第 5 章　信息化和信息系统

5.1　信息系统与信息化

5.1.1　信息系统与信息化——考点梳理

1．信息的基本概念

信息论已发展成为一个内涵非常丰富的学科，与控制论和系统论并称为现代科学的“三论”。

香农指出，信息就是能够用来消除不确定性的东西。

1）信息的特征

（1）客观性。

（2）普遍性。

（3）无限性。

（4）动态性，并随时间变化。

（5）相对性。

（6）依附性。

（7）变换性。通过处理被变换（内容和形式变化）。

（8）传递性。

（9）层次性。

（10）系统性。

（11）转化性。有效的使用信息，可以将信息转化为物质或能量。

2）信息的质量属性

（1）精确性，对事物状态描述的精准程度。

（2）完整性，对事物状态描述的全面程度，完整信息应包括所有重要事实。

（3）可靠性，指信息的来源、采集方法，传输过程是可以信任的，符合预期。

（4）及时性，指获得信息的时刻与事件发生时刻的间隔长短。

（5）经济性，指信息获取、传输带来的成本在可以接受的范围之内。

（6）可验证性，指信息的主要质量属性可以被证实或者证伪的程度。

（7）安全性，指在信息的生命周期中，信息可以被非授权访问的可能性。

3）信息的功能

（1）为认识世界提供依据。

（2）为改造世界提供指导。

（3）为有序的建立提供保证。

（4）为资源开发提供条件。

（5）为知识生产提供材料。

信息的传输模型如图 5-1 所示。

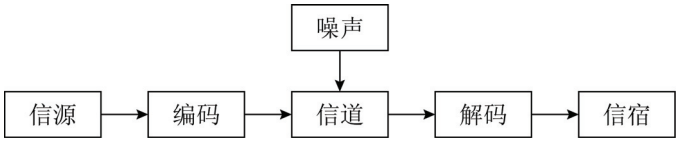

图 5-1　信息传输模型

2．信息系统的基本概念

系统是由相互联系、相互依赖、相互作用的事物或过程组成的具有整体功能和综合行为的统一体。

系统的特性如下：

（1）目的性。

（2）整体性。

（3）层次性。

（4）稳定性。

（5）突变性。

（6）自组织性。

（7）相似性。

（8）相关性。

（9）环境适应性。

对于信息系统而言，以下特性会表现得比较突出：

（1）开放性。系统的开放性是指系统的可访问性，这个特性决定了系统可以被外部环境识别以及外部环境或者其他系统可以按照预定的方法来使用系统的能力。

（2）脆弱性。这个特性与系统的稳定性相对应，即系统可能存在着丧失结构、功能、秩序的特性，这个特性往往容易隐藏，并不易被外界感知。脆弱性差的系统一旦被侵入，整体性就会被破坏，甚至面临系统崩溃、瓦解。

（3）健壮性。系统具有的能够抵御出现非预期状态的特性称为健壮性，也称鲁棒性。要求具有高可用性的信息系统，会采取冗余技术、容错技术、身份识别技术、可靠性技术等来抵御系统出现非预期的状态，保持系统的稳定性。

简单地说信息系统就是输入数据，通过加工处理产生信息的系统。

面向管理和支持生产是信息系统的显著特点，以计算机为基础的信息系统可以定义为：结合管理理论和方法，应用信息技术解决管理问题，提高生产效率，为生产或信息化过程以及管理和决策提供支撑的系统。

管理模型、信息处理模型和系统实现条件三者的相互结合产生信息系统抽象模型，如图 5-2 所示。

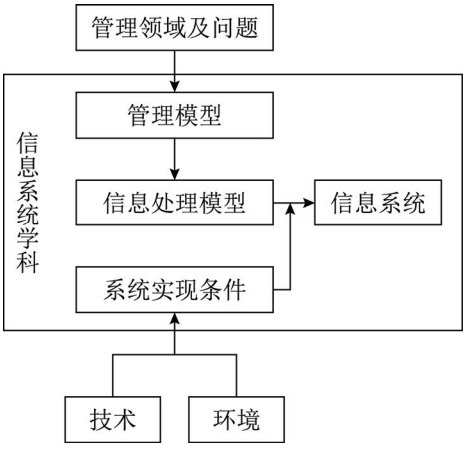

图 5-2　信息系统抽象模型

采用现代管理理论（例如软件工程、项目管理等）作为计划、设计、控制的方法将硬件、软件、数据库、网络等部件按照规划的结构和秩序有机地整合到一个有清晰边界的信息系统中，以达到既定系统的目标，这个过程就称为信息系统集成。

3．信息化的基本概念

信息化从“小”到“大”分为以下五个层次：

（1）产品信息化。

（2）企业信息化。

（3）产业信息化。

（4）国民经济信息化。

（5）社会生活信息化。

信息化的基本内涵启示我们：信息化的

- 主体是全体社会成员，包括政府、企业、事业、团体和个人。
- 时域是一个长期的过程。
- 空域是政治、经济、文化、军事和社会的一切领域。
- 手段是基于现代信息技术的先进社会生产工具。
- 途径是创建信息时代的社会生产力，推动社会生产关系及社会上层建筑的改革。

- 目标是让国家的综合实力、社会的文明素质和人民的生活质量得到全面提升。

国家信息化体系六要素如图 5-3 所示。

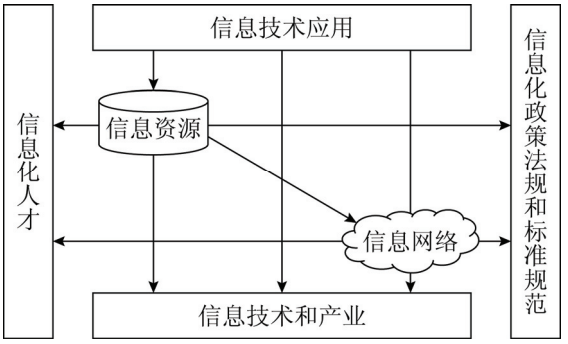

图 5-3　国家信息化体系六要素关系图

（1）信息资源。

信息资源的开发和利用是国家信息化的核心任务，是国家信息化建设取得实效的关键。

（2）信息网络。

信息网络是信息资源开发和利用的基础设施，包括电信网、广播电视网和计算机网络。

（3）信息技术应用。

信息技术应用是信息化体系六要素中的龙头，是国家信息化建设的主阵地。

（4）信息技术和产业。

信息产业是信息化的物质基础。

（5）信息化人才。

人才是信息化的成功之本。

（6）信息化政策法规和标准规范。

其是国家信息化快速、有序、健康和持续发展的保障。

4．信息系统生命周期

软件的生命周期通常包括：可行性分析与项目开发计划、需求分析、概要设计、详细设计、编码、测试、维护等阶段。

信息系统的生命周期可以简化为系统规划（可行性分析与项目开发计划）、系统分析（需求分析）、系统设计（概要设计、详细设计）、系统实施（编码、测试）、运行维护等阶段。

为便于论述针对信息系统项的项目管理，信息系统的生命周期还可以简化为立项（系统规划）、开发（系统分析、系统设计、系统实施）、运维及消亡四个阶段，在开发阶

段不仅包括系统分析、系统设计、系统实施，还包括系统验收等工作。如果从项目管理的角度来看，项目的生命周期又划分为启动、计划、执行和收尾四个典型的阶段。

五阶段的信息系统生命周期，如图 5-4 所示。

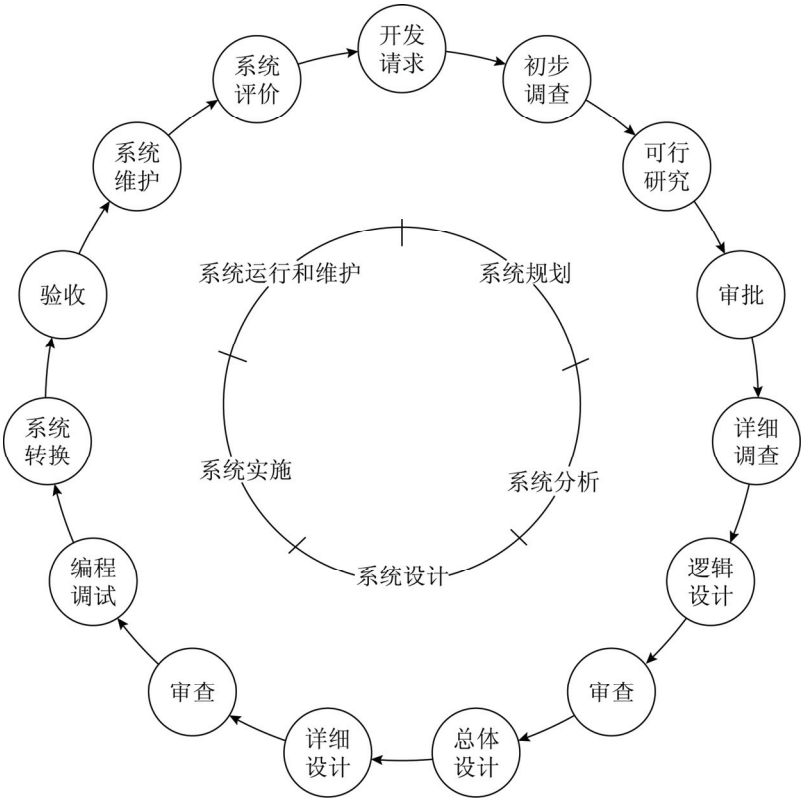

图 5-4 信息系统的生命周期

1）系统规划阶段

系统规划阶段的任务是对组织的环境、目标及现行系统的状况进行初步调查，根据组织目标和发展战略，确定信息系统的发展战略，对建设新系统的需求做出分析和预测，同时考虑建设新系统所受的各种约束，研究建设新系统的必要性和可能性。根据需要与可能，给出拟建系统的备选方案。对这些方案进行可行性研究，写出可行性研究报告。可行性研究报告审议通过后，将新系统建设方案及实施计划编写成系统设计任务书。

2）系统分析阶段

系统分析阶段的任务是根据系统设计任务书所确定的范围，对现行系统进行详细调查，描述现行系统的业务流程，指出现行系统的局限性和不足之处，确定新系统的基本目标和逻辑功能要求即提出新系统的逻辑模型。

系统分析阶段又称为逻辑设计阶段，这个阶段是整个系统建设的关键阶段，也是信

息系统建设与一般工程项目的重要区别所在。系统分析阶段的工作成果体现在系统说明书中，这是系统建设的必备文件。它既是给用户看的，又是下一个阶段的工作依据，因此系统说明书既要通俗，又要准确。用户通过系统说明书可以了解未来系统的功能，判断是不是所要求的系统。系统说明书一旦讨论通过，就是系统设计的依据，也是将来验收系统的依据。

3）系统设计阶段

简单地说，系统分析阶段的任务是回答系统“做什么”的问题，而系统设计阶段要回答的问题是“怎么做”。该阶段的任务是根据系统说明书中规定的功能要求，考虑实际条件，具体设计实现逻辑模型的技术方案即设计新系统的物理模型。这个阶段又称为物理设计阶段，可分为总体设计（概要设计）和详细设计两个子阶段。这个阶段的技术文档是系统设计说明书。

4）系统实施阶段

系统实施阶段是将设计的系统付诸实施的阶段，这一阶段的任务包括计算机等设备的购置、安装和调试、程序的编写和调试、人员培训、数据文件转换、系统调试与转换等。这个阶段的特点是几个互相联系、互相制约的任务同时展开，必须精心安排、合理组织。系统实施是按实施计划分阶段完成的，每个阶段应写出实施进展报告。系统测试之后写出系统测试分析报告。

5）系统运行和维护阶段

系统投入运行后，需要经常进行维护和评价，记录系统运行的情况，根据一定的规则对系统进行必要的修改，评价系统的工作质量、评估经济效益。

5.1.2　信息系统与信息化——历年真题

1．信息要满足一定的质量属性，其中信息的（　　）指信息的来源、采集方法，传输过程是可以信任的，符合预期。

A．完整性　　B．可靠性　　C．可验证性　　D．保密性

2．以下关于信息化的叙述中，不正确的是（　　）。

A．信息化的主体是程序员、工程师、项目经理、质量管控人员

B．信息化的时域是一个长期的过程

C．信息化的手段是基于现代信息技术的先进社会生产工具

D．信息化的目标是使国家的综合实力、社会的文明素质和人民的生活质量全面达到现代化水平

3．信息系统是由计算机硬件、网络通讯设备、计算机软件，以及（　　）组成的人机一体化系统。

A．信息资源、信息用户和规章制度　　B．信息资源、规章制度

C．信息用户、规章制度　　D．信息资源、信息用户和场地机房

4．以下关于信息系统生命周期开发阶段的叙述中，（　　）是不正确的。

A．系统分析阶段的目标是为系统设计阶段提供信息系统的逻辑模型

B．系统设计阶段是根据系统分析的结果设计出信息系统的实现方案

C．系统实施阶段是将设计阶段的成果部署在计算机和网络上

D．系统验收阶段是通过试运行，以确定系统是否可以交付给最终客户

5．某信息系统项目采用结构化方法进行开发，按照项目经理的安排，项目成员小张绘制了下图，如图 5-5 所示。此时项目处于（　　）阶段。

A．总体规划　　B．系统分析

C．系统设计　　D．系统实施

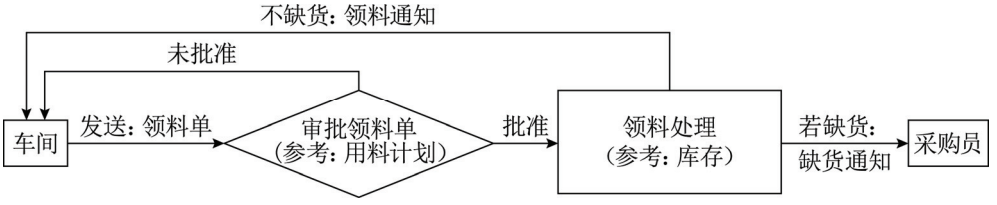

图 5-5　真题配图

参考答案

1	2	3	4	5
B	A	A	C	B

5.2　信息系统开发方法

5.2.1　信息系统开发方法——考点梳理

1．结构化方法

结构是指系统内各个组成要素之间的相互联系、相互作用的框架。结构化方法也称为生命周期法，是一种传统的信息系统开发方法，由结构化分析（Structured Analysis，SA）、结构化设计（Structured Design，SD）和结构化程序设计（Structured Programming，SP）三部分有机组合而成。其精髓是自顶向下、逐步求精和模块化设计。

结构化方法的主要特点：

（1）开发目标清晰化。

（2）开发工作阶段化。

（3）开发文档规范化。

（4）设计方法结构化。

结构化方法的不足和局限性：

（1）开发周期长。

（2）难以适应需求变化。

（3）很少考虑数据结构。

2．面向对象方法

OO（Object-Oriented，面向对像）方法是当前的主流开发方法，拥有很多不同的分支体系，主要包括 OMT（Object Model Technology，对象建模技术）方法、Coad/Yourdon 方法、OOSE（Object-Oriented Software Engineering，面向对象的软件工程）方法和 Booch 方法等。而 OMT、OOSE 和 Booch 已经统一成为 UML（United Model Language，统一建模语言）。

使用 OO 方法构造的系统具有更好的复用性，其关键在于建立一个全面、合理、统一的模型（用例模型与分析模型）。

OO 方法使系统的描述及信息模型的表示与客观实体相对应，符合人们的思维习惯，有利于系统开发过程中用户与开发人员的交流和沟通，缩短开发周期。OO 方法适用于各类信息系统的开发，但是 OO 方法也存在明显的不足，例如必须依靠一定的 OO 技术支持，在大型项目的开发上具有一定的局限性，不能让系统分析以前的开发环节。

一些大型信息系统的开发通常是将结构化方法和 OO 方法结合起来。首先，使用结构化方法进行自顶向下的整体划分；然后，自底向上地采用 OO 方法进行开发。因此，结构化方法和 OO 方法仍是两种在系统开发领域中相互依存的、不可替代的方法。

3．原型化方法

原型化方法也称为快速原型法，或者简称为原型法。从原型是否实现功能来分，可分为水平原型和垂直原型两种。从原型的最终结果来分，可分为抛弃式原型和演化式原型。

原型法的开发过程如图 5-6 所示。

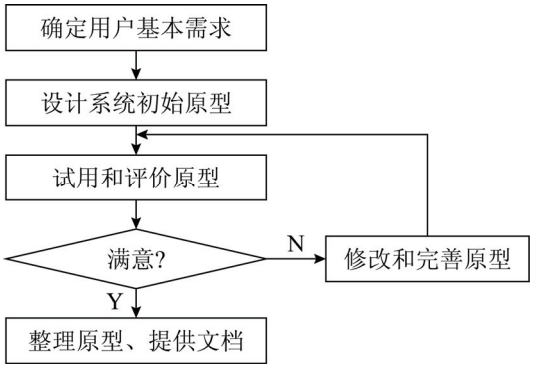

图 5-6　原型法的开发过程

原型法的特点：

- 原型法可以使系统开发的周期缩短、成本和风险降低、速度加快，获得较高的综合开发效益。
- 原型法是以用户为中心来开发系统的，用户参与的程度大大提高，开发的系统符合用户的需求，因而增加了用户的满意度，提高了系统开发的成功率。
- 由于用户参与了系统开发的全过程，对系统的功能和结构容易理解和接受，有利于系统的移交、有利于系统的运行与维护。

原型法的不足之处：

- 开发的环境要求高。
- 管理水平要求高。

4．面向服务的方法

OO 的应用构建在类和对象之上，随后发展起来的建模技术将相关对象按照业务功能进行分组，就形成了构件（Component）的概念。对于跨构件的功能调用，则采用接口的形式暴露出来，进一步将接口的定义与实现进行解耦，催生了服务和面向服务（Service-Oriented，SO）的开发方法。

从应用的角度来看，组织内部、组织之间各种应用系统的互相通信和互操作性直接影响着组织对信息的掌握程度和处理速度。如何使信息系统快速响应需求与环境变化，提高系统可复用性、信息资源共享和系统之间的互操作性，成为影响信息化建设效率的关键问题，而 SO 的思维方式恰好满足了这种需求。

目前，SO 方法是一个较新的领域，许多研究和实践还有待进一步深入。但是，它代表着不拘泥于具体技术实现方式的一种新的系统开发思想，已经成为信息系统建设的大趋势，越来越多的组织开始实施 SO 的信息系统建设。

5.2.2 信息系统开发方法——历年真题

1．常用的信息系统开发方法中，不包括（　　）。

A．结构化方法　　B．关系方法　　C．原型法　　D．面向对象方法

2．许多企业在信息化建设过程中出现了诸多问题，如：信息孤岛多、信息不一致难以整合共享；各应用系统之间、企业上下级之间、企业与上下游伙伴之间业务难以协同，信息系统难以适应快捷的业务变化等。为解决这些问题，企业信息化建设采用（　　）架构已是流行趋势。

A．面向过程　　B．面向对象　　C．面向服务　　D．面向组件

3．面向对象软件开发方法的主要优点包括（　　）。

①符合人类思维习惯

②普遍适用于各类信息系统的开发

③构造的系统复用性好

④适用于任何信息系统开发的生命周期

A．①③④　　B．①②③　　C．②③④　　D．①②④

参考答案

1	2	3
B	C	B

5.3　常规信息系统集成技术

5.3.1　常规信息系统集成技术——考点梳理

系统集成是指将计算机软件、硬件、网络通信等技术和产品集成为能够满足用户特定需求的信息系统，包括总体策划、设计开发、实施、服务及保障。

1．网络标准与网络协议

网络协议是为计算机网络中进行数据交换而建立的规则、标准或约定的集合。网络协议由三个要素组成，分别是语义、语法和时序。

1）OSI 协议

（1）物理层：具体标准有 RS232、V.35、RJ-45、FDDI。

（2）数据链路层：常见的协议有 IEEE 802.3/.2、HDLC、PPP、ATM。

（3）网络层：在 TCP/IP 协议中，网络层具体协议有 IP、ICMP、IGMP、IPX、ARP 等。

（4）传输层：在 TCP/IP 协议中，具体协议有 TCP、UDP、SPX。

（5）会话层：常见的协议有 RPC、SQL、NFS。

（6）表示层：常见的协议有 JPEG、ASCII、GIF、DES、MPEG。

（7）应用层：在 TCP/IP 协议中，常见的协议有 HTTP、Telnet、FTP、SMTP。

2）网络协议和标准

以太网规范 IEEE 802.3 是重要的局域网协议，内容包括：

- IEEE 802.3 标准以太网 10Mb/s 传输介质为细同轴电缆。
- IEEE 802.3u 快速以太网 100Mb/s 双绞线。
- IEEE 802.3z 千兆以太网 1000Mb/s 光纤或双绞线。

广域网协议包括 PPP 点对点协议、ISDN 综合业务数字网、xDSL（DSL 数字用户线路的统称：HDSL、SDSL、MVL、ADSL）、DDN 数字专线、x.25、FR 帧中继、ATM 异步传输模式。

3）TCP/IP

（1）应用层协议。

这些协议主要有 FTP、TFTP、HTTP、SMTP、DHCP、Telnet、DNS 和 SNMP 等。

① FTP（File Transport Protocol，文件传输协议）。

② TFTP（Trivial File Transfer Protocol，简单文件传输协议）。

③ HTTP（Hypertext Transfer Protocol，超文本传输协议）。

④ SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）。

⑤ DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）。

⑥ Telnet（远程登录协议）。

⑦ DNS（Domain Name System，域名系统）。

⑧ SNMP（Simple Network Management Protocol，简单网络管理协议）。

（2）传输层协议。

传输层主要有两个协议：TCP 和 UDP（User Datagram Protocol，用户数据报协议）。

TCP 是整个 TCP/IP 协议族中最重要的协议之一。

UDP 是一种不可靠的、无连接的协议。

（3）网络层协议。

网络层中的协议主要有 IP、ICMP（Internet Control Message Protocol，网际控制报文协议）、IGMP（Internet Group Management Protocol，网际组管理协议）、ARP（Address Resolution Protocol，地址解析协议）和 RARP（Reverse Address Resolution Protocol，反向地址解析协议）等。

2．网络设备

网络互联设备如表 5-1 所列。

表 5-1　网络互联设备

互联设备	工作层次	主要功能
中继器	物理层	对接收信号进行再生和发送，只起到扩展传输距离用，对高层协议是透明的，但使用个数有限（例如，在以太网中只能使用 4 个）
网桥	数据链路层	根据帧物理地址进行网络之间的信息转发，可缓解网络通信繁忙度，提高效率。只能够连接相同 MAC 层的网络
路由器	网络层	通过逻辑地址进行网络信息之间的转发，可完成异构网络之间的互联互通，只能连接使用相同网络层协议的子网
网关	高层（4～7 层）	最复杂的网络互联设备，用于连接网络层以上执行不同协议的子网
集线路	物理层	多端口中继器
二层交换机	数据链路层	是指传统意义上的交换机，多端口网桥
三层交换机	网络层	带路由功能的二层交换机
多层交换机	高层（4～7 层）	带协议转换的交换机

3．网络服务器

网络服务器是指在网络环境下运行相应的应用软件，为网上用户提供共享信息资源和各种服务的高性能计算机（或者计算机集群），英文名称叫作 Server（Cluster）。而集群对客户端而言，逻辑上仍是一台计算机。

4．网络存储技术

主流的网络存储技术主要有三种，分别是直接附加存储（Direct Attached Storage）、网络附加存储（Network Attached Storage）和存储区域网络（Storage Area Network）。

1）直接附加存储 DAS

DAS 是将存储设备通过型计算机系统接口电缆直接连到服务器，其本身是硬件的堆叠，存储操作依赖于服务器，不带有任何存储操作系统。因此，有些文献也将 DAS 称为 SAS（Server Attached Storage，服务器附加存储）。

2）网络附加存储 NAS

采用 NAS 技术的存储设备不再通过 I/O 总线附属于某个特定的服务器，而是通过网络接口与网络直接相连，由用户通过网络访问。

NAS 技术支持多种 TCP/IP 网络协议，主要是 NFS（Net File System，网络文件系统）和 CIFS（Common Internet File System，通用 Internet 文件系统）来进行文件访问，所以 NAS 的性能特点是可以进行小文件级的共享存取。

NAS 存储支持即插即用，可以在网络的任一位置建立存储，基于 Web 管理，使设备的安装、使用和管理更加容易。NAS 可以很经济地解决存储容量不足的问题，但难以获得满意的性能。

3）存储区域网络 SAN

SAN 是通过专用交换机将磁盘阵列与服务器连接起来的高速专用子网。它没有采用文件共享存取方式，而是采用块级别存储。SAN 是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统，其最大特点是将存储设备从传统的以太网中分离了出来，成为独立的存储区域网络。

根据数据传输过程采用的协议，其技术划分为 FC SAN（光纤通道 SAN）、IP SAN（基于 IP 网络的 SAN）和 IB SAN（无限带宽 SAN）技术。

5．网络接入技术

（1）PSTN（Public Switching Telephone Network，公用交换电话网络）。

（2）ISDN（Integrated Services Digital Network，综合业务数字网）。

（3）ADSL（Asymmetrical Digital Subscriber Loop，非对称数字用户线路）。

（4）FTTx+LAN 接入包括：

FTTC（Fiber To The Curb，光纤到路边）；FTTZ（Fiber To The Zone，光纤到小区）；FTTB（Fiber To The Building，光纤到楼）；FTTF（Fiber To The Floor，光纤到楼层）和 FTTH（Fiber To The Home，光纤到户）。

（5）同轴光纤技术（Hybrid Fiber-Coaxial，HFC）。

（6）无线接入

无线网络是指以无线电波作为信息传输媒介，无线网络既包括允许用户建立远距离无线连接的全球语音和数据网络，又包括为近距离无线连接进行优化的红外线技术及射频技术，与有线网络的用途十分类似，最大的不同在于传输媒介的不同。目前最常用的无线网络接入技术主要有 WiFi 和移动互联接入（4G）。

6．网络规划与设计

网络设计工作包括：

（1）网络拓扑结构设计。

（2）主干网络（核心层）设计。

（3）汇聚层和接入层设计。

（4）广域网连接与远程访问设计。

（5）无线网络设计。

（6）网络安全设计。

（7）设备选型。

7．数据库管理系统

常见的数据库管理系统主要有 Oracle、MySQL、SQL Server、MongoDB 等，前三种均为关系数据库，而 MongoDB 是非关系数据库。

8．数据仓库技术

数据仓库是一个面向主题的、集成的、非易失的、随时间变化的数据集合，用于支持管理决策。

大众观点的数据仓库的体系结构如图 5-7 所示。

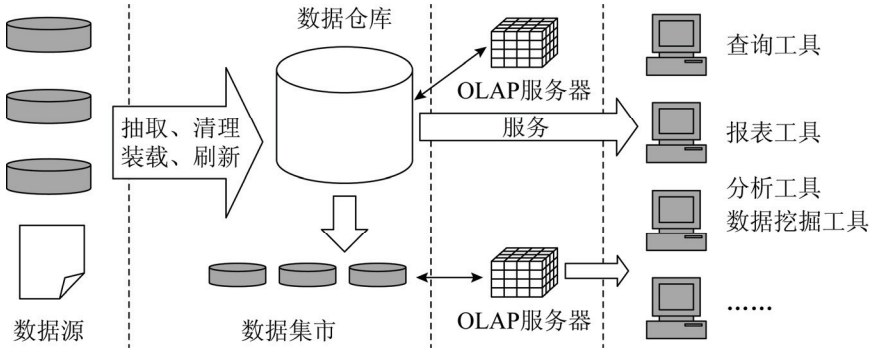

图 5-7　数据仓库体系结构

（1）数据源：是数据仓库系统的基础，是整个系统的数据源泉。通常包括企业内部信息和外部信息。

（2）数据的存储与管理：是整个数据仓库系统的核心。数据仓库的真正关键是数据的存储和管理，针对现有各业务系统的数据进行抽取、清理，并有效集成，按照主题进行组织。数据仓库按照数据的覆盖范围可以分为企业级数据仓库和部门级数据仓库（通常称为数据集市）。

（3）OLAP 服务器：对分析需要的数据进行有效集成，按多维模型予以组织，以便进行多角度、多层次的分析并发现趋势。其具体实现可以分为：ROLAP、MOLAP 和 HOLAP。

（4）前端工具：主要包括各种查询工具、报表工具、分析工具、数据挖掘工具以及各种基于数据仓库或数据集市的应用开发工具。其中数据分析工具主要针对 OLAP 服务器，报表工具、数据挖掘工具主要针对数据仓库。

9．中间件技术

目前还没有对中间件形成一个统一的定义，下面是两种现在普遍比较认可的定义：

（1）在一个分布式系统环境中处于操作系统和应用程序之间的软件。

（2）中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源，中间件位于客户机服务器的操作系统之上，管理计算资源和网络通信。

中间件作为一大类系统软件，与操作系统、数据库管理系统并称“三套车”。

它的优越性体现在以下几个方面：缩短应用的开发周期、节约应用的开发成本、减少系统初期的建设成本、降低应用开发的失败率、保护已有的投资、简化应用集成、减少维护费用、提高应用的开发质量、保证技术进步的连续性、增强应用的生命力。

由底向上从中间件的层次上来划分，可分为底层型中间件、通用型中间件和集成型中间件三个大的层次。

（1）底层型中间件的主流技术有 JVM（Java 虚拟机）、CLR（公共语言运行库）、ACE（自适配通信环境）、JDBC（Java 数据库连接）和 ODBC（开放数据库互连）等，代表产品主要有 SUN JVM 和 Microsoft CLR 等。

（2）通用型中间件的主流技术有 CORBA（公共对象请求代理体系结构）、J2EE、MOM（面向消息的中间件）和 COM 等，代表产品主要有 IONA Orbix、BEA Web Logic 和 IBM MQSeries 等。

（3）集成型中间件的主流技术有 Workflow 和 EAI（企业应用集成）等，代表产品主要有 BEA Web Logic 和 IBM Web Sphere 等。

10．高可用性和高可靠性的规划与设计

计算机系统的可用性用平均无故障时间（MTTF）来度量，即计算机系统平均能够正常运行多长时间才发生一次故障。系统的可用性越高，平均无故障时间越长。可维护性用平均维修时间（MTTR）来度量，即系统发生故障后维修和重新恢复正常运行平均花费的时间。计算机系统的可用性定义为：MTTF/(MTTF+MTTR)×100%。

5.3.2 常规信息系统集成技术——历年真题

1.（　　）是与 IP 协议同层的协议，可用于互联网上的路由器报告差错或提供有关意外情况的信息。

A．IGMP　　B．ICMP　　C．RARP　　D．ARP

2．虽然不同的操作系统可能装有不同的浏览器。但是这些浏览器都符合（　　）协议。

A．SMP　　B．HTTP　　C．HTML　　D．SMTP

3．在计算机网络设计中，主要采用分层分级设计模型。其中（　　）的主要目的是完成网络访问策略控制、数据包处理、过滤、寻址，以及其他数据处理的任务。

A．接入层　　B．汇聚层　　C．主干层　　D．核心层

4．以下关于网络规划、设计与实施工作的叙述中，不正确的是（　　）。

A．在设计网络拓扑结构时，应考虑的主要因素有地理环境、传输介质与距离以及可靠性

B．在设计主干网时，连接建筑群的主干网一般考虑以光缆作为传输介质

C．在设计广域网连接方式时，如果网络用户有 www、E-mail 等具有 Internet 功能的服务器，一般采用专线连接或永久虚电路连接外网

D．无线网络不能应用于城市范围的网络接入

5．（　　）是一种软件技术，在数据仓库中有广泛的应用，通过访问大量的数据实现数据处理分析要求，实现方式是从数据仓库中抽取详细数据的一个子集，并经过必要的聚集存储到该服务器中供前端分析工具读取。

A．联机分析处理（OLAP）　　B．联机事务处理（OLTP）

C．数据采集工具（ETL）　　D．商业智能分析（BI）

6．一般而言，大型软件系统中实现数据压缩功能的模块，工作在 OSI 参考模型的是（　　）。

A．应用层　　B．表示层　　C．会话层　　D．网络层

7．在 1 号楼办公的小李希望在本地计算机上通过远程登录的方式访问放置在 2 号楼的服务器，为此将会使用到 TCP/IP 协议族中的（　　）协议。

A．Telnet　　B．FTP　　C．HTTP　　D．SMTP

参考答案

1	2	3	4	5	6	7
B	B	B	D	A	B	A

5.4　软件工程

5.4.1　软件工程——考点梳理

软件工程由方法、工具和过程三个部分组成。

1．需求分析

软件需求是指用户对新系统在功能、行为、性能、设计约束等方面的期望。根据 IEEE 的软件工程标准词汇表，软件需求是指用户解决问题或达到目标所需的条件或能力，是系统或系统部件要满足合同、标准、规范或其他正式规定文档所需具有的条件或能力，以及反映这些条件或能力的文档说明。

1）需求的层次

（1）业务需求。

业务需求是指反映企业或客户对系统高层次的目标要求，通常来自项目投资人、购买产品的客户、客户单位的管理人员、市场营销部门或产品策划部门等。通过业务需求可以确定项目视图和范围，项目视图和范围文档把业务需求集中在一个简单、紧凑的文档中，该文档为以后的开发工作奠定了基础。

（2）用户需求。

用户需求描述的是用户的具体目标，或用户要求系统必须能完成的任务。也就是说，用户需求描述了用户能使用系统来做些什么，通常采取用户访谈和问卷调查等方式对用户使用的场景进行整理，从而建立用户需求。

（3）系统需求。

系统需求是从系统的角度来说明软件的需求，包括功能需求、非功能需求和设计约束等。功能需求也称为行为需求，它规定了开发人员必须在系统中实现的软件功能，用户利用这些功能来完成任务，满足业务需要。功能需求通常是通过系统特性的描述表现出来的，所谓特性是指一组逻辑上相关的功能需求，表示系统为用户提供某项功能（服务），使用户的业务目标得以满足；非功能需求是指系统必须具备的属性或品质，又可细分为软件质量属性（例如，可维护性、可维护性、效率等）和其他非功能需求。设计约束也称为限制条件或补充规约，通常是对系统的一些约束说明，例如，必须采用国有自主知识产权的数据库系统，必须运行在 UNIX 操作系统之下等。

2）质量功能部署

质量功能部署（Quality Function Deployment，QFD）是一种将用户要求转化成软件需求的技术。其目的是最大限度地提升软件工程过程中用户的满意度，为了达到这个目标，QFD 将软件需求分为三类，分别是常规需求、期望需求和意外需求。

3）需求获取

常见的需求获取方法包括用户访谈、问卷调查、采样、情节串联板、联合需求计划等。

4）需求分析

一个好的需求应该具有无二义性、完整性、一致性、可测试性、确定性、可跟踪性、正确性、必要性等特性。因此，需要分析人员把杂乱无章的用户要求和期望转化为用户需求，这就是需求分析的工作。

在实际工作中，一般使用实体联系图（E-R 图）表示数据模型，用数据流图（Data Flow Diagram，DFD）表示功能模型，用状态转换图（State Transform Diagram，STD）表示行为模型。

5）软件需求规格说明书

软件需求规格说明书（Software Requirement Specification，SRS）是需求开发活动的产物，编制该文档的目的是使项目干系人与开发团队对系统的初始规定有一个共同的理解，使之成为整个开发工作的基础。SRS 是软件开发过程中最重要的文档之一，对于任何规模和性质的软件项目都不应该缺少。

在国家标准 GB/T 8567—2006 中，提供了一个 SRS 的文档模板和编写指南，其中规定 SRS 应该包括以下内容：①范围。②引用文件。③需求。④合格性规定。⑤需求可追踪性。⑥尚未解决的问题。⑦注解。⑧附录。

6）需求验证

需求验证也称为需求确认，其活动是为了确定以下几个方面的内容：

（1）SRS 正确地描述了预期的、满足项目干系人需求的系统行为和特征。

（2）SRS 中的软件需求是从系统需求、业务规格和其他来源中正确推导而来的。

（3）需求是完整和高质量的。

（4）需求的表示在所有地方都是一致的。

（5）需求为继续进行系统设计、实现和测试提供了足够的基础。

在实际工作中，一般通过需求评审和需求测试工作来对需求进行验证。需求评审就是对 SRS 进行技术评审，SRS 的评审是一项精益求精的技术，它可以发现那些二义性的或不确定性的需求，为项目干系人提供在需求问题上达成共识的方法。需求的遗漏和错误具有很强的隐蔽性，仅仅通过阅读 SRS，很难完成在特定环境下的系统行为，只有在业务需求基本明确、用户需求部分确定时，同步进行需求测试才可能及早发现问题，从而在需求开发阶段以较低的代价解决这些问题。

7）UML

UML 是一种定义良好、易于表达、功能强大且普遍适用的建模语言。

从总体上来看，UML 的结构包括构造块、规则和公共机制三个部分。

（1）UML 中的事物。

- 结构事物：结构事物在模型中属于最静态的部分，代表概念上或物理上的元素。

- 行为事物：行为事物是 UML 模型中的动态部分，代表时间和空间上的动作。
- 分组事物：分组事物是 UML 模型中组织的部分。
- 注释事物：注释事物是 UML 模型的解释部分。

（2）UML 中的关系。

UML 用关系把事物结合在一起，主要有下列四种关系：

- 依赖（dependency）：依赖是两个事物之间的语义关系，其中一个事物发生变化会影响另一个事物的语义。
- 关联（association）：关联描述一组对象之间连接的结构关系。
- 泛化（generalization）：泛化是一般化和特殊化的关系，描述特殊元素的对象可替换一般元素的对象。
- 实现（realization）：实现是类之间的语义关系，其中的一个类指定了由另一个类保证执行的契约。

（3）UML 视图。

UML 对系统架构的定义是系统的组织结构，包括系统分解的组成部分，以及它们的关联性、交互机制和指导原则等提供系统设计的信息。具体来说，就是指以下 5 个系统视图：

- 逻辑视图：逻辑视图也称为设计视图，它表示了设计模型中在架构方面具有重要意义的部分，即类、子系统、包和用例实现的子集。
- 进程视图：进程视图是可执行线程和进程作为活动类的建模，它是逻辑视图的一次执行实例，描述了并发与同步结构。
- 实现视图：实现视图对组成基于系统的物理代码的文件和构件进行建模。
- 部署视图：部署视图把构件部署到一组物理节点上，表示软件到硬件的映射和分布结构。
- 用例视图：用例视图是最基本的需求分析模型。

8）面向对象分析

类之间的主要关系有关联、依赖、泛化、聚合、组合和实现等，它们在 UML 中的表示方式如图 5-8 所示。

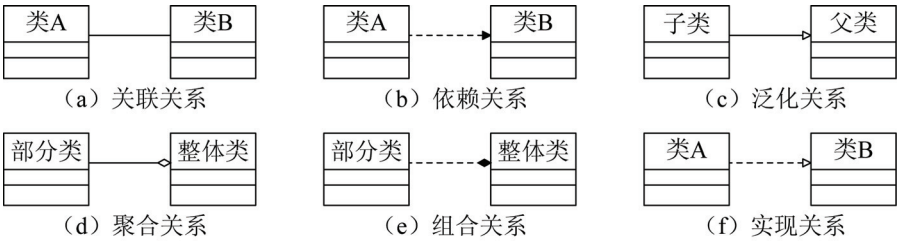

图 5-8　类之间的关系表示

（1）关联关系。关联提供了不同类的对象之间的结构关系，它在一段时间内将多个类的实例连接在一起。关联体现的是对象实例之间的关系，而不表示两个类之间的关系。

（2）依赖关系。两个类 A 和 B，如果 B 的变化可能会引起 A 的变化，则称类 A 依赖于类 B。

（3）泛化关系。泛化关系描述了一般事物与该事物中的特殊种类之间的关系，也就是父类与子类之间的关系。继承关系是泛化关系的反关系，也就是说，子类继承了父类，而父类则是子类的泛化。

（4）共享聚集。共享聚集关系通常简称为聚合关系，它表示类之间的整体与部分的关系，其含义是“部分”可能同时属于多个“整体”，“部分”与“整体”的生命周期可以不相同。

（5）组合聚集。组合聚集关系通常简称为组合关系，它也是表示类之间的整体与部分的关系。与聚合关系的区别在于，组合关系中的“部分”只能属于一个“整体”，“部分”与“整体”的生命周期相同，“部分”随着“整体”的创建而创建，也随着“整体”的消亡而消亡。

（6）实现关系。实现关系将说明和实现联系起来。接口是对行为而非实现的说明，而类中则包含了实现的结构。一个或多个类可以实现一个接口，而每个类分别实现接口中的操作。

2．软件架构设计

软件架构为软件系统提供了一个结构、行为和属性的高级抽象对象，软件架构设计由构件的描述、构件的相互作用（连接件）、指导构件集成的模式以及这些模式的约束组成。

1）软件架构风格

软件架构设计的一个核心问题是能否达到架构级的软件复用，也就是说能否在不同的系统中使用同一个软件架构。

将软件架构分为数据流风格、调用/返回风格、独立构件风格、虚拟机风格和仓库风格。

2）软件架构评估

在架构评估过程中，评估人员所关注的是系统的质量属性。

从目前已有的软件架构评估技术来看，可以归纳为三类主要的评估方式，分别是基于调查问卷（或检查表）的方式、基于场景的方式和基于度量的方式。这三种评估方式中，基于场景的评估方式最为常用。

3．软件设计

软件设计是需求分析的延伸与拓展。需求分析阶段解决“做什么”的问题，而软件设计阶段解决“怎么做”的问题。

1）结构化设计（Structured Design，SD）

Structured Design 方法的基本思想是将软件设计成由相对独立且具有单一功能的模

块组成的结构，分为概要设计和详细设计两个阶段。

在概要设计中，将系统开发的总任务分解成许多个基本的、具体的任务，而为每个具体任务选择适当的技术手段和处理方法的过程称为详细设计。根据任务的不同，详细设计又可分为多种，例如输入/输出设计、处理流程设计、数据存储设计、用户界面设计、安全性和可靠性设计等。

2）面向对象设计

OOD 是面向对象分析（Object Oriented Design，OOD）方法的延续，其基本思想包括抽象、封装和可扩展性，其中可扩展性主要通过继承和多态来实现。

3）设计模式

根据处理范围不同，设计模式可分为类模式和对象模式。类模式处理类和子类之间的关系，这些关系通过继承建立，在编译时就被确定下来，属于静态关系；对象模式处理对象之间的关系，这些关系在运行时变化，更具动态性。

根据目的和用途不同，设计模式可分为创建型模式、结构型模式和行为型模式三种。

4．软件工程的过程管理

软件过程是软件生命周期中的一系列相关活动，即用于开发和维护软件及相关产品的一系列活动。软件产品的质量取决于软件过程，具有良好软件过程的组织能够开发出高质量的软件产品。

5．软件测试及其管理

1）测试的方法

软件测试方法可分为静态测试和动态测试。静态测试是指被测试程序不在机器上运行，而采用人工检测和计算机辅助静态分析的手段对程序进行检测。对文档的静态测试主要以检查单的形式进行，而对代码的静态测试一般采用桌前检查（Desk Checking）、代码走查和代码审查。

动态测试是指在计算机上实际运行程序进行软件测试，一般采用白盒测试和黑盒测试方法。

白盒测试也称为结构测试，主要用于软件单元测试中。

黑盒测试也称为功能测试，主要用于集成测试、确认测试和系统测试中。

2）测试的类型

根据国家标准 GB/T 15532—2008，软件测试可分为单元测试、集成测试、确认测试、系统测试、配置项测试和回归测试等类别。

6．软件集成技术

EAI 所连接的应用包括各种电子商务系统、ERP、CRM、SCM、OA、数据库系统和数据仓库等。从单个企业的角度来说，EAI 可以包括表示集成、数据集成、控制集成和业务流程集成等多个层次和方面，当然也可以在多个企业之间进行应用集成。

表示集成是黑盒集成，无须了解程序与数据库的内部构造。常用的集成技术主要有

屏幕截取和输入模拟技术。

为了完成控制集成和业务流程集成，必须首先解决数据和数据库的集成问题。在集成之前，必须首先对数据进行标识并编成目录，另外还要确定元数据模型，保证数据在数据库系统中分布和共享。因此，数据集成是白盒集成。

控制集成也称为功能集成或应用集成，是在业务逻辑层上对应用系统进行集成的。

业务流程集成也称为过程集成，这种集成超越了数据和系统，它由一系列基于标准的、统一数据格式的工作流组成。

EAI 技术可以适用于大多数要实施电子商务的企业，以及企业之间的应用集成。EAI 使得应用集成架构里的客户和业务伙伴，都可以通过集成供应链内的所有应用和数据库实现信息共享。

5.4.2 软件工程——历年真题

1．软件需求包括三个不同的层次：业务需求、用户需求和功能需求。其中业务需求（　　）。

A．反映了组织结构或客户对系统、产品高层次的目标要求。在项目视图与范围文档中予以说明

B．描述了用户使用产品必须实现的软件功能

C．定义了开发人员必须实现的软件功能

D．描述了系统展现给用户的行为和执行的操作等

2．软件需求包括三个不同的层次，分别为业务需求、用户需求和功能及非功能需求。（　　）属于用户需求。

A．反映了组织机构或客户对系统、产品高层次的目标要求，其在项目视图范围文档中予以说明

B．描述用户使用产品必须要完成的任务，其在使用实例文档或方案脚本说明中予以说明

C．定义了开发人员必须实现的软件功能，使得用户能完成他们的任务，从中满足了业务需求

D．软件产品为了满足用户的使用，对用户并发、处理速度、安全性能等方面的需求

3．使用 UML 对系统进行分析设计时，需求描述中的“包含”“组成”“分为”“部分”等词常常意味着存在（　　）关系，图 5-9 表示了这种关系。

A．关联　　B．聚集

C．泛化　　D．继承

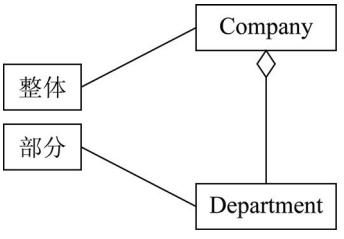

图 5-9　真题配图

4.（　　）也称为设计视图，它表示了设计模型中在架构方面具有重要意义的部分，即类、子系统、包和用例实现的子集。

A．逻辑视图　　B．进程视图

C．实现现图　　D．用例视图

5．软件架构是软件开发过程中的一项重要工作，（　　）不属于软件架构设计的主要工作内容。

A．制定技术规格说明　　B．编写需求规格说明书

C．技术选型　　D．系统分解

6．软件测试是为评价和改进产品质量、识别产品的缺陷和问题而进行的活动，以下关于软件测试的叙述中，（　　）是不正确的。

A．软件测试是软件开发中一个重要的环节

B．软件测试被认为是一种应该包括在整个开发和维护过程中的活动

C．软件测试是在有限测试用例集合上，静态验证软件是否达到预期的行为

D．软件测试是检查预防措施是否有效的主要手段，也是识别由于某种原因预防措施无效而产生错误的主要手段

7．软件测试是软件开发过程中的一项重要内容，将测试分为白盒测试、黑盒测试和灰盒测试，主要是（　　）对软件测试进行分类。

A．从是否关心软件内部结构和具体实现的角度

B．从是否执行程序的角度

C．从软件开发阶段的细分角度

D．从软件开发复杂性的角度

8．以下关于软件测试的叙述中，不正确的是（　　）。

A．在集成测试中，软件开发人员应该避免测试自己开发的程序

B．软件测试工作应该在需求阶段就开始进行

C．如果软件测试完成后没有发现任何问题，那么应首先检查测试过程是否存在问题

D．如果项目时间比较充裕，测试的时间可以长一些，如果项目时间紧张，测试时间可以少一些

参考答案

1	2	3	4	5	6	7	8
A	B	B	A	B	C	A	D

5.5 新一代信息技术

5.5.1 新一代信息技术——考点梳理

1．物联网

物联网（Internet of Things）主要解决物品与物品（Thing to Thing，T2T）、人与物品（Human to Thing，H2T）、人与人（Human to Human，H2H）之间的互连。

在物联网应用中有两项关键技术，分别是传感器技术和嵌入式技术。

- RFID（Radio Frequency Identification，射频识别）是物联网中使用的一种传感器技术。
- 嵌入式技术是综合了计算机软硬件、传感器技术、集成电路技术、电子应用技术为一体的复杂技术。

如果将物联网用人体做一个简单比喻，则传感器相当于人的眼睛、鼻子、皮肤等器官；网络就是神经系统，用来传递信息；嵌入式系统则是人的大脑，在接收到信息后要进行分类处理。

物联网架构可分为三层，分别是感知层、网络层和应用层。

- 感知层由各种传感器构成，包括温湿度传感器、二维码标签、RFID 标签和读写器、摄像头、GPS 等感知终端。感知层是物联网识别物体、采集信息的来源。
- 网络层由各种网络，例如互联网、广电网、网络管理系统和云计算平台等组成，其是整个物联网的中枢，负责传递和处理感知层获取的信息。
- 应用层是物联网和用户的接口，它与行业需求结合，实现物联网的智能应用。

物联网技术在智能电网、智慧物流、智能家居、智能交通、智慧农业、环境保护、医疗健康、城市管理（智慧城市）、金融服务保险业、公共安全等方面有非常关键和重要的应用。

物联网在城市管理中的综合应用即智慧城市。智慧城市建设主要包括以下几部分：

- 通过传感器或信息采集设备全方位地获取城市系统数据。
- 通过网络将城市数据关联、融合、处理、分析成信息。
- 通过充分共享、智能挖掘将信息变成知识。
- 结合信息技术，把知识应用到各行各业形成智慧。

智慧城市建设参考模型包括有依赖关系的五层和对建设有约束关系的三个支撑体系，如图 5-10 所示。

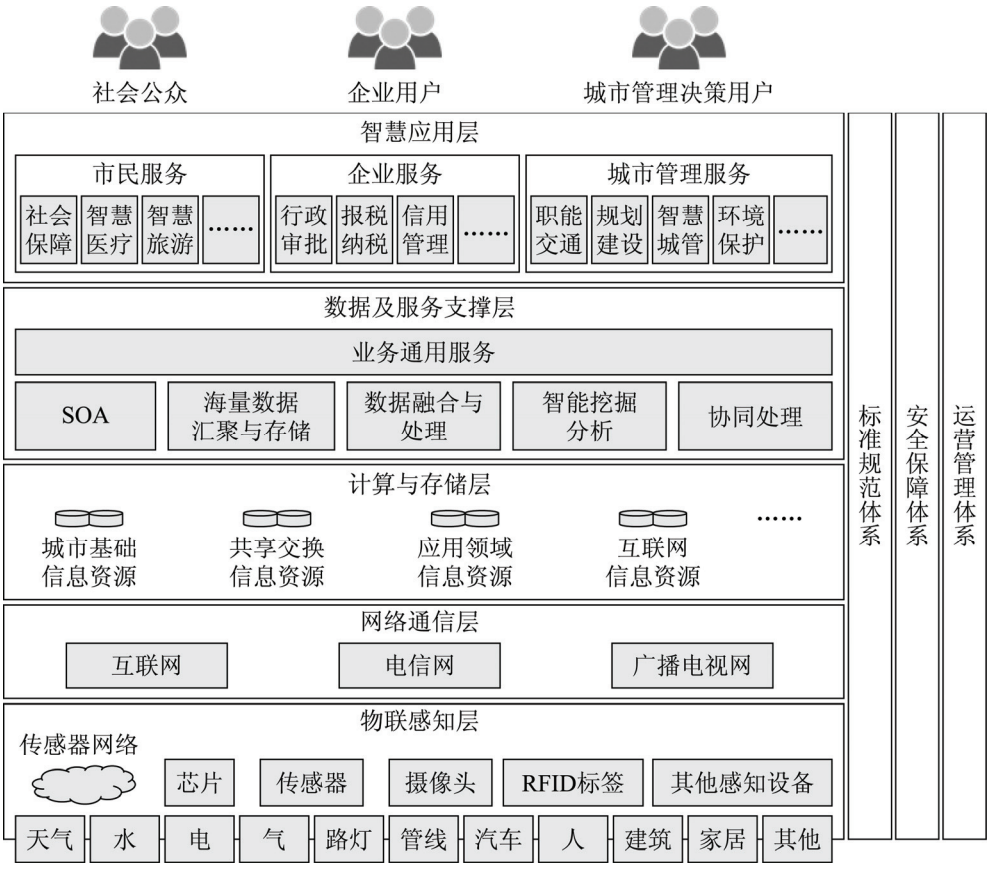

图 5-10　智慧城市建设参考模型

2．云计算

云计算（Cloud Computing）是一种基于互联网的计算方式，通过这种方式在网络上配置为共享的软件资源、计算资源、存储资源和信息资源，可以按需求提供给网上终端设备和终端用户。

1）云计算概念

所谓“云”是一种抽象的比喻，表示用网络来包裹服务和资源的一种状态，对用户而言这种包裹隐藏了服务或资源共享的实现细节。云计算是继大型机-终端计算模式转变为客户端-服务器计算模式之后的又一种计算模式的转变。在这种模式下，用户不再需要了解“云”中基础设施的细节，也不必具有相应的专业知识，更无须直接进行控制便可以将信息系统的运行维护完全交给“云”平台的管理者。云计算通常通过互联网来提供动态、易扩展而且经常是虚拟化的资源，并且计算能力也可作为一种资源通过互联网流通。

云计算的主要特点包括：宽带网络连接，快速、按需、弹性的服务。

2）云计算服务的类型

- IaaS（基础设施即服务），向用户提供计算机能力、存储空间等基础设施方面的服务。
- PaaS（平台即服务），向用户提供虚拟的操作系统、数据库管理系统、Web 应用等平台化的服务。
- SaaS（软件即服务），向用户提供应用软件（如 CRM、办公软件等）、组件、工作流等虚拟化软件的服务。

3）发展云计算的主要任务

（1）增强云计算服务能力。

（2）提升云计算自主创新能力。

（3）探索电子政务云计算发展新模式。

（4）加强大数据开发与利用。

（5）统筹布局云计算基础设施。

（6）提升安全保障能力。

3．大数据

大数据（Big Data）指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产。

1）大数据的特点

业界通常用 5 个 V——Volume（大量）、Variety（多样）、Value（价值）、Velocity（高速）和 Veracity（真实性）来概括大数据的特征。

2）大数据的价值与应用

大数据应用实例如下：

（1）大数据征信。

（2）大数据风控。

（3）大数据消费金融。

（4）大数据财富管理。

（5）大数据疾病预测。

3）大数据发展应用的目标

2015 年国务院印发了《促进大数据发展行动纲要》。纲要提出了立足我国国情和现实的需要，推动大数据发展和应用在未来 5～10 年逐步实现以下目标：

（1）打造精准治理、多方协作的社会治理新模式。

（2）建立运行平稳、安全高效的经济运行新机制。

（3）构建以人为本、惠及全民的民生服务新体系。

（4）开启大众创业、万众创新的创新驱动新格局。

（5）培育高端智能、新兴繁荣的产业发展新生态。

4．移动互联

移动互联是移动互联网的简称，它是将移动通信与互联网两者结合到一起而形成的。其工作原理为：用户通过移动终端来对互联网上的信息进行访问，并获取一些所需要的信息，人们可以享受一系列的信息服务带来的便利。

移动互联网的核心是互联网，因此一般认为移动互联网是桌面互联网的补充和延伸，应用和内容仍是移动互联网的根本。

移动互联网有以下特点：

（1）终端移动性。

（2）业务使用的私密性。

（3）终端和网络的局限性。

（4）业务与终端、网络的强关联性。

移动互联在市场领域和应用开发领域形成了一些特点，这些特点在移动互联领域内有着划时代的重要意义，例如：

（1）重视对传感技术的应用。

（2）有效地实现人与人的连接。

（3）浏览器竞争及孤岛问题突出。

5.5.2　新一代信息技术——历年真题

1．射频识别（RFID）是物联网中常用的无线通信技术，它通过（　　）识别特定目标并读写相关数据。

A．磁条　　B．红外线

C．无线电信号　　D．光束扫描

2．（　　）是物联网应用的重要基础，是两网融合的重要技术之一。

A．遥感和传感技术　　B．智能化技术

C．虚拟计算技术　　D．集成化和平台化

3．自从第一台电子计算机问世以来，信息系统经历了由低级到高级、由单机到网络、由数据处理到智能处理、由集中式计算到云计算的发展历程。以下关于云计算的叙述中，（　　）是不正确的。

A．云计算凭借数量庞大的云服务器为用户提供远超单台服务器的处理能力

B．云计算支持用户在任意位置获取应用服务，用户不必考虑应用的具体位置

C．云计算的扩展性低，一旦扩展则需要重新构建全部数据模型

D．云计算可以构造不同的应用，同一个“云”可以同时支撑不同的应用运行

4．Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. Advocates claim that cloud computing allows companies to avoid up-front infrastructure costs. Cloud computing now has few service form, but it is not including（　　）.

A．IaaS　　B．PaaS　　C．SaaS　　D．DaaS

5．以下关于大数据的叙述中，（　　）是不正确的。

A．大数据不仅是技术，更是思维方式、发展战略和商业模式

B．缺少数据资源和数据思维，对产业的未来发展会有严重影响

C．企业的价值与其数据资产的规模、活性、解释并运用数据的能力密切相关

D．大数据中，各数据价值之和远远大于数据之和的价值

6．以下关于移动互联网发展趋势的叙述中，（　　）是不正确的。

A．移动互联网与 PC 互联网协调发展，共同服务经济社会

B．移动互联网与传统行业融合，衍生新的应用模式

C．随着移动设备的普及，移动互联网将逐步替代 PC 互联网

D．移动互联网对用户的服务将更泛在、更智能、更便捷

7．以下关于移动互联网的描述，不正确的是：（　　）。

A．移动互联网使得用户可以在移动状态下接入和使用互联网服务

B．移动互联网是桌面互联网的复制和移植

C．传感技术能极大地推动移动互联网的成长

D．在移动互联网领域，仍存在浏览器竞争及“孤岛”问题

参考答案

1	2	3	4	5	6	7
C	A	C	D	D	C	B

5.6 信息系统安全技术

5.6.1 信息系统安全技术——考点梳理

1．信息安全的有关概念

1）信息安全概念

信息安全强调信息（数据）本身的安全属性，主要包括以下内容：

- 秘密性（Confidentiality）：信息不被未授权者知晓的属性。
- 完整性（Integrity）：信息是正确的、真实的、未被篡改的、完整无缺的属性。

- 可用性（Availability）：信息可以随时正常使用的属性。

针对信息系统，安全可以划分为以下四个层次：设备安全、数据安全、内容安全、行为安全。

2）信息安全等级保护

《信息安全等级保护管理办法》将信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级，信息系统受到破坏后会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。第五级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

5 个信息安全等级之间的区别，见表 5-2 所列。

表 5-2　《信息安全等级保护管理办法》中 5 个等级的区别

信息系统受到破坏后					
面向对象	第一级	第二级	第三级	第四级	第五级
对公民、法人和其他组织的合法权益	损害	严重损害	—	—	—
对社会秩序和公共利益	不损害	损害	严重损害	特别严重损害	
对国家安全	—	不损害	损害	严重损害	特别严重损害

2．信息加密，解密与常用算法

1）信息加密概念

加密前的原始数据称为明文，加密后的数据称为密文，从明文到密文的过程称为加

密（Encryption）。

合法收信者接收到密文后实行与加密变换相逆的变换，去掉密文的伪装恢复出明文，这一过程称为解密（Decryption）。

加密技术包括两个元素：算法和密钥。

对称加密以数据加密标准（Data Encryption Standard，DES）算法为典型代表，非对称加密通常以 RSA（Rivest Shamir Adleman）算法为代表。

2）对称加密技术

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥即加密密钥也可以用作解密密钥，这种方法在密码学中叫作对称加密算法。对称加密算法使用起来简单快捷、密钥较短、破译困难。

3）非对称加密技术

公开密钥密码的基本思想是将传统密码的密钥 K 一分为二，分为加密钥 K_e 和解密钥 K_d，用加密钥 K_e 控制加密，用解密钥 K_d 控制解密，而且计算复杂性确保加密钥 K_e 在计算上不能推出解密钥 K_d。这样即使是将 K_e 公开也不会暴露 K_d，也不会损害密码的安全，于是便可将 K_e 公开而只对 K_d 保密。由于 K_e 是公开的，只有 K_d 是保密的，所以便从根本上克服了传统密码在密钥分配上的困难。当前公开密钥密码包括基于大合数因子分解困难性的 RAS 密码类和基于离散对数问题困难性的 ELGamal 密码类。

4）Hash 函数的概念

Hash 函数将任意长的报文 M 映射为定长的 Hash 码。Hash 函数的目的就是要产生文件、报文或其他数据块的“指纹”——Hash 码。Hash 函数可提供保密性、报文认证以及数字签名功能。

5）数字签名的概念

签名是证明当事者的身份和数据真实性的一种信息。在信息化环境下，以网络为信息传输基础的事物处理中，事物处理各方应采用电子形式的签名即数字签名。

完善的数字签名体系应满足以下 3 个条件：

（1）签名者事后不能抵赖自己的签名。

（2）任何其他人不能伪造签名。

（3）如果当事的双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证签名来确认其真伪。

利用 RSA 密码可以同时实现数字签名和数据加密。

6）认证的概念

认证又称鉴别、确认，它是证实某事是否名副其实或是否有效的一个过程。

认证和加密的区别在于：加密用以确保数据的保密性，阻止对手的被动攻击，例如截取、窃听等；而认证用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，例如冒充、篡改、重播等。认证往往是许多应用系统中安全保护的第

一道设防，因而极为重要。

认证系统常用的参数有口令、标识符、密钥、信物、智能卡、指纹、视网纹等。

认证和数字签名技术都是确保数据真实性的措施，但两者有着明显的区别：

（1）认证总是基于某种收发双方共享的保密数据来认证被鉴别对象的真实性，而数字签名中用于验证签名的数据是公开的。

（2）认证允许收发双方互相验证其真实性，不准许第三者验证而数字签名允许收发双方和第三者都能验证。

（3）数字签名具有发送方不能抵赖、接收方不能伪造和具有在公证人前解决纠纷的能力，而认证则不一定具备。

3．信息系统安全

1）计算机设备安全

保证计算机设备的运行安全是信息系统安全最重要的内容之一。计算机设备安全主要包括计算机实体及其信息的完整性、机密性、抗否认性、可用性、可审计性、可靠性等几个关键因素。

计算机设备安全包括：物理安全、设备安全、存储介质安全、可靠性技术。

2）　网络安全

常见的网络威胁包括：

（1）网络监听。

（2）口令攻击。

（3）拒绝服务攻击（DoS）。

（4）漏洞攻击，例如利用 WEP 安全漏洞和 OpenSSL 安全漏洞实施攻击。

（5）僵尸网络（Botnet）。

（6）网络钓鱼（Phishing）。

（7）网络欺骗主要有 ARP 欺骗、DNS 欺骗、IP 欺骗、Web 欺骗、Email 欺骗等。

（8）网站安全威胁主要有 SQL（Structured Query Language）注入攻击、跨站攻击、旁注攻击等。

网络安全防御技术包括：

（1）防火墙。

防火墙是一种较早使用、实用性很强的网络安全防御技术，它阻挡对网络的非法访问和不安全数据的传递，使得本地系统和网络免于受到网络安全威胁。在网络安全中，防火墙主要用于逻辑隔离外部网络与受保护的内部网络。防火墙主要是实现网络安全的安全策略，而这种策略是预先定义好的，是一种静态安全技术。在策略中涉及的网络访问行为可以实施有效管理，而策略之外的网络访问行为则无法控制。防火墙的安全策略由安全规则表示。

（2）入侵检测与防护。

入侵检测与防护的技术主要有两种：入侵检测系统和入侵防护系统。

入侵检测系统（IDS）注重的是网络安全状况的监管，通过监视网络或系统资源寻找违反安全策略的行为或攻击迹象并发出报警，因此绝大多数 IDS 系统都是被动的。

入侵防护系统（IPS）则倾向于提供主动防护，注重对入侵行为的控制。其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失。

（3）VPN。

VPN（虚拟专用网络）是依靠 ISP（Internet 服务提供商）和其他 NSP（网络服务提供商）在公用网络中建立专用的、安全的数据通信通道的技术。VPN 可被认为是加密和认证技术在网络传输中的应用。

（4）安全扫描。

（5）网络蜜罐技术。

蜜罐技术是一种主动防御技术，是入侵检测技术的一个重要发展方向，也是一个“诱捕”攻击者的陷阱。蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机和服务器给攻击者提供一个容易攻击的目标。攻击者往往在蜜罐上浪费时间，延缓对真正目标的攻击。

3）操作系统安全

针对操作系统的安全威胁按照行为方式划分，通常有下面四种：

（1）切断，这是对可用性的威胁。

（2）截取，这是对机密性的威胁。

（3）篡改，这是对完整性的攻击。

（4）伪造，这是对合法性的威胁。

按照安全威胁的表现形式来分，操作系统面临的安全威胁有以下几种：

（1）计算机病毒。

（2）逻辑炸弹。

（3）特洛伊木马。

（4）后门。

（5）隐蔽通道。

4）数据库系统安全

一般而言，数据库安全涉及以下这些问题：

（1）物理数据库的完整性。

（2）逻辑数据库的完整性。

（3）元素安全性。

（4）可审计性。

（5）访问控制。

（6）身份认证。

（7）可用性。

（8）推理控制。

（9）多级保护。

5）应用系统安全

当前 Web 面临的主要威胁包括：可信任站点的漏洞、浏览器和浏览器插件的漏洞、终端用户的安全策略不健全、携带恶意软件的移动存储设备、网络钓鱼、僵尸网络、带有键盘记录程序的木马等。

Web 威胁防护技术主要包括：

（1）Web 访问控制技术。

（2）单点登录（Single Sign-On，SSO）技术。

（3）网页防篡改技术。

（4）Web 内容安全。

5.6.2　信息系统安全技术——历年真题

1．信息的（　　）要求采用的安全技术保证信息接收者能够验证在传送过程中信息没有被修改，并能防范入侵者用假信息代替合法信息。

A．隐蔽性　　B．机密性

C．完整性　　D．可靠性

2．针对信息系统，安全可以划分为四个层次，其中不包括：（　　）。

A．设备安全　　B．人员安全

C．内容安全　　D．行为安全

3．通过收集和分析计算机系统或网络的关键节点信息，以发现网络或系统中是否有违反安全策略的行为和被攻击的迹象的技术被称为（　　）。

A．系统检测　　B．系统分析

C．系统审计　　D．入侵检测

4．为了保护网络系统的硬件、软件及其系统中的数据，需要相应的网络安全工具。以下安全工具中，（　　）被比喻为网络安全的大门，用来鉴别什么样的数据包可以进入企业内部网。

A．杀毒软件　　B．入侵检测系统

C．安全审计系统　　D．防火墙

5．按照行为方式，可以将针对操作系统的安全威胁划分为切断、截取、篡改、伪造四种。其中（　　）是对信息完整性的威胁。

A．切断　　B．截取

C．篡改　　D．伪造

6．GB/T 22240—2008《信息安全技术 信息系统安全等级保护定级指南》标准将信息系统的安全保护等级分为五级。“信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害”是（　　）的特征。

A．第二级　　B．第三级　　C．第四级　　D．第五级

参考答案

1	2	3	4	5	6
C	B	D	D	C	B

5.7 信息化发展与应用

5.7.1 信息化发展与应用——考点梳理

1．信息化发展与应用的新特点

当前，信息技术发展的总趋势是从典型的技术驱动发展模式向应用驱动与技术驱动相结合的模式转变，信息技术发展趋势和新技术应用主要包括以下几个方面。

（1）高速度大容量；

（2）集成化和平台化；

（3）智能化；

（4）虚拟计算；

（5）通信技术；

（6）遥感和传感技术；

（7）移动智能终端；

（8）以人为本；

（9）信息安全。

2．国家信息化发展战略

我国信息化发展目标：根据《2006—2020 年国家信息化发展战略》，在 2006～2020 年期间，我国信息化发展的战略目标是：综合信息基础设施基本普及，信息技术自主创新能力显著增强，信息产业结构全面优化，国家信息安全保障水平大幅提高，国民经济和社会信息化取得明显成效，新型工业化发展模式初步确立，国家信息化发展的制度环境和政策体系基本完善，国民信息技术应用能力显著提高，为迈向信息社会奠定坚实基础。具体目标如下：

（1）促进经济增长方式的根本转变。

（2）实现信息技术自主创新、信息产业发展的跨越。

（3）提升网络普及水平、信息资源开发利用水平和信息安全保障水平。

（4）增强政府公共服务能力、社会主义先进文化传播能力、中国特色的军事变革能力和国民信息技术应用能力。

我国信息化发展的主要任务和发展重点发如下：

（1）促进工业领域信息化深度应用。

（2）加快推进服务业信息化。

（3）积极提高中小企业信息化应用水平。

（4）协力推进农业农村信息化。

（5）全面深化电子政务应用。

（6）稳步提高社会事业信息化水平。

（7）统筹城镇化与信息化互动发展。

（8）加强信息资源开发利用。

（9）构建下一代国家综合信息基础设施。

（10）促进重要领域基础设施智能化改造升级。

（11）着力提高国民信息能力。

3．电子政务

电子政务是政府机构应用现代信息和通信技术，将管理和服务通过网络技术进行集成，在网络上实现政府组织结构和工作流程的优化重组，超越时间、空间与部门分隔的限制，全方位地向社会提供优质、规范、透明、符合国际水准的管理和服务。电子政务作为信息技术与管理的有机结合，成为当代信息化最重要的领域之一。

应用模式为——电子政务根据其服务的对象不同，基本上可以分为以下四种模式：

（1）政府对政府（Government to Government，G2G）。

（2）政府对企业（Government to Business，G2B）。

（3）政府对公众（Government to Citizen，G2C）。

（4）政府对公务员（Government to Employee，G2E）。

4．电子商务

电子商务（Electronic Commerce，EC）是利用计算机技术、网络技术和远程通信技术，实现整个商务过程的电子化、数字化和网络化。要实现完整的电子商务会涉及到很多方面，除了买家、卖家外，还要有银行或金融机构、政府机构、认证机构、配送中心等机构的加入才行。由于参与电子商务中的各方在物理上是互不见面的，因此整个电子商务过程并不是物理世界商务活动的翻版，网上银行、在线电子支付等条件和数据加密、电子签名等技术在电子商务中发挥着不可或缺的作用。

电子商务应该具有以下基本特征：

（1）普遍性。

（2）便利性。

（3）整体性。

（4）安全性。

（5）协调性。

电子商务按照交易对象，电子商务模式包括：

- 企业与企业之间的电子商务（B2B）。
- 商业企业与消费者之间的电子商务（B2C）。
- 消费者与消费者之间的电子商务（C2C）。
- 电子商务与线下实体店有机结合，向消费者提供商品和服务称为 O2O 模式。

5．工业和信息化融合

我国企业信息化发展的战略要点：

（1）以信息化带动工业化。

（2）信息化与企业业务全过程的融合、渗透。

（3）信息产业发展与企业信息化良性互动。

（4）充分发挥政府的引导作用。

（5）高度重视信息安全。

（6）企业信息化与企业的改组改造和现代企业制度有机结合。

（7）“因地制宜”地推进企业信息化。

推进信息化与工业化深度融合：

两化融合是指电子信息技术广泛应用到工业生产的各个环节，信息化成为工业企业经营管理的常规手段。信息化进程和工业化进程不再相互独立进行，不再是单方的带动和促进关系，而是两者在技术、产品、管理等各个层面相互交融，彼此不可分割，并催生出工业电子、工业软件、工业信息服务等新产业。两化融合是工业化和信息化发展到一定阶段的必然产物。

6．智慧化

1）智慧化概念

智慧是指感知、学习、思考、判断、决策并指导行动的能力。传统上，智慧是高等动物具有的特征，随着信息技术的发展，大数据、云计算、网络传输、网络存储、各类传感器、控制器以及高速网络接入的成熟普遍应用，依托强大的计算能力和集成能力使各类信息系统具备了智慧化能力即不通过或极少通过人为的干预就能自动发挥管理和控制的功能，提供服务。

智能一般具备这样的特点：一是具有感知能力；二是具有记忆和思维能力；三是具有学习能力和自适应能力。

2）智慧化应用

智慧城市建设参考模型包括有依赖关系的五层（功能层）和对建设有约束关系的三个支撑体系（见图 5-10 智慧城市建设参考模型）。

5.7.2　信息化发展与应用——历年真题

1．两化（工业化和信息化）深度融合的主攻方向是（　　）。

A．智能制造　　B．数据挖掘　　C．云计算　　D．互联网+

2．2015 年国务院发布的《关于积极推进“互联网+”行为的指导意见》提出：到（　　）年，网络化、智能化、服务化、协同化的“互联网+”产业生态体系基本完善，“互联网+”成为经济社会创新发展的重要驱动力量。

A．2018　　B．2020　　C．2025　　D．2030

3．作为两化融合的升级版，（　　）将互联网与工业、商业、金融业等行业全面融合。

A．互联网+　　B．工业信息化　　C．大数据　　D．物联网

参考答案

1	2	3
A	C	A

5.8　信息系统服务管理

5.8.1　信息系统服务管理——考点梳理

典型的信息系统项目有如下特点：

- 项目初期目标往往不太明确。
- 需求变化频繁。
- 智力密集型。
- 系统分析和设计所需人员层次高，专业化强。
- 涉及的软件厂商硬件厂商和承包商多，联系、协调复杂。
- 软件和硬件常常需要个性化定制。
- 项目生命期通常较短。
- 通常要采用大量的新技术。
- 使用与维护的要求高。
- 项目绩效难以评估和量化。

信息系统工程监理工作的主要内容可以概括为“四控、三管、一协调”。

（1）投资控制。

（2）进度控制。

（3）质量控制。

（4）变更控制。

（5）合同管理。

（6）信息管理。

（7）安全管理。

（8）沟通协调。

IT 服务管理（IT Service Management，ITSM）是一套帮助组织对 IT 系统的规划、研发、实施和运营进行有效管理的方法，其是一套方法论。

ITSM 的核心思想是：IT 组织不管是组织内部的还是外部的，都是 IT 服务提供者，其主要工作就是提供低成本、高质量的 IT 服务。

2009 年 4 月，工业和信息化部软件服务业司成立了信息技术服务标准工作组（以下简称工作组），负责研究并建立信息技术服务标准体系，制定信息技术服务领域的相关标准，并按照信息服务生命周期提出一套完整的 IT 服务标准体系（Information Technology Service Standards，ITSS），其包含了 IT 服务的规划设计、部署实施、服务运营、持续改进和监督管理等全生命周期阶段应遵循的标准，涉及信息系统建设、运行维护、服务管理、治理及外包等业务领域，是一套体系化的信息技术服务标准库，全面规范了信息技术服务产品及其组成要素，用于指导实施标准化和可信赖的信息技术服务。

5.8.2 信息系统服务管理——历年真题

1．信息系统工程监理的内容可概括为：四控、三管、一协调，其中“三管”主要是针对项目的（　　）进行管理。

A．进度管理、成本管理、质量管理

B．合同管理、信息管理、安全管理

C．采购管理、配置管理、安全管理

D．组织管理、范围管理、挣值管理

2．以下对项目管理和项目监理的理解中，正确的是（　　）。

A．项目监理属于项目管理的监控过程组

B．项目监理属于项目管理的执行过程组

C．项目管理与项目监理是独立两个过程，没有任何关系

D．项目建设方和项目承建方都需要开展项目管理工作，而项目监理要由第三方负责

参考答案

1	2
B	D

5.9　信息系统规划

信息系统规划——考点梳理

大型信息系统作为一种典型的大系统，除具有大系统的一些共性特点，还具备以下独有的特点：

（1）规模庞大。

（2）跨地域性。

（3）网络结构复杂。

（4）业务种类多。

（5）数据量大。

（6）用户多。

信息系统规划流程：

（1）分析企业信息化现状。

（2）制定企业信息化战略。

（3）信息系统规划方案拟定和总体构架设计。

信息系统规划方法：

（1）信息系统规划（Information System Planning，ISP）。

（2）企业系统规划（Business System Planning，BSP）。

5.10　企业首席信息官及其职责

企业首席信息官及其职责——考点梳理

企业首席信息官（CIO）的主要职责包括：

（1）提供信息，帮助企业决策。

（2）帮助企业制定中长期发展战略。

（3）有效管理 IT 部门。

（4）制定信息系统发展规划。

（5）建立积极的 IT 文化。

5.11 信息系统安全管理

5.11.1 信息系统安全管理——考点梳理

1．信息系统安全策略的概念与内容

信息系统安全策略是指针对本单位的计算机业务应用信息系统的安全风险（安全威胁）进行有效地识别、评估后所采取的各种措施、手段，以及建立的各种管理制度、规章等。

安全策略的核心内容就是“七定”，即定方案、定岗、定位、定员、定目标、定制度、定工作流程。

2．建立安全策略需要处理好的关系

（1）安全与应用的依存关系。

（2）风险度的观点。

（3）适度安全的观点。

（4）木桶效应的观点。

（5）信息系统安全等级保护的概念：《计算机信息系统安全保护等级划分准则》（GB 17859—1999）将计算机信息系统分为以下 5 个安全保护等级。

第一级　用户自主保护级。通过隔离用户与数据，使用户具备自主安全保护的能力。它为用户提供可行的手段，保护用户和用户信息，避免其他用户对数据的非法读写与破坏，该级适用于普通内联网用户。

第二级　系统审计保护级。实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。该级适用于通过内联网或国际网进行商务活动且需要保密的非重要单位。

第三级　安全标记保护级。具有系统审计保护级的所有功能。此外，还需提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述，具有准确地标记输出信息的能力；消除通过测试发现的任何错误。该级适用于地方各级国家机关、金融单位机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位。

第四级　结构化保护级。建立于一个明确定义的形式安全策略模型之上，要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道，必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算机的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制，支持系统管理员和操作员的职能，提供可信设施管理，增强了配置管理控制。系统具有相当强的抗渗透能力。该级适用于中央级国家机关、广播电视部门、重要物资储备单位、

社会应急服务部门、尖端科技企业集团、国家重点科研单位机构和国防建设等部门。

第五级　访问验证保护级。满足访问控制器需求，访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的，必须足够小才能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算机在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最低程度。

支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很强的抗渗透能力，该级适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位。

信息系统的安全保护等级由两个定级要素决定，等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

3．信息系统安全策略设计原则

8 个总原则：

（1）主要领导人负责原则。

（2）规范定级原则。

（3）依法行政原则。

（4）以人为本原则。

（5）注重效费比原则。

（6）全面防范、突出重点原则。

（7）系统、动态原则。

（8）特殊的安全管理原则。

10 个特殊原则：

（1）分权制衡原则。

（2）最小特权原则。

（3）标准化原则。

（4）用成熟的先进技术原则。

（5）失效保护原则。

（6）普遍参与原则。

（7）职责分离原则。

（8）审计独立原则。

（9）控制社会影响原则。

（10）保护资源和效率原则。

4．信息安全系统工程

1）信息安全系统工程概述

信息系统业界又被称作信息应用系统、信息应用管理系统、管理信息系统。信息安全系统服务于业务应用信息系统，并与之密不可分，但又不能混为一谈。术语之间的关

系如图 5-11 所示。

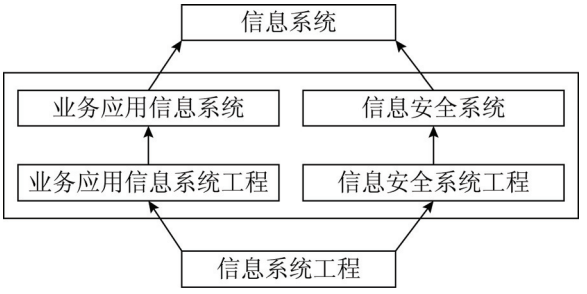

图 5-11　术语之间的关系

信息系统工程即建造信息系统的工程，包括两个独立且不可分割的部分，即信息安全系统工程和业务应用信息系统工程（如图 5-9 所示）。

信息安全系统工程是指为了达到建设好信息安全系统的特殊需要而组织实施的工程，它是信息系统工程的一部分。

2）信息安全系统

我们用一个“宏观”三维空间图来反映信息安全系统的体系架构及其组成，如图 5-12 所示。

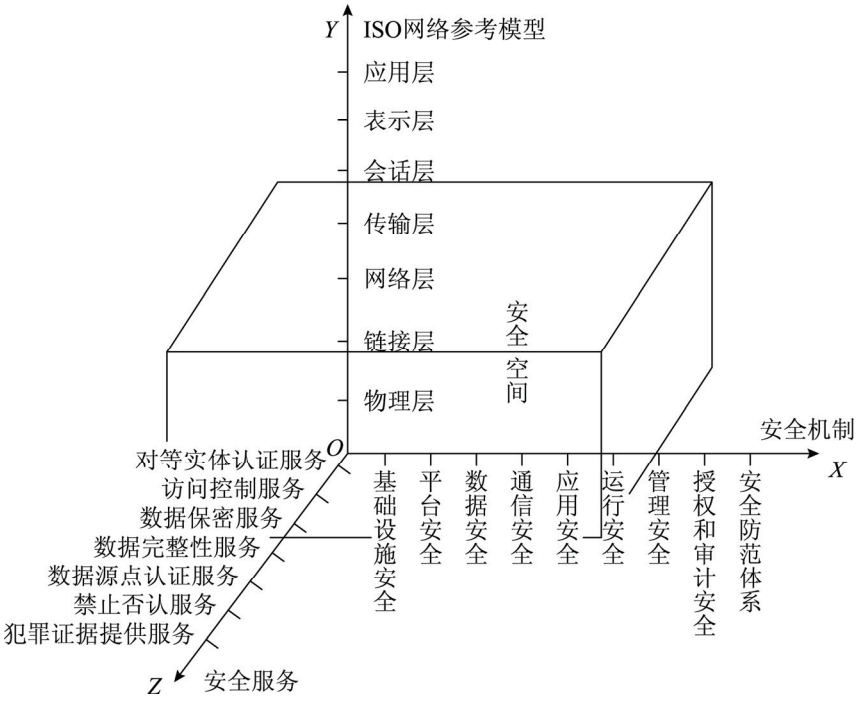

图 5-12　信息安全空间

由 X、Y、Z 三个轴形成的信息安全系统三维空间就是信息系统的“安全空间”。随着网络逐层扩展，这个空间不仅范围逐步加大，安全的内涵也就更丰富，达到具有认证、权限、完整、加密和不可否认五大要素，也叫作“安全空间”的五大属性。

3．信息安全系统架构体系

信息安全系统大体划分为三种架构体系：MIS+S 系统、S-MIS 系统和 S2-MIS 系统。

- MIS+S（Management Information System+Security）系统为“初级信息安全保障系统”或“基本信息安全保障系统”。
- S-MIS 系统架构（Security- Management Information System）系统为“标准信息安全保障系统”。
- S2-MIS 系统架构（Super Security-Management Information System）系统为“超安全的信息安全保障系统”。

4．信息安全系统工程基础

信息安全系统工程活动离不开以下相关工程：

（1）硬件工程。
（2）软件工程。
（3）通信及网络工程。
（4）数据存储和灾备工程。
（5）系统工程。
（6）测试工程。
（7）密码工程。
（8）企业信息化工程。

信息安全系统工程应该吸纳安全管理的成熟规范部分，这些安全管理包括：

（1）物理安全。
（2）计算机安全。
（3）网络安全。
（4）通信安全。
（5）输入/输出产品的安全。
（6）操作系统安全。
（7）数据库系统安全。
（8）数据安全。
（9）信息审计安全。
（10）人员安全。
（11）管理安全。
（12）辐射安全。

5．信息安全系统工程体系结构

信息安全系统工程能力成熟度模型（Information Security System Engineering Capability Maturity Model，ISSE-CMM）是一种衡量信息安全系统工程实施能力的方法，是使用面向工程过程的一种方法。

ISSE 将信息安全系统工程实施过程分解为：工程过程、风险过程和保证过程三个基本的部分。

6．PKI 公开密钥基础设施

1）公钥基础设施基本概念

公钥基础设施（Public Key Infrastructure，RKI）是以**不对称密钥加密**技术为基础，以数据机密性、完整性、身份认证和行为不可抵赖性为安全目的来实施和提供安全服务的具有普适性的安全基础设施。其内容包括数字证书、不对称密钥密码技术、认证中心、证书和密钥的管理、安全代理软件、不可否认性服务、时间邮戳服务、相关信息标准、操作规范等。

认证中心：CA（Certification Authority）是 PKI 的核心，它是公正、权威、可信的第三方网上认证机构。

在 PKI/CA 架构中，一个重要的标准就是 X.509 标准，数字证书就是按照 X.509 标准制作的。

2）数字证书的生命周期

阶段一：安全需求确定。

阶段二：证书登记。

阶段三：证书分发。

阶段四：证书撤回。

阶段五：证书更新。

阶段六：证书审计。

3）信任模型

X.509 规范中给出了适于目标的定义：如果实体 A 认为实体 B 严格地按 A 所期望的那样行动，则 A 信任 B。因此，信任涉及假设、预期和行为。这明确地意味着信任是不可能被定量测量的，信任是与风险相关的，而且信任的建立不可能总是全自动的。然而信任模型的概念是有用的，因为它显示了 PKI 中信任最初是怎样建立的，允许人们对基础结构的安全性以及被这种结构所强加的种种限制进行更详尽地推理，以确定 PKI 的可信任程度。

4）应用模式

（1）电子商务。

（2）电子政务。

（3）网上银行。

（4）网上证券。

（5）其他应用。

7．PMI 权限（授权）管理基础设施

PMI（Privilege Management Infrastructure）即权限管理基础设施或授权管理基础设施。PMI 授权技术的核心思想是以资源管理为核心，将对资源的访问控制权统一交由授权机构进行管理，即由资源的所有者来进行访问控制管理。

1）PMI 与 PKI 的区别

PMI 主要进行授权管理，证明这个用户有什么权限，能干什么即“你能做什么”。

PKI 主要进行身份鉴别，证明用户身份即“你是谁”。

2）属性证书定义

对一个实体权限的绑定是由一个被数字签名了的数据结构来提供的，这种数据结构称为属性证书，由属性证书管理中心签发并管理。一些应用使用属性证书来提供基于角色的访问控制。

3）访问控制

访问控制是为了限制访问主体（或称为发起者，是一个主动的实体，例如用户、进程、服务等）对访问客体（需要保护的资源）的访问权限，从而使计算机信息应用系统在合法范围内使用；访问控制机制决定用户和代表一定用户利益的程序能做什么以及能做到什么程度。

访问控制有两个重要过程：

（1）认证过程，通过“鉴别（Authentication）”来检验主体的合法身份。

（2）授权管理，通过“授权（Authorization）”来赋予用户对某项资源的访问权限。

访问控制机制可分为强制访问控制（Mandatory Access Control，MAC）和自主访问控制（Discretionary Access Control，DAC）两种。

- 强制访问控制：系统独立于用户行为强制执行访问控制，用户不能改变他们的安全级别或对象的安全属性。这样的访问控制规则通常对数据和用户按照安全等级划分标签，访问控制机制通过比较安全标签来确定是授予还是拒绝用户对资源的访问。
- 自主访问控制：允许对象的属主来制定针对该对象的保护策略。通常 DAC 通过授权列表（或访问控制列表）来限定哪些主体针对哪些客体可以执行什么操作。这样可以非常灵活地对策略进行调整。

4）基于角色的访问控制

基于角色的访问控制 RBAC（Role-Based Access Control）技术，有效地克服了传统访问控制技术中存在的不足。

用户不能自主地将访问权限授权给别的用户，这是 RBAC 与 DAC 的根本区别所在。

基于角色的访问控制中，角色由应用系统的管理员定义。

5）PMI 支撑体系

目前我们使用的访问控制授权方案，主要有以下 4 种。

（1）DAC 自主访问控制方式：该模型针对每个用户指明能够访问的资源，对于不在指定的资源列表中的对象不允许访问。

（2）ACL（Access Control List）访问控制列表方式：该模型是目前应用最多的方式。目标资源拥有访问权限列表，指明允许哪些用户访问。如果某个用户不在访问控制列表中，则不允许该用户访问这个资源。

（3）MAC 强制访问控制方式，该模型在军事和安全部门中应用较多，目标具有一个包含等级的安全标签（例如：不保密、限制、秘密、机密、绝密）；访问者拥有包含等级列表的许可，其中定义了可以访问哪个级别的目标，例如，允许访问秘密级信息，这时，秘密级、限制级和不保密级的信息是允许访问的，但机密和绝密级信息不允许访问。

（4）RBAC 基于角色的访问控制方式：该模型首先定义一些组织内的角色，例如局长、科长、职员；再根据管理规定给这些角色分配相应的权限，最后对组织内的每个人根据具体业务和职位分配一个或多个角色。

8．信息安全审计

1）安全审计概念

安全审计（Security Audit）是记录、审查主体对客体进行访问的使用情况，保证安全规则被正确执行，并帮助分析安全事故产生的原因。

安全审计是信息安全保障系统中的一个重要组成部分，是落实系统安全策略的重要机制和手段，通过安全审计识别与防止计算机网络系统内的攻击行为，追查计算机网络系统内的泄密行为。安全审计具体包括两方面的内容：

（1）采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，及时响应（如报警）并进行阻断。

（2）对信息内容和业务流程进行审计，可以防止内部机密或敏感信息的非法泄漏和单位资产的流失。

因此信息安全审计系统被形象地比喻为“黑匣子”和“监护神”。

安全审计功能包括：

（1）安全审计自动响应功能。

（2）安全审计数据生成功能。

（3）安全审计分析功能。

（4）安全审计浏览功能。

2）建立安全审计系统

建设安全审计系统的主体方案一般包括利用网络安全入侵监测预警系统，实现网络与主机信息监测审计；对重要应用系统运行情况的审计和基于网络旁路监控方式安全审计等。

3）分布式审计系统

分布式审计系统由审计中心、审计控制台和审计 Agent 组成。

- 审计中心是对整个审计系统的数据进行某种存储和管理，并进行应急响应的专用软件，它基于数据库平台，采用数据库方式进行审计数据管理和系统控制，并在无人看守情况下长期运行。
- 审计控制台是给管理员提供审计数据查阅使用的，其对审计系统进行规则设置。审计控制台具有报警功能的界面软件，可以有多个审计控制台软件同时运行。
- 审计 Agent 主要可以分为网络监听型 Agent、系统嵌入型 Agent、主动信息获取型 Agent 等。

5.11.2　信息系统安全管理——历年真题

1．访问控制是为了限制访问主体对访问客体的访问权限，从而使计算机系统在合法范围内使用的安全措施，以下关于访问控制的叙述中，（　　）是不正确的。

A．访问控制包括两个重要的过程：鉴别和授权

B．访问控制机制分为两种：强制访问控制（MAC）和自主访问控制（DAC）

C．RBAC 基于角色的访问控制对比 DAC 的先进之处在于：用户可以自主的将访问的权限授权给其他用户

D．RBAC 不是基于多级安全需求的，因为基于 RBAC 的系统中主要关心的是保护信息的完整性，即“谁可以对什么信息执行何种动作”

2．信息系统访问控制机制中，（　　）是指对所有主体和客体部分分配安全标签用来标识所属的安全级别，然后在访问控制执行时对主体和客体的安全级别进行比较，确定本次访问是否具有合法性的技术或方法。

A．自主访问控制　　B．强制访问控制

C．基于角色的访问控制　　D．基于组的访问控制

3．在信息系统安全保护中，信息安全策略控制用户对文件、数据库表等客体的访问属于（　　）安全管理。

A．安全审计　　B．入侵检测

C．访问控制　　D．人员行为

4．安全审计是通过测试公司信息系统对一套确定标准的符合程度来评估其安全性的系统方法，安全审计的主要作用不包括（　　）。

A．对潜在的攻击者起到震慑或警告作用

B．对已发生的系统破坏行为提供有效的追究证据

C．通过提供日志，帮助系统管理员发现入侵行为或潜在漏洞

D．通过性能测试，帮助系统管理员发现性能缺陷或不足

5．以下关于信息系统审计的叙述中，不正确的是（　　）。

A．信息系统审计是安全审计过程的核心部分

B．信息系统审计的目的是评估并提供反馈、保证及建议

C．信息系统审计是了解规划、执行及完成审计工作的步骤与技术，并尽量遵守国际信息系统审计与控制协会的一般公认信息系统审计准则、控制目标和其他法律与规定

D．信息系统审计的目的可以是收集并评估证据以决定一个计算机系统（信息系统）是否有效做到保护资产、维护数据完整、完成组织目标

6．《计算机信息系统安全保护等级划分准则》规定了计算机系统安全保护能力的 5 个等级。其中，按照（　　）的顺序从左到右安全能力逐渐增强。

A．系统审计保护级、结构化保护级、安全标记保护级

B．用户自主保护级、访问验证保护级、安全标记保护级

C．访问验证保护级、系统审计保护级、安全标记保护级

D．用户自主保护级、系统审计保护级、安全标记保护级

7．某信息系统采用了基于角色的访问机制，其角色的权限是由（　　）决定的。

A．用户自己　　B．系统管理员

C．主体　　D．业务要求

参考答案

1	2	3	4	5	6	7
C	B	C	D	A	D	B

5.12　信息系统综合测试与管理

5.12.1　信息系统综合测试与管理——考点梳理

1．软件测试模型

所谓测试模型就是测试和测试对象的基本特征、基本关系的抽象描述。它是测试理论专家们根据大量的实际测试应用总结出来的，能够代表某一类应用的内在规律，并对应于适合此类应用的一组测试框架性的东西。

软件测试过程的主要模型有 V 模型、W 模型、H 模型、X 模型、前置测试模型。

软件测试 V 模型如图 5-13 所示。

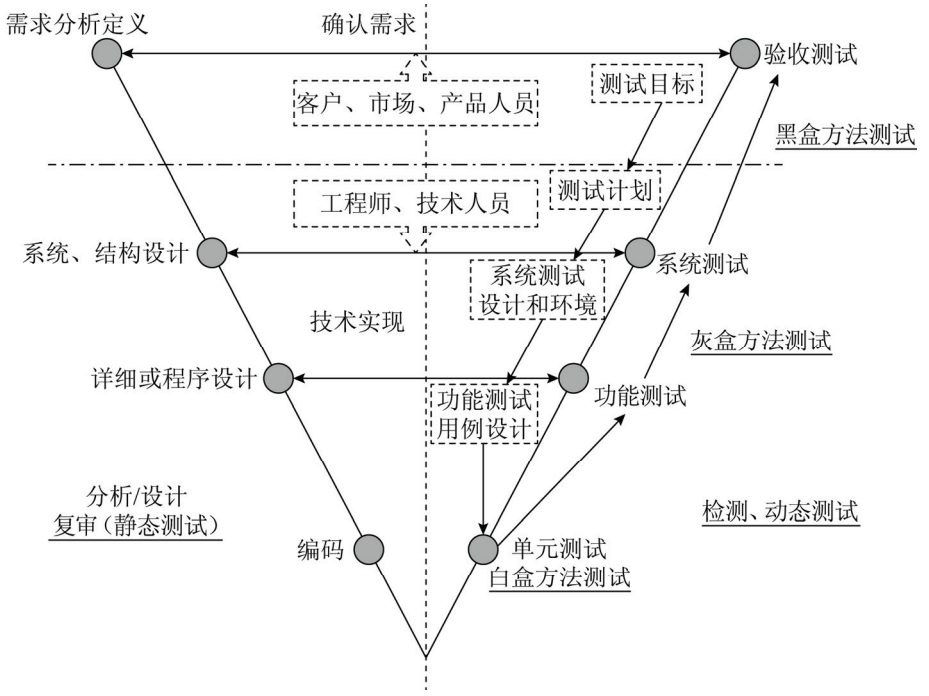

图 5-13　软件测试 V 模型

2）软件测试类型

- 按照开发阶段划分，软件测试类型分为单元测试、集成测试、系统测试和验收测试。
- 按照测试实施组织划分，软件测试类型分为开发方测试、用户测试、第三方测试。
- 按照测试技术划分，软件测试类型分为黑盒测试、白盒测试和灰盒测试。
- 按照测试执行方式划分，软件测试类型分为静态测试和动态测试。
- 按照测试对象类型划分，软件测试类型分为功能测试、界面测试、流程测试、接口测试、安装测试、文档测试、源代码测试、数据库测试、网络测试和性能测试。
- 按照质量属性划分，软件测试类型分为容错性测试、兼容性测试、安全性测试、可靠性测试、维护性测试、可移植性测试和易用性测试。
- 按照测试地域划分，软件测试类型分为本地化测试和国际化测试。

3）软件维护类型

- 改正性维护是指改正在系统开发阶段已发生，而系统测试阶段尚未发现的错误。这方面的维护工作量要占整个维护工作量的 17%～21%。
- 适应性维护是指使用软件适应信息技术变化和管理需求变化而进行的修改。这方面的维护工作量占整个维护工作量的 18%～25%。人们常常为改善系统硬件环境和运行环境而产生系统更新换代的需求；企业的外部市场环境和管理需求的不断

变化也使得各级管理人员不断提出新的信息需求。

- 完善性维护是为扩充功能和改善性能而进行的修改，主要是指对已有的软件系统增加一些在系统分析和设计阶段中，没有规定的功能与性能。这方面的维护占整个维护工作的 50%～60%，比重较大。
- 预防性维护是为了改进应用软件的可靠性和可维护性，为了适应未来的软硬件环境的变化，主动增加预防性的新功能，以使应用系统适应各类变化而不被淘汰。这方面的维护工作量占整个维护工作量的 4%。

2．软件测试技术

1）黑盒测试法

黑盒测试也称功能测试，它是通过测试来检测每个功能是否能正常使用。

在测试时，把被测程序视为一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下在程序接口进行测试，它只检查程序功能是否按照需求规格说明书的规定正常使用，程序是否能适当地接收输入数据而产生正确的输出信息，并且保持外部信息（例如数据库或文件）的完整性。黑盒测试主要检查程序外部结构，不考虑内部逻辑结构，主要针对软件界面和软件功能进行测试。

黑盒测试注重于测试软件的功能需求，主要发现以下几类错误：

（1）是否有不正确或遗漏的功能。

（2）在接口上，能否正确地接收输入数据，能否产生正确地输出信息。

（3）访问外部信息是否有错。

（4）性能上是否满足要求。

（5）界面是否错误，是否不美观。

（6）初始化或终止错误。

黑盒测试的优点主要有以下几点：

（1）比较简单，不需要了解程序内部的代码及实现。

（2）与软件的内部实现无关。

（3）从用户角度出发，能很容易地知道用户会用到哪些功能，会遇到哪些问题。

（4）基于软件开发文档，所以也能知道软件实现了文档中的哪些功能。

（5）在做软件自动化测试时较为方便。

黑盒测试的缺点主要有以下两点：

（1）不可能覆盖所有的代码，覆盖率较低，大概只能达到总代码量的 30%。

（2）自动化测试的复用性较低。

2）白盒测试法

白盒测试将测试对象看作一个透明的盒子，按照程序内部的结构测试程序，检验程序中的每条通路是否都能按预定要求正确工作，而不用管它的功能。通过在不同点检查程序的状态，确定实际的状态是否与预期的状态一致。因此白盒初试又称为结构测试或

逻辑驱动测试。

白盒测试允许测试人员利用程序内部的逻辑结构及有关信息，设计或选择测试案例，对程序所有逻辑路径进行测试，是一种穷举路径的测试方法。但即使每条路径都测试过了，仍然可能存在错误。

3．信息系统测试管理

测试管理是为了实现测试工作预期目标，以测试人员为中心对测试生命周期及其所涉及的相应资源进行有效的计划、组织、领导和控制的协调活动。

测试管理的主要因素包括测试策略的制定、测试项目进度跟进、项目风险的评估、测试文档的评审、测试内部和外部的协调沟通、测试人员的培养等。

测试管理内容主要有以下几个方面：

- 测试目标明确，进行测试计划及过程监控准则的制订。
- 测试团队搭建和测试人员管理。
- 测试实施过程的监控，包括测试计划执行的跟踪和测试人员的工作安排等内容。
- 测试风险的评估和风险的应对策略。
- 测试外部的沟通协调和测试问题的确认处理。
- 测试资产、测试产品的统一管理。
- 测试规范的制定。
- 测试绩效考核的制定与考评。

5.12.2　信息系统综合测试与管理——历年真题

1．某软件系统交付后，开发人员发现系统的性能可以进一步优化和提升，由此产生的软件维护属于（　　）。

A．更正性维护　　B．适应性维护　　C．完善性维护　　D．预防性维护

2．软件维护工作包括多种类型，其中（　　）的目的是检测并更正软件产品中的潜在错误，防止它们成为实际错误。

A．更正性维护　　B．适应性维护　　C．完善性维护　　D．预防性维护

参考答案

1	2
C	D