第二部分：

——系统工程与信息系统安全工程ISSE

主要内容

- 系统工程
- 信息安全工程ISSE

参考

- 系统工程导论
  - 陈宏民 高等教育出版社
- 系统工程导论
  - 安德鲁.P.塞奇 詹姆斯.E.阿姆斯特朗 西安交通大学

主要内容

- **系统工程**
  - 系统
  - 系统工程
  - 系统工程过程
- **信息安全工程ISSE**

什么是“系统”

- 系统是由相互作用和相互依赖的若干组成部分或要素结合而成的具有特定功能的有机整体。
- 系统的概念包含三个基本要点：
  - 系统由要素组成
  - 系统要素间存在各种联系
  - 系统实现一定的功能和目的

系统的模型

■ 系统的普遍模型

每一个系统都是由一些子系统所组成，可以根据不同的要求将系统分解成不同的子系统。

■ 系统的边界和接口

系统的边界由定义和描述一个系统的一些特征来形成，边界之内是系统，边界之外是环境。系统的子系统由子系统之间的边界勾划出来，子系统之间的相互联接或相互作用称为接口，接口处于子系统的边界上。

系统的基本性质

- 整体性
- 涌现性
- 相关性
- 层次性
- 目的性
- 成长性
- 环境适应性

什么是“系统工程”

■ 系统工程的定义

– ‘系统工程’是组织、管理、规划、研究、设计、制造、试验和使用‘系统’的科学方法，是一种对所有‘系统’都具有普遍意义的科学方法

钱学森

系统工程的特质

- 跨学科
- 更针对复杂系统
- 整体最优（成本、进度、可支持性、技术性能…）
- “软硬”结合

系统工程的理论基础

- **自然科学**
  - 数学、运筹学、统计学、概率论…
- **社会科学**
  - 经济学、社会学、行为科学…
- **工程技术**
  - 控制理论、计算机科学、信息技术

常见的四类系统工程问题

- 排序
- 组集
- 适度
- 连接

系统工程方法

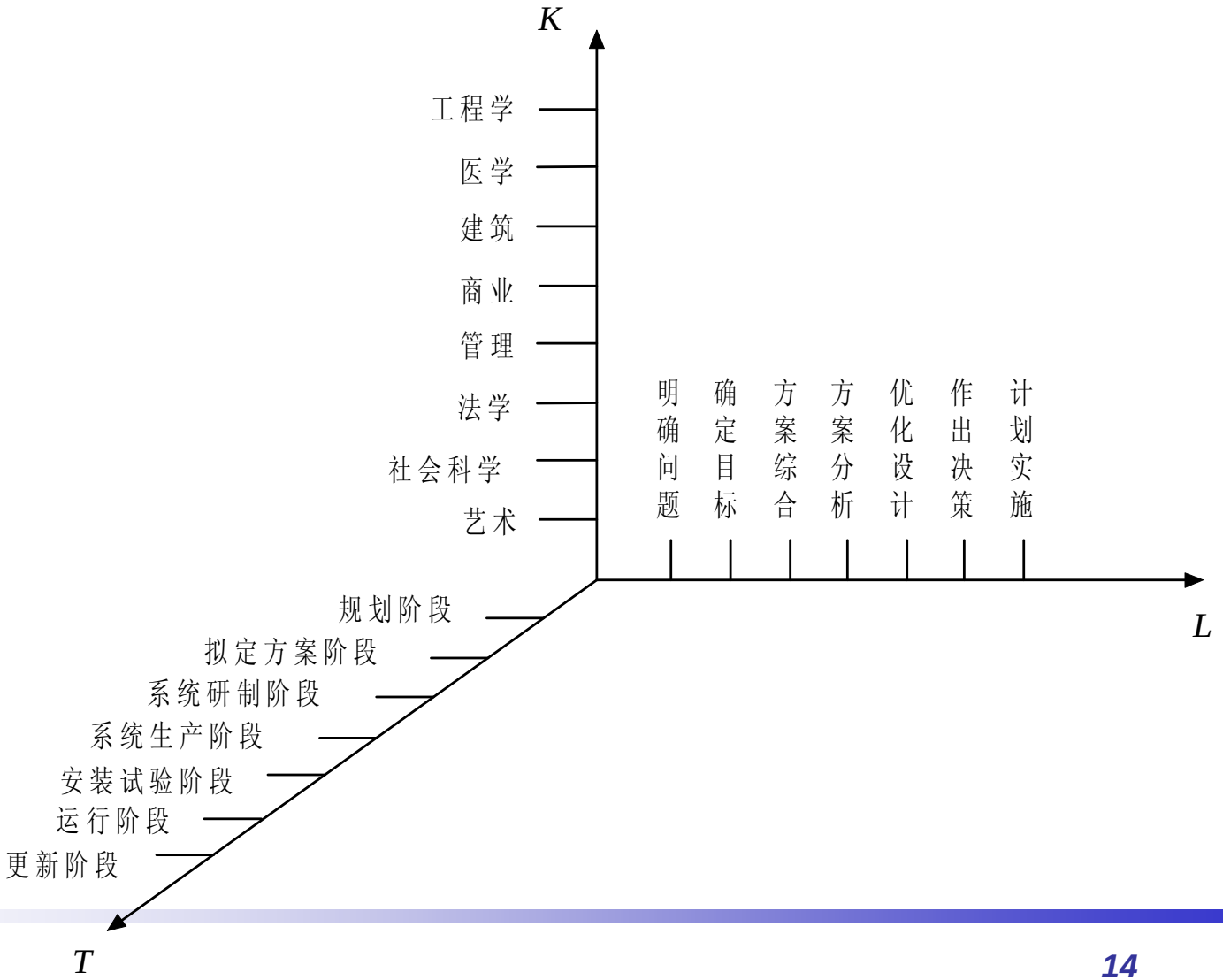
- 系统工程方法指处理复杂系统问题常用的一些具体方法
  - 系统分析方法
  - 系统评价方法
  - 系统仿真方法
  - 系统预测方法
  - 系统决策方法

系统工程方法论

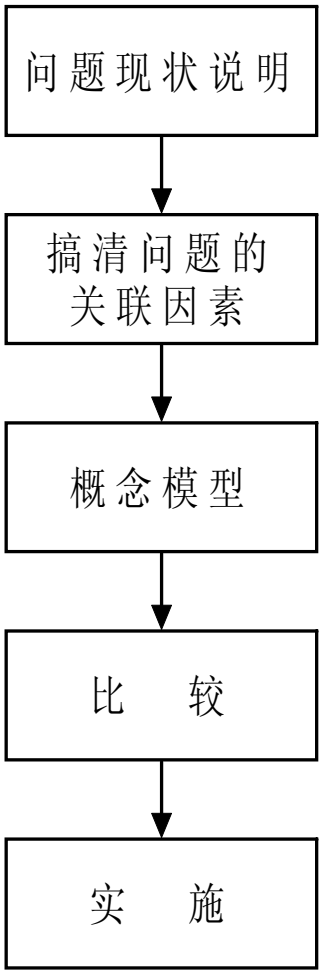
- 研究、分析和处理‘系统工程’问题的思想、程序和基本原则叫做系统工程方法论
  - 霍尔三维结构
  - 切克兰德的“调查学习模式”
  - 顾基发的“物理-事理-人理系统方法”
  - 综合集成系统方法
  - 螺旋式推进系统方法

霍尔三维结构

- 专业维
- 时间维
- 逻辑维



切克兰德的“调查学习模式”



说明现状，目的是为了改善现状，弄清问题本身的基本定义

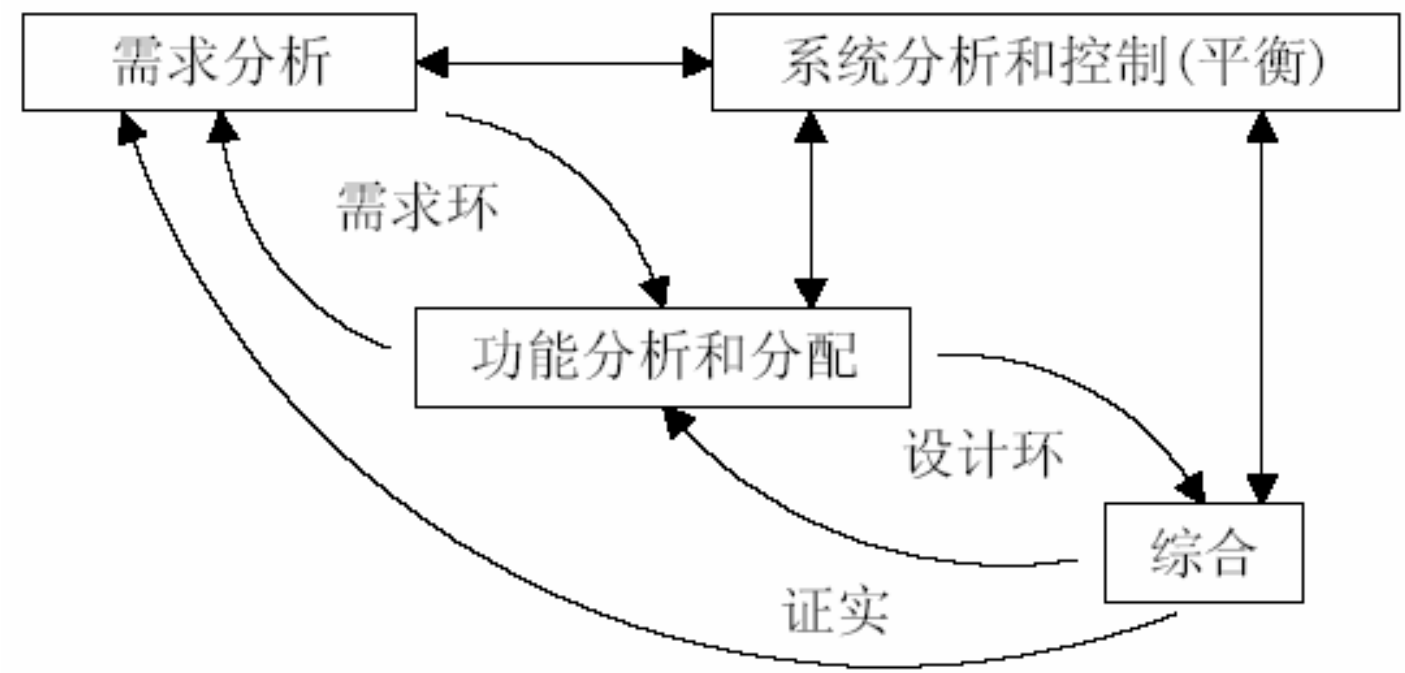
搞清楚与改善有关的各种因素及因素间的相互关系

运用系统观点和系统思考描述系统活动的现状，可用结构模型和有流向的框图表达

根据数学模型的理论和方法，改进上述概念模型，然后将概念模型和现状进行比较得出满意的可行解

对改善方案予以实施

典型的系统工程模型

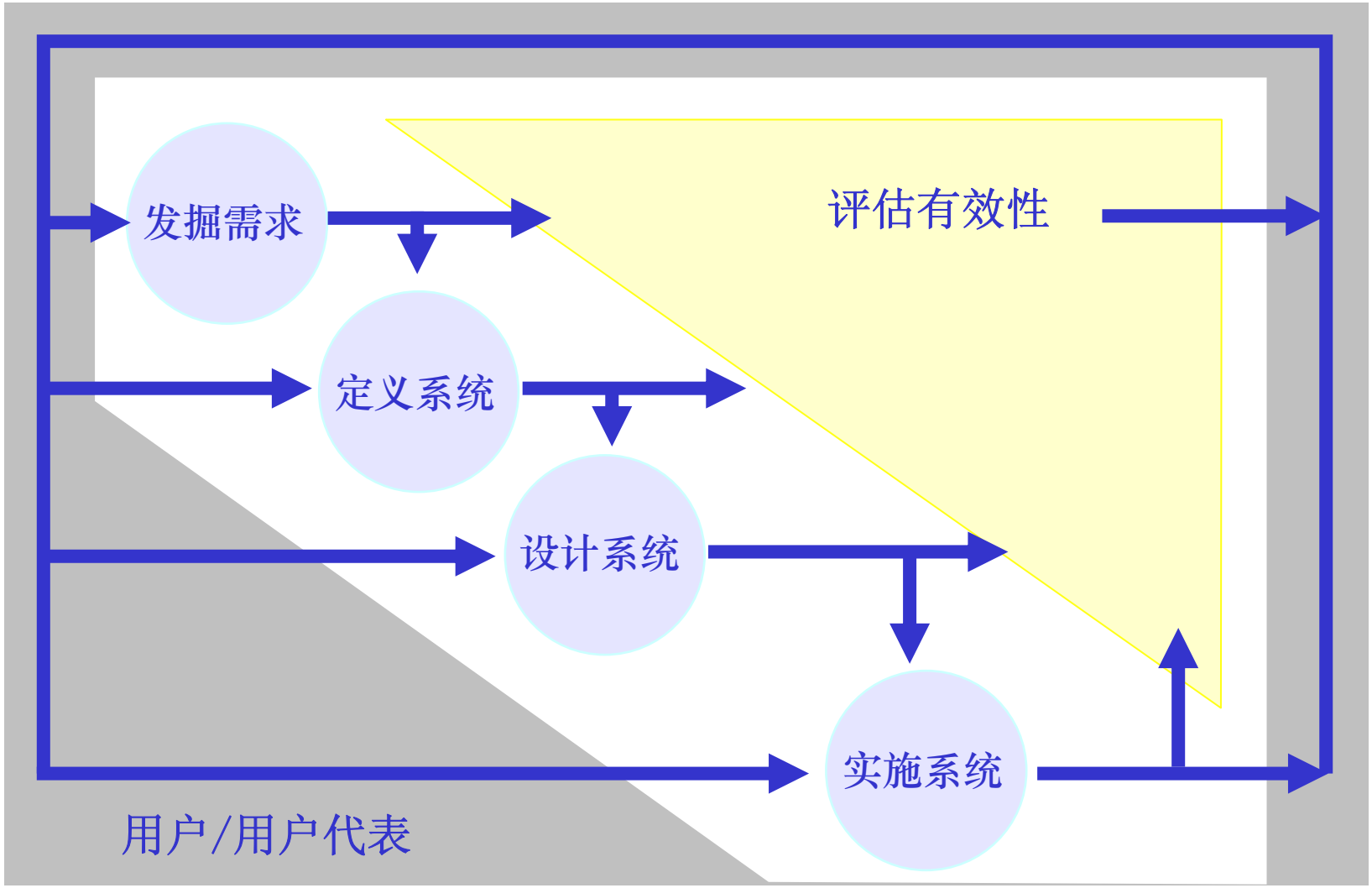


问题与解决方案

- “问题”是“我们期望系统做什么？”
  - 问题空间是约束条件、风险、策略和一些界限
  - 问题空间要根据客户的任务或业务需求来定义
- “解决方案”是“系统怎样实现我们的期望？”
  - 解决方案空间是开发系统以满足用户需求时所有已结束的行为和创造出的产品

系统工程过程

系统工程过程概述（针对信息系统）



系统工程过程

- 发掘需求
- 定义系统功能
- 设计系统
- 实施系统
- 有效性评估

发掘需求

- 针对用户需求以及用户环境中的相关策略、法规、标准的一系列判断
  - 任务或者期望的功能
  - 效率考虑
  - 环境
  - 约束条件（政策和策略）

任务/业务的描述

- 系统构建的目标是使一个机构的本职任务/业务能够顺利实施，且应能更好的推动任武/业务的发展。
- 需求来自于用户的，来源于机构的任务/业务，必须与其策略、目标和战略一致。
  - 结合上级机构与其他可能受影响的机构的任务和功能来考虑
  - 需要标明本机构的重要资产（信息类别、可用资源等）
  - 对任务环境的描述（常规/意外）
  - 标识用户的角色、承担的责任以及在该系统生命周期各阶段的授权
  - 系统的管理需求（系统管理、使用的约束条件）
- 不应该对系统的设计与执行产生过度的约束

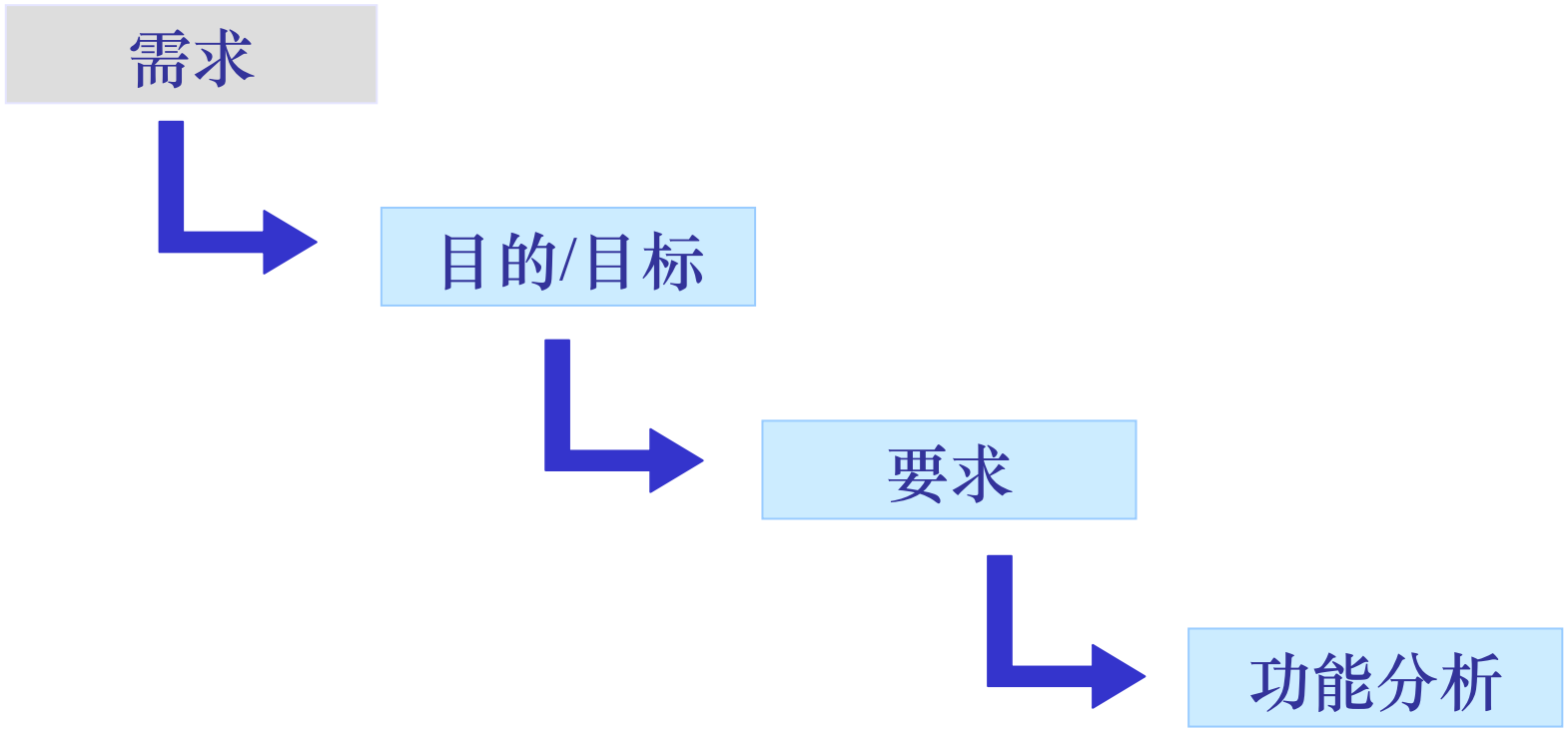
需要考虑的策略和政策

- 对机构具有约束力的政策、法规和标准
  - 要考虑潜在的约束政策
- 例：
  - 美国“Sarbanes-Oxley”法律
  - 中国网络电话的应用

系统工程过程

- 发掘需求
- 定义系统功能
- 设计系统
- 实施系统
- 有效性评估

定义系统功能的基本过程



目标

- 由系统工程师根据需求分析明确系统要完成的功能，包括该功能的实现应达到的程度以及系统的外部接口。
- 目标必须明确、可测、可验证
  - 目标描述能够通过描述系统的预期运行效果而满足需求
  - 系统工程师必须能将目标同此前提出的需求相联系，并能够从理论上加以解释
  - 各目标都有一个用来描述为了满足该目标而所需条件的有效性度量（MoE）

系统背景/环境

- 在技术系统的背景和环境中，系统工程师要确定本系统与系统边界外元素发生相互作用时的功能与接口
  - 系统的物理边界和逻辑边界，以及系统输入/输出的一半特性
  - 针对信息、信号、能量和资源在系统与环境或其他系统之间双向流动的描述
  - 应指出为完成用户任务所需的信息处理类型（例如：对等通信，广播通信，信息存储，一般访问，受限访问）

要求

- 功能要求
  - 描述系统所需完成的任务、动作和行为
- 性能要求
  - 功能要求实现的程度，目标有效性度量（MoE）
  - 质、量、适用范围、合时性、有备性
- 保障要求（保证要求）
  - 使用户确性系统功能/性能可靠性的要求
- 接口、互操作性设计要求

要求的延伸与平衡

- 根据功能的要求和其他条件，可能延伸出其求
- 需要根据可接受风险、生命周期成本和进度、资金要求等权衡功能、性能要求
- 系统工程师与用户需要共同商议评估要求的正确性、完整性、一致性、互依赖性、冲突和可测试性
- 必须在系统有效性和可用性方面的达成一致

要求跟踪矩阵 RTM

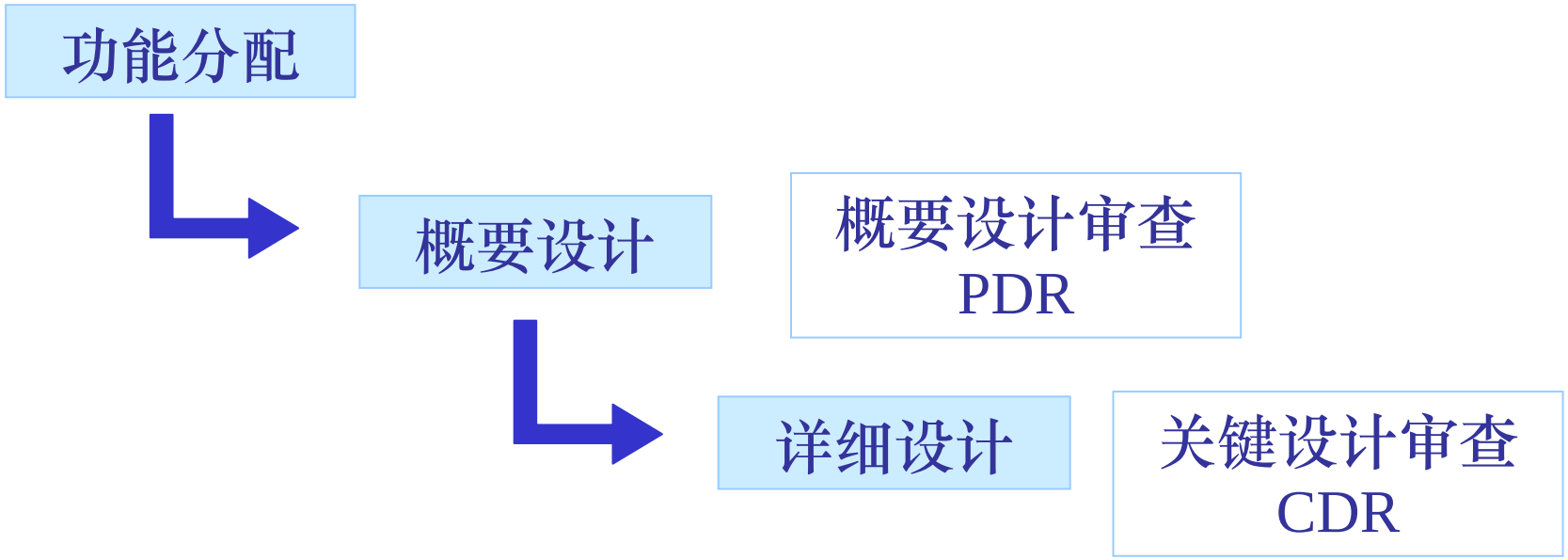
功能分析

- 主要内容是分析功能之间或功能与环境之间的联系
  - 图、表
  - 功能列表一般分层，通常是树形结构
- 连带关系同弱耦合结构的平衡
  - 连带关系：每一个模块或子系统产生一个系统功能，该系统功能由紧密联系的低层功能构成）
  - 弱耦合结构：各模块或子系统之间在很大程度上保持相互独立

系统工程过程

- 发掘需求
- 定义系统功能
- 设计系统
- 实施系统
- 有效性评估

设计系统



功能分配

- 明确各组件在实现其功能时应采取的物理形式
  - 软件、硬件、固件、人
  - 说明各种用来将功能和要求分配给各组件的体系结构的概念并同系统负责人对概念和物理上的可行性取得一致性意见
- 规划系统的验证、集成和有效性测试，
- 针对系统设计分配资金、人员、工具和时间资源，用于系统的测试、后勤、生命周期支持
- 配置管理CM
  - 配置管理工作的主要目的是为了保证项目资料得到清晰、有效地管理，加快工作效率的同时，也避免一些意想不到的风险，如：代码丢失或恶意修改等。同时，有效地配置管理工作，还可作为公司建立复用资源库的主要来源之一

概要设计

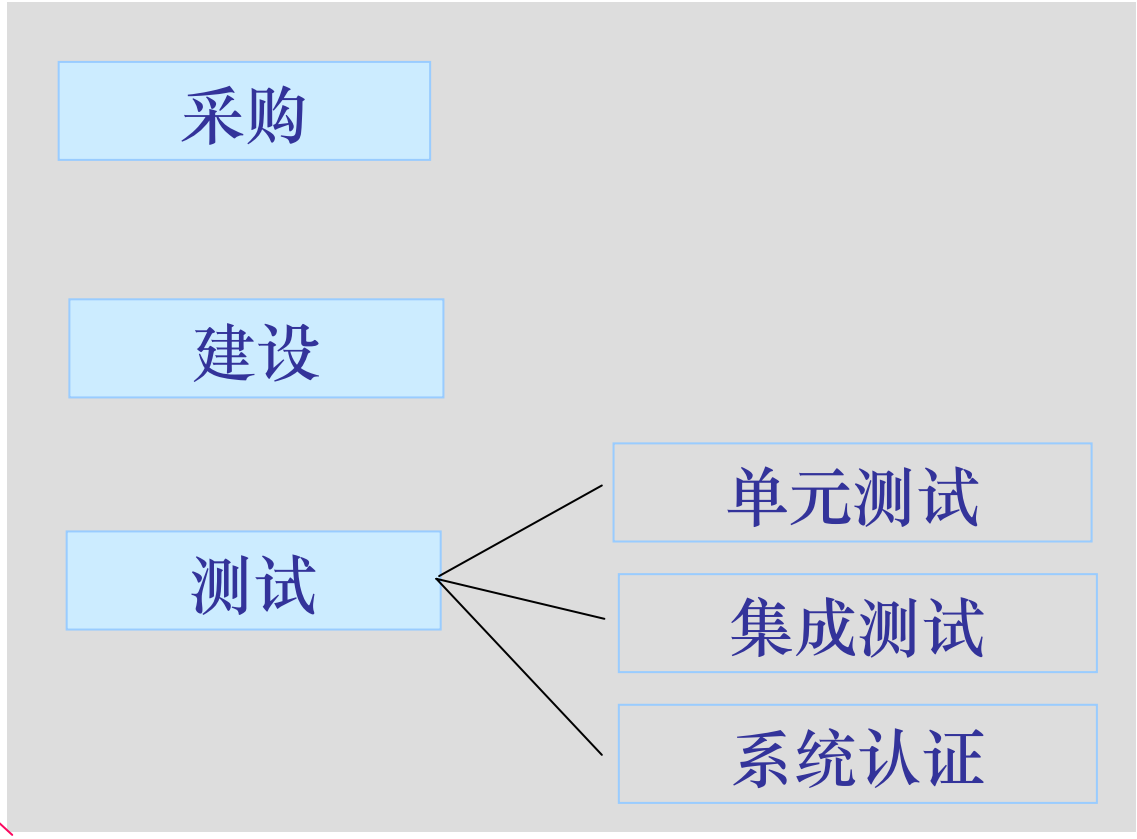
- 先决条件
  - 明确且达成一致的系统要求
  - 确定的体系结构
- 确定规范
  - 命名规则：类、模块等如何命名
  - 采用的设计方法
  - 文档模板
  - 工作量估计和计划
- 概要设计的输出：经分配的系统基线配置

详细设计

- 详细设计将产生
  - 更低层次的产品规范
  - 具体的工程与接口控制图
  - 原型
  - 具体的测试计划与流程
  - 集成后勤支持计划ILSP

系统工程过程

- 发掘需求
- 定义系统功能
- 设计系统
- 实施系统
- 有效性评估



系统验证审查 SVR

系统工程过程

- 发掘需求
- 定义系统功能
- 设计系统
- 实施系统
- 有效性评估

有效性评估

– 检测的主要因素

- 系统是否达到了任务的需求
- 系统是否能够依照机构所期望的方式操作

- 互操作性：系统是否能正确地通过外部接口共享信息
- 可用性：用户使用系统是否能够提高任务的成功性
- 训练：用户要合格的操作和维护系统需要何种程度的指令
- 人机接口：人机接口问题是否会导致用户出错，从而对系统和任务不利
- 成本：建立、更新、和维护系统是否在经济上可行