电子科技大学

University of Electronic Science and Technology of China

信息安全工程

王瑞锦

2020年10月20日

联系方式

- 办公地点：主楼中427
- E-mail：ruijinwang@uestc.edu.cn

教材及参考书目

- 《信息安全工程与实践》，王瑞锦等，人民邮电出版社，2017年10月
- 《信息安全工程》，严承华，清华大学出版社，2017年7月
- 《信息安全工程》， Anderson， Ross等，清华大学出版社，2012年1月
- 《工程思维》，宫晓李等，机械工业出版社，2018年1月
- 《信息安全管理》，汤永利等，电子工业出版社，2017年1月

课程性质

- 专业选修课（Elective）
- 专业核心课（Compulsory）

课程特点

- 抽象：概念、原理等要通过具体的实例理解；
- 思维：工程思维；
- 应用：理论、技术与实践相结合；

工程教育认证毕业能力要求12条

- **1工程知识：**能够将数学、自然科学、工程基础和专业知识用于解决复杂工程问题。
- **2问题分析：**能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析复杂工程问题，以获得有效结论。
- **3设计/开发解决方案：**能够设计针对复杂工程问题的解决方案，并在设计过程中体现创新意识，考虑社会、健康、安全、法律、文化及环境等因素。
- **4研究：**能够基于科学原理并采用科学方法对复杂工程问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论。
- **5使用现代工具：**能够针对复杂工程问题，开发、选择与使用恰当合理的技术、资源、现代工程工具和信息技术工具，并能够理解其局限性。

工程教育认证毕业能力要求12条

- **6工程与社会：**能够基于工程相关背景知识进行合理分析，评价专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。
- **7环境和可持续发展：**能够理解和评价针对复杂工程问题的专业工程实践对环境、社会可持续发展的影响。
- **8职业规范：**具有人文社会科学素养、社会责任感，能够在工程实践中理解并遵守工程职业道德和规范，履行责任。
- **9个人和团队：**能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色。
- **10沟通：**能够就复杂工程问题与业界同行及社会公众进行有效的沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

工程教育认证毕业能力要求12条

- **11项目管理**：理解并掌握工程管理原理与经济决策方法，并能在多学科环境中应用。
- **12 终身学习**：具有自主学习和终身学习的意识，有不断学习和适应发展的能力。

主要内容

- 主要内容

从**工程**的角度出发，对信息安全从**规划与控制、需求与分析、实施与评估全过程**的描述，并结合具体的信息安全工程的实现，描述信息安全工程的内容。通过几个实施案例加强对信息安全工程的认识。

学习目标

- **目标要求**

  掌握信息安全工程的基本原理、基本方法与操作，了解系统安全工程能力成熟度模型、信息安全工程实施、信息安全风险评估、信息安全策略、信息安全工程与等级保护。

GR6.1 掌握至少一个应用领域中软件工程技术的应用方法和应用实践；

GR10.1 能够撰写报告和设计文稿，清晰阐述复杂软件工程问题；

课程具体目标

CO1:建立关于信息安全工程的基本概念，了解信息安全工程的发展历史、核心技术及最新前沿领域；

CO2:对信息安全工程基础知识、系统方法、技术标准等有一个基本了解；

CO3:掌握信息安全工程实施相关理论和方法，理解并遵守工程职业道德和规范；

CO4:建立学生的工程意识、培养工程分析问题、解决问题能力。

考核方式

- 平时考核（20%）：作业，考勤
- 期中考试（10%）：开卷考试
- 期末考核（70%）：闭卷考试

课程目录

课程目录

本章学习目标

- 了解信息安全的发展和现状，学习信息安全的目标。
- 对信息安全保障进行深入学习了解，包括模型和框架。
- 掌握信息安全工程概念、实施方法和技术支持。

第一章 信息安全工程基础

项目：是指一系列独特的、复杂的并相互关联的活动，这些活动有着一个明确的目标或目的，必须在特定的时间、预算、资源限定内，依据规范完成。

基本特征：

- 项目开发是为了实现一个或一组特定目标。
- 项目受到预算、时间和资源的限制。
- 项目的复杂性和一次性。
- 项目是以客户为中心的。

注：以上定义来源于百度百科

第一章 信息安全工程基础

工程：是科学和数学的某种应用，通过这一应用，使自然界的物质和能源的特性能够通过各种结构、机器、产品、系统和过程，是以最短的时间和最少的人力做出高效、可靠且对人类有用的东西。将自然科学的理论应用到具体工农业生产部门中形成的各学科的总称。

工程是对技术的选择、整合、集成和协同，单个的技术仅仅是工程的基础和要素。

主要职能：

- 研究、开发、设计、施工、生产、操作、管理及其他职能

注：以上定义来源于百度百科

软件工程基本定义

- 《计算机科学技术百科全书》：软件工程是应用计算机科学、数学、逻辑学及管理科学等原理，开发软件的工程。软件工程借鉴传统工程的原则、方法，以提高质量、降低成本和改进算法。

NATO(北大西洋公约组织)：把软件开发从“艺术”和“个体行为”向“工程”和“群体协同工作”转化。

第一章 信息安全工程基础

- **卓越工程师应该具备哪些素质？**

- 信息安全工程用一句话如何来概括？

第一章 信息安全工程基础

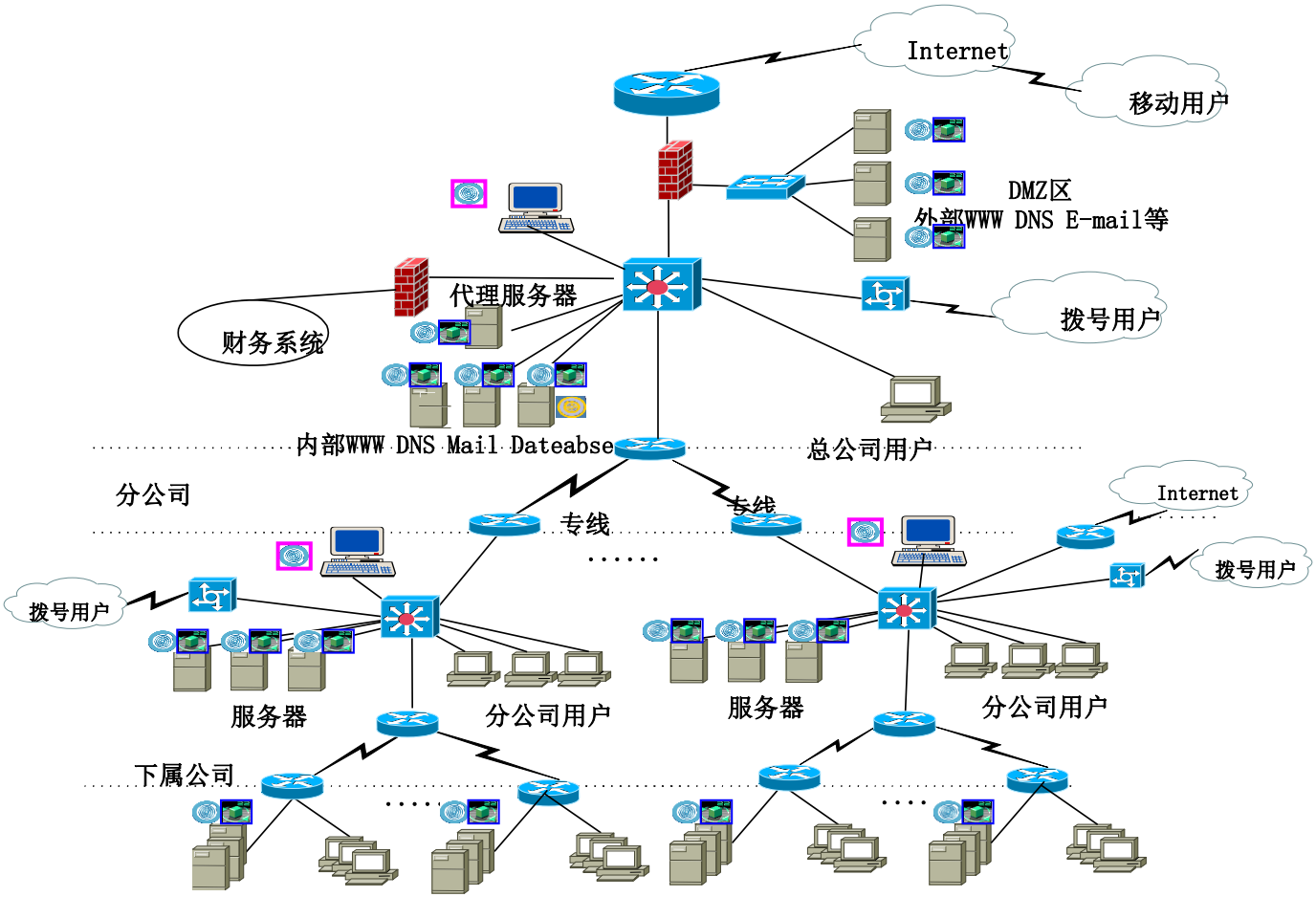
安全工程的重要性

- 如果在大楼的设计和实施阶段没有考虑消防，把楼盖完了，再去设置消防通道，必然会导致成本的上升和安全性的下降。

- 安全工程在信息化建设中的重要性有过之而无不及。

第一章 信息安全工程基础

- 某公司网络拓扑图



第一章 信息安全工程基础

- 《通信的数学理论》：信息是能够用来消除随机不确定性的东西。
- 信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。
- **信息是一种资产， 同其他重要的商业资产一样，对组织而言具有一定价值， 需要适当的保护。**
- **Cyberspace:控制论（cybernetics）+空间（space）网络空间**

第一章 信息安全工程基础

信息化建设中的案例

- **A公司开展家用电话自助刷卡支付业务**

❖ 用户可以通过其网站查询个人付款信息

❖ 第三方安全测评发现该网站存在SQL注入漏洞，可以泄露用户交易信息

—信息安全是信息的影子

1.1 信息安全的发展

- **第一时期　20世纪40~70年代　通信安全时期**
  - 主要标志：香农发表的《保密系统的通信理论》、DH体制
- **第二时期　20世纪70~80年代　计算机安全时期**
  - 计算机硬件和网络技术发展，数据传输可以通过网络实现
- **第三时期　20世纪90年代起　信息系统安全时期**
  - 互联网技术发展，网络规模的扩大化以及网络的开放性
- **第四时期　21世纪起　信息安全保障时期**
  - 主要标志：1998年NSA提出的《信息保障技术框架》IATF
- **第五时期　2009年至今**
  - Cyber Security/Information Assurance（CS/IA）

1.1 信息安全概述

- 信息安全是要在很大的范围内保护信息免受各种威胁， 从而确保业务的连续性、坚守业务损失并且使投资和商务机会获得最大的回报。

——信息安全已成为国家安全、社会安全和人民生活安全的重要组成部分。

——没有网络安全就没有国家安全。

——网络空间安全一级学科设置。

信息安全的目标

- 设备安全：信息系统设备安全
- 数据安全：确保数据本身的安全属性
- 行为安全：主体行为的过程和结果
- 内容安全：语义层次安全

信息安全的目标：设备安全

- **设备的稳定性：**保证设备在一定时间内不出故障的概率。
- **设备的可靠性：**保证设备能在一定时间内正确执行任务的概率。
- **设备的可用性：**设备随时可以正确使用的概率。

信息安全的目标：数据安全

◆ **保密性：**保证机密信息不被窃听，数据不被未授权者知晓的属性。

◆ **完整性：**保证数据的一致性，防止数据被非法用户篡改。

◆ **可用性：**数据可以随时正常使用的属性。。

◆ **真实性：**对信息的来源进行判断，能对伪造来源的信息予以鉴别。

◆ **不可抵赖性：**建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

◆ **可控制性：**对信息的传播及内容具有控制能力。

信息安全的目标：行为安全

- **行为的秘密性：**行为的过程和结果不能危害数据的秘密性，必要时行为的过程和结果也应是保密的。
- **行为的完整性：**行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的。
- **行为的可控性：**当行为过程偏离预期时，能够发现、控制或纠正。

信息安全的目标：内容安全

- 信息内容在**政治上**是健康的。
- 信息内容在**法律上**符合国家法律法规。
- 信息内容符合中华民族优良的**道德**规范。

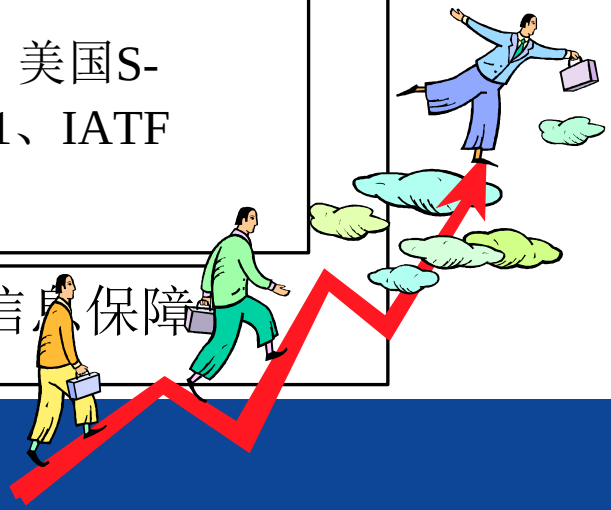
信息安全的基本范畴

- 信息资源：各种资源化的信息。
- 信息价值：信息资源优势的反映。
- 信息作用：信息实现价值过程中对环境或自身的影响或改变。
- 信息损失：信息价值的损失（量度）。
- 信息载体：记录、传输和保存信息的媒介。
- 信息环境：与信息活动有关的外部环境集合。

1.2 信息安全保障

信息保障是信息安全的新发展

20世纪40-70年代	20世纪70-80年代	20世纪90年代后
需求：保密 威胁：窃听、密码分析 标志：公钥密码体制、DES	需求：保密、完整性、可用性 威胁：非法访问、恶意代码、弱口令 标志：TCSEC	需求：保密、完整性、可用性、真实性、不可否认性 威胁：外部各方威胁 标志：美国S-3600.1、IATF
通信保密	信息系统安全	信息保障



1.2 信息安全保障

在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。

1.2 信息安全保障

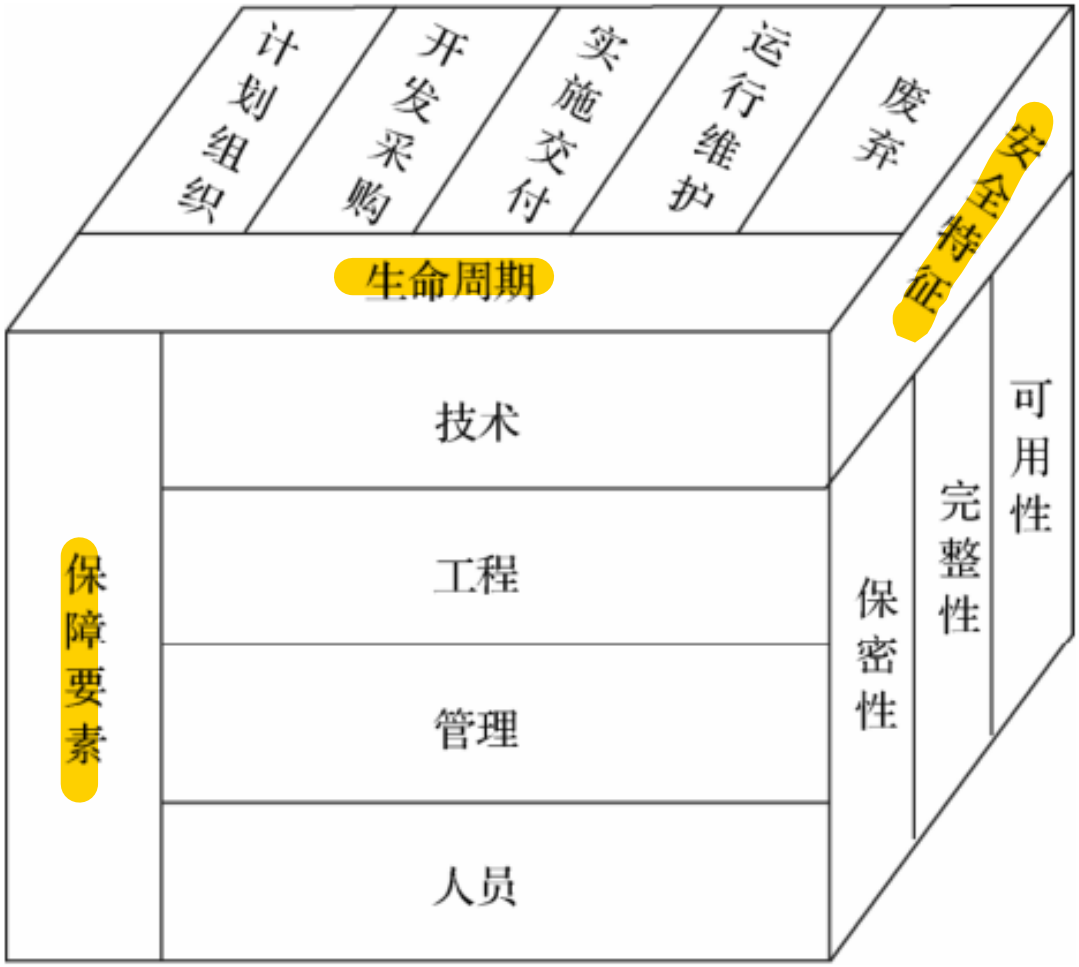
- 信息保障，强调信息安全的保护能力，同时重视提高系统的入侵检测能力、事件响应能力和快速恢复能力，关注的是信息系统整个生命周期的保护、检测、响应和恢复等安全机制，即PDRR安全模型。

1.2 信息系统安全保障模型

主要包括：

- 保障要素
- 生命周期
- 安全特征

1.2 信息系统安全保障模型



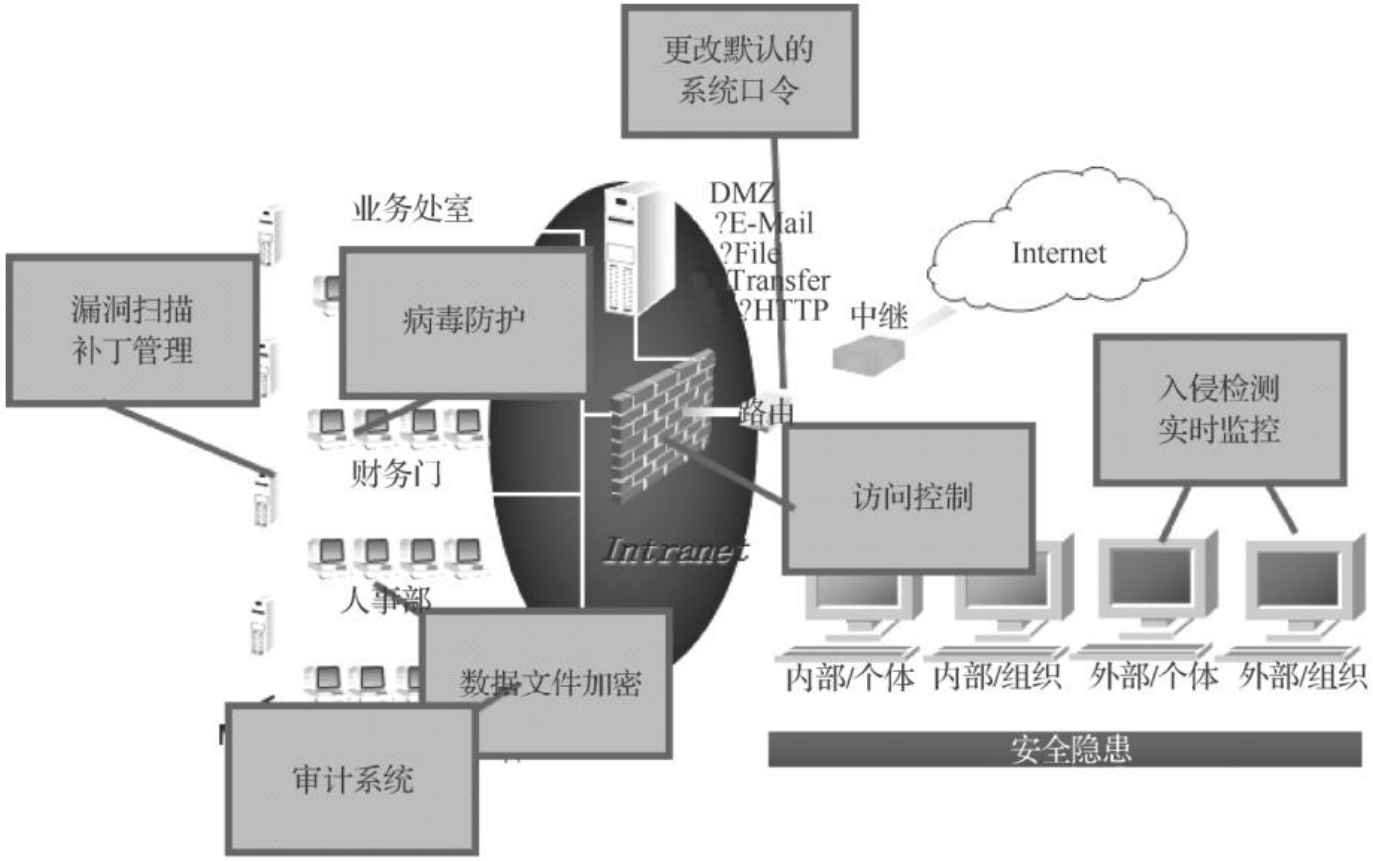
1.2 保障要素

主要包括：

- 信息安全技术体系
- 信息安全工程过程
- 信息安全管理体系
- 高素质的人员队伍

1.2 保障要素

- 信息安全技术体系



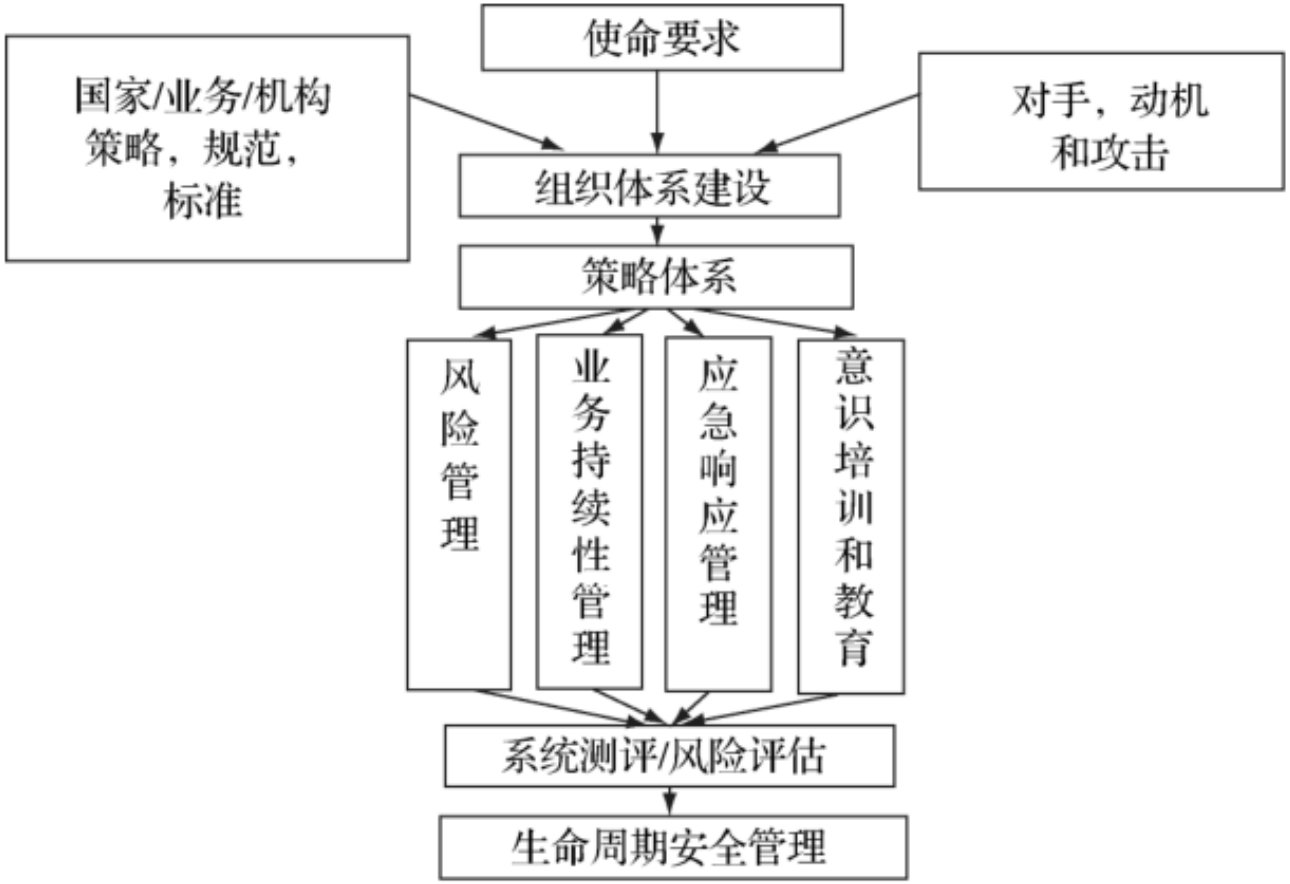
1.2 保障要素

- 信息安全工程过程

复杂的系统工程，解决安全问题应从工程学、方法论的角度来考虑，通过工程过程实现信息安全保障。

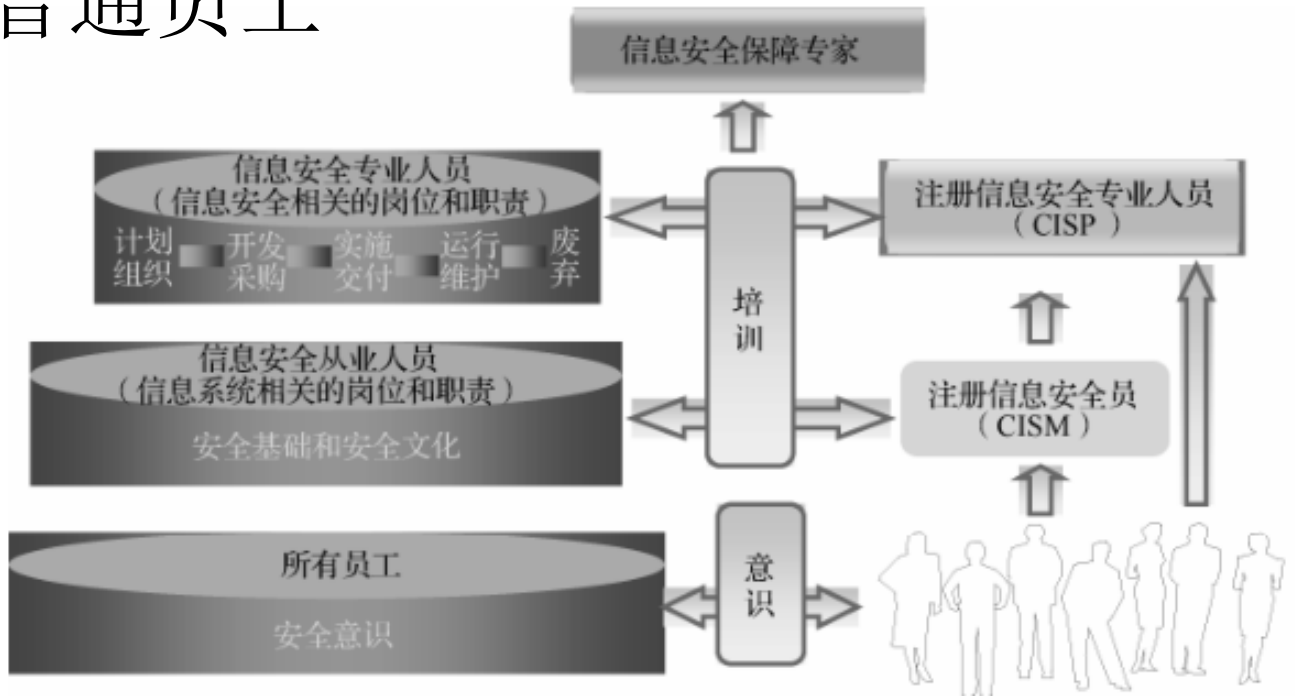
1.2 保障要素

- 信息安全管理体系



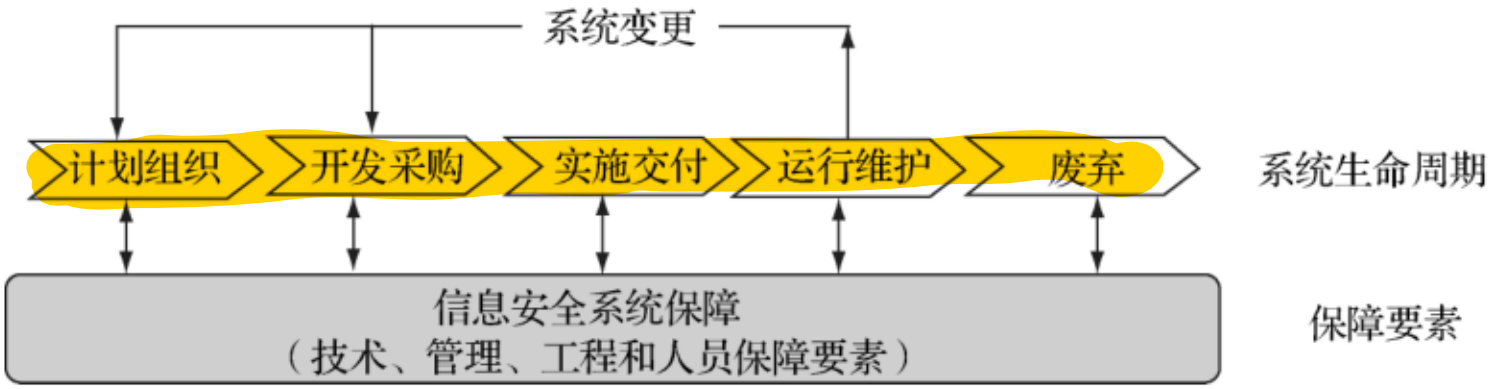
1.2 保障要素

- 高素质人员队伍
  - 信息安全专业人员
  - 信息安全从业人员
  - 所有的普通员工



1.2 生命周期

- 信息系统安全保障生命周期与安全保障要素



1.2 生命周期

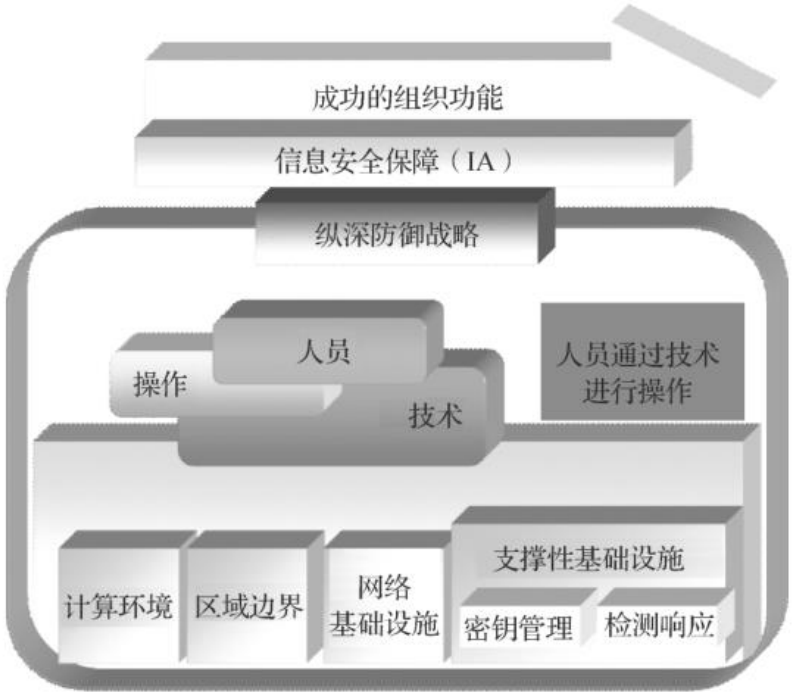
- 生命周期

整个生命周期被抽象成**计划组织、开发采购、实施交付、运行维护和废弃**等五个阶段以及在运行维护阶段由于系统变更所产生的反馈，形成生命周期完整的闭环结构。

1.2 信息保障技术框架

- 信息保障技术框架（IATF）是由美国国家安全局（NSA）指定的描述信息保障的指导性文件。

纵深防御战略



1.2 信息保障技术框架

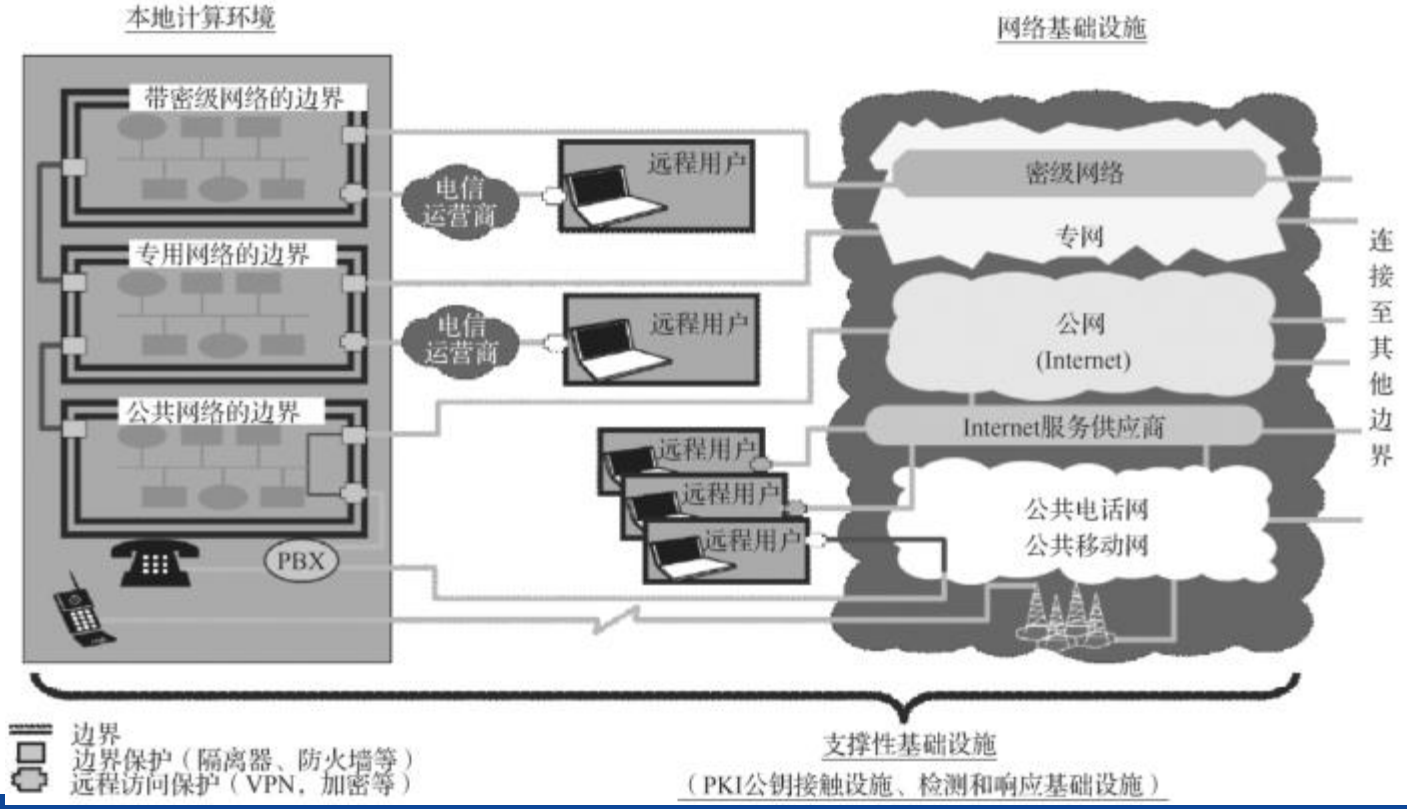
- **纵深防御战略**

核心因素：**人员、技术和操作**。

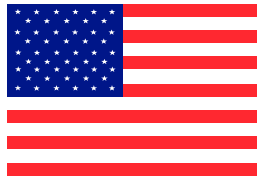
- **人员（People）**：人员是信息保障体系的核心，是第一位的要素。
- **技术（Technology）**：完善的信息安全技术体系是实现信息保障的重要手段。
- **操作（Operation）**：构成安全保障的主动防御体系。

1.2 信息保障技术框架

IATF 将信息系统的信息保障技术层面划分成 4 个技术框架焦点域：本地计算环境、区域边界、网络及基础设施、支撑性基础设施。

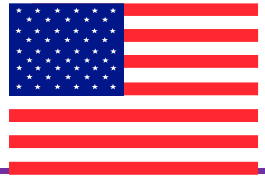


1.2 信息安全保障体系的建设



- 美国
  - 克林顿政府时期：《克林顿政府对关键基础设施保护的政策》、《信息系统保护国家计划V1.0》等。
  - 布什政府时期：《信息时代的关键基础设施保护》、《确保网络空间的国家战略》、《网络空间安全：迫在眉睫的危机》、“网络风暴”、《联邦网络空间安全及信息保护研究与发展计划》、《四年一度防务评审》、“网络风暴Ⅱ”等。

1.2 信息安全保障体系的建设



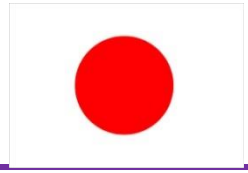
- 奥巴马政府时期：《提交第44届总统的保护网络空间安全的报告》、“模拟网络战”、《总统关于白宫国土安全和反恐组织的声明》、《网络空间政策评估—保障可信和强健的信息和通信基础设施》、成立“国家网络空间安全和通信集成中心”、“网络拂晓”、《美国国家安全战略报告》、“网络风暴III”、《网络空间国际战略》、《电邮隐私法案》等。

- 特朗普政府时期：“美国优先”、“持续介入”、“国家紧急状态法案”，人员调整、机构调整（提升国土安全部和国防部的地位）、《增强联邦政府网络与关键基础设施网络安全总统行政令》、《国家安全战略报告》 等。

1.2 信息安全保障体系的建设

- 俄罗斯
  - 1997年：叶利钦批准《俄罗斯国家安全构想》。
  - 2000年：普京批准《国家信息安全学说》。
  - 2009年：梅德韦杰夫批准《俄罗斯联邦2020年前国家安全战略》
  - 2019年：俄罗斯断网测试。

1.2 信息安全保障体系的建设



- 1999年《21世纪信息通信构想》、《信息通信产业技术战略》
- 2000年：修改《21世纪信息通信技术研究开发基本计划》、制定相关法律法规和政策。
- 2001年：“e-Japan战略”、“e-Japan重点计划”和“e-Japan2002计划”。
- 2003年：《日本信息安全综合战略》。
- 2004年：“u-Japan”。
- 2009年和2010年：《第二份信息安全基本计划》、《保护国民信息安全战略》。
- 其他措施：设立信息安全机构、政策措施提高产业竞争能力。

1.2 信息安全保障体系的建设

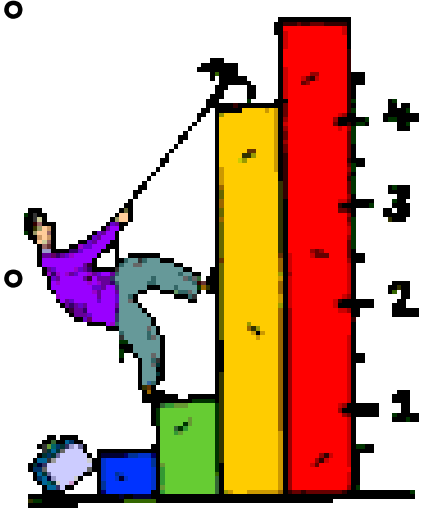
- 2000年：党的十五届五中全会要求强化信息网络安全保障体系。
- 2001年：“国家信息化领导小组”、“国务院信息化工作办公室”。
- 2008年：“国务院信息化工作办公室”职能合并至国家工业和信息化部。
- 先后颁布《保守国家秘密法》、《计算机信息系统安全保护条例》、《国家信息化领导小组关于加强信息安全保障工作的意见》、《电子签名法》、《信息安全等级保护管理办法》等。

1.2 信息安全保障体系的建设

- 2010年11月20日-12月20日：国家计算机病毒应急处理中心举办了“信息网络安全和计算机移动终端病毒疫情调查活动”。
- 2011年7月19日：中国互联网络信息中心发布《第28次中国互联网络发展状况统计报告》。
- 2012年1月31日：ZDNet公布网络防御能力排行榜显示，被不少西方人视为“网络空间入侵者”的中国，自身的网络防御能力其实很脆弱。
- 2015年7月1日：《中华人民共和国国家安全法》
- 2017年6月1日：《中华人民共和国网络安全法》

1.2 信息安全保障体系的建设

- 信息安全保障建设工作的要求：
  - 充分认识信息安全的国家战略地位。
  - 做好信息安全法的立法工作。
  - 构建和完善信息安全组织管理体制。
  - 强化国家信息安全技术防护体系。
  - 加大信息安全投入。
  - 从国家战略高度来看待信息安全人才的培养。



1.3 信息安全工程的概念

- **信息安全工程：**研究如何建立能够面对错误、攻击和灾难的可靠信息系统。
- **与软件工程的区别：**

软件工程： 保证事情发生（比如“能提供pdf格式文档的报表输出”）；

安全工程：保证事情不能发生（比如“要提供pdf格式文档的防拷贝功能”）。

信息安全工程，需要考虑到特定信息系统的安全保护需求、可能存在的安全隐患以及相应的解决方法。

1.3 信息安全工程的概念

- 例一：银行

1.3 信息安全工程的概念

- 例二：机场

1.3 信息安全工程的概念

- 例三：家庭

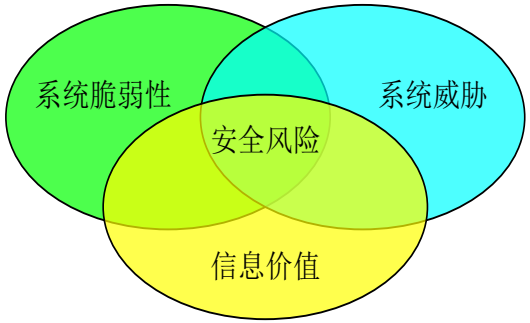
1.3 信息安全工程的概念

- 信息安全不单单是技术问题，而是策略、管理和技术的有机结合，是一项复杂的系统工程。

- 目前存在的主要现象：
  - “头痛医头，脚痛医脚”
  - 简单的安全产品的堆砌

1.3 信息安全工程的概念

- 在工程上，信息安全是与风险相联系的概念，通过风险管理与控制来实现。
- 信息安全风险是信息价值、系统脆弱性和系统威胁等三个变量的函数。



- 信息安全工程:采用SE的概念、原理、技术和方法，来研究、设计、开发、实施、管理、维护和评估信息系统的安全，是将实践流程、管理技术和当前能够得到的最好的技术方法相结合的过程。

信息安全工程应考虑的因素

- 信息安全具有全面性

  系统安全程度取决于系统最薄弱的环节。

- 信息安全具有生命周期性

  一个不断往复和上升的螺旋式的安全模型。

- 信息安全具有动态性

  系统处于不断更新、不断完善、不断进步的动态过程中。

- 信息安全具有层次性

  用多层次的安全技术、方法与手段、分层次地化解安全风险。

- 信息安全具有相对性

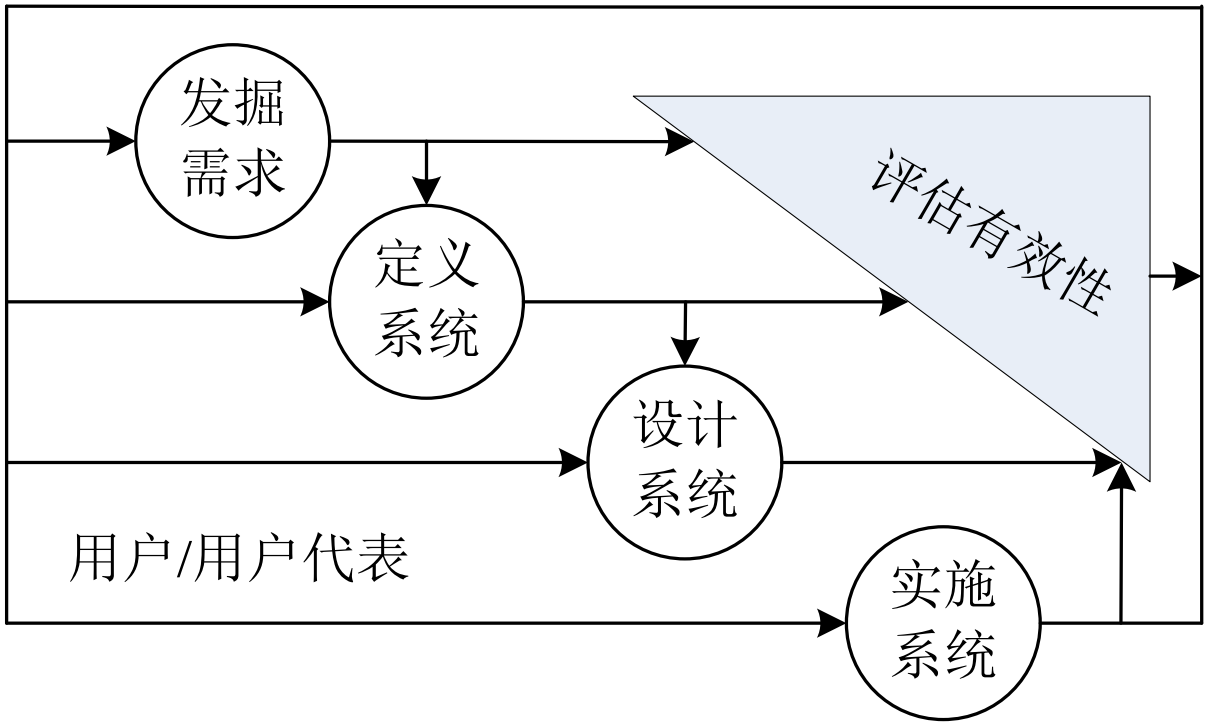
  安全是相对的，没有绝对的安全。

1.3 信息安全工程的发展

- 狭义“工程”：以某组设想的目标为依据，应用有关的科学知识和技术手段，通过一群人的有组织活动将某个（或某些）现有实体（自然的或人造的）转化为具有预期使用价值的人造产品过程。
- 广义“工程”：由一群人为达到某种目的，在一个较长时间周期内进行协作活动的过程。
- 工程是一种过程，各种工程都具有各自生命周期过程的规律。由于信息安全的特性，信息安全工程的方法是用来满足各方面的任务安全要求，与系统工程方法紧密相关。

1.3 信息安全工程的发展

- 早期的信息安全工程方法理论来自于系统工程（SE）过程的方法。



系统工程基本概念（百度百科）

- **实现系统最优化的科学。**1957年前后正式定名。1960年左右形成体系。**是一门高度综合性的管理工程技术，**涉及应用数学（如最优化方法、概率论、网络理论等）、基础理论（如信息论、控制论、可靠性理论等）、系统技术（如系统模拟、通信系统等）以及经济学、管理学、社会学、心理学等各种学科。
- **主要任务是**根据总体协调的需要，把自然科学和社会科学中的基础思想、理论、策略和方法等从横的方面联系起来，应用现代数学和电子计算机等工具，对系统的构成要素、组织结构、信息交换和自动控制等功能进行分析研究，借以达到最优化设计，最优控制和最优管理的目标。

1.3 信息安全工程的发展

- 在SE基础上，美国军方提出了信息系统安全工程（ISSE），在1994年2月28日发布《信息系统安全工程手册v1.0》。
- 1987年，卡内基 梅隆大学软件研究所提出了软件过程能力成熟度模型（CMM），1991年推出1.0版。
- 1993年5月，美国家安全局采用CMM方法学，针对安全方面的特殊需求，首次提出信息安全工程能力成熟度模型（SSE-CMM）。
- 1996年8月，公共系统安全工程（FPSSE）CMM工作组公布SSE-CMM第1个版本，1997年4月SSE-CMM评估方法。1999年4月SSE-CMM v2.0和SSE-CMM评定方法v2.0。
- 2002年3月,SSE-CMM v2.0被接受为ISO/IEC 21827《信息技术-系统安全工程-能力成熟度模型》。

1.3 信息安全工程的发展

- 在我国，信息安全工程的实施是基于等级保护制度。
  - 1994年2月，《中华人民共和国计算机信息系统安全保护条例》。
  - 1999年9月，GB17859-1999《计算机信息系统安全保护等级划分准则》。
  - 《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）》。
  - 2004年9月，《关于信息安全等级保护工作的实施意见》。
  - 2007年6月，《信息安全等级保护管理办法》。
  - 2007年7月，“全国重要信息系统安全等级保护定级工作电视电话会议”。

本章总结

- 信息实质:通过信号、指令等来调节与控制物质和能量。
- 信息安全的基本范畴。
- 信息安全工程:研究如何建立能够面对错误、攻击和灾难的可靠信息系统，在工程上是与风险相联系。
- 信息保障:确保信息和信息系统能够安全运行的防护性行为，采用“深度防御”的信息保障战略。
- 信息安全工程实施方法：ISSE过程和SSE-CMM模型。
- 在我国，信息安全工程的实施，是基于等级保护制度。

课堂作业：

1）什么是信息安全工程？
2）信息安全目标是什么？包括哪些内容？
3）信息安全保障是什么？保障模型有哪些要素和特征？
4）简单描述信息系统安全保障的生命周期。

2）课后作业：

综述近3年（2017—2020）国内外信息安全保障建设状况？（美国、俄罗斯、英国、德国、法国、意大利、荷兰、比利时、丹麦、卢森堡、西班牙、葡萄牙、瑞典、芬兰、以色列、爱尔兰、巴西、日本、印度、澳大利亚、加拿大、新加坡、韩国、土耳其、非洲、欧盟、中国）

- 格式要求：时间、部门、政策（至少3个）及相关内容，注明参考文献；
- 小组完成：3-4人组成，明确分工；
- 使用工具：MS Word或者LaTex
- 时间：11月30日前