



中华人民共和国国家标准

GB/T 20299.1—2006

建筑及居住区数字化技术应用 第1部分：系统通用要求

Digital technique application of building and residence community—
Part 1: System general requirement

2006-07-11 发布

2006-12-01 实施



中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

中 华 人 民 共 和 国
国 家 标 准
建筑及居住区数字化技术应用
第 1 部分:系统通用要求
GB/T 20299.1—2006

*

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.bzcbs.com

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 2.75 字数 81 千字
2006 年 11 月第一版 2006 年 11 月第一次印刷

*

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

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 4

4 总体结构 5

5 通信系统 6

6 信息网络平台与其他服务应用系统 7

7 信息安全 9

8 安全保密 11

9 设备监控系统 11

10 火灾自动报警及消防联动控制系统 12

11 安全防范系统 13

12 综合布线系统 14

13 基础系统集成 24

14 电源与接地 24

15 环境 24

16 机房系统 25

17 家用电子系统 28

18 IC卡应用 31

附录 A（资料性附录） 家用电子系统应用层功能实现要求 34

图 1 建筑及居住区数字化技术应用框架 5

图 2 综合布线的分层结构 15

图 3 综合布线结构 15

图 4 集中式综合布线的结构 15

图 5 功能元素的安置 16

图 6 设备和测试接口 17

图 7 带组合 BD 和 FD 的综合布线系统例子 18

图 8 平衡布线的信道、永久链路和 CP 链路 19

图 9 主干布线模型 22

图 10 主干/水平组合信道 22

图 11 无线覆盖区域的 TO 网格示例 23

图 12 家庭网络提供的典型服务 29

图 13 UI 和 PI 示意图 29

图 14 家用电子系统应用示例 30

图 15 住宅网关连接和接口示意图 30

表 1	最大信道长度	17
表 2	线缆分类	18
表 3	信道衰减	21
表 4	开机时机房温度要求	25
表 5	停机时机房温度要求	25
表 6	开机时机房湿度要求	25
表 7	停机时机房湿度要求	25
表 8	电源参数	27

前 言

GB/T 20299《建筑及居住区数字化技术应用》分为四个部分：

- 第1部分：系统通用要求
- 第2部分：检测验收
- 第3部分：物业管理
- 第4部分：控制网络通信协议应用要求

本部分为 GB/T 20299 的第1部分。

本部分由中华人民共和国建设部和信息产业部共同提出。

本部分由全国信息技术标准化技术委员会和建设部标准定额研究所归口。

本部分起草单位：建设部信息中心、中国电子技术标准化研究所、北京市质量技术监督局、北京宽网社区数字化建设有限公司、成都长城宽带网络服务有限公司、北京经世博文科技发展有限公司、日本理光公司、日本电信电话株式会社(NTT)、北京卡斯特信息系统技术有限公司、国家电子计算机质量监督检验中心、北京航天智慧科技发展有限公司、北京清华力合电子科技有限公司、中国航天二院通信中心、浙江正原电气股份有限公司、深圳市共济科技有限公司、北京东方英卡数字信息技术有限公司、武汉天喻信息产业股份有限公司、上海三零卫士信息安全有限公司、太极计算机有限公司。

本部分主要起草人：王立建、徐冬梅、王毅、李翔宇、姚世全、黄家英、王辉、杨玉柱、朱煦、程卫东、孟亚平、张建军、成金爱、杜虹、曲天光、濮容声、汪宝森、赵英然、徐全平、王坤、赵晓光、周慧琳、吴东亚、黄景楠、刘吕刚、李勇。

引 言

1. 本标准 GB/T 20299—2006 编制的目的是为了规范和指导建筑及居住区数字化建设,提高工程设计和施工的质量,维护消费者利益。
2. 本标准是面向建筑和居住区的数字化技术应用服务,规范建立包括通信系统、信息系统、监控系统的数字化技术应用平台(见图 1)。本标准的第 1 部分为系统通用要求,本部分支持物业数字化服务。当前信息技术在建筑领域业已广泛引用,居民居住区社会化服务需求强烈,面向 WTO,相关行业和地方主管部门相互加强合作,共同推进建筑信息化产业的发展 and 加强市场的统一规范与管理是必要的。
3. 信息安全是指为防止内部或外部、人为或非人为、意外事故或恶意攻击对信息基础设施、应用服务系统和信息内容的破坏而进行的安全保护。信息安全工作应贯穿于信息系统整个生命周期,在攻防对抗中不断发展,为认真贯彻《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)的要求和 2004 年 1 月全国信息安全保障工作会议精神,因此本标准将信息安全作为内容列入是非常必要的。
4. 本标准中的消防、信息安全和安全保密要求符合国家相关法规及标准规定。

建筑及居住区数字化技术应用

第1部分：系统通用要求

1 范围

GB/T 20299 的本部分规定了建筑及居住区数字化技术应用平台,该平台由通信系统、信息系统与监控系统以及支持这些系统工程的基础设施包括信息网络平台、综合布线系统、电源与接地、环境、机房系统、基础系统集成等组成。

本部分适用于建筑及居住区数字化技术应用系统平台的设计和实施,也可作为建筑及居住区选择数字化技术系统配置的依据。

2 规范性引用文件

下列文件中的条款通过 GB/T 20299 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。

注:为便于读者应用,本章中引用文件的排序为 a)、b)、c)……分别对应于 4、5、6……各章,不同章中引用同一标准时,两章中可以同时出现。

a) 总体结构

GB/T 20299.2—2006 建筑及居住区数字化技术应用 第2部分:检测验收

GB/T 20299.3—2006 建筑及居住区数字化技术应用 第3部分:物业管理

GB/T 20299.4—2006 建筑及居住区数字化技术应用 第4部分:控制网络通信协议应用要求

b) 通信系统

GB/T 15839 64~1 920 kbit/s 会议电视系统进网技术要求

GY/T 106 有线电视系统技术规范

YD/T 847 视听电信业务中 64~1 920 kbit/s 信道的帧结构

YD 5032 会议电视系统工程设计规范

YDN 065—1997 邮电部电话交换设备总技术规范书

c) 信息网络平台及其他服务应用系统

GB 2312 信息交换用汉字编码字符集 基本集

GB 5007.1 信息技术 汉字编码字符集(基本集)24点阵字型

GB 5007.2 信息技术 汉字编码字符集(辅助集)24点阵字型

GB 5199 信息技术 汉字编码字符集(基本集)16点阵字型

GB 13000.1 信息技术 通用多八位编码字符集(UCS) 第一部分:体系结构与基本多文种平面 (GB 13000.1—1993, idt ISO/IEC 10646-1:1993)

GB 15629.11 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分:无线局域网媒体访问控制和物理层规范(GB 15629.11—2003, ISO/IEC 8802-11:1999, MOD)

GB 15629.11—2003/XG1—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分:无线局域网媒体访问控制和物理层规范 第1号修改单

GB 15629.1102 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分:无线局域网媒体访问控制和物理层规范:2.4 GHz 频段较高速物理层扩展规范

- GB 16793 信息技术 通用多八位编码字符集(I区) 汉字 24 点阵字型 宋体
- GB 16794.1 信息技术 通用多八位编码字符集(I区) 汉字 48 点阵字型 第 1 部分:宋体
- GB 17698 信息技术 通用多八位编码字符集(I区) 汉字 16 点阵字型
- GB 18030 信息技术 信息交换用汉字编码字符集 基本集的扩充
- GB/T 18031 信息技术 数字键盘汉字输入通用要求
- ISO/IEC TR 8802-1 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 1 部分:局域网标准概述
- ISO/IEC 8802-2 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 2 部分:逻辑链路控制
- ISO/IEC 8802-3 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 3 部分:带碰撞检测的载波侦听多址访问(CSMA/CD)的访问方法和物理层规范
- d) 信息安全
- GB 4943 信息技术设备的安全(GB 4943—2001, idt IEC 60950:1999)
- GB 17859 计算机信息系统 安全保护等级划分准则
- GB/T 18336.1 信息技术 安全技术 信息技术安全性评估准则 第 1 部分:简介和一般模型 (GB/T 18336.1—2001, idt ISO/IEC 15408-1:1999)
- GB/T 18336.2 信息技术 安全技术 信息技术安全性评估准则 第 2 部分:安全功能要求 (GB/T 18336.2—2001, idt ISO/IEC 15408-2:1999)
- GB/T 18336.3 信息技术 安全技术 信息技术安全性评估准则 第 3 部分:安全保证要求 (GB/T 18336.3—2001, idt ISO/IEC 15408-3:1999)
- GB/T 19716 信息技术 信息安全管理实用规则(GB/T 19716—2005, ISO/IEC 17799, MOD)
- GB/T 20261 信息技术 系统安全工程能力成熟度模型(GB/T 20261—2006, ISO/IEC 21827:2002, MOD)
- e) 安全保密
- f) 设备监控系统
- GB/T 50314 智能建筑设计标准
- g) 火灾自动报警及消防联动控制系统
- GB 50045 高层民用建筑设计防火规范
- GB 50116 火灾自动报警系统设计规范
- GB/T 50314 智能建筑设计标准
- GBJ 16—1987 建筑设计防火规范
- h) 安全防范系统
- GB 16796 安全防范报警设备 安全要求和试验方法
- GB 50198 民用闭路监视电视系统工程技术规范
- i) 综合布线系统
- GB/T 18233 信息技术 用户建筑群的通用布缆(GB/T 18233—¹⁾, idt ISO/IEC 11801:2002)
- ISO/IEC 14763-1:1999 信息技术 用户建筑群布缆的实施和运行 第 1 部分:管理
- ISO/IEC TR 14763-2:2000 信息技术 用户建筑群布缆的实施和运行 第 2 部分:布铜缆的规划和安装
- ISO/IEC 14709-1:1997 信息技术 用于应用的用户建筑群布缆配置 第 1 部分:综合业务数字网(ISDN)基本访问

1) 即将发布。

ISO/IEC 14709-2:1998 信息技术 用于应用的用户建筑群布缆配置 第2部分:综合业务数字网(ISDN)基群访问

ISO/IEC 18010:2002 信息技术 用户建筑群布缆的通路和空间

j) 基础系统集成

k) 电源与接地

GB 50057 建筑物防雷设计规范(2000年修订版)

GB/T 50314—2000 智能建筑设计标准

JGJ/T 16—1992 民用建筑电气设计规范

l) 环境

GB 6566 建筑材料放射性核素限量

GB 18580 室内装饰装修材料 人造板及其制品中甲醛释放限量

GB 18581 室内装饰装修材料 溶剂型木器涂料中有害物质限量

GB 18582 室内装饰装修材料 内墙涂料中有害物质限量

GB 18583 室内装饰装修材料 胶粘剂中有害物质限量

GB 18584 室内装饰装修材料 木家具中有害物质限量

GB 18585 室内装饰装修材料 壁纸中有害物质限量

GB 18586 室内装饰装修材料 聚氯乙烯卷材地板中有害物质限量

GB 18587 室内装饰装修材料地毯、地毯衬垫及地毯胶粘剂有害物质释放限量

GB 18588 混凝土外加剂中释放氨的限量

GB/T 18883 室内空气质量标准

GB 50325 民用建筑工程室内环境污染控制规范

m) 机房系统

GB/T 2887 电子计算机场地通用规范

GB 9361 计算机场地安全要求

GB 50052 供配电系统设计规范

GB 50057 建筑物防雷设计规范(2000年修订版)

GB 50116 火灾自动报警系统设计规范

GB 50174 电子计算机机房设计规范

SJ/T 10796—2001 防静电活动地板通用规范

n) 家用电子系统

SJ/T 11310—2005 信息设备资源共享协同服务 第1部分:基础协议

SJ/T 11311—2005 信息设备资源共享协同服务 第4部分:设备验证

ISO/IEC 10192-1 信息技术 家用电子系统(HES)接口 第1部分:通用接口(UI)类型1

ISO/IEC 10192-2 信息技术 家用电子系统(HES)接口 第2部分:简单接口(SI)类型1

ISO/IEC TR 14543-1 信息技术 HES体系结构 第1部分:简介

ISO/IEC TR 14543-2 信息技术 HES体系结构 第2部分:设备模块性

ISO/IEC TR 14543-3 信息技术 HES体系结构 第3部分:通信层和启动

ISO/IEC TR 14543-4 信息技术 HES体系结构 第4部分:混合使用建筑中家庭和建筑的自动控制

ISO/IEC 15045-1 信息技术 家用电子系统(HES)网关 第1部分:用于HES的家庭网关模型

o) IC卡应用

GB/T 16649.1 识别卡 带触点的集成电路卡 第1部分:物理特性(GB/T 16649.1—2006, ISO/IEC 7816-1:1998,MOD)

GB/T 16649.2 识别卡 带触点的集成电路卡 第2部分:触电的尺寸和位置(GB/T 16649.2—2006,ISO/IEC 7816-2:1999,IDT)

GB/T 16649.3 识别卡 带触点的集成电路卡 第3部分:电信号和传输协议(GB/T 16649.3—2006,ISO/IEC 7816-3:1997,IDT)

GB/T 16649.5 识别卡 带触点的集成电路卡 第5部分:应用标识符的编号体系和注册规程(GB/T 16649.5—2002,neq ISO/IEC 7816-5:1994)

GB/T 16649.8 识别卡 带触点的集成电路卡 第8部分:与安全相关的行业间命令(GB/T 16649.8—2002,ISO/IEC 7816-8:1999,IDT)

SJ/T 11230 接口设备基本应用编程接口规范

CJ/T 166—2002 建设事业 IC 卡应用技术

ISO/IEC 7816-4 识别卡 带触点的集成电路卡 第4部分:用于交换的行业间命令

ISO/IEC 7816-9 识别卡 带触点的集成电路卡 第9部分:附加的行业间命令和安全属性

ISO/IEC 10373-6 识别卡 测试方法 第6部分:接近式卡

ISO/IEC 14443-1 识别卡 无触点的集成电路卡 接近式卡 第1部分:物理特性

ISO/IEC 14443-2 识别卡 无触点的集成电路卡 接近式卡 第2部分:射频接口

ISO/IEC 14443-3 识别卡 无触点的集成电路卡 接近式卡 第3部分:初始化和防冲突

ISO/IEC 14443-4 识别卡 无触点的集成电路卡 接近式卡 第4部分:传输协议

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

网络 network

结点和互连分支的一种安排。

3.1.2

计算机网络 computer network

为数据通信目的将数据处理结点互连起来的一种网络。

3.1.3

局域网(LAN) local area network(LAN)

一种位于有限地理区域的用户宅院内的计算机网络。

3.1.4

信息网络 information network

运载各种信息应用的计算机网络。

3.1.5

媒体访问控制(MAC) medium access control(MAC)

用来建立暂时控制传输媒体的数据站顺序的一种技术。

3.1.6

过程接口 process interface(PI)

家用电子系统中设备和网络之间的任何接口,在 OSI 参考模型中位于第七层之上。

3.1.7

通用接口 universal interface(UI)

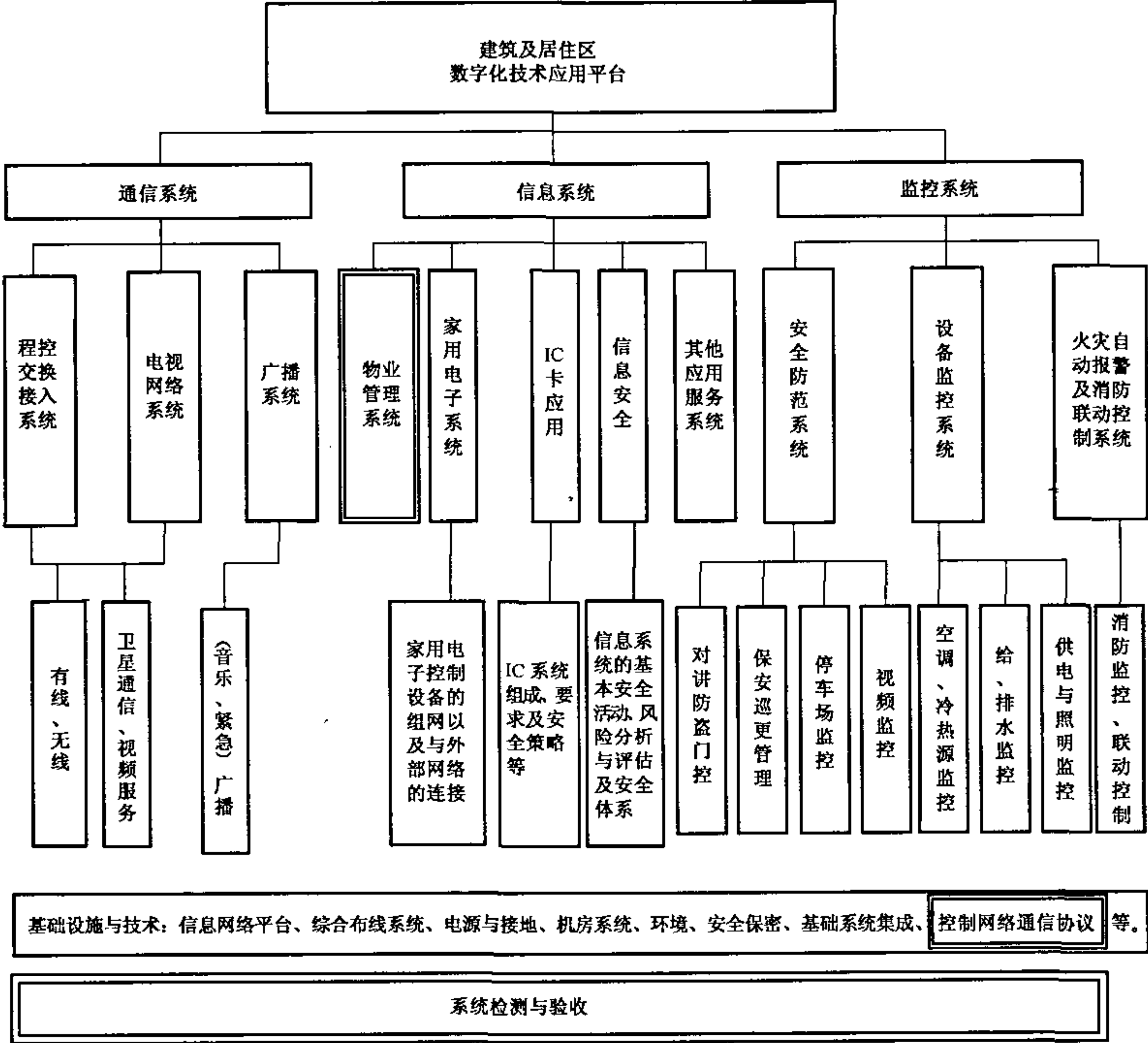
家庭网络和被连接的设备之间的标准化接口,置于网络层之上,UI 规范包括必需的机械、电气、功能和规程特性接口。

3.2 缩略语

- NAU 网络连接单元
- MAC 媒体访问控制
- MSDU MAC 服务数据单元
- IGRS 智能互联、资源共享与协同服务
- IP 网际协议

4 总体结构

建筑及居住区数字化技术应用主要由通信系统、信息系统与监控系统及基础设施组成,见图 1。



注：双方框表示不属于本部分内容。

图 1 建筑及居住区数字化技术应用框架

- a) 通信系统实现语音和视频通信,包括程控交换接入系统、电视网络系统和广播等子系统组成;
- b) 信息系统包括家用电子系统、物业管理系统、IC 卡应用、信息安全和其他应用服务系统;
- c) 监控系统包括安全防范、建筑设备监控和火灾自动报警及消防联动等三个子系统组成;
- d) 基础设施包括信息网络平台、综合布线系统、电源与接地、机房系统、环境、安全保密、基础系统集成等。

信息系统中的物业管理部分参见本标准的第3部分:GB/T 20299.3;与本部分对应的检测验收参见本标准的第2部分:GB/T 20299.2;控制网络通信协议通用要求参见本标准的第4部分:GB/T 20299.4。

5 通信系统

5.1 总则

5.1.1 本部分按程控交换系统、电视网络系统、广播系统及其接入系统四个子系统进行描述。

5.1.2 在通信系统中,应坚持采用先进、成熟、实用的技术,所采用的系统和设备应符合标准化、开放性的要求,并具有灵活性和可扩展性。

5.1.3 应选用符合用户要求且本地区和有关部门允许入网的产品,与公网互联的设备还应符合相关公网接口标准。

5.2 要求

5.2.1 程控交换系统

5.2.1.1 本系统中所使用的电信设备应具有信息产业部或国家相关部门的入网许可证。

5.2.1.2 小区或建筑物内应根据用户需求,可设置相应容量的程控交换系统。程控交换系统可以是用户小交换机,也可以是市话网的一个端局、支局或其他用户终端设备。

5.2.1.3 程控交换系统功能上应符合工程设计文件的要求,并具有高稳定性、高可靠性,便于扩充容纳新业务和新技术。

5.2.1.4 电信设备应具有铜缆、光纤等各类接口,接口性能应符合设计要求及相关国家规范和标准,具体接口规范见 YDN 065—1997 第10部分的要求及规定。

5.2.1.5 小区或建筑物内出现移动通信盲区时,应设置移动通信中继收发设备,以提高移动通信的覆盖率。

5.2.1.6 通信线路是构成通信网的重要部分,线缆的种类和技术指标应符合工程设计文件的要求。

5.2.2 电视网络系统

5.2.2.1 小区或建筑物内如设置卫星电视、视频会议及视频点播等系统,应符合 GB/T 15839、YD/T 847、YD 5032 及 GY/T 106 的要求,并遵循相关管理部门的规定。

5.2.2.2 有线电视系统应采用双向传输方式,以适应交互式业务发展的需求。

5.2.2.3 视频点播系统应实现数字信息点播服务,例如:股票信息点播、教育信息点播、视频点播、有线电视自动收费管理等。

5.2.2.4 视频会议系统应可通过具有视频压缩技术的设备向使用者显示图像并进行同步通话。

5.2.2.5 根据承载视频会议的网络的不同,设备和网络间接口应满足相应通信网络接口的技术规范。

5.2.3 广播系统

5.2.3.1 广播系统的功能应符合工程设计文件要求,能够向小区公共场所提供音乐节目和公共传呼信息,并和紧急广播系统结合,在必要时进行紧急广播。

5.2.3.2 广播系统应提供外部接口,以利于与其他相关系统的连接。

5.2.3.3 广播系统要实施分区控制,分区的划分应与消防分区一致,并能够按一定的优先级控制播出。

5.2.3.4 对于广播系统与消防广播共用设备,应满足 10.2 的要求。

5.2.4 接入系统

5.2.4.1 小区或建筑物内应设立宽带网络接入系统,网络类型可采用多种不同的方式或其组合。

5.2.4.2 接入系统应提供准确的计费服务,并支持用户开户、销户、暂停、访问记录查询、流量控制等服务。

5.2.4.3 无线接入应能够提供高质量的话音、数据以及模拟和数字视频业务。

6 信息网络平台与其他服务应用系统

6.1 总则

6.1.1 信息网络平台包括局域网(含无线局域网)及其管理系统;应用系统包括内部信息服务、互联网信息服务等。

6.1.2 信息网络平台是数据传输、信息资源共享的基础。信息网络平台应具有同广域网连接的能力,根据需要与 Internet 连接。

6.1.3 信息系统总体安全策略应符合国家有关信息安全法律、法规、制度等的规定和要求。

6.2 要求

6.2.1 局域网

局域网内主干网应具有高可靠性、灵活性、可扩充性和可管理性,其设计要有冗余度,并能支持多种网络协议,根据需求随时扩充配置新的网络。局域网的类型选择和具体配置要根据社区用户数、实际应用系统特性、流量变化特征、用户访问频度和网络覆盖范围等因素来进行。

局域网相关技术参见 ISO/IEC TR 8802-1、ISO/IEC 8802-2、ISO/IEC 8802-3、GB 15629.11 和 GB 15629.1102。

局域网应满足下列要求:

- a) 为提高系统的灵活性和可扩充性,核心交换机应具备灵活的端口扩充能力、模块扩充能力,局域网的设计应该层次化。例如:大型社区局域网可采用三层结构:核心层、汇聚层和接入层;
- b) 局域网和 Internet 之间宜保持采用防火墙进行逻辑隔离;Internet 出口可考虑两路出口;
- c) 局域网宜充分考虑利用模块冗余、设备冗余和链路冗余等技术手段,以提高系统的可靠性;
- d) 局域网运行时,应避免冗余链路设计系统中的数据帧在系统中循环传送;同时也宜控制数据帧的广播域;
- e) 局域网应具有用户接入认证和计费功能,尽可能避免用户冒用,并保证系统计费记录的完整性;
- f) 无线局域网应根据社区用户的接入需求选择接入技术、确定系统容量,合理布放无线接入点,并注意墙壁、窗户和电梯等所引起的信号吸收现象,尽可能减少无线接入的盲点;
- g) 局域网内任意两点之间的传输延迟宜要求不超过 10 ms,系统实际带宽不应低于系统设计要求,并实现了系统设计的各项功能;
- h) 局域网应具有支持多种业务应用服务的能力,例如:Web 访问服务、ftp 服务、电子邮件服务和视频服务等等;
- i) IP 地址的规划与管理应该坚持四个原则:统一性原则(地址分配应统一规划、统一协调、统一管理)、层次性原则、连续性原则和唯一性原则;
- j) 为了加强系统的可维护性和可管理性,局域网至少应该保持系统设计文档、工程实施文档、工程验收文档和工程监理文档等;
- k) 系统的安全设计与实施应参照本部分第 7 章的规定。

6.2.2 局域网管理

局域网管理系统可支持的功能包括:配置管理、故障管理、性能管理、安全管理和帐户管理等。实际设计与应用可根据实际的环境和设备需求,提供下面的全部或某些管理功能:

- a) 配置管理应提供通信资源的标识、初始化、重新设置和关机、操作参数以及资源之间相互关系的建立和发现;

- b) 故障管理应提供故障的预防、检测、诊断和纠正；
- c) 性能管理应提供对通信资源行为和通信活动有效性的评价；
- d) 安全管理应提供资源的保护；
- e) 帐户管理应提供成本的标识和分发以及费用设置。

6.2.3 其他应用服务系统

6.2.3.1 应用软件产品文档

- a) 具有产品标识和运行环境说明；
- b) 具有安装和维护的有关说明；
- c) 对程序中用户可调用的所有功能有完整的描述；
- d) 提供产品正常运行的边界值范围；
- e) 用户文档的所有信息应正确，不能有歧义和错误的表达；
- f) 用户文档自身内容间以及与产品实际运行结果间不应相互矛盾，术语的含义应处处一致；
- g) 用户文档对用户是易于理解的；
- h) 用户文档应便于浏览，有目录和索引。

6.2.3.2 功能性

应用软件系统在运行、功能、正确性和一致性上应分别满足下列要求：

- a) 应用程序安装之后，应能正常运行。
- b) 用户文档中提到的所有功能应是可执行的。程序应按照用户文档中的给定形式、在规定的边界值范围内使用相应的设施、性质和数据执行其功能。
- c) 程序和数据应与用户文档中的全部描述相对应。
- d) 程序和数据本身不能自相矛盾，并且同用户文档不能相互矛盾。每个术语应处处具有相同的含义。提供给用户的交互界面及交互行为应有一致的结构。

6.2.3.3 可靠性

系统不应陷入用户无法控制的状态，既不应崩溃也不应丢失数据，即使用户未按用户文档中的描述在规定的环境中使用合法的数据进行合法的操作。只有那些不能用任何程序捕获的硬中断和操作系统中断除外。

6.2.3.4 易用性

- a) 易理解性：程序的问题、消息和结果应是易理解的。
- b) 易浏览性：产品应以易观察、易读的形式向用户提供信息；输入输出应设计清晰、易于浏览。
- c) 可操作性：具有严重后果的功能执行应是可逆的，或应给出该后果的明显警告并在执行该命令前要求确认。

6.2.3.5 效率

应遵循用户文档中的效率说明。

6.2.3.6 可维护性

应遵循用户文档中的可维护性说明。

6.2.3.7 可移植性

应遵循用户文档中的可移植性说明。

6.2.3.8 中文特性

- a) 软件产品涉及的中文编码应遵从中文编码标准 GB 2312、GB 13000.1 以及 GB 18030；
- b) 软件产品涉及的中文字型应遵从中文字型标准 GB 5007.1、GB 5007.2、GB 5199、GB 16793、GB 16794.1 以及 GB 17698；
- c) 软件产品涉及的中文输入法应遵从中文输入法标准 GB/T 18031。

7 信息安全

7.1 总则

7.1.1 信息系统安全应符合国家有关安全法律、法规、制度等的规定和要求,对涉及人身安全的信息设备,应有主管部门颁发的 3C 认证标志。设备安全应符合 GB 4943,信息系统安全应符合 GB 17859、GB/T 18336.1、GB/T 18336.2、GB/T 18336.3、GB/T 19716 及 GB 20261 等标准。

7.1.2 应采取一定的信息安全措施,确保运营服务信息系统的安全,确保运营服务系统不会对用户造成信息安全损害。

7.1.3 应明确系统本身可能受到的安全威胁以及可能对用户造成的安全威胁,采取措施应对和消除安全威胁。

7.2 要求

7.2.1 信息系统基本安全活动

信息系统基本安全活动包括:

- a) 根据信息系统的特点和服务对象的需求,基于风险分析的结果,确定信息系统的安全等级;
- b) 安全策略的制定、发布、教育、评价、修正等活动;
- c) 建立信息安全相关的机构,设置相应的岗位,确定相关的责任,并建立相配套的管理、考核和奖惩体系;
- d) 保障信息安全相关工作的人力资源投入,建立相关的人员选拔、考核、培训体系,并规划和实施针对一般运营服务人员和普通用户的安全教育、宣传活动;
- e) 确定信息系统中的关键信息资产,并进行资产分类管理;
- f) 应根据信息系统的安全等级,建立相应的物理和环境安全保护体系;
- g) 应根据信息系统的安全等级,建立相应的信息安全技术保障体系,技术保障体系要求参见 7.2.3;
- h) 建立和维护系统的运行安全体系,主要包括针对信息系统以及普通用户的应急响应体系、安全基础设施服务体系、定期的安全风险评估体系等;
- i) 应根据信息系统的安全等级,对相应的信息系统承包商、信息软硬件产品进行安全资质审查、实施过程的质量监督和控制;
- j) 应根据信息系统的安全等级,对系统运行过程中可能发生的升级、完善等活动做好安全规划,对系统的拆除应提前做好规划和处理。

7.2.2 风险分析与评估

- a) 应对信息系统进行风险分析,并将风险分析的结果作为确定相应系统安全等级的主要依据。
- b) 应建立定期和不定期风险评估的机制。
- c) 信息系统的安全风险分析与评估,宜由有相应资质的机构完成。
- d) 风险分析与评估宜采用适用的方法,对每一个识别出的信息资产,按照资产的“保密性”、“完整性”、“可用性”和“可控性”四个最基本的安全要求,分析可能受到的威胁和后果,提出相应的安全需求建议。

7.2.3 应制定明确的安全策略

安全策略应涉及:

- a) 物理安全策略:确定在物理访问、保护方面的安全规定。
- b) 访问控制策略:规定内部网与外部网之间,以及内部网段之间的访问规定和策略要求。
- c) 安全检测策略:规定对系统安全实施定期检查的周期、方法等。
- d) 审计与监控策略。
- e) 网络防病毒策略。

- f) 备份与灾难恢复策略。

7.2.4 安全体系方面

7.2.4.1 信息安全措施

信息系统应从以下几个方面采取安全措施：

- a) 建立明确的信息安全体系,包括明确的安全策略、网络系统配置安全服务和安全机制运行说明,指明在哪些部位必须配置哪些安全服务和安全机制,以及规定如何进行安全管理;
- b) 采取措施保护局域网;
- c) 采取措施保护基础通信设施;
- d) 采取措施保护边界;
- e) 配置或依托公共信息安全基础设施;
- f) 具体安全措施的采取应根据系统的实际情况确定。

7.2.4.2 保护本地计算环境

本地计算环境可采取的安全措施有：

- a) 保护机房环境、主机和外部设备的物理安全;
- b) 计算环境涉及的局域网、主机设备、操作系统、应用支撑系统(包括 WEB 系统、数据库系统等)和应用系统,都应该采取相应的措施保护在计算环境内存储、传输和处理的数据的保密性;
- c) 计算机环境涉及的局域网、主机设备、操作系统、应用支撑系统和应用系统,都应该采取相应的措施保护本地计算环境内存储、传输和处理的数据的完整性,以及系统的完整性。系统完整性措施包括主机漏洞扫描、防病毒和补丁管理等;
- d) 确保本地计算环境内的网络平台、操作系统、应用支撑系统以及应用系统正常地运行,并使授权用户得到所需的系统和应用服务;
- e) 具有足够的防止内外人员进行违规操作和攻击的能力。

7.2.4.3 保护网络基础设施

可采取的保护网络基础设施的措施有：

- a) 加强机房和通信缆线的物理环境保护;
- b) 保护骨干通信网络和网络基础服务系统的可用性,保证基础设施所支持的业务应用的可用性;
- c) 保护网络基础设施控制信息,保护网络基础服务系统的保密性和完整性;
- d) 根据用户需求提供物理隔离或逻辑隔离的网络体系。

7.2.4.4 保护边界

根据安全需求,可采取的边界保护措施有：

- a) 建立网络访问控制体系,如防火墙系统,实现进出网络边界的访问控制;
- b) 根据安全需求,在网络边界之间建立安全的通信连接,以保护通过边界传输的数据的保密性;
- c) 保证所有的边界节点都是合法的并在有效的安全管理控制之下;
- d) 要考虑边界的冗余配置、容错和负载均衡机制,以及加强边界设备自身安全保护,保证通过边界的通信的连续性;
- e) 建立系统远程访问安全系统,以保护系统边界远程访问的安全;
- f) 建立基于网络的入侵检测系统以防止入侵者的攻击;
- g) 建立基于网络的防病毒系统,以防止病毒入侵;
- h) 建立漏洞扫描系统以改进系统的配置和功能设置。

7.2.4.5 支撑性安全基础设施

信息系统安全保护,可采用的支撑性安全基础设施有：

- a) 公共密钥基础设施(PKI);

- b) 密钥管理系统;
- c) 安全管理系统;
- d) 应急响应体系。

8 安全保密

8.1 总则

本章规定涉及国家秘密的党政机关、企事业单位建筑数字化工程的安全保密要求,适用于涉及国家秘密的党政机关、企事业单位建筑住宅数字化工程。

8.2 要求

涉及国家秘密的党政机关、企事业单位的建筑中涉密计算机信息系统的建设、涉密网和非涉密网建设、专用电话(红机)布线、通信线、电源线、地线的布线以及涉密信息系统安全保密测评均应按国家有关法律、法规及有关规定执行。

9 设备监控系统

9.1 总则

9.1.1 建筑设备监控系统由监控网络(监控网络协议见本标准第4部分:GB/T 20299.4—2006)和所支撑的应用系统组成,按功能可分为空调与通风监控、变配电监控、照明监控、给排水监控、热源和热交换监控、冷源监控和电梯、自动扶梯监控等子系统,各子系统符合GB/T 50314。

9.1.2 监控系统用于对建筑及居住区中的各种机电设备进行监测、控制及自动化管理,达到安全、可靠、节省资源、节省人力和综合管理的目的。

9.1.3 监控系统与有通信接口的设备以通信方式相连时,应保证通信数据的畅通。

9.2 要求

9.2.1 空调与通风监控系统

9.2.1.1 对空调系统进行温度、湿度(温度、湿度要求见15.2.2)自动控制,应实现按预定时间表自动启停和节能优化启停控制,应实现空调机组设备的联锁和保护控制。

9.2.1.2 实现对空调设备运行状态、故障的监测、记录与报警。

9.2.1.3 对变风量系统实现节能运行方式。

9.2.1.4 对通风用送、排风机的运行状态进行监测和控制,并可按空气环境参数要求自动控制启停。

9.2.2 变配电监控系统

9.2.2.1 实现对变配电系统进行电压、电流、有功功率、功率因数、用电量等参数的测量与记录。

9.2.2.2 对高、低压开关柜、直流电源柜、变压器、自备发电系统的工作状态和故障进行监视。

9.2.3 照明监控系统

按照照度或预设时间表对公共照明设备包括开关、调光、场景等进行控制。

9.2.4 给排水监控系统

9.2.4.1 对给排水系统的运行状态与故障状态实行监控、记录,自动调整投运水泵台数。

9.2.4.2 对中水系统的运行状态与故障状态进行监控。

9.2.5 热源和热交换监控系统

9.2.5.1 实现系统的负荷调节、预定时间表自动启停和节能优化控制。

9.2.5.2 实现对热源和热交换系统设备的联动控制。

9.2.5.3 实现对供回水压差或供回水温度的自动控制。

9.2.5.4 实现对热源和热交换设备运行状态、故障等进行监视、记录与报警。

9.2.6 冷源监控系统

9.2.6.1 实现系统的负荷调节、预定时间表自动启停和节能优化控制。

9.2.6.2 实现系统设备的联动控制。

9.2.6.3 实现对系统运行参数、状态、故障等的监视、记录与报警。

9.2.6.4 实现对供回水压差或供回水温度的自动控制。

9.2.7 电梯和自动扶梯监控系统

对电梯和自动扶梯系统运行状态和故障进行监控。

10 火灾自动报警及消防联动控制系统

10.1 总则

10.1.1 火灾自动报警及消防联动系统由火灾自动报警及消防联动系统及其所支撑的应用组成。

10.1.2 火灾自动报警系统是电气系统的一部分,系统设计首先应符合建筑电气设计的一般要求;同时,火灾自动报警系统又是一种消防安全设备,必须符合安全方面的有关规定。相关规定见 GB 50116。

10.1.3 消防控制室是火灾自动报警系统的控制和信息中心,也是火灾时灭火作战的指挥与信息中心。消防控制的设置范围、位置、建筑耐火性等相关规定见标准 GB 50045 和 GBJ 16—1987,消防控制室的设备组成、安全要求、设备功能、设备布置、联动控制要求见标准 GB/T 50314。

10.2 要求

10.2.1 火灾自动报警系统

- a) 设有手动和自动两种触发装置。自动触发装置,即火灾探测器,是系统中最基本的触发装置,它自动探测火灾,产生和发出火灾报警信号并将火灾报警信号传输给火灾报警控制器。手动触发装置,即手动火灾报警按钮,它是系统中必不可少的组成部分。
- b) 火灾报警控制器容量和每一总线回路所在连接的火灾探测器即控制块(或信号模块)的地址编码总数均宜留一定余量。
- c) 火灾自动报警系统的设备,应采用经国家有关产品质量监督检测中心检验合格的产品。

10.2.2 消防联动控制系统

- a) 消防控制设备应由下列部分或全部组成:
 - 1) 火灾报警装置;
 - 2) 火灾报警控制器;
 - 3) 自动灭火系统的控制装置;
 - 4) 室内消火栓系统的控制装置;
 - 5) 防烟、排烟系统及空调通风系统的控制装置;
 - 6) 水喷淋控制装置;
 - 7) 防火门、防火卷帘的控制装置;
 - 8) 电梯返回控制装置;
 - 9) 火灾应急广播的控制装置;
 - 10) 火灾应急照明与疏散指示标志的控制装置。
- b) 消防控制设备的控制方式:
 - 1) 消防控制设备应根据建筑的分类、工程规模、管理体制及功能要求综合确定其控制方式,并接收、显示其反馈信号;
 - 2) 大型建筑群采用分散与集中相结合控制。
- c) 消防控制设备的控制电源及信号回路电压应采用直流 24 V。
- d) 消防控制室要求见 GB 50116。

11 安全防范系统

11.1 总则

11.1.1 安全防范系统应满足 GB 16796 的要求,其主要由视频监控系统、入侵报警系统、巡更系统、出入口控制(门禁)系统、汽车停车场管理系统及访客对讲或可视对讲系统等组成。

11.1.2 安全防范系统设计应根据“以防为主、打防并举”和安全防范工作实行“人防、技防、物防相结合”的原则,既要考虑到技防设施的先进性、实用性和系统的可扩展性,以便不断采用新技术、新设备,还要考虑各种高科技的物防设施及管理 and 操作这些设备的工作条件,创造良好的人机界面和方便、舒适、高效的人文环境。

11.1.3 综合运用信息技术、计算机网络技术、安全防范技术,依靠计算机平台,将安防各子系统集成、联网,使安全防范具有综合管理能力,构成先进、可靠、经济、配套的安全防范系统。

11.2 要求

11.2.1 视频监控系统

- a) 闭路电视监控系统应符合 GB 50198;
- b) 主要功能包括:视频监控系统开通稳定运行、矩阵监控主机的自动/手动切换、遥控、编程、巡检、计算机对摄像机的控制、记录、采集、编程等功能或数字硬盘的记录功能;
- c) 视频监控系统与安全防范各子系统的联动功能。

11.2.2 入侵报警系统

- a) 系统控制功能及通讯功能:包括报警管理和报警信息处理,报警探测器盲区;
- b) 系统联动功能:包括入侵报警系统、视频监控系统、出入口控制(门禁)系统等相关安全防范系统的联动功能;
- c) 控制主机的性能以及报警联网功能;
- d) 控制中心的电子地图上应显示所有报警点的位置。

11.2.3 巡更系统

电子巡更系统目前有离线和在线两种,在线联网式巡更系统一般应具有以下功能:

- a) 实现巡更路线的设定和修改;
- b) 实现巡更时间的设定和修改;
- c) 在重要部门及巡更路线上安装巡更站点;
- d) 应具有对巡更时间、地点、人员和顺序等数据的显示、归档、查询和打印等功能;
- e) 控制中心的电子地图上应显示出所有巡更站点所在位置,当保安人员在规定时间内没有到达指定地点巡逻时,控制中心即发出声、光提示信号;
- f) 对在线联网巡更系统,还要检测与其他系统联动功能;离线式巡更系统具有信息钮和巡更棒的防水性、抗干扰性。

11.2.4 出入口控制(门禁)系统

- a) 系统主机在线控制和离线控制情况下,一般应具有下列功能:出入口控制器工作的准确性、实时性和存储信息的功能;在线控制时,系统主机和出入口控制器之间的信息传输及数据加密功能;系统对非法强行入侵及时报警的功能;
- b) 应保证与本系统相关的综合管理、防盗及消防系统报警时的联动功能的正常运行。

11.2.5 汽车停车场管理系统

汽车停车场管理系统包括入口管理系统、出口管理系统、计费系统和管理中心以及停车场的出入口的安全性等功能。

11.2.6 访客对讲或可视对讲系统

- a) 访客对讲系统应具有联动功能;

- b) 可实现住户与访客及管理中心之间的语音通话(或通话同时可视访客图像)的功能,通话语音清楚,图像清晰;
- c) 通过室内分机可以开启防盗门电控锁;
- d) 门口主机可以利用密码、钥匙或感应卡开启防盗门电控锁;
- e) 停电时应由备用电源供电。

11.2.7 室内紧急呼救按钮

室内每户安装紧急呼救按钮,与物业管理中心连网使用。

11.2.8 安全防范中心控制室

- a) 中心控制室应配置计算机,控制主机,该中心应能够监视和记录安全防范的各种信息,能够完成防盗报警信息的自动搜索、自动记录和打印功能,对监控目标进行实时电视监控及实施图像的切换、镜头光圈的控制、焦距的放大与缩小等功能,并能完成图像的录像。
- b) 中心控制室的供电、接地、防雷见 14 章,机房要求见第 16 章。

12 综合布线系统

12.1 总则

12.1.1 综合布线系统由园区主干布线子系统、楼宇主干布线子系统和水平布线子系统组成,包括平衡布线和光纤布线。综合布线支持话音、数据、文本、图像和视频等服务。

12.1.2 综合布线应符合 GB/T 18233 的规定,同时可参照 ISO/IEC 14763-1:1999、ISO/IEC TR 14763-2:2000、ISO/IEC 14709-1:1997、ISO/IEC 14709-2:1998 和 ISO/IEC 18010:2002。

12.2 要求

12.2.1 综合布线系统的结构

12.2.1.1 功能元素

综合布线的功能元素如下:

- a) 园区配线架(CD);
- b) 园区主干线缆;
- c) 楼宇配线架(BD);
- d) 楼宇主干线缆;
- e) 楼层配线架(FD);
- f) 水平线缆;
- g) 汇集点(CP);
- h) 汇集点线缆(CP 线缆);
- i) 多用户电信插座(MUTO);
- j) 电信插座(TO)。

综合布线系统由上述多个功能元素组成,每个功能元素都有其自身的功能。要形成一个综合布线系统,不需要包括所有的功能元素,但最基本的元素是必不可少的。最基本的功能元素是楼层配线架(FD)、电信插座(TO)和连接 FD 和 TO 的线缆。使用这三种功能元素,便可实现最简单的水平布线系统。

12.2.1.2 系统结构

综合布线系统具有分层式星形结构,如图 2 所示。

综合布线包括 3 个布线子系统:园区主干、楼宇主干和水平布线。多个布线子系统连接在一起可建立结构如图 3 所示的最大配置的综合布线系统。配线架提供一种配置布线的手段以支持不同的拓扑结构,如总线形、星形及环形。

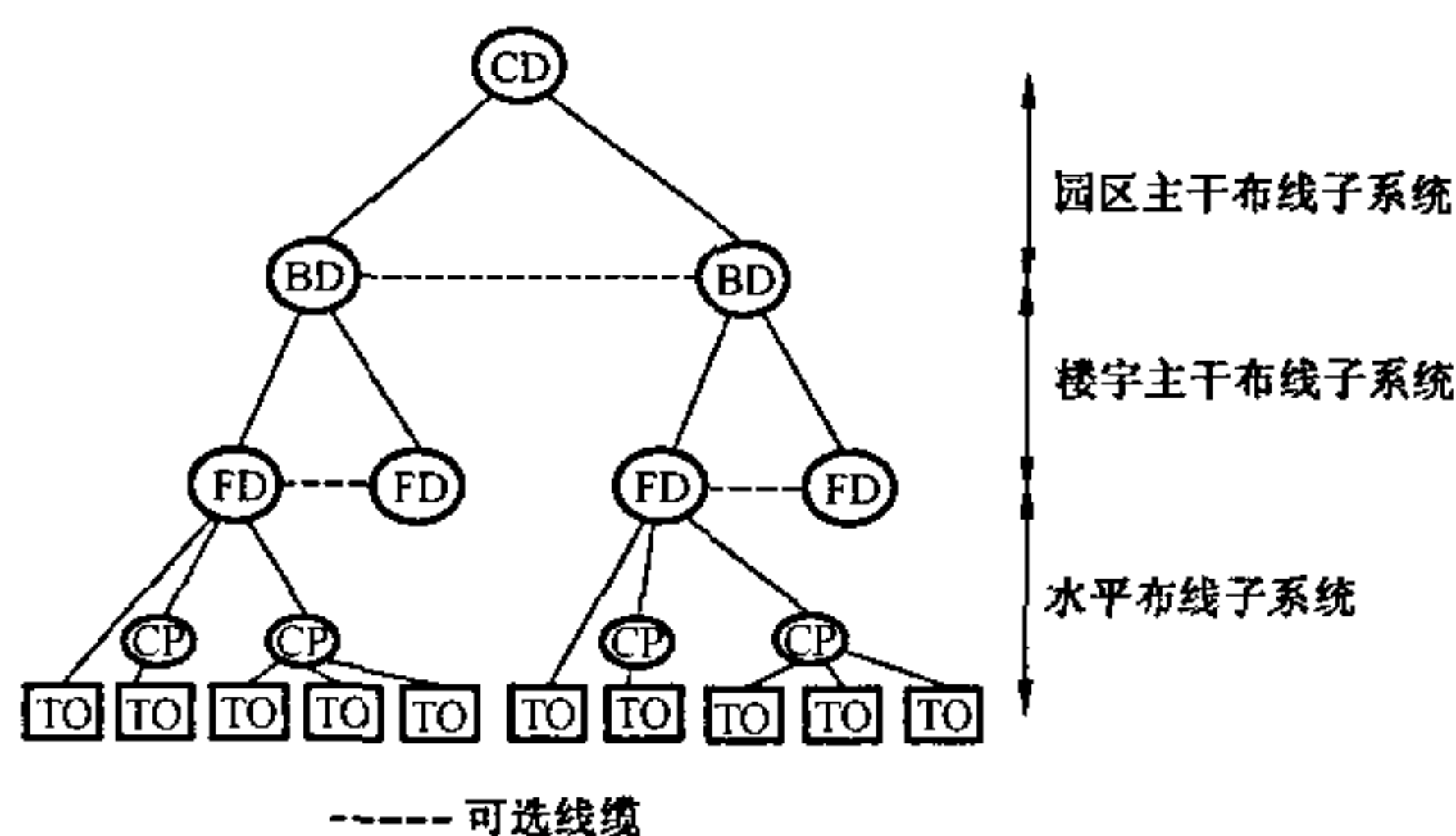


图 2 综合布线的分层结构

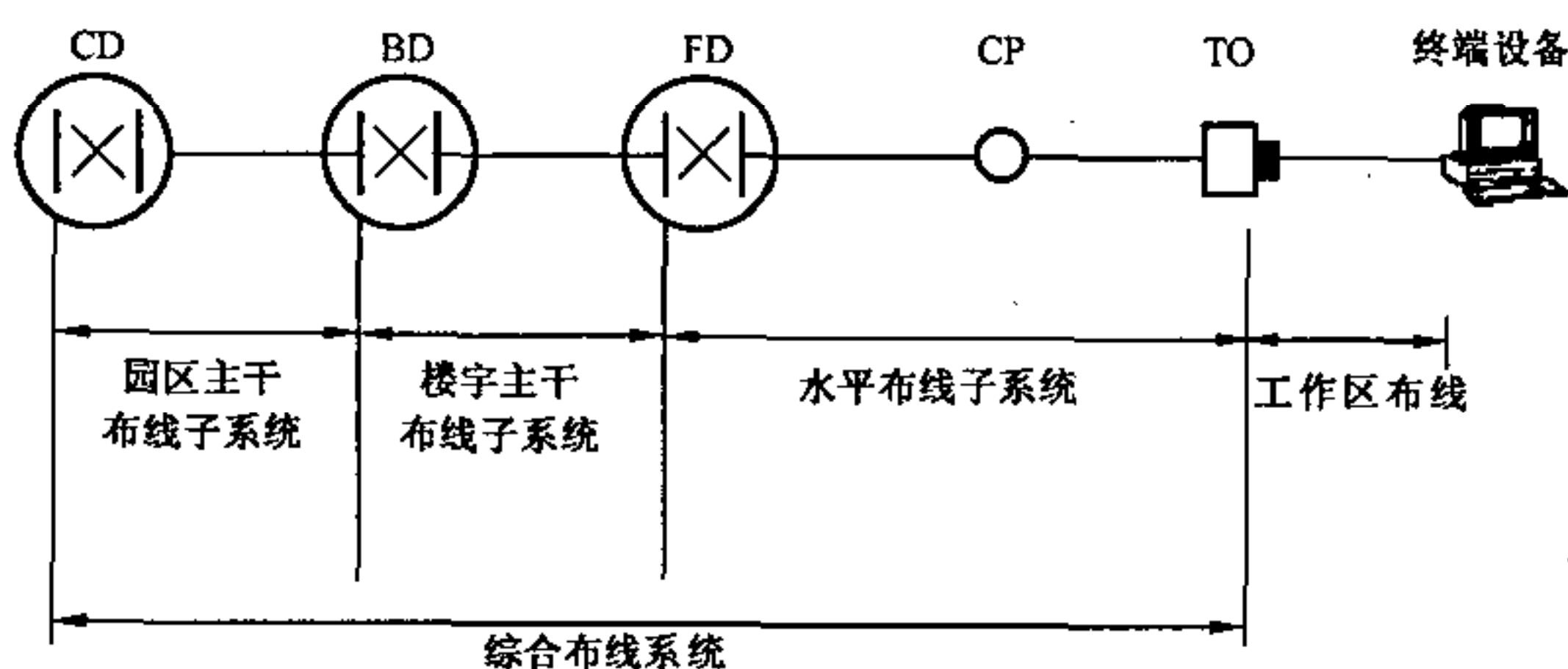


图 3 综合布线结构

布线子系统之间的连接可以有源的(特定应用设备),或无源的。与特定应用设备的连接可采用互连或交连方法。布线子系统之间的无源连接通常通过快接跳线或压接跳线用交(叉)连(接)实现。

集中式布线是建立主干/水平组合式信道的布线技术。信道通过在配线架中的无源连接实现。这种无源连接可以是交叉连接,也可以是互连连接。对于集中式光纤布线,可以在配线架中使用接合建立连接,但这种方法无疑会丧失重新配置布线的能力。集中式布线的结构如图 4 所示。

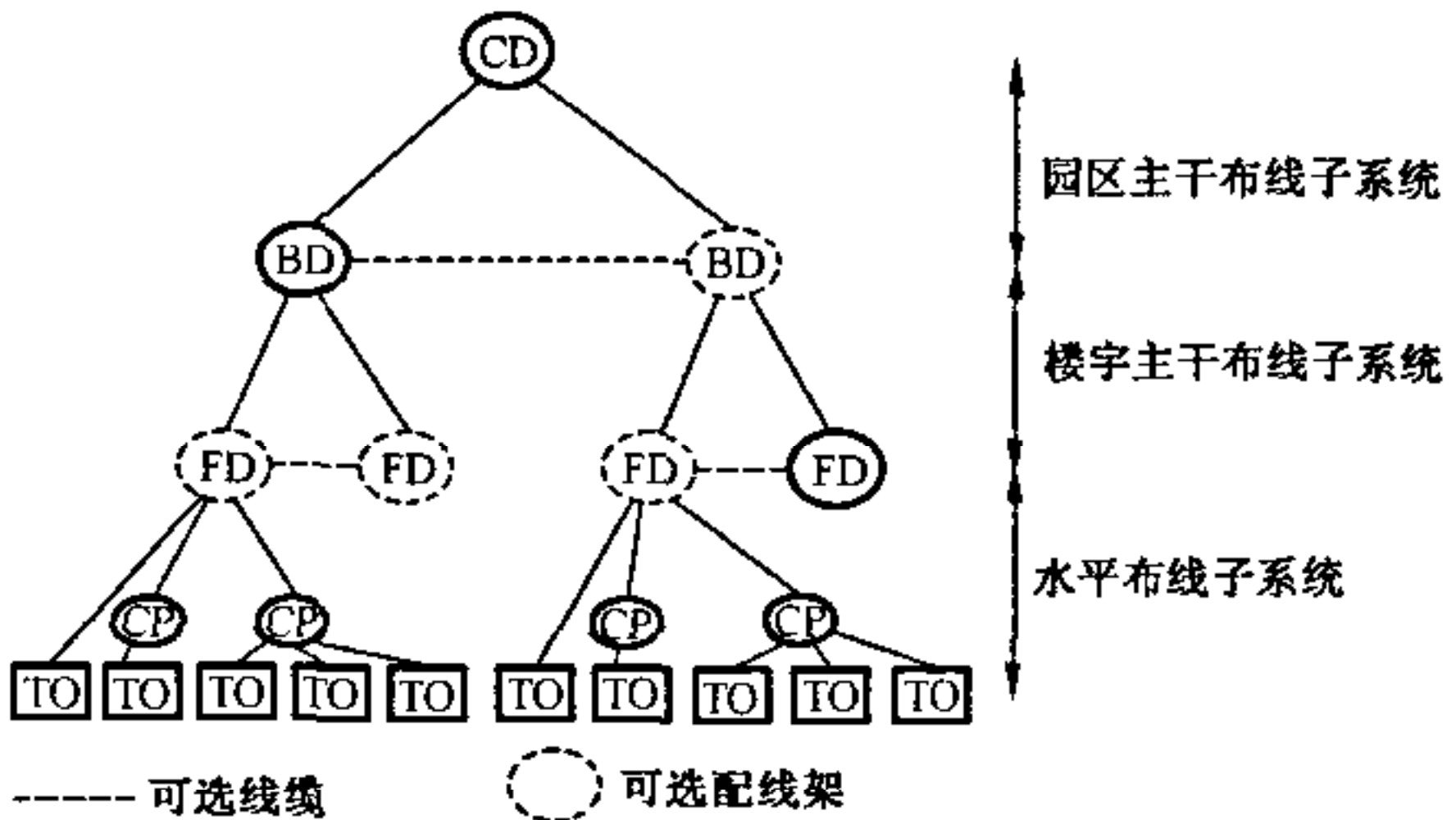


图 4 集中式综合布线的结构

12.2.1.2.1 园区主干布线子系统

园区主干布线子系统从园区配线架延伸到园区内各楼宇的楼宇配线架。当存在多个楼宇时,该子系统包括:

- a) 园区主干线缆;
- b) 楼宇入口设施内的布线部件;
- c) 园区配线架中的压接跳线和快接跳线;
- d) 终接园区主干线缆(园区或楼宇配线架处均有此终接)的连接硬件。

设备跳线用来将传输设备连接到布线子系统,但本标准不将其当作布线子系统的一部分,因为这些

跳线是专门针对应用的。园区主干布线可提供楼宇配线架之间直接连接。当这样使用时,这一布线应是基本分层结构布线的附加部分,见图 2。

12.2.1.2.2 楼宇主干布线子系统

楼宇主干布线子系统从楼宇配线架延伸到楼层配线架。当它存在时,子系统包括:

- a) 楼宇主干线缆;
- b) 楼宇配线架中的压接跳线和快接跳线;
- c) 终接楼宇主干线缆(楼宇配线架或楼层配线架均有此终接)的连接硬件。

虽然设备跳线用来将传输设备连接到布线子系统,但本标准不将其当作布线子系统的部分,因为这些跳线是专门针对应用的。楼宇主干布线可提供楼层配线架之间直接连接。当这样使用时,这一布线应该是基本分层结构布线的附加部分,见图 2。

12.2.1.2.3 水平布线子系统

水平布线子系统从楼层配线架延伸到电信插座。该子系统包括:

- a) 水平线缆;
- b) 楼层配线架中的压接跳线或快接跳线;
- c) 电信插座处水平线缆的机械终接;
- d) 楼层配线架处水平线缆的机械终接,包含例如互连或交叉连接在内的连接硬件;
- e) 汇集点(可选);
- f) 电信插座。

尽管工作区和设备跳线分别用来将终端和传输设备连接到布线子系统,但本标准不将其当作布线子系统的一部分,因为这些跳线是专门针对应用的。水平线缆应该连续地从楼层配线架延伸到电信插座,除非安装了汇集点。

12.2.1.3 功能元素的安置

图 5 示出一个楼内如何安置功能元素的举例。配线架的安置要求可参考 ISO/IEC TR 14763-2:2000。

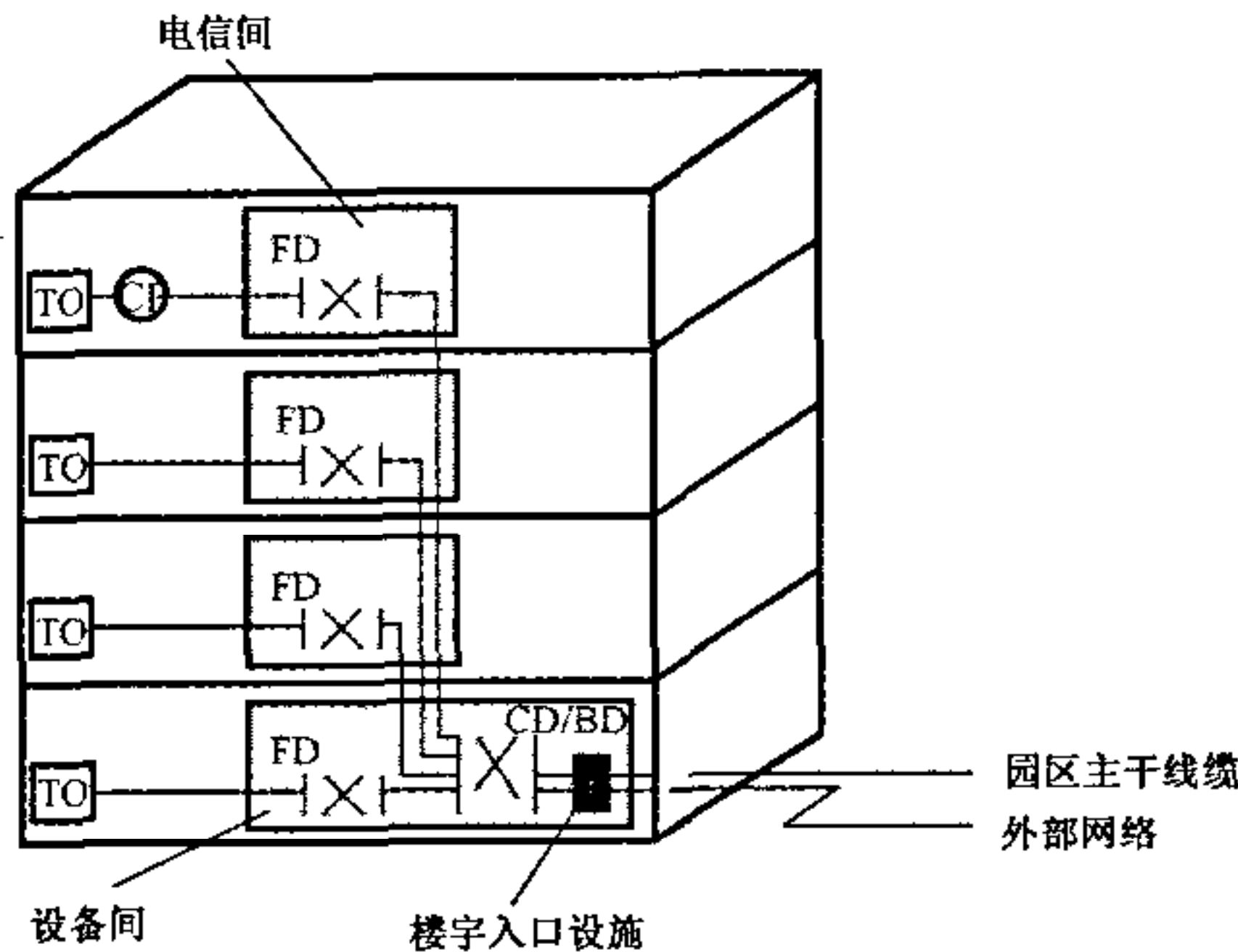


图 5 功能元素的安置

线缆使用线槽或线管敷设。线缆在线槽或线管的敷设管理要求可参考 ISO/IEC 18010:2002。

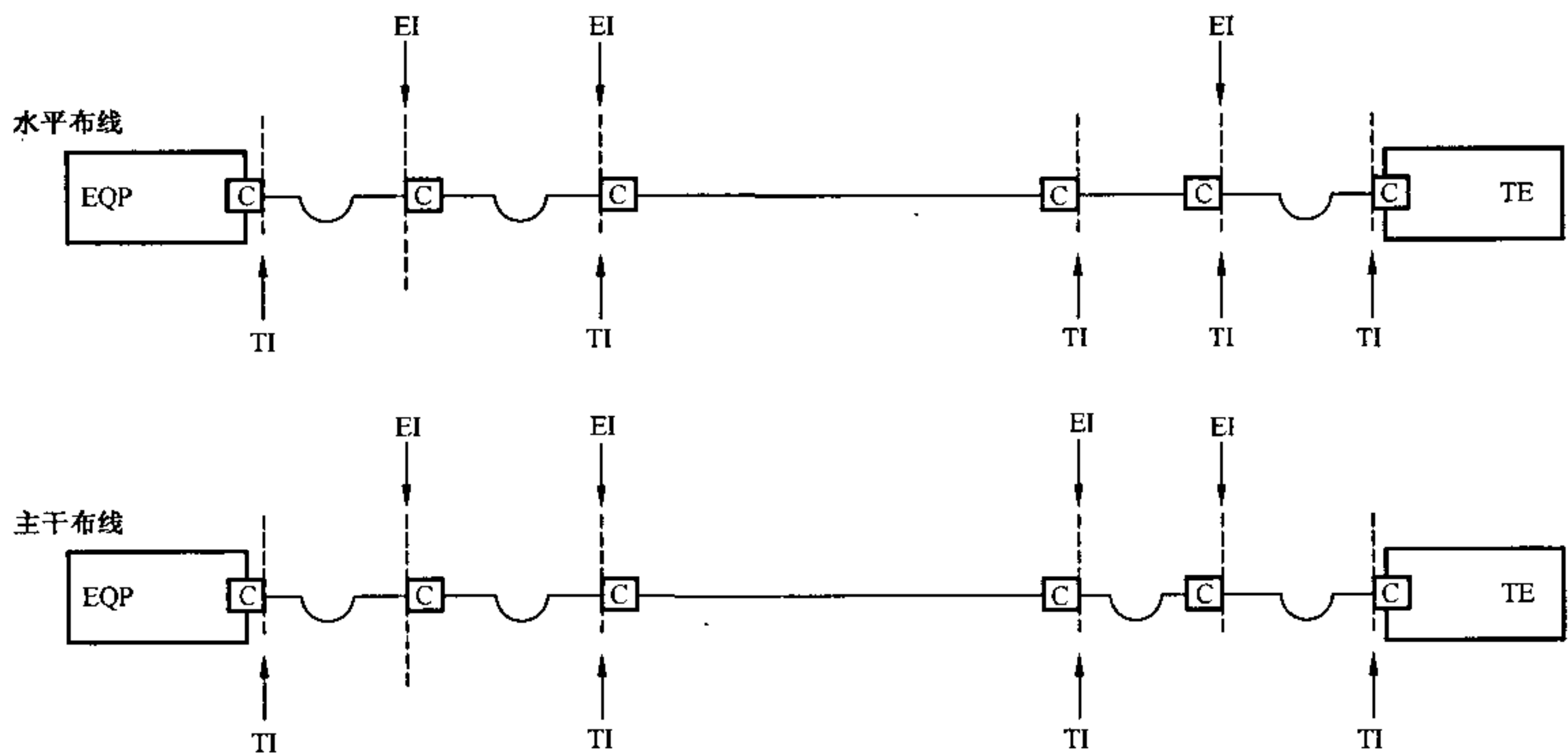
配线架放置在设备间或电信间。电信插座位于工作区。

12.2.1.4 接口

12.2.1.4.1 设备接口和测试接口

连接综合布线的设备接口位于每个子系统的末端,任何配线架可有在任意端口连接到外部服务的设备接口,汇集点不提供到综合布线系统的设备接口,图 6 示出了与水平和主干布线子系统的可能设备接口。

与综合布线的测试接口位于每个子系统的末端及汇集点(存在的话)。图 6 示出了与水平布线子系统的可能测试接口。



EI—设备接口;EQP—传输设备;TI—测试接口;TE—终端设备;□—连接

图 6 设备和测试接口

12.2.1.4.2 信道和永久链路

信道是 LAN 交换机/集线器(图 6 中的 EQP)等设备和终端设备之间的传输通路。典型的信道将由水平子系统及其工作区和设备跳线构成。对于更长的可达距离,信道将由两个或更多个子系统(包括工作区和设备跳线)构成。信道的性能不包括专门针对应用的设备的连接。

永久链路是包括已安装线缆末端处的连接硬件的该安装布线子系统传输通路。在水平布线子系统中,永久链路由电信插座、水平线缆、可选 CP 和楼层配线架处的水平线缆终端接点组成。永久链路包括已安装布线末端处的连接。

12.2.1.4.3 外部网络接口

在外部网络接口处为提供公用电信服务而进行的与公用网络的连接。

12.2.1.5 尺寸和配置

12.2.1.5.1 配线架

综合布线实现中包括的子系统数目和类型取决于园区或楼宇的布局、尺寸及用户的策略。通常,每个园区中应该有一个园区配线架、每个楼宇一个楼宇配线架、每个楼层一个楼层配线架。如果建筑物仅包含很小的单个楼宇,单个楼宇配线架就足够为其提供服务,就不需要园区主干布线子系统。同样,较大的楼宇可通过园区配线架互连多个楼宇配线架实现。

楼层配线架设计应保证快接跳线/压接跳线和设备跳线的长度最小,管理应保证工作期间保持设计长度。

信道最大长度如表 1 表示。

表 1 最大信道长度

信 道	长度/m
水平	100
水平+楼宇主干+园区主干	2 000

注:在水平布线子系统的某些实现中,FD 到 TO 的最大距离可能小于 100 m。

每个楼层应至少设置一个楼层配线架。对于超过 1 000 m² 的楼层空间,对当作办公用的每 1 000 m² 楼层空间提供至少一个楼层配线架。如果楼层空间人员稀少(例如,大堂),允许使用放置在相

邻楼层的配线架。可以对多个配线架的功能进行组合。图 7 示出了综合布线的例子,图 7 中前面的楼宇给出每个配线架分开放置的例子,后面的楼宇给出楼层配线架和楼宇配线架的功能已经组合成单个配线架的例子。

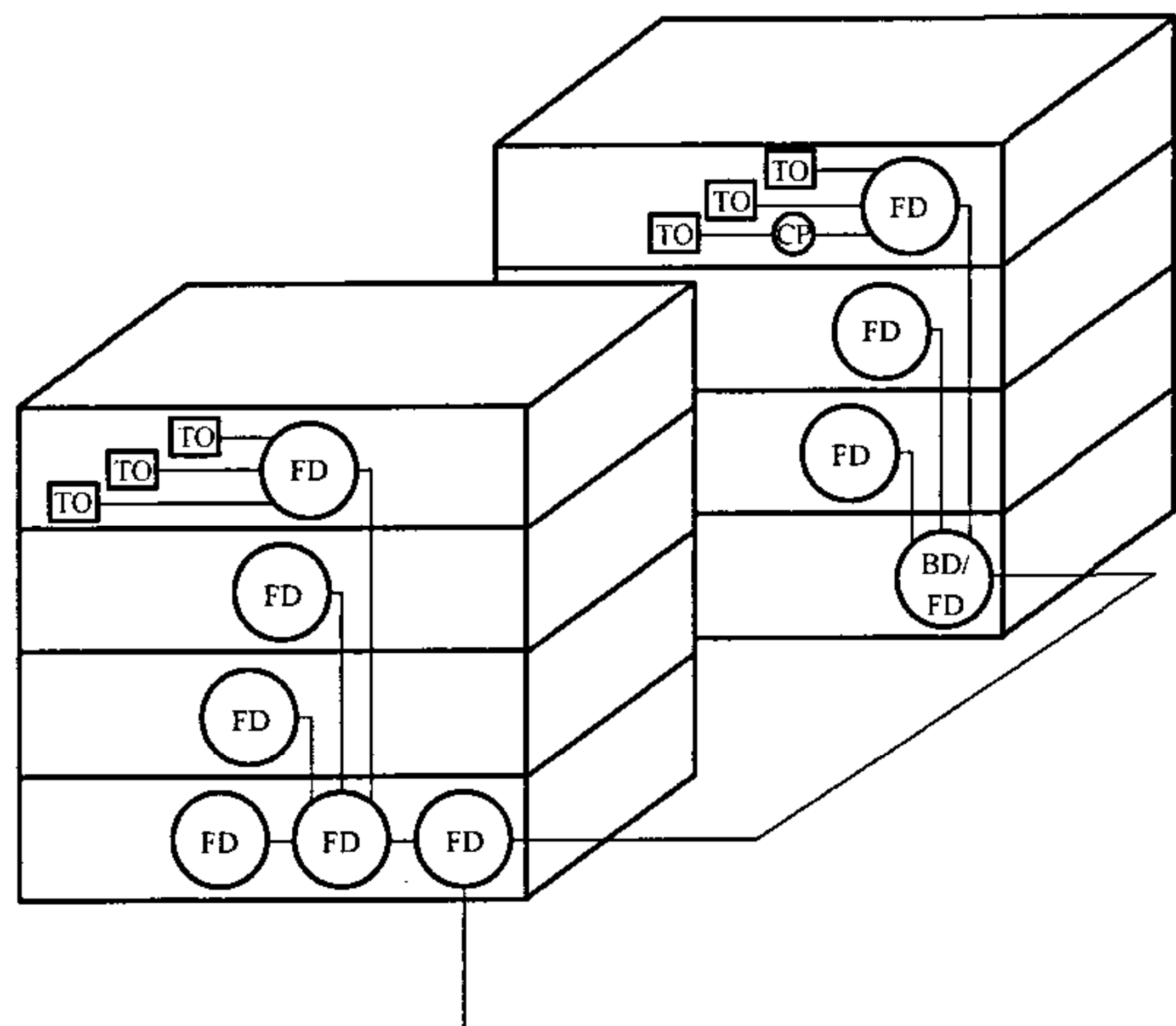


图 7 带组合 BD 和 FD 的综合布线系统例子

在某些情况下,为了安全和可靠性,布线设计中可以使用冗余。

12.2.1.5.2 线缆

包括平衡线缆和光缆。具体分类见表 2。

表 2 线缆分类

	线缆类别
4 对 100 Ω 平衡线缆	屏蔽双绞线
	非屏蔽双绞线
光缆	单模光缆
	多模光缆

具体性能见 12.2.2。

12.2.1.5.3 连接硬件

综合布线中涉及连接硬件为两类：

- a) 平衡线缆连接硬件；
- b) 光缆连接硬件。

其中,平衡线缆连接硬件是指电信插座、转接面板、汇集点连接器、接合和交叉连接。光缆连接硬件是指 SC-D 连接器、SFF 连接器和与连接器相配合的光耦合器。

12.2.1.5.4 工作区跳线和设备跳线

工作区跳线连接电信插座和终端设备,设备跳线连接设备和综合布线的配线架。两者都是非永久的。信道设计时应考虑这些跳线的性能。

12.2.1.5.5 快接跳线和压接跳线

快接跳线和压接跳线用于配线架的交叉连接,信道设计中应考虑这些跳线的性能。

12.2.1.5.6 电信插座 (TO)

综合布线设计应保证在整个可用的楼层空间安装电信插座。当电信插座密度高时,将增强布线适应变化的能力。电信插座可单独或成组地存在。

- a) 每个单独的工作区应至少有两个 TO。
- b) 第一个插座宜是终接 4 对平衡线缆。
- c) 第二个插座可以是:
 - 1) 光纤;
 - 2) 4 对平衡线缆。
- d) 每个电信插座应有用户可见的永久标识。
- e) 如果使用不平衡变换器和阻抗匹配适配器等装置,应该处于插座的外部。

12.2.1.5.7 汇集点

在开放办公室环境中,在楼层配线架和电信插座之间的水平布线中可安装汇集点。FD 和任意 TO 之间允许有一个汇集点。汇集点应该只包含无源硬件并且不应作为交叉连接使用。

另外,在使用汇集点的地方:

- a) 放置汇集点以便每个工作区组至少由一个汇集点提供服务;
- b) 一个汇集点最多供 12 个工作区使用;
- c) 汇集点应位于易操作的位置;
- d) 对于平衡布线,汇集点的位置距楼层配线架至少有 15 m;
- e) 汇集点应该是管理系统的一部分。

12.2.1.5.8 电信间和设备间

设备间应该为放置其中的无源部件、有源装置和外部网络接口提供所有设施(空间、电源、环境控制等)。每个电信间应该直接访问主干布线子系统。

设备间是放置设备的楼宇内的一个区域。由于设备(例如,PBXs 或扩展性的计算机装置)的特征和复杂性,因此,设备间与电信间区别对待。设备间中可放置多个配线架。如果电信间供多个楼宇配线架使用,它应当作为设备间。

12.2.1.5.9 楼宇入口设施

在建筑及居住区主干、公用和专用网络线缆(包括来自天线的线缆)进入楼宇,以及对内部线缆转接时,则要求有楼宇入口设施。楼宇入口设施包括楼宇外部的入口点和通向园区配线架或楼宇配线架的通路。在终接外部线缆的地方,本地法规可能要求特殊设施。在此终接点可以发生外部到内部线缆的变化。

12.2.2 综合布线的性能

12.2.2.1 平衡布线

12.2.2.1.1 概述

本条规定通用平衡布线的最低性能。针对信道、永久链路和 CP 链路规定了平衡布线的性能(见图 8)。

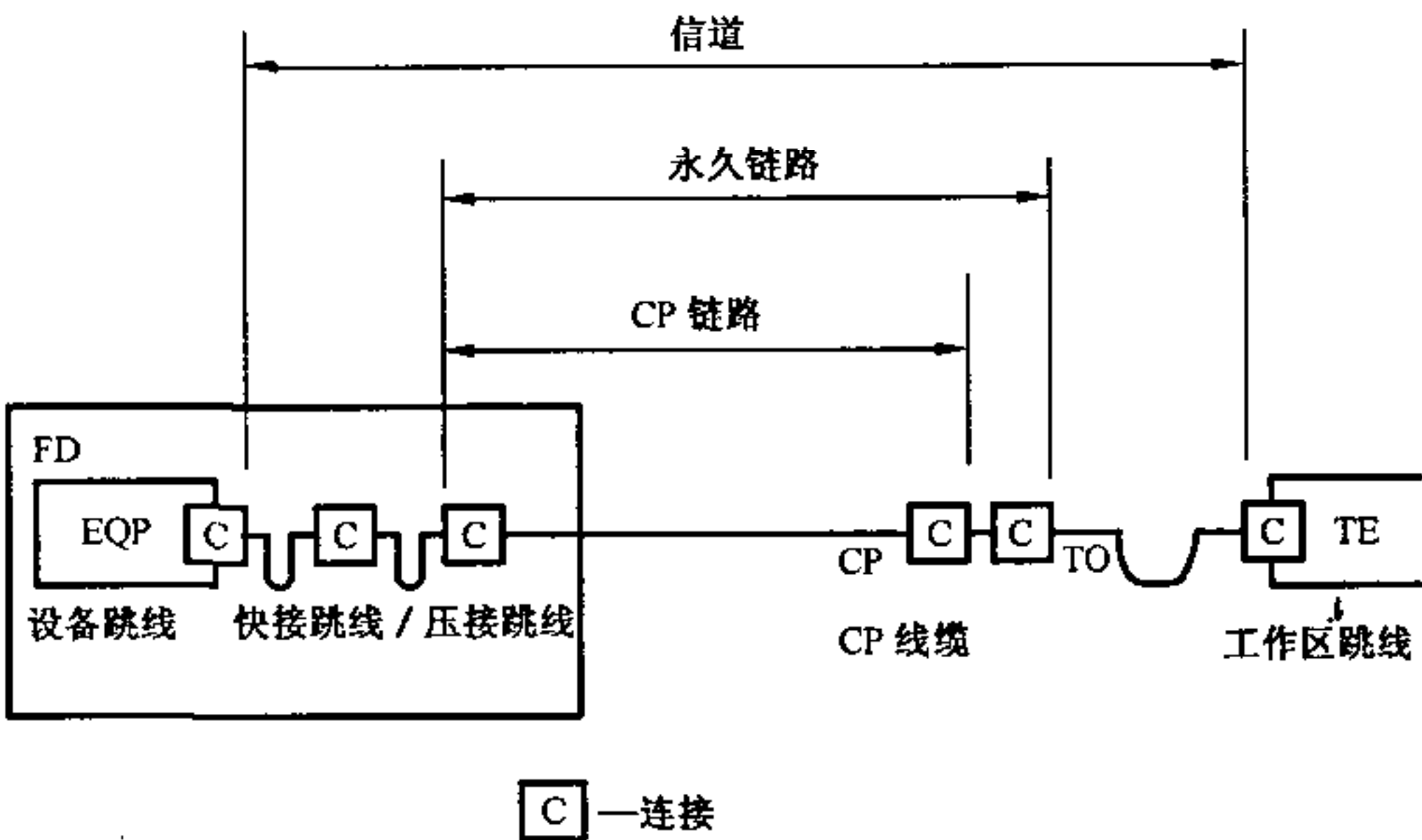


图 8 平衡布线的信道、永久链路和 CP 链路

平衡布线要求如下:

- a) 信道的物理长度不超过 100 m;
- b) 永久链路水平线缆的物理长度不超过 90 m。当跳线、设备和工作区跳线的总长度超过 10 m 时,允许的固定水平线缆的物理长度相应减少;
- c) 如放置汇集点,距楼层配线架至少有 15 m;
- d) 当使用多用户 TO 组件时,工作区跳线的长度不应超过 20 m;
- e) 压接跳线/快接跳线线缆的长度不应超过 5 m。

对于平衡布线,性能规范分成 6 个类别(A 至 F,见 12.2.2.1.3)。

12.2.2.1.2 布局

信道性能是有源设备之间的连接的性能。信道仅包括线缆的无源部分、连接硬件、工作区跳线、设备跳线和快接跳线。不考虑连接有源设备硬件接口处的连接。

应用支持仅取决于信道性能,信道依次取决于线缆长度、连接数量、连接器终接的质量和性能。在信道比较长的情况下,通过使用较少的连接或使用更高性能的部件可能获得等价的信道性能。

12.2.2.1.3 平衡布线分类

本部分规定下列平衡布线类别。

A 类:规定高达 100 kHz。

B 类:规定高达 1 MHz。

C 类:规定高达 16 MHz。

D 类:规定高达 100 MHz。

E 类:规定高达 250 MHz。

F 类:规定高达 600 MHz。

规定 A 类信道以便它能提供最低传输性能来支持 A 类应用。同样,B、C、D、E 和 F 信道提供传输性能分别支持 B、C、D、E 和 F 类应用。

安装水平布线中的信道、永久链路和 CP 链路应该提供至少 D 类性能。

12.2.2.1.4 平衡布线的性能

本条规定的参数适用于屏蔽或非屏蔽线缆部件、有或无整体屏蔽的信道。

信道的标称阻抗是 100 Ω 。该阻抗通过合适的设计和适当选择布线组件达到(不对应于布线各组件的标称阻抗)。

要求性能项目如下:

- a) 回波损耗;
- b) 插入损耗/衰减;
- c) 近端串扰衰减(NEXT)
 - 1) 线对到线对的 NEXT
 - 2) 功率和 NEXT (PS NEXT)
- d) 衰减与串扰比(ACR)
 - 1) 线对到线对的 ACR
 - 2) 功率和 ACR(PS ACR)
- e) 等电平远端串扰衰减(ELFEXT)
 - 1) 线对到线对的 ELFEXT
 - 2) 功率和 ELFEXT (PS ELFEXT)
- f) 直流(d. c.)回路电阻;

- g) 直流(d. c.)电阻不平衡;
- h) 电流运载容量;
- i) 工作电压;
- j) 功率容量;
- k) 传播延迟;
- l) 延迟偏差;
- m) 不平衡衰减;
- n) 耦合衰减。

12.2.2.2 光纤布线性能

12.2.2.2.1 概述

本部分规定光纤的四种类型来支持各种应用类别,3 种多模光纤类型(OM1、OM2 和 OM3)和一种单模光纤类型(OS1)。同时规定下列布光缆类别:

在上述引用的光纤类型上,OF-300 类型的信道支持的应用最短为 300 m。

在上述引用的光纤类型上,OF-500 类型的信道支持的应用最短为 500 m。

在上述引用的光纤类型上,OF-2000 类型的信道支持的应用最短为 2 000 m。

12.2.2.2.2 组件选择

需要的信道长度、被支持的应用和布线的估计寿命将确定对光纤组件的选择。光纤信道的性能要求基于使用每个规定传输窗口中的单个光波长。

在应用标准中可找到波长多路复用和解多路复用组件的要求。对涉及波长多路复用的综合布线没有特殊要求。

12.2.2.2.3 信道衰减

信道衰减应不超过表 3 中所示的值。该值基于总分配给连接硬件的 1.5 dB。如果应用的功率预算允许,可以使用附加的连接器和接合。在规定的波长上,信道和永久链路的衰减不应超过在那个波长上对部件规定的衰减值的和(一定长度的光缆衰减由光缆衰减系数乘以光缆长度获得)。

表 3 信道衰减

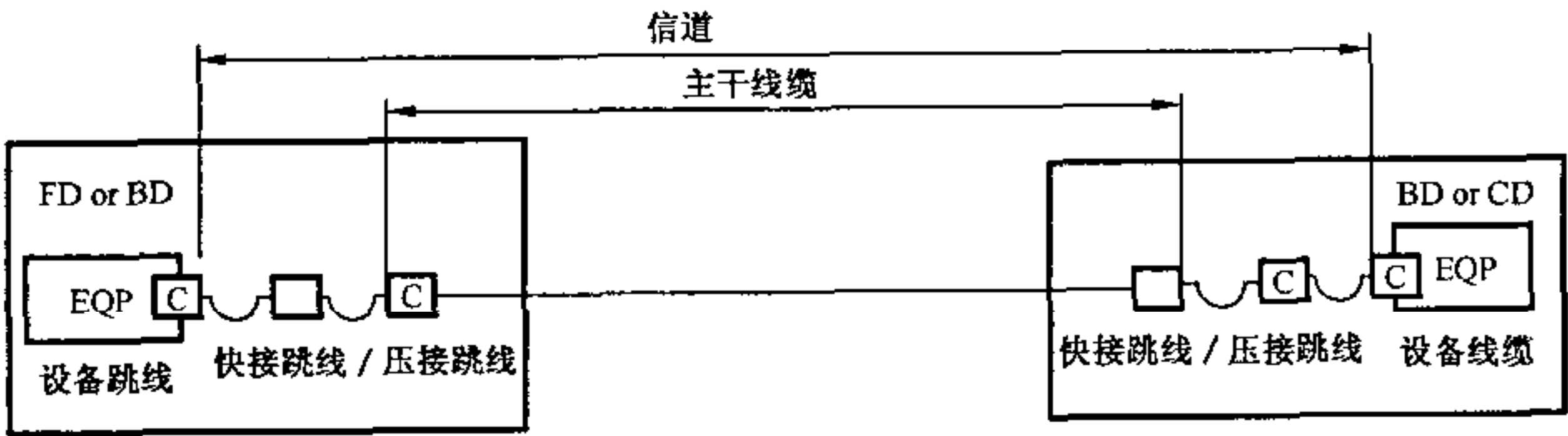
信道衰减 dB				
信道	多模		单模	
	850 nm	1 300 nm	1 310 nm	1 550 nm
OF-300	2.55	1.95	1.80	1.80
OF-500	3.25	2.25	2.00	2.00
OF-2000	8.50	4.50	3.50	3.50

12.2.2.2.4 信道拓扑

图 9 和图 10 模型适用于水平和主干光纤布线。应注意用来终接光纤布线的连接系统可包括配合的连接硬件和接合(永久的或可重复使用的),并注意该交叉连接可由可重复使用的接合组成。

把光纤敷放到 TO 通常不需要在 FD 处的传输设备(除非主干布线子系统的光纤设计与水平布线子系统不同)。这允许创建如图 10 所示的主干/水平组合信道。这三个图示出了跳线连接式信道、接合式信道和直通式信道(它不需要使用 FD)。用跳线连接的信道和接合的信道的设计也可应用于园区/楼宇主干组合信道。

采用永久接合的信道和直通信道可用作减少信道衰减和集中配线的手段。然而,集中配线可能降低综合布线的整体灵活性。



EQP—设备；C—连接；FD—楼层配线架；BD—楼宇配线架；CD—园区配线架

图 9 主干布线模型

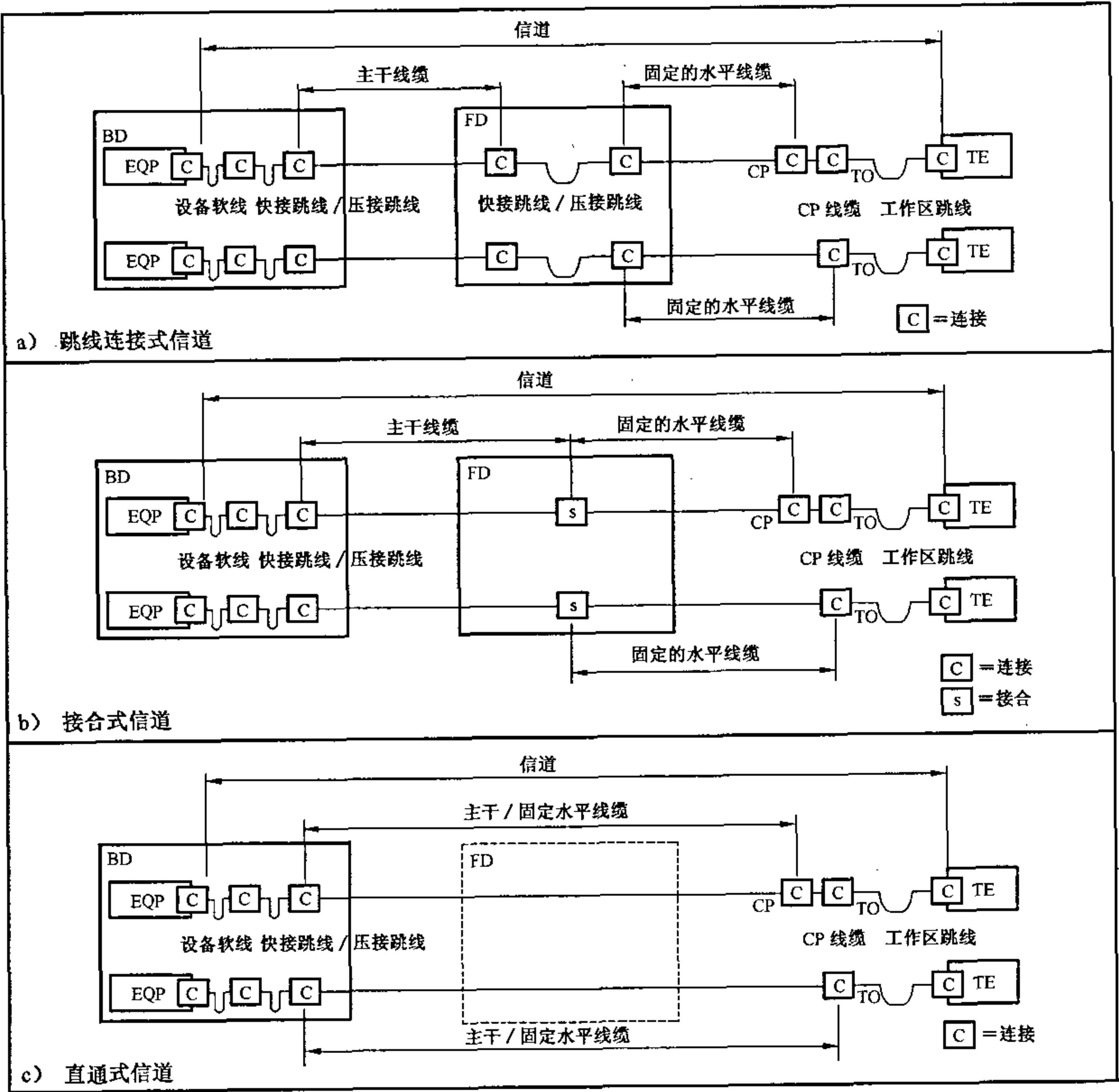


图 10 主干/水平组合信道

为了适应于给定类别的信道中配合连接和接合数量的不断增加，信道的总长度可能不得不减少，以适应附加的衰减。

12.2.2.2.5 传播延迟

对于某些应用，了解光纤信道的延迟很重要。这可保证与由多级联信道组成的复杂网络的端到端延迟要求的适应性。由于这个原因，知道光纤信道的长度很重要。根据线缆性能可计算传播延迟。

12.2.2.3 屏蔽实施、电磁性能、接大地、管理

12.2.2.3.1 屏蔽实施

本条适用于屏蔽线缆元素。为电气安全和电磁性能两者提供充分的接地所必需的规程可参照国家或行业标准，并应符合所用产品厂商的规定。

12.2.2.3.2 电磁性能

为了获得优化的 EMC 性能，布线屏蔽体应等电位联结到大地。形成屏蔽信道部分的所有布线组件应加以屏蔽，并满足屏蔽要求。屏蔽布线链路应满足屏蔽布线的要求。线缆屏蔽体应通过满足布线屏蔽要求所必需的足以维护屏蔽连续性的低阻抗连接进行终接。应向供应商索取如何接入低阻抗终接的说明书并遵守之。工作区、设备跳线 and 设备连接宜加以屏蔽，这样做才能提供屏蔽的连续性。

12.2.2.3.3 接大地

应该按照第 14 章要求接大地并进行连接。线缆的全部屏蔽体应被连接在每个配线架上。通常，这些屏蔽体被连接到设备机架，而设备机架被依次连接到楼宇大地。

注：高的工作频率和/或高的寄生电流或寄生场要求用低阻抗接大地，该低阻抗可以用网状系统来实现。

连接的设计应能确保：

- a) 大地通路应该是永久、连续和低阻抗的。建议每个设备机架各自连接，以便保证大地通路的连续性。
- b) 线缆屏蔽体对它所互连的布线系统的所有部分提供连续的大地通路。

该连接确保：感应到布线的电压（通过来自电力线的或其他干扰源的任何干扰）直接通往楼宇地线，不会引起对所发送信号的干扰。在楼宇内不同系统的所有接地电极引线应连接在一起，以减少地线电位差的影响。在该网络上任何两条地线之间，该楼宇接地系统不应超过 1 V(r. m. s) 的接地电位差极限值。

12.2.2.3.4 管理

管理是综合布线的基本方面，只有正确地管理布线和使用，才能充分发挥综合布线的灵活性。管理包括准确标识和记录构成布线系统的所有组件以及通路、配线架和安装它的空间。当布线进行变更时，应该记录它们的所有变化。对于大型的安装，极力推荐用计算机管理记录。

12.2.3 无线接入点的综合布线

在设计无线接入时，水平布线应考虑以下几点：

- a) 最少的配置、结构和拓扑；
- b) 永久链路和信道的性能要求；
- c) TO 的覆盖区域和位置；
- d) 与无线接入点的接口。

无线覆盖区域的 TO 网格示例见图 11。

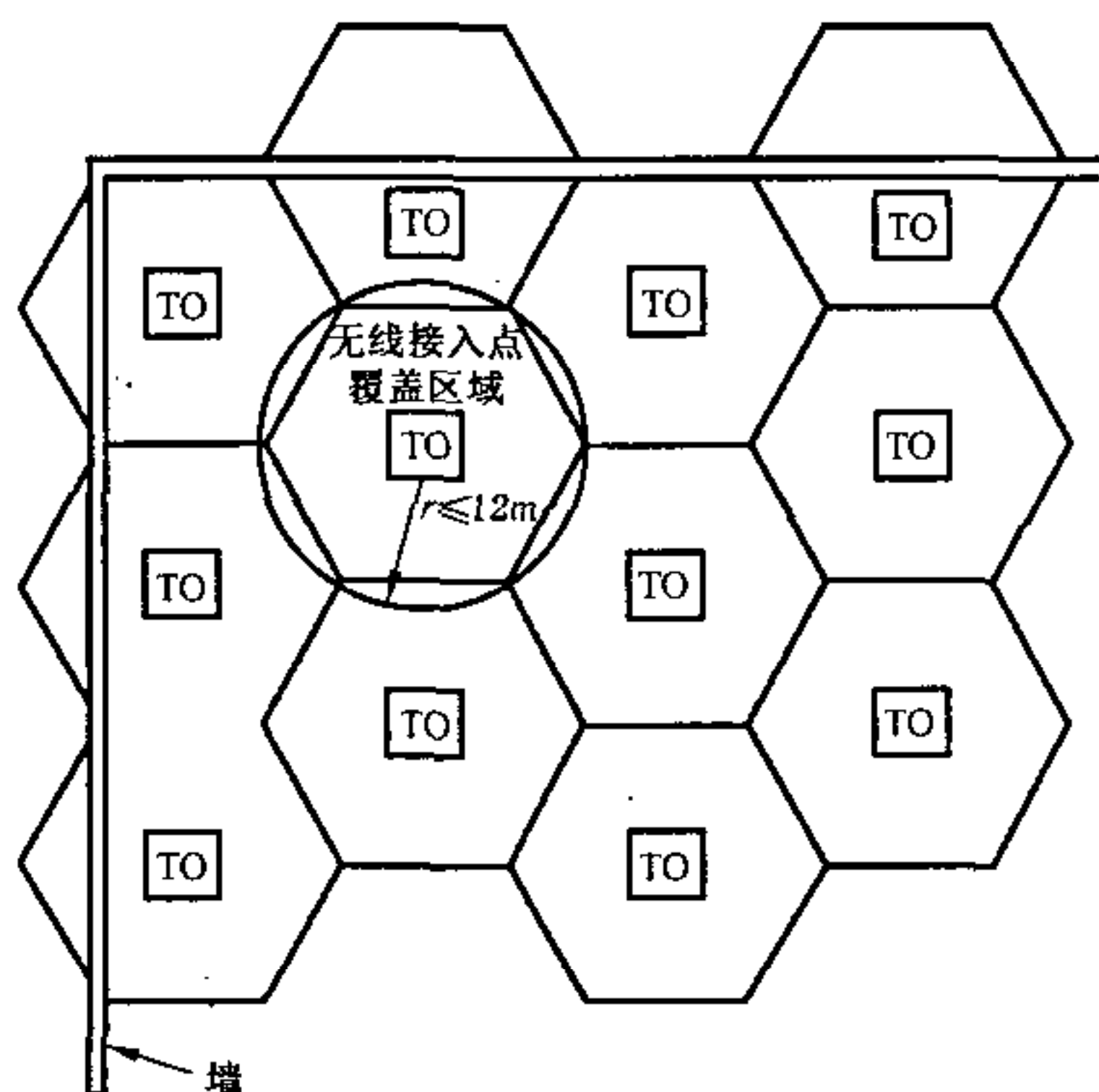


图 11 无线覆盖区域的 TO 网格示例

13 基础系统集成

13.1 总则

13.1.1 基础系统集成是通信系统、信息系统、监控系统和基础设施及技术的集成,该集成包括多网(信息、语音、视频、监控)融合的结构模式。

13.1.2 集成是实现协调调度与综合优化控制,使整个建筑数字化工程构成一个有机的整体,达到信息综合、资源共享的目的。

13.2 要求

13.2.1 设备的通信协议和接口应符合国家或国际现行有关标准的规定。

13.2.2 集成系统工作的准确性、可靠性

- a) 被集成的各子系统与集成系统之间通信应准确无误,各子系统应能物理的、逻辑的互连,实现信息共享、协同工作;
- b) 集成系统对各子系统有很好的控制功能;
- c) 系统运行中,在正常、满负载的条件下应具有很好的响应和可靠性。

14 电源与接地

14.1 总则

14.1.1 电源与接地关系到保证建筑物内各系统的正常运行和安全,应保证其可靠性和安全性。

14.1.2 电源与接地应符合 GB 50057、GB/T 50314 及 JGJ/T 16—1992。

14.2 要求

14.2.1 电源系统

14.2.1.1 供电电源质量或采取稳频稳压及不间断供电等措施后的电源质量应满足 GB/T 50314 中对电源的要求。

14.2.1.2 两路供电电源的自动切换应满足设计要求。

14.2.1.3 应急电源的启动和投入应满足设计要求。

14.2.1.4 不间断电源的工作状况和工作时间应满足设计要求。

14.2.1.5 数字化系统的总控制室应设置专用配电箱,各子系统电源应可独立控制,电源的容量和出回路应留有余量并要求整个电源系统有备用容量。

14.2.1.6 电力干线与弱电干线宜分别设置独立的竖井。

14.2.1.7 电源插座应采用带有接地极的插座,并符合国家标准要求。

14.2.2 接地

14.2.2.1 建筑物应采用总等电位联结,各数字化系统的接地应引至建筑物联合接地装置,接地电阻不应大于 $1\ \Omega$ 。

14.2.2.2 防雷保护接地,应按国家标准 GB 50057(2000 年修订版)执行。

15 环境

15.1 总则

15.1.1 环境包括建筑物的室内空调环境、空气环境质量、空间环境、视觉照明环境和室内电磁干扰环境。

15.1.2 智能建筑的环境工程主要指为用户创造舒适性的条件,包括天花板、墙壁、地板、照明、空气调节、噪声的控制等方面。建筑物和场馆用建筑及装饰装修材料应符合 GB 18580、GB 18581、GB 18582、GB 18583、GB 18584、GB 18585、GB 18586、GB 18587、GB 18588 和 GB 6566 等标准要求。

15.2 要求

15.2.1 室内空调环境

室内温度、相对湿度值应符合标准 GB/T 18883 的规定。

15.2.2 空气环境质量

室内空气污染物总量控制指标应符合标准 GB 50325、GB/T 18883 的规定。

16 机房系统

16.1 总则

16.1.1 机房系统应符合相关国家标准 GB/T 2887、GB 9361、GB 50052、GB 50057、GB 50116、GB 50174和 SJ/T 10796—2001。

16.2 要求

16.2.1 温度

机房系统内温度必须满足电子设备的要求，按开机时和停机时加以规定，见表 4、表 5。

表 4 开机时机房温度要求

项 目	指 标		
	A 级		B 级
	夏季	冬季	
温度/℃	23±2	20±2	15~30
温度变化率/(℃/h)	<5 不得凝露		<5 不得凝露

表 5 停机时机房温度要求

项 目	指 标	
	A 级	B 级
温度/℃	5~35	5~35
温度变化率/(℃/h)	<5 不得凝露	<5 不得凝露

16.2.2 湿度

机房系统内湿度必须满足电子设备的要求，按开机时和停机时加以规定，见表 6、表 7。

表 6 开机时机房湿度要求

项 目	指 标	
	A 级	B 级
相对湿度/%	45~65	40~70

表 7 停机时机房湿度要求

项 目	指 标	
	A 级	B 级
相对湿度/%	40~70	20~80

16.2.3 尘埃

机房系统内的尘埃依机器要求而定，主机房内粒径大于或等于 0.5 μm 的尘埃个数应小于或等于 18 000 粒/dm³。

16.2.4 噪声

电子设备停机时机房内的噪声在主机房中心处应小于 65 dB(A)。

16.2.5 照明

16.2.5.1 普通照明

机房系统在距地面 0.8 m 处,照度不应低于 300 lx,其他房间按 GB/T 2887 执行。

16.2.5.2 应急照明

机房系统、终端室、已记录的媒体存放间应设应急照明,其照度在距地面 0.8 m 处不应低于 5 lx。

主要通道及有关房间依据需要应设疏散照明,其照度在距地面 0.8 m 处不应低于 1 lx。

16.2.6 无线电干扰环境场强

机房系统内无线电干扰环境场强,在频率范围 0.15 MHz ~ 1 000 MHz 时不大于 126 dB。

16.2.7 磁场干扰环境场强

机房系统内磁场干扰环境场强不大于 800 A/m(相当于 10 Oe)。

16.2.8 风量

16.2.8.1 总送风量、总回风量

机房系统内的总送风量、总回风量应满足设计要求。

16.2.8.2 新风量

空调系统的新风量应取下列三项中的最大值:

- a) 室内总送风量的 5%;
- b) 按工作人员每人 40 m³/h;
- c) 维持室内正压所需风量。

16.2.8.3 出口风速

采用活动地板下送风时,出口风速不应大于 3 m/s。

16.2.9 正压

电子设备主机房必须维持一定的正压,主机房与其他房间、走廊间的压差不应小于 4.9 Pa,与室外静压差不应小于 9.8 Pa。

16.2.10 装修材料

机房系统内装修材料的选择应符合 GB 9361 和 GB 50174 中的规定。

16.2.11 漏水

机房系统内有空调系统或供暖系统,必要时在空调机四周、暖气四周、水管沿线等处,敷设漏水传感系统。

16.2.12 接地电阻

16.2.12.1 机房系统接地装置的设置应满足人身的安全及电子设备的正常运行和系统设备的安全要求。

16.2.12.2 机房系统一般具有下列四种接地方式:

- a) 交流工作接地,接地电阻不应大于 4Ω;
- b) 安全保护接地,接地电阻不应大于 4Ω;
- c) 直流工作接地,接地电阻应按电子设备系统的具体要求确定;
- d) 防雷保护接地,应按 GB 50057 执行。

16.2.12.3 交流工作接地、安全保护接地、直流工作接地、防雷保护接地等四种接地宜共用一组接地装置,其接地电阻值应 $\leq 1\Omega$ 。若防雷接地单独设置接地装置时,其余三种接地宜共用一组接地装置,其接地电阻不应大于其中最小值,并按 GB 50057 要求采取防止反击措施。

16.2.12.4 对直流工作接地有特殊要求需单独设置接地装置的电子设备系统,其接地电阻值应按电子设备的要求确定,专用接地或直流接地宜采用一点接地,在室内不应与其他接地相连,此时距其他接地

装置的地下距离不应小于 20 m。

16.2.12.5 诸地之间的关系及接法应依不同电子设备系统的要求而定。

16.2.12.6 电子设备系统的接地应采取单点接地并宜采取等电位措施。

16.2.12.7 当多个电子设备系统共用一组接地装置时,宜将各电子设备系统分别采用接地线与接地体相连接。

16.2.13 防雷

16.2.13.1 机房系统电源进线应按 GB 50057 采取防雷措施。机房系统电源应采用地下电缆进线。当不得不采用架空进线时,在专用电力变压器低压配电母线处,应装设低压避雷器。

16.2.13.2 机房系统一般采用专用配电柜(箱)配电,并在电源进线的总配电柜(箱)处加装防浪涌装置。

16.2.13.3 信息系统的所有外露导电物应建立一等电位连接网络。信息系统的各种箱体、壳体、机架等金属组件与建筑物的共用接地系统做总等电位联结。

16.2.14 频率

交流电源频率为 50 Hz。

16.2.15 电源参数

16.2.15.1 电子设备供电电源质量根据电子设备的性能、用途和运行方式(是否联网)等情况,可分为 A、B、C 三级。

16.2.15.2 电源参数允许的变动范围见表 8。

表 8 电源参数

等级	A	B	C
静态电压偏移范围/(%)	-5~+5	-10~+10	-15~+10
静态频率偏移范围/Hz	-0.2~+0.2	-0.5~+0.5	-1~+1
电压波形畸变率/(%)	5	7	10
允许断电持续时间/ms	0~4	4~200	200~500

注：如电源参数不符合表 8 的要求,宜采用 UPS 供电,并完成相关检测。

16.2.16 静电防护

16.2.16.1 基本工作间不用活动地板时,可铺设导静电地面,导静电地面可采用导电胶与建筑地面粘牢,导静电地面的体积电阻率均应为 $1.0 \times 10^7 \Omega \cdot \text{cm} \sim 1.0 \times 10^{10} \Omega \cdot \text{cm}$,其导电性能应长期稳定,且不易发尘。

16.2.16.2 电子设备主机房内采用的活动地板可由钢、铝或其他阻燃材料制成。活动地板表面应是导静电的,严禁暴露金属部分。单元活动地板的系统电阻应符合 SJ/T 10796—2001 的规定。

16.2.16.3 电子设备主机房内的工作台面及座椅垫套材料应是导静电的,体积电阻率均应为 $1.0 \times 10^7 \Omega \cdot \text{cm} \sim 1.0 \times 10^{10} \Omega \cdot \text{cm}$ 。

16.2.16.4 电子设备主机房内的导体必须与大地做可靠的联接,不得有对地绝缘的孤立导体。

16.2.16.5 导静电地面、活动地板必须进行静电接地。

16.2.16.6 静电接地的连接线应有足够的机械强度和化学稳定性。导静电地面和台面采用导电胶与接地导体粘接时,其接触面积不宜小于 10 cm^2 。

16.2.16.7 静电接地可以经过限流电阻及自己的连接线与接地装置相连,限流电阻的阻值宜为 $1 \text{ M}\Omega$ 。

16.2.16.8 活动地板面的静电电压应小于 1 000 V。

16.2.17 供配电

16.2.17.1 机房系统用电负荷等级及供电要求应按 GB 50052 的规定执行。

16.2.17.2 依据电子设备的用途,其供电方式可分为三类:

- a) 一类供电:需建立不间断供电系统;
- b) 二类供电:需建立备用的供电系统;
- c) 三类供电:按一般用户供电考虑。

16.2.17.3 机房系统供配电系统应考虑电子设备有扩展、升级等可能性,并应预留备用容量。

16.2.17.4 机房系统低压供配电系统应采用频率 50 Hz、电压 220 V/380 V, TN-S 或 TN-C-S 系统。

16.2.17.5 机房系统应设置一定数量的维修和测试用电源插座。

16.2.17.6 机房系统活动地板下的低压配电线路宜采用铜芯屏蔽导线或铜芯屏蔽电缆,电源线应尽可能远离电子设备信号线并避免并排敷设。当不能避免时,应采取相应的技术措施。活动地板下敷设的电缆一般采用金属线槽保护。

16.2.18 消防

16.2.18.1 机房系统应按 GB 9361 中的规定设置气体灭火系统,并应按现行有关规范的要求执行。

16.2.18.2 机房系统应设火灾自动报警系统,并应符合 GB 50116 的规定。

16.2.18.3 报警系统和自动灭火系统应与空调、通风系统联动。空调系统所采用的电加热器,应设置无风断电保护。

16.2.18.4 设置气体固定灭火系统,应配置自动关闭门、窗、风道装置。

16.2.18.5 电子设备主机房宜采用感烟探测器。当设有固定灭火系统时,应采用感烟、感温两种探测器的组合。

16.2.18.6 当电子设备主机房内设置空调设备时,应受主机房内电源切断开关的控制。机房内的电源切断开关应靠近工作人员的操作位置和主要出入口。

16.2.19 安全

16.2.19.1 机房系统的安全设计应符合 GB 9361 的规定。

16.2.19.2 根据机房系统的重要性,可安装门禁系统、视频监视系统、入侵报警系统。

16.2.19.3 电子设备主机房出口应设置向疏散方向开启且能自动关闭的门。并应保证在任何情况下都能从机房内打开。

16.2.19.4 凡设有气体灭火装置的机房系统,应安装排气装置。

16.2.19.5 机房系统内存放废弃物应采用有防火盖的金属容器。

16.2.19.6 机房系统内应采取防鼠害措施。在易受鼠害的场所,机房内的电缆和电线上应涂敷驱鼠药剂。

16.2.20 空气质量

16.2.20.1 机房系统内的空气质量要求见第 15 章。

17 家用电子系统

17.1 总则

家用电子系统(HES)是指遵循 HES 标准(参见 ISO/IEC TR 14543 系列标准)的家用控制系统(Home Control System),它是由家庭网络和与之相连接的所有设备组成,同时包括各家庭应用过程中的控制、通信和管理规则。如图 12。

家用电子系统分为以下三类:

- a) 第一类家用电子系统是指具有遥控应用传输能力的家用控制系统,这些应用包括控制、监视、测量、报警以及低速数据传送等;
- b) 第二类家用电子系统除应实现第一类系统的传输能力外,还具有交换话音或者类话音传输带

宽的信息传输能力；

- c) 第三类家用电子系统除实现第二类系统的传输能力外，还具有高质量的音视频和高速数据的信息传输能力。

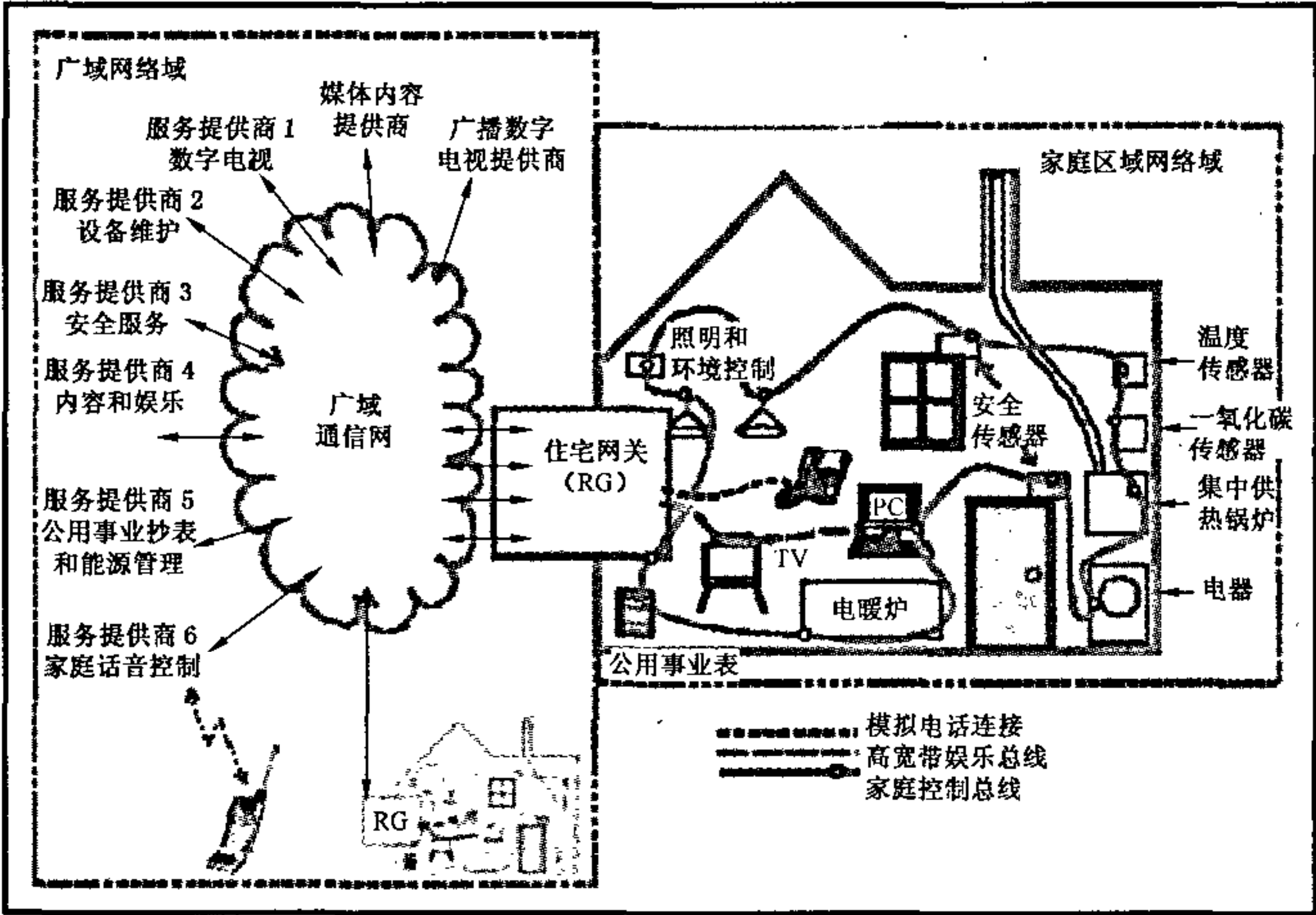


图 12 家庭网络提供的典型服务

家用电子系统由两大部分构成：家用电子设备与家用网络系统构成，两部分之间通过通用接口（UI）和过程接口（PI）进行连接，以便保证设备网络的独立性。这样，与媒体相关的家庭网络，以及与应用相关的设备，可以各自开发，如图 13。相关接口技术参见 ISO/IEC 10192。

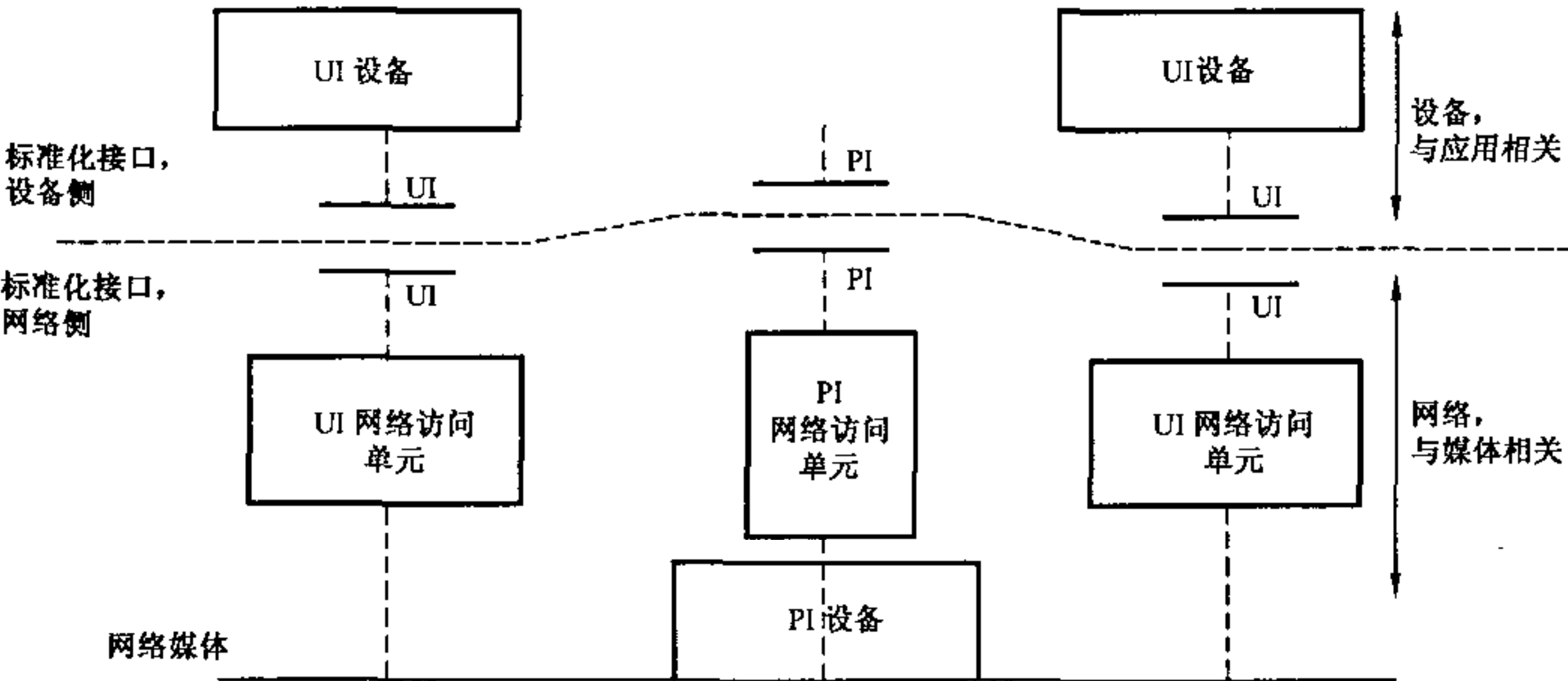


图 13 UI 和 PI 示意图

PI 用于某些简单设备，这些设备并不要求完全实现家用电子系统（HES）的应用协议。UI 允许任何实现了 UI 的设备连接到任何实现了 UI 的家庭网络中。

家用电子系统的设计、安装和验收应该充分注意照明设备、供暖设备、烹饪设备、洗涤设备、能源管理设备、供水控制设备、火警和盲人控制设备、家用紧急报警系统、计算设备和通信设备等多种应用的集成，提高不同应用之间的互连、互通、互操作。家用电子设备与家用网络系统之间的接口、家用电子设备的组网以及设备与网络之间、设备与设备之间的通信，如图 14 所示。

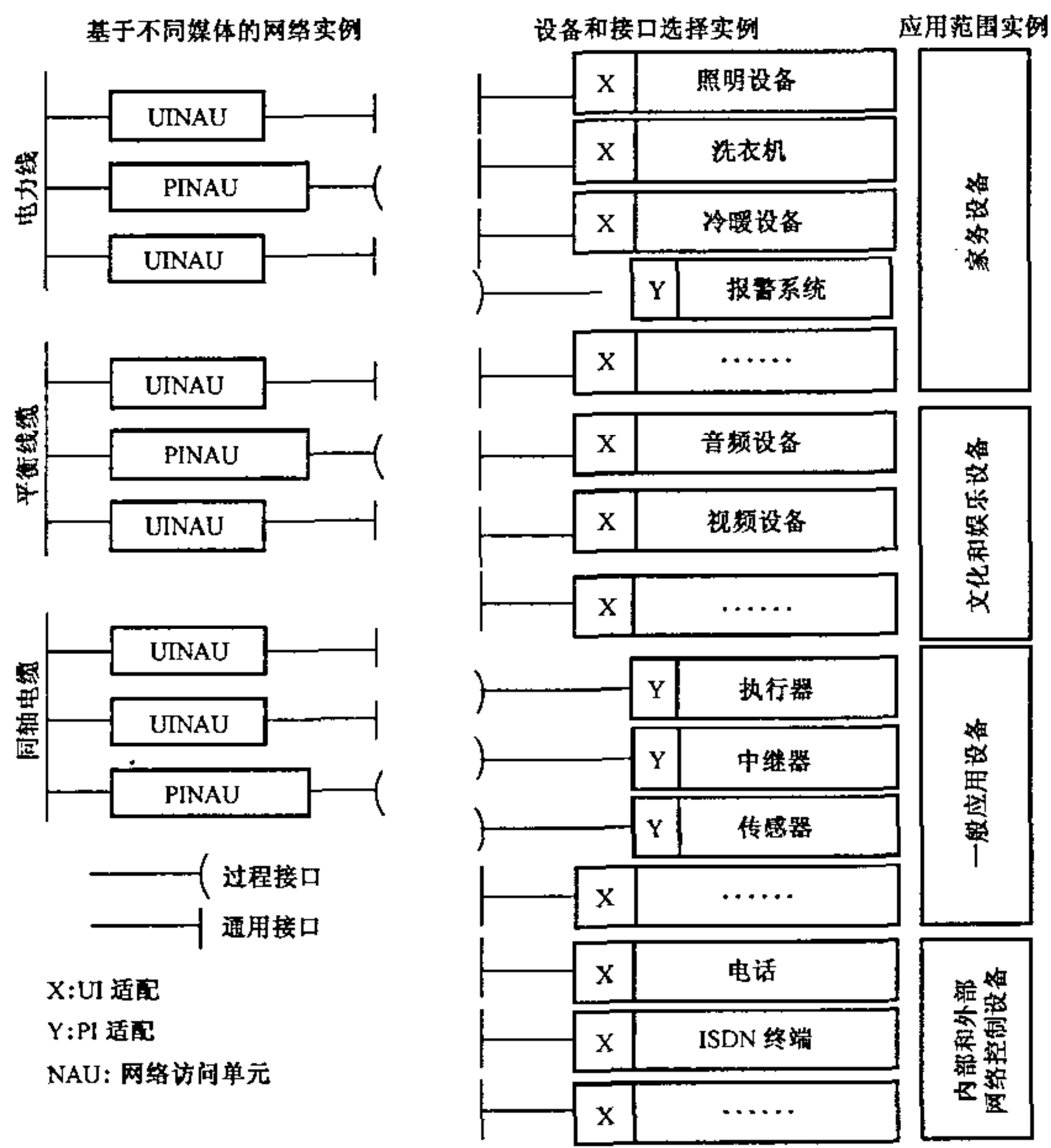


图 14 家用电子系统应用示例

住宅网关是家用电子系统中的一种设备,用于将家庭网络中不同类型的网络连接起来,同时将家用电子系统与家庭外的广域网连接起来。如图 15。参见 ISO/IEC 15045-1。

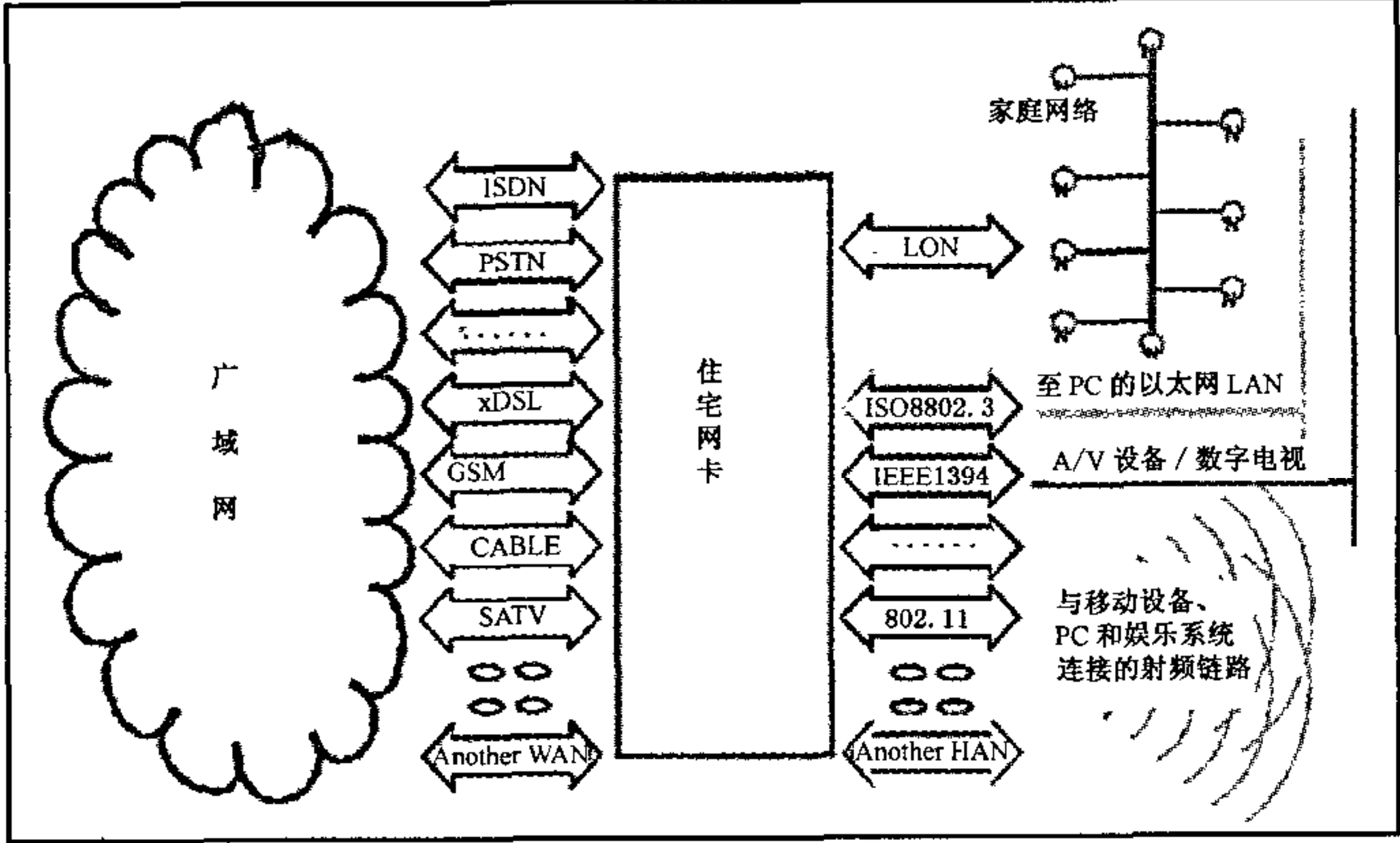


图 15 住宅网关连接和接口示意图

17.2 要求

家用电子系统应满足下列要求:

- a) 家用电子设备与家庭网络之间宜相对独立,并通过 UI 或者 PI 接口实现连接;
- b) 家用电子系统宜与所在居住区智能控制系统或物业管理系统互连,但应避免居住区的智能控制系统直接与家用电子系统的传感器、执行器和设备自身直接相连,应通过业主单元网络接口(Tenant Unit Network Interface)实现家用电子系统与建筑物智能控制系统之间的互连,以阻断一些涉及业主隐私的动作。使用者单元网络控制接口应提供的功能至少应该包括:总线负载极小化(Bus Load Minimization)、访问保护(Access Protection)、功能性检查(Functional Checks)等;
- c) 在确保系统互连互通的前提下,家庭电子设备的网络传输介质的选择应充分考虑技术的成熟性、设备的移动性、家庭的美观性、操作的方便性等。可选择网络传输媒体包括:电话线、电力线、平衡线缆、同轴电缆、自由空间(例如:红外技术、蓝芽技术或者无线局域网技术)等;
- d) 家用电子系统应采用国家或行业推荐的低层通信协议。应用层协议宜实现《信息设备资源共享协同服务》系列标准(其中已发布 SJ/T 11310—2005, SJ/T 11311—2005)中所定义的功能。

17.3 家用电子系统应用层协议实现要求

参考 SJ/T 11310—2005 和 SJ/T 11311—2005 中的要求,家用电子系统应用层协议实现时应该至少满足下列要求:

- a) 设备宣告:每个设备在设备启动、设备配置信息变化、设备关闭、设备离开网络时应发送相应的设备宣告消息;设备正常运行过程中应根据宣告中声明的间隔持续发送设备宣告消息。同时,每个设备应该能够正确地侦听并理解网络上其他设备发出的设备宣告消息。
- b) 设备/服务查找:每个设备均应实现对设备/服务查找的响应及作为查找发起方的发起设备/服务查找支持。
- c) 非安全设备管道:每个设备应至少实现对设备非安全管道的支持。
- d) 设备组:每个设备应实现加入对等设备组的支持,以及能够加入至少一个主从设备组的支持。如果设备作为家用电子系统的主控设备,则还应至少实现作为主从设备组主控设备所需要的支持。
- e) 服务调用:每个设备均应实现对协议中所定义的会话创建、服务调用的支持。
- f) 异步事件:每个设备均应实现包括设备/服务在内的在线/离线事件订阅及相应事件通知的支持。

详见附录 A。

18 IC 卡应用

18.1 总则

18.1.1 IC 卡系统主要由 IC 卡、终端设备、密钥管理与发卡系统、充值系统、应用及管理系统及安全策略等组成。

18.1.2 IC 卡系统适用于本部分所涉及 IC 卡应用的各种场合,如:门禁、巡更、停车、三表付费、物业管理等。鉴于 IC 卡的应用领域不断扩展,建议在 IC 卡系统建设中应充分考虑“一卡多用”的原则,为未来应用的扩展保留充分的空间以及必要的系统接口。

18.1.3 IC 卡安全策略应符合国家有关信息安全法律、法规的规定和要求,建议使用安全性较强的带有 CPU 的 IC 卡(以下简称智能 IC 卡)。

18.1.4 系统中应用的 IC 卡,应符合 GB/T 16649.1、GB/T 16649.2、GB/T 16649.3、CJ/T 166—2002、ISO/IEC 14443-1、ISO/IEC 14443-2、ISO/IEC 14443-3、ISO/IEC 10373-6 等相关规范的要求。对于带有 CPU 的 IC 卡除上述标准外,还应符合 GB/T 16649.5、ISO/IEC 7816-4、ISO/IEC 14443-4 等规范要求。其他可供参考的规范包括:GB/T 16649.8、ISO/IEC 7816-9 等。

18.2 要求

18.2.1 IC 卡的基本要求

18.2.1.1 IC 卡选型

在建筑及居住区中应用的 IC 卡,提倡采用符合 18.1.4 要求的智能 IC 卡,不得使用没有安全保护措施的存储卡。如使用逻辑加密卡产品,应充分考虑其安全性较差、产品生命周期一般短于系统周期的特点,只能在有其他安全保障措施的环境中作为过渡性技术手段使用,且应为今后升级到智能 IC 卡保留必要的接口并备有能满足系统预计使用寿命的充足的备卡。对于有多个应用的 IC 卡,除符合 18.1.4 的要求外,必须支持应用间的隔离和防火墙,并支持应用的扩展。

18.2.1.2 IC 卡应用卡片结构

IC 卡应用的卡片结构应符合 CJ/T 166 中的规定,对于其中未做规定的应用应符合下述原则:

- a) 所用卡片必须保证“一卡一密”,不得使用统一的密钥;
- b) 多应用的 IC 卡应做到应用间的隔离,并支持应用的扩展;
- c) 应支持卡片的合法性验证;
- d) 对于安全性有一定要求的应用,应考虑采用安全报文技术保证信息在传递过程中的保密性和防篡改性;
- e) 对于需要识别持卡人身份的应用,应首先验证持卡人 PIN 密码或进行生物特征鉴别;
- f) 对于采用电子签名技术的应用,应首先识别持卡人身份;
- g) 使用过程产生意外中断,应具有自动恢复机制。

18.2.2 终端设备

IC 卡系统中使用的终端设备应符合 CJ/T 166 和 SJ/T 11230 中的规定。

所有不与后台控制系统相连脱机使用的终端设备必须支持一个以上的 PSAM 卡座;对于需要检查卡片合法性的终端设备应具有黑名单管理模块和数据定期更新的能力。

对于需要保存交易记录的终端设备其保存的交易记录应采用保密存储的方式或交易记录带有不可伪造的数字签名,并有交易意外中断恢复机制。

终端设备与计算机系统进行的数据交换必须采用数字加密技术保证信息的安全和不可篡改与伪造或处于可以保证数据传输安全的环境当中。

18.2.3 密钥管理与发卡系统

IC 卡应用系统应包含密钥管理与发卡系统,如该系统外包应检查承包机构的安全资质和是否具备必要的安全管理制度和环境。

密钥管理系统遵循“集中管理、统一配发”的原则,应符合 CJ/T 166—2002《建设事业 IC 卡应用技术》中的规定,完备申请及报批手续。

密钥管理系统必须具备根密钥的备份机制和密钥一旦泄露后的密钥紧急更新机制,密钥产生后的转移、复制、分散等环节一般应通过加密机或智能 IC 卡进行,并能保证密钥的安全。

卡片的订购、生产、传递、交接应有完善的文字记录并保证数量的准确。

上述系统的使用应在能保证安全的环境中进行,一般至少应有 2 人以上在现场操作并做记录或有不能篡改或伪造的操作日志。

上述记录资料至少应保留 3 个月或卡片发行方要求的保管周期。

18.2.4 应用及管理系统

系统中应用的密钥必须保存在加密机或 PSAM 卡中,不得存储在计算机中。

对于智能 IC 卡系统必须采用双向认证措施,以保证只有合法的系统才能操作合法的卡片以及只有合法的 IC 卡才可以得到相应的服务。

对于准备长期使用的非智能 IC 卡系统应有向智能 IC 卡升级必须的接口。

应用系统应有可靠的数据备份机制和系统瘫痪后的恢复机制和应急手段,系统出现故障后应及时恢复或启动应急措施。

对于需要识别持卡人身份的应用应有卡片挂失和黑名单管理功能。

涉及资金交易的系统必须有基于交易记录的资金清算系统,交易记录应能保存 3 个月或管理方要求的保存周期。

如使用支持应用下载功能的 IC 卡(如 Java 卡),应有能保证应用下载过程中的防伪造、防篡改的安全措施。

18.2.5 安全策略

除上述基本要求之外,IC 卡系统的安全策略还应考虑:

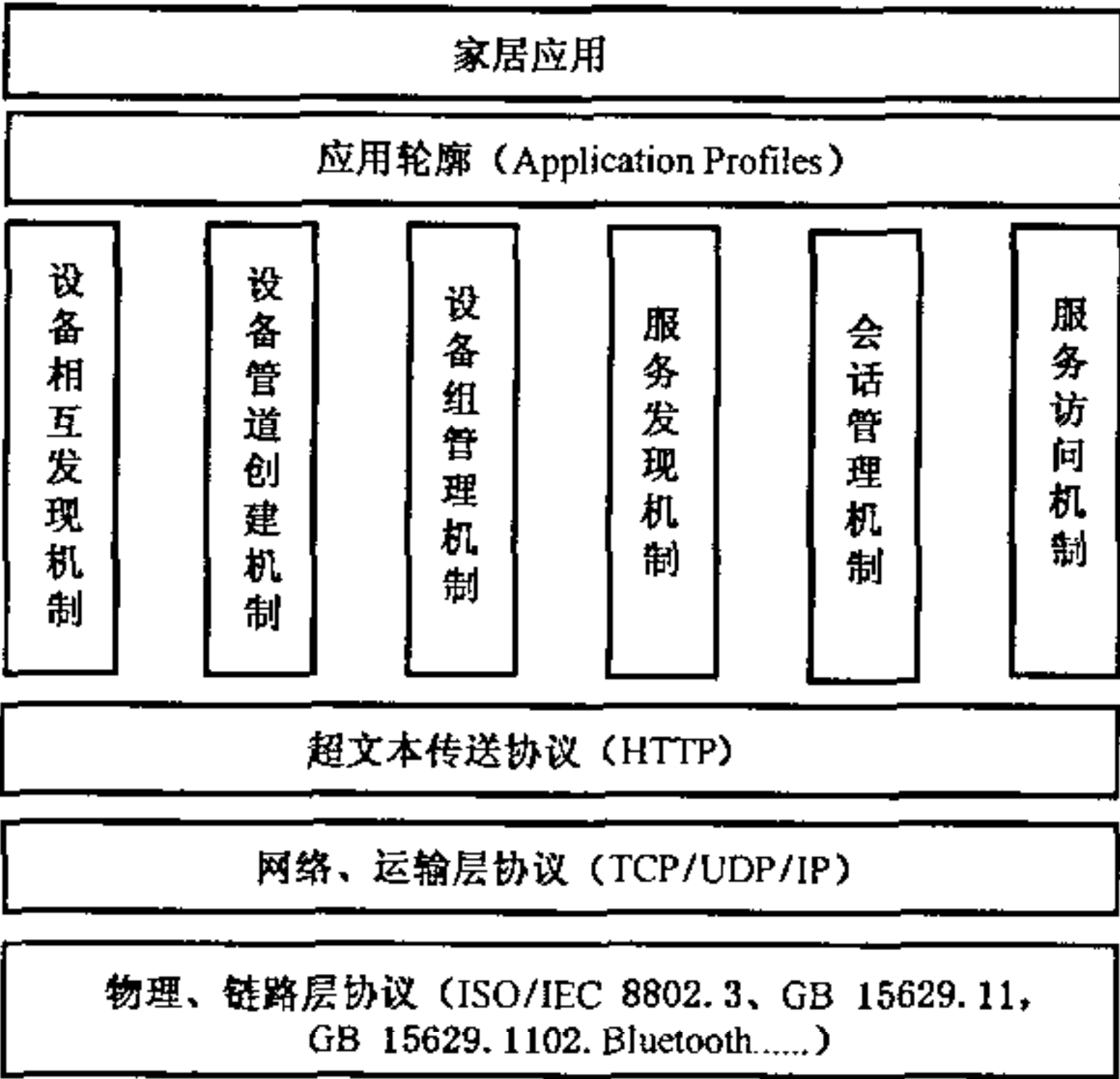
- a) 一般应定期对安全风险进行评估并制订相应的改进措施;
- b) 对于外包的系统或服务提供商应事先进行安全资格审查并定期进行检查;
- c) 系统中使用的密钥算法原则上应符合《商业密码管理条例》的相关规定;
- d) IC 卡内应有检查 IC 卡合法性的密钥以防止伪卡的产生;
- e) IC 卡数据结构应保证只有合法的操作者才可以修改其职权范围内的信息;
- f) 应用数字签名技术应通过随机数、序列变量或时间戳保证数字签名的可检查性,防止重发风险;
- g) 交易系统应有定期数据合法性稽核检查机制;
- h) 对于使用持卡人数字签名代替手工签名的应用应优先考虑使用公开密钥体系 PKI 技术,其私钥应优先考虑在 IC 卡内部产生、存储和使用,并保证不能以任何措施导出 IC 卡;或密钥对的产生、更新过程在一个 CA 系统的安全控制之下;
- i) 有一定安全要求的系统,PIN 和其他数据的传递应采用加密方式;
- j) 安全要求较高的持卡人身份识别建议采用指纹等生物特征识别技术,并优先选择在 IC 卡内完成识别。

附录 A
(资料性附录)

家用电子系统应用层功能实现要求

A.1 《信息设备资源共享协同服务》标准概述

《信息设备资源共享协同服务》系列电子行业标准(下文简称 IGRS)的目标是在企业、公共场所、个人以及家庭所涉及的信息设备互连时,通过遵循共同资源描述及功能服务接口标准,使设备能够有效实现资源开放及服务协同,提高设备间功能的互操作性,为用户提供全新应用体验。IGRS 系列标准由 6 部分构成:基础协议、应用框架、基础应用、设备测试验证规范、设备类型规范、服务类型规范。其中第 1 部分 SJ/T 11310—2005、第 4 部分 SJ/T 11311—2005 已经发布。其框架结构图如下所示:



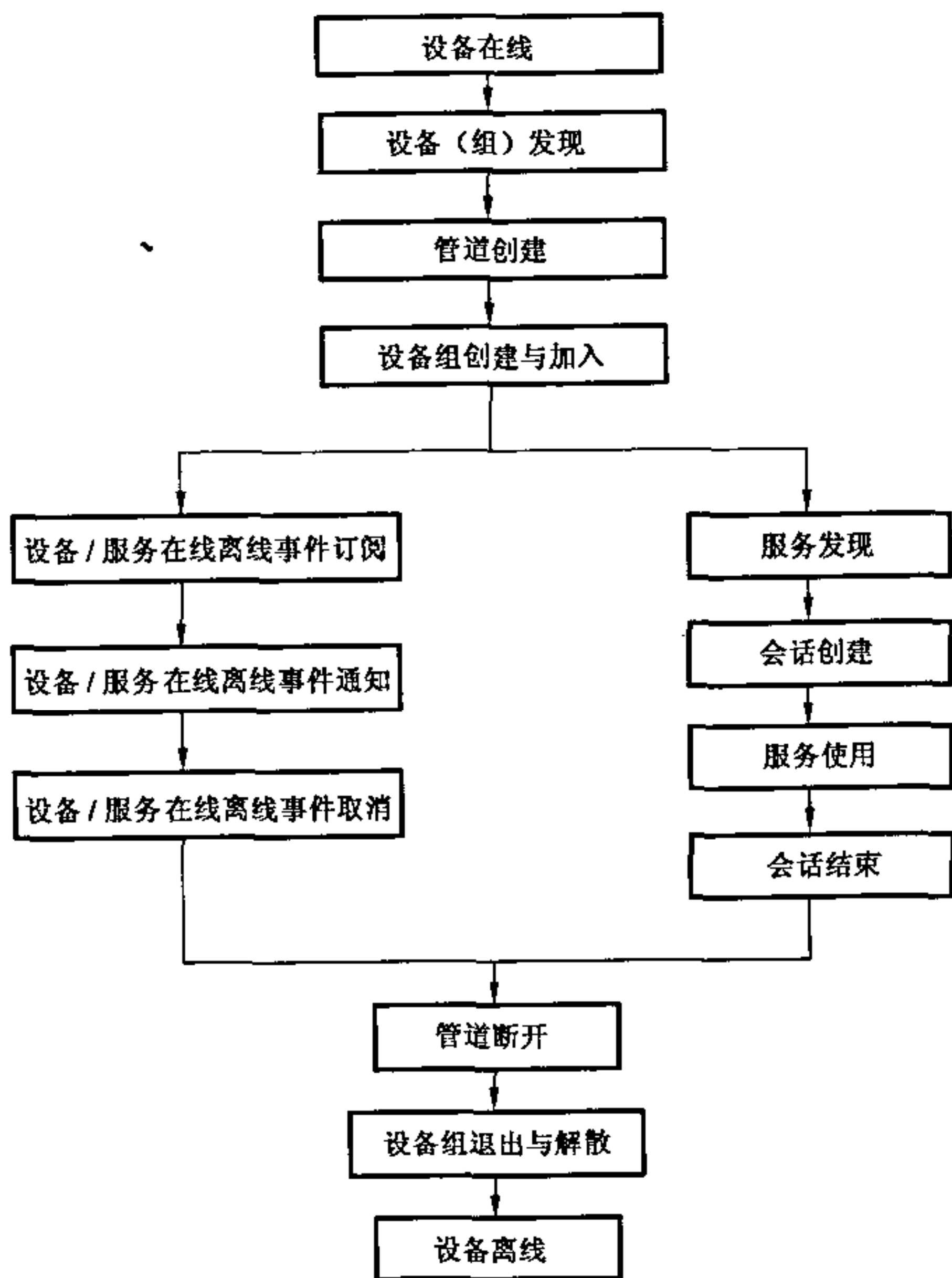
上图中,设备相互发现机制定义家电设备在网络上宣告自身及发现其他设备信息的机制,设备管道创建机制定义相互发现的两个家电设备间建立可靠的交互机制,设备组管理机制定义多个家电设备形成特定的设备群组的规则,服务发现机制定义客户发现服务的机制,会话管理机制定义客户访问服务时的会话创建和维护机制,服务访问机制定义客户调用服务的交互规则。应用轮廓是基于基础协议、面向最终应用而定义的一系列应用交互规则,如面向家庭多媒体应用的音频/视频应用框架定义家庭场景中各种音频/视频相关设备为实现音频/视频应用所应具备的服务与客户间的配合关系。

IGRS 标准本身是一个应用层的标准,支持各种底层的连接介质,因此适合于家用电子系统的应用和实施。家用电子系统通过实现 IGRS 标准可以简化各设备之间连接配置的复杂性,同时可以在各个设备之间共享彼此的资源,为用户提供更多更新的应用体验。

下面给出了 IGRS 基础协议所定义的 IGRS 设备交互过程的主要步骤说明,IGRS 基础协议的细节及 IGRS 其余部分的细节参见《信息技术 信息设备 资源共享及协同服务》系列标准文档。

A.2 IGRS 设备交互过程

IGRS 设备交互过程如下图所示:



A. 2. 1 设备在线

IGRS 设备在正常工作期间,应以一定的时间间隔向所连接的各个网络中按指定的组播地址发送设备在线宣告信息。设备在线宣告信息中应包含设备名称、设备类型、设备安全属性需求、设备详细信息获取地址等设备信息。

A. 2. 2 设备(组)发现

IGRS 设备可通过在指定的组播地址上监听设备在线宣告信息以发现网络上存在的 IGRS 设备(组)。

IGRS 设备可向所连接的各个网络中按指定的组播地址发送设备(组)查找请求,收到请求的符合查找条件的 IGRS 设备(组)应向发起查找请求的 IGRS 设备返回设备查找响应。

A. 2. 3 设备管道创建

IGRS 设备之间除了基于 UDP 的组播查找与单播响应这一交互过程无需事先建立设备间的连接关系外,其余设备间的各种交互均应建立在设备管道基础上。

IGRS 设备发现网络中的目标 IGRS 设备后,可通过 IGRS 标准中的设备管道机制与目标 IGRS 设备建立可靠的设备管道。

IGRS 标准通过设备管道机制封装并简化了 IGRS 应用交互过程中 TCP 连接的创建和管理过程。任意两个 IGRS 设备在同一时刻只存在一条设备管道。

IGRS 设备可通过设置允许接入的 IGRS 设备列表以及最大的管道并发数目来控制其他 IGRS 设备的管道创建请求。

设备管道分两种:

- a) 安全设备管道:两设备间有共同支持的安全机制,并基于该机制进行了相应的鉴别交互而建立的设备间管道称为安全设备管道;

- b) 非安全设备管道:两设备间无共同支持的安全机制,没有经过相应的鉴别交互建立的设备间管道称为非安全设备管道。

IGRS 设备应在设备在线宣告消息中包含本设备在设备管道创建过程中所使用的安全机制和相关参数。IGRS 设备可通过解析目标 IGRS 设备的在线宣告消息从而选取合适的安全机制与目标 IGRS 设备建立安全设备管道。

IGRS 设备间管道机制包括设备管道创建、设备管道维持机制。两个 IGRS 设备通过安全设备管道创建过程形成相互的信任关系。

两个 IGRS 设备之间创建设备管道后,可通过设备在线状态检测请求与响应消息进行交互检测对方的在线状况。

A.2.4 设备组创建与加入

IGRS 设备在线后默认处于一个全局对等设备组中,所有的 IGRS 设备属于全局对等设备组。

IGRS 设备可通过设备配置来创建或加入对等设备组。同一个对等设备组的各 IGRS 设备间的交互规则应通过 IGRS 标准外的安全通道协商确定。

IGRS 设备发现网络中存在的主从设备组后,可向该主从设备组的主设备发起加入设备组请求。主设备可通过配置规则决定是否对请求加入的设备进行身份鉴别,同时可以配置允许加入的设备列表和设备组内最多设备数目以控制其他设备的加入。

用户可以创建主从设备组,指定某个 IGRS 设备为该主从设备组的主设备。主设备负责以一定的间隔在网络上发送主从设备组宣告消息。

IGRS 设备可以创建和/或加入特定对等设备组和主从设备组,但并不必需创建和/或加入特定对等设备组和主从设备组。

IGRS 设备可以同时创建和/或加入多个特定设备组和主从设备组。

A.2.5 服务发现

IGRS 客户可通过在指定的组播地址上监听服务在线宣告信息来发现网络上存在的 IGRS 服务。

IGRS 客户也可向目标 IGRS 设备发送获取设备详细描述文档请求以获取设备详细描述文档。设备详细描述文档中包含该设备上的服务列表,服务列表中记录了各服务的名称、类型及指向服务描述文档的 URL 地址。

IGRS 客户也可按指定的组播地址向网络中的所有 IGRS 设备发送服务查找请求,在服务查找请求中可包含待查找的服务类型、名称、其他属性等。收到服务查找请求且拥有符合查找条件的服务的 IGRS 设备应向发起服务查找的 IGRS 客户返回服务查找响应。

IGRS 客户也可通过设备间管道向指定的 IGRS 设备发送服务查找请求,收到服务查找请求的 IGRS 设备应根据请求中的查找条件返回相应的查找结果。

处于主从设备组中的 IGRS 设备上的 IGRS 客户也可通过设备管道向指定的 IGRS 设备发送服务在线离线事件订阅请求,在订阅请求中描述订阅条件。当收到服务在线离线事件订阅请求的 IGRS 设备上出现符合订阅请求条件的服务时,IGRS 设备应通过事件通知消息通知发起订阅请求的客户。

A.2.6 会话建立

IGRS 客户通过服务发现机制发现目标 IGRS 设备上的服务后,可在设备管道基础上通过会话机制建立后续服务访问的支撑环境。

IGRS 服务可从 IGRS 客户所在设备和该服务所在设备的设备间关系以及该服务允许访问的用户列表两个维度实现服务访问控制。IGRS 服务可设置最大的并发访问数量。

IGRS 设备间的关系包括设备是否处于同一个设备组内,IGRS 客户所在设备是否为 IGRS 服务所在设备的可信设备,IGRS 客户所在设备是否为 IGRS 服务所在设备的指定可信设备。

IGRS 服务所在设备在会话建立过程中获取 IGRS 客户所在设备信息、相应的用户身份及用户鉴别信息。根据上述获取的信息检查 IGRS 客户的访问权限,同时根据 IGRS 服务的并发支持能力实现并发控制。在同一时刻 IGRS 客户与 IGRS 服务之间只能存在一个会话。会话建立成功后,IGRS 客户可对 IGRS 服务进行调用、数据查询和数据获取等操作。

A.2.7 服务调用

IGRS 客户与 IGRS 服务建立会话后,应根据 IGRS 服务在服务描述文档中描述的各种接口,通过规定的服务调用机制实现对 IGRS 服务的使用。

IGRS 服务支持的标准接口包括服务数据查询接口、服务数据变化事件订阅接口和服务数据通知接口等。

A.2.8 会话结束

当 IGRS 客户结束对 IGRS 服务的使用后,IGRS 客户可拆除与 IGRS 服务之间的会话,反之,IGRS 服务也可以主动拆除与 IGRS 客户之间的会话。

A.2.9 设备/服务在线离线事件订阅

两个 IGRS 设备建立设备管道后,任何一个 IGRS 设备上的 IGRS 客户可向对方发起事件订阅请求以订阅设备/服务在线离线事件。收到订阅请求的 IGRS 设备可决定是否接受订阅并将结果通过事件订阅响应消息返回给 IGRS 客户所在的 IGRS 设备。

IGRS 客户可向目标 IGRS 设备发起事件订阅请求,订阅目标设备上的服务在线离线事件。

IGRS 客户可向主从设备组中的主设备发起事件订阅请求,订阅设备组范围内的设备在线离线事件和服务在线离线事件。

事件订阅的有效时间由接受事件订阅的 IGRS 设备决定并在订阅响应消息中通知发起订阅的 IGRS 客户。IGRS 客户可在有效期内发起续订请求以延长本次事件订阅的有效期。

A.2.10 设备/服务在线离线事件通知

收到 IGRS 客户的事件订阅请求的 IGRS 设备在检测到有符合订阅条件的设备/服务在线离线事件发生时,应通过设备管道向 IGRS 客户发送通知消息,在通知消息中描述事件内容。

A.2.11 设备/服务在线离线事件取消订阅

IGRS 客户成功地向目标 IGRS 设备进行设备/服务在线离线事件订阅后,可在事件订阅的有效期内通过设备管道向目标 IGRS 设备发送取消订阅请求以结束本次事件订阅。

在事件订阅有效期结束后,IGRS 设备应使得事件订阅纪录无效。

A.2.12 设备管道断开

两个 IGRS 设备间的设备管道创建成功后,在下列情况下管道断开:

- a) 一方设备离线:设备管道建立后,任何一端 IGRS 设备检测到另一端 IGRS 设备离线后,应立即使得两个设备间的管道断开;
- b) 管道空闲超时:设备安全管道建立后,如果基于该管道没有会话存在,且如果在一定的时间内两个 IGRS 设备间没有发生除设备在线状态检测消息外的设备交互,则任何一端 IGRS 设备应使得该管道断开;
- c) 一方设备主动拆除管道:设备管道建立后,任何一端设备在离开网络前、断电前或由于设备管理等方面的因素可发送管道拆除通知消息给管道的另一端设备。收到该消息的设备应立即使管道断开。

当设备管道断开后,如有基于原安全设备管道发送的消息,应与发出消息的设备进行新的安全设备管道创建过程。对于安全设备管道,上述的 3 个设备管道断开条件均为应实现内容;对于非安全设备管道而言,b)为可选条件,a)和 c)为应实现内容。

A.2.13 设备组解散与退出

同一对等设备组内的所有 IGRS 设备都退出该设备组后,该对等设备组解散。

主从设备组内的主设备可根据管理的需要解散该设备组。主设备解散主从设备组时应向网络中组播宣告设备组离线消息。如果主从设备组内的 IGRS 从设备收到设备组离线通知消息或通过设备在线检测机制判断主设备已经离线,则表明该主从设备组已解散,从设备从该主从设备组退出。

在下列情况下设备组内的 IGRS 从设备将主动退出设备组:

- a) 设备离线:如果 IGRS 设备由于网络连接断开、设备断电或设备管理等方面的因素不再定期向网络中发送设备在线宣告消息,则认为该设备离线。设备离线意味着该设备已经从其加入的所有设备组中退出;
- b) 主动退出:主从设备组内的 IGRS 设备可通过设备管道向设备组中的主设备发送退出设备组请求主动退出设备组;对等设备组内的 IGRS 设备可通过更改其所在设备组的信息主动退出设备组。

A.2.14 设备离线

设备在发出设备离线宣告或者其在线宣告的有效周期结束前未能再次发送设备宣告消息,则认为该设备离线。

设备在线宣告基于组播机制。由于组播机制的不可靠特性,可引入设备在线状态检测机制来可靠检测设备是否在线。两个 IGRS 设备之间建立设备管道后,任何一端 IGRS 设备可通过设备管道发送设备在线状态检测消息检测另一端的 IGRS 设备是否在线。收到在线状态检测消息的 IGRS 设备应向发起检测消息的 IGRS 设备返回设备在线状态检测响应消息。如果发起检测消息的 IGRS 设备在一定时间内没有收到被检测设备的响应消息,则认为被检测设备已经离线。

主从设备组内的 IGRS 设备如果收到主设备发来的包含某个设备的离线事件通知,则认为该设备已经离线。

