电子科技大学

University of Electronic Science and Technology of China

第2章 ISSE 过程

章节内容

- 2.1 ISSE概述
- 2.2 信息安全需求的挖掘
- 2.3 信息安全系统的定义
- 2.4 信息安全系统的设计
- 2.5 信息安全系统的实施
- 2.6 信息安全系统的评估
- 2.7 ISSE实例

2.1 信息系统安全工程概述

著名科学家钱学森院士认为：

系统工程是组织管理系统规划、研究、制造、实验、使用的科学方法，是一种对所有系统都具有普遍意义的科学方法。

- 系统工程是软科学

不同于一般的工程技术学科，如水利工程、机械工程等“硬”工程；系统工程偏重于工程的组织与经营管理一类“软”科学的研究。

2.1 信息系统安全工程概述

- 信息系统建设基于系统工程的思想和方法。
- 任何系统均有其产生、发展、成熟、消亡或更新换代的过程，这个过程称为系统的生命周期。
- 信息系统建设的周期阶段：系统规划、系统分析与设计、系统实施、系统运行与维护。

2.1 信息系统安全工程概述

《信息系统安全工程手册 V1.0》

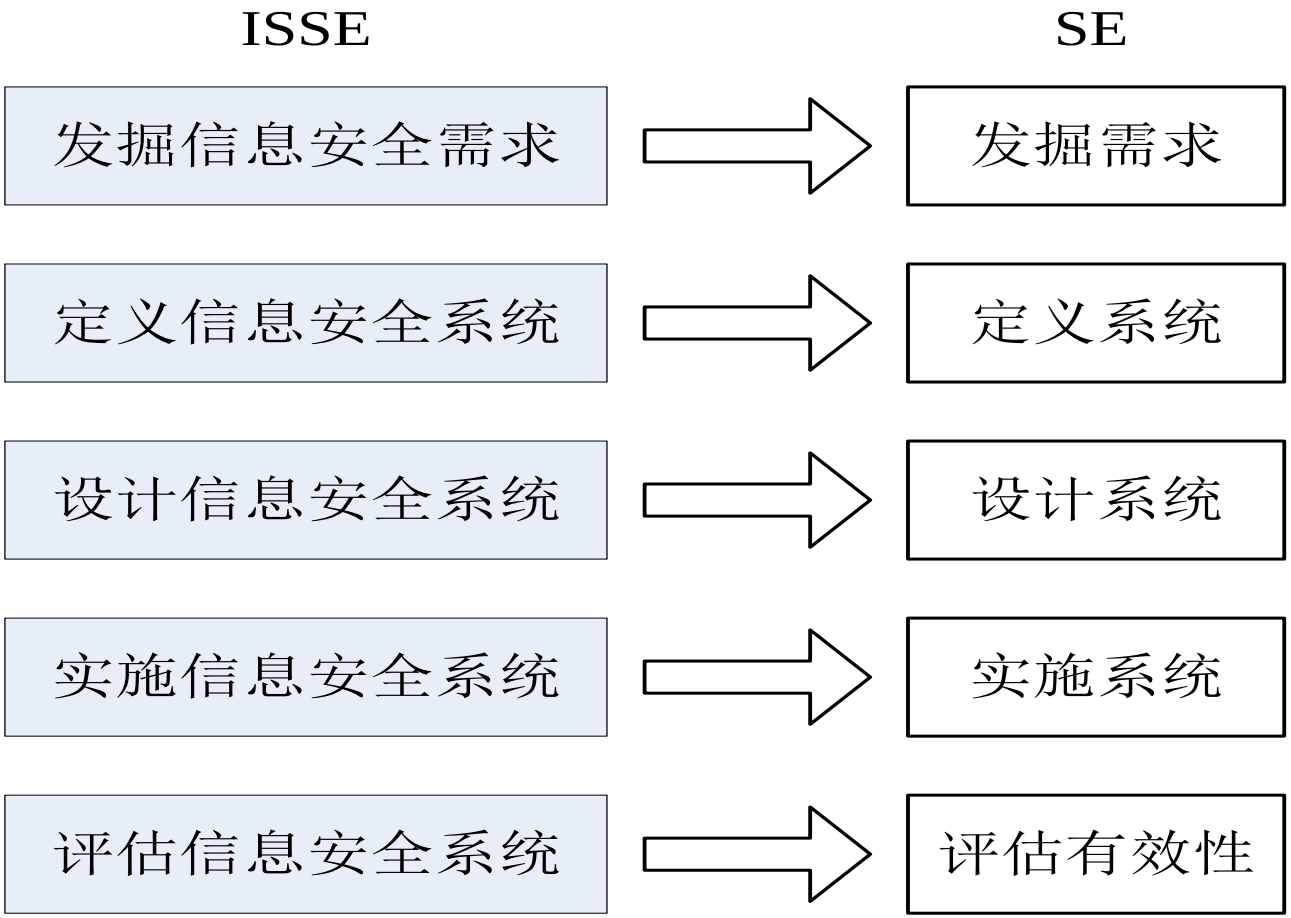
这是一种用来在设计和实现信息系统的过程中，为信息系统提供安全保障的系统工程方法，其目的是使信息系统成为系统工程和系统获取过程的必要部分，将**信息系统安全集成到系统工程中，以获得最优的信息系统安全解决方案**。

2.1 信息系统安全工程概述

- 信息系统安全工程（ISSE）是对信息系统建设中涉及的多种要素按照系统论的科学方法来进行操作的一种**安全工程理论**，是系统工程学、系统采购、风险管理、认证和鉴定以及生命周期的支持过程的一部分，是系统工程过程的一个自然扩展。
- **ISSE主要用来：**设计、实现独立的软硬件系统，为集成的计算机系统的设计和重构提供服务。
- **ISSE的指导思想:**将安全工程与信息系统开发集成。

2.1 信息系统安全工程概述

◆ ISSE 与 SE 的关系



2.1 信息系统安全工程概述

- **ISSE的主要活动：**
  - ◆分析并描述信息保障的用户愿望。
  - ◆基于用户愿望产生信息保障的需求。
  - ◆确定信息保护的级别，以一个可接受的信息保障的风险水准来满足要求。
  - ◆根据需求，构建一个功能上的信息保障体系结构。
  - ◆根据物理体系结构和逻辑体系结构分配信息保障的具体功能。
  - ◆设计信息系统，实现信息保障的功能构架。

2.1 信息系统安全工程概述

- 考虑成本、规划、进度和操作的适宜性及有效性等因素，平衡信息保障风险与其他的ISSE问题。
- 与其他的信息保障和系统工程原则如何进行权衡。
- 将ISSE过程与系统工程和采购过程集成。
- 测试与评估系统，验证是否达到设计保护的要求和信息保障的需求。
- 创建并保留标准化的文档。
- 为用户部署系统，并根据其需要，调整系统，继续进行生命周期内的安全支持。

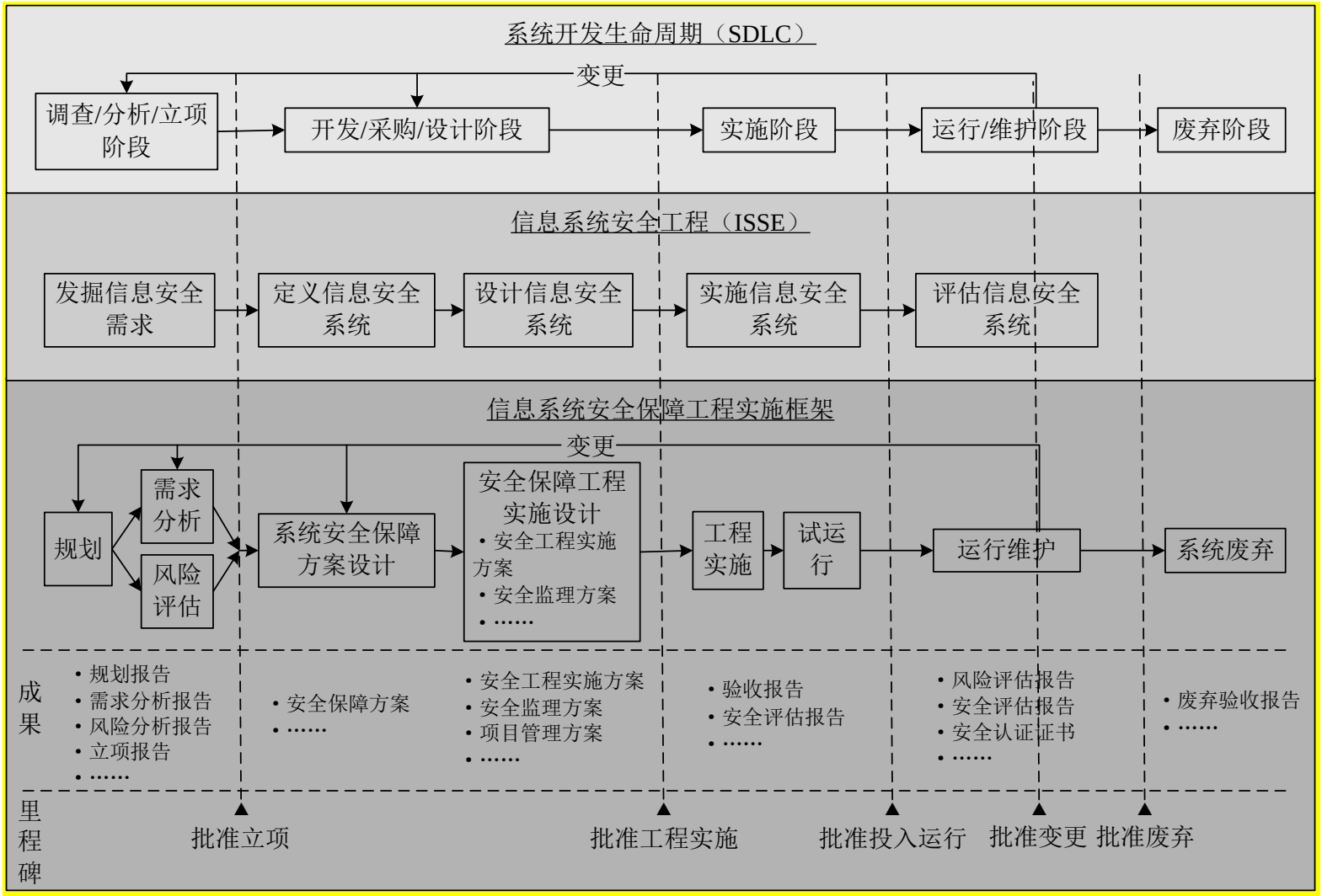
2.1 信息系统安全工程概述

- **ISSE的基本功能：**
  - ◆安全规划与控制
  - ◆确定安全需求
  - ◆支持安全设计
  - ◆分析安全操作
  - ◆支持安全生命周期
  - ◆管理安全风险

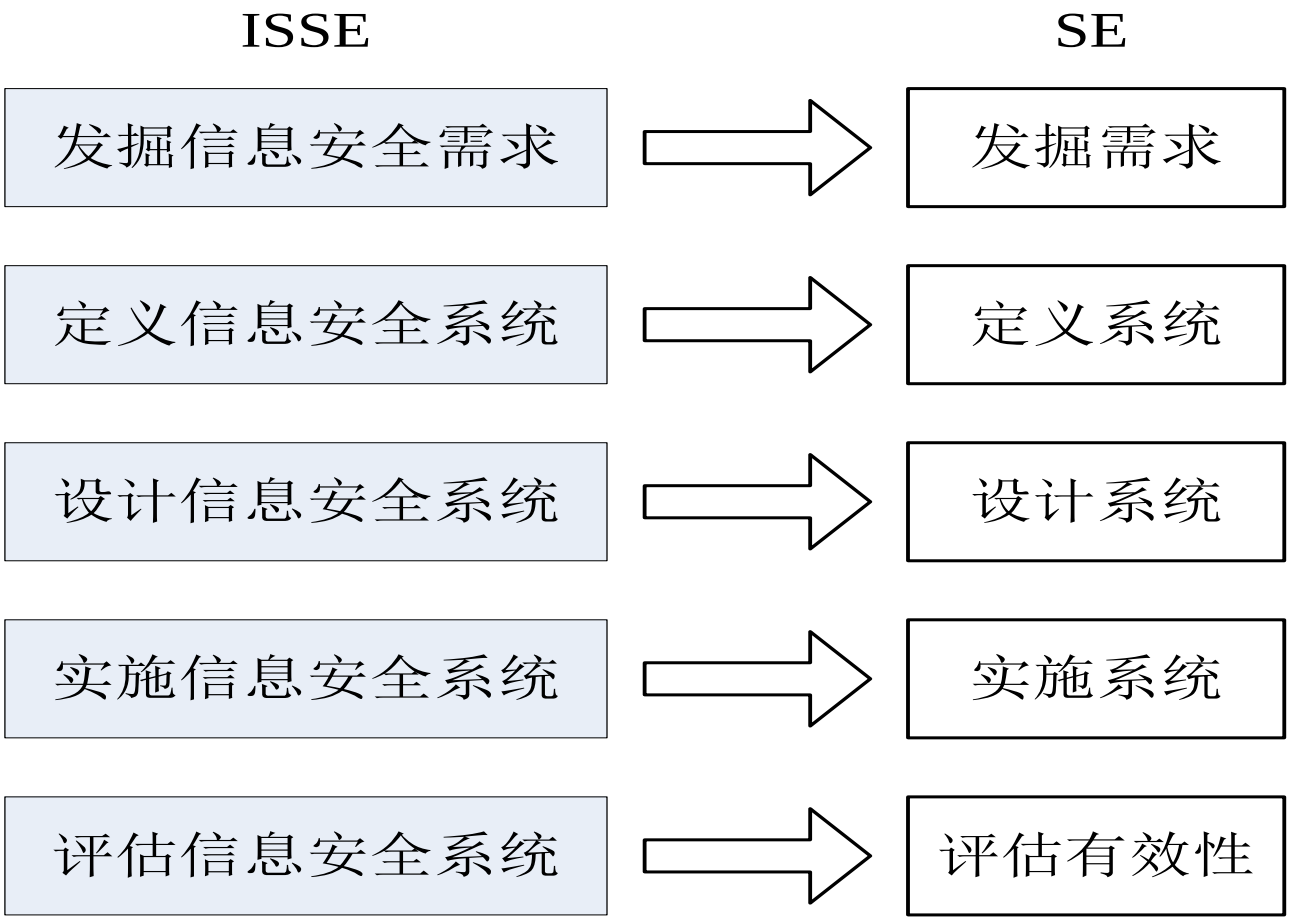
2.1 信息系统安全工程概述

- ISSE的体系结构是一个顺序结构，前一项的结果是后一项的输入，具有严格顺序性，是按照时间维的发展。
- 违背时间顺序将导致系统建设的盲目性，导致信息系统安全工程建设的失败。

信息系统安全保障工程实施简要框架

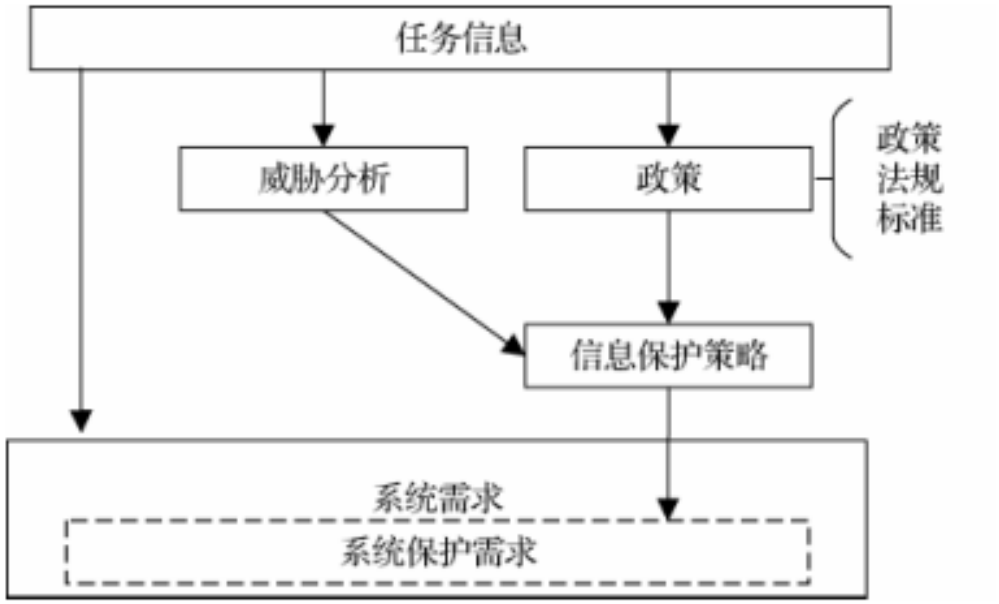


2.2 信息安全需求的挖掘



2.2 信息安全需求的挖掘

- 了解用户的工作任务需求、相关政策、法规、标准、惯例，以及在使用环境中受到的威胁；
- 确认系统的用户、他们的行为特点、在信息保护生命周期各阶段的角色、责任和权力等。
- 信息保护的需求应该来自用户的角度，大致分为了解信息保护需求掌握信息系统威胁、考虑信息安全策略三部分



2.2 了解信息保护需求

- **主要原则：**需要考虑系统可能受到的各方面的影响以及可能造成的损失。帮助用户弄清楚什么信息在收到何种破坏时会对系统的任务造成危害。

2.2 了解信息保护需求

ISSE需要：

- 首先要考虑的是存在哪些信息威胁以及这些威胁会带来怎样的损失
- 帮助用户分析信息和业务流程的关系
- 对系统资源的调查和资源的价值的分析
- 完成系统风险的排序，对信息进行分级划分，根据相应的排序最终形成系统的安全策略

2.2 掌握信息系统威胁

- 对信息系统的威胁，指可以利用信息系统的脆弱性，可能造成某个有害结果的事件或对信息系统造成危害的潜在事实。

➢ 主要威胁：

- ◆检测恶意攻击。
- ◆了解安全缺陷。
- ◆掌握系统漏洞。
- ◆分析结构隐患。

➢ 涉及信息主体的威胁：

- ■ 动机或者意图。
- ■ 威胁的能力。
- ■ 主要途径。
- ■ 可能性大小。
- ■ 影响及结果。

2.2 考虑信息安全策略

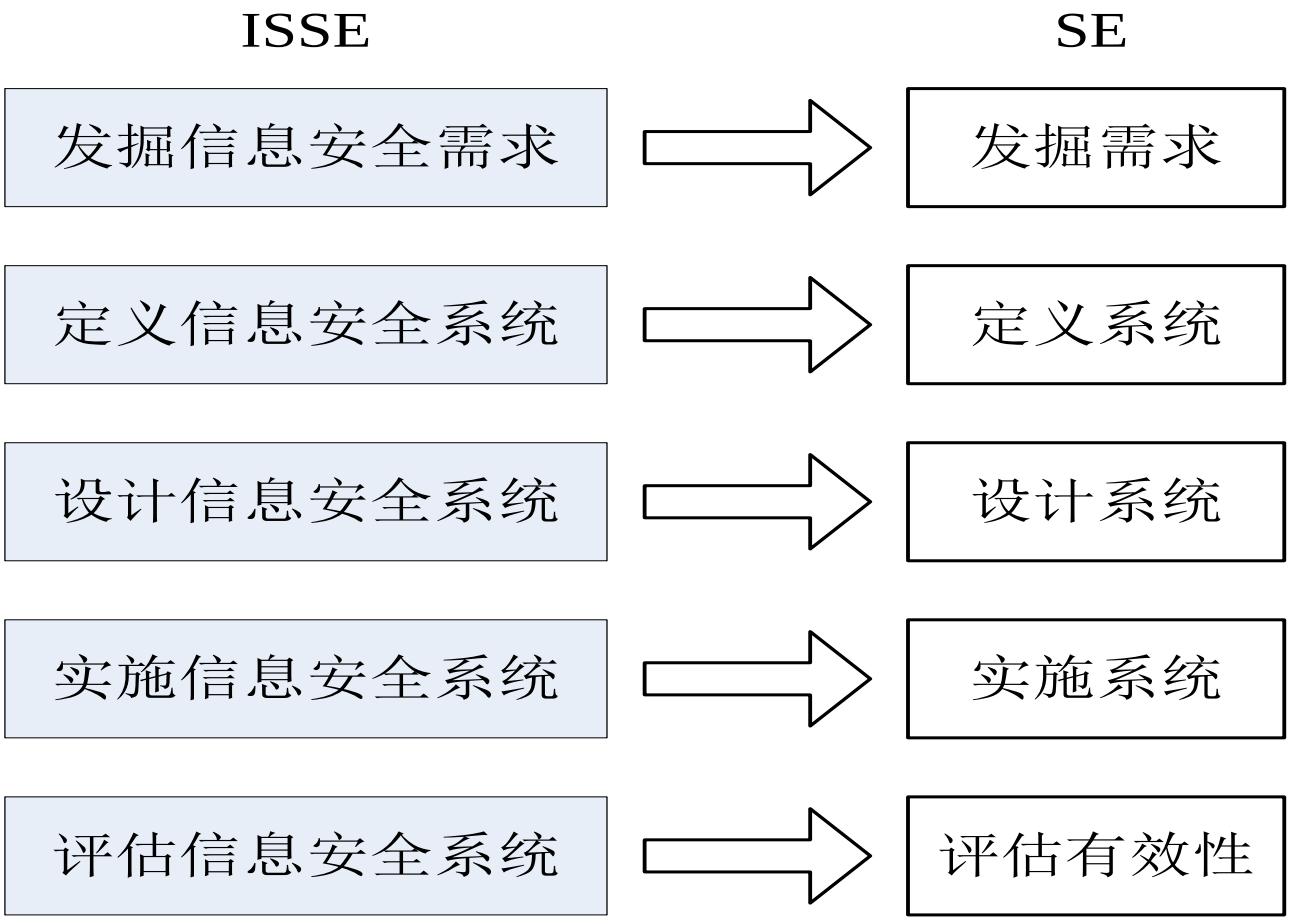
- 信息安全策略：

  要保护什么？用什么保护方法？如何保护？

- 信息安全的策略要提供：
  - 法律和法规、信息保护的内容和目标、信息保护的职责落实办法、实施信息保护的方法、事故的处理。
- 整个安全策略的制定过程包括：确定信息安全策略的范围、风险评估/分析或者审计以及信息安全策略的审查、批准和实施。

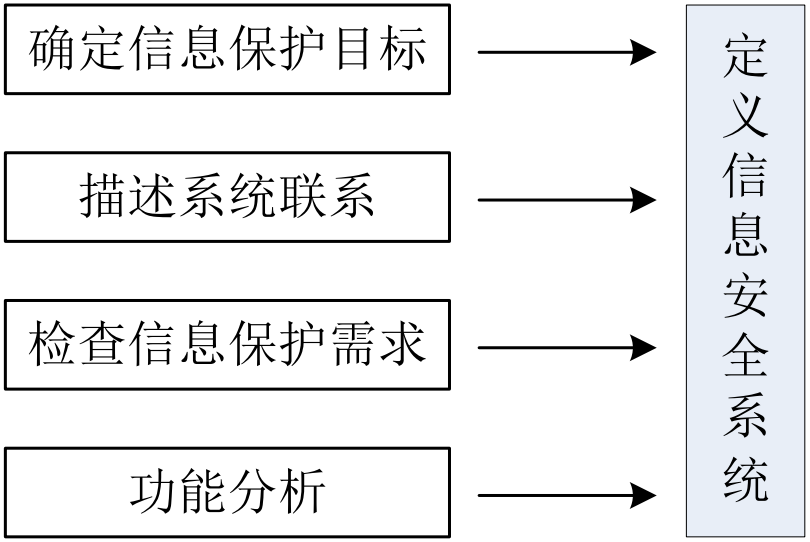
制定好顶层设计，由高层管理机构批准并颁布

2.3 定义信息安全系统


ISSE
SE
发掘信息安全需求
发掘需求
定义信息安全系统
定义系统
设计信息安全系统
设计系统
实施信息安全系统
实施系统
评估信息安全系统
评估有效性

2.3 信息系统安全的定义

- **定义信息安全系统：**确定信息安全系统将要保护什么，如何完成其功能，以及描述信息安全系统的边界和环境的联系情况。
- 任务的信息保护需求和信息系统环境被细化为信息安全保护的**对象、需求和功能**集合。



2.3.1 确定信息保护目标

- 描述信息保护的对象：
  - 信息保护目标支持系统中的什么任务对象？
  - 有哪些与信息保护目标和任务相关的威胁？
  - 失去目标会有什么后果？
  - 受什么样的信息保护策略或方针的支持？

保证有效性度量

2.3.2 描述系统联系

- **系统联系**是信息安全系统的边界和环境，即系统与外界交互的功能和接口。

➢ 描述系统联系需要做的工作：

◆在系统的任务处理过程、与其他系统和环境之间确定物理的和逻辑的边界。

◆描述信息的输入和输出、系统与环境之间或与其他系统之间的信号与能量的双向流动情况。

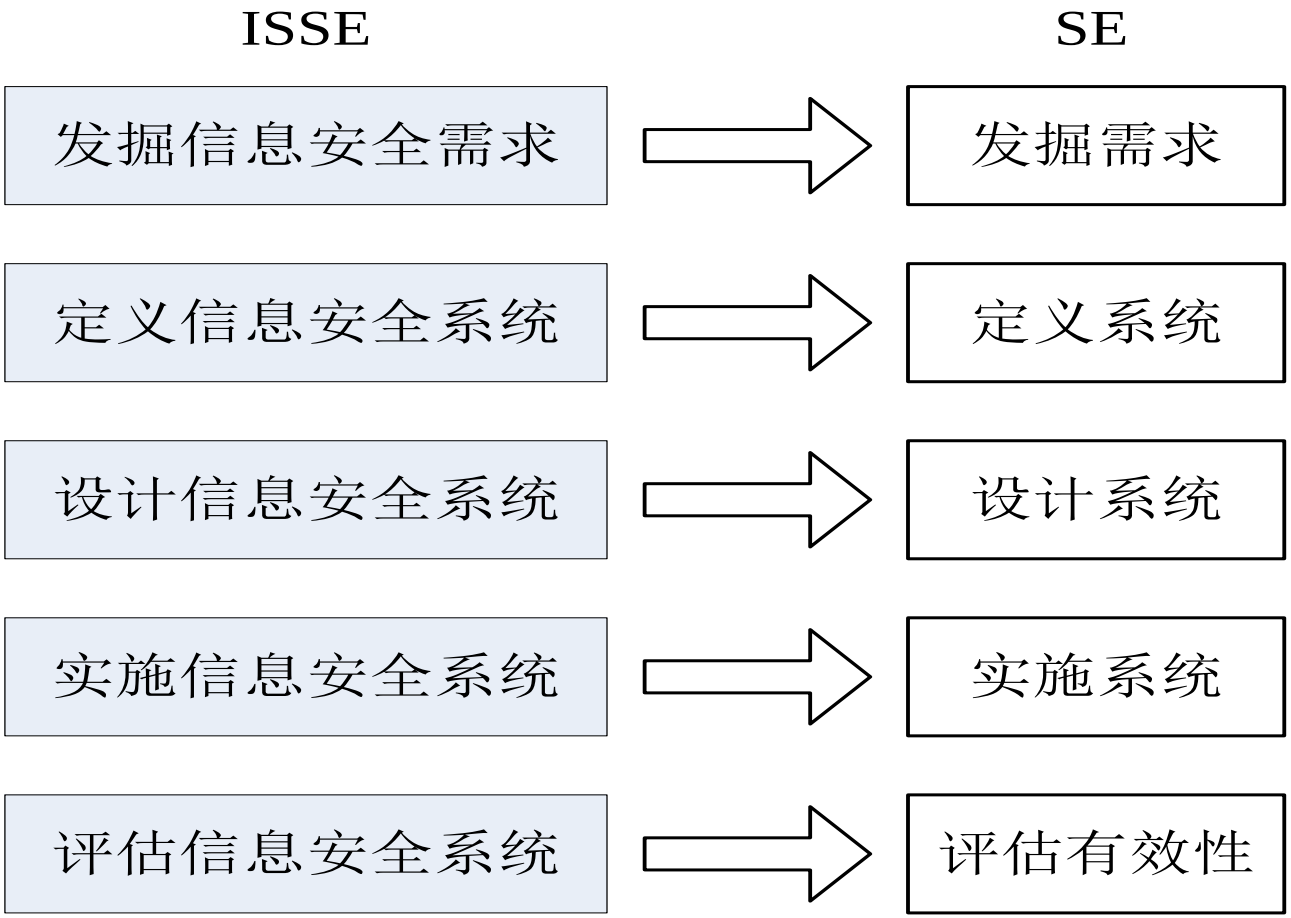
2.3.3 检查信息保护需求

- 对上述过程中的分析（包括目标、任务、威胁、系统联系等）进行特征检查。
- 从最初的用户愿望，经过充分定义，并演变为一系列的系统保护规范时，信息保护的需求能力可能出现缺失，需要检查信息保护需求的正确性、完整性、一致性、依赖性、无冲突和可测试性等特征。

2.3.4 功能分析

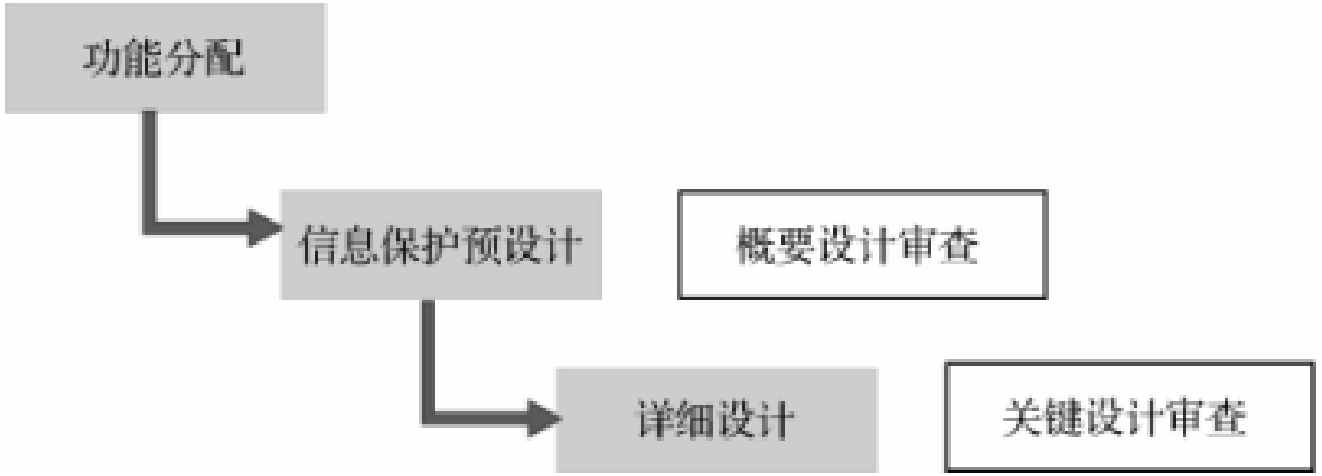
- ISSE使用许多系统工程工具来理解信息保护功能，并将功能分配给系统中各种信息保护的配置项。
- 在定义信息安全系统中，对功能进行分析，必须分析备选系统体系结构、信息保护配置项，以及信息保护子系统是如何成为整个系统的一部分，这些功能是否能达到原设定的目标，如何才能与整个系统协调工作。

2.4 设计信息安全系统


ISSE
SE
发掘信息安全需求
发掘需求
定义信息安全系统
定义系统
设计信息安全系统
设计系统
实施信息安全系统
实施系统
评估信息安全系统
评估有效性

2.4 信息系统安全的设计

- 信息系统安全工程师要与系统工程师合作，一起分析待建系统的体系结构，完成功能的分析和分配、信息保护预设计以及信息保护详细设计等工作。



2.4 功能分配

- **功能分配目标：**ISSE要为系统制定一个理论和实践都可行的、协调一致的信息保护系统体系架构。

➢ 功能分配过程要做到：

◆提炼、验证并检查安全要求与威胁评估的技术原理。

◆确保一系列的低层要求能够满足系统级的要求。

◆完成系统级体系结构、配置项和接口定义。

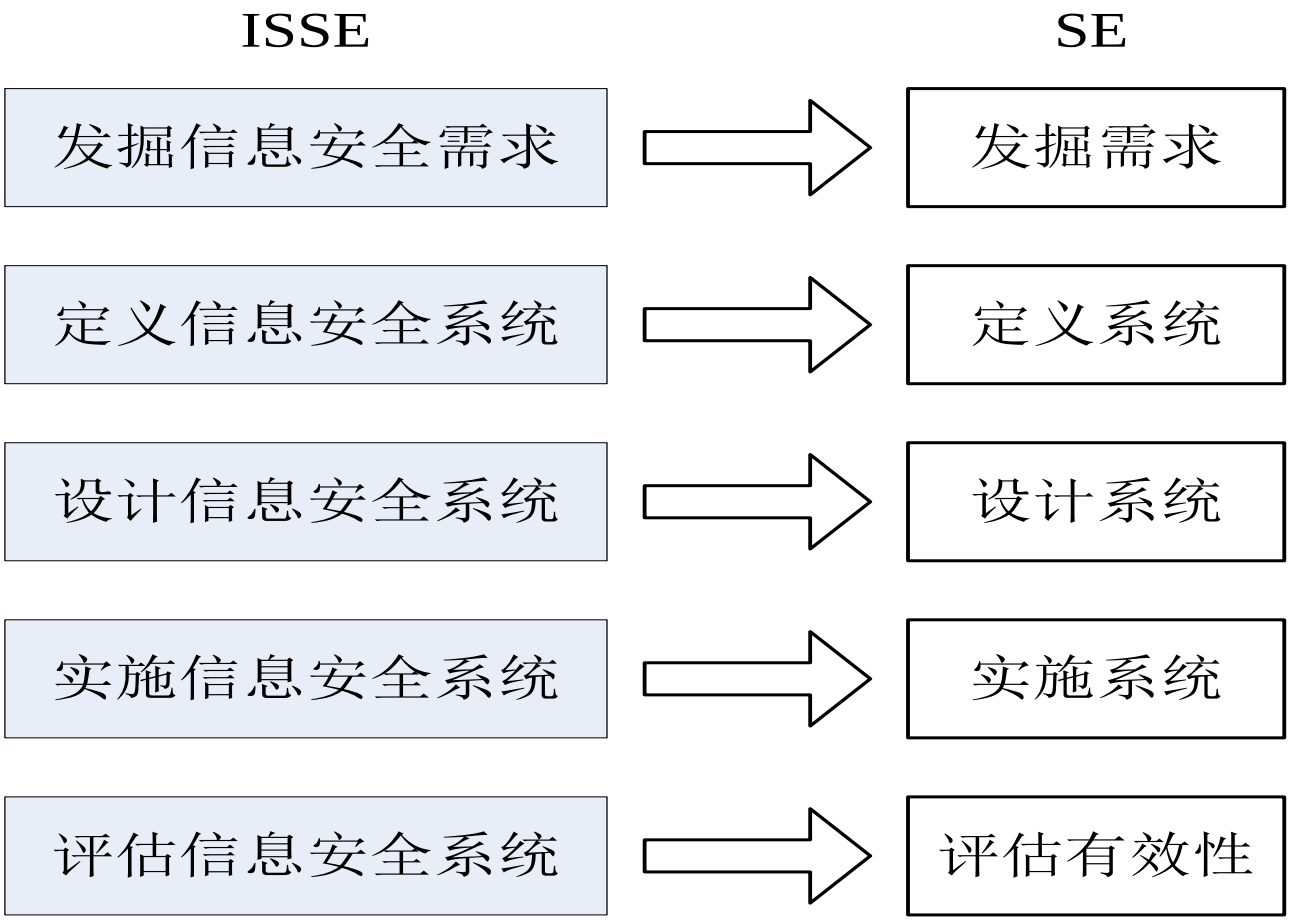
2.4 信息保护预设计

- **ISSE工程师完成初步系统安全设计，考虑生命周期支持。**具体包括：
  - ◆根据之前分析系统安全体系结构的结果，对已经定义好的安全功能进行检查和修改。
  - ◆选择相应的安全机制类型，验证并保证满足所有的安全需求。
  - ◆加入系统工程过程，并支持认证/认可（C/A）和管理决策，提出风险分析结果。

2.4.3 信息保护详细设计

- **完善配置方案、细化产品规范、检查细节规范：**
  - 检查、细化并改进预设计阶段的成果。
  - 提供细节设计资料以支持系统层和配置层的设计。
  - 检查关键设计的原理和合理性。
  - 设计信息保护测试与评估程序。
  - 实施并追踪信息保护的保障机制。
  - 检验配置项层设计与上层方案的一致性。
  - 提供各种测试数据。
  - 检查和更新信息保护的风险和威胁计划。
  - 加入系统工程过程，并支持认证/认可（C/A）和管理决策，提出风险分析结果。

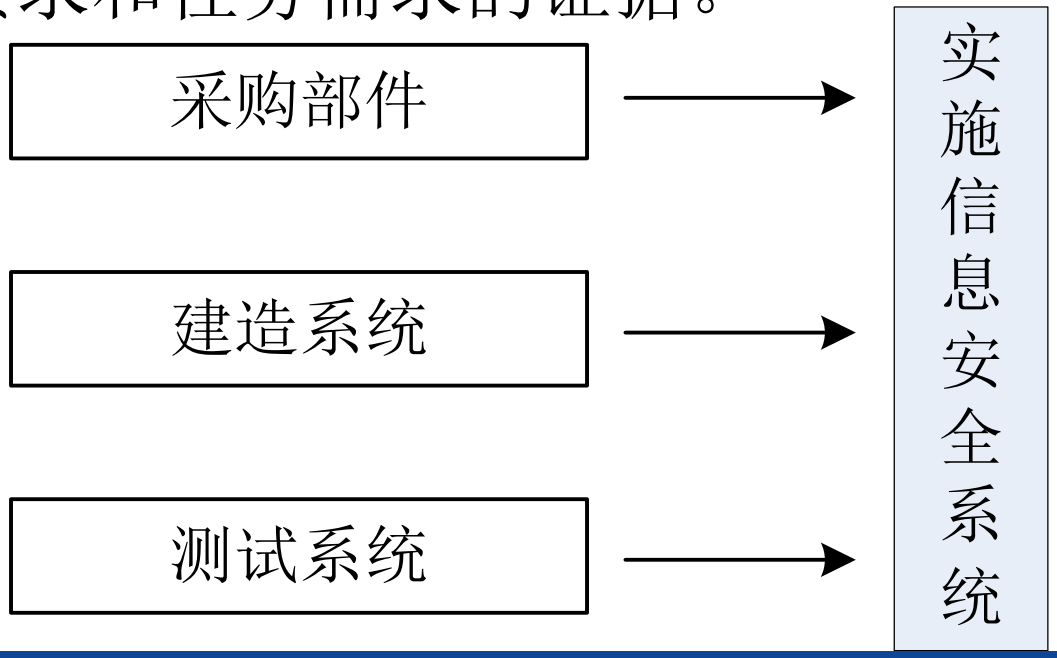
2.5 信息系统安全的实施



2.5 信息系统安全的实施

目标：满足信息安全需求的信息保护子系统的各配置项购买或建造出来，采办、集成、配置、测试、记录和培训。

结束标志：最终系统有效性行为评估，给出满足系统要求和任务需求的证据。



2.5 采购部件

- 根据市场产品的研究、偏好和最终的效果，来决定是购买还是自行生产的方式来获得。
- 考虑安全因素、可操作性、性能、成本、进度、风险等影响。应做到：
  - ◆确保考虑全部相关的安全因素。
  - ◆察看现有产品是否能满足系统部件的需求，最好有多种产品可供选择。
  - ◆验证一系列潜在的可行性选项。
  - ◆新技术和新产品如何运用到系统中去。

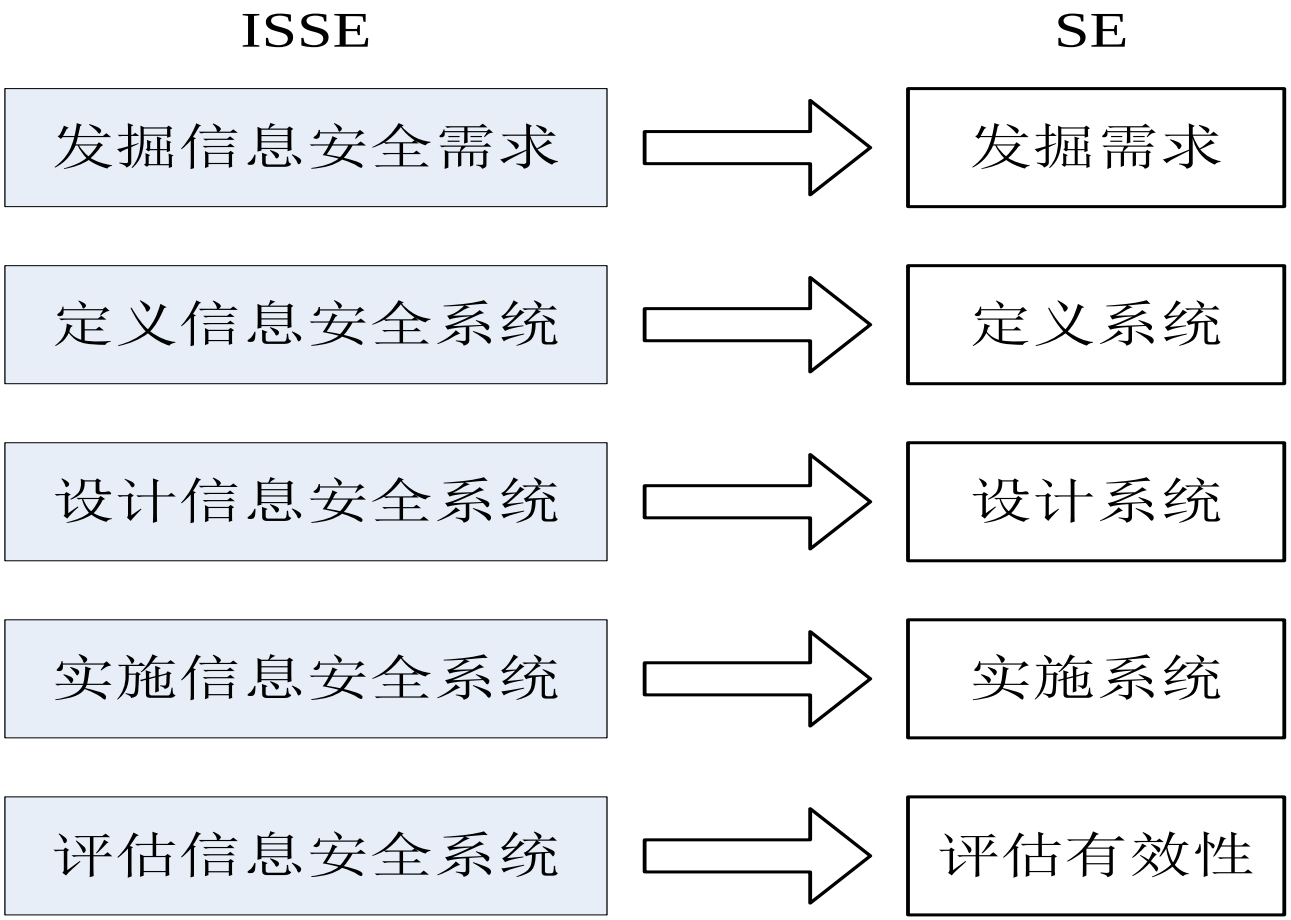
2.5 建造系统

- 确保已设计出必要的保护机制，并使该机制能够实现。具体考虑：
  - 部件的集成是否满足系统安全规范？
  - 部件的配置是否保证了必要的安全特性，以及安全参数能否正确配置以便提供所要求的安全服务？
  - 对设备、部件是否有物理安全保护措施？
  - 组装、建造系统的人员是否对工作流程有足够的知识和权限？

2.5 测试系统

- 给出测试计划、工作流程、测试用例、工具等，检验信息安全系统的实现效果，具体工作：
  - 检查、细化并改进设计信息安全系统的阶段结果。
  - 检验解决方案的信息保护需求和约束限制等条件，并实施相关的系统验证和确认机制与决策。
  - 跟踪实施与系统实施和测试相关的系统保障机制。
  - 鉴别测试数据的可用性。
  - 提供安全支持计划，包括逻辑上的、有关维护和培训等方面。
  - 加入系统工程过程，并支持认证/认可（C/A）和管理决策，提出风险分析结果。

2.6 信息系统安全的评估



2.6 信息系统安全的评估

- **ISSE强调信息保护系统的有效性，**主要指系统在保密性、完整性、可用性、不可否认性等方面的有效性。**有效性评估重点：**
  - 互操作安全性，即是否通过外部接口正确地保护信息？
  - 可用性，即是否能给用户提供信息资源与信息保护？
  - 用户需要接受什么样的培训，才能正确地操作和维护信息保护系统？
  - 人机界面或接口是否有缺陷，从而导致出错？
  - 建造和维护信息系统的成本是否可以接受？
  - 确定风险和可能的任务影响，并提供报告。

2.7 ISSE实施的案例

✦ 信息保护目标和任务过程的相关威胁

- 确保该系统满足五大信息安全基本性质的目标：
  - ✓ 数据完整性：保证企业上机网络中用户之间传送的资源是完整的、未经篡改的数据包。
  - ✓ 可用性：保证合法上机用户在申请其权限之内的公共资源时，服务器能够提供其需要的资源。
  - ✓ 可靠性：保证在企业需要的时间段内，系统不会因为外部或内部攻击以及其他问题导致停止响应甚至崩溃的情况。
  - ✓ 数据机密性：保证任意用户的身份信息和用户口令等私密信息在系统中得到机密性保护。
  - ✓ 不可抵赖性：任意用户都不能否认自己进行的每一次操作，不能抵赖自己执行的非法操作。

- 根据网络安全 PDRR 模型（Protection、Detection、Reaction、Recovery，即防护、检测、响应、恢复）在 4 个方面建立安全技术体系。

本章总结

- ISSE是对信息系统建设中涉及的多种要素按照系统论的科学方法来进行操作的一种安全工程理论。
- ISSE过程分为**信息安全需求挖掘、信息系统安全定义、信息系统安全设计、信息系统安全实施和信息系统安全评估**等阶段。
- 在建设信息系统安全保障体系时，可以按照ISSE过程的思想，充分考虑对信息系统进行安全需求分析、设计、开发和维护，保障系统在全生命周期内的安全服务。

作业

- 课堂作业
  1）什么是信息系统安全工程？
  2）ISSE的主要过程包括哪些？
  3）ISSE的基本功能有哪些？
  4）简要概述ISSE的实施框架。