

前言

本书根据《信息系统监理师》考试大纲编制，为考点重点精粹。此科目背诵内容比较多，多以理论理解为主。

路漫漫其修远兮，学习本身不是一件轻松躺平的事，成功就是坚持不下去的时候，再坚持一会。
本书已覆盖 90%以上的考点，考生认真学通此书，必可顺利上岸通关！

由于编者水平所限，书中难免会有不当之处，欢迎各位考生不吝赐教并提出宝贵的意见，相信大家的反馈会为未来再次修订提供良好的帮助。



抖音：软考羽仪老师 微信：yuyilaoshi4

第一篇目录

第一章 信息化发展	3
第二章 信息系统工程	7
第三章 信息网络系统	16
第四章 信息资源系统	20
第五章 信息应用系统	24
第六章 信息安全	26
第七章 运行维护	28

第一篇 信息系统工程知识

第一章 信息化发展

一、信息与信息化

1、信息的概念

- ❖ 数据由原始事实组成
- ❖ DIKW 模型很好地诠释了数据、信息、知识和智慧之间的关系
- ❖ 有价值的信息特征：便捷性、准确性、完整性、经济性、灵活性、相关性、可靠性、安全性、简单性、及时性、可检验性
- ❖ 信息化的概念

信息化	基本内涵（口诀：主权、常识、空域、手工、涂改、飙升）
主体	全体社会成员，包含政府、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
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提升

❖ 国家信息化战略与规划

组织信息化趋势	呈现出产品信息化、产业信息化、社会生活信息化和国民经济信息化等趋势和方向。	
国家信息化趋势	第一步到 2020 年	核心关键技术部分领域达到国际先进水平，信息产业国际竞争力大幅提升，信息化成为驱动现代化建设的先导力量；
	第二步到 2025 年	建成国际领先的移动通信网络，根本改变核心关键技术受制于人的局面，实现技术先进、产业发达、应用领先、网络安全坚不可摧的战略目标，涌现一批具有强大国际竞争力的大型跨国网信企业；
	第三步到 21 世纪中叶	信息化全面支撑富强民主文明和谐的社会主义现代化国家建设，网络强国地位日益巩固，在引领全球信息化发展方面有更大作为。

二、信息基础设施

1、新型基础设施建设（新基建）

- ❖ 基础设施包括交通、能源、水利、物流等以传统基础设施和信息网络为核心的新型基础设施，在国家发展全局中具有**战略性、基础性、先导性**作用。
- ❖ 新型基础设施是以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系；
- ❖ 新基建主要包括**5G 基建、特高压、城际高速铁路和城际轨道交通、新能源汽车充电桩、大数据中心、人工智能、工业互联网**等七大领域。
- ❖ 新型基础设施主要包括如下三个方面

新型基础设施	说明

监理师讲义第一篇-羽仪老师

信息基础设施 “技术新”	(1) 以 5G、物联网、工业互联网、卫星互联网为代表的通信网络基础设施； (2) 以人工智能、云计算、区块链等为代表的新技术基础设施； (3) 以数据中心、智能计算中心为代表的算力基础设施等。
融合基础设施 “应用新”	融合基础设施主要指深度应用互联网、大数据、人工智能等技术，支撑传统基础设施转型升级，进而形成的融合基础设施。融合基础设施包括智能交通基础设施、智慧能源基础设施等。
创新基础设施 “平台新”	创新基础设施主要指支撑科学研究、技术开发、产品研制的具有公益属性的基础设施。创新基础设施包括重大科技基础设施、科教基础设施、产业技术创新基础设施等。

(关键词：“信息技术，应用融合，创新平台”)

2、云计算

- ◆ 云计算的特征：为超大规模、高可扩展性、虚拟化、高可靠性、通用性、廉价性和灵活定制。
- ◆ 按服务类型分类：云计算基础设施云、平台云和应用云。
- ◆ 按部署范围分类：公有云、私有云和混合云。
- ◆ 云计算的服务类型

层次	解释
IaaS 基础设施即服务	是以服务形式提供服务器、存储和网络硬件。
PaaS 平台即服务	PaaS 一般包含数据库、中间件及开发工具，均以服务形式通过互联网提供。
SaaS 软件即服务	将应用程序以服务形式提供给用户，SaaS 一般通过浏览器将程序提供给成千上万的用户使用。

3、大数据

- ◆ 大数据 4V 特征：规模性大 (Volume)、多样性 (Variety)、价值高 (Value) 但密度低、速度快 (Velocity)。
- ◆ 结构分类：结构化数据（符合关系型数据库，二维表）；半结构化数据（不符合关系型数据库）；非结构化数据（没有固定结构的数据，比如文本、图片、各类报表）。
- ◆ Hadoop 生态系统：Hadoop2.0 主要由三部分组成
 - ① HDFS：分布式文件存储系统，有高容错性、适合大数据批处理、可构建在廉价机器上等优点，缺点是不支持低延迟数据访问、小文件存取、并发写入、文件随机修改
 - ② MapReduce：计算模型，用于大规模数据集的并行运算。
 - ③ Yarn：Hadoop 的资源管理任务全交由 Yarn 处理，从而实现存储、任务、资源的分离。
- ◆ 大数据应用：包括数据采集、数据存储、数据计算和数据展现与交互。

4、物联网（物物相联之网）

- ◆ 具有互连、识别与通信、智能化三个特点。
- ◆ 从产业的角度来看，物联网具备的六个特点：感知识别普适化；异构设备互连化；互联网终端规模化；管理调控智能化；应用服务链条化；经济发展跨越化。
- ◆ 从应用角度来看，物联网具备领域性、多样化的特征。
- ◆ 物联网的分类
 - ① 按照部署方式分类：私有物联网（是私人拥有的小型网络）、公有物联网（主要由所属机构自己运营维护）、社区物联网（由两个或两个以上的机构协同运行和维护）和混合物联网（在后台统一运行维护）。
 - ② 基于物联网业务对传输速率的需求分类：高速率、中速率及低速率业务。

5、工业互联网（不是一种技术门类，而是一种社会形态）

- ◆ 工业互联网：包含网络、平台、数据、安全四大体系。
 - ① 网络体系是基础，包括网络互连、数据互通、标识解析；

监理师讲义第一篇-羽仪老师

- ② 平台体系是中枢，包括边缘层(与设备连接)、IaaS 层、PaaS 层、SaaS 层四部分，是工业互联网的“操作系统”；
③ 数据体系是工业互联网的要素，是工业互联网价值创造的源泉；
④ 安全体系是工业互联网的保障，针对工业互联网涉及范围广、影响大、企业防护基础弱的特点，提供设备、控制、网络、平台、工业应用的整体保护，保障工业互联网平稳运行。
- ❖ 工业互联网的关键技术
- ① 5G 技术：大带宽、低延时、高可靠。
 - ② TSN 技术：时间敏感网络。
 - ③ IPv6 技术：从 64 位扩展到 128 位。
 - ④ 标识解析体系：标识还是体系自有，阻碍了发展。
 - ⑤ 边缘计算技术；工业智能技术；数字孪生技术；区块链技术；虚拟现实（VR）/增强现实（AR）技术。

6、区块链

- ❖ 区块链技术作为以去中心化方式集体维护可信数据库的技术。区块链可以理解为一个多方协作数据库，区块链技术是一种分布式账本的记账技术。
- ❖ 区块链特点：具有多方协作、不可篡改、可追溯三大特点。
- ❖ 按照开放程度进行分类：区块链可分为公有链、私有链和联盟链。
- ❖ 区块链的核心技术

关键技术	说明
分布式存储	区块链本质上是一个分布式的公共账本，将各个区块连成一个链条，实际上是一种点对点的记账系统（一个总账本），每一个节点都可以记录信息。
共识机制	(1) 是在互不信任的网络中对事件前后顺序达成共识的一种算法。区块链技术正是运用共识算法在各个节点间建立去中心化的信任网络，解决记账不一致性的问题，为特定场景中的应用提供保障。 (2) 主流的共识机制主要有 PoW、PoS、DPoS、Paxos、PBFT 等。
智能合约	智能合约是一种基于预定义事件触发、不可篡改、自动执行的计算机协议，旨在以数字方式促进、验证或强制执行合同的谈判或履行。
加密算法	加密算法将明文信息转换成密文信息，信息的接收方能够通过密钥对密文信息进行解密，获得明文信息。加密算法分为对称加密和非对称加密（主要应用）两种。
跨链技术	本质上是一种将区块链上的数据或信息安全可信地转移到另外一条区块链上，并在其链上产生预期效果的一种技术。
分片技术	分片是一种通过将数据库分割为不同片区以达到系统扩容的技术。当多笔交易数据进入区块链系统中，各片区将分别处理一部分输入的交易数据，使更多的交易能够同时被处理和验证。

5、人工智能

- ❖ 弱人工智能：指不能真正实现推理和解决问题的智能机器，并不真正拥有智能，也不会有自主意识。
- ❖ 强人工智能：是指真正能思维的智能机器，并且有自我意识的，这类机器可分为类人（机器的思考和推理类似人的思维）与非类人（机器产生了和人完全不一样的知觉和意识，使用和人完全不一样的推理方式）两大类。
- ❖ 人工智能具有以下特征：由人类设计，为人类服务；能感知环境；有适应特性。
- ❖ 人工智能的关键技术包括：机器思维、机器感知、机器行为、机器学习、计算智能、分布智能、智能系统、人工心理和人工情感。

6、虚拟现实（VR）和增强现实（AR）

- ❖ VR/AR 的区别

	VR	AR
设备区别	鉴于 VR 是纯虚拟场景，VR 装备多配有位置追踪器、数据手套、动作捕捉系统、数据头盔等，用于用户与虚拟场景的互动。	虚拟与实景的结合，所以设备一般都配有 3D 摄像头，只要安装 AR 软件，带摄像头的产品都可以进行 AR 体验。

监理师讲义第一篇-羽仪老师

技术区别	VR的核心是绘图相关的各项技术，目前在游戏领域应用最广，最为关注的是沉浸感，对图形处理器性能要求较高。	AR则强调复原人类视觉，应用计算机视觉技术对真实场景进行3D建模再处理，重视CPU的处理能力。
应用场景区别	VR的虚拟现实特性使其具有沉浸感和私密性，决定了其在游戏、娱乐、教育、社交等领域具有天然优势	AR的增强现实特性决定了其更偏向于与现实交互，适用于生活、工作、生产等场景。

❖ VR/AR 的关键技术：虚拟现实建模；计算机图形学和计算机动画。

7、信息化应用

- ❖ 关注普遍引入监理服务的领域，即数字政府、数字经济、智慧城市和数字乡村。
- ❖ 数字政府
 - ① 特征：信息传播的平等化、社会生活的全面数据化、政府服务的精准化、政府治理的智慧化。
 - ② 发展历程：第一阶段，电子政府；第二阶段，网络政府； 第三阶段，数字政府。
 - ③ 数字政府应用场景：政务服务一网通办；城市治理一网统管；政府运行一网协同。
- ❖ 数字经济
 - ① 数字经济“四化”框架，即数字产业化（**先导产业**）、产业数字化（**主阵地**）、数字化治理（**治理模式**）和数据价值化（**关键生产要素**）。
 - ② 数字经济三大定律：梅特卡夫定律（网络价值等于其节点数的平方）、摩尔定律（计算机芯片的处理能力每18个月就翻一番）、达维多定律（进入市场的第一代产品能够自动获得50%市场份额）。
 - ③ 五个基本特征：数字化、网络化、智能化、商业化、共享化。
- ❖ 智慧城市
 - ① 我国城市数字化经历了从数字城市、智慧城市到新型智慧城市、数字孪生城市的发展历程。
 - ② 新型智慧城市的特征：新型智慧城市具有开放、共建、共享、服务均等化、城市特色化的特征。
 - ③ 新型智慧城市应用系统涵盖：智慧政府、智慧民生、智慧交通、智慧产业、智慧经济等的智慧化。
 - ④ 智慧城市信息基础设施包括：**城市骨干网、无线城市、三网融合**（电信网、广播电视网和互联网）。
- ❖ 数字乡村：就是在农村普及数字化、信息化的各种发展模式。数字乡村建设涵盖的内容可以归纳为乡村信息基础设施、乡村要素数据信息互通、乡村产业数字化、乡村治理数字化、乡村民生数字化、生态宜居数字化六个方面。

第二章 信息系统工程

一、信息系统

- ❖ 信息系统是一组相互关联的元素或组件，它们收集（输入）、操作（处理）、存储和传播（输出）数据与信息，并提供满足目标的反馈机制。
- ❖ 信息系统的五个基本功能包括：输入、存储、处理、输出和控制。
- ❖ 诺兰将计算机信息系统的发展道路划分为六个阶段：**初始阶段、传播阶段、控制阶段、集成阶段、数据管理阶段和成熟阶段。**
- ❖ 信息系统的物理结构

具体分类	概念
集中式 结构	<p>(1) 优点：资源集中，便于管理，资源利用率较高。</p> <p>(2) 缺点：集中式架构的维护与管理越来越困难，不利于调动用户在信息系统建设过程中的积极性、主动性和参与感；资源过于集中会造成系统的脆弱，易使整个系统瘫痪。</p>
分布式 结构	<p>(1) 优点：可以根据应用需求来配置资源，提高信息系统对用户需求与外部环境变化的应变能力，系统扩展方便，安全性好，某个节点所出现的故障不会导致整个系统停止运作。</p> <p>(2) 缺点：由于资源分散，且又分属于各个子系统，系统管理的标准不易统一，协调困难，不利于对整个资源的规划与管理。</p> <p>(3) 特性：分布性、对等性、并发性、缺乏全局时钟、故障多样</p>

- ❖ 信息系统的通用结构自底向上可分为
 - ① **机房基础设施**：指机房基础环境、安防系统、电气系统、精密空调系统、环境检测系统、消防系统。
 - ② **物理资源**：指网络、服务器、存储、终端、外设等硬件。
 - ③ **虚拟资源**：指网络资源、计算资源、存储资源等。
 - ④ **平台资源**：指支撑应用系统运行的基础软件，如操作系统、数据库、中间件等。
 - ⑤ **应用**：指面向各类应用的软件系统。如财务软件、人力资源管理软件、办公自动化软件、监控软件、流程管理软件、安全分析软件等。
 - ⑥ **数据**：主要是指业务数据、运维数据、安全数据等。
- ❖ 从工程建设的角度：信息网络系统、信息资源系统和信息应用系统。
- ❖ 信息系统建设原则
 - ① **高层管理人员介入原则**：深度介入信息系统开发建设以及运行是CIO的职责所在
 - ② **用户参与开发原则**：有确定的范围；参与全过程；深度参与
 - ③ **自顶向下规划原则**
 - ④ **工程化原则**
 - ⑤ 其他原则：创新性、整体性、发展性、经济性等原则。

二、系统工程（组织管理技术）

1、系统工程方法

- ❖ **系统工程方法**
 - (1) **霍尔三维结构**：由**时间维、逻辑维和知识维**组成的三维空间结构。
 - ① 时间维分为规划、制定方案、研制、生产、安装、运行、更新七个时间阶段。
 - ② 逻辑维包括问题确定、目标确定、系统综合、系统分析、方案选择、评价、决策、实施计划七个逻辑步骤。
 - ③ 知识维需要运用包括工程、医学、建筑、商业、法律、管理、社会科学、艺术在内的各种知识和技能。
 - (2) **切克兰德方法**
 - ① 核心不是“最优化”，而是“**比较**”与“**探寻**”。

监理师讲义第一篇-羽仪老师

② 工作过程的七个步骤：认识问题；初步定义；建立概念模型；比较及探寻；选择；设计与实施；评估与反馈。

(3) 并行工程方法：并行工程强调以下三点：

- ① 在产品的设计开发期间将概念设计、结构设计、工艺设计、最终需求等结合起来。
- ② 各项工作由与此相关的项目小组完成。
- ③ 依据适当的信息系统工具，反馈与协调整个项目的进行。

(4) 综合集成法

- ① 分类：简单系统和巨系统
- ② 开放的复杂巨系统的主要性质：开放性、复杂性、进化与涌现性、层次性、巨量性。

(5) WSR 系统方法

- ① **物理、事理、人理**三者合理配置、有效利用以解决问题的一种系统方法论。
- ② 物理主要应用自然科学中的各种科学方法；事理主要使用各种运筹学、系统工程、管理科学、控制论和一些数学方法；人理可以细分为关系、感情、习惯、知识、利益等。

2、系统工程生命周期

- ❖ 生命周期的七个阶段：**探索性研究阶段；概念阶段；开发阶段；生产阶段；使用阶段；保障阶段；退役阶段。**
- ❖ 生命周期方法：**计划驱动方法**（整个过程始终遵守规定流程的系统化方法）；**渐进迭代式开发**（适用于较小的、不太复杂的系统；重点在于灵活性）；**精益开发**（动态的、知识驱动的、以客户为中心）；**敏捷开发**（关键目标在于灵活性）。
- ❖ 信息系统生命周期为五个阶段：**系统规划；系统分析；系统设计；系统实现；系统运行与评价。**

三、软件工程

1、软件架构

❖ 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**。

❖ 软件架构风格

名称	说明
数据流风格	包括批处理序列和管道/过滤器
调用/返回风格	包括主程序/子程序、数据抽象和面向对象，以及层次结构
独立构件风格	包括进程通信和事件驱动的系统
虚拟机风格	包括解释器和基于规则的系统
仓库风格	包括数据库系统、黑板系统和超文本系统

- ❖ 在架构评估过程中，**评估人员所关注的是系统的质量属性**。
- ❖ 评估方式主要可以归纳为以下三类：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**。
- ❖ 基于场景的方式主要包括：架构权衡分析法、软件架构分析法和成本效益分析法。

2、需求的层次

- ❖ **常规需求**。用户认为系统**应该做到**的功能或性能，实现越多用户会越满意。
- ❖ **期望需求**。用户想当然**认为系统应具备**的功能或性能，但并不能正确描述自己想要得到的这些功能或性能需求。如果期望需求没有得到实现，会让用户感到不满意。
- ❖ **意外需求**。意外需求也称为兴奋需求，是用户要求范围外的功能或性能，实现这些需求用户会更高兴，但不实现也不影响其购买的决策。

3、需求获取

- ❖ **需求获取**是确定和理解不同的项目干系人对系统的需求和约束的过程。
- ❖ 常见的需求获取方法包括用户访谈、问卷调查、采样、会议讨论法、界面原型法、情节串联板、联合需求计划等。

4、需求分析

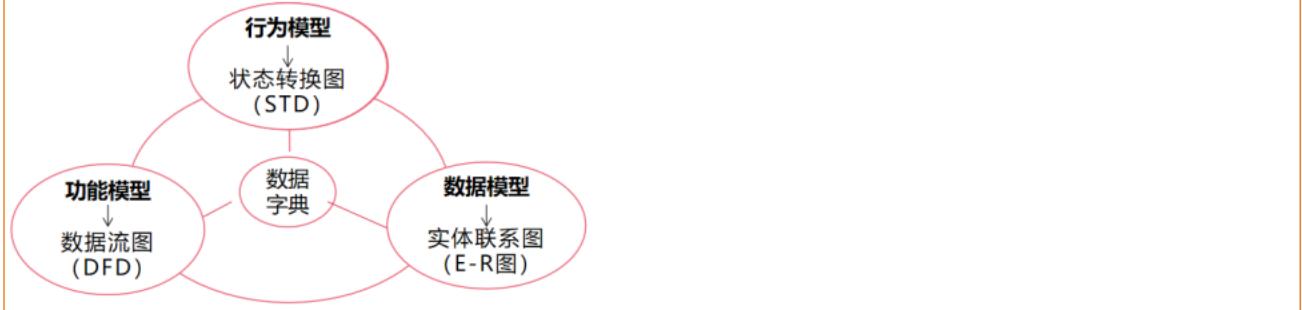
- ❖ **需求分析**将提炼、分析和审查已经获取到的需求，以确保所有的项目干系人都明白其含义并找出其中的错误、遗漏或其他不足的地方。

监理师讲义第一篇-羽仪老师

- 在需求获取阶段获得的需求是杂乱的。一个好的需求应该具有无二义性、完整性、一致性、可测性、确定性、可跟踪性、正确性、必要性等特性。

(1) 结构化分析

- 使用 SA (结构化) 方法进行需求分析，其建立的模型的**核心是数据字典**，围绕这个核心，有三个层次的模型，如图所示：



(2) 面向对象分析

- 面向对象分析的基本任务是运用**面向对象(OOA)**方法，对问题域进行分析和理解，正确认识其中的事物及它们之间的关系，找出描述问题域和系统功能所需的类和对象，定义它们的属性和职责，以及它们之间所形成的各种联系。
- OOA 模型包括**用例模型和分析模型（分析阶段的核心工作）**。
 - 用例是一种描述系统需求的方法，使用用例的方法来描述系统需求的过程就是用例建模；
 - 分析模型描述系统的基本逻辑结构，展示对象和类如何组成系统（静态模型），以及它们如何保持通信，实现系统行为（动态模型）。

三、软件设计

软件设计是需求的延伸与拓展。需求阶段解决“做什么”的问题，而软件设计阶段解决“怎么做”的问题。同时，它也是系统实施的基础，为系统实施工作做好铺垫。

1、结构化设计

- 结构化设计(SD)是一种面向数据流的方法，其目的在于确定软件结构。它以 SRS 和 SA 阶段所产生的 DFD 和 数据字典 等文档为基础，是一个**自顶向下、逐层分解、逐步求精和模块化**的过程。SD 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。
- 从管理角度讲，其分为**概要设计**和**详细设计**两个阶段。
- 在 SD 中，需要遵循一个基本的原则：**高内聚，低耦合**。
- 内聚表示**模块内部**各成分之间的联系程度；耦合表示**模块之间**联系的程度。

2、面向对象设计

- 面向对象设计(OOD)是 OOA 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。
- OOD 的主要任务是**对类和对象进行设计**，这是 OOD 中最重要的组成部分，也是最复杂和最耗时的部分。其主要包括类的属性、方法，以及类与类之间的关系。OOD 的结果就是设计模型。对于 OOD 而言，在支持可维护性的同时，提高软件的可复用性是一个至关重要的问题，如何同时提高软件的可维护性和可复用性，是 OOD 需要解决的核心问题之一。

3、设计模式

分类	解析
处理范围不同	分为类模式和对象模式 (1) 类模式处理类和子类之间的关系， 静态关系 (2) 对象模式处理对象之间的关系； 动态性
目的和	分为创建型模式、结构型模式和行为型模式三种 (1) 创建型模式主要用于创建对象，包括工厂方法模式、抽象工厂模式、原型模式、单例模式和建造者模式等；

监理师讲义第一篇-羽仪老师

用途不同	(2) 结构型模式 主要用于处理类或对象的组合，包括适配器模式、桥接模式、组合模式、装饰模式、外观模式、享元模式和代理模式等 (3) 行为型模式 主要用于描述类或对象的交互以及职责的分配，包括职责链模式、命令模式、解释器模式、迭代器模式、中介者模式、备忘录模式、观察者模式、状态模式、策略模式、模板方法模式、访问者模式等
------	---

四、软件实现

1、软件编码

- ❖ 程序设计风格：源程序文档化、数据说明、语句结构和输入/输出方法。
- ❖ 程序复杂性度量：定量度量软件的性质
- ❖ 编码效率包括：程序效率、算法效率、存储效率和 I/O 效率。

2、软件测试

(1) 测试的方法

测试方法	具体分类	说明
静态测试		(1) 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。静态测试包括对文档的静态测试和对代码的静态测试。 (2) 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、代码走查、代码审查和静态分析 工具等方法。
动态测试	白盒测试 (结构测试)	(1) 测试人员对软件内部结构和实现细节 有详细的了解 。 (2) 优点 ：是可以检查程序内部的逻辑和结构，并且可以更容易地找到潜在问题。 (3) 缺点 ：时间消耗较大，因为需要深入分析源代码，并可能因过于关注细节而忽略用户体验和功能需求。
	黑盒测试 (功能测试)	(1) 测试人员 不关心软件内部的实现细节 ，而是只关注程序的输入和输出结果。 (2) 优点 ：是可以从用户角度发现问题，并且相对于白盒测试更容易实施。 (3) 缺点 ：是无法检查程序内部的逻辑和结构，可能会漏掉一些潜在的错误。

五、部署交付

1、持续交付

- ❖ 持续交付是一个完全自动化的过程，当业务开发完成的时候，可以做到一键部署。持续交付提供了一套更为完善的解决传统软件开发流程的方案，主要体现在：
 - ① 在需求阶段，抛弃了传统的需求文档的方式，使用便于开发人员理解的用户故事；
 - ② 在开发测试阶段，做到持续集成，让测试人员尽早进入项目开始测试；
 - ③ 在运维阶段，打通开发和运维之间的通路，保持开发环境和运维环境的统一。

3、持续部署

- ❖ 容器技术目前是**部署中最流行的技术**，常用的持续部署方案有 Kubernetes+Docker 和 Matrix 系统两种。
- ❖ 完整的镜像部署包括三个环节：**Build—Ship—Run**。
 - ① Build：跟传统的编译类似，将软件编译形成 RPM 包或者 Jar 包；
 - ② Ship：将所需的第三方依赖和第三方插件安装到环境中；
 - ③ Run：就是在不同的地方启动整套环境。
- ❖ 在部署原则中提到**两大部署方式**
 - ① 蓝绿部署是指在部署的时候**准备新旧两个部署版本**，通过域名解析切换的方式将用户使用环境切换到新版本中，当出现问题的时候，可以快速地将用户环境切回旧版本，并对新版本进行修复和调整。
 - ② 金丝雀部署是指当有新版本发布的时候，**先让少量用户使用新版本**，并且观察新版本是否存在

监理师讲义第一篇-羽仪老师

在问题。如果出现问题，就及时处理并重新发布；如果一切正常，就稳步地将新版本适配给所有的用户。

六、数据工程

1、数据建模

- ❖ 概念模型（信息模型），它是按用户的观点来对数据和信息建模，也就是说，把现实世界中的客观对象抽象为某一种信息结构，这种信息结构不依赖于具体的计算机系统，也不对应某个具体的DBMS，它是概念级别的模型。
- ❖ 逻辑模型
 - ① 是在概念模型的基础上确定模型的数据结构，目前主要的数据结构有层次模型、网状模型、关系模型、面向对象模型和对象关系模型。其中，**关系模型成为目前最重要的一种逻辑数据模型**。
 - ② 关系模型数据操作主要包括查询、插入、删除和更新数据，这些操作必须满足关系的完整性约束条件。关系的完整性约束包括三大类型**实体完整性、参照完整性和用户定义的完整性**。其中实体完整性、参照完整性是关系模型必须满足的完整性约束条件，用户定义的完整性是应用领域需要遵照的约束条件体现了具体领域中的语义约束。
- ❖ 物理模型：是在逻辑数据模型的基础上，考虑各种具体的技术实现因素，进行数据库体系结构设计，**真正实现数据在数据库中的存放**。

2、数据建模

- ❖ 数据需求分析。数据需求分析通常不是单独进行的，而是融合在整个系统需求分析的过程之中。数据需求分析采用**数据流图**作为工具。
- ❖ 概念模型设计。
- ❖ 逻辑模型设计。
- ❖ 物理模型设计。

3、元数据：是关于数据的数据

4、数据标准化

- ❖ 数据标准化的主要内容包括**元数据标准化、数据元标准化、数据模式标准化和数据分类与编码标准化**。
- ❖ 数据标准化阶段
 - ① 确定数据需求。本阶段将产生数据需求及相关的元数据、域值等文件。
 - ② 制定数据标准。本阶段要处理“确定数据需求”阶段提出的数据需求。这个阶段将产生供审查和批准的成套建议。
 - ③ 批准数据标准。本阶段的数据管理机构对提交的数据标准建议、现行数据标准的修改或封存建议进行审查。
 - ④ 实施数据标准。本阶段涉及在各信息系统中实施和改进已批准的数据标准。

5、数据运维

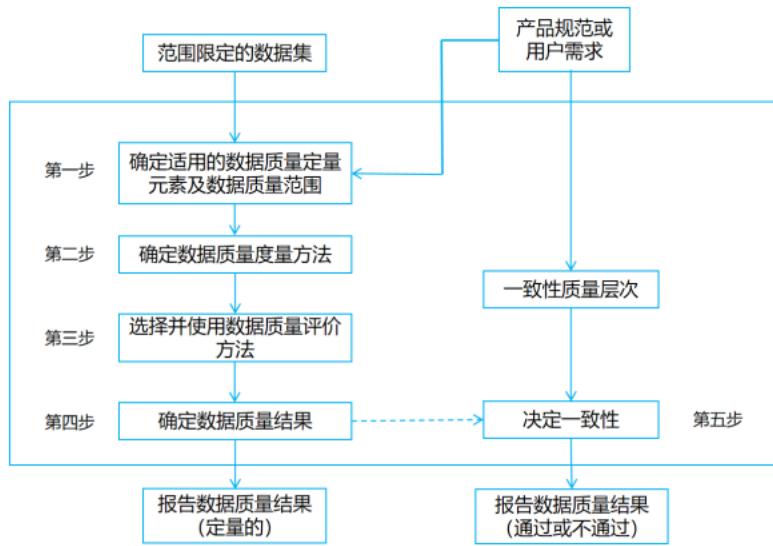
- ❖ 数据存储首先要解决的是存储介质的问题。存储介质是数据存储的载体，是数据存储的基础。存储介质并不是越贵越好、越先进越好，要根据不同的应用环境，合理选择存储介质。存储介质的类型主要有**磁带、光盘和磁盘**三种。
- ❖ 数据备份结构可以分为四种：**DAS 备份结构、基于 LAN 的备份结构、LANFREE 备份结构和 SERVER-FREE 备份结构**。
- ❖ 常见的备份策略主要有三种：**完全备份、差分备份和增量备份**。
- ❖ 数据容灾
 - ① 从技术上看，衡量容灾系统有两个主要指标，即**RPO(恢复点目标) 和 RTO(恢复时间目标)**，其中 RPO 代表了当灾难发生时允许丢失的数据量，而 RTO 则代表了系统恢复的时间。
 - ② **数据备份是数据容灾的基础**；容灾不是简单备份。真正的数据容灾就是要避免传统冷备份所具有先天不足，它在灾难发生时能全面、及时地恢复整个系统。
 - ③ 根据容灾系统保护对象的不同，容灾系统分为**应用容灾**和**数据容灾**两类。应用容灾用于**克服灾难对系统的影响**，保证应用服务的完整、可靠和安全等一系列要求，使得用户在任何情况下都能得

监理师讲义第一篇-羽仪老师

到正常的服务；数据容灾则关注于保证用户数据的高可用性，在灾难发生时能够保证应用系统中的数据尽量少丢失或不丢失，使得应用系统能不间断地运行或尽快地恢复正常运行。

6、数据质量评价与控制

- ❖ 数据质量元素分为数据质量定量元素和数据质量非定量元素。
- ❖ 数据质量评价过程（如图所示）



❖ 数据清理的三个步骤

- ① **数据分析**：是指从数据中发现控制数据的一般规则，比如字段域、业务规则等，通过对数据的分析，定义出数据清理的规则，并选择合适的清理算法。
- ② **数据检测**：是指根据预定义的清理规则及相关数据清理算法，检测数据是否正确，比如是否满足字段域、业务规则等，或检测记录是否重复。
- ③ **数据修正**：是指手工或自动地修正检测到的错误数据或重复的记录。

7、数据利用与开发

- ❖ 数据挖掘的目标是发现隐藏于数据之后的规律或数据间的关系，从而服务于决策。
- ❖ **数据挖掘的主要任务**：数据总结、关联分析、分类和预测、聚类分析和孤立点分析。
- ❖ 数据挖掘流程一般包括**确定分析对象、数据准备、数据挖掘、结果评估与结果应用** 5个阶段。为完成这些阶段的任务，需要不同专业人员参与其中，专业人员主要包括业务分析人员、数据挖掘人员和数据管理人员。
- ❖ **数据服务**
 - ① **数据目录服务**：是用来快捷地发现和定位所需数据资源的一种检索服务，是实现数据共享的重要基础功能服务之一。
 - ② **数据查询与浏览及下载服务**：是网上数据共享服务的重要方式，用户使用数据的方式有查询数据和下载数据两种。
 - ③ **数据分发服务**：是指数据的生产者通过各种方式将数据传送到用户的过程。数据分发服务的核心内容包括数据发布、数据发现、数据评价等。

8、数据库安全

❖ 数据库安全威胁

维度	表现方式		说明
安全后果	非授权的信息泄露		未获授权的用户有意或无意得到信息。通过对授权访问的数据进行推导分析获取非授权的信息也属于这一类。
	非授权的数据修改		包括所有通过数据处理和修改而违反信息完整性的行为。非授权修改不一定会涉及非授权信息泄露，因为即使不读取数据也可以进行破坏。
	拒绝服务		包括会影响用户访问数据或使用资源的行为。
威胁	无意	自然或意外灾害	如地震、水灾、火灾等。这些事故可能会破坏系统的软硬件，导致完整性破坏和拒绝服务。

监理师讲义第一篇-羽仪老师

方式	系统软硬件中的错误	这会导致应用实施错误的策略，从而导致非授权的信息泄露、数据修改或拒绝服务。
	人为错误	导致无意地违反安全策略，导致的后果与软硬件错误类似。
	授权用户	他们滥用自己的特权造成威胁。
	恶意代理	病毒、特洛伊木马和后门是这类威胁中的典型代表。

- ❖ 数据库安全机制：包括用户的身份认证、存取控制、数据库加密、数据审计、推理控制等内容。

9、系统集成

- ❖ 系统集成的内容包括技术环境的集成、数据环境的集成和应用程序的集成。
- ❖ 在技术上需要遵循的基本原则包括：**开放性、结构化、先进性和主流化**。

10、网络集成

- ❖ **传输子系统**
 - ① **传输是网络的核心**，是网络信息的“公路”和“血管”。
 - ② 目前主要的传输介质分为无线传输介质和有线传输介质两大类。常用的无线传输介质主要包括无线电波、微波、红外线等，常用的有线传输介质主要包括双绞线、同轴电缆、光纤等。
- ❖ **交换子系统**：网络按所覆盖的区域可分为局域网、城域网和广域网，由此网络交换也可以分为局域网交换技术、城域网交换技术和广域网交换技术。
- ❖ **安全子系统**：
 - ① 使用防火墙技术，防止外部侵犯。防火墙技术主要有分组**过滤技术**、**代理服务器**和**应用网关**等。
 - ② 使用数据加密技术，防止任何人从通信信道窃取信息。目前主要的加密技术包括对称加密算法(如 DES)和非对称加密算法(如 RSA)。
 - ③ 访问控制，主要是通过设置口令、密码和访问权限保护网络资源。
- ❖ **网管子系统**：关键的任务便是保证网络良好地运行。
- ❖ **网络操作系统**：主要任务是调度和管理网络资源，并为网络用户提供统一、透明使用网络资源的手段。
- ❖ **服务器集成**：选择网络服务器时要考虑以下因素：①CPU 的速度和数量；②内存容量和性能；③总线结构和类型；④磁盘容量和性能；⑤容错性能；⑥网络接口性能；⑦服务器软件等。
- ❖ **服务子系统**。网络服务是网络应用最核心的问题

11、数据集成

- ❖ 数据集成处理的主要对象是系统中各种异构数据库中的数据。数据仓库技术是数据集成的关键。
- ❖ 数据集成可以分为**基本数据集成、多级视图集成、模式集成和多粒度数据集成**（是异构数据集成中最难处理的问题）四个层次。
- ❖ 异构数据集成：数据集成的目的是为应用提供统一的访问支持，因此集成后的数据必须保证一定的完整性，包括数据完整性和约束完整性。

12、软件集成

- ❖ DCOM 作为 COM 的扩展，不仅继承了 COM 的优点，而且针对分布环境提供了一些新的特性，如位置透明性、网络安全性和跨平台调用等。
- ❖ COM+为 COM 的新发展或 COM 更高层次上的应用，其底层结构仍然以 COM 为基础，几乎包容了 COM 的所有内容。
- ❖ **.NET 开发框架**



监理师讲义第一篇-羽仪老师

- ❖ J2EE 的体系结构：客户端层、服务器端组件层、EJB 层、信息系统层。

13、应用集成

- ❖ 用语言做比喻，语法、语义、语用三者对应到系统集成技术上，**网络集成解决语法的问题，数据集成解决语义的问题，应用集成解决语用的问题。**
- ❖ 对应用集成的技术要求
 - ① 具有应用间的互操作性：应用的互操作性提供不同系统间信息的有意义交换。此外，它还提供系统间功能服务的使用功能，特别是资源的动态发现和动态类型检查。
 - ② 具有分布式环境中应用的可移植性：提供应用程序在系统中迁移的潜力并且不破坏应用所提供的或正在使用的服务。这种迁移包括静态的系统重构或重新安装以及动态的系统重构。
 - ③ 具有系统中应用分布的透明性：分布的透明性屏蔽了由系统的分布所带来的复杂性。
- ❖ 系统集成栈

应用集成（互操作性）

数据集成（互通）

网络集成（互连）

14、安全系统

- ❖ 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”。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。

轴	三维模型	三维模型刻度组成
X 轴	安全机制	基础设施实体安全，平台安全，数据安全，通信安全，应用安全，运行安全，管理安全，授权和审计安全，安全防范体系
Y 轴	OSI 网络参考模型	物理层，数据链路层，网络层，传输层，会话层，表示层，应用层
Z 轴	安全服务	对等实体认证服务，数据保密服务，数据完整性服务，数据源点认证服务，禁止否认服务，犯罪证据提供服务

15、安全服务

- ❖ 对等实体认证服务：用于两个开放系统同等层中的实体建立链接或 数据传输时，对对方实体的合法性、真实性进行确认，以防假冒。
- ❖ 数据保密服务：包括多种保密服务，为了防止网络中各系统之间的数据被 截获或被非法存取而泄密，提供密码加密保护。数据保密服务可提供链接方式和无链接方式两种数据保密，同时也可对用户可选字段的数据进行保护。
- ❖ 数据完整性服务：用以防止非法实体对交换数据的修改、插入、删除以及在数据交换过程中的数据丢失。
- ❖ 数据源点认证服务：用于确保数据发自真正的源点，防止假冒。
- ❖ 禁止否认服务：用以防止发送方在发送数据后否认自己发送过此数据，接收方在收到数据后否认自己收到过此数据或伪造接收数据，由两种服务组成：不得否认发送和不得否认接收。
- ❖ 犯罪证据提供服务：指为违反国内外法律法规的行为或活动，提供各类数字证据、信 息线索等。

16、工程体系架构

- ❖ 信息安全管理能力成熟度模型 (ISSE-CMM) 是一种衡量信息安全管理实施能力的方法，是 使用面向工程过程的一种方法 ISSE-CMM 主要适用于**工程组织、获取组织和评估组织**。
- ❖ ISSE 将信息安全管理实施过程分解为**工程过程、风险过程和保证过程**三部分。

17、ISSE-CMM 体系结构

- ❖ ISSE-CMM 的体系结构可以在整个信息安全管理范围内决定信息安全管理组织的 成熟性。这个体系结构的目标是落实安全策略，从管理和制度化方面突出信息安全管理的基本特征。为此，该模型采用两维设计，**其中的一维是“域”， 另一维是“能力”**。

(1) 域维/安全工程过程域

- ❖ 由基本实施组成 11 个安全工程过程域：实施安全控制、评估影响、评估安全风险、 评估威胁、

监理师讲义第一篇-羽仪老师

评估脆弱性、建立保证论据、协调安全、监控安全态、提供安全输入、确定安全需求、验证和证实安全。

- ❖ 11个与项目和组织实施有关的过程域：保证质量、管理配置、管理项目风险、和控制技术工程项目、规划技术工程项目、定义组系统工程过程、改进组织的系统工程过程、管理产品线的演变、管理系统工程支持环境、提供不断更新技能和知识、与供应商协调

(2) 能力维/公共特性

级别	公共特性
Level 1: 非正规实施级	执行基本实施
Level 2: 规划和跟踪级	规划执行
	规范化执行
	验证执行
	跟踪执行
Level 3: 充分定义级	定义标准化过程
	执行已定义的过程
	协调安全实施
Level 4: 量化控制级	建立可测度的质量目标
	对执行情况实施客观管理
Level 5: 持续改进级	改进组织能力
	改进过程的效能

第三章 信息网络系统

一、信息网络系统体系框架和 OSI 七层模型

1、信息网络系统体系框架模型

信息网络系统体系框架	内容
网络传输平台	包括传输、路由、交换、有线和无线接入等设备和系统。
网络和应用服务平台	包括域名解析系统(DNS)、地址分配系统、业务应用系统(例如 OA、WWW、电子邮件、语音会议、视频会议、VOD、人脸识别等系统)。
安全服务平台	包括信息加解密、防火墙、入侵检测、漏洞扫描、病毒查杀、安全审计、数字证书等。
网络管理和维护平台	负责整个信息网络系统的管理和维护,如果对外提供业务服务,还需要专门的运营系统。
环境系统	包括机房建设、环境监控、智能安防、节能降耗、综合布线等。

2、开放系统互连(OSI) 七层模型

层级	含义
物理层	最底层 , 规定了承载其上的各层发送和接收具体数据的物理硬件方法。包括路由器、交换机、各种传输设备、服务器、计算机、移动基站、手机等设备之间, 需要特定的物理信道进行基本数据的发送和接收。
数据链路层	负责将物理层透明传输过来的比特流组织成有意义的数据包, 规定了数据包的格式和大小, 规范了发送和接收特定数据包的寻址方式、同步控制、差错控制和流量控制机制。
网络层	网络层定义和规范了不同网络间的通信规则, 包括寻址和路由选择, 链路连接的建立、保持和终止等。
传输层	是为会话层提供建立可靠的端到端的透明数据传输机制, 根据发送端和接收端的地址定义一个跨网络的多个设备甚至是跨多个网络的逻辑连接(并非物理层所处理的物理连接), 同时完成发送端和接收端的差错纠正和流量控制功能。
会话层	会话层的基本功能是向两个表示层实体提供建立、管理、拆除和使用连接的方法, 这种表示层之间的连接就叫作会话。
表示层	表示层的典型服务包括数据翻译(例如信息编解码、加密解密等)、格式化(例如数据格式转换、数据压缩等)、语法选择(语法的定义及不同语言之间的翻译)等。
应用层	最顶层 , 直接向用户提供信息通信服务, 例如常见的互联网网站访问服务(万维网)、邮件服务、视频会议服务、游戏服务等, 都会对应不同的应用程序和相应的服务协议, 万维网服务使用的就是HTTP(超文本传输)协议。

二、TCP/IP 协议族

1、TCP/IP 协议族

层级	主要常见的协议
应用层	协议有网络远程访问协议(Telnet)、文件传输协议(FTP)、简单电子邮件传输协议(SMTP)等, 用来接收来自传输层的数据, 或按不同的应用要求与方式将数据传输至传输层。
传输层	协议有用户数据报协议(UDP)、TCP, 负责上面应用层协议发送和接收具体数据的机制和过程。 TCP 是面向连接的协议, 在收发数据前, 必须和对方建立可靠的连接; UDP 是非连接协

监理师讲义第一篇-羽仪老师

	议，传输数据之前源端和终端不建立连接，并不保证数据一定能传送到，也不保证按顺序传输。
互联网络层	协议有 Internet 控制报文协议 (ICMP)、IP、Internet 组管理协议 (IGMP)，主要负责网络中数据包的具体传输等。该层最基本的协议是 IPv4 和 IPv6 。
物理和数据链路层	主要协议有地址解析协议 (ARP)、反向地址转换协议 (RARP)，主要功能是提供链路管理错误检测、对不同通信媒介的有关信息细节问题进行有效处理等。

2、IPv4 协议和 IPv6 协议

(1) IPv4 地址

- ❖ 由 **32 位**二进制数组成，即由 4 个字节组成，为便于阅读和分析，通常称其为点分十进制表示法（例如 192.121.123.56）。IPv4 由网络位和主机位两大部分组成，前者用于标识网络，后者用于标识网络内部不同主机。
- ❖ IPv4 地址分为 A、B、C、D、E 五类，A、B、C 类地址用于不同类型的网络规模，D 类地址专门用于组播地址。
 - ① **A类地址**适用于**大型**网络建设，支持 126 个网络，每个网络最多支持 16 777214 个主机地址；
 - ② **B类地址**适用于**中型**网络建设，支持 16384 个网络，每个网络最多支持 65534 个主机地址；
 - ③ **C类地址**适用于**小型**网络建设，支持 209 万余个网络，每个网络最多支持 254 个主机地址。
- ❖ NAT 一般在家庭网关、企业网关或者接口路由器等设备上实现。使用私网地址的主机需要通过地址转换技术 (NAT) 与公网 IPv4 地址的主机进行通信。
- ❖ 路由是指路由器从一个接口上收到数据包，根据数据包目的地址进行定向并转发到另一个接口的过程。TCP/IP 的互联网络层实现不同网络中两个主机设备之间的数据传输，路由发挥了重要的作用，每一个 IP 数据包从发送端源头到接收端目的地，中间要经过若干路由器（或其他互联网络层设备）。路由器获得路由条目的方式（即路由的类型）包括：**直连路由、静态路由、动态路由**。

(2) IPv6 协议

- ❖ 由 **128 位**二进制数组成，是 IPv4 地址长度的 4 倍。解决 IPv4 地址不够问题。

三、网络传输平台

- ❖ 负责信息的传输，一般由**传输媒介、传输设备、路由设备、交换设备、有线接入设备、无线接入设备和相关系统**组成。传统的网络传输设备是软件和硬件一体，当前的趋势是软件和硬件分离，例如软件定义网络 (SDN)。

1、网络传输平台的一般架构和主要技术

- ❖ **网络传输媒介：**处于 OSI 的物理层。传输媒介一般分为有线和无线两大类，有线媒介包括光纤、双绞线、同轴电缆等；无线媒介一般按照波长来区分，包括长波 (3~30kHz)、中波 (0.03~3MHz)、短波 (3~30MHz)、超短波 (30~300MHz)、微波 (0.3~300GHz) 等。
- ❖ **网络传输技术：**基于光纤的同步数字序列 SDH、准同步数字序列 PDH、密集波分复用 DWDM，基于同轴电缆的混合光纤同轴电缆 HFC，基于无线媒介的 Wi-Fi、数字微波通信 DMC、卫星小数据站 VSAT、数字卫星通信系统、2G 到 6G 移动通信系统等。
- ❖ **网络路由、交换和组网技术，按照物理覆盖和管理范畴划分组网**

分类	内容
局域网 (LAN)	早期的局域网技术包括以太网、令牌环网、光纤分布式数据网等，目前基本采用各类 以太网交换机 组建局域网，包括百兆、千兆、万兆以太网交换机。无线局域网 Wi-Fi 作为局域网的无线接入，例如手机等各类终端可以通过 Wi-Fi 接入局域网。 VLAN 是一种将局域网设备从逻辑上划分成一个个虚拟网段（更小的局域网）
城域网 (MAN)	一个城市范围内建设的网络。
广域网 (WAN)	跨地区、跨省市、跨国家的更大规模网络的统称，用来连接地区的城域网、省网 和各个国家的网络，Internet 是全球最大的广域网，它覆盖的范围遍布全世界。 当前广域网技术主要集中在 TCP/IP 领域，以及基于 TCP/IP 的多协议标记交换 (MPLS) 技术、虚拟专用网络 (VPN) 技术等。

监理师讲义第一篇-羽仪老师

有线、无线接入技术	随着光纤接入网（OAN）的部署和应用的普及，无源光网络（PON）逐步获得广泛应用，PON 有几种类型，包括以太网无源光网络（EPON）、千兆无源光网络（GPON）和 10G 无源光网络（10G-PON）。无线接入技术包括 Wi-Fi 和蓝牙等。
-----------	--

2、运营商网络架构

- ❖ 典型的运营商网络由全国骨干网、省级骨干网、城域网和接入网组成。
- ❖ 典型的城域网一般由**核心层、汇聚层和接入层**三层架构组成。核心层主要是路由器设备，汇聚层汇聚交换机设备，接入层面向各类园区、楼宇、住宅小区等商业、家庭和个人用户

3、4G/5G 移动通信

- ❖ 第 1 代：模拟蜂窝通信系统；第 2 代：数字蜂窝移动通信系统；第 3 代：数字移动通信系统
- ❖ **4G 移动通信**：高速率、高容量；网络频谱更宽；智能性能更高；兼容性能更平滑；更高质量、更低费用的通信；更好安全性。
- ❖ **5G 移动通信**
 - ① 5G 的三大类应用场景：即增强移动宽带、超高可靠低时延通信和海量机器类通信
 - ② 主要性能指标：峰值速率达到 10~20Gbit/s，以满足高清视频、虚拟现实等大数据量传输；空中 接口时延低至 1ms，满足自动驾驶、远程医疗等实时应用；具备百万连接/平方公里的设备连接能力，满足物联网通信；频谱效率比 4GLTE 提升 3 倍以上；连续广域覆盖和高移动性下，用户体验速率达到 100Mbit/s；流量密度达到 10Mbps/m2 以上；移动性支持 500km/h 的高速移动。

4、物联网组网技术

- ❖ 物联网架构可分为三层：**感知层、网络层和应用层**。

技术	解释
感知层	感知层的关键技术包括各种传感器技术、射频识别技术、条码、二维码技术、GPS 技术、NFC 技术、微机电系统技术等。
网络层	负责连通感知层和应用层，安全、顺畅地传输数据和指令。
应用层	承载着物联网应用的信息数据和业务处置逻辑，对感知层收集到的信息数据进行处理，对感知层下达相关处置指令。

四、网络和应用服务平台

- ❖ 负责服务于整个网络业务应用正常运行的各类通用的业务逻辑的实现。
- ❖ 常见的互联网服务有 E-mail 电子邮件服务、WWW 万维网服务、DNS 域名解析服务、FTP 文件传输服务、Telnet 远程登录服务等。

五、安全服务平台

信息网络系统 安全体系框架	解释
物理安全	包括环境安全、供配电系统、安防系统和消防系统四个部分。
网络安全	网络结构；访问控制；网络入侵防护；网络安全审计。网络安全设备和手段主要包括：防火墙、利用 Vlan 等技术进行安全域划分、入侵检测系统/入侵防御系统、网络安全审计。
主机安全	身份鉴别；访问控制；安全漏洞和攻击防御；主机安全审计等。
应用安全	身份和访问控制；应用安全漏洞；会话管理等。
数据安全	机密数据保护；数据备份恢复等。
安全管理	安全组织和责任；风险管理工作机制；应急处理工作机制；容灾备份工作机制；制定系统上线、切换办法、安全运维方案等。

六、网络管理和维护平台

- ❖ 网络管理的五大功能：故障管理、配置管理、性能管理、计费管理和安全管理。
- ❖ 网络管理和维护系统：网络管理系统的功能体系结构从下至上可以分为网元/网络层（最底层）、管理应用层和表示层。

七、环境系统建设

- ❖ 机房建设：机房装修、空调系统、电气系统、接地和防雷系统、消防系统、环境监控系统、节能降耗系统等。
- ❖ 综合布线：建筑群子系统、干线条系统和配线条系统。
- ❖ 监控系统：机房动力环境系统监控；机房系统/网络设备监控；机房门禁监控；机房环境消防监控。
- ❖ 节能降耗：选址是否有利于节能和降低能源成本；机房内部的规划布局能否提高空调使用效率；各种设备本身是否具备一定的节能降耗措施；基于人工智能等技术手段，对能源消耗情况进行智能分析和决策。

第四章 信息资源系统

一、数据资源平台

- ❖ 数据资源平台负责信息系统中的数据存储、计算和相关处理，硬件层面包括各类服务器、存储设备和备份设备等，软件层面包括操作系统、数据库系统、中间件系统、云计算系统、虚拟化系统、集群系统等。

1、计算服务器人工智能服务器

- ❖ **计算服务器：**主要承载和提供各类业务应用、管理服务及数据资源共享服务，计算服务器相比于普通的计算机，要求具有高速的CPU计算能力、较大的存储空间、长时间的可靠运行、强大的I/O外部数据吞吐能力以及更好的扩展性。
- ❖ **人工智能（AI）服务器：**人工智能包括算力、算法和数据三个方面；AI芯片分为训练芯片（注重强大的计算能力）和推理芯片（注重综合指标）。

2、数据存储和备份设备

- ❖ 目前市场上的存储产品主要有磁盘阵列、磁带机与磁带库、光盘库、存储区域网络（SAN）和网络附加存储（NAS）、对象存储、集中式存储和分布式存储等。
- ❖ **SAN：**采用光纤通道技术，高带宽、低延迟。但是价格较高，可扩展性较差。
- ❖ **NAS：**将存储设备通过标准网络拓扑结构（例如以太网）连接到一群计算机上。以文件为传输协议，通过TCP/IP实现网络化存储，可扩展性好、价格便宜、用户易管理，例如目前在集群计算中应用较多的NFS文件系统。
- ❖ **对象存储：**允许保留大量的非结构化数据；兼具SAN的高速直接访问磁盘的特点及NAS的分布式共享的特点。
- ❖ **集中式存储和分布式存储**
 - ① **集中式存储：**数据集中存储于中心节点，缺点就是核心部件集中，冗余性和扩展能力较差。
 - ② **分布式存储：**数据分散存储在多台独立的存储设备上，成本较低，扩展能力强，但是延迟高、有数据一致性问题。

3、主流数据库技术和系统

- ❖ 数据从组织的角度主要分为**结构化数据**和**非结构化数据**两类。
- ❖ **数据库系统分类**
 - ① **关系型数据库：**存储的格式可以直观地反映实体间的关系。关系型数据库有Oracle、DB2、MySQL、Microsoft SQL Server、Microsoft Access等多个品种。
 - ② **非关系型数据库（NoSQL）：**指**分布式的、非关系型的、不保证遵循ACID原则**的数据存储系统。NoSQL数据库适合文档形式、图片形式、文件形式等，使用灵活，应用场景广泛。非关系型数据库有MongoDB、HBase、Redis、Neo4j等。国产的非关系型数据库包括GaussDB(for Mongo)等。

4、典型数据中心组网技术

- ❖ 数据中心通常指的是互联网数据中心为互联网业务提供商、互联网内容提供商、政府、企业、媒体、各类网站甚至是个人提供大规模、高质量、安全可靠的专业化服务器托管、空间租用、云计算资源租用、业务应用部署等服务。
- ❖ **数据中心网络：**网络连接模块；业务接入模块；后台管理模块。
- ❖ **数据中心组网架构：**核心层；汇聚层；接入层。

二、云资源系统

- ❖ 云资源系统通过云计算，把基础设施、物理资源、虚拟资源、平台资源、应用及数等资源集合起来，作为服务资源池，以不同的服务模式，通过网络提供给用户。

1、云计算

- ❖ 云计算功能架构分为**服务和管理**两大部分
 - ① 在**服务**方面，主要向用户提供基于云的各种服务，共包含三种模式：**SaaS、PaaS 和 IaaS**。其中，SaaS层的作用是将应用主要基于Web的方式提供给用户；PaaS层的作用是将一个应用的开发

监理师讲义第一篇-羽仪老师

和部署平台作为服务提供给用户；IaaS 层的作用是将各种底层的计算(如虚拟机)和存储等资源作为服务提供给用户。

② 在管理方面，主要提供云相关的管理功能，以确保整个云计算中心能够安全、稳定地运行，并且能够被有效地管理。

- ❖ 云计算层次结构：显示层、中间层、基础设施层和管理层。
- ❖ 云计算关键技术：虚拟化技术、分布式数据存储技术、资源管理技术、云计算平台管理技术和多租户隔离技术等。
- ❖ 云计算运营模式
 - ① 云计算服务角色：云服务提供商、云服务消费者、云服务代理商、云计算审计、服务承运商。
 - ② 云计算责任模型：云服务责任承担能力评估、云服务安全使用能力评估。
- ❖ 云计算的基础设施、物理硬件、资源抽象和控制层都处于云服务提供者的完全控制下，所有安全责任由云服务提供者承担。应用软件层、软件平台层、虚拟化计算资源层的安全责任则由双方共同承担，越靠近底层的云计算服务(即 IaaS)，客户的管理和安全责任越大；反之，云服务提供者的管理和安全责任越大。在 IaaS 中，客户的责任是最大的，SaaS 中客户的责任最小，PaaS 中客户的责任介于 IaaS 和 SaaS 之间。
- ❖ 云计算服务的交付：模式一：组织所有，自行运营；模式二：组织所有，运维外包；模式三：组织所有，运维外包，外部运行；模式四：组织租赁，外部运行，资源独占；模式五：组织租赁，外部运行，资源共享调度；模式六：公共云服务。

2、云服务产品

- ❖ 云服务器特点：高可用性、稳定性与安全性、弹性。
- ❖ 存储类产品

	块存储	对象存储
概念	高可用、高可靠、低成本、可定制化的块存储设备	通过云提供的海量、安全、低成本、高可靠的云存储服务
特点	弹性可扩展；多存储类型；多存储类型；简单易用；快照备份；分类。	访问灵活；视频录像秒级回放；提供多维度、多层次的安全防护与访问控制；提供安全令牌服务；提供跨区域复制功能实现数据异地容；图片处理；让客户的音视频文件轻松应对各种终端设备；内容加速分发。

- ❖ 网络类产品

	专有网络 VPC	负载均衡	弹性公网 IP
特点	一个独立的虚拟化网络，可提供独立的路由器和交换机组件，实现彻底逻辑隔离。	高可用；低成本。	灵活独立的公网 IP 资源；动态绑定和解绑；按需购买和灵活管理。
应用场景	本地数据中心+云上业务的混合云模式、多租户的安全隔离、主动访问公网的抓取类业务。	高访问量的业务、横向扩张系统、消除单点故障、同城容灾(多可用区容灾)。	业务系统高可靠的需求、带宽使用成本降低的需求、保证系统实时性的需求、游戏业务精确分区和游戏玩家多房间接入需求。

- ❖ 数据库类产品：
 - ① 云关系型数据库的功能特点有：便宜易用、高性能、高安全性、高可靠性
 - ② 云关系型数据库的应用场景有：异地容灾、数据多样化存储、持久化缓存数据、大数据分析。
- ❖ 安全类产品
 - ① DDoS 高防 IP 的应用场景：DDoS 高防 IP 可服务于云内及云外的所有客户，主要使用场景包括金融、娱乐(游戏)、媒资、电商、政府等对用户体验的实时性要求较高的业务。
 - ② Web 应用防火墙(WAF)应用场景：DDoS 高防 IP 可服务于云内及云外的所有客户，主要使用场景包括金融、娱乐(游戏)、媒资、电商、政府等对用户体验的实时性要求较高的业务。
- ❖ 管理工具类产品的应用场景：云服务监控、系统监控、及时处理异常场景、及时扩容场景、站点监控、自定义监控等。

3、云服务质量评估

- ❖ 云服务的质量包括各种功能性和非功能性的交付水平。

监理师讲义第一篇-羽仪老师

- ❖ 云主机服务质量评估：通用处理能力；系统处理能力；行业应用承载能力；交付服务内容评估。
- ❖ 对象存储服务质量评估：数据存储的持久性；数据可销毁性；数据可迁移性；数据私密性；数据知情权；服务可审查性；服务功能；服务可用性。

4、IaaS 模式（基础设施即服务）

- ❖ 资源抽象：主要是将下层的物理硬件资源统一进行抽象，抽象成和单个物理硬件无关的资源集合，上层无须关心物理机器的型号，**只需专注于具体的资源即可**。
- ❖ 计算负载管理：云计算主机是通过云计算技术将 IT 设备的硬件、存储及网络等资源统一虚拟化为相应的资源池，再从资源池分割成独立的虚拟主机（服务器）的产品。
- ❖ 数据存储管理：根据不同的应用环境，通过采取合理、安全、有效的方式将数据保存到某些介质上，并能保证有效地访问。
- ❖ 网络管理：监测、控制和记录网络资源的性能和使用情况，以使网络有效运行。
- ❖ 安全服务：主要内容包括安全机制、安全连接、安全协议和安全策略等。重要的数据采用 **RAID 0+1** 方式存储。
- ❖ 云服务计费平台：通过采集 IaaS、PaaS 和 SaaS 服务资源数据，来计算出所提供的服务资源费用。

5、PaaS 模式（平台即服务）

- ❖ 中间件：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。
- ❖ 中间件功能：通信支持；应用支持；公共服务。
- ❖ 中间件分类

分类	说明
事务式中间件 (事务处理管理程序)	当前应用最广泛的中间件之一，其主要功能是提供联机事务处理所需要的通信、并发访问控制、事务控制、资源管理、安全管理、负载平衡、故障恢复和其他必要的服务。
过程式中间件 (事务处理管理程序)	过程式中间件一般从逻辑上分为两部分： 客户机和服务器 。
面向消息中间件 (消息中间件)	(1) 利用高效可靠的 消息机制 ，来实现不同应用间大量的数据交换。 (2) 消息中间件的通信模型有两类： 消息队列和消息传递 。
面向对象中间件 (分布对象中间件)	是分布式计算技术和面向对象技术发展的结合。分布对象模型是面向对象模型在分布异构环境下的自然拓展。
Web 应用服务器	J2EE 架构 是应用服务器方面的主流标准。

- ❖ **数据中台 (Paas)**：包括基础中台、技术中台、数据中台和业务中台，它们合称为“大中台”。
- ❖ 容器：容器是没有自己的操作系统的，直接共享宿主机的内核，优势：“轻量化”。

6、SaaS 模式（软件即服务）

- ❖ 定义：SaaS，软件部署在云端，让用户通过互联网来使用它，即云服务提供商把系统的应用软件层作为服务出租出去，而消费者可以使用任何云终端设备接入计算机网络，然后通过网页浏览器或者编程接口使用云端的软件。SaaS 依托于互联网
- ❖ 面向个人用户的服务包括：账务管理、文件管理、照片管理、在线文档编辑、表制作、资源整合、日程表管理、联系人管理等；
- ❖ 面向企业用户的服务包括：在线存储管理、网上会议、项目管理、CRM、ERP、人力资源管理 (HRM)、销售管理 (STS)、协调办公系统 (EOA)、财务管理、在线广告管理，以及针对特定行业和领域的应用服务等。
- ❖ 适合做 SaaS 应用软件的特点：复杂、高效的多用户支持、模块化结构、多租户、多币种、多语言、多时区支持、非强交互性软件。
- ❖ 适合云化并以 SaaS 模式交付给用户的软件包括：企事业单位的业务处理类软件、协同工作类软件、办公类软件、软件工具类。
- ❖ SaaS 模式具有的优势具体如下：云终端少量安装或不用安装软件、有效使用软件许可证、数据安全性得到提高、人们再也不用复制数据并随身携带、有利于消费者摆脱 IT 运维的技术“泥潭”而专注于自己的核心业务、消费者能节约大量前期投资。

监理师讲义第一篇-羽仪老师

- ❖ SaaS 云服务的实际应用包括：电子邮件和在线办公软件、计费开票软件、CRM、协作工具、CMS、财务软件、销售工具、ERP、在线翻译等。

7、云数据中心

- ❖ 云计算数据中心包括计算资源、存储资源、电力资源、交互能力，以及弹性、负载均衡及虚拟化资源部署方式，而所有的计算、存储及网络资源都是以服务的方式提供的。
- ❖ 云数据中心五大要素：**面向服务；资源池化；高效智能；按需供给；低碳环保。**
- ❖ 总体架构：云数据中心架构自下而上由数据中心机房层（基础）、物理资源层、基础设施层、平台服务层、软件服务层、终端用户层六大部分构成。

核心技术	内容
网络架构设计	良好的可扩展性、多路径容错能力、低时延、高带宽网络传输能力、模块化设计、网络扁平化、绿色节能。
网络融合技术	光纤以太网通道技术、数据中心桥接技术及多链接透明互连技术等。
网络性能测试	(1) 网络性能测试一般是利用如 ICMP 和 TCP 等网络协议开展测试，主要有 主动测试、被动测试及主、被动这两种测试相结合的测试方法。 (2) 主动测试比较适合对端到端的时延、丢包及时延变化等参数的测量，而 被动测试 则更适用于对路径吞吐量等流量参数的测试
虚拟化技术	对计算机系统软硬件资源的划分和抽象。分为 硬件仿真技术、全虚拟化技术、半虚拟化技术。
安全技术	安全管理包括管理制度、管理机构、人员管理、系统建设、系统运维。
节能技术	电能利用效率（PUE）是评价数据中心能源效率的指标，是数据中心消耗的所有能源与 IT 负载使用的能源之比。PUE 的值越接近于 1，表示一个数据中心的绿色化程度越高。

8、规划与建设

- ❖ GB 50174《数据中心设计规范》分级的原则是从机房的使用性质、管理要求及重要数据丢失或网络中断在经济或社会上造成的损失或影响程度确定的，从高到低分为**A、B、C 三级**。
- ❖ 各类型的数据中心发展特点：城市数据中心向实时性和弹性化发展；边缘数据中心实现计算能力下沉；数据中心和网络建设协同布局；试点探索建设国际化数据中心。
- ❖ 建设项目分类：包括建筑工程、机房空调与配电网工程、供电系统工程、机房工艺工程等方面。
- ❖ 建设布局
 - ① **选址要求：**电力供给充足且稳定可靠、水源应充足、自然环境清洁、应远离产生粉尘、油烟、有害气体及生产或贮存具有腐蚀性、易燃、易爆物品的场所；应尽量远离无线电干扰源、电波发射塔等强磁干扰，远离强振动源和强噪声源；不宜建在公共停车库的正上方；宜建在住宅小区和商业区内。
 - ② **功能单元布局的总体原则：**整体性原则、安全性原则、模块化原则、灵活性及可扩展性原则、可维护性原则、经济性原则。

第五章 信息应用系统

一、信息应用系统的分类

- ❖ 信息应用系统分为**业务信息系统、管理信息系统与决策支持系统、专用信息系统**。
- ❖ **业务信息系统**
 - ① **企业资源规划（ERP）**：企业的所有资源包括三大流：**物流、资金流和信息流**。ERP 是对这三种资源进行全面集成管理的管理信息系统。
 - ② **电子商务**：公司与公司（B2B）、公司与消费者（B2C）、消费者与消费者（C2C）等。
- ❖ **管理信息系统与决策支持系统**
 - ① **管理信息系统（MIS）**：一个由人和计算机等组成的，能进行管理信息的收集、传输、存储、加工、维护和使用的系统。
 - ② **决策支持系统（DSS）**：帮助决策者利用数据和模型解决半结构化决策问题和非结构化决策问题的交互式系统，是服务于高层决策的管理信息系统，可分为专用 DSS、DSS 工具和 DSS 生成器。
- ❖ **专用信息系统**
 - ① **知识管理系统（KSM）**：用于存储和检索知识、改进协作、定位知识源、获取和使用知识的系统。
 - ② **专家系统（ES）**：一种模拟人类专家解决领域问题的计算机程序系统。
 - ③ **虚拟现实系统（VRS）**：需要特殊的接口设备，将模拟世界的景象、声音和感觉传送给用户。
 - ④ **办公自动化（OA）系统**：是一个人机结合的综合性的办公事务管理系统，或称办公事务处理系统。
- ❖ 信息应用系统之间的关系并不是取代关系，而是互相促进、共同发展的关系。在一个企业里，多种系统可能同时存在，也可能只有其中的一种或多种。更高级的是几种信息应用系统互相融合为一体。

二、典型信息应用系统

1、事务处理系统（TPS）

- ❖ **事务处理系统（TPS）**：对企业管理中日常事务所发生的数据进行输入、处理和输出。TPS 的数据处理周期由以下五个阶段构成：**数据输入、数据处理、数据库的维护、文件报表的生成和查询处理**。TPS 面对的是结构化程度很高的管理问题，因此可以采用结构化生命周期法来进行开发。

TPS 数据处理周期	内容
数据输入	第一阶段，数据输入方式有三种，即人工、自动及二者结合。
数据处理	(1) 批处理 ：将事务数据积累到一段时间后进行定期处理， 无法实时 。 (2) 联机事务处理 OLTP ：对所发生的事务数据进行 立即处理 ，并将处理结果提供给终端用户，成本高
数据库的维护	对数据库的访问形式分为四种：检索、修改、存入和删除。
文件报表的产生	TPS 的输出就是为终端用户提供所需的有关文件和报表。
查询处理	PS 支持终端用户的批次查询或联机实时查询，典型的查询方式是用户通过屏幕显示获得查询结果。对不同级别的用户授予不同的访问权限。

- ❖ **企业资源规划（ERP）**：为企业提供的功能：支持决策的功能；为处于不同行业的企业提供**有针对性的 IT 解决方案**；从企业内部的供应链发展为全行业和跨行业的供应链。

2、管理信息系统与决策支持系统

- ❖ **管理信息系统（MIS）**：管理信息系统由四大部件组成，即信息源、信息处理器、信息用户和信息管理者。**计算机实时处理的系统均属于闭环系统，而批处理系统一般属于开环系统**。
- ❖ **决策支持系统（DSS）**
 - ① DSS 的两种基本结构形式是**两库结构**和**基于知识的结构**。
 - ② DSS 的组成：**数据的重组和确认；数据字典的建立；数据挖掘和智能体；模型建立**。

3、专用信息系统

- ❖ **知识管理系统（KSM）**：获取、存储、共享和使用知识是任何知识管理的关键。知识被创建后，它通常存储在包含文档、报告、文件和数据库的知识库中。

监理师讲义第一篇-羽仪老师

❖ 专家系统 (ES)

① **特点:** 求解的问题是半结构化或非结构化问题；是人类专家在问题领域的推理，而不是模拟问题领域本身；包含数据级、知识库级和控制级**三级知识**；它面对的往往是**实际的问题**，而不是纯学术的问题；问题求解的**通用性较差**。

② **组成:** 知识库；综合数据库；推理机；知识获取；解释程序；人机接口。

❖ 虚拟现实系统 (VRS)：虚拟现实系统 (VRS) 使一个或多个用户能够在计算机模拟环境中移动和反应。虚拟现实模拟需要特殊的接口设备，将模拟世界的景象、声音和感觉传送给用户。

❖ 办公自动化 (OA) 系统

① **OA 的主要功能:** 事务处理；信息管理；辅助决策。

② **OA 的组成:** 计算机设备；办公设备；数据通信及网络设备；软件系统。

第六章 信息安全

一、信息安全的属性及发展阶段

基本属性	内容
保密性	保证信息为授权者享用而不泄露给未经授权者。
完整性	保证信息从真实的发信者传送到真实的收信者，过程中没被非法添加、删除、替换。
可用性	保证信息和信息系统随时为授权者提供服务，保证合法用户对信息和资源的使用不会被不合理地拒绝。
可控性	保证管理者能够对信息实施必要的控制管理，以对抗社会犯罪和外敌侵犯。
不可否认性	人们要为自己的信息行为负责，提供保证依法管理需要的公证、仲裁信息证据。
❖ 信息安全的发展大致分为通信保密、信息安全和信息安全保障三个阶段。	

二、信息安全的主要技术和措施

主要技术	具体措施
身份认证	(1) 可以分为用户与主机间的认证和主机与主机之间的认证 (2) 常见的认证措施：身份认证；静态密码；智能卡；短信密码；动态口令；USB Key；生物识别；双因素认证；nfogo 认证；虹膜认证。
访问控制	防止对任何资源进行未授权的访问，从而使计算机系统在合法的范围内使用。 用户是主体，文件是客体，读取文件操作是请求，一个主体请求一个客体。 常见的访问控制机制： (1) 自主访问控制（DAC）：让客体的所有者来定义访问控制规则。 (2) 基于角色的访问控制（Role-BAC）：将主体划分为不同的角色，然后对每个角色的权限进行定义。 (3) 基于规则的访问控制（Rule-BAC）：制定某种规则，将主体、请求和客体的信息结合起来进行判定。 (4) 强制访问控制（MAC）：一种基于安全级别标签的访问控制策略。
入侵检测系统	(1) 可以分为实时入侵检测和事后入侵检测两种。 (2) 实时入侵检测在网络连接过程中进行，一旦发现入侵迹象立即断开入侵者与主机的连接，并收集证据和实施数据恢复。这个检测过程是不断循环进行的。 (3) 事后入侵检测则是由具有网络安全专业知识的网络管理人员定期或不定期进行的，不具有实时性，因此防御入侵的能力不如实时入侵检测系统。
防火墙	(1) 由软件和硬件设备组合而成，在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。由 服务访问规则、验证工具、包过滤和应用网关 四个部分组成。 (2) 防火墙分为四类： 基于路由器的防火墙、用户化的防火墙工具组件、建立在通用操作系统上的防火墙、具有安全操作系统的防火墙。 (3) 防火墙的基本特性： 所有网络数据流都必须经过防火墙；只有符合安全策略的数据流才能通过防火墙；自身应具有非常强的抗攻击免疫力；应用层防火墙具备更细致的防护能力；数据库防火墙具有针对数据库恶意攻击的阻断能力。
网闸	(1) 网络隔离技术，由 两套各自独立的系统 分别连接安全和非安全的网络，两套系统之间通过网闸进行信息摆渡，保证两套系统之间没有直接的物理通路。 (2) 网络隔离技术的产品和方案 ① 独立网络方案： 内部网络和外部网络物理断开。两个网络之间如有数据交换需要，则采用人工操作。 ② 终端级解决方案： 双主板，双硬盘型；单主板，双硬盘型；单主板，单硬盘型。
防病毒	防病毒策略： 拒绝访问能力；病毒检测能力；控制病毒传播的能力；清除能力；恢复能力；替代操作。
数据加密技术	(1) 是指将一个信息（明文）经过加密钥匙及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函数、解密钥匙还原成明文。分为专用密钥和公开密钥两种。 (2) 专用密钥（对称密钥或单密钥），加密和解密时使用同一个密钥，即同一个算法。例如对称 加密算法 DES 和麻省理工学院（MIT）的 MIT 许可证中的 Kerberos 算法。 (3) 公开密钥（非对称密钥），加密和解密时使用两个不同的密钥，即不同的算法，虽然

监理师讲义第一篇-羽仪老师

	<p>两者之间存在一定的关系，但不可能轻易地从一个推导出另一个。有一个公用的加密密钥，有多个解密密钥，如 RSA 算法。</p> <p>(4) 数字签名：以解决伪造、抵赖、冒充和篡改等问题。数字签名（又称公钥数字签名、电子签章）是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现的，用于鉴别数字信息的方法。数字签名一般采用非对称加密技术（例如 RSA）。</p>
--	---

三、网络安全等级保护

1、网络安全等级保护定级基础

保护定级	内容
第一级 自主保护级	指等级保护对象受到破坏后，会对 相关公民、法人和其他组织的合法权益造成损害 ，但不危害国家安全、社会秩序和公共利益。
第二级 指导保护级	指等级保护对象受到破坏后，会对 相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害 ，或者对 社会秩序和公共利益造成危害 ，但不危害国家安全。
第三级 监督保护级 （比较常见）	指等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对 国家安全造成危害 。
第四级 强制保护级	指等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对 国家安全造成严重危害 。
第五级 专控保护级	指等级保护对象受到破坏后，会对 国家安全造成特别严重危害 。

❖ 定级要素与等级的关系

信息安全被破坏时受侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

❖ 确定信息系统安全保护等级的流程：确定等级对象；初步确定等级；专家评审；主管部门核准；备案审核、批复。

❖ 等保测评的主要内容：物理安全；网络安全；主机安全；应用安全；数据安全。

❖ 等级保护整体流程：系统定级、专家评审、网安备案、系统测评、系统整改、复测、出具报告等。

❖ 等保测评的完整工作周期一般为三个月。

四、数据安全的主要策略及方法

❖ 数据安全的三项基本特点

数据安全	特点
机密性	指个人或团体的信息不为其他不应获得者获得。
完整性	是指在传输、存储信息或数据的过程中，确保信息或数据不被未授权地 篡改 或在篡改后能够被迅速发现
可用性	其设计的重点在于让产品的设计能够符合使用者的习惯与需求。

❖ 威胁数据安全的因素：硬盘驱动器损坏、人为错误、黑客攻击、病毒侵害、信息窃取、自然灾害、电源故障、电磁干扰。

❖ 主要防护技术：磁盘阵列、数据备份、双机容错、网络附加存储（NAS）、数据迁移、异地容灾。

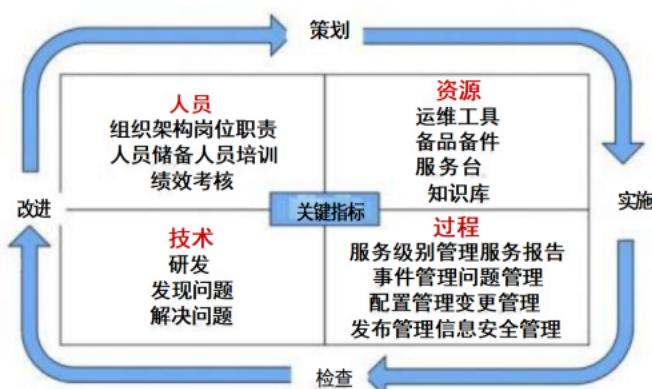
第七章 运行维护

一、运行维护概述

◆ 基本概念	
基本概念	特点
信息系统运维	实施完成后的信息系统正式进入生产环境交付使用阶段的维护和保养工作
运行维护服务	在使用信息系统过程中提出的各类需求提供的综合服务。
运行维护服务	主要包括机房基础设施、物理资源、虚拟资源、平台资源、应用和数据等。
运行维护服务级别协议 SLA	指 业主单位 与运维服务提供方之间为约定运维服务内容和各项服务指标所签署文件。
运行维护服务交付	是指在服务级别协议中，运维服务提供方承诺在服务期内向业主单位提供的运行维护服务内容。运维服务交付的内容包括 例行操作、响应支持、优化改善、调研评估 等。
运行维护监理	运维服务提供方受业主单位委托，依据国家有关法律法规、标准规范、监理合同，对运维服务团队提供的运行维护服务实施监督管理。
◆ 运行维护的发展历程：单一化的网络管理(NSM) → 一体化的运行维护服务管理(ITSM) → 以业务支撑为核心的业务服务运维管理(BSM)	
◆ ITSM 主要强调以 最终用户为核心，以流程为导向 ，提供高质量、低成本、高效的信息技术服务。	
◆ 目前，我国大多数业主单位及运维服务团队的管理层次仍停留在 ITSM 初级阶段或者 NSM 阶段 。③	
◆ 运行维护发展趋势：新技术不断涌现、运维服务模式转型升级、自主创新能力进一步加强。	

二、运行维护服务能力

- ◆ 运行维护服务能力模型：按照 ITSS 体系要求，可以从**人员、技术、过程、资源**四个维度评价运维服务团队的能力。



- ◆ **运维服务级别管理**
 - ① 运维服务目录：识别和分析业主单位的运行维护服务需求，形成项目级的运维服务目录
 - ② 运维服务对象：机房基础设施、物理资源、虚拟资源、平台资源、应用和数据等。
 - ③ 运维服务内容：包括**调研评估、例行操作、响应支持和优化改善**。
- ◆ **人员**
 - ① 组织架构：如成立运维保障部门，包括运维保障领导小组、运维保障调度组、运维保障技术组、运维保障专家组等；
 - ② 岗位职责：运维服务提供方的运维团队岗位设置一般包括**管理岗、技术岗、操作岗**等岗位。
 - ③ 人员储备：建立起与运维服务相关的人员储备计划和机制。
 - ④ 人员培训：根据运维服务需求，建立运行维护服务培训计划，在制订培训计划时应识别培训要求，并提供及时和有效的培训。
 - ⑤ 绩效考核：建立与运维服务相关的绩效考核体系或机制，并明确奖惩规则。
- ◆ **技术**：运维团队根据运行维护服务能力策划要求，开展技术研发和技术成果应用等活动，保证技术能力可以满足业主单位不同服务场景下的服务要求，包括运维服务能力长期发展的需求调研与分析、

技术管理、预期目标等，实现其服务价值。

❖ 资源

- ① **运维工具**: 运行维护工具可分为过程管理工具、监控工具和专用工具。
- ② **备品备件**: 运维服务团队需要建立备件库，保证设备或系统的正常运行。包括制定备件库管理规范、制订备件采购计划或方案、制定出入库制度、制定备件的检测、报废制度。
- ③ **服务台**: 负责在各时间段，提供给用户或服务人员利用电话、邮箱、即时通信、网络或其他自动化手段，针对发生的事件、用户请求、变更等进行交流的途径。服务台是运维服务团队的重要组成部分，为用户和服务人员提供联络手段的同时，使用专门的工具进行记录并管理相关内容。
- ④ **知识库**: 运维服务团队应对运行维护工作相关的经验进行积累，形成可在运维团队内共享、可重复使用的知识和信息。

三、运行维护服务交付过程

- ❖ 包括**运维服务需求识别、运维服务交付内容、运维服务交付方式**。

1、运维服务需求识别

- ❖ 分类：例行操作服务；响应支持服务；优化改善服务；调研评估服务。

2、运维服务交付内容

交付 内容	说明
调 研 评 估	运维服务方案的主要内容如下：（1）需求的调研、评估和服务方案的制定；（2）系统版本管理方案的制定；（3）需求变更方案的制定与评估；（4）软件升级方案的制定与评估；（5）系统优化方案的制定与评估；（6）重大配置变更评估和方案的制定；（7）系统迁移需求的调研、评估和方案的制定。
例 行 操 作	按照约定的触发条件或预先规定的常态服务，运维服务提供方对信息系统的例行操作一般分为 监控、预防性检查和常规作业 。
响 应 支 持	运维服务提供方对信息系统的响应支持工作一般包括：应用级启停、系统级启停、用户注册、权限配置、更新驱动、用户口令重置、参数调整、系统配置、故障处理。
优 化 改 善	对操作系统、数据库、应用服务器中间件等的集成性优化；优化系统参数、配置文件，更新系统错误或性能更新包；对现有系统进行功能更新，应用系统升级；对客户端错误或已知漏洞进行修复；对性能和可靠性进行优化改善；对业务逻辑、符合度的优化改善；对应用服务能力进行优化，如对应用进程数、应用线程数的优化；应用日志级别及日志空间的调整。
❖ 运维服务交付方式：运维服务提供方可以选择 现场交付 或 远程交付 的方式开展运行维护工作。	

四、运行维护应急管理

- ❖ **建立应急管理制度**: 业主单位负责制定应急响应制度，明确应急响应的目标、原则、范围及各项管理制度。应急管理制度要遵循统一领导、分级负责、预防为主、快速响应的原则。
- ❖ **规范应急响应组织**: 应急管理组织架构由运维项目相关单位组成，包括**业主单位的信息化主管部门、信息系统的运维服务提供方、运维服务执行单位**等。
- ❖ **制定应急响应预案**: 对风险要素进行评估，形成风险评估报告，形成应对措施，开展应急演练。
- ❖ **组织培训并开展应急演练**: 制订应急演练计划、演练脚本；对应急组织人员进行培训，讲解应急演练预案、应急演练计划和脚本；对应急演练的整个过程进行详细记录，并形成报告；要保证应急演练的过程不影响业务的正常运行。
- ❖ **应急响应工作总结**: 运维服务团队定期对发生的应急事件和应急响应工作进行分析与回顾，并总结经验。