部分及其他城市监控报警联网系统相关标准规定的 SIP 协议的设备。

SIP 设备与非 SIP 设备之间的信息交换过程是:

- 非 SIP 设备通过 SIP 网关接入 SIP 服务器,此时 SIP 服务器将此 SIP 网关与非 SIP 设备一起视为一个虚拟 SIP 设备;
- 上述非 SIP 设备和 SIP 网关一起构成的虚拟 SIP 设备与其他 SIP 设备之间的信息交换过程同 8.2 的规定。

8.4 视音频编解码要求

联网系统采用的视音频编解码技术应满足下列要求:

8.4.1 联网系统的视频压缩编解码标准推荐采用 H. 264/MPEG-4;音频编解码标准推荐采用 G. 711/G. 723. 1/G. 729。在适用于安防领域的 AVS 标准发布后,宜优先采用 AVS 标准。

8.4.2 编码设备供应商应提供编码设备的解码模块。解码模块的结构、接口和校验程序应符合城市监控报警联网系统相关标准的规定。

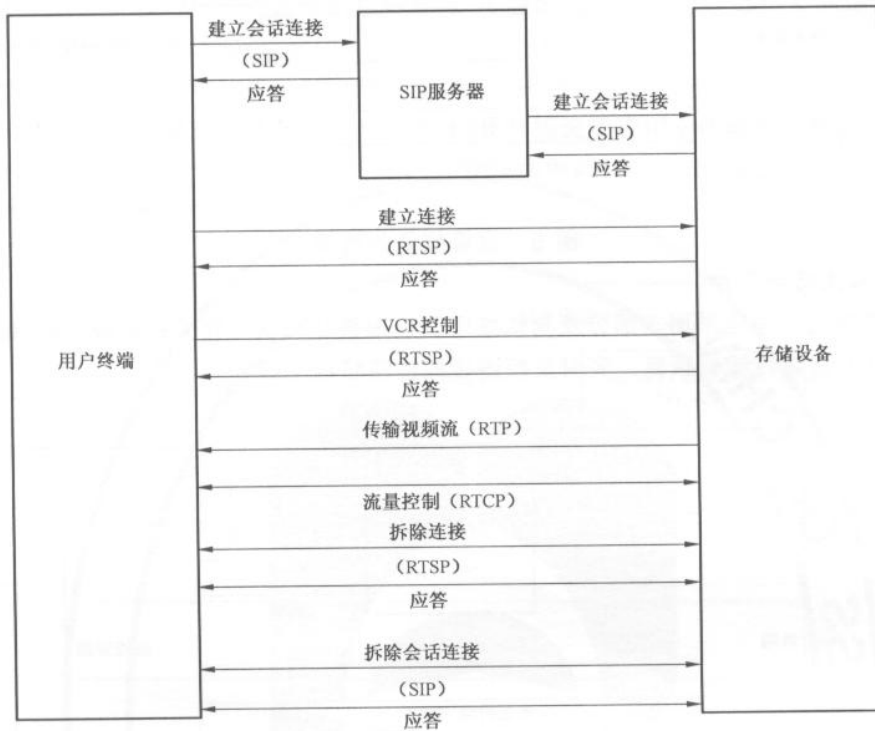


图 8 历史图像的传输

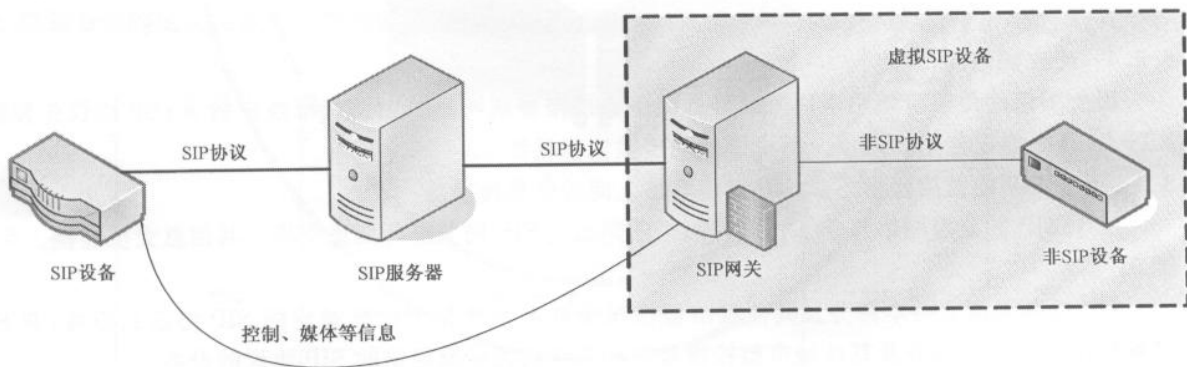


图 9 基于 SIP 的监控网络与非 SIP 监控网络之间信息交换连接关系

9 联网系统安全性要求

9.1 物理安全

9.1.1 环境安全

监控中心机房宜按照 GB/T 20271—2006 中 4.1.1.1 的要求,选择机房场地、实现机房内部安全防护、防火、供电配电、空调恒温、防水、防潮、防静电以及电磁防护。

通信线路的安全应按照 GB/T 20271—2006 中 4.1.1.2 的要求对通信线路进行安全防护。

9.1.2 设备安全

应按照 GB/T 20271—2006 中 4.1.2.1 的设备标记要求、计算中心防盗和机房外部设备的防盗要求实现设备的安全保护。

应按照 GB/T 20271—2006 中 4.1.2.2 的基本运行支持、安全可用要求和不间断运行要求设计和实现设备的可用性。

9.1.3 防雷接地

应综合设计系统的防雷和接地。系统各组成部分的防雷和接地设计应遵从 GB 50348—2004 中 3.9 的规定。

9.1.4 记录介质安全

应按照 GB/T 20271—2006 中 4.1.3 的公开数据介质保护、内部数据介质保护、重要数据介质保护、关键数据介质保护和核心数据介质保护的要求进行记录介质安全保护。

9.2 运行安全

9.2.1 网络安全监控

应按照 GB/T 20271—2006 中 4.2.3 的安全探测机制的要求,设置探测器,实时监听网络数据流,监视和记录内、外部用户出入网络的相关操作。宜使用防火墙、入侵检测系统、漏洞扫描工具来提高网络通信的安全性。

9.2.2 审计

指对被审计人员、设备或系统在联网系统内所进行活动的真实性、合法性、有效性进行审查和评价。

应按照 GB/T 20271—2006 中 4.2.4 的要求,支持对审计功能的开启和关闭、身份鉴别事件、系统管理员/安全员/审计员/操作员所实施的操作、其他与系统安全相关的事件做审计,并做好相应的审计响应,例如实时报警、违例进程终止、服务取消等措施。

9.2.3 恶意代码防护

应按照 GB/T 20271—2006 中 4.2.7 的严格管理、网关防护、整体防护、防管结合和多层防御的要求,对包括计算机病毒在内的恶意代码进行必要的安全防护。

9.2.4 备份与故障恢复

应按照 GB/T 20271—2006 中 4.2.6 的要求,对配置信息、用户信息、日志、报警记录等数据进行定期备份,关键存储部件宜采用冗余磁盘阵列技术并支持失效部件的在线更换,对重要的设备进行冗余配置以实现双机热备或者冷备,对重要的数据应做异地备份。

9.3 信息安全

9.3.1 身份认证

应对接入系统的设备和用户进行身份认证。设备应采用 UUID 进行唯一标识。宜采用基于 PKI/CA 体系的数字证书认证方式结合口令密码技术做双因子认证。

9.3.2 访问控制

在身份鉴别的基础上,系统宜采用某种访问控制模型对用户进行访问控制(例如基于角色的访问控制或者基于属性证书的访问控制)。

9.3.3 防抵赖

数据源应对需要防抵赖的数据进行数字签名运算。

9.3.4 完整性保护

系统宜采用数字摘要、数字时间戳及数字水印等技术防止信息的完整性被破坏。

9.3.5 数据保密

应对需要保密的数据在存储和传输过程中进行加密。

9.3.6 安全域隔离

应将联网系统划分为不同的安全域,如监控中心局域网、公安专网、公共网络等,不同的安全域之间

应进行相应的隔离。

9.4 通信和网络安全

9.4.1 网络传输的安全

当联网系统使用公安专网、公共网络、无线网络进行传输时,应分别符合相关部门对各个网络的安全管理规定或标准。

9.4.2 公安专网的接入安全

当其他网络需要与公安专网进行数据交换时,应采取相应措施保障公安专网的安全。宜在如下方案中选择:

- a) 将模拟视频输出信号接入由公安部门认可的视频编码设备,然后接入公安监控中心。视频编码设备既可放置在社会监控中心,也可放置在公安监控中心。
- b) 社会监控中心将数字图像单向传输给公安监控中心。当与公安专网接口时,应符合公安专网的安全管理规定。

9.4.3 双网并存

在公安监控中心设置两套完全物理隔离的监控系统,一套直接连接公安专网,另一套连接社会监控中心。

10 联网系统电磁兼容性要求

10.1 系统抗电磁干扰性能应满足 GA/T 367—2001 中 9.1 的要求;传输线路的抗干扰设计应符合 GB 50348—2004 中 3.6.2 的规定。

10.2 系统电磁辐射防护性能应满足 GA/T 367—2001 中 9.2 的要求。

11 联网系统电源要求

11.1 重要监控点应配置备用电源,备用电源应能延长供电不少于 8 h。

11.2 监控中心配电系统应满足系统运行的要求,并有一定的余量。监控中心应配备用电源,备用电源应能保证对监控中心内报警设备及监控核心设备延长供电不少于 8 h。

11.3 监控中心内系统宜采用两路独立电源供电,并在末端自动切换。电源质量应符合 GB 50348—2004 中 3.12.5 的要求。

12 联网系统环境与环境适应性要求

系统所使用设备的环境适应性应符合 GA/T 367—2001 中第 7 章的要求。

13 联网系统可靠性要求

13.1 监控中心关键设备应采取冗余设计,以保障系统正常运行或快速恢复。一级监控中心的关键设备宜采用双机热备的方式,保障系统不间断运行;二级、三级监控中心的关键设备宜根据系统规模采用冷备份或设置备品备件方式,采用冷备方式时系统恢复时间不应超过 30 min。

13.2 系统的设计应以结构化、规范化、模块化、集成化的方式实现,以提高系统的可靠性、可维修性和可维护性。各级监控中心的后台管理软件的设计应能保证当管理子系统出现故障时不影响系统中各业务功能子系统、各级子网络的运行;某一子系统、子网络发生故障时,不影响其他子系统、子网络的运行。

13.3 系统前端硬件设备宜采用支持固件在线升级的产品。当设备异常时应能自动重新启动或由监控中心控制其重新启动。

13.4 系统整体可靠性指标应在子系统、子系统所属各组成设备间进行逐级合理分配,各设备平均无故障时间(MTBF)应不小于其 MTBF 分配指标。系统硬件设备的平均无故障时间(MTBF)最低应不小于 20 000 h。对硬盘录像机中的硬盘可适当降低要求。

13.5 系统验收后的首次故障时间应不小于 90 d。

14 联网系统运行和维护要求

14.1 硬件系统监测及维护

14.1.1 硬件监测记录要求

- a) 应建立联网系统硬件设备性能参数表,性能参数由设备供应商提供;
- b) 应建立日常硬件监测、维护计划。结合硬件设备性能参数表,明确每天需要监测的硬件参数并记录。

14.1.2 硬件系统维护要求

- a) 前端设备的在线(“在线”是指设备处于与联网系统相连、处于正常工作状态、并能随时接受联网系统访问的状态)率应不低于 95%,监控中心内用户终端可用率应不低于 80%;
- b) 当监测到设备发生故障后,维护机构应在 4 h 内做出响应和初步判断,并根据故障的严重程度制定维修计划,重要设备的故障应在 12 h 内予以排除。

14.2 软件系统维护

软件系统维护包括操作系统维护和应用软件维护。

14.2.1 操作系统维护

当操作系统运行状态异常时,可通过重新启动、重新配置、重新安装操作系统等手段进行维护。

当操作系统存在缺陷,影响或可能影响应用软件系统的正常运行或威胁系统安全时,应能进行操作系统的升级或者更换其他操作系统。

14.2.2 应用软件维护

- a) 应用软件在使用过程中出现错误或发现潜在设计缺陷时,应能进行改正性维护;
- b) 当用户在使用过程中提出系统功能变动和改进需求时,应能进行完善性维护;
- c) 当应用软件的配置或硬件应用环境改变时,为了保证系统的正常稳定运行,应能进行适应性维护;
- d) 宜采用更新升级的维护机制,自动检查软件更新状态并提供更新部署。

14.3 数据维护

维护的数据可包括系统配置参数、系统管理日志、用户管理数据、视音频和报警数据等。

14.3.1 数据备份

应制定每日和每个数据更新周期(如 15d)的数据备份计划,每日宜对前一天的系统管理日志和用户管理数据的更新做备份,每个数据更新周期宜对本周期内的有用数据做备份。

14.3.2 数据恢复

数据恢复前应制定具体合理的恢复工作计划,数据恢复的方案应根据数据备份的方案制定,数据恢复完成后应检测数据的完整性。

14.3.3 数据整理

应制定计划,定期对系统内数据进行整理,清理不必要的数据、文件。

14.4 维护机构

应设立系统维护部门负责联网系统的维护工作。

系统维护部门的职责应包括以下三种:

- a) 制定维护计划;
- b) 执行日常维护和维修工作;
- c) 与系统承建商和/或设备供应商协调进行故障排除或升级改造等工作。

附录 A

(资料性附录)

推荐采用的联网系统组网模式

A.1 数字接入方式的模数混合型监控系统

监控中心中同时存在模拟、数字两种控制和处理设备,监控中心本地对视频图像的切换、控制通过视频切换设备完成,监控管理平台实现对数字视音频等数据的网络传输和管理。

视频编码设备放置在靠近前端设备处,将若干路模拟视频信号进行数字化、编码压缩,转换为可以在网络上传输的数据包(或直接使用网络摄像机),通过 IP 网络(有线/无线方式)传送到监控中心。在监控中心内,视频解码设备将数字视频信号转换成模拟视频信号接入视频切换设备。

本模式宜在监控点与监控中心之间使用 IP 网络传输的情况下改造原有模拟监控系统时采用,如图 A.1 所示。

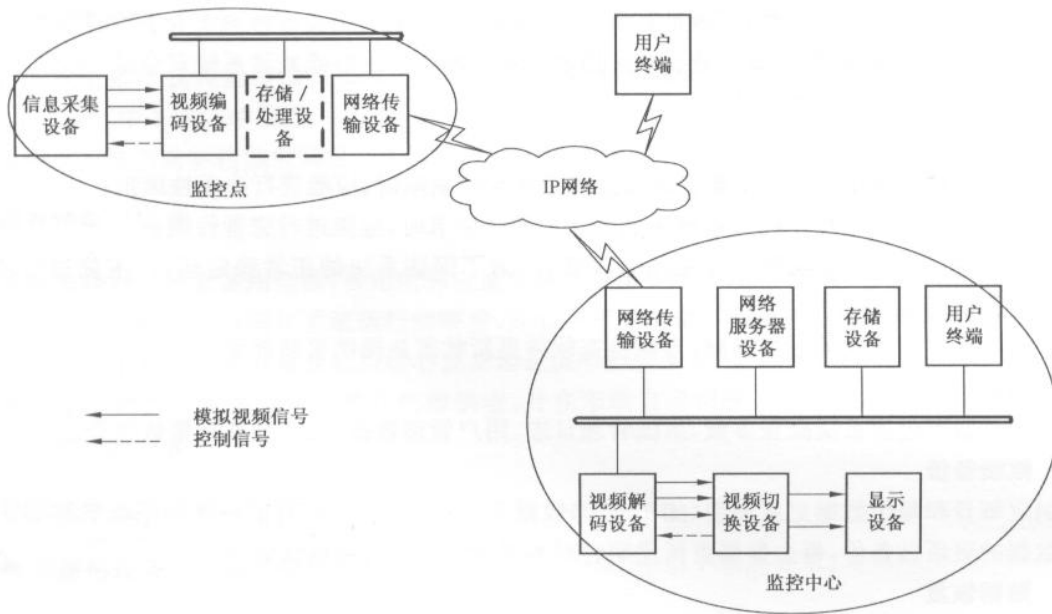


图 A.1 数字接入方式的模数混合型监控系统

A.2 模拟接入方式的模数混合型监控系统

监控中心中同时存在模拟、数字两种控制和处理设备,监控中心本地对视频图像的切换、控制通过视频图像切换设备完成,监控管理平台实现对数字视音频和控制等数据的网络传输和管理。

前端设备通过模拟视频传输设备将模拟视(音)频信号接入监控中心。

模拟视频信号接入监控中心网络的方式可以有两种:

- 视频分配器首先将每一路模拟视频信号分成两路输出,一路接入到视频切换设备,另一路接入到视频编码设备,见图 A.2 的监控中心 A;
- 模拟视频信号首先接入视频图像切换设备,视频图像切换设备的视频输出端分别接显示设备和视频编码设备,见图 A.2 的监控中心 B。

视频解码设备将数字视频解码后接入视频图像切换设备,送到显示设备供监视和浏览。

需要注意的是,为了实现统一控制的功能,应保证视频编码/解码设备能兼容视频图像切换矩阵。

本模式宜在监控点与监控中心之间使用专线传输情况下新建监控系统或者改造模拟监控系统时采用,如图 A.2 所示。

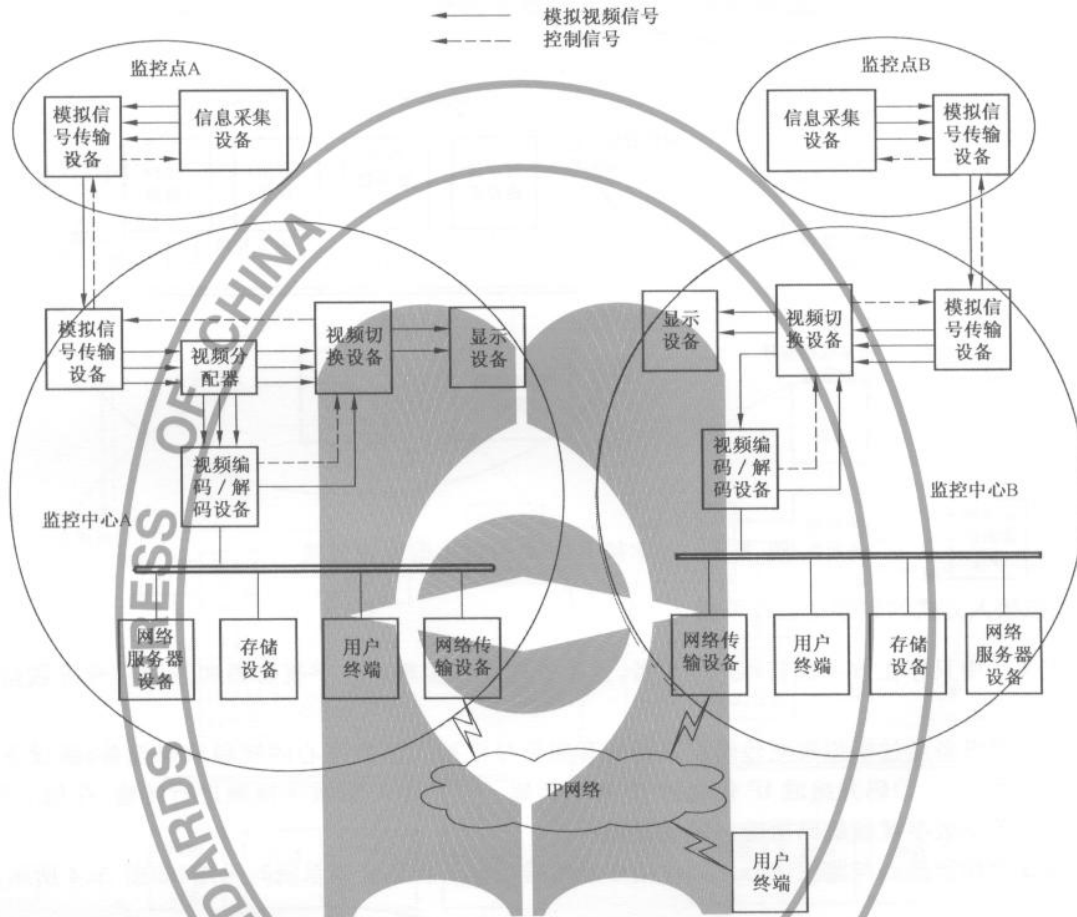


图 A.2 模拟接入方式的模数混合型监控系统

A.3 数字接入方式的数字型监控系统

监控中心中只存在数字控制和处理设备,监控管理平台实现对数字视音频和控制等数据的网络传输和管理。

视频编码设备放置在靠近前端设备处,将若干路模拟视频信号进行数字化、编码压缩,转换为可以在网络上传输的数据包(或直接使用网络摄像机),通过 IP 网络(有线/无线方式)传送到监控中心。监控中心对数字视频进行传输、存储和管理,视频解码设备将数字视频解码后送显示设备显示。

本模式宜在监控点和监控中心之间使用 IP 网络传输的情况下新建监控系统时采用,如图 A.3 所示。

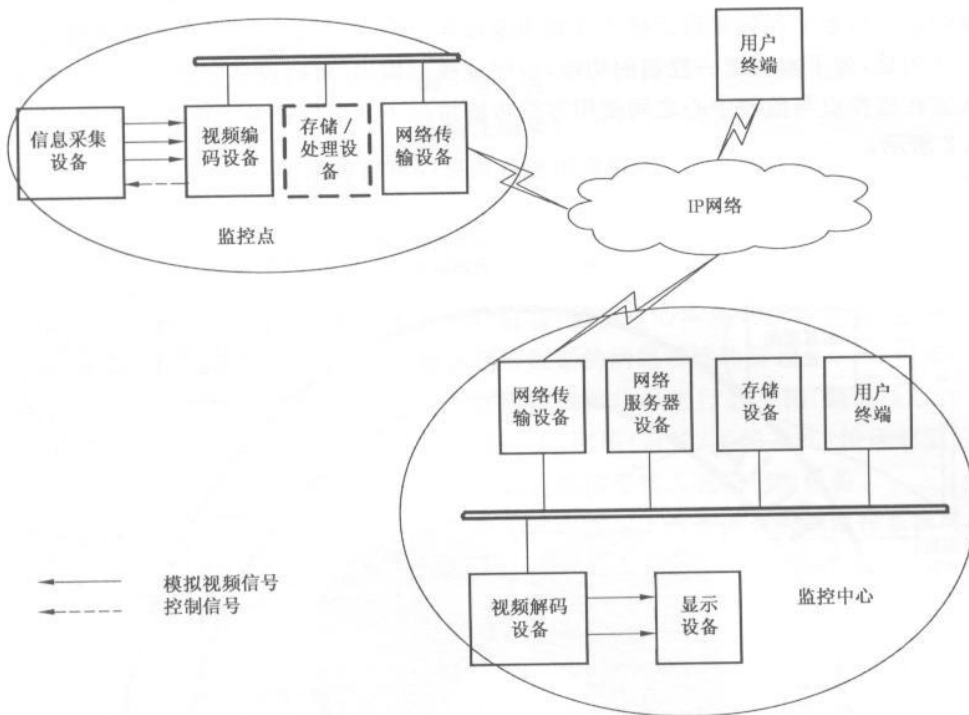


图 A.3 数字接入方式的数字型监控系统

A.4 模拟接入方式的数字型监控系统

监控中心中只存在数字控制和处理设备,监控管理平台实现对数字视音频和控制信号等数据的网络传输和管理。

监控前端设备通过模拟视频传输设备将视音频信号汇接入监控中心的视频编码设备,该设备将模拟视频信号数字化、编码并组成 IP 包通过 IP 网络传输。监控中心对数字视频进行传输、存储和管理,视频解码设备将数字视频解码后送显示设备显示。

本模式宜在监控点与监控中心之间使用专线传输情况下新建监控系统时采用,如图 A.4 所示。

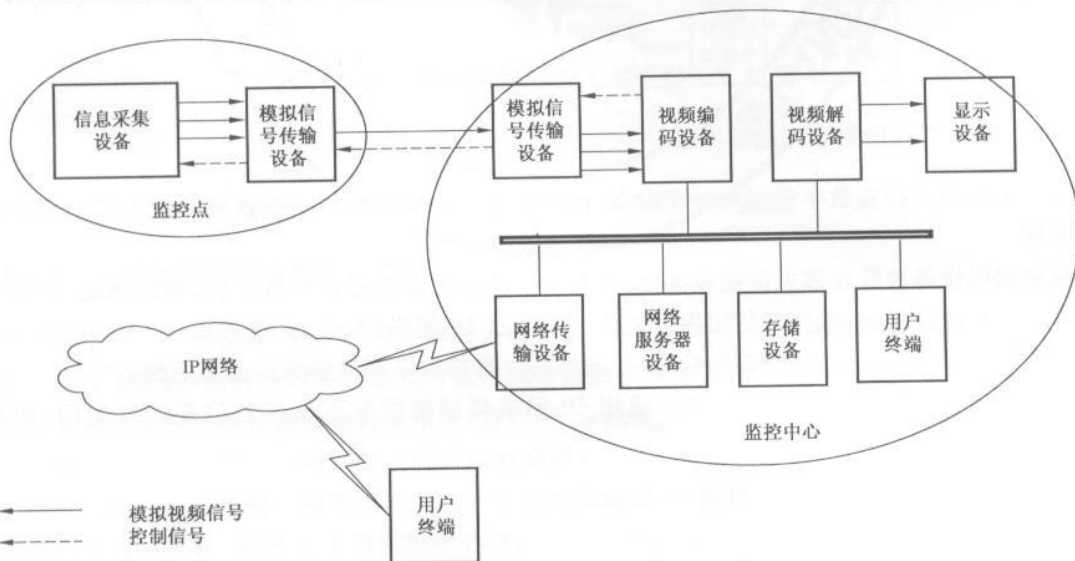


图 A.4 模拟接入方式的数字型监控系统

A.5 双级联方式的模数混合型监控系统

本模式在“模拟接入方式的模数混合型监控系统”(附录 A.2)的基础上,监控中心之间的级联采用模拟级联方式和数字级联方式,即监控中心之间通过模拟视频信号传输设备传输实时监视图像信号和 IP 网络传输实时监视图像和历史图像。

本模式宜在监控点与监控中心之间使用专线传输情况下改造模拟监控系统时采用,如图 A.5 所示。

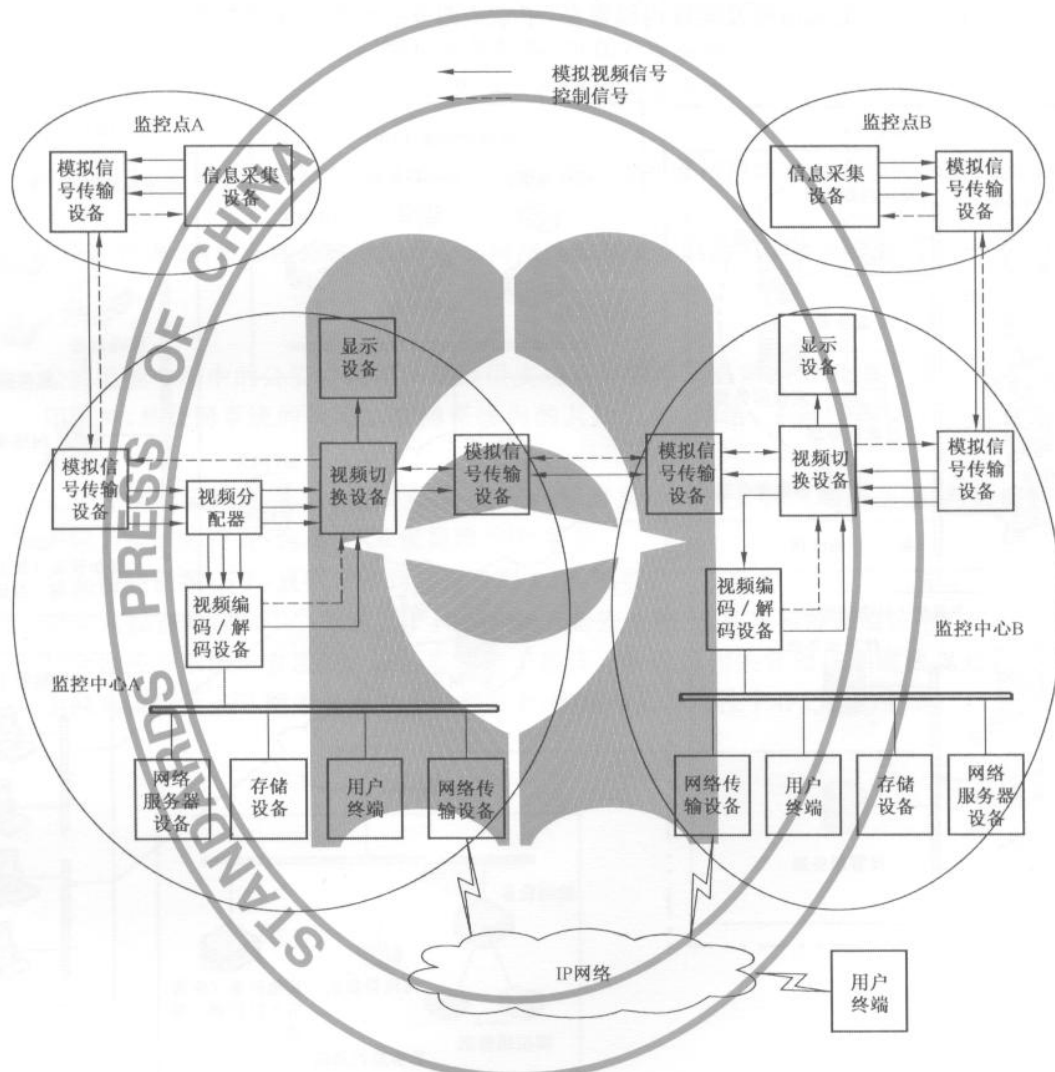


图 A.5 双级联方式的模数混合型监控系统

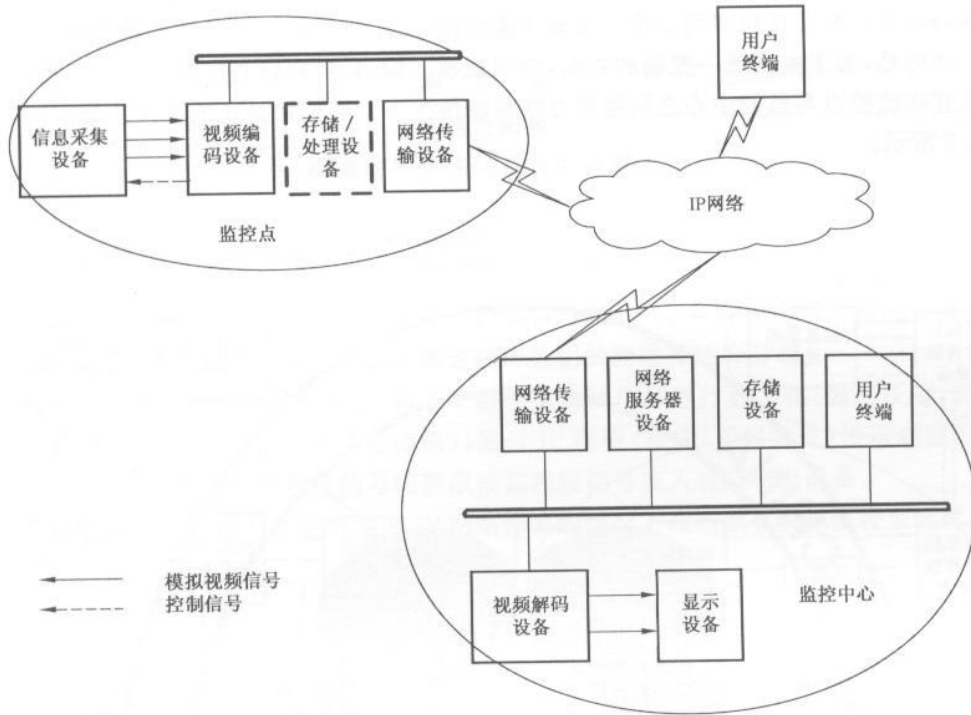


图 A.3 数字接入方式的数字型监控系统

A.4 模拟接入方式的数字型监控系统

监控中心中只存在数字控制和处理设备, 监控管理平台实现对数字视音频和控制信号等数据的网络传输和管理。

监控前端设备通过模拟视频传输设备将视音频信号汇接入监控中心的视频编码设备, 该设备将模拟视频信号数字化、编码并组成 IP 包通过 IP 网络传输。监控中心对数字视频进行传输、存储和管理, 视频解码设备将数字视频解码后送显示设备显示。

本模式宜在监控点与监控中心之间使用专线传输情况下新建监控系统时采用, 如图 A.4 所示。

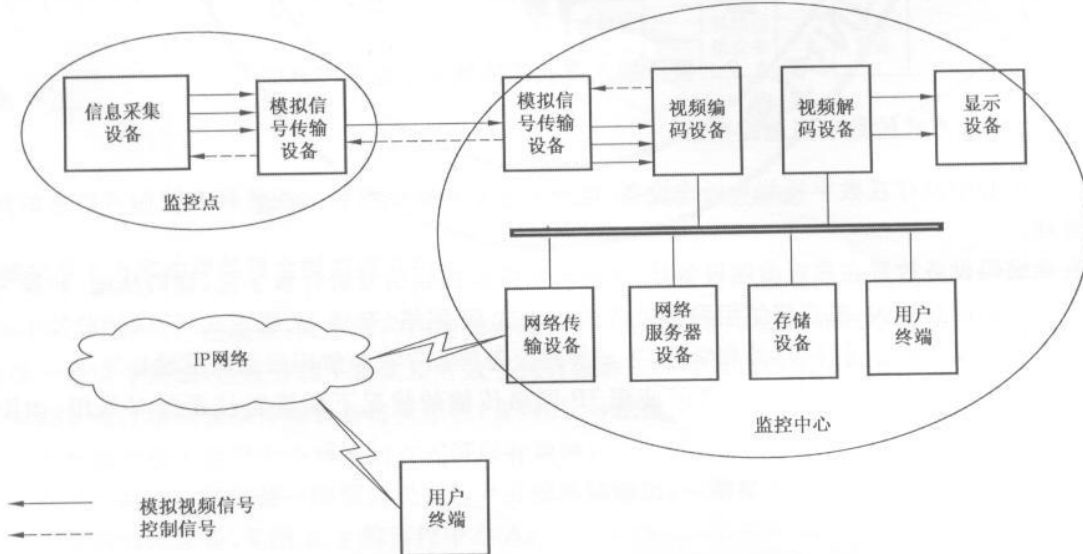


图 A.4 模拟接入方式的数字型监控系统

A.5 双级联方式的模数混合型监控系统

本模式在“模拟接入方式的模数混合型监控系统”(附录 A.2)的基础上,监控中心之间的级联采用模拟级联方式和数字级联方式,即监控中心之间通过模拟视频信号传输设备传输实时监视图像信号和 IP 网络传输实时监视图像和历史图像。

本模式宜在监控点与监控中心之间使用专线传输情况下改造模拟监控系统时采用,如图 A.5 所示。

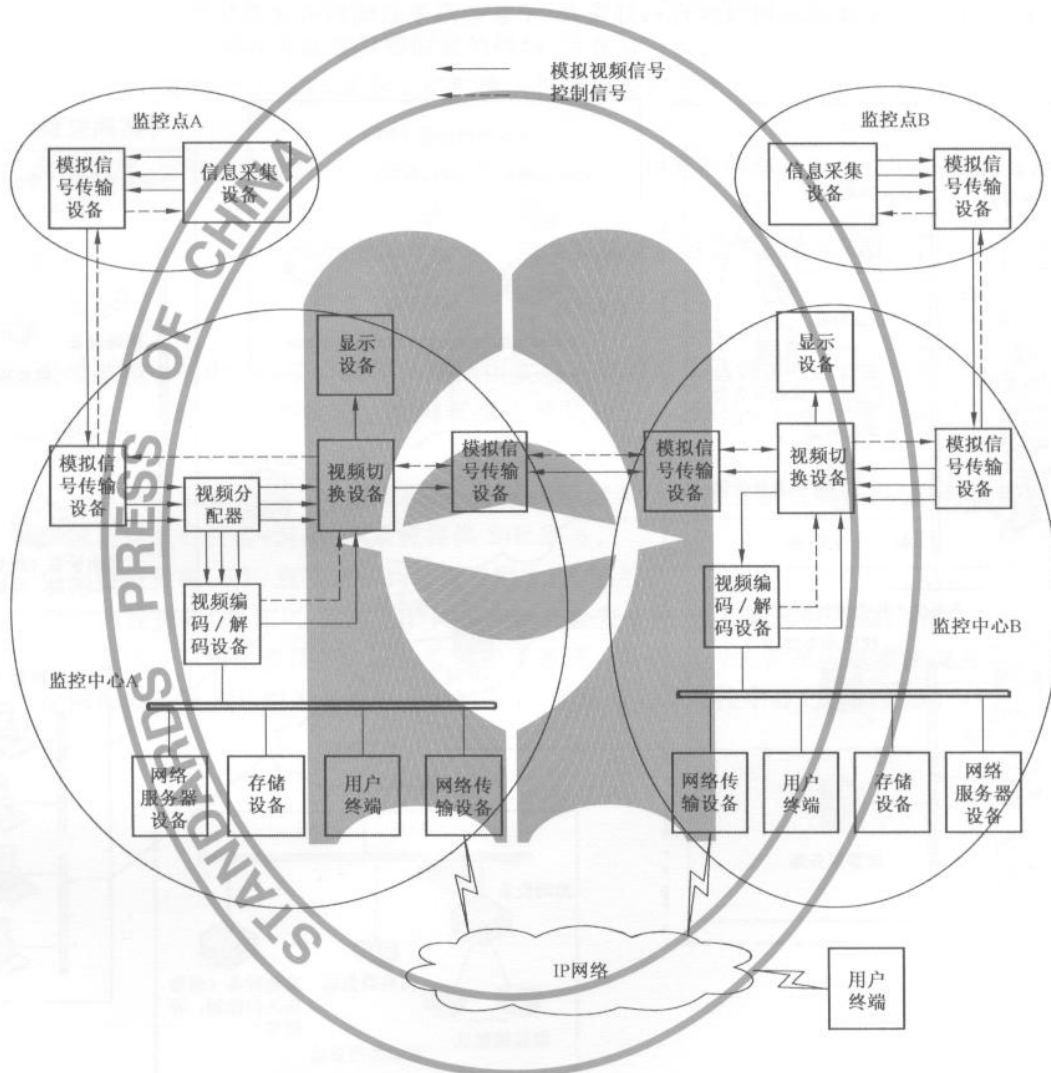


图 A.5 双级联方式的模数混合型监控系统

附录 B
(资料性附录)
联网系统互联结构参考实例

B.1 联网系统互联结构参考实例

联网系统内部主要组成结构及实现内部设备、子系统间互联的参考实例如图 B.1。

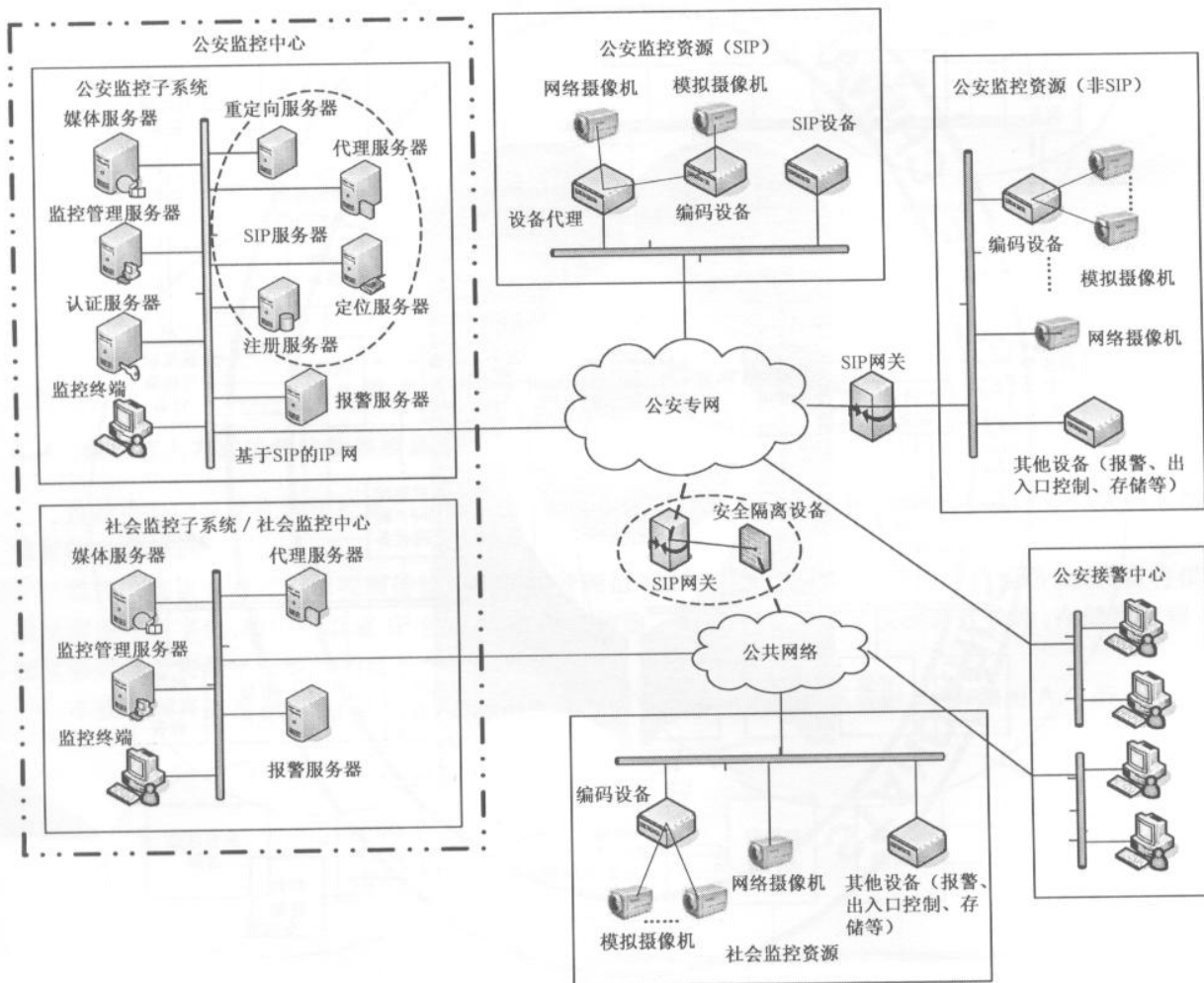


图 B.1 联网系统构成示意图

图 B.1 所示的联网系统主要由以下部分组成：

- a) 公安监控中心：内含公安专网监控和社会资源监控两个相互物理隔离的子系统，其中公安专网监控子系统中包含有可以提供 SIP 服务的各种服务器，所使用的内部网络为使用城市监控报警联网系统相关标准所规定的通信协议(SIP)的 SIP 网；社会资源监控子系统可以是一个社会监控中心，也可以是一台能够调用社会监控资源的监控终端；
- b) 公安监控资源(非 SIP)：公安专网内不支持本部分及其他城市监控报警联网系统相关标准规定的通信协议(SIP)的监控资源；

- c) 公安监控资源(SIP):公安专网内支持本部分及其他城市监控报警联网系统相关标准规定的通信协议(SIP)的监控资源,主要特征是内部网络及设备支持城市监控报警联网系统相关标准所规定的 SIP 协议;
- d) 社会监控子系统/社会监控中心:是指非公安性质的其他社会单位管理和使用的监控子系统/监控中心。主要特征是其网络环境是非公安专网;
- e) SIP 网关:负责在 SIP 网络与非 SIP 网络之间进行协议转换,以实现网络之间的信息交互;
- f) SIP 设备:支持本部分及其他城市监控报警联网系统相关标准规定的通信协议(SIP)的所有相关设备,如网络摄像机、编码器、报警、出入口控制、存储设备等;
- g) 公安接警中心:接收并处理报警信息的机构,可在公安监控中心内,也可在公安监控中心外;
- h) 公安专网:本部分 3.1.15 所定义的网络。目前相关管理标准或法规要求与公共网络之间实施物理隔离;
- i) 公共网络:所有不属于公安专网的 IP 网络。包括公共通信网络和专为联网系统建设的独立网络等;
- j) 安全隔离设备:负责在公安专网和公共网络间实施安全隔离的设备或设施。

B.2 互联方法

- a) 公安监控中心中的公安监控子系统提供实现系统联网所必需的 SIP 服务及其他各种监控应用服务,是联网系统的核心。联网系统内的其他设备、网络、子系统都要通过适当方式与其相联。
- b) 公安专网与公安监控中心直接相连,是联网系统实现内部互联的网络基础,与公安监控中心一起为接入的设备、网络、子系统提供 SIP 服务。
- c) 公安监控资源(SIP)直接连接到公安专网上,实现与公安监控中心之间的互联。
- d) 公安监控资源(非 SIP)通过 SIP 网关连接到公安专网上,实现与公安监控中心之间的互联。
- e) 社会监控子系统未直接接入到公安监控子系统。若以后相关管理标准或法规允许,可通过安全隔离设备及 SIP 网关连接到公安专网上,实现与公安监控中心之间的互联。

参 考 文 献

- [1] GB 4943—2001 信息技术设备的安全
 - [2] GB 8898—2001 音频、视频及类似电子设备安全要求
 - [3] GB 16796—1997 安全防范报警设备安全要求和试验方法
 - [4] GB 17859—1999 计算机信息系统安全保护等级划分准则
 - [5] GB 50057—1994 建筑物防雷设计规范
 - [6] GA/T 74—2000 安全防范系统通用图形符号
 - [7] GA/T 75—1994 安全防范工程程序与要求
 - [8] GA 308—2001 安全防范系统验收规则
 - [9] GA/T 368—2001 入侵报警系统技术要求
 - [10] GA/T 388—2002 计算机信息系统安全等级保护操作系统技术要求
 - [11] GA/T 390—2002 计算机信息系统安全等级保护通用技术要求
 - [12] GA/T 391—2002B 计算机信息系统安全等级保护管理要求
 - [13] GA 607—2006 公安信息网络 IP 地址编码规范
 - [14] RFC 3261 SIP:会话初始协议
 - [15] ITU-T E. 651 IP 接入网流量工程参考连接
 - [16] ITU-T Y. 1231 IP 方面—体系结构、接入、网络容量和资源管理,IP 接入网结构
-

中华人民共和国公共安全
行业标准
城市监控报警联网系统 技术标准
第1部分:通用技术要求
GA/T 669.1—2008

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn
电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

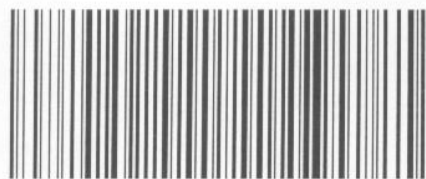
*

开本 880×1230 1/16 印张 2 字数 52 千字
2008年10月第一版 2008年10月第一次印刷

*

书号:155066·2-19163 定价 24.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533



GA/T 669.1—2008